RAPPORT DE PENTEST

PERNON Etienne

CCI CAMPUS – ALSACE - JEU. 31 OCT 2024

Table des matières

I. Déroulement des tests

A. Découverte du réseau

Réalisation d'un scan rapide du réseau avec le logiciel Nmap en demandant les services et une analyse de OS *(operating system)* ainsi que les port ouvert.

- Commande : nmap -O -sV -F 192.168.0.0/24

Découverte d'une machine vulnérable : metasploitable

Identification de l'appareil:

- IP : 192.168.0.196 *(volatile)*
- MAC : B8 :8D :12 :0E :43 :24 *(volatile)*
- Nom : Metasploitable

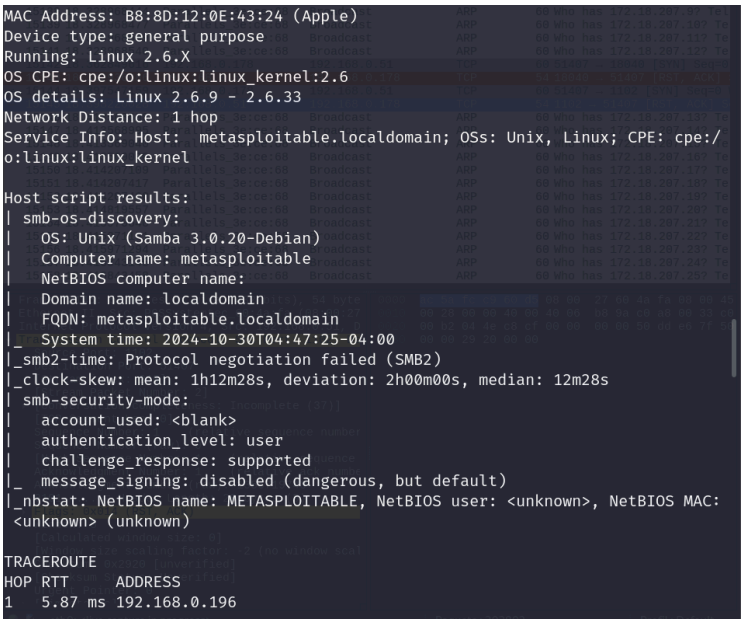
Peine encourue selon le Code Pénal français

323.1 : L'attaquant a maintenu une connexion frauduleuse sur le réseaux nommé « cyber »

323.2 & 323.3 : L'attaquant a perturbé le bon fonctionnement du réseaux « cyber » en réalisant des attaques de spoofing d'adresse Ip et d'adresse Mac.

