

Résumé

J'ai été engagé pour effectuer un test de pénétration deux VM afin de déterminer son exposition à une attaque ciblée.

Toutes les activités ont été menées de manière à simuler un acteur malveillant engagé dans une attaque ciblée contre la VM dans le but de :

- Identifier si un attaquant distant pourrait pénétrer les défenses des VM.
- Déterminer l'impact d'une faille de sécurité sur :
 - Confidentialité des données privées de l'entreprise
 - Infrastructure interne et disponibilité des systèmes d'information des VM

Les efforts ont porté sur l'identification et l'exploitation des faiblesses de sécurité qui pourraient permettre à un attaquant distant d'obtenir un accès non autorisé aux données de l'organisation. Les attaques ont été menées avec le niveau d'accès d'un utilisateur général d'Internet. L'évaluation a été menée conformément aux recommandations du NIST SP 800-1151, tous les tests et actions étant effectués dans des conditions contrôlées.

- La configuration de l'environnement du test d'intrusion est très importante pour réaliser un test d'intrusion dans de bonnes conditions.
- **Installez Kali**
- on a fait l'installation de Kali Linux sur une machine virtuelle vmfusion car sinon il faut beaucoup de ressources pour la faire tourner dans la mémoire vive uniquement
- La Distribution Kali Linux est conçue spécialement pour les tests d'intrusion.
- Avant chaque test d'intrusion, il faut s'assurer que ces outils sont à jour et intègres.

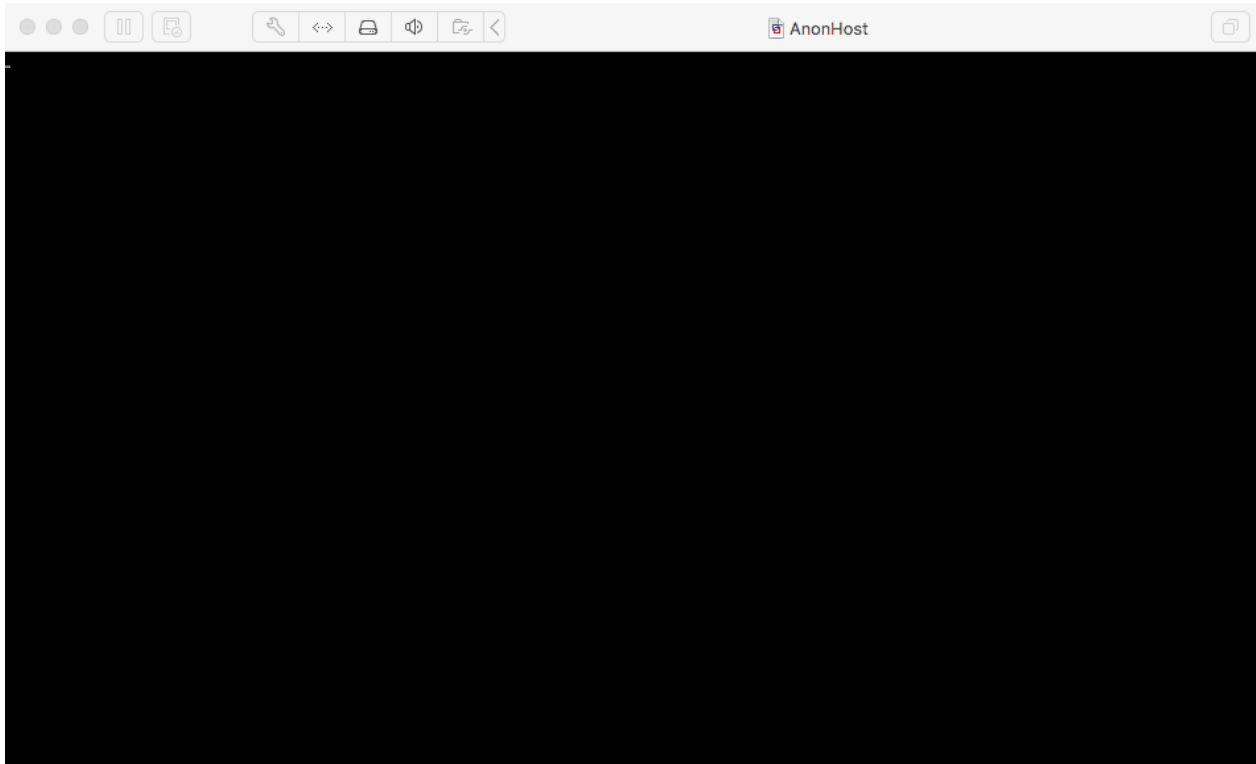
```
apt-get update && apt-get upgrade  
apt-get dist-upgrade
```

