MOPS
Réalisation pratique d’un test d’intrusion

Alexis LE MASLE
M2 Cybersécurité

Introduction

Durant ce tp, nous avons cherché à découvrir le plus de choses possible sur le réseau de l'entreprise "Entreprise". Nous devons réussir à compromettre par la suite le réseau de entreprise.net sans rien casser pour que l'entreprise puisse continuer de travailler.

Questions

Question 1

Pour identifier le serveur DNS du domaine entreprise.net, on peut utiliser la commande:

```
$ dnsrecon -d entreprise.net
[*] Performing General Enumeration of Domain: entreprise.net
[-] DNSSEC is not configured for entreprise.net
[*]      SOA ns1.entreprise.net 10.0.0.24
[*]      NS ns1.entreprise.net 10.0.0.24
[*]      MX mail.entreprise.net 35.35.35.44
[*]      A entreprise.net 24.24.24.15
[*] Enumerating SRV Records
[*]      SRV _http._tcp.entreprise.net www.entreprise.net 35.35.35.1 80
0
[*]      SRV _ldap._tcp.dc._msdcs.entreprise.net entreprise.net
24.24.24.15 389 0
[+] 2 Records Found
```

Le serveur DNS est donc le serveur "ns1.entreprise.net" à l'adresse 10.0.0.24

Question 2

Grâce à la commande de la question 1 on trouve le serveur MX appelé "mail.entreprise.net" à l'adresse 35.35.35.44.

Question 3

Plusieurs commandes existent pour déterminer les autres machines se trouvant sur le plan d'adressage 35.35.35.0/24.
Ici on utilise la commande : `nmap -sP 35.35.35.0/24`

On a alors obtenu de nouvelles adresses ip ainsi que des noms de machines.
35.35.35.1 --> www.entreprise.net
35.35.35.29 --> ftp.entreprise.net
35.35.35.42 --> zeus.entreprise.net
35.35.35.44 --> mail.entreprise.net
35.35.35.254 --> routeur3.local.lan

En utilisant ensuite la commande `dnsrecon -r 35.35.35.0/24` on peut obtenir une nouvelle adresse associée à un nouveau nom:
35.35.35.21 --> oldserver.entreprise.net

Pour finir j'ai utilisé la commande proposée `dnsrecon -d entreprise.net -t brt -D /usr/share/dnsenum/dns.txt` à dévoilé la machine backup.entreprise.net à l'adresse 192.168.1.14.

Via le DNS nous avons donc pu obtenir une liste d'adresses ip et de noms de machines sur le réseau 35.35.35.0/24.

Question 4

ICMP

Pour obtenir les routes utilisées par les paquets ICMP vers l'adresse 35.35.35.1 (www.entreprise.net) , on utilise la commande:

```
sudo traceroute -I www.entreprise.net
traceroute to www.entreprise.net (35.35.35.1), 30 hops max, 60 byte
packets
 1  _gateway (42.42.42.1)  3.518 ms  3.601 ms  3.705 ms
 2  router1.local.lan (10.0.0.1)  3.813 ms  3.920 ms  4.030 ms
 3  router2.local.lan (20.0.0.2)  4.137 ms  4.244 ms  4.352 ms
 4  www.entreprise.net (35.35.35.1)  6.131 ms  6.136 ms  6.726 ms
```

53/UDP

De même que ICMP, on utilise:

```
traceroute -U -p 53 www.entreprise.net
traceroute to www.entreprise.net (35.35.35.1), 30 hops max, 60 byte
packets
 1  _gateway (42.42.42.1)  6.716 ms  6.731 ms  6.861 ms
 2  router1.local.lan (10.0.0.1)  6.940 ms  7.020 ms  7.102 ms
 3  router4.local.lan (50.0.0.4)  7.130 ms  7.212 ms  7.278 ms
 4  router3.local.lan (40.0.0.3)  7.357 ms  7.519 ms  7.523 ms
 5  www.entreprise.net (35.35.35.1)  7.537 ms  7.888 ms 7.987 ms
```

80/TCP

```
sudo traceroute -T -p 80 www.entreprise.net
traceroute to www.entreprise.net (35.35.35.1), 30 hops max, 60 byte
packets
 1  _gateway (42.42.42.1)  2.901 ms  3.007 ms  3.103 ms
 2  router1.local.lan (10.0.0.1)  3.201 ms  3.316 ms  3.369 ms
 3  router2.local.lan (20.0.0.2)  3.471 ms  3.574 ms  3.677 ms
 4  router3.local.lan (40.0.0.3)  3.829 ms  3.933 ms  4.036 ms
 5  www.entreprise.net (35.35.35.1)  4.137 ms  5.088 ms  5.187 ms
 6  www.entreprise.net (35.35.35.1)  6.048 ms  5.186 ms  2.932 ms
```

On observe ici que notre paquet est passé deux fois dans www.entreprise.net de suite pour le port 80.

