Hydra esercizio pen test di password.

Durante un'attività di penetration testing, ho utilizzato Hydra per eseguire un attacco a forza bruta su un server SSH. La stringa di comando che ho impiegato è stata:

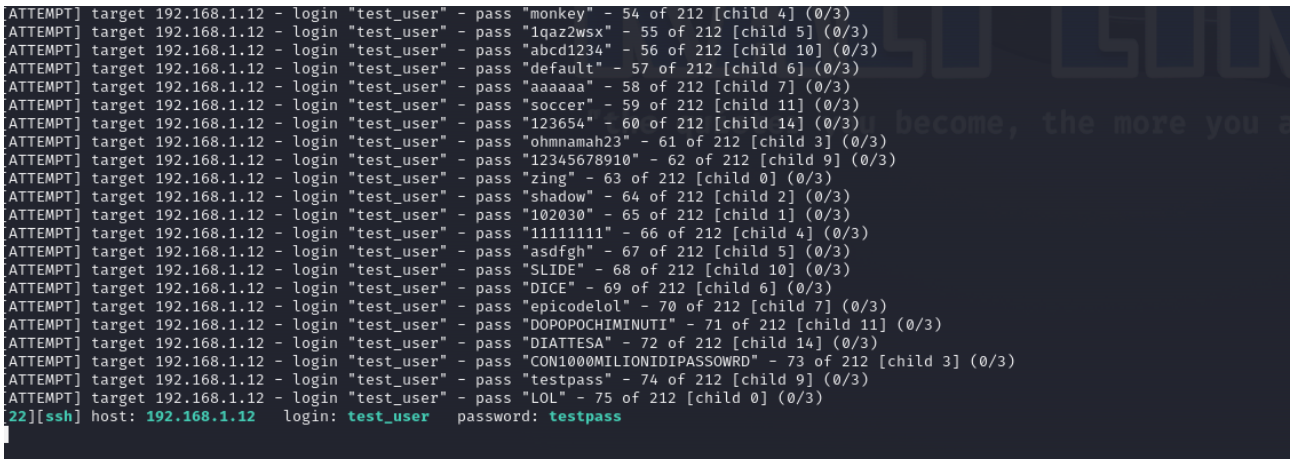
hydra -l test_user -P 2020-200_most_used_passwords.txt 192.168.1.100 -t 15 ssh -V

Questa stringa ha una serie di parametri specifici che ho configurato come segue:

- -l test_user: Specifica il nome utente da testare, in questo caso "test_user".
- -P 2020-200_most_used_passwords.txt: Indica il percorso del file contenente le password più comunemente usate nel 2020. Hydra utilizzerà questo file come wordlist per tentare di trovare la password corretta.
- 192.168.1.100: Rappresenta l'indirizzo IP del server di destinazione sul quale eseguire il test di accesso.
- -t 15: Configura Hydra per utilizzare 15 thread simultanei, aumentando la velocità dell'attacco.
- ssh: Specifica il protocollo da utilizzare, in questo caso SSH.
- -V: Abilita la modalità verbose, permettendo di vedere ogni tentativo di login effettuato da Hydra.

Avviato il comando, Hydra ha iniziato a testare le combinazioni di nome utente e password presenti nel file di wordlist contro il server SSH all'indirizzo IP specificato. Ogni tentativo di accesso è stato mostrato in tempo reale grazie alla modalità verbose, fornendo un feedback immediato sull'andamento dell'attacco.