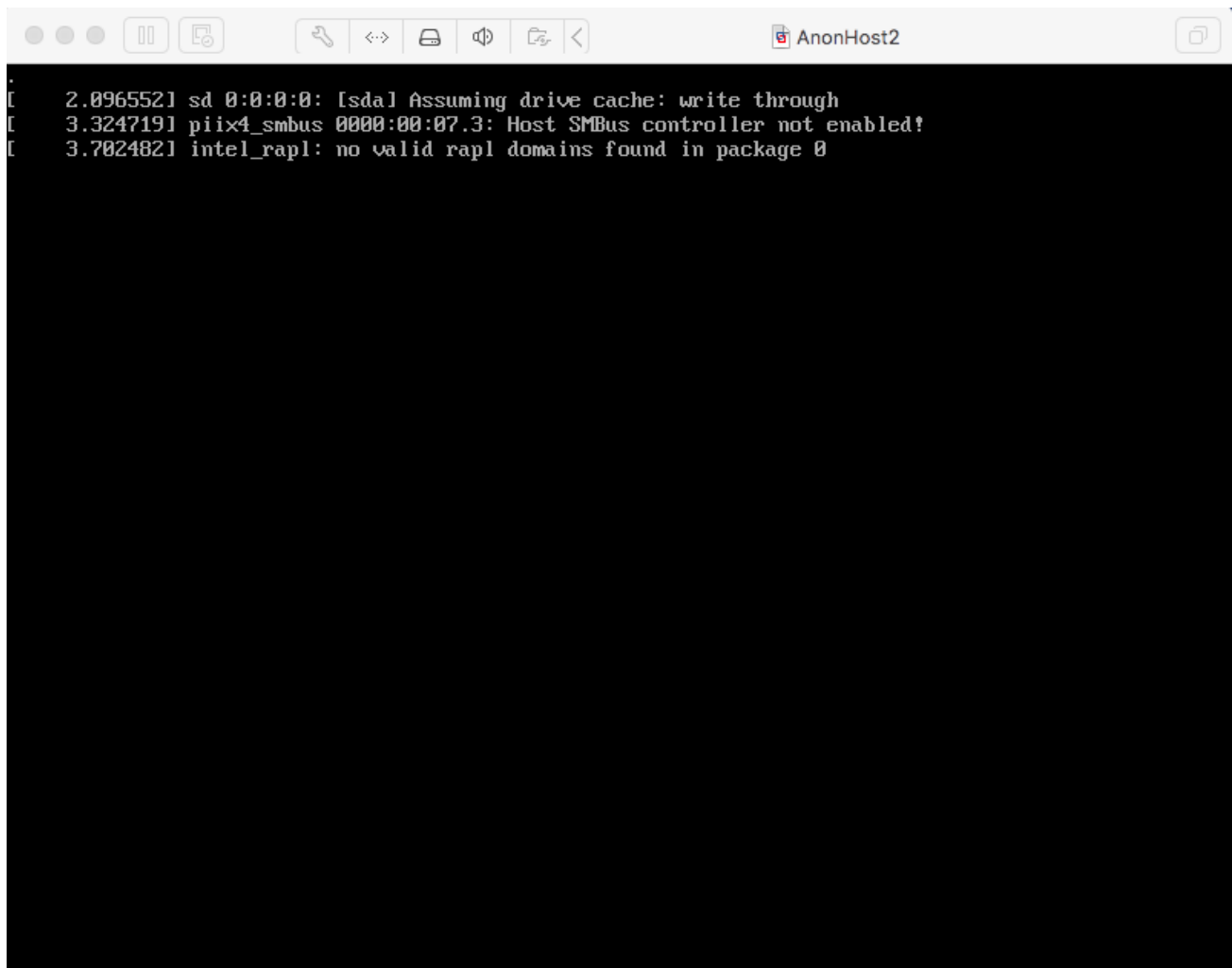
- **Installez Openvas** acronyme de Open source Vulnerability Assessment Scanner,
- Il faut un scanner de vulnérabilité openVAS.