8080/TCP

```
sudo traceroute -T -p 8080 www.entreprise.net
traceroute to www.entreprise.net (35.35.35.1), 30 hops max, 60 byte
packets
 1  _gateway (42.42.42.1)  2.607 ms  2.664 ms  2.781 ms
 2  router1.local.lan (10.0.0.1)  2.869 ms  2.895 ms  3.022 ms
 3  router4.local.lan (50.0.0.4)  3.120 ms  3.147 ms  3.246 ms
 4  router3.local.lan (40.0.0.3)  3.338 ms  3.505 ms  3.524 ms
 5  www.entreprise.net (35.35.35.1)  10.078 ms  10.087 ms  15.166 ms
```

Question 5

Grâce à ces routes, on peut commencer à dessiner un schéma du réseau. En effet on constate que nos paquets passent d'abord par la Gateway à l'adresse 42.42.42.1 puis par le routeur 1 à l'adresse 10.0.0.1. Ensuite selon le protocole utilisé les routeurs par lesquels nos paquets passent ne sont pas les mêmes.

En se fiant aux trois protocoles utilisés (ICMP, TCP et UDP), on peut déterminer du moins provisoirement l'existence d' une gateway et de quatre routeurs nommé 1, 2, 3 et 4. Dans nos trois tests, le paquet passe par routeur1 puis pars routeur2 et enfin routeur3 si le protocole utilisé est TCP port 80 ou ICMP. Si c'est le protocol UDP port 53, le paquet passe par routeur1 puis routeur4 avant de rejoindre routeur3.

De nos quatre routeurs, seul un change lors d'un différent protocole, le routeur 1 et 3 restent toujours présent, on peut donc en déduire une architecture en forme de carré pour les quatres routeurs.

On peut émettre l'hypothèse d'un routage protocolaire.

Toutes les adresses ip, routeurs et masques de sous-réseau trouvé se trouvent dans le schéma situé à la fin du rapport. (Schéma)

Question 6

Afin de déterminer depuis combien de temps la machine 35.35.35.1 est allumée on peut utiliser la commande `sudo hping3 35.35.35.1 -p 80 -S --tcp-timestamp -c 4`

Voici un des résultats du ping:

```
len=56 ip=35.35.35.1 ttl=59 DF id=0 sport=80 flags=SA seq=1 win=28960
rtt=7.5 ms
  TCP timestamp: tcpts=4294899997
  HZ seems hz=100
  System uptime seems: 497 days, 2 hours, 16 minutes, 39 seconds
```

La ligne "System uptime" nous permet donc déterminer que la machine 35.35.35.1 est allumée depuis 497 jours environs au moment du ping.

Question 7

Afin de répondre à cette question, j'ai utilisé la commande `sudo snmpwalk -c public -v 2c 50.0.0.4 > snmp_50.0.0.4.txt` avec redirection d'output dans un fichier afin de pouvoir le lire plus facilement.

Dans ce fichier j'ai pu trouver les différentes interface du routeur 4 (50.0.0.4) ainsi que ses connexions aux autres routeurs et les masques de sous-réseau.

Par exemple:

```
iso.3.6.1.2.1.4.20.1.1.40.0.0.4 = IpAddress: 40.0.0.4
iso.3.6.1.2.1.4.20.1.1.50.0.0.4 = IpAddress: 50.0.0.4
iso.3.6.1.2.1.4.20.1.1.127.0.0.1 = IpAddress: 127.0.0.1
```

On y retrouve donc 50.0.0.4 qui est l'adresse de l'interface que nous avons détecté avec traceroute plus tôt. Il y'a aussi 40.0.0.4 d'affichée et on se souvient avoir vu qu'une des adresses du routeur 3 était 40.0.0.3. On garde cette ip de côté pour l'instant.

On peut ensuite lire un peu plus bas:

```
iso.3.6.1.2.1.4.20.1.3.40.0.0.4 = IpAddress: 255.255.255.0
iso.3.6.1.2.1.4.20.1.3.50.0.0.4 = IpAddress: 255.255.255.0
iso.3.6.1.2.1.4.20.1.3.127.0.0.1 = IpAddress: 255.0.0.0
```

En lisant la fin de "iso." on peut retrouver les trois adresses ip et cette fois elles sont associée à ce qui semble être le masque de sous-réseau associé à chacun des réseau des interfaces du routeur.

On vient donc pour l'instant d'apprendre que le routeur 4 a deux interfaces, 50.0.0.4 et 40.0.0.4 ayant toutes les deux un réseau en /24 (255.255.255.0).

