Antonio Podda S7L2

Relazione: Sfruttamento della Vulnerabilità Telnet su Metasploitable

Fase 1: Avvio della console di Metasploit

Per iniziare, si è aperto il terminale su Kali Linux e si è avviata la console di Metasploit con il seguente comando:

```
msfconsole
```

La console di Metasploit consente di utilizzare moduli specifici per individuare e sfruttare vulnerabilità su sistemi target.

Fase 2: Selezione del modulo Telnet Scanner

Una volta aperta la console, si è selezionato il modulo auxiliary/scanner/telnet/telnet_version utilizzando il comando:

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

Questo modulo permette di effettuare una scansione del servizio Telnet attivo su una macchina target, determinandone la versione e potenzialmente recuperando informazioni utili.

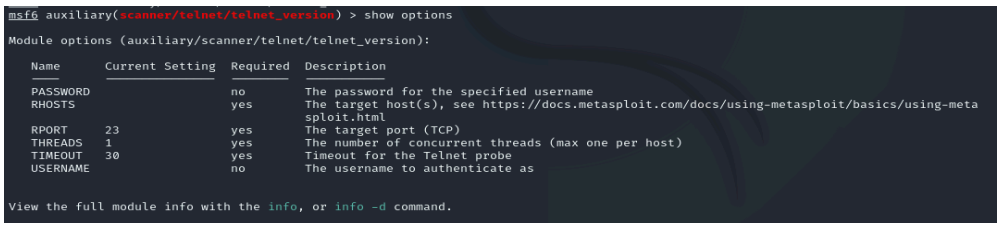
Fase 3: Controllo e configurazione dei parametri

Per visualizzare le opzioni disponibili per il modulo scelto, si è utilizzato il comando:

```
show options
```

I principali parametri visualizzati sono stati:

- RHOSTS: Indirizzo IP della macchina target (Metasploitable).
- RPORT: Porta su cui è in ascolto il servizio Telnet (default `23`).
- THREADS: Numero di thread utilizzati per l'analisi.



Successivamente, è stato configurato l'indirizzo IP della macchina target con il seguente comando:

```
set RHOSTS 192.168.1.40
```

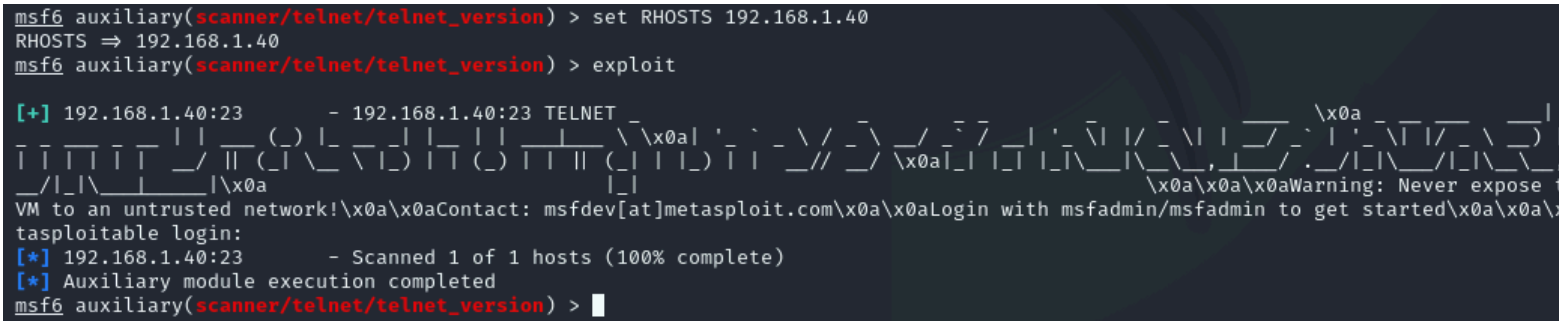
Fase 4: Avvio della scansione

Una volta configurati i parametri, si è lanciato il modulo utilizzando il comando:

```
exploit
```

L'output del modulo ha mostrato con successo informazioni relative al servizio Telnet, inclusa la presenza di credenziali predefinite. Nel caso specifico, sono state recuperate le credenziali:

- Username: `msfadmin`
- Password: `msfadmin`



Fase 5: Verifica dell'accesso al servizio Telnet

Per verificare l'efficacia dell'exploit e l'autenticità delle credenziali recuperate, è stato effettuato un collegamento al servizio Telnet della macchina Metasploitable con il comando:

bash

Copia codice

```
telnet 192.168.1.40
```

Al prompt di login, sono state inserite le credenziali trovate:

- Username: `msfadmin`
- Password: `msfadmin`

Il login ha avuto successo, confermando la vulnerabilità del servizio Telnet e la validità delle credenziali.

Conclusioni

In questo esercizio:

1. È stata sfruttata la vulnerabilità del servizio Telnet su Metasploitable utilizzando Metasploit.
2. Sono state identificate e recuperate le credenziali predefinite msfadmin/msfadmin.
3. Si è verificato l’accesso al servizio Telnet con successo, dimostrando come servizi con credenziali deboli o predefinite rappresentino un rischio di sicurezza.
4.