RELAZIONE PROGETTO S6-L5

Authentication cracking con Hydra

Introduzione

L'autenticazione è uno dei principali meccanismi di sicurezza utilizzati per proteggere l'accesso a sistemi, applicazioni e reti. Tuttavia, se le credenziali di accesso non sono adeguatamente protette, gli attaccanti possono tentare di bypassare tali misure. Uno degli strumenti più potenti per eseguire attacchi di cracking delle credenziali è Hydra. Hydra è uno strumento open-source utilizzato per eseguire attacchi di forza bruta su una varietà di protocolli e servizi, tra cui SSH, FTP, HTTP, Telnet, e molti altri.

Cos'è Hydra?

Hydra (o THC-Hydra) è uno strumento di cracking delle password utilizzato per effettuare attacchi di forza bruta e dizionario su vari protocolli di rete. Il programma è noto per la sua velocità e flessibilità nell'attaccare i sistemi di autenticazione, sfruttando diverse tecniche, come gli attacchi a dizionario, gli attacchi combinati e le forze bruta (brute force).

Hydra supporta un'ampia gamma di protocolli, rendendolo uno degli strumenti più usati dai professionisti della sicurezza per testare la robustezza delle password di sistemi remoti. È particolarmente utile per simulare attacchi di cracking delle password e per testare la sicurezza delle reti aziendali e dei server.

Come funziona l'Authentication Cracking con Hydra?

L'attacco di cracking delle password tramite Hydra si basa sulla tecnica della forza bruta, che consiste nel tentare sistematicamente tutte le possibili combinazioni di password, o tramite un dizionario di password comuni, fino a trovare quella corretta. Il programma interagisce direttamente con i servizi di rete come SSH, FTP, HTTP, ecc., tentando di inviare combinazioni di credenziali fino a che una di queste non venga accettata dal sistema di destinazione.

Fasi principali dell'attacco di cracking con Hydra:

1. Scelta del servizio di destinazione:

Hydra può essere configurato per attaccare una vasta gamma di servizi, tra cui SSH, FTP, RDP, e HTTP. In questo esempio, supponiamo che si stia cercando di attaccare un servizio SSH.

2. Selezione delle credenziali da testare:

Esistono due principali modalità di attacco:

- Attacco a dizionario: Hydra tenta tutte le password contenute in un file di dizionario (lista di password comuni).

- Attacco a forza bruta: Hydra tenta tutte le combinazioni possibili di caratteri, ma è molto più lento e costoso in termini di risorse.

3. Impostazione delle opzioni di Hydra:

Hydra richiede di specificare l'indirizzo IP del sistema target, il servizio da attaccare (es. SSH), e il file di dizionario o l'elenco delle possibili combinazioni di password. Inoltre, l'attacco può essere configurato per limitare il numero di tentativi al secondo, il che aiuta a evitare il blocco del sistema di destinazione a causa di troppi tentativi.

4. Esecuzione dell'attacco:

Una volta che le credenziali da testare e il target sono configurati, Hydra inizia a tentare le combinazioni di username e password in modo rapido ed efficiente. Ogni tentativo viene inviato al sistema target, che risponde con un "successo" o un "errore". Se una delle combinazioni è corretta, l'attacco si interrompe e Hydra segnala la password corretta.

Comando Hydra per l'autenticazione SSH

Un esempio di comando per un attacco di cracking delle credenziali SSH con Hydra potrebbe essere:

hydra -l username -P /path/to/dictionary.txt ssh://192.168.1.10

In questo comando:

- `-l username`: specifica il nome utente da testare.

- `-P /path/to/dictionary.txt`: fornisce il percorso al file dizionario contenente le password da provare.

- `ssh://192.168.1.10`: indica il servizio SSH in esecuzione sulla macchina di destinazione, con l'indirizzo IP 192.168.1.10.

Tecniche di difesa contro gli attacchi di cracking con Hydra

Esistono diverse contromisure per proteggere i sistemi dagli attacchi di cracking delle credenziali:

1. Uso di password forti e complesse: Le password devono essere lunghe, complesse e contenere una combinazione di lettere, numeri e caratteri speciali.

