Report sulla Scansione e Sfruttamento della Vulnerabilità Telnet sulla Macchina Metasploitable

Introduzione

In questo esercizio, ho utilizzato Kali Linux per sfruttare una vulnerabilità del servizio Telnet presente su una macchina virtuale Metasploitable. L'obiettivo principale era quello di identificare la versione del servizio Telnet in esecuzione sulla macchina target e successivamente verificare le credenziali di accesso.

Configurazione delle Macchine Virtuali

Ho configurato due macchine virtuali su VirtualBox con i seguenti indirizzi IP:

- **Kali Linux**: 192.168.1.111
- **Metasploitable**: 192.168.1.112

Ho assicurato che entrambe le macchine fossero connesse alla stessa rete locale in modalità "Scheda con bridge" (Bridge Adapter).

Passaggi Eseguiti

1. Avvio di Metasploit su Kali Linux

Per prima cosa, ho avviato Metasploit sulla macchina Kali Linux. Ho aperto un terminale e ho eseguito il comando:

```
sudo msfconsole
```

2. Caricamento del Modulo Telnet Version Scanner

Una volta caricato Metasploit, ho selezionato il modulo telnet_version con il seguente comando:

```
use auxiliary/scanner/telnet/telnet_version
```

3. Visualizzazione delle Opzioni del Modulo

Per verificare le opzioni disponibili per il modulo, ho eseguito il comando:

```
show options
```

4. Configurazione del Target

Ho configurato l'indirizzo IP della macchina Metasploitable come target (RHOSTS):

```
set RHOSTS 192.168.1.112
```

Ho anche verificato che la porta di destinazione (RPORT) fosse impostata correttamente su 23.

5. Esecuzione della Scansione

Ho eseguito la scansione per identificare la versione del servizio Telnet in esecuzione sulla macchina Metasploitable:

run

6. Analisi dei Risultati

L'output del comando ha restituito informazioni dettagliate sulla versione del servizio Telnet in esecuzione. Ad esempio:

[*] 192.168.1.112:23 - 192.168.1.112:23 - Telnet Banner: "Debian Linux Telnetd"

[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

7. Verifica delle Credenziali di Accesso

Ho preso nota delle credenziali di accesso fornite dall'output della scansione (ad esempio, msfadmin:msfadmin). Successivamente, ho aperto un nuovo terminale su Kali Linux e ho eseguito il comando per connettermi al servizio Telnet della macchina Metasploitable:

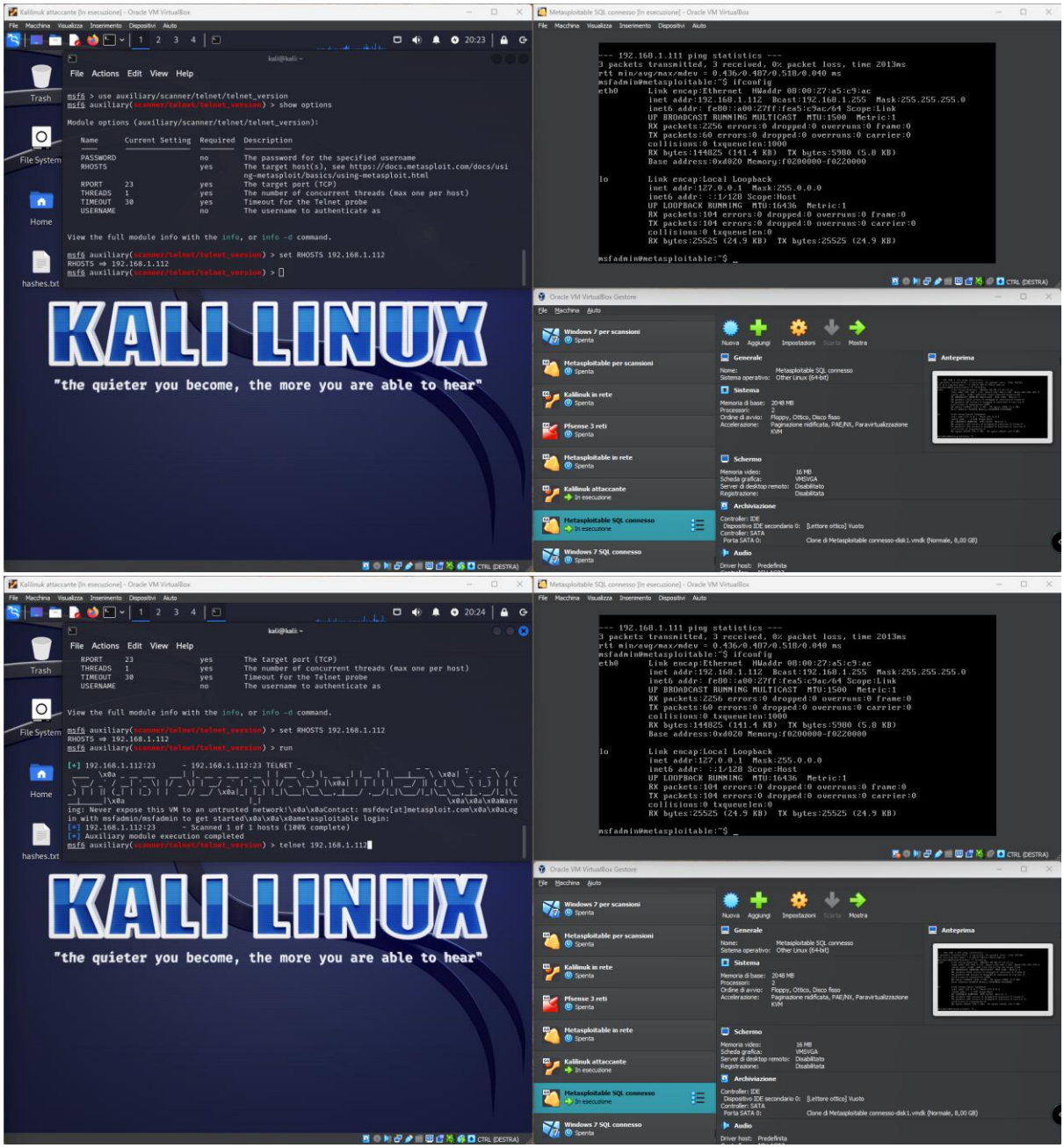
telnet 192.168.1.112

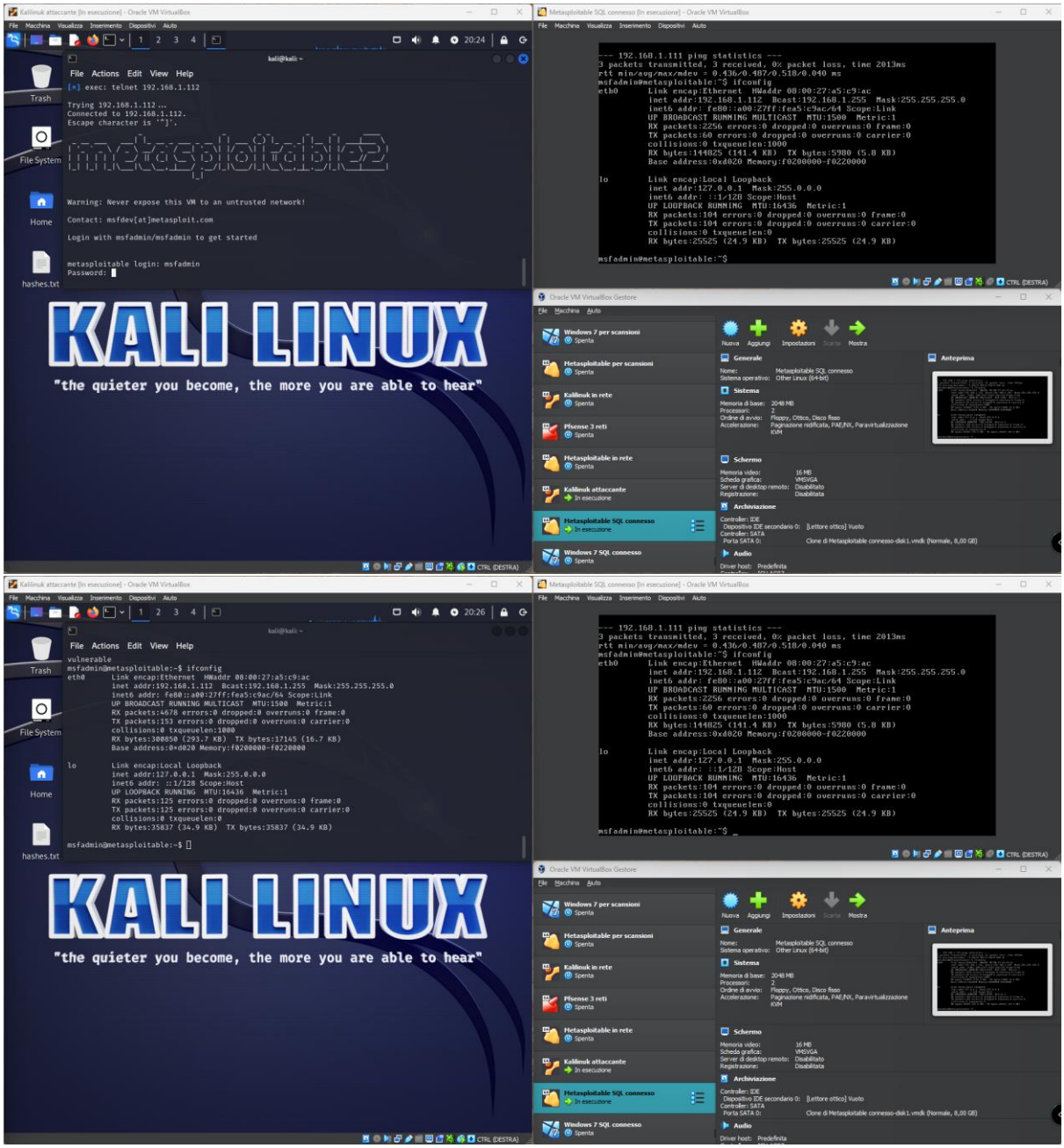
Ho inserito le credenziali quando richiesto e ho verificato l'accesso con successo.

