Vlan pe dreapta

PROIECT CYBER-OPS

PRACTICA VARA 2024

LĂCĂTUȘU TUDOR-BOGDAN
BOTICEAN ȘTEFAN-ANDREI
PERIAT CRISTIAN
GAFTON NICOLAS-ADELIN
JUGĂNARU GEORGE-RĂZVAN
DEHELEAN RĂZVAN-LUCIAN

OVERVIEW PROJECT

P1

Partea 1: Reteaua fizica

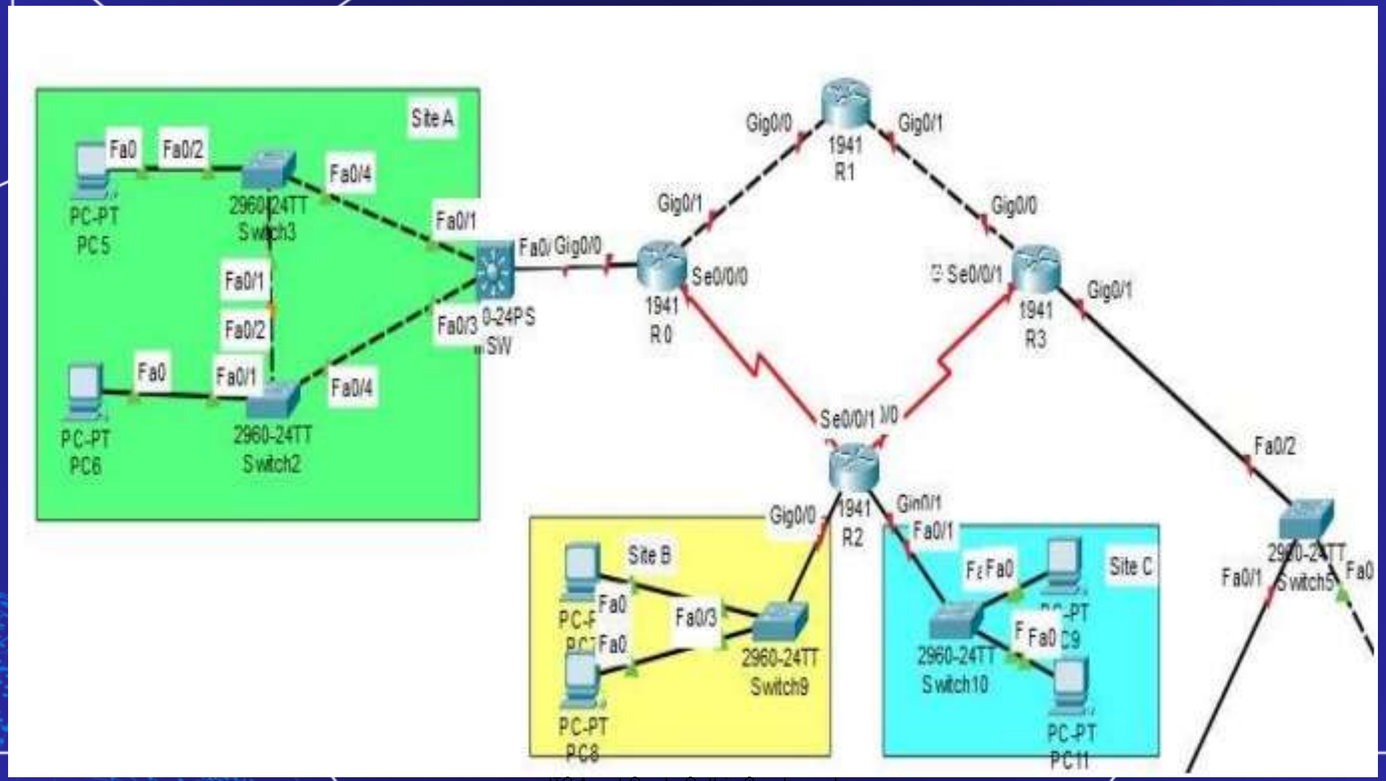
P2

Partea 2: GNS3

P3

Partea 3: Blue Team/Red Team

PRTEA 1



ITC Avant Garde Gothic Condensed

Alocare IP și Subnetare:
- Subnetarea rețelelor se face în acord cu cerințele stabilite.
- Se calculează corect necesarul de adrese IP.

