Vexilologicans

Documentația Proiectului

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

August 29, 2024

Contents

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.

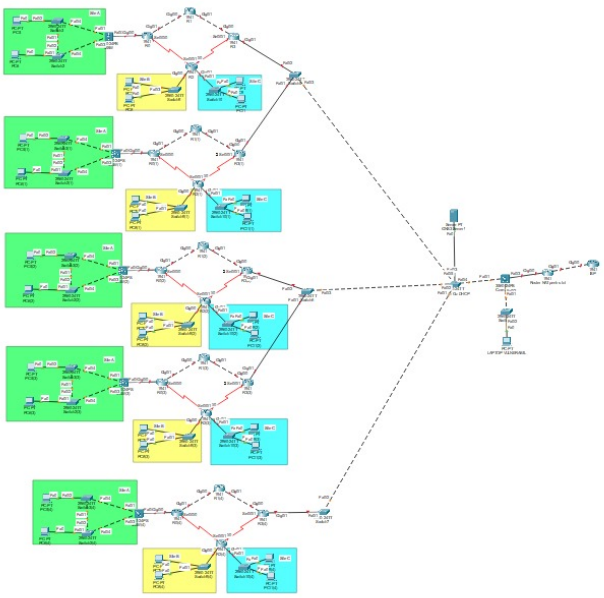

Figure 1: Topologia completă a tuturor echipei.

Chapter 1

CCNA Fizic

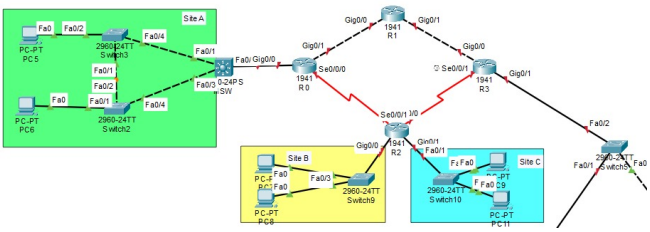

Figure 1.1: Topologia echipei noastre.

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.

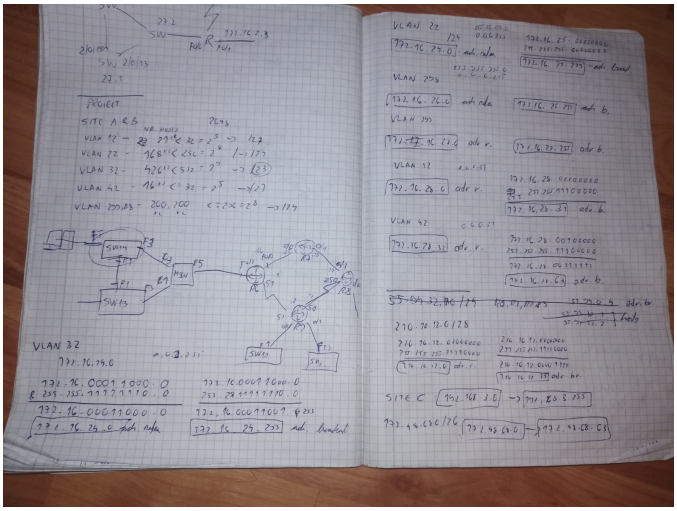

Figure 1.2: Subnetarea.

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‘.

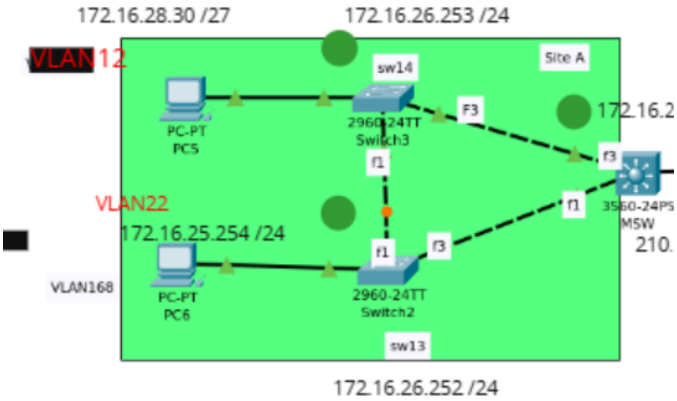

Figure 1.3: VLAN-uri diferite pentru PC-uri.

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.