Conclusione

Questo esercizio ha dimostrato come identificare e sfruttare una vulnerabilità del servizio Telnet utilizzando Metasploit. Ho appreso come configurare le macchine virtuali, eseguire scansioni di vulnerabilità e analizzare i risultati ottenuti. Questo processo è fondamentale per migliorare la sicurezza delle reti e dei sistemi informatici.

Screenshot


KALI LINUX
"the quieter you become, the more you are able to hear"
KALI LINUX
"the quieter you become, the more you are able to hear"


Kalilinux attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
[*] exec: telnet 192.168.1.112
Trying 192.168.1.112 ...
Connected to 192.168.1.112.
Escape character is '^]'.
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
KALI LINUX
"the quieter you become, the more you are able to hear"
Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox
--- 192.168.1.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2013ms
rtt min/avg/max/mdev = 0.436/0.407/0.510/0.040 ms
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a5:c9:ac
inet addr:192.168.1.112 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea5:c9ac/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2256 errors:0 dropped:0 overruns:0 frame:0
TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:144025 (141.4 KB) TX bytes:5980 (5.8 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:104 errors:0 dropped:0 overruns:0 frame:0
TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:25525 (24.9 KB) TX bytes:25525 (24.9 KB)
msfadmin@metasploitable:~$
Oracle VM VirtualBox Gestore
Windows 7 per scansioni
Metasploitable per scansioni
Kalilinux in rete
Pfsense 3 reti
Metasploitable in rete
Kalilinux attaccante
Metasploitable SQL connesso
Windows 7 SQL connesso
Nuova
Aggiungi
Impostazioni
Scarta
Mostra
Generale
Sistema
Schermo
Archiviazione
Audio
Anteprima

Kalilinux attaccante [In esecuzione] - Oracle VM VirtualBox
File Actions Edit View Help
vulnerable
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a5:c9:ac
inet addr:192.168.1.112 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea5:c9ac/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:4678 errors:0 dropped:0 overruns:0 frame:0
TX packets:153 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:300850 (293.7 KB) TX bytes:17145 (16.7 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:125 errors:0 dropped:0 overruns:0 frame:0
TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:35837 (34.9 KB) TX bytes:35837 (34.9 KB)
msfadmin@metasploitable:~$
KALI LINUX
"the quieter you become, the more you are able to hear"
Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox
--- 192.168.1.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2013ms
rtt min/avg/max/mdev = 0.436/0.407/0.510/0.040 ms
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a5:c9:ac
inet addr:192.168.1.112 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea5:c9ac/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2256 errors:0 dropped:0 overruns:0 frame:0
TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:144025 (141.4 KB) TX bytes:5980 (5.8 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:104 errors:0 dropped:0 overruns:0 frame:0
TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:25525 (24.9 KB) TX bytes:25525 (24.9 KB)
msfadmin@metasploitable:~$
Oracle VM VirtualBox Gestore
Windows 7 per scansioni
Metasploitable per scansioni
Kalilinux in rete
Pfsense 3 reti
Metasploitable in rete
Kalilinux attaccante
Metasploitable SQL connesso
Windows 7 SQL connesso
Nuova
Aggiungi
Impostazioni
Scarta
Mostra
Generale
Sistema
Schermo
Archiviazione
Audio
Anteprima