Sujet 4 - SMURF Attack
(4 personnes)

23 octobre 2023

1 Votre histoire

Vous êtes quatres personnes vous vous êtes donné pour défi de faire attaquer l'un d'entre vous par une autre machine. Chacun va proposer une seule méthode, lequel fera la meilleure attaque par rebond ? Le protocole central de ce sujet sera ICMP.

2 Tous les joueurs

Vous devez avoir un programme python utilisant scapy en écoute qui va permettre d'afficher lors de la réception d'un ping :

- Son type (echo / reply)
- L'adresse MAC Source
- L'adresse MAC Destination
- L'adresse IP Source
- L'adresse IP Destination

3 Joueur 1 : Smurf attack basique

De base l'attaque par rebond consiste à envoyer un paquet avec en adresse source une adresse de broadcast pour que la réponse soit envoyée à tout le monde. Testons pour voir si cela fonctionne !

Votre programme devra donc envoyer à tout le monde un paquet ICMP echo contenant en adresse MAC source l'adresse de broadcast (FF :FF :FF :FF :FF :FF). Est-ce que la réponse est bien envoyée à tout le monde ? Que ce soit le cas ou non, testez cette fois avec l'adresse IP source en broadcast.
Si rien ne fonctionne, proposez une autre méthode (autre que les trois autres bien sûr).

4 Joueur 2 : Smurf attack niveau 2

Cette fois, on va taper sur la couche 2 de TCP/IP. Vous allez envoyer des paquets avec les caractéristiques suivantes :

— Adresse Mac source : Vous
— Adresse Mac de destination : Joueur 3
— Adresse IP Source : Joueur 2
— Adresse IP destination : Joueur 1

Pour que cette expérience fonctionne, il faudra sans doute que le joueur 3 active le forwarding sur sa machine. Commencez par un seul paquet puis après vous en ferez plusieurs.

5 Joueur 3 : Smurf attack niveau 3

Vous allez envoyer des paquets ICMP "echo" forgés en couche 3 avec en adresses :

— IP Src : Joueur 1
— IP Dst : Joueur 2

Si tout se passe bien alors c'est le joueur 1 qui doit recevoir le "reply".

6 Joueur 4 : Level 4

Comme les autres joueurs vous allez tenter de faire l'attaque par rebond mais cette fois en utilisant un protocole très "complexe" (lol) de la couche 4 -> Le procotole UDP ! Pour que cela fonctionne il faut qu'une machine accepte de se mettre dans un état vulnérable à cette attaque car elle doit activer le service "echo" de la couche UDP. Pour se faire la victime (qui servira de rebond pour attaquer une autre machine) devra utiliser les commandes ci-dessous :

```
sudo apt install xinetd
```

Puis elle devrait tout simplement modifier le fichier /etc/xinetd.d/echo et changer le "yes" devant "disable" en "no" sur la version UDP. Ensuite il devra redémarrer le service xinetd avec :

```
sudo service xinetd restart
```

Maintenant à vous d'envoyer un paquet echo sur le port 7 de la victime en indiquant une adresse de broadcast en source. Votre programme python doit pouvoir le faire mais si vous souhaitez tester sur la victime que tout est bon, vous pouvez utiliser netcat :

```
nc -uvn ip_de_la_machine 7
```

Si tout marche bien alors lorsque vous écrivez un message vous devez recevoir ce même message. Il ne vous reste plus qu'à faire la même chose avec votre programme et faire en sorte que ce soit quelqu'un d'autre qui reçoive la réponse.

Utilisez Wireshark pour vérifier si tout se passe bien et si ce n'est pas le cas, n'hésitez pas à regarder pourquoi et à l'expliquer dans le fichier readme.

7 Ressources

Vous disposez de pas mal de ressources sur Internet pour réaliser cette activité comme par exemple :

— ChatGPT : Il sera très frileux si vous lui proposez directement ce sujet mais il pourra vous aider si vous lui demandez des fonctions simples.

8 Trop facile ?

Il vous reste 3h et vous avez déjà fini ? Allez plus loin, allez au-délà de la note de 4/4 en implémentant un système de détection de SMURF attack pour chacune des méthodes appliquées par les joueurs.