- Il faut également un outil d'exploitation de vulnérabilité comme le célèbre Metasploit framework.

Affichez et modifiez ce document dans Word sur votre ordinateur, votre tablette ou votre téléphone. Vous pouvez modifier le texte, insérer du contenu (images, formes, tableaux, etc.) et enregistrer le document dans le cloud à partir de Word sur votre appareil Windows, Mac, Android ou iOS.

Installer les deux VM



A terminal window titled "AnonHost2" with a standard macOS-style title bar. The terminal displays three lines of kernel boot logs: a timestamped message for the sd driver assuming write-through cache, a message for the piix4_smbus driver stating the SMBus controller is not enabled, and a message for the intel_rapl driver stating no valid domains were found.

```
[ 2.096552] sd 0:0:0:0: [sd] Assuming drive cache: write through
[ 3.324719] piix4_smbus 0000:00:07.3: Host SMBus controller not enabled?
[ 3.702482] intel_rapl: no valid rapl domains found in package 0
```

Scanner les vulnérabilités d'un système

Pour être efficace dans un test d'intrusion, il faut suivre le processus suivant : **recherche d'empreinte, énumération des systèmes actifs et recherche de vulnérabilités.**

Recherchez les empreintes, collectez les informations

C'est vraiment la première étape d'un test d'intrusion. La recherche d'empreintes à la collecte d'information se fait en utilisant des sites Web qui sont à votre disposition, par exemple :

Énumérez les systèmes actifs

Il existe des tas de logiciels pour énumérer les systèmes actifs d'un réseau à la recherche de réponses. Cela dit, nous allons utiliser NMAP

En tapant simplement la commande « nmap », nous allons avoir une première aide qui nous permet de taper des lignes de commande simple.

arp-scan 192.168.24. 0/24

nous pouvons par exemple scanner toutes les adresses IP de votre réseau pour voir quelles sont les réponses :

Essayer de déterminer tous les systèmes qui a sur l'infrastructure qu'on veut tester c'est pour ça on utilise le Scan de sous réseau
nmap

ifconfig

nmap -sP 192.168.24.0/24

```

(vagrant@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.24.153 netmask 255.255.255.0 broadcast 192.168.24.255
    inet6 fe80::20c:29ff:fecf:1619 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:cf:16:19 txqueuelen 1000 (Ethernet)
    RX packets 79 bytes 33444 (32.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 87 bytes 12464 (12.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 16 bytes 880 (880.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 880 (880.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

```

(vagrant@kali)-[~]
$ sudo nmap -sP 192.168.24.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-19 10:52 EDT
Nmap scan report for 192.168.24.1
Host is up (0.00028s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.24.2
Host is up (0.00044s latency).
MAC Address: 00:50:56:F5:63:91 (VMware)
Nmap scan report for 192.168.24.154
Host is up (0.00040s latency).
MAC Address: 00:0C:29:BA:BA:BA (VMware)
Nmap scan report for 192.168.24.155
Host is up (0.00047s latency).
MAC Address: 00:50:56:CF:CF:CF (VMware)
Nmap scan report for 192.168.24.254
Host is up (0.00039s latency).
MAC Address: 00:50:56:F8:1F:74 (VMware)
Nmap scan report for 192.168.24.153
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.10 seconds

```

```

(vagrant@kali)-[~]
$ █

```

ça va nous scanner et essayer de nous déterminer le maximum d'IP qu'il peut trouver.

Sudo arp-scan 192.168.24. 0/24

Ca nous donne les adresse mac

```
(vagrant@kali)-[~]
$ arp-scan 192.168.24.0/24
pcap_activate: eth0: You don't have permission to capture on that device
(socket: Operation not permitted)

(vagrant@kali)-[~]
$ sudo arp-scan 192.168.24.0/24
Interface: eth0, type: EN10MB, MAC: 00:0c:29:cf:16:19, IPv4: 192.168.24.153
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.24.1    00:50:56:c0:00:08    VMware, Inc.
192.168.24.2    00:50:56:f5:63:91    VMware, Inc.
192.168.24.154  00:0c:29:ba:ba:ba    VMware, Inc.
192.168.24.155  00:50:56:cf:cf:cf    VMware, Inc.
192.168.24.254  00:50:56:f8:1f:74    VMware, Inc.

