HACKING CON METASPLOIT

1)PUNTI CHIAVE

- Configurazione IP Metasploitable/Kali
- Scansione servizio ftp Metasploitable
- Configurazione attacco Metasploit
- Accesso Metasploitable

2)INTRODUZIONE

Metasploit è un tool utilizzato nel penetration testing e nella ricerca delle vulnerabilità che permette di identificare e sfruttare le stesse nei sistemi operativi.

Lo scopo principale è quello di studiare e mettere al sicuro la propria infrastruttura informatica.

Le principali caratteristiche sono:

- **Interfaccia ----->** offre sia un'interfaccia CLI che un'interfaccia grafica, rendendo lo strumento accessibile a tutti.
- **Libreria di exploit ----->** possono essere utilizzati per testare la sicurezza di diversi sistemi operativi.
- **Payload ----->** sono pezzi di codice che vengono eseguiti una volta che un exploit ha avuto successo. (es: shell di comando, reverse shell e Meterpreter).
- **Gestione degli Exploit ----->** permette una gestione efficace degli exploit, facilitando l'organizzazione, la ricerca e l'utilizzo di exploit specifici per diversi target.

3)OBIETTIVO

L’obiettivo è di ottenere accesso alla macchina Metasploitable attraverso l’uso di **Metasploit,**usando il servizio **FTP** come target.

4)STRUMENTI

- **Metasploitable ----->** macchina target
- **Metasploit ----->** piattaforma di attacco

5)SVOLGIMENTO

5.1) CONFIGURAZIONE IP METASPLOITABLE/KALI

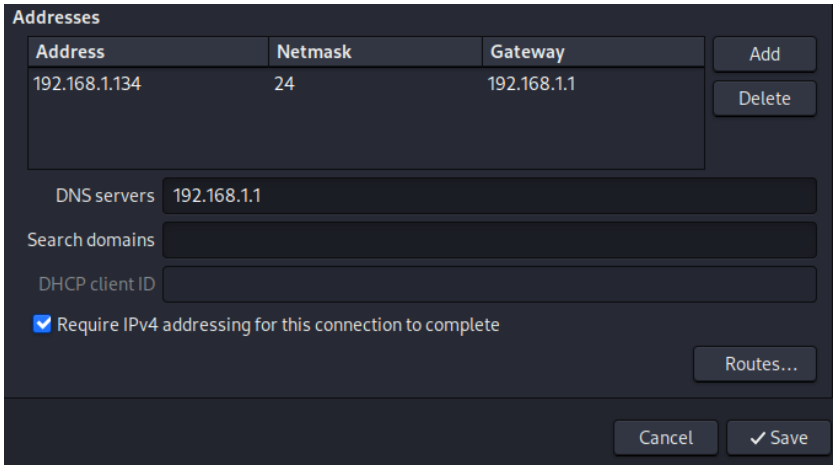


*Fig.1 Configurazione IP Kali

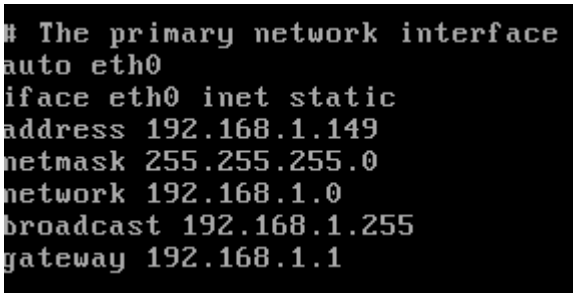


*Fig.2 Configurazione IP Metasploitable

Prima di passare alla configurazione dell'attacco, si procede con la configurazione IP delle macchine.

Su **Kali ----> *Edit Connection,*** si modifica l'indirizzo IP statico esistente con ***192.168.1.134***

Su **Metasploitable ----> nano /etc/network/interfaces**, si imposta (come richiesto) l'indirizzo IP in ***192.168.1.149***

Per verificare la connessione di entrambe le macchine viene effettuato effettuato un **ping.**

5.2) SCANSIONE SERVIZIO FTP METASPLOITABLE

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.98 ( https://nmap.org ) a
:53 -0500
Nmap scan report for 192.168.1.149
Host is up (0.0049s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
```

**Fig.3 Scansione servizi Metasploitable*

Prima di passare all'exploit, è stata effettuata una piccola scansione del servizio **FTP** per vedere quale servizio è attivo e su quale porta gira.

5.3) CONFIGURAZIONE ATTACCO METASPLOIT

```
└─$ msfconsole
àMetasploit tip: Run modules in the background with run -j so you can
keep working

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ 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 D
ate  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 Ex
ecution