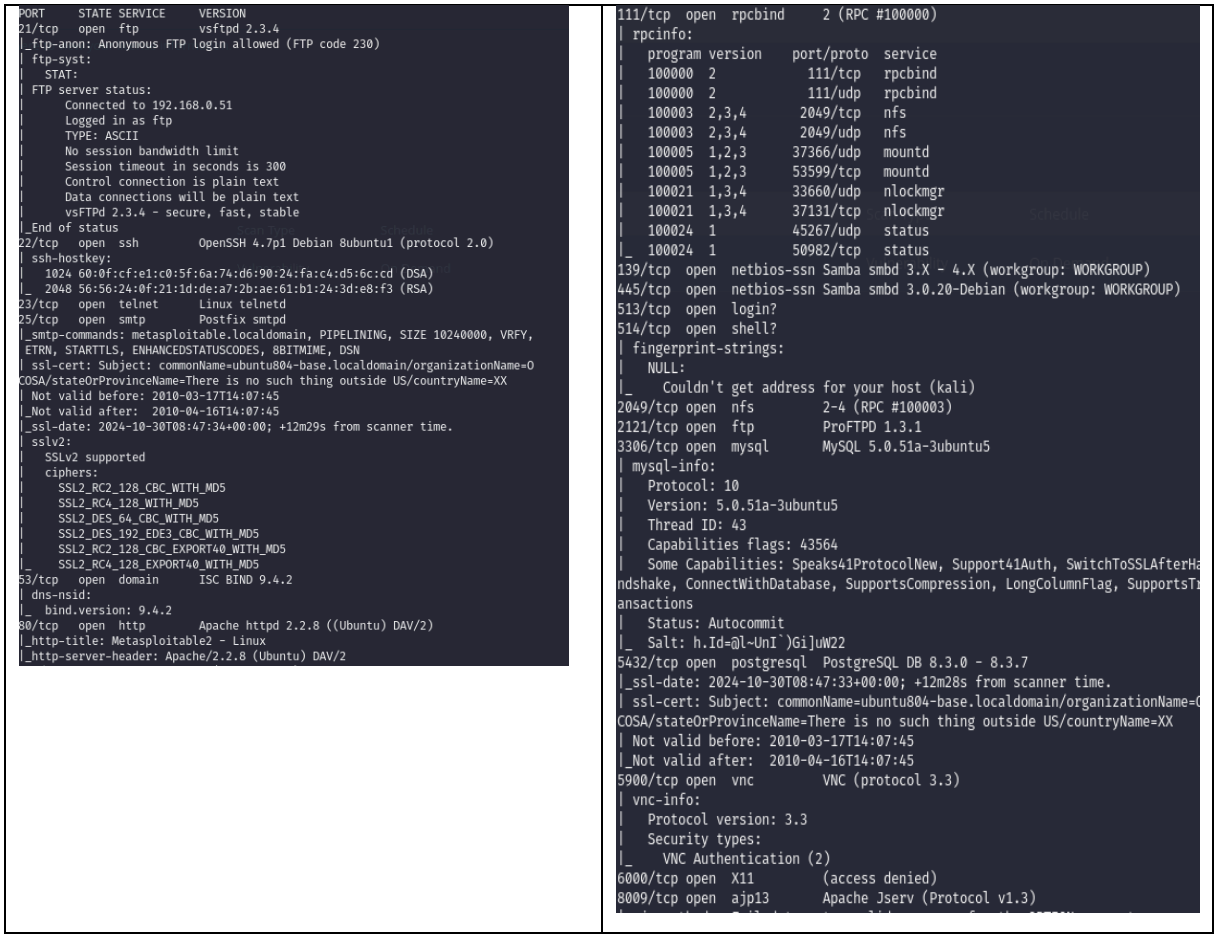
- System d’exploitation : linux 2.6.9 / Debian

Cette analyse de OS la machine infectée n’est pas clair sur la distribution de linux utilisé par l’attaquant, l’utilisation de Debian ou d’Ubuntu est encore équivoque. Cependant l’utilisation du server de fichier Samba 3 pour Debian impose que l’OS de la machine soit aussi un Debian pour l’accueillir, l’hypothèse d’un OS Ubuntu est donc exclue.



DESCRIPTIF DE LA MACHINE : METASPLOITABLE

Liste des ports ouvert :



```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.51
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2024-10-30T08:47:34+00:00; +12m29s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

```
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      37366/udp   mountd
|   100005  1,2,3      53599/tcp   mountd
|   100021  1,3,4      33660/udp   nlockmgr
|   100021  1,3,4      37131/tcp   nlockmgr
|   100024  1          45267/udp   status
|_  100024  1          50982/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
513/tcp  open  login?
514/tcp  open  shell?
| fingerprint-strings:
|   NULL:
|_    Couldn't get address for your host (kali)
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 43
|   Capabilities flags: 43564
|   Some Capabilities: Speaks41ProtocolNew, Support41Auth, SwitchToSSLAfterHa
ndshake, ConnectWithDatabase, SupportsCompression, LongColumnFlag, SupportsTr
ansactions
|   Status: Autocommit
|_  Salt: h.Id=@l~UnI`)Gi]uW22
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2024-10-30T08:47:33+00:00; +12m28s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
```

LISTE DES PORT DE LA MACHINE METASPLOITABLE

- À la suite de nos premières requêtes nous avons eu des difficultés à communiquer avec la machine cible

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -A -O -sV -F 192.168.0.196
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-30 10:03 CET
Nmap scan report for 192.168.0.196
Host is up.
All 100 scanned ports on 192.168.0.196 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT     ADDRESS
1   ... 30

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 59.19 seconds
```

