Unità 2 - S6-L5

Data: 31/10/2025

Alessandro Pietro Salerno

Report di Attività: Penetration Test (Authentication Cracking)

Obiettivo: Authentication cracking con Hydra

1. Introduzione

Questo report documenta le attività svolte durante la fase 1 dell'esercizio di laboratorio "Authentication cracking con Hydra". L'obiettivo primario di questa fase è duplice:

1. Consolidare le conoscenze relative alla configurazione di servizi di rete, nello specifico **SSH (Secure Shell)**.
2. Acquisire familiarità pratica con lo strumento di attacco a dizionario **Hydra** per testare la robustezza delle credenziali di autenticazione.

L'attività è stata condotta in un ambiente di laboratorio controllato, utilizzando la stessa macchina (Kali Linux) sia come target che come sistema attaccante (IP Target: 127.0.0.1).

2 Svolgimento - Fase 1: Attacco a SSH