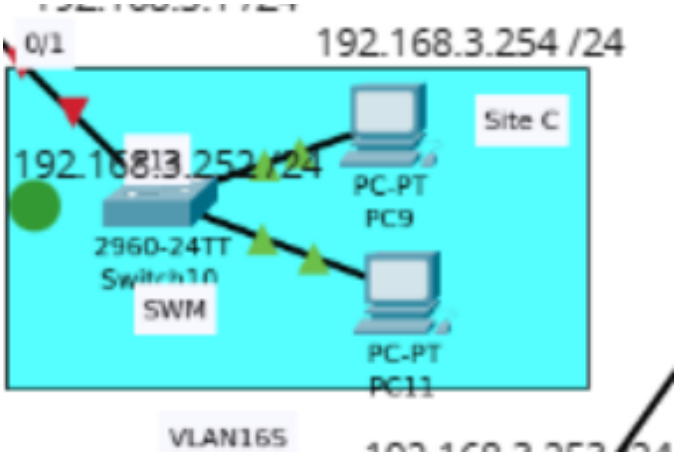

Figure 1.4: 1 singur VLAN în Site C.

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 Măsuri 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.

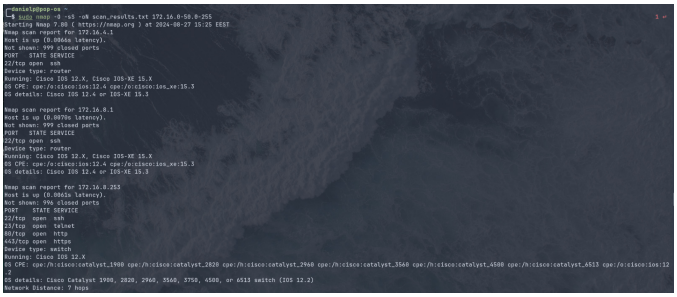

Figure 3.1: nmap scan.

```
danielp@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.

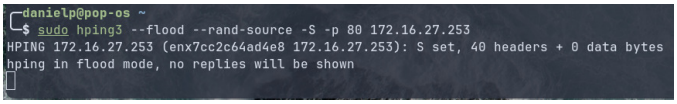

Figure 3.3: Syn flood.

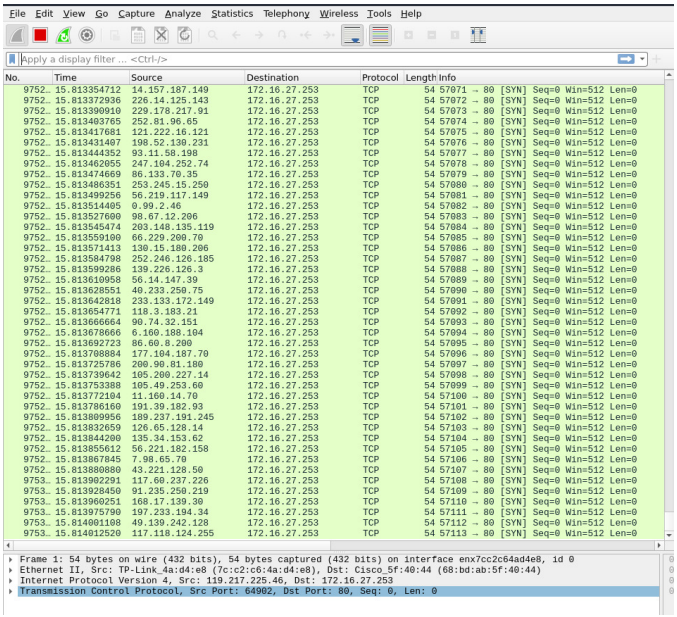

Figure 3.4: Syn flood Wireshark.

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

Figure 3.5: UDP flood.

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

