METASPLOIT HACKING

Scopo dell'Esercizio

L'obiettivo di questo esercizio è utilizzare Metasploit per sfruttare una vulnerabilità relativa a Telnet sulla macchina Metasploitable. In particolare, verrà utilizzato il modulo auxiliary **telnet_version** per identificare e sfruttare una vulnerabilità associata al protocollo Telnet.

Dettagli di Configurazione

- Indirizzo IP di Kali Linux: 192.168.50.100/24
- Indirizzo IP di Metasploitable: 192.168.50.101

Exploit

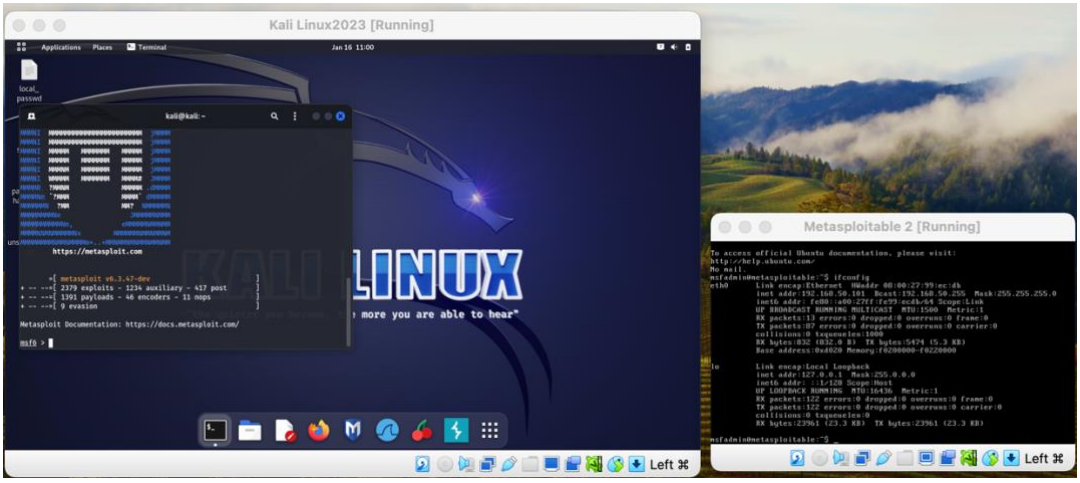
L'exploit è un insieme di comandi, script o tecniche che sfruttano vulnerabilità di un sistema per ottenere accesso non autorizzato o effettuare altre operazioni malevoli. Nel contesto della sicurezza informatica, l'exploit può essere utilizzato per testare la robustezza di un sistema o, in mani malintenzionate, per compromettere la sicurezza di un sistema.

Protocollo Telnet

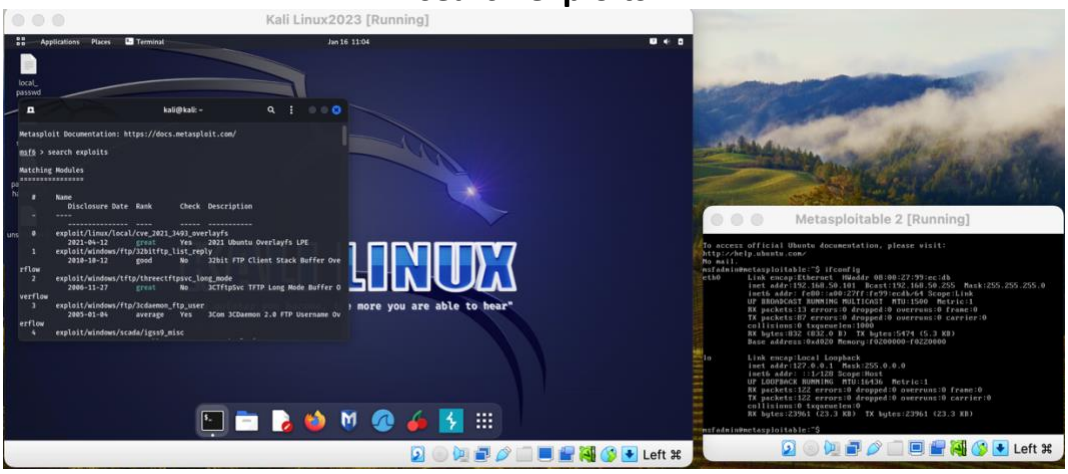
Telnet è un protocollo di rete utilizzato per stabilire una connessione remota tra dispositivi. Tuttavia, è noto per essere insicuro poiché invia dati, inclusi nomi utente e password, in chiaro senza crittografia.