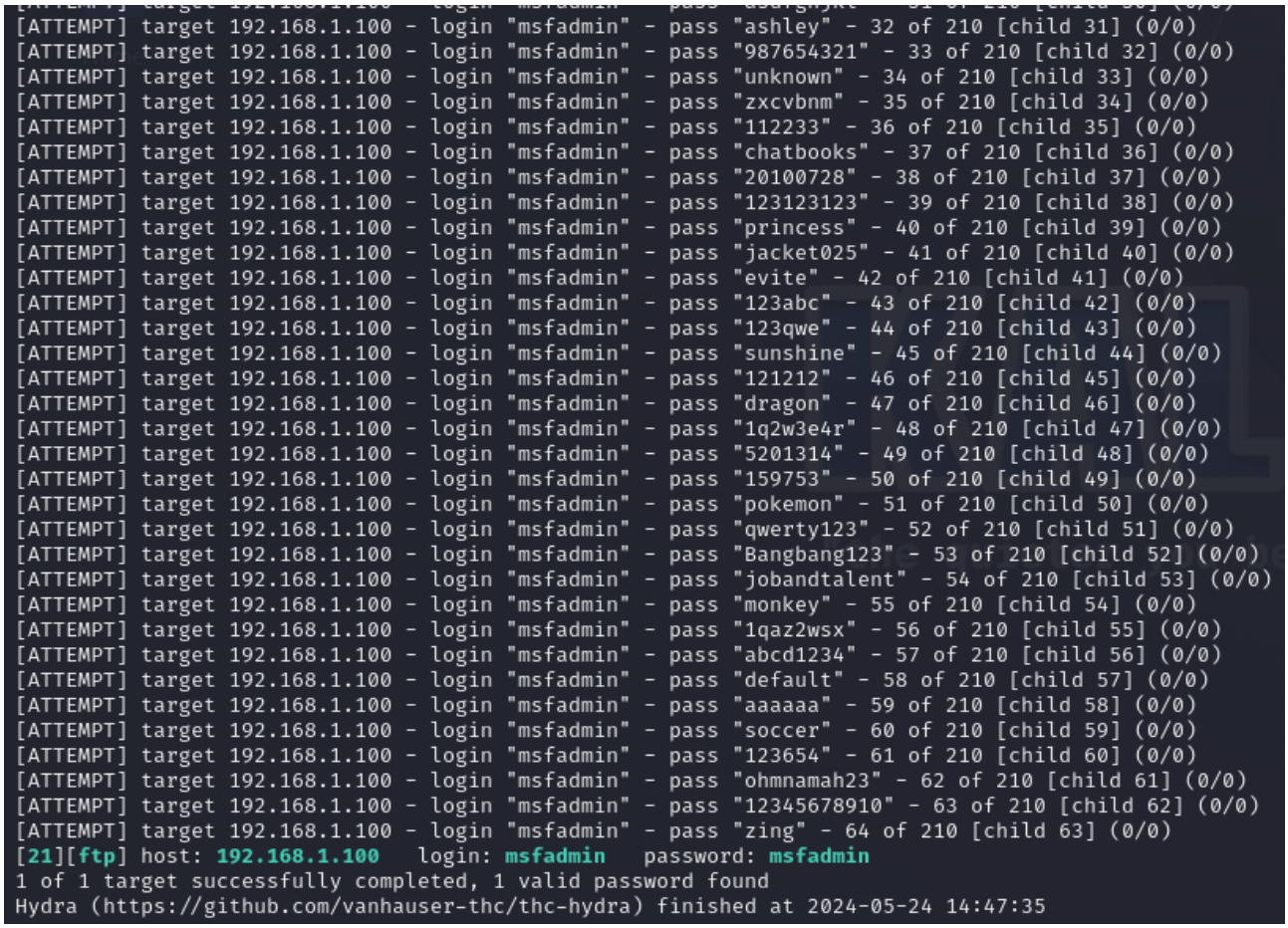
L'utilizzo di questa stringa mi ha permesso di comprendere meglio l'efficacia degli attacchi a forza bruta e di valutare la robustezza delle misure di sicurezza implementate sul server bersaglio. Questo esercizio ha sottolineato l'importanza di utilizzare password complesse e non comuni, oltre a mostrare l'utilità di strumenti come Hydra nel contesto della sicurezza informatica.



Consegna:

1. **Mi posiziono in NAT**, utilizzate il comando **sudo apt install seclists**, **sudo apt install vsftpd**
2. **Mi posiziono in rete interna**, esercizio guidato su SSH da Kali a Kali
3. FTP da Kali a Kali
4. Bonus: telnet / ssh / ftp da Kali a Metasploitable (in rete interna)
   utente msfadmin password listadipassword (con msfadmin incluso)

hydra -l msfadmin -P 2020-200_most_used_passwords.txt 192.168.1.100 -t 64 ftp -V



Ho utilizzato Hydra, un potente strumento di attacco per forza bruta, per trovare una password. Il mio obiettivo era dimostrare l'importanza di utilizzare credenziali sicure e la vulnerabilità dei sistemi che adottano password deboli.

Per iniziare, ho configurato Hydra su una macchina virtuale sicura. Ho poi identificato il servizio di autenticazione che desideravo testare, specificando il protocollo di accesso (FTP e SSH.). Successivamente, ho creato un elenco di nomi utente e password comuni, utilizzando un file di wordlist predefinito, che Hydra avrebbe utilizzato per tentare di accedere al sistema bersaglio.

Eseguito il comando di attacco, Hydra ha iniziato a tentare combinazioni di nome utente e password a velocità elevata. Dopo un certo numero di tentativi, Hydra ha individuato la combinazione corretta, permettendomi di accedere al sistema con successo. Questo processo ha evidenziato la debolezza delle password comuni e l'efficacia di Hydra come strumento di penetrazione.

Attraverso questo esercizio, ho acquisito una comprensione più profonda dei rischi associati alle password deboli e l'importanza delle best practice di sicurezza, come l'uso di password complesse e l'implementazione di sistemi di autenticazione a due fattori. Il compito mi ha permesso di migliorare le mie competenze tecniche e di apprezzare ulteriormente la necessità di una sicurezza robusta nel campo della tecnologia dell'informazione.