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

*Fig.4 Ricerca exploit servizio FTP

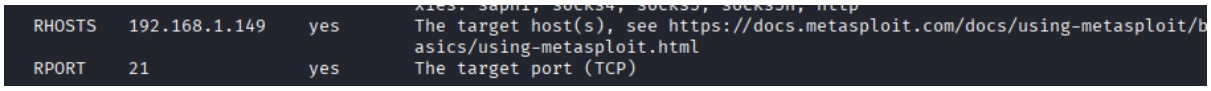


*Fig.5 Configurazione target

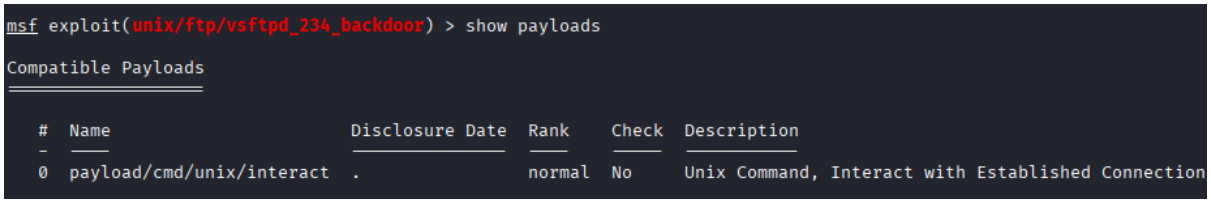
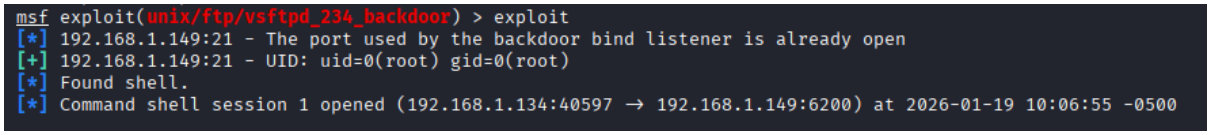


*Fig.6 Configurazione payload



*Fig,7 Run dell'exploit

Dopo la scansione, si passa alla ricerca di un possibile exploit del servizio **vsftpd** attraverso il comando ***search vsftpd*** e come in ***Fig.4***, risultano 2 exploit:

- **auxiliary/dos/ftp/vsftpd_232 ----->** ci permette di causare un attacco DOS al servizio FTP
- **exploit/unix/ftp/vsftpd_234_backdoor ----->** ci permette di avere accesso alla macchina tramite una backdoor

Dato che l'obiettivo è **di avere accesso al root della macchina target,** viene utilizzato il secondo exploit.

Prossimo step è la selezione del target dove viene inserito **l'IP e la porta della Metasploitable** (192.168.1.149;21) e la configurazione del payload disponibile per quell'exploit.

Dopo aver configurato e lanciato l'attacco.si può notare che si hanno permessi root***(gid=0(root))***, che consentono di creare, modificare o eliminare qualsiasi file presente sul target.

Inoltre, viene evidenziata anche l'effettiva connessione con la macchina target sulla porta **6200**(la porta della backdoor).

5.4) ACCESSO METASPLOITABLE

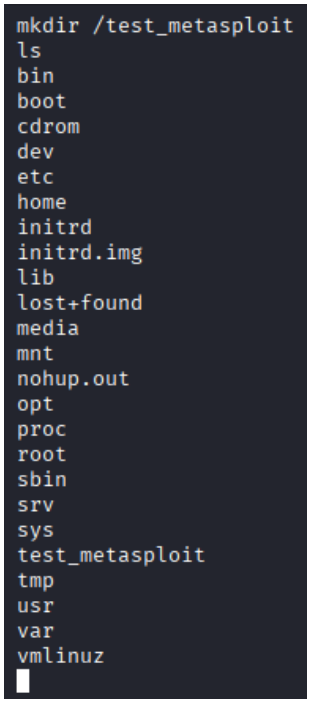


*Fig.8 creazione cartella in root (/)

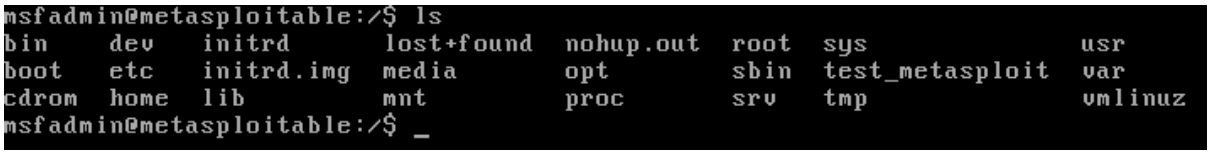


*Fig.9 Verifica attacco

Per verificare l'effettivo successo dell'exploit, vengono inseriti dei comandi come:

- **pwd** ----> per stampare la directory dove ci si trova
- **ls** ----> per stampare il contenuto all'interno di "/"
- **mkdir** ----> per creare una cartella all'interno del root

Come ultimo passaggio è stata effettuata la verifica tramite il comando **ls** nella Metasploitable e come mostrato in ***Fig.9***, l'exploit è stato effettuato con successo.

---

6)CONCLUSIONE

L'attività svolta ha dimostrato come una vulnerabilità nota in un servizio obsoleto possa essere sfruttata per ottenere il controllo totale di un sistema remoto. Attraverso l'uso di **Metasploit**, è stato possibile

automatizzare le fasi di exploit, evidenziando la criticità di una backdoor che garantisce i privilegi di **root**.

Per mitigare questi attacchi potenzialmente dannosi, è necessario:

- **Configurazione del Firewall ----->** Poiché la backdoor apre una connessione sulla porta **6200**, un firewall dovrebbe bloccare qualsiasi traffico in entrata
- **Patching dei software ----->** Passare a versioni aggiornate dei servizi riduce drasticamente la probabilità di successo degli exploit
- **Disabilitazione di servizi non necessari ----->** Se il protocollo non è necessario, deve essere disabilitato o sostituito con una versione più sicura (FTP ----> SFTP