En descendant encore dans le fichier on voit:

```
iso.3.6.1.2.1.4.21.1.1.10.0.0.0 = IpAddress: 10.0.0.0
iso.3.6.1.2.1.4.21.1.1.20.0.0.0 = IpAddress: 20.0.0.0
iso.3.6.1.2.1.4.21.1.1.30.0.0.0 = IpAddress: 30.0.0.0
iso.3.6.1.2.1.4.21.1.1.35.35.35.0 = IpAddress: 35.35.35.0
iso.3.6.1.2.1.4.21.1.1.40.0.0.0 = IpAddress: 40.0.0.0
iso.3.6.1.2.1.4.21.1.1.50.0.0.0 = IpAddress: 50.0.0.0
```

On y voit une liste d'adresses réseau de 10 à 50 avec aussi le réseau 35.35.35.0. On sait que le routeur 4 est lié au routeur 1 et au routeur 3, que le routeur 1 est lié au réseau 10.0.0.0 ainsi qu'au réseau 20.0.0.0 et que le routeur 3 est lié au réseau 35.35.35.0. On peut

donc déduire qu'il s'agit d'une liste des sous-réseaux auxquels sont connecté le routeur 4 est les routeurs qui lui sont directements liés.

Encore plus bas on voit:

```
iso.3.6.1.2.1.4.21.1.7.10.0.0.0 = IpAddress: 50.0.0.1
iso.3.6.1.2.1.4.21.1.7.20.0.0.0 = IpAddress: 50.0.0.1
iso.3.6.1.2.1.4.21.1.7.30.0.0.0 = IpAddress: 40.0.0.3
iso.3.6.1.2.1.4.21.1.7.35.35.35.0 = IpAddress: 40.0.0.3
iso.3.6.1.2.1.4.21.1.7.40.0.0.0 = IpAddress: 0.0.0.0
iso.3.6.1.2.1.4.21.1.7.50.0.0.0 = IpAddress: 0.0.0.0
```

Le réseau 10.0.0.0 est lié à 50.0.0.1, or nous savons que le routeur 1 est lié au réseau 10.0.0.0. On peut donc déduire que ce qui vient du réseau 10.0.0.0 sort du routeur 1 par son interface 50.0.0.1 pour atteindre le routeur 4.

De la même manière, ce qui vient du réseau 20.0.0.0 sort aussi par l'interface du routeur 1 50.0.0.1 puisque le routeur 1 est aussi lié au réseau 20.0.0.0.

Ce qui vient du réseau 30.0.0.0 et du réseau 35.35.35.0 sort par l'interface 40.0.0.3. Nous savons aussi que le routeur 3 est lié au réseau 35.35.35.0, au réseau 40.0.0.0 et nous découvrons donc qu'il est lié au réseau 30.0.0.0 qui semble être le sous-réseau entre le routeur 2 et le routeur 3 puis que nous connaissons son seul autre sous-réseau qui est 35.35.35.0.

Pour finir on a les sous-réseaux 40.0.0.0 et 50.0.0.0 qui sont les réseaux lié au routeur 4 directement.

Plus bas:

```
iso.3.6.1.2.1.4.21.1.11.10.0.0.0 = IpAddress: 255.255.255.0
iso.3.6.1.2.1.4.21.1.11.20.0.0.0 = IpAddress: 255.255.255.0
iso.3.6.1.2.1.4.21.1.11.30.0.0.0 = IpAddress: 255.255.255.0
iso.3.6.1.2.1.4.21.1.11.35.35.35.0 = IpAddress: 255.255.255.0
iso.3.6.1.2.1.4.21.1.11.40.0.0.0 = IpAddress: 255.255.255.0
iso.3.6.1.2.1.4.21.1.11.50.0.0.0 = IpAddress: 255.255.255.0
```

Grâce à ces lignes, on apprend que tous les sous-réseaux que nous avons découvert sont en /24 soit un masque de 255.255.255.0

Maintenant que nous connaissons tous les masques de sous-réseau, on peut utiliser la commande nmap -sP xx.xx.xx.xx/24 pour déterminer toutes les ip de ces réseaux et donc les interfaces qu'il pourrait nous manquer sur les routeurs.
Par exemple `nmap -sP "30.0.0.0/24` nous permet de déterminer l'existence de l'adresse ip 30.0.0.2 correspondant donc au routeur 2.

Les adresses ip des interfaces ont donc été ajoutée sur le schéma de fin.

Question 8

Voir le schéma.

Question 9

Voir Question 3.

Question 10

L'option -sS nécessite les privilèges super utilisateur car il utilise un SYN scan et l'option -sT utilise la fonction connect() de l'OS donc les privilèges sont égalements nécessaire.