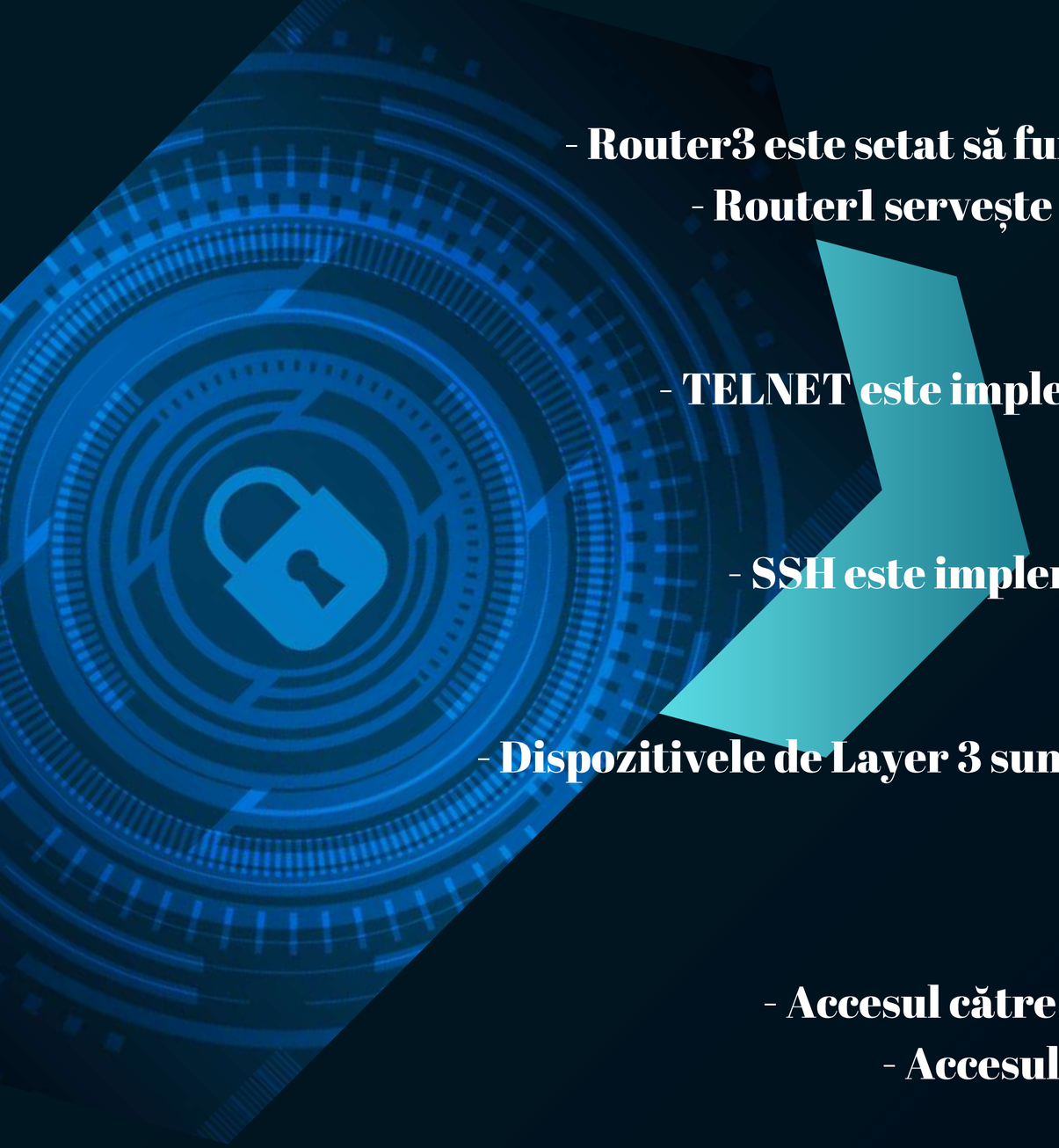
Configurare IP-uri:
- PC-uri: Ultimele adrese IP disponibile sunt alocate pentru PC-uri.
- Routere: Primele adrese IP disponibile sunt utilizate pentru routere.
- Switch-uri: Penultimele adrese IP disponibile sunt rezervate pentru switch-uri.