SVOLGIMENTO DEI COMANDI:

Avvio msfconsole



search exploits



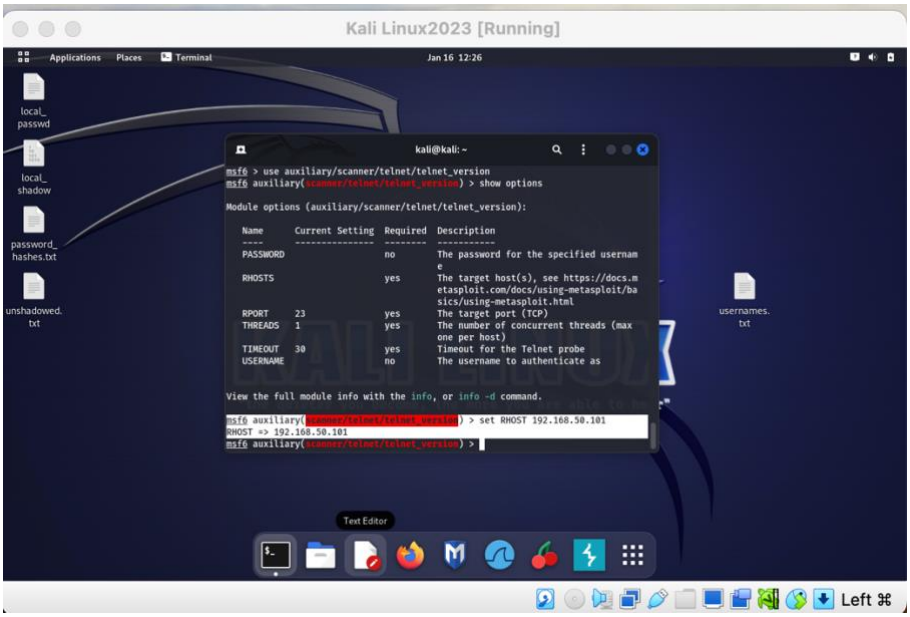
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) >
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

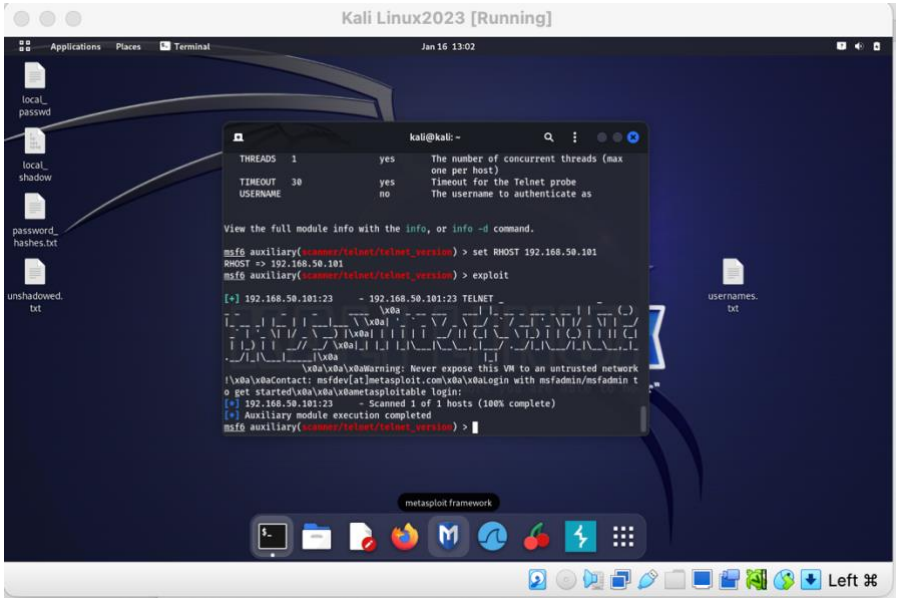
Module options (auxiliary/scanner/telnet/telnet_version):

