TP Nmap

07-12-2023

Dans ce TP, vous devez rendre un document pdf avec les commandes utilisées pour répondre à chaque question et des captures d'écran de l'exécution de ces commandes. Si les captures d'écran de la commande ne peuvent pas être enregistrées dans une seule capture d'écran, prenez une capture d'écran du début et de la fin de l'exécution.

Pour les questions où il vous est demandé d'écrire le résultat dans un fichier, vous devez nommer le fichier avec le numéro de l'exercice et de la question, mettre le tout dans un fichier zip nommé avec votre numéro d'inscription. Ce fichier doit être soumis avec votre rapport TP.

Voici les domaines et la plage IP attribués à chaque étudiant. Dans les exercices 2 et 3, chaque étudiant doit travailler uniquement sur les domaines et les sous-réseaux qui lui sont attribués.

```
User,Domain 2,Domaine 2,Net
21005,essahraa.net,www.bnm.mr,102.216.27.0/24
21006,somelec.mr,mattel.mr,102.214.129.0/24
21007,radiomauritanie.mr,finances.gov.mr,82.151.69.0/24
21070,masrvi-mobile.com,presidence.mr,102.219.207.0/24
21071,primature.gov.mr,economie.gov.mr,102.36.185.0/24
22005,bci-banque.com,madar.mr,41.138.128.0/24
22010,madar.mr,masrvi-mobile.com,41.188.120.0/24
22015,msgg.gov.mr,ar.taqadoumy.mr,41.188.122.0/24
22016,finances.gov.mr,bci-banque.com,102.36.184.0/24
22022,presidence.mr,bea.mr,82.151.65.0/24
22027,saharamedias.net,www.bankily.mr,41.223.99.0/24
22033,www.bankily.mr,somelec.mr,102.216.27.0/24
22038,cnss.mr,primature.gov.mr,102.214.129.0/24
22039,economie.gov.mr,www.ami.mr,82.151.69.0/24
22045,ar.taqadoumy.mr,radiomauritanie.mr,102.219.207.0/24
22055,mauritaniaairlines.mr,saharamedias.net,102.36.185.0/24
22058,www.bnm.mr,alakhbar.info,41.138.128.0/24
22063,mattel.mr,mauritaniaairlines.mr,41.188.120.0/24
22067,www.ami.mr,essahraa.net,41.188.122.0/24
22073,alakhbar.info,msgg.gov.mr,102.36.184.0/24
22075,bea.mr,ansade.mr,82.151.65.0/24
22087,ansade.mr,cnss.mr,41.223.99.0/24
```

Exercice 1

Dans cet exercice, vous devez être connecté au réseau local de SupNum.

1. Trouver tous les hôtes actifs sur le réseau et enregistrer le résultat dans un fichier au format greppable de nmap .
2. Combien de points d'accès Unifi sont installés sur le réseau.
3. Trouver les ports populaire ouverts sur supnum.mr.

4. Identifier les services des ports ouverts sur le serveur supnum.mr.

Exercice 2

Dans cet exercice, vous travaillerez avec le réseau associé à votre matricule.

1. Trouver tous les hôtes actifs sur le réseau et enregistrer le résultat dans un fichier au format greppable de nmap.
2. En utilisant uniquement la liste des IP des hôtes actifs, scanner les ports suivants : 21,22,25,80,81,443,6443,8080. Vous devez enregistrer le résultat de l'analyse dans un format de fichier nmap grepable.
3. Avec nmap, Identifier le système d'exploitation des hôtes actifs.

Exercice 3

Dans cet exercice, vous travaillerez avec les domaines associé à votre matricule.

```
vpn
www
mail
app
ftp
zmail
ns
```

1. Exécuter une énumération DNS à l'aide de dnsenum. Utiliser la liste ci-dessus comme dictionnaire pour le bruteforce des sous-domaine. Assurez-vous que vous n'utilisez pas l'option de recherche inversée (reverse lookup).
2. Exécuter une énumération DNS à l'aide de dnsrecon. De plus, assurez-vous d'effectuer l'énumération en utilisant `crt.sh` et d'enregistrer la sortie dans un fichier csv.
3. Identifier pour vos deux domaines le CMS Web utilisé.
4. Identifier les top ports nmap pour vos deux domaines.
5. Pour les ports ouverts, identifier les services en cours d'exécution et enregistrez les résultats dans un format nmap grepable.

Exercice 4

Dans cet exercice, vous devrez configurer un client wireguard. Cela peut être fait avec les instructions suivantes.

```
sudo apt update -y
sudo apt install wireguard -y
#Generate wireguard keys
wg genkey | sudo tee /etc/wireguard/private.key
sudo chmod go= /etc/wireguard/private.key
sudo cat /etc/wireguard/private.key | wg pubkey | sudo tee /etc/wireguard/
    public.key

#Client config
```

```
sudo nono /etc/wireguard/wg0.conf
#####
[Interface]
PrivateKey = base64_encoded_peer_private_key_goes_here
Address = 192.168.7.8/32

[Peer]
PublicKey = L3VaWh5gzTMTUPxAwLQXSwowsrgE5X2k/PkQF1a1Z1c=
AllowedIPs = 192.168.7.1/32
Endpoint = 34.125.83.187:51820
####
```

1. Trouver les hôtes actifs sur le réseau 192.168.7.0/24 et sauvegarder la liste de ces Ip dans un fichier target.txt.
2. Utiliser nmap pour scanner les IP du fichier target.txt.
3. Identifier tous les ports ouverts sur le serveur 192.168.7.1.
4. Quel est le système d'exploitation sur le serveur 192.168.7.1.
5. Sur le serveur 192.168.7.1, quels services s'exécutent sur les port : 3306, 22, 5432, 3307 et quelles sont leurs versions