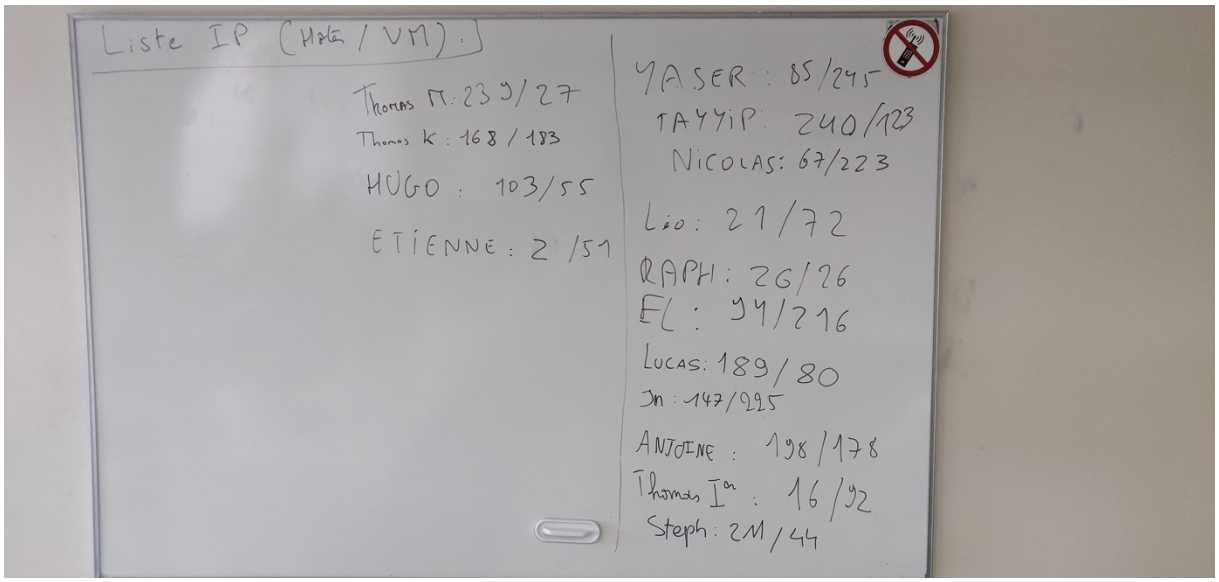
- Par la suite nous avons été **éjectés à plusieurs reprises** du réseau puis l'adresse IP de la machine metasploitable a changé.
- Les adresses des machines de l'équipe de penteste ont également subi des changements ou des inversions intempestives.

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -O -Pn -sV -F 192.168.0.196
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-30 11:18 CET
Nmap done: 1 IP address (0 hosts up) scanned in 2.07 seconds
```

CONCLUSION : Nous pouvons donc en conclure que l'attaquant a accès au service DHCP du réseau « cyber » par exploitation d'une attaques de spoofing d'adresse Ip / MAC sur le réseaux en question.

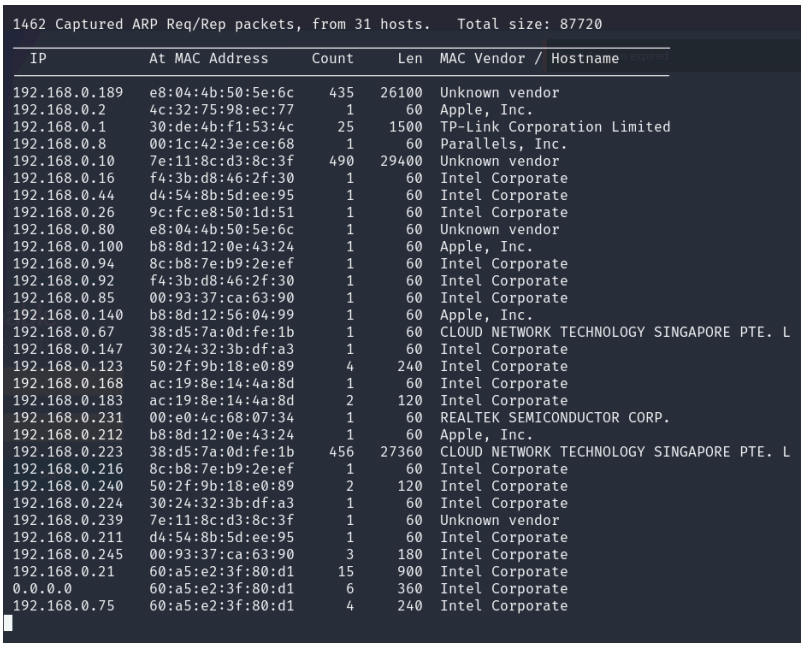
Traque de la machine metasploitable

Dans le but de mieux connaître le réseau dans lequel notre équipe évolue nous avons décidé de noter les adresses ip de nos machine Host & de nos VM kali présente sur le réseau :



Combiné avec la commande « netdiscover -p » nous avons pu différencier nos machine de la machine suspect :

Note : veuillez exécuter le paramètre -p pour que la recherche de netdiscover soit en mode passive.