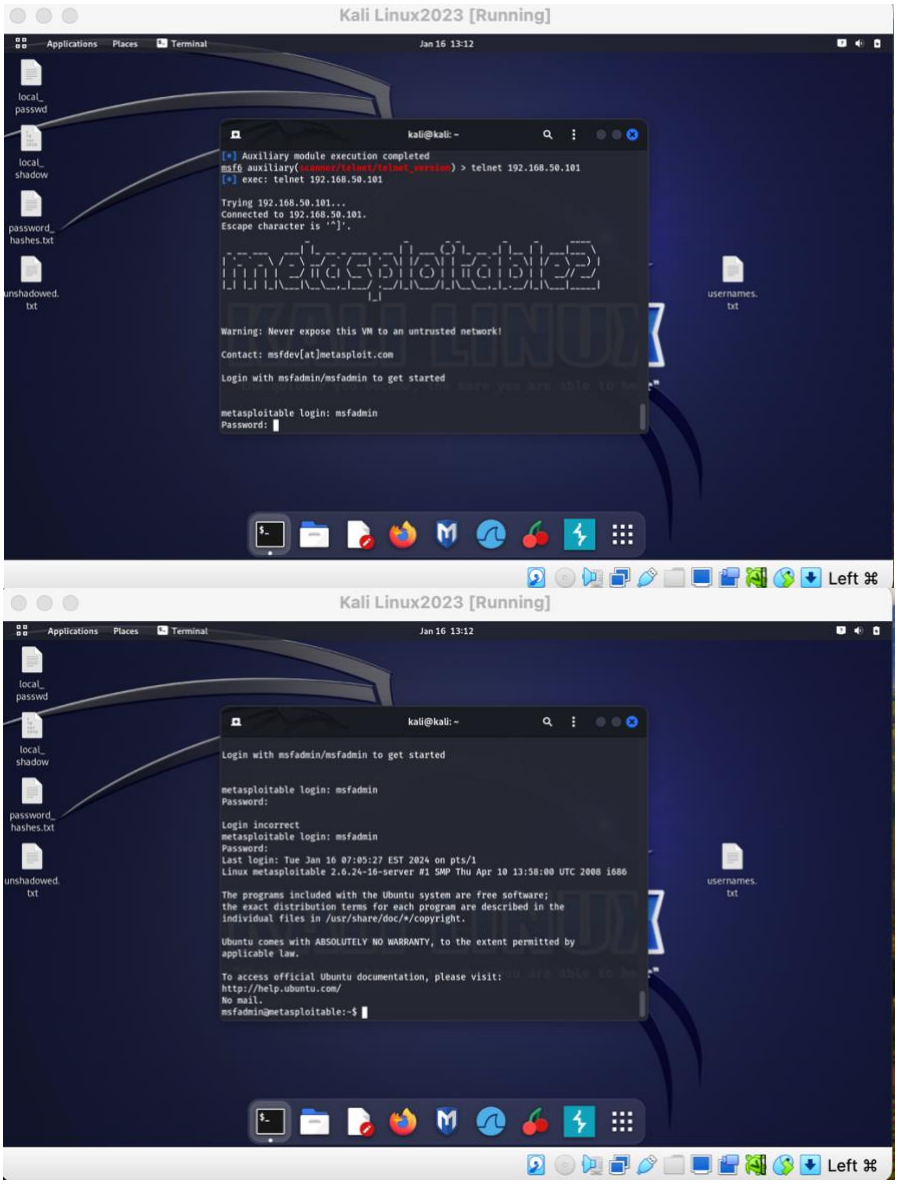
Name	Current Setting	Required	Description
PASSWORD		no	The password for the specified username
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	23	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)
TIMEOUT	30	yes	Timeout for the Telnet probe
USERNAME		no	The username to authenticate as

