Report – Scansione del Servizio Telnet tramite Metasploit

---

1. Introduzione

Lo scopo di questo esercizio è analizzare il servizio **Telnet** presente sulla macchina vulnerabile **Metasploitable**, utilizzando il framework **Metasploit**.
L'attività rientra nella fase di **information gathering** e **service enumeration**, fondamentali in un processo di penetration testing.

In particolare, è stato utilizzato il modulo:

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

per individuare la presenza del servizio Telnet e raccogliere informazioni sulla sua versione e configurazione.

---

2. Ambiente di Test

L'ambiente di laboratorio è costituito da:

- **Attaccante**: Kali Linux
- **Target**: Metasploitable 2
- **Rete**: configurazione Host-Only / NAT (stessa subnet)

Entrambe le macchine virtuali sono correttamente configurate per comunicare tra loro.

---

3. Metodologia

3.1 Individuazione del Target

È stato individuato l’indirizzo IP della macchina Metasploitable tramite il comando:

```
ifconfig
```

L’indirizzo IP ottenuto è stato utilizzato come target della scansione (`RHOSTS`).

3.2 Avvio di Metasploit

Sulla macchina Kali Linux è stato avviato il framework Metasploit tramite il comando:

```
msfconsole
```

Una volta avviata la console, è stato caricato il modulo di scansione Telnet.

3.3 Caricamento del Modulo Telnet

Il modulo utilizzato è:

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

Successivamente sono state visualizzate le opzioni disponibili tramite:

```
show options
```

e impostato l’indirizzo IP del target:

```
set RHOSTS <IP_Metasploitable>
```

3.4 Esecuzione della Scansione

La scansione del servizio Telnet è stata avviata con il comando:

```
run
```

Il modulo ha tentato la connessione alla porta **23/TCP**, predefinita per il servizio Telnet, al fine di ottenere il banner del servizio.

---

4. Risultati Ottenuti

L'output della scansione ha confermato che:

- Il servizio **Telnet è attivo** sulla macchina Metasploitable
- Il server Telnet risponde con un **banner informativo**
- Sono state ottenute informazioni sul sistema operativo e sulla versione del servizio

Questo comportamento indica una configurazione **insicura**, poiché il servizio espone informazioni sensibili che possono essere utilizzate da un attaccante per pianificare attacchi successivi.

---

5. Analisi di Sicurezza

L'utilizzo di Telnet rappresenta un rischio significativo per la sicurezza in quanto:

- Le comunicazioni avvengono **in chiaro**
- Le credenziali possono essere intercettate tramite attacchi di sniffing
- Il banner del servizio facilita attività di **fingerprinting**
- Il servizio è spesso soggetto ad attacchi di **brute force**

In un contesto reale, la presenza di Telnet su un sistema rappresenta una **grave vulnerabilità**.

---

6. Contromisure

Per mitigare i rischi associati al servizio Telnet si raccomanda di:

- Disabilitare Telnet
- Utilizzare **SSH** come alternativa sicura
- Limitare l’accesso ai servizi di rete tramite firewall
- Evitare l’esposizione di banner informativi

---

7. Conclusione

L’esercizio ha dimostrato come sia possibile, tramite Metasploit, individuare e analizzare un servizio Telnet attivo su un sistema vulnerabile.
La scansione ha evidenziato una configurazione non sicura, confermando l’importanza delle attività di enumerazione per identificare potenziali punti di attacco all’interno di una rete.