**Practica 2024 - Proiect de integrare a cunoștințelor**

Acest produs este proprietatea Asociației Centrului de Instruire Savnet și poate fi utilizat numai în evaluările Asociației Centrului de Instruire Savnet. Nerespectarea acestei prevederi induce răspunderea părții vinovate conform reglementărilor în vigoare.

Toate punctele rezolvate trebuiesc documentate si inclusiv justificate (screenshot). La final, pe langa prezentarea proiectului, se va trimite inclusiv documentatia facuta.

**Continut**

**Partea I – CCNA (fizic)**  … 2

**Partea II – CCNA (GNS3)** … 5

**Partea III - CyberSecurity** … 6

|  |
| --- |
| **Partea I – CCNA (fizic)** |

**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 |

**Cerinte:**

1. Subnetați rețelele în funcție de tabelul de mai sus, luand in considerare nr de hosti și adresele IP de pornire mentionate. Calculati x optim pentru Site A & B.
2. Configurați Vlan-urile si modurile porturilor conform topologiei.
3. In Site C se va folosi vlan 1 pentru un PC si vlan 2 pentru alt PC. Amandoua PC-uri facand parte din acelasi SUBNET.
4. Configurați EFICIENT Rootbridge-ul din Site A si inclusiv folositi optiunea mai buna a STP-ului.
5. Configurați IP-urile subnetate mai sus astfel:
   1. PC-uri - ultimele IP-uri disponibile
   2. Router – primul IP disponibil
   3. Switch-uri - penultimele IP-uri disponibile
   4. În partea de WAN puteți configura după cum doriți din plaja aferentă de IP-uri
6. Configurați OSPF pe toate routerele cu Passive interface unde este necesar, exceptand rețeaua dintre MSW si R0 si testati daca in reteaua interna fiecare are conectivitate cu fiecare.
7. Configurați ruta default dinspre MSW spre R0.
8. Rutare statică de la R0 către rețelele lipsa.
9. Testati Conectivitatea !
10. Configurați R3 ca server de DHCP pentru LAN-urile din Site A.

Atentie DNS = 8.8.8.8

1. Configurați R1 ca server de DHCP pentru LAN-urile din Site B & C.

Atentie DNS = 8.8.8.8

1. Pe router-ul R0 configurați NAT pentru rețelele interne și testați functionalitatea lui.

NAT static pentru fiecare PC si doar 1 Switch pentru test.

Restul Switch-urilor vor avea PAT.

1. Configurați Telnet pe toate Device-urile de L2.
2. Configurați SSH pe toate Device-urile de L3.
3. Configurați serviciul de NTP client pe toate echipamentele de L2 din infrastructură, unde sv de NTP este echipamentul de L3 al fiecarei retele.
4. Configurați ACL-uri astfel incat:
   1. Sa poti accesa Site C doar din celelalte 2 Site-uri
   2. Sa poti accesa doar un PC (la alegere) din Site B

Pentru toate grupele:

Trebuie configurat:

\*pentru reteaua dintre Core-MSW si “Router NAT pentru tot” veti alege un range de IP-uri cu /24\*

* “Router NAT pentru tot” cu OSPF si toate regulile de NAT static de care va fi nevoie ca fiecare PC sa aibe acces la internet. Interfata care duce catre ISP va fi configurata sa primeasca IP prin DHCP.
* Core-MSW are nevoie de IP-uri si OSPF activ. Configurati cu IP la alegere pentru reteaua Laptop-ului vulnerabil.
* Switch-Cu-DHCP are nevoie sa fie configurat un DHCP ce va emite IP pentru reteaua de tip multi-access.

|  |
| --- |
| **Partea II – CCNA (GNS3)** |

Obligatoriu: Topologia sa fie la fel cu cea din poza.

Optional: Puteti adauga device-uri cum doriti voi, insa trebuie sa exista un router ce conecteaza 2 CLOUD-uri. Aici va lasati voi imaginatia sa curga.

Aceasta retea va fi legatura voastra cu laptop-urile cu acces prin wireless.

Scenariu:

Ati primit doar un model de topologie de la un necunoscator. Voi, avand experienta necesara, veti putea configura IP-urile dupa bunul plac. Insa aici tine si de networking in realitate, adica nu folositi aceleasi IP-uri ca si celelalte grupe.

Observatie:

Pentru a putea fi folosit Kali Linux in gns3, va trebui sa il conectati la un NAT si sa primiti IP prin DHCP. Dupa ce aveti IP, dati urmatoarele comenzi:

* apt update && apt upgrade
* apt install net-tools
* apt install iputils-ping
* apt install iproute2

Requirement:

Router-ul pe interfata de g0/0 trebuie sa primeasca IP prin DHCP-ul configurat pe **Switch-Cu-DHCP.**

Configurati OSPF pentru conectivitatea cu reteaua fizica, iar pentru accesul la reteaua wireless veti crea rute statice in functie de IP-urile device-urilor.

Se va implementa un NAT static pe router-ul din GNS3 pentru fiecare PC din retele, astfel incat sa se poata realiza conectivitatea intre mediul de emulare si real.

(Puteti face si pentru device-urile de infrastructura)

A diagram of a computer network

Description automatically generated

|  |
| --- |
| **Partea III - CyberSecurity** |

Ati fost angajati sa testati infrastructura creata precedent. Modalitatile prin care se doreste verificarea acesteia sunt:

* + - 1. Atac de Recon
      2. Atacuri de tip DoS:
         1. Syn Flood
         2. ICMP Flood
         3. UDP Flood
         4. ICMP Amplification
      3. Atac de tip DHCP Starvation
      4. Atac de tip MitM bazat pe arp spoofing
      5. Atac pentru STP
      6. Atac pentru a sparge parola de telnet a Switch-urilor (HINT: Hydra)

Pe langa verificarea infrastructurii, se va incerca un atac pe angajati. Va fi nevoie sa creati un exploit pentru un remote shell. Incercati sa faceti un scenariu prin care oamenii ar fi interesati sa acceseze acel exploit. (HINT: setoolkit).

**Acum ca ati reusit sa descoperiti ce atacuri functioneaza, va trebui sa implementati modalitati de anularea tuturor atacurilor reusite precedent.**

**Neajustarea securitatii semnifica task incomplet => nu primiti salariul pentru proiectul in cauza.**

Sugestii:

* Rate limit
* DHCP snooping
* Dynamic Arp Inspection
* Switchport portsecurity
* ACL
* BPDUguard
* Root Guard

**OPTIONAL: Testati infrastructura tuturor grupelor, daca primiti acordul lor.**

**Orice alt atac este binevazut (daca nu a functionat atacul, aratati dovezi ca ati incercat si documentati pasii facuti si unde au aparut probleme)**

**Echipa care va ataca fara consimtamant, va fi penalizata.**

**Punctul final:**

Ati terminat cu conectivitatea din fiecare retea…insa mai aveti putin ! Verificati daca puteti accesa prin ping laptopul vulnerabil. Daca puteti…abia acum vine partea dificila.

Cautati pe google CVE-2017-0144 si vedeti despre ce e vorba.

Toata lumea pana in momentul acesta trebuie sa fie gata cu toate celelalte cerinte. Va veti ajuta toti in exploatarea acestei vulnerabilitati. Testati prin mai multe metode.

Intrebati coordonatorul pentru HINT-uri.

Fiti creativi !