2. Autenticazione a due fattori (2FA): Abilitare l'autenticazione a due fattori riduce notevolmente il rischio di accesso non autorizzato, poiché richiede un secondo fattore (come un codice inviato tramite SMS) oltre alla password.

3. Bloccare gli IP dopo un certo numero di tentativi falliti: Configurare i sistemi per bloccare temporaneamente l'accesso da un indirizzo IP dopo un numero predefinito di tentativi falliti può rallentare o impedire gli attacchi di forza bruta.

4. Monitoraggio delle attività di login: La rilevazione di attività sospette, come tentativi di login provenienti da indirizzi IP sconosciuti o da più posizioni geografiche, può aiutare a prevenire attacchi in corso.

SVOLGIMENTO

Per completare l'esercizio, segui questi passaggi:

1. Configurazione del servizio SSH

Prima di tutto, assicuriamoci che il servizio SSH sia abilitato sulla macchina Kali. Puoi verificarlo e abilitarlo con i seguenti comandi:

sudo systemctl status ssh # Controlla se SSH è attivo

sudo systemctl start ssh # Avvia il servizio SSH se non è in esecuzione

sudo systemctl enable ssh # Assicurati che SSH si avvii automaticamente al boot

Successivamente, crea un nuovo utente per testare la connessione SSH:

sudo adduser test\_user ( inseriremo la password “testpass”)

Verifica la connessione SSH al tuo sistema (sostituisci `ip\_kali` con l'IP della tua macchina Kali):

ssh test\_user@ip\_kali

Se la connessione è andata a buon fine, accederemo come `test\_user`.

2. \*\*Attacco con Hydra\*\*

Una volta verificato che l'accesso SSH funziona, passiamo all'attacco di cracking della password utilizzando Hydra. Prima, assicuriamoci di avere Seclists installato per avere delle wordlist di username e password:

sudo apt-get install seclists

Ora, prepariamoci a eseguire il comando Hydra per effettuare il cracking. La sintassi per utilizzare le wordlist di Seclists (sostituendo `username\_list` e `password\_list` con i percorsi alle tue liste) è la seguente:

hydra -L /path/to/username\_list -P /path/to/password\_list ssh://ip\_kali

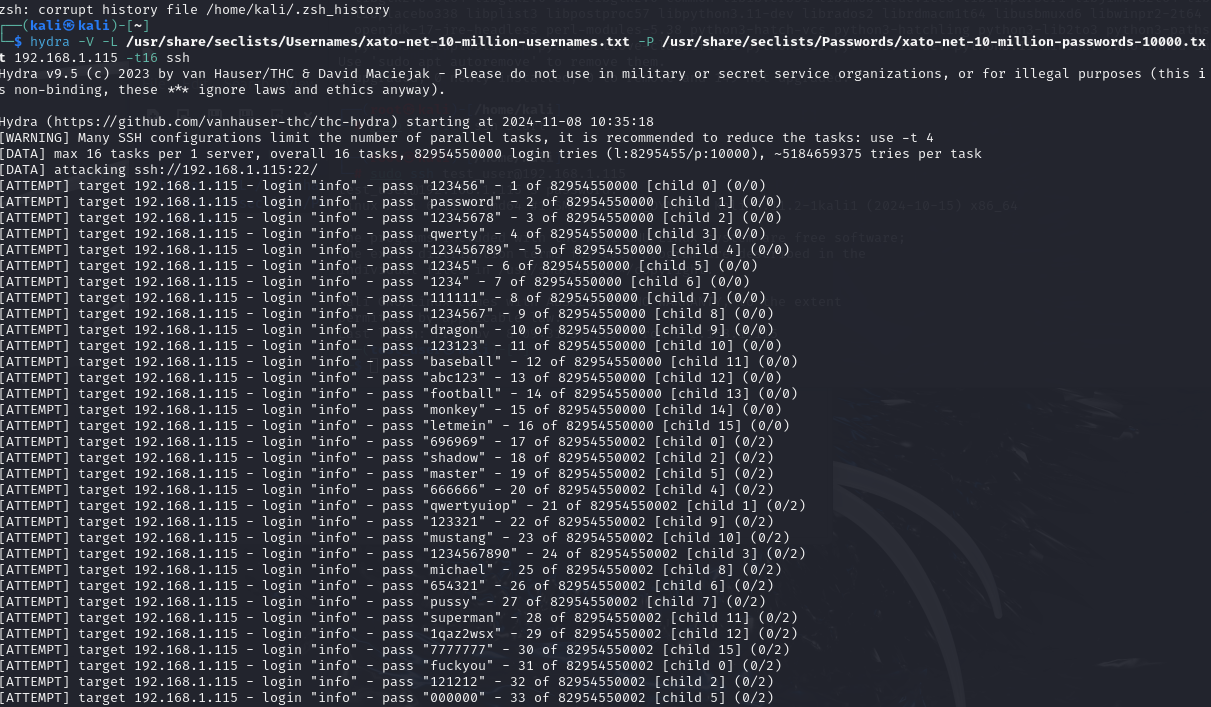
Dove:

- L specifica la lista degli username (puoi usare una lista come `SecLists/User-Names/top-usernames-shortlist.txt`).

-P specifica la lista delle password (puoi usare una lista come `SecLists/Passwords/rockyou.txt`).

- `ssh://ip\_kali` è il target (sostituisci `ip\_kali` con l'indirizzo IP della macchina Kali).





Ovviamente l’attacco vedremo che ci impiegherà molto molto tempo, e per ovviare a questa cosa sapendo la password potremmo cercare una lista molto più corta dove sappiamo che al suo interno c’è la password da noi cercata.

FTP

FTP (File Transfer Protocol) è un protocollo di rete per trasferire file tra un client e un server. Usa due canali: uno per i comandi (porta 21) e uno per i dati (porta 20). Permette di caricare e scaricare file in modalità attiva o passiva. Essendo non crittografato, è vulnerabile agli attacchi e viene spesso sostituito da protocolli più sicuri come SFTP e FTPS.

Passaggi da eseguire su kali in ordine:

* Il comando `sudo apt-get install vsftpd` installa \*\*vsftpd\*\* (Very Secure FTP Daemon), un server FTP sicuro e leggero per Linux. Questo programma consente di configurare un server FTP con supporto per connessioni crittografate (FTPS), accesso anonimo e varie opzioni di configurazione per gestire utenti e permessi sui file.

sudo apt-get install vsftpd

* Il comando `sudo systemctl status vsftpd` mostra lo stato del servizio \*\*vsftpd\*\* (Very Secure FTP Daemon) sul sistema. Con questo comando puoi vedere se il server FTP è attivo (running), inattivo (inactive), o se ha avuto errori di avvio.

sudo systemctl status vsftpd

* Il comando `sudo systemctl start vsftpd` avvia il servizio \*\*vsftpd\*\* (Very Secure FTP Daemon) sul sistema, rendendo attivo il server FTP e permettendo ai client di connettersi e trasferire file.

sudo systemctl start vsftpd

* Il comando `sudo systemctl enable vsftpd` configura il servizio \*\*vsftpd\*\* per avviarsi automaticamente all'accensione del sistema, assicurando che il server FTP sia attivo dopo ogni riavvio.

sudo systemctl enable vsftpd

* Il comando `ftp localhost` tenta di stabilire una connessione FTP al server locale (il computer stesso) utilizzando l’indirizzo \*\*localhost\*\* (127.0.0.1). Se il server FTP (come \*\*vsftpd\*\*) è attivo sul sistema, questo comando avvierà una sessione FTP, permettendoti di inserire credenziali e trasferire file sulla macchina locale.

ftp localhost

Il comando `hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-10000.txt ftp://192.168.1.115 -t16` utilizza \*\*Hydra\*\* per eseguire un attacco di \*\*forza bruta\*\* su un server FTP (192.168.1.115). Prova combinazioni di \*\*nomi utente\*\* e \*\*password\*\* prese dalle liste fornite, cercando di indovinare le credenziali corrette. L'opzione `-t16` indica che vengono usati 16 thread simultanei per velocizzare l'attacco.

hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-10000.txt ftp://192.168.1.115 -t16



