SIVAPALAN Thushanth
GAMEIRO Théo
MARTINS Alexandre

19/05/2022

Documentation failles de sécurités :

1°/ *Attaque DDOS :*

Notre infrastructure, contient un site internet en « https », aucun service de blocage d'IP est installé. Nous avons mis en place un logiciel qui se nomme psad, qui est un logiciel linux qui bloque les ports scan. De base, le logiciel empêche les scans de ports et bloque en même temps les machines qui tentent d'attaquer les services d'une machine. Nous avons donc des ports activés, il existe donc des failles d'intrusions, ainsi qu'un risque de DDOS.

```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-05-19 14:07 PDT
Nmap scan report for 192.168.1.12
Host is up (0.0000040s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
443/tcp  open  https
3306/tcp open  mysql
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 11.79 seconds
```

Le site internet est en HTTPS, nous avons mis en place le site sur le port 443, donc il est protégé par un certificat SSL, qui est malheureusement auto-signé. À savoir que le site est ainsi protégé, par les attaques de sniffer avec le logiciel Wire Shark.

Le pare-feu mit en place possède des règles qui permette de limiter les attaques qui arriveront sur la carte WAN, aucun service stoppant les attaques de DDOS ont été mis en place. Ainsi les attaquants extérieurs ne pourront pas attaquer le pare-feu sans connaitre le port, le pare-feu est en https donc logiquement le port par défaut devrait être 443, mais nous l'avons changé le port du pare-feu en 8443.

2°/ *Attaque Wifi* Publique :

La faille existant sur le dispositif wifi publique, est la complexité du mot de passe intégré, le mdp est : « toto ». Ainsi, une simple attaque de brute force afin de casser le mot de passe est possible. Nous avons mis en place une sécurité WEP, qui est très faible sur l'aspect sécurité.