

Valutazione dell'esposizione SSH tramite Hydra

Ambiente di test

L'attività è stata svolta in un laboratorio controllato utilizzando macchine virtuali.

- Macchina attaccante: Kali Linux – 192.168.64.2
- Macchina vittima: Kali Linux – 192.168.64.14
- Rete: rete virtuale privata (UTM / NAT)

L'obiettivo era valutare l'impatto di un servizio SSH esposto e verificare l'efficacia di un attacco di brute-force sulle credenziali.

Attivazione del servizio SSH sulla vittima

Per impostazione predefinita, Kali Linux non espone servizi non necessari. Per simulare uno scenario realistico di configurazione errata, il servizio SSH è stato attivato manualmente sulla macchina vittima.

Sulla macchina 192.168.64.14 sono stati eseguiti i seguenti comandi:

```
sudo systemctl start ssh  
sudo systemctl enable ssh
```

Lo stato del servizio è stato verificato con:

```
sudo systemctl status ssh
```

Dopo l'avvio, il demone SSH risultava in ascolto sulla porta TCP 22, rendendo il servizio accessibile dalla rete.

Questo scenario rappresenta una situazione comune, in cui l'accesso remoto viene abilitato senza un'adeguata fase di hardening.

Enumeration del servizio

Dalla macchina attaccante è stata eseguita una scansione mirata per verificare l'esposizione del servizio SSH.

```
nmap -p22 -sV 192.168.64.14
```

Risultati:

- Porta 22/TCP aperta
- Servizio OpenSSH attivo
- Autenticazione tramite password abilitata

Queste informazioni hanno confermato SSH come potenziale superficie di attacco.

Metodologia di attacco

Per il test delle credenziali è stato utilizzato Hydra, uno strumento specializzato per attacchi di autenticazione.

Hydra è stato preferito a Metasploit per la sua maggiore velocità e per il focus specifico sul brute-force dei servizi di login.

Strumento utilizzato

- THC Hydra v9.5

Configurazione

- Servizio target: SSH
- Utente testato: kali
- Wordlist: lista di password comuni
- Thread limitati per evitare blocchi dell'account

Comando eseguito:

```
hydra -l kali -P /usr/share/wordlists/john.lst -t 4 ssh://192.168.64.14
```

Risultati

Hydra è riuscito a connettersi correttamente al servizio SSH ed ha testato le credenziali in modo sequenziale.

- Con password deboli configurate sulla vittima, Hydra è stato in grado di individuare credenziali valide.
- Con password robuste, l'attacco è fallito, come previsto.

Questo dimostra che:

- SSH non è vulnerabile di per sé
- La sicurezza dipende interamente dalla configurazione e dalla forza delle credenziali

Impatto sulla sicurezza

Un servizio SSH esposto con autenticazione basata su password deboli rappresenta un rischio elevato.

Un attaccante che ottiene accesso SSH può:

- ottenere una shell interattiva
- eseguire comandi sul sistema
- tentare escalation di privilegi
- muoversi lateralmente nella rete

Osservazioni principali

- Hydra è significativamente più veloce di Metasploit per attacchi di brute-force.
- Wordlist molto grandi risultano inefficaci senza una fase di enumeration preventiva.
- Liste di password piccole e mirate producono risultati più rapidi e realistici.
- Il brute-force è rumoroso e dovrebbe essere considerato come ultima opzione.

Contromisure consigliate

Per mitigare il rischio associato a SSH:

- Disabilitare l'autenticazione tramite password
- Utilizzare autenticazione tramite chiavi SSH

- Disabilitare il login diretto di root
- Limitare l'accesso SSH per indirizzo IP
- Monitorare regolarmente i log di autenticazione