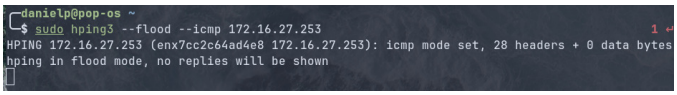

Figure 3.6: ICMP flood.

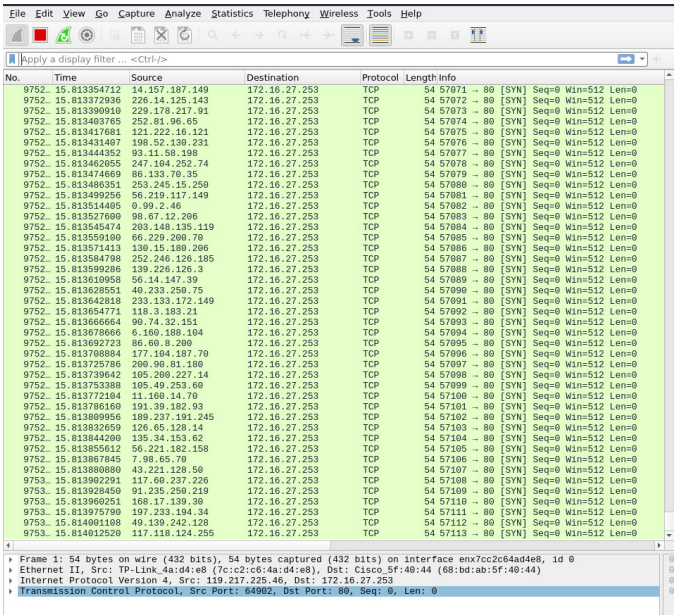

Figure 3.7: ICMP flood Wireshark.

3.1.3 Atac de tip DHCP Starvation

Am derulat acest atac prin intermediul Tool-ului Yersinia.

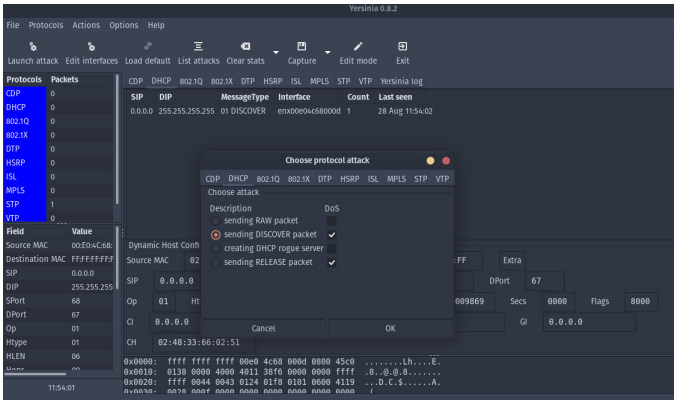

Figure 3.8: DHCP starvation.

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.

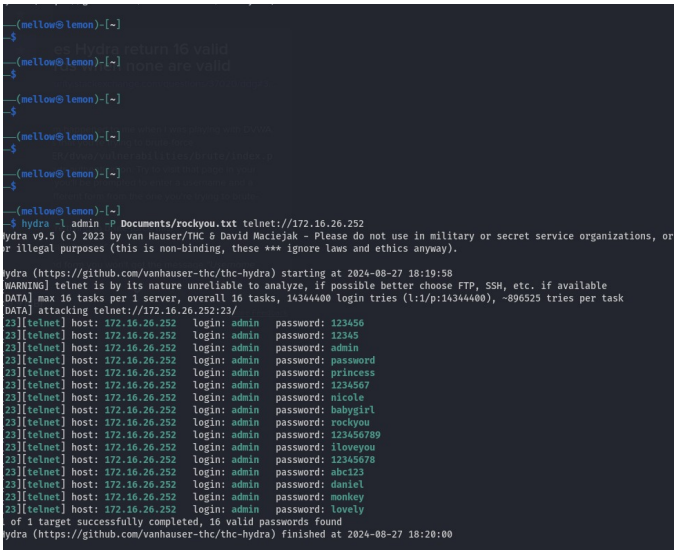

Figure 3.9: Password cracked successfully.

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.

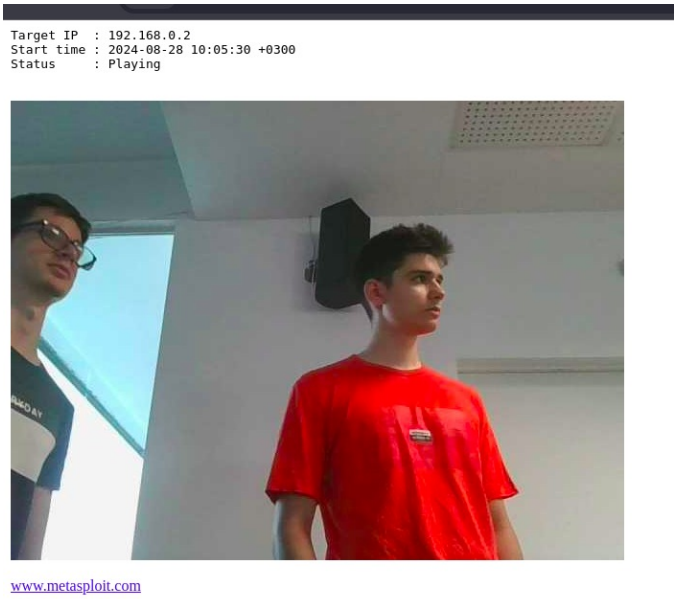

Figure 3.10: Camera PC-ului atacat.

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.