Relazione: Sfruttamento della Vulnerabilità Telnet su Metasploitable con Metasploit

Introduzione

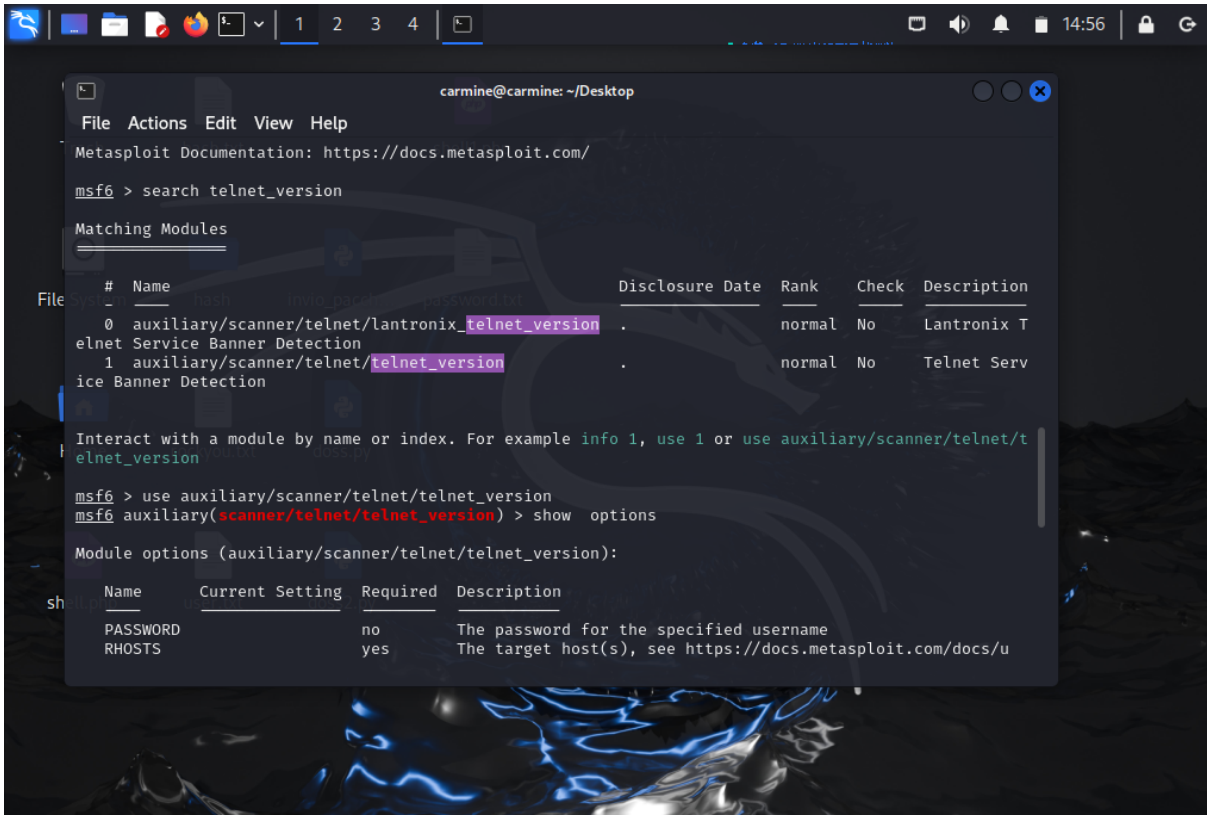
L'obiettivo di questo esperimento è stato quello di sfruttare una vulnerabilità relativa al protocollo Telnet sulla macchina virtuale Metasploitable, utilizzando il framework Metasploit su una macchina Kali Linux. Questa attività è stata svolta al fine di acquisire i dati d'accesso e l'accesso della macchina metasploitable2 e per comprendere le potenziali minacce legate all'esposizione di servizi come Telnet.