```
1462 Captured ARP Req/Rep packets, from 31 hosts.   Total size: 87720
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
192.168.0.189   e8:04:4b:50:5e:6c    435   26100  Unknown vendor
192.168.0.2     4c:32:75:98:ec:77      1      60  Apple, Inc.
192.168.0.1     30:de:4b:f1:53:4c     25    1500  TP-Link Corporation Limited
192.168.0.8     00:1c:42:3e:ce:68      1      60  Parallels, Inc.
192.168.0.10    7e:11:8c:d3:8c:3f    490   29400  Unknown vendor
192.168.0.16    f4:3b:d8:46:2f:30      1      60  Intel Corporate
192.168.0.44    d4:54:8b:5d:ee:95      1      60  Intel Corporate
192.168.0.26    9c:fc:e8:50:1d:51      1      60  Intel Corporate
192.168.0.80    e8:04:4b:50:5e:6c      1      60  Unknown vendor
192.168.0.100   b8:8d:12:0e:43:24      1      60  Apple, Inc.
192.168.0.94    8c:b8:7e:b9:2e:ef      1      60  Intel Corporate
192.168.0.92    f4:3b:d8:46:2f:30      1      60  Intel Corporate
192.168.0.85    00:93:37:ca:63:90      1      60  Intel Corporate
192.168.0.140   b8:8d:12:56:04:99      1      60  Apple, Inc.
192.168.0.67    38:d5:7a:0d:fe:1b      1      60  CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. L
192.168.0.147   30:24:32:3b:df:a3      1      60  Intel Corporate
192.168.0.123   50:2f:9b:18:e0:89      4     240  Intel Corporate
192.168.0.168   ac:19:8e:14:4a:8d      1      60  Intel Corporate
192.168.0.183   ac:19:8e:14:4a:8d      2     120  Intel Corporate
192.168.0.231   00:e0:4c:68:07:34      1      60  REALTEK SEMICONDUCTOR CORP.
192.168.0.212   b8:8d:12:0e:43:24      1      60  Apple, Inc.
192.168.0.223   38:d5:7a:0d:fe:1b    456   27360  CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. L
192.168.0.216   8c:b8:7e:b9:2e:ef      1      60  Intel Corporate
192.168.0.240   50:2f:9b:18:e0:89      2     120  Intel Corporate
192.168.0.224   30:24:32:3b:df:a3      1      60  Intel Corporate
192.168.0.239   7e:11:8c:d3:8c:3f      1      60  Unknown vendor
192.168.0.211   d4:54:8b:5d:ee:95      1      60  Intel Corporate