Configurare VLAN-uri:
- VLAN-urile sunt configurate și porturile sunt setate conform topologiei definite.

Configurare IP și Rutare

Configurare Rootbridge și STP:
- Rootbridge este configurat eficient, iar protocolul STP este implementat optim.

Configurare OSPF:
- Protocolul OSPF este configurat pe routerele din topologia rombului (R0, R1, R2, R3).



1 DHCP

- Router3 este setat să funcționeze ca server DHCP pentru dispozitivele din SITE A.
- Router1 servește ca server DHCP pentru dispozitivele din SITE B și C.

2 TELNET

- TELNET este implementat pe toate dispozitivele de Layer 2 (Switch-uri).

3 SSH

- SSH este implementat pe toate dispozitivele de Layer 3 (Routere).

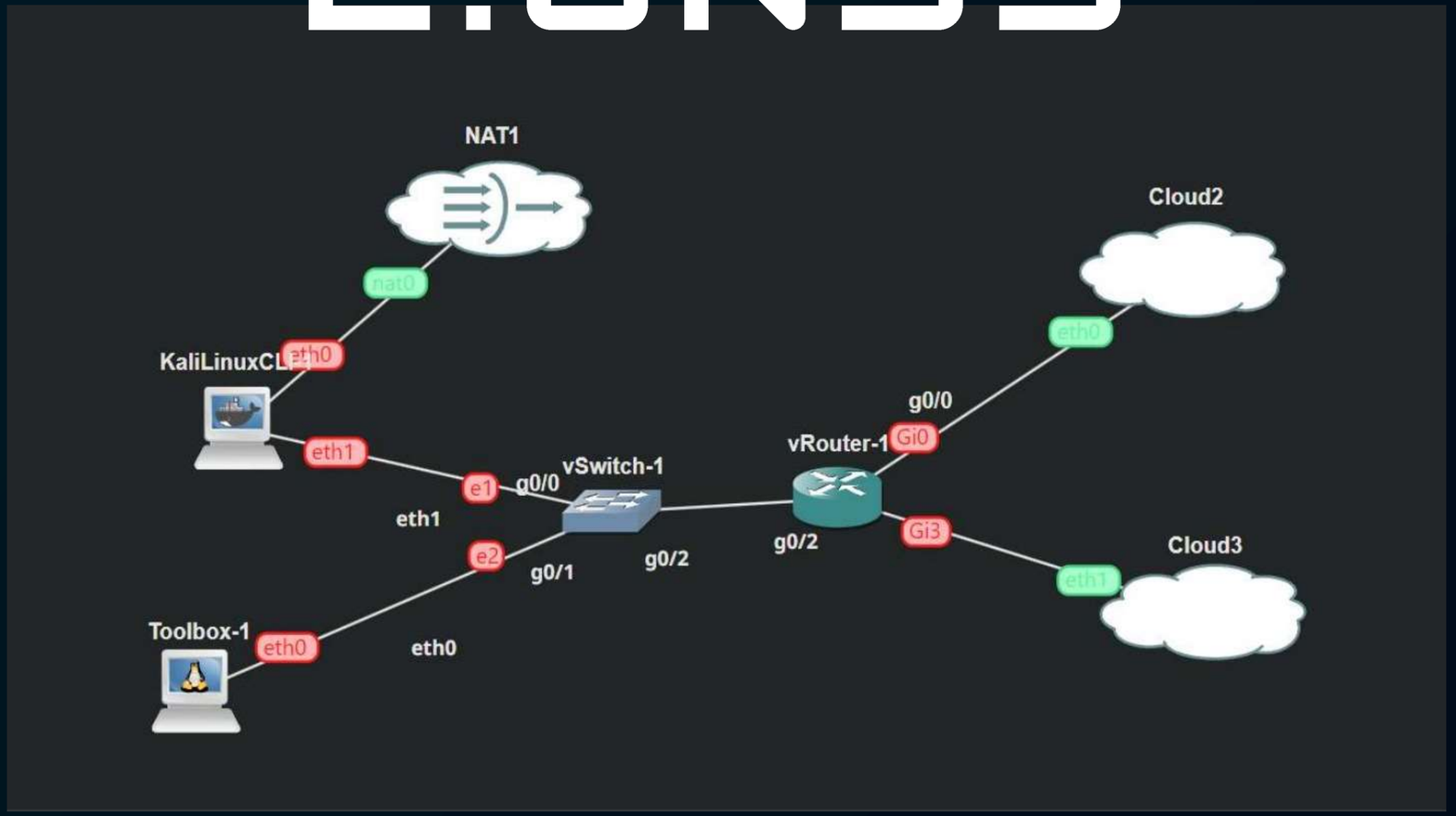
4 NTP

- Dispozitivele de Layer 3 sunt configurate ca servere NTP, iar cele de Layer 2 ca clienți NT

5 ACL

- Pe Router2:
- Accesul către Site C este restricționat la celelalte două site-uri.
- Accesul este permis doar la un singur PC din Site B.

PARTEA 2:GNS3



Partea 2:Gns3

Configurații IP și Conectivitate
- Routerul principal trebuie să primească un IP automat prin DHCP de la un switch configurat special.
- Configurarea OSPF asigură conectivitatea cu rețeaua fizică și permite utilizarea rutelor statice pentru accesul la rețeaua wireless.

Implementarea NAT
- NAT static este configurat pe routerul din GNS3 pentru fiecare PC din rețea, asigurând astfel conectivitatea între mediul de emulare și rețeaua reală.

Integrarea Kali Linux
- Kali Linux este conectat la NAT și configurat pentru testarea și securizarea rețelei.

PARTEA 3 : CYBERSECURITY

ATACURI

Atac de Recon:
- Se colectează informații despre rețea pentru a identifica vulnerabilități posibile.

Syn Flood:
- Un server este suprasolicitat prin trimiterea de pachete SYN, fără a finaliza conexiunile, blocând astfel accesul legitim.

ICMP Flood:
- O rețea este inundată cu pachete ICMP (ping), ceea ce duce la copleșirea și blocarea resurselor.

UDP Flood:
- Un volum mare de pachete UDP este trimis pentru a satura lățimea de bandă și a perturba serviciile.

ICMP AMP:
- Se exploatează serverele de reflecție pentru a amplifica traficul ICMP trimis către o țintă, provocând astfel un atac de tip DoS.

DHCP Starvation:

- Alocarea adreselor IP este blocată prin epuizarea tuturor adreselor disponibile din serverul DHCP.

MitM (ARP Spoofing):

- Traficul dintre două dispozitive este interceptat și modificat prin falsificarea adreselor ARP.

Atac STP:

- Topologia rețelei este perturbată prin injectarea de mesaje STP false, pentru a manipula traficul.

Spargerea parolei de Telnet:

- Parola Telnet a unui dispozitiv este spartă folosind forța brută, obținând astfel acces neautorizat.

Clonarea unui Site Legit:

- Se creează o clonă a unui site legitim, cum ar fi putty.org, pentru a înșela utilizatorii.

Crearea unui Payload:

- Un payload malițios este generat și plasat pe un server web local.

Activarea Serverului Web:

- Serverul Apache este pornit pentru a livra payload-ul către victimă.

REVERSE SHELL

Exploatarea:

- Victima descarcă și execută payload-ul, deschizând astfel o sesiune de control de la distanță (reverse shell) pe propriul sistem.

Lansarea unui Ransomware:

- Un ransomware este descărcat și rulat, criptând datele victimei pentru a cere o recompensă.

DEFENSE

Storm-Control împotriva DoS:

- Traficul de broadcast și multicast este limitat pentru a preveni atacurile de tip DoS, iar interfața este închisă dacă se depășește limita stabilită.

DHCP Snooping împotriva DHCP Starvation:

- Traficul DHCP este monitorizat și filtrat pentru a preveni alocarea frauduloasă de adrese IP.

Protecție împotriva MiTM (ARP Spoofing):

- Pachetele ARP falsificate sunt verificate și blocate; se limitează numărul de adrese MAC pe port.

Protecție împotriva atacurilor STP (BPDU Guard):

- Porturile care primesc mesaje BPDU sunt dezactivate automat pentru a preveni buclele neintenționate.

V A
MUTUMIN!