Question 11

Question 12

Question 13

Voir Question 7.

Question 14

La détection d'OS active se fait avec nmap grâce à l'option "-O" ou "-A".
Exemple:

```
sudo nmap -A -T4 35.35.35.44`
445/tcp open  microsoft-ds Windows Server 2003 R2 3790 Service Pack 2
microsoft-ds
```

Donc on peut supposer que la machine 35.35.35.44 (mail.entreprise.net) a un OS Windows Server 2003 Service Pack 2

Question 15

Question 16

Lors des scans des services réseaux ouvert, nous avons pu voir que chaque machine avait un service SNMP de MikroTik, de plus la détection du temps de démarrage de la machine 35.35.35.29 et de la machine 35.35.35.44 nous rendait le même résultat. On peut en conclure que ces adresses ip sont en réalité sur la même machine. De plus, le fait que l'id des pings fait avec hping3 soit toujours à 0 nous indique qu'il y'a quelque chose de spécial ainsi que le fait que le traceroute en tcp sur le port 80 nous fasse passer deux fois dans 35.35.35.1. Lorsqu'on utilise traceroute en tcp sur le port 8080 on n'obtient plus ce doublon à cette adresse. On peut donc en conclure que la machine à l'adresse 35.35.35.1 effectue un NAT et redirige le port 80 vers le serveur http.

Nous avons appris plus tard que tout cela était provoqué par l'utilisation d'une solution MikroTik.

Schéma du réseau

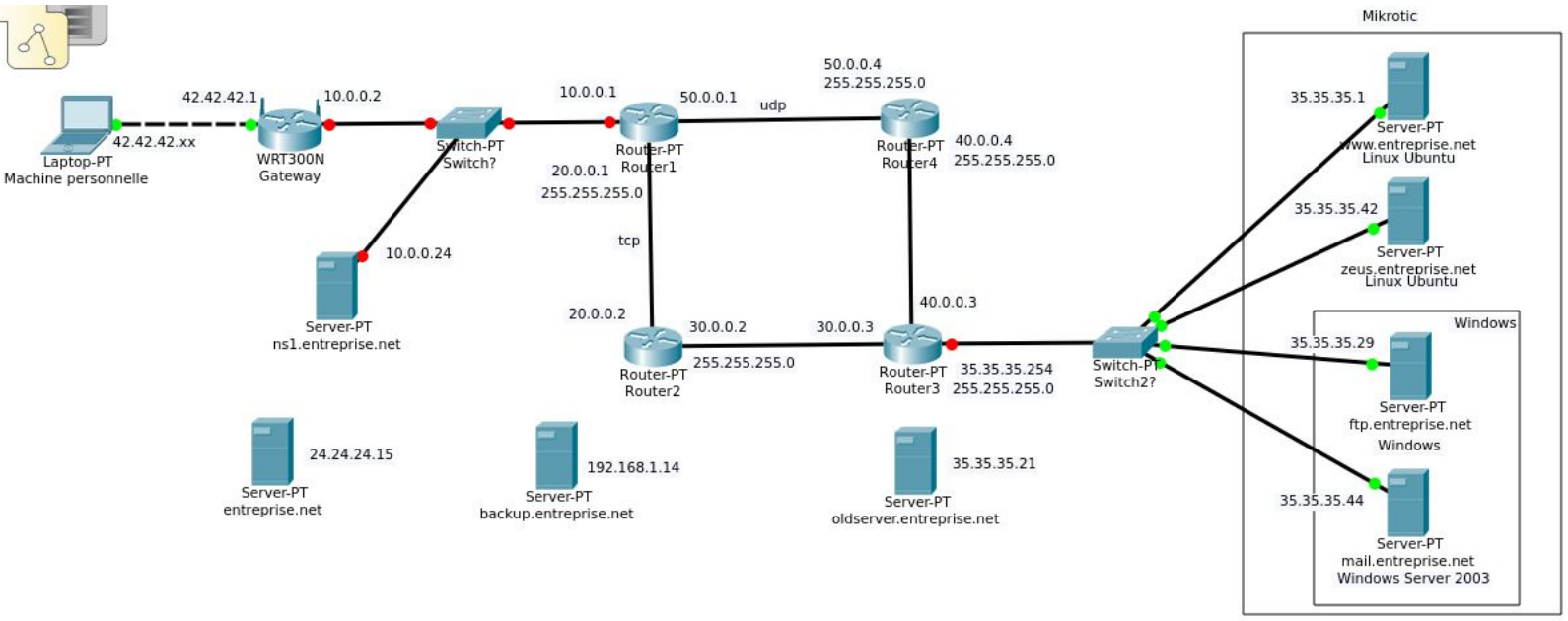

Schéma des données récoltées sur le réseau.