192.168.0.245   00:93:37:ca:63:90      3     180  Intel Corporate
192.168.0.21    60:a5:e2:3f:80:d1     15     900  Intel Corporate
0.0.0.0         60:a5:e2:3f:80:d1      6     360  Intel Corporate
192.168.0.75    60:a5:e2:3f:80:d1      4     240  Intel Corporate
```

LISTE DES MACHINE CONNECTE AU RESEAU CYBER

En combinant nos informations nous avons pu identifier *(à cette instant)* que la metasploitable est :

- IP : 192.168.0.100
- MAC : B8 :8D :12 :0E :43 :24

Durant nos tests nous avons constaté que l’adresse MAC de la machine suspect a été modifier, cependant nous n’avons pas eu l’occasion de récolter la preuve de ce changement d’adresse MAC.

B. Recherche de vulnérabilité sur la metasploitable

Une fois que la machine suspecte a été clairement identifier et que nous pouvions la tracer, nous avons lancer les scans de vulnérabilité via Nessus / Nmap.

Dans le navigateur

Via le navigateur nous avons pu se connecter à une interface WEB de la machine suspect :

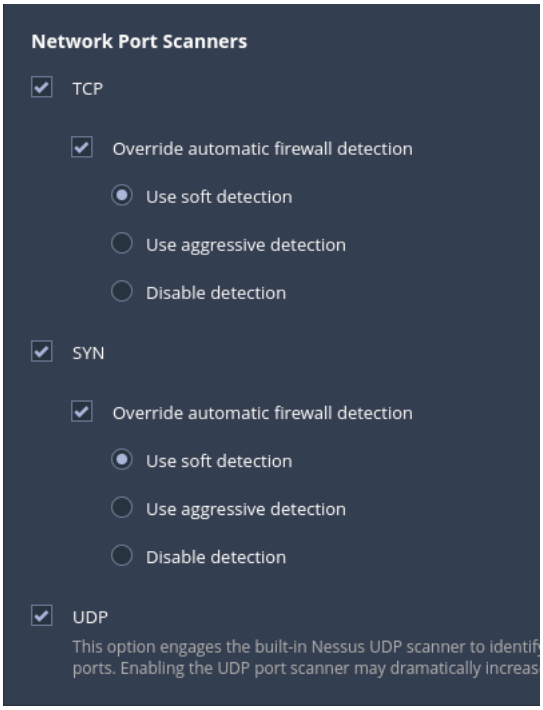
PAGE WEB RETOURNE VIA L'ADRESSE DE LA MACHINE : METASPLOITABLE

Note : Nous n'investiguerons pas plus ce moyen de connexion car nous avons l'obligation d'exécuter nos tests en mode passif.

Analyse via Nessus Essential

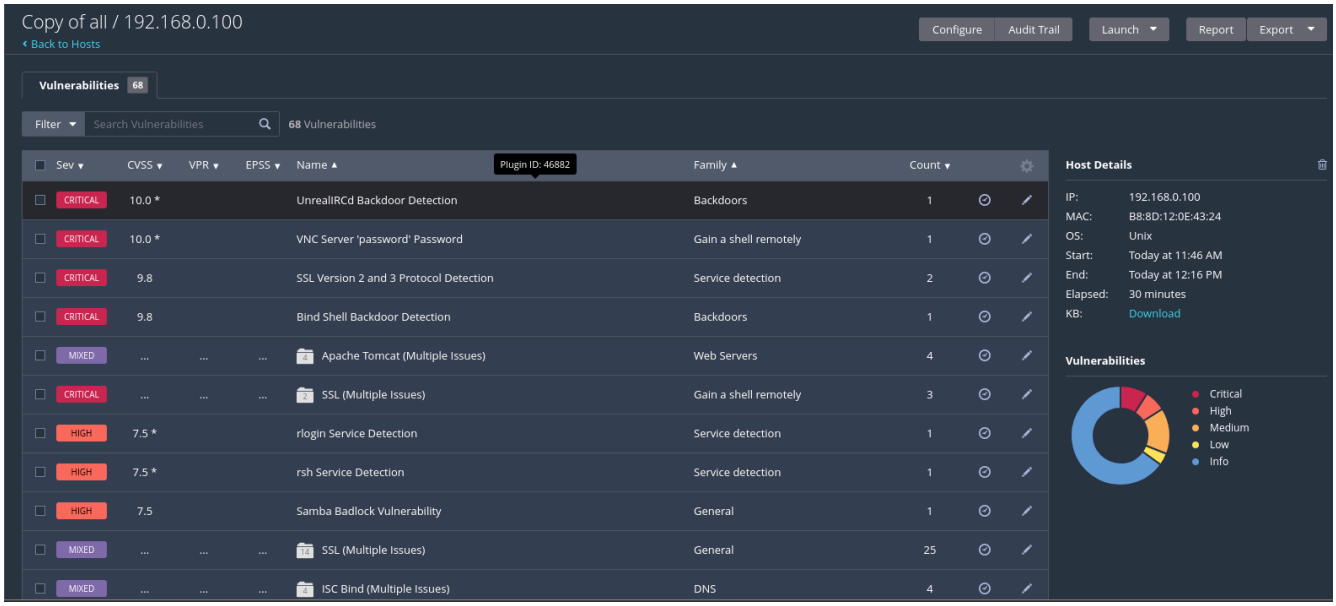
Nous avons lancer un scan avancer via l'application Nessus en version Essential.

Notez que le scan n'a pas été lancé en mode agressif :



SCAN AVANCEE : POINT DE CONFIGURATION IMPORTANT

L’analyse de Nessus a révélé 68 failles de sécurité sur la machine metasploitable. Nous pouvons noter qu’il y a 9% de faille critique dont 5 avec une criticité score de criticité de 10/10.



VUE D’ENSEMBLE DES VULNERABILITE

LISTE VULNERABILITES LES PLUS CRITIQUE

Criticité	Nom	Identification	Score
CRITICAL	UnreallRCd Backdoor Detection	CVE-2010-2075	10
	VNC server 'password' Password	/	10
	SSL Version 2 and 3 Protocl Detection	/	9.8
	Bind shell backdoor Detection	/	9.8
	Apache Tomcat SeoL (<= 5.5.X)	/	10
	Apache Tomct AJP Connector Request Injecgion (GostCat)	CVE-2020-1745 CVE-2020-1998	9.8