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

msf6 auxiliary(scanner/telnet/telnet_version) > set RHOST 192.168.50.101
RHOST => 192.168.50.101


Kali Linux2023 [Running]
Applications Places Terminal
Jan 16 12:26
kali@kali: ~
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options
Module options (auxiliary/scanner/telnet/telnet_version):
Name Current Setting Required Description
PASSWORD no The password for the specified username
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 23 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 30 yes Timeout for the Telnet probe
USERNAME no The username to authenticate as
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOST 192.168.50.101
RHOST => 192.168.50.101
msf6 auxiliary(scanner/telnet/telnet_version) >
local_passwd
local_shadow
password_hashes.txt
unshadowed.txt
usernames.txt
Text Editor
Left ⌘


Kali Linux2023 [Running]
Applications Places Terminal
Jan 16 13:02
kali@kali: ~
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 30 yes Timeout for the Telnet probe
USERNAME no The username to authenticate as
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOST 192.168.50.101
RHOST => 192.168.50.101
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
[+] 192.168.50.101:23 - 192.168.50.101:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login:
[+] 192.168.50.101:23 - Scanned 1 of 1 hosts (100% complete)
[+] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
local_passwd
local_shadow
password_hashes.txt
unshadowed.txt
usernames.txt
metasploit framework
Left ⌘



Conclusione

L'esecuzione dell'esercizio di exploit sulla macchina Metasploitable attraverso Telnet ha fornito una panoramica chiara delle vulnerabilità associate a questo protocollo di rete e delle modalità di sfruttamento tramite Metasploit.

Risultati dell'Esercizio

Dopo la corretta configurazione del modulo **telnet_version** e l'individuazione del target Metasploitable (192.168.50.101), l'esecuzione dell'exploit ha restituito un successo. L'analisi del banner Telnet ha rivelato informazioni utili sulla versione e ha permesso l'accesso al sistema.

Analisi della Vulnerabilità

La vulnerabilità sfruttata è riconducibile alla mancanza di sicurezza intrinseca del protocollo Telnet, che trasmette dati, inclusi nomi utente e password, in modo non crittografato.

Questo rende il sistema vulnerabile a intercettazioni malevole e accessi non autorizzati.

Raccomandazioni di Sicurezza

In luce di questi risultati, è fortemente raccomandato:

Evitare l'uso di Telnet: Date le sue vulnerabilità di sicurezza, Telnet dovrebbe essere evitato in favore di protocolli più sicuri come SSH, che forniscono comunicazioni cifrate.

Aggiornamento e Patching: Mantenere sempre i sistemi aggiornati con le patch di sicurezza più recenti per mitigare vulnerabilità note.

Monitoraggio del Traffico di Rete: Implementare sistemi di monitoraggio del traffico di rete per rilevare e prevenire eventuali attività sospette o tentativi di exploit.

Politiche di Accesso Sicure: Implementare politiche di accesso basate sul principio del privilegio minimo necessario e applicare rigorose pratiche di autenticazione per limitare l'accesso non autorizzato.

Riflessioni Finali

L'esercizio ha evidenziato l'importanza della sicurezza delle comunicazioni di rete e la necessità di adottare misure proattive per proteggere i sistemi. L'uso di strumenti come Metasploit, se applicato in un contesto etico e formativo, può fornire una comprensione approfondita delle vulnerabilità e delle contromisure necessarie per proteggere gli ambienti di rete.