Ambiente di Lavoro

- **Sistema Operativo:** Kali Linux (192.168.101.201)
- **Target:** Metasploitable (192.168.101.40)
- **Strumenti:** Metasploit

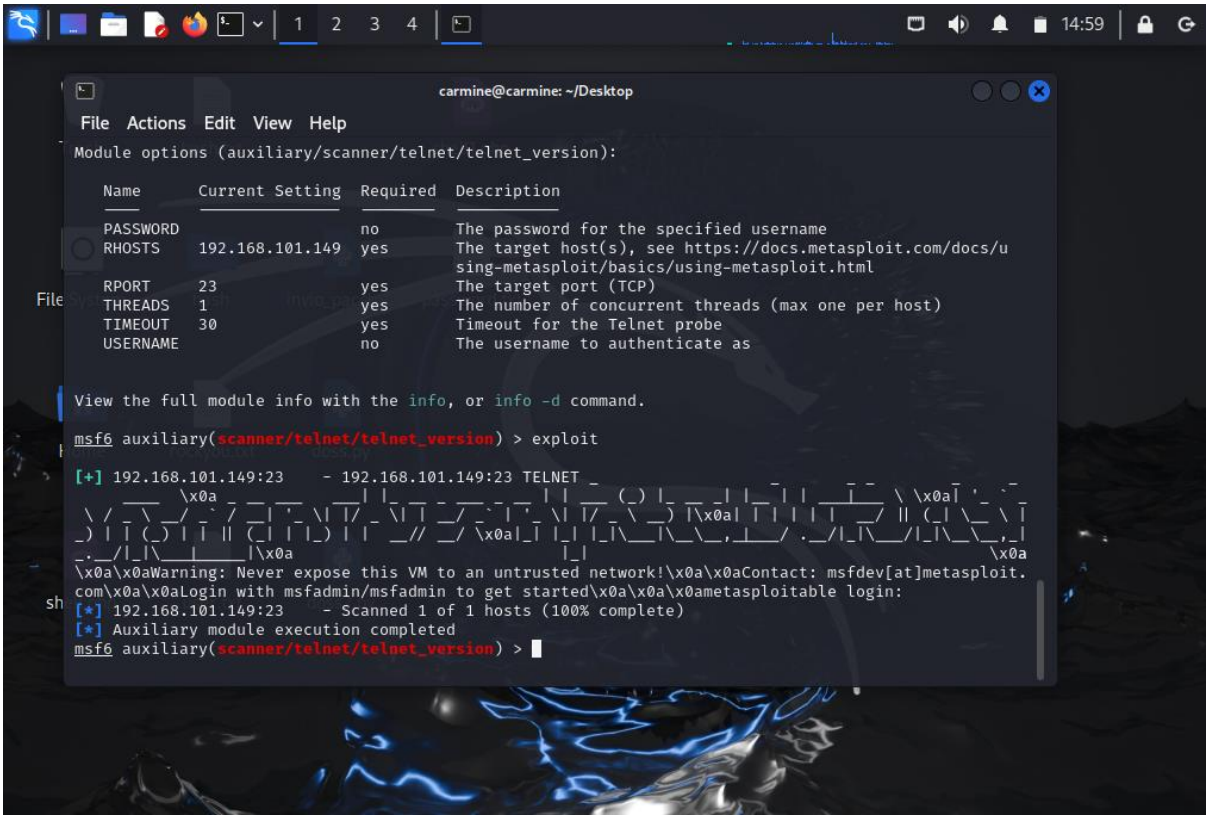
Procedimento

1. **Configurazione della Rete:**
    a. **Kali Linux:** L'indirizzo IP è stato configurato manualmente su 192.168.101.201.
    b. **Metasploitable:** L'indirizzo IP è stato configurato manualmente su 192.168.101.149.
    c. **Verifica della Connettività:** È stata effettuata una Ping test dalla macchina Kali alla macchina Metasploitable per verificare la corretta comunicazione tra le due macchine.
2. **Avvio di Metasploit:**
    a. È stato aperto un terminale su Kali Linux e avviato Metasploit con il comando **`msfconsole`**.
3. **Ricerca del Modulo:**
    a. All'interno della console Metasploit, è stato utilizzato il comando **`search_telnet`** per individuare i moduli disponibili per lo sfruttamento di vulnerabilità legate al protocollo Telnet.