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.021 seconds (126.67 hosts/sec). 5 responded

(vagrant@kali)-[~]
$
```

Nmap -O 192.168.24.0/24

Ca nous donne les ports ouverts

```
(vagrant@kali)-[~]
$ sudo nmap -O 192.168.24.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-19 11:10 EDT
Nmap scan report for 192.168.24.1
Host is up (0.00055s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
88/tcp    open  kerberos-sec
445/tcp   open  microsoft-ds
MAC Address: 00:50:56:C0:00:08 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=5/19%OT=88%CT=1%CU=40079%PV=Y%DS=1%DC=D%G=Y%M=005056%T
OS:M=60A52A90%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10B%TI=Z%CI=RD%II=
OS:RI%TS=A)OPS(O1=M5B4NW5NNT11SLL%02=M5B4NW5NNT11SLL%03=M5B4NW5NNT11%04=M5B
OS:4NW5NNT11SLL%05=M5B4NW5NNT11SLL%06=M5B4NNT11SLL)WIN(W1=FFFF%W2=FFFF%W3=F
OS:FFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%0=M5B4NW5SLL%CC=Y%Q
OS:=)T1(R=Y%DF=Y%T=40%S=O%A=S+F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%
OS:W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T=40%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=
OS:)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=40%W=0%S=Z%A=
OS:S%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK
OS:=0%RUD=G)IE(R=Y%DFI=S%T=40%CD=S)

Network Distance: 1 hop

Nmap scan report for 192.168.24.2
Host is up (0.00026s latency).
All 1000 scanned ports on 192.168.24.2 are closed
MAC Address: 00:50:56:F5:63:91 (VMware)
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized
Running: VMware Player
OS CPE: cpe:/a:vmware:player
OS details: VMware Player virtual NAT device
Network Distance: 1 hop

Nmap scan report for 192.168.24.154
Host is up (0.00082s latency).
Not shown: 997 filtered ports
```

Nmap scan report for 192.168.24.154
 Host is up (0.00082s latency).
 Not shown: 997 filtered ports
 PORT STATE SERVICE
 22/tcp open ssh
 139/tcp open netbios-ssn
 445/tcp open microsoft-ds
 MAC Address: 00:0C:29:BA:BA: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: Linux 3.X|4.X
 OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
 OS details: Linux 3.10 - 4.11, Linux 3.2 - 4.9
 Network Distance: 1 hop

Nmap scan report for 192.168.24.155
 Host is up (0.00069s latency).
 Not shown: 995 closed ports
 PORT STATE SERVICE
 22/tcp open ssh
 79/tcp open finger
 80/tcp open http
 443/tcp open https
 3306/tcp open mysql
 MAC Address: 00:50:56:CF:CF:CF (VMware)
 Device type: general purpose
 Running: Linux 3.X|4.X
 OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
 OS details: Linux 3.2 - 4.9
 Network Distance: 1 hop

Nmap scan report for 192.168.24.254
 Host is up (0.00030s latency).
 All 1000 scanned ports on 192.168.24.254 are filtered
 MAC Address: 00:50:56:F8:1F:74 (VMware)
 Too many fingerprints match this host to give specific OS details
 Network Distance: 1 hop


```
Nmap scan report for 192.168.24.155
Host is up (0.00069s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
79/tcp    open  finger
80/tcp    open  http
443/tcp   open  https
3306/tcp  open  mysql
MAC Address: 00:50:56:CF:CF:CF (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
```

```
Nmap scan report for 192.168.24.254
Host is up (0.00030s latency).
All 1000 scanned ports on 192.168.24.254 are filtered
MAC Address: 00:50:56:F8:1F:74 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
Nmap scan report for 192.168.24.153
Host is up (0.000091s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
```

OS detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 256 IP addresses (6 hosts up) scanned in 44.87 seconds