	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	CVE-2008-0166	10

Vulnérabilités critique permettant de mettre hors d'état de nuire le hacker

UnrealIRCd 3.2.8.1 - Backdoor Command Execution

CVE : 2010-2075

Criticité : 10 / 10

Explication : Via un accès à la machine metasploitable il est possible d'utiliser le service remote IRC server en détournant la fonction DEBUG3_DOLOG_SYSTEM pour exécuter du code arbitraire sur la machine cible. Ce moyen détourné permet l'installation d'un trojan/backdoor sans que son code soit analysé par l'antivirus.

Commentaire : Pour être exploité cette faille nécessite donc l'exploitation d'une autre vulnérabilité nous permettant d'accéder à la machine en physique ou via un shell distant.

Liens utiles :

- https://www.exploit-db.com/exploits/16922
- https://nvd.nist.gov/vuln/detail/CVE-2010-2075

VNC Server 'password' Password

CVE : néant
Criticité : 10 / 10

Explication : VNC est une application permettant un accès graphique d'un ordinateur distance. Le mot de passe permettant de se connecter à la machine metasploitable étant **'password'** il est possible d'acquérir un shell en mode administrateur sur cette machine.

Commande : xtightvncviewer
Mot de Passe : password

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

CVE : 2008-0166

Criticité : 10 / 10

Explication : Les distributions de linux basé sur Debian compromettent la fonction de génération de nombre aléatoire de la librairie OpenSSH en la rendant plus prévisible et donc plus **sensible aux attaques par brute force**.

Version OpenSSL : 0.9.8c-1 => 0.9.8g-9

Pour exploiter cette faille il faut repérer un trafic encrypter grâce au package OpenSSL *(version* 0.9.8c-1*)* depuis une machine Debain. Il faudra alors réaliser une attaque par brute force sur la clef d'encryptions en question.

Liens utiles :

- https://cert.ssi.gouv.fr/avis/CERTA-2008-AVI-246/
- https://www.exploit-db.com/exploits/5632
- https://nvd.nist.gov/vuln/detail/CVE-2008-0166