4. **Selezione del Modulo:**
    a. Tra i moduli trovati, è stato selezionato il modulo **`auxiliary/scanner/telnet/telnet_version`.** Questo modulo è stato scelto in quanto permette di ottenere informazioni sulla versione del servizio Telnet in esecuzione sulla macchina target, un primo passo fondamentale per identificare eventuali vulnerabilità.
5. **Configurazione del Modulo:**
    a. Il modulo è stato configurato con i seguenti parametri:
        - RHOSTS: 192.168.101.149 (indirizzo IP della macchina target)
        - RPORT: 23 (porta standard del servizio Telnet)

6. **Esecuzione del Modulo:**
    a. È stato eseguito il comando `exploit` per avviare lo scanner. E come possiamo vedere ci dà i dati d'accesso (password e username).



7. **Analisi dei Risultati:**
   a. Siamo riusciti ad entrare nella macchina metasploitable2 aprendo un altro terminale ed eseguendo il comando telnet 192.168.101.149

Conclusioni

Sulla base dell'esperimento condotto, è possibile trarre le seguenti conclusioni:

1. **Vulnerabilità di Telnet:** È stata evidenziata la pericolosità di servizi come Telnet, che, se non adeguatamente protetti, possono rappresentare un punto di ingresso per attacchi informatici. La facilità con cui è stato possibile ottenere informazioni sulla versione del servizio Telnet in esecuzione sulla macchina Metasploitable dimostra come un attaccante possa rapidamente identificare potenziali vulnerabilità.
2. **Efficacia di Metasploit:** Metasploit si è dimostrato uno strumento potente e versatile per la valutazione della sicurezza di un sistema. Il modulo `auxiliary/scanner/telnet/telnet_version` ha permesso di eseguire una scansione rapida ed efficace del servizio Telnet, fornendo informazioni cruciali per la successiva fase di sfruttamento.
3. **Importanza dell'aggiornamento:** L'utilizzo di software obsoleti, come nel caso del servizio Telnet, aumenta significativamente il rischio di essere vittima di attacchi informatici. È fondamentale mantenere aggiornati tutti i sistemi e le applicazioni, applicando prontamente le patch di sicurezza rilasciate dai vendor.
4. **Necessità di misure di sicurezza:** Oltre all'aggiornamento dei software, è necessario adottare altre misure di sicurezza, come:
    a. **Disabilitazione di servizi non necessari:** Se possibile, disabilitare servizi come Telnet che non sono essenziali per il funzionamento del sistema.
    b. **Utilizzo di firewall:** Implementare un firewall per filtrare il traffico in entrata e in uscita, bloccando le connessioni provenienti da indirizzi IP sospetti.
    c. **Sistemi di rilevamento delle intrusioni:** Utilizzare sistemi IDS (Intrusion Detection System) per monitorare l'attività di rete e rilevare eventuali anomalie.
    d. **Gestione delle credenziali:** Adottare politiche di gestione delle password robuste, evitando password deboli e riutilizzando le stesse credenziali su più sistemi.

In conclusione, l'esercizio ha evidenziato come la sicurezza informatica sia un tema di fondamentale importanza. Anche sistemi apparentemente semplici, come Metasploitable, possono essere compromessi se non vengono adottate le adeguate misure di protezione. È quindi fondamentale acquisire le competenze necessarie per valutare la sicurezza dei sistemi e per mitigare i rischi associati agli attacchi informatici.