```
(vagrant@kali) [~]
$ nmap -sV -T4 -F 192.168.24.155
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-19 11:48 EDT
Stats: 0:00:41 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 11:49 (0:00:10 remaining)
Stats: 0:01:34 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.07% done; ETC: 11:50 (0:00:00 remaining)
Nmap scan report for 192.168.24.155
Host is up (0.00077s latency).
Not shown: 95 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 1.5)
79/tcp    open  finger?
80/tcp    open  http     nginx 1.6.2
443/tcp   open  telnet   Linux telnetd
3306/tcp  open  mysql    MySQL 5.5.5-10.0.30-MariaDB-0+deb8u2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 109.07 seconds

(vagrant@kali) [~]
$
```

Machine-IP / OS & Version			
192.168.24.155/ linux3.2			
Port	Proto (TCP/UDP)	Service Name (IANA)	Binary & Version
22	TCP	Ssh	Open ssh 6.7p1 Debian 5+deb8u3
79	Tcp	Finger	?
80	Tcp	http	Ngnix 1.6.2

443	Tcp	https	Linux telnetd
3306	Tcp	Mysql	Mysql 5.5.5-1O-MariaDB-O+deb8u2

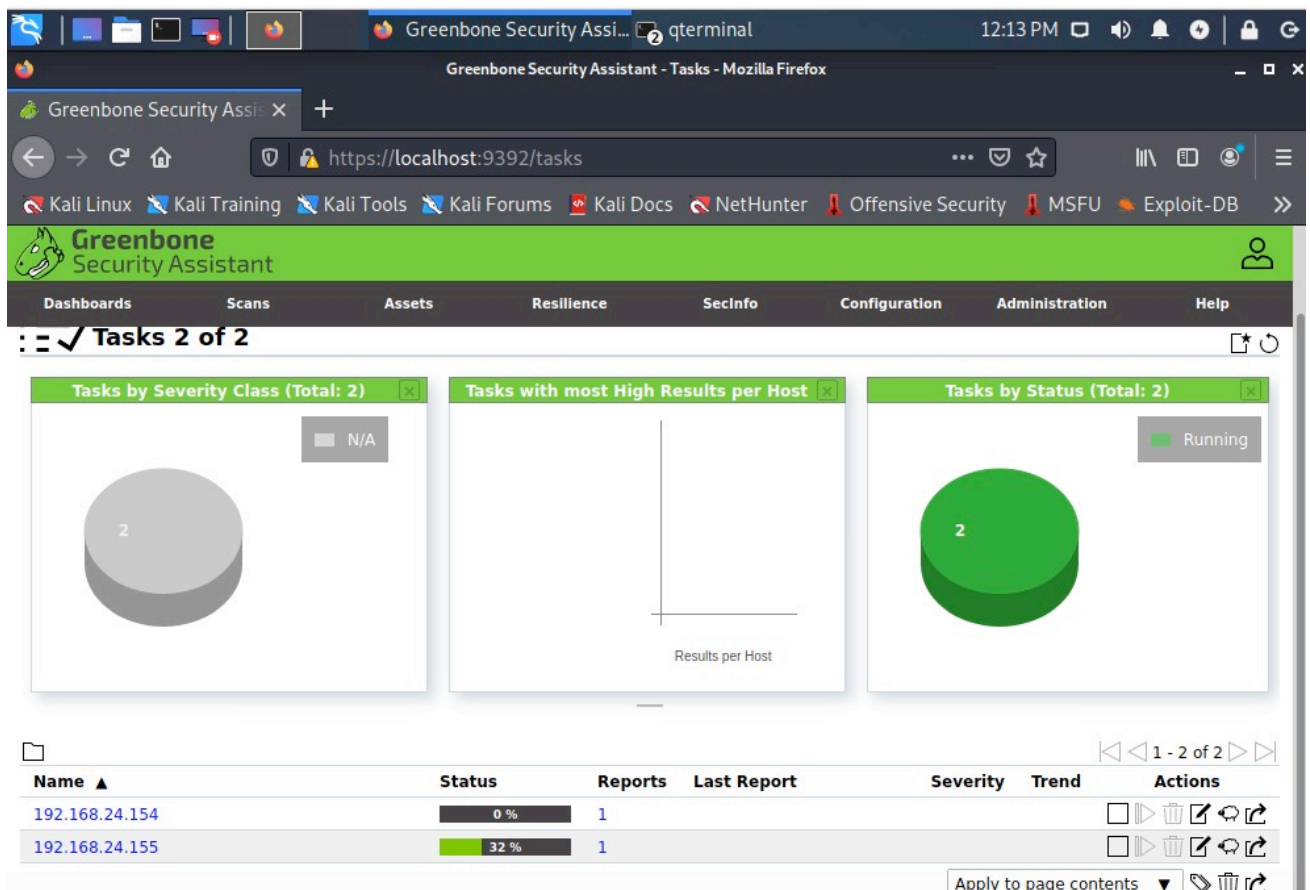
vagrant@kali: ~			
File Actions Edit View Help			
Currently scanning: 192.168.88.0/16 Screen View: Unique Hosts			
5 Captured ARP Req/Rep packets, from 5 hosts. Total size: 300			
IP	At MAC Address	Count	Len MAC Vendor / Hostname
192.168.24.1	00:50:56:c0:00:08	1	60 VMware, Inc.
192.168.24.2	00:50:56:f5:63:91	1	60 VMware, Inc.
192.168.24.154	00:0c:29:ba:ba:ba	1	60 VMware, Inc.
192.168.24.155	00:50:56:cf:cf:cf	1	60 VMware, Inc.
192.168.24.254	00:50:56:f8:1f:74	1	60 VMware, Inc.

Machine-IP / OS & Version			
192.168.24.154/ linux3.10			
Port	Proto (TCP/UDP)	Service Name (IANA)	Binary & Version
22	TCP	ssh	Open ssh 6.6.1
139	Tcp	Netbios-ssn	Samba smbd 3.X
445	Tcp	Microsoft-ds	Samba smbd 3.X

Recherchez les vulnérabilités

Après installation openvas, nous pouvons accéder aux logiciels en connectant sur l'adresse :
<https://localhost:9392/>

nous allons utiliser **un scan** pour scanner notre réseau de test avec la machine virtuelle active.



Greenbone Security Assistant - Targets - Mozilla Firefox

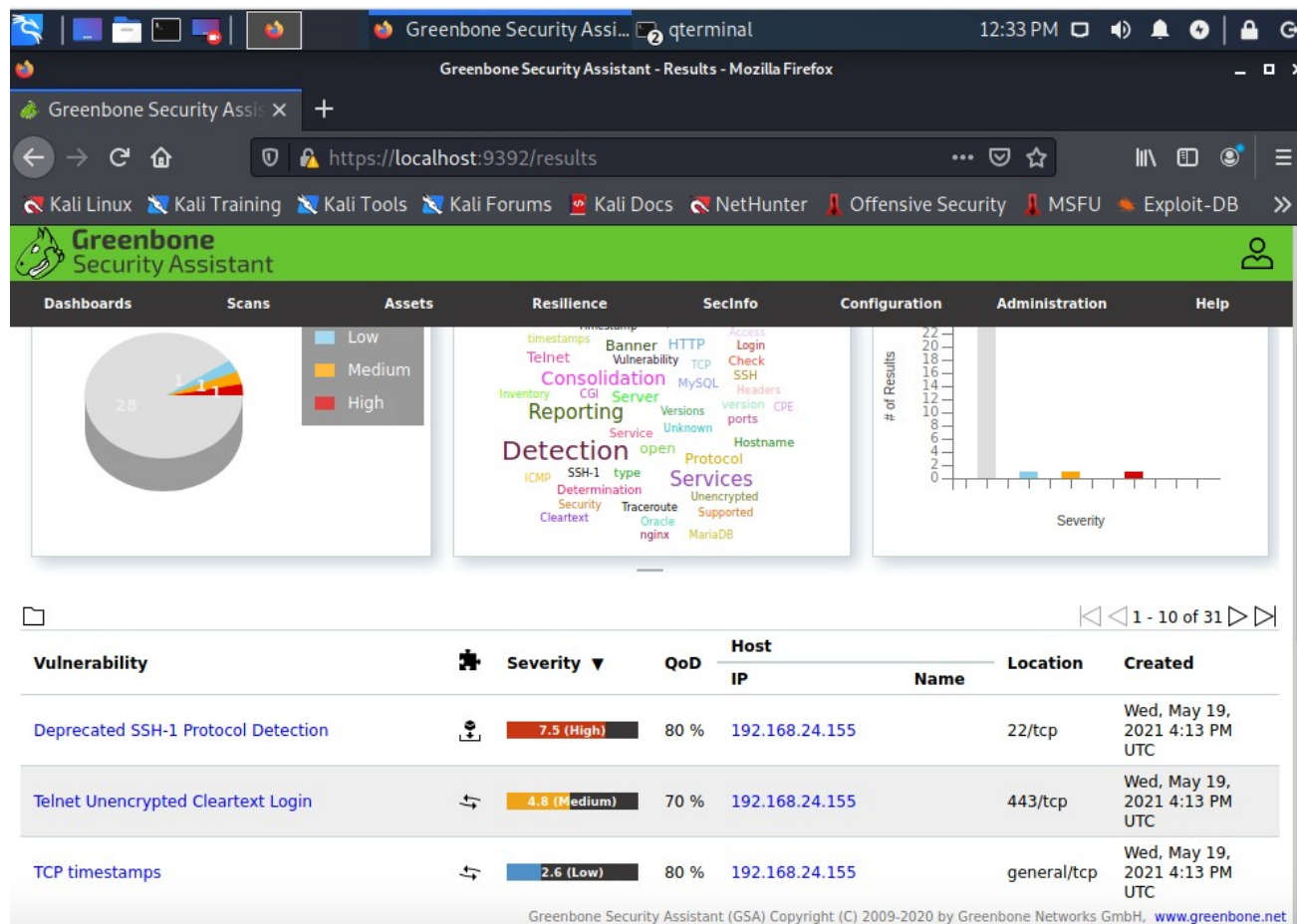
Greenbone Security Assistant

Targets 2 of 2

Name	Hosts	IPs	Port List	Credentials	Actions
192.168.24.154	192.168.24.154	1	All IANA assigned TCP		
192.168.24.155	192.168.24.155	1	All IANA assigned TCP		

(Applied filter: sort=name first=1 rows=10)

Une fois le scan terminé, nous pouvons analyser le résultat.



Nous voyons qu'il y a plusieurs vulnérabilités qui sont catégorisées en fonction de leur sévérité.

Quand on clique sur une vulnérabilité, nous pouvons en voir le **détail**.

Machine-IP / OS & Version			
192.168.24.155/ linux3.10			
Port	Service	Issue	Solution
22	SSH	Deprecated SSH-1 Protocol detection	Reconfigure the SSH service to only provide/accept the SSH protocol version SSH-2
23	Telnet	telnet Unencrypted Cleartext Login	Reconfigure the SSH service to only provide/accept the SSH protocol version SSH-2
	TCP	TCP timestamps	Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
Conclusion:			

Machine-IP / OS & Version			
192.168.24.154/ linux3.10			

Port	Service	Issue	Solution
Conclusion:			

Conclusion

- Il est très important que tous les collaborateurs soient formés à **identifier le SPAM**. Beaucoup d'outils sont à la disposition de tous pour casser les mots de passe. Il faut donc respecter des **règles de complexité** minimums pour établir un mot de passe.
- Il faut toujours utiliser des **protocoles chiffrés** pour échanger des données sensibles. Par exemple, les sites sur lesquels vous rentrez un mot de passe doivent être en HTTPS.

Remarque

Avec viruelbox je n'arrive pas à les détecter le réseau le Nat

j'ai remarqué que chacun était sur son propre réseau

ils ne sont pas sur le même réseau si on les met en NAT

ça marche pas avec virtuel box donc j'ai refait tous sur vmfusion j'ai importé Kali Linux les deux vm

je n'ai pas eu le temps pour terminer la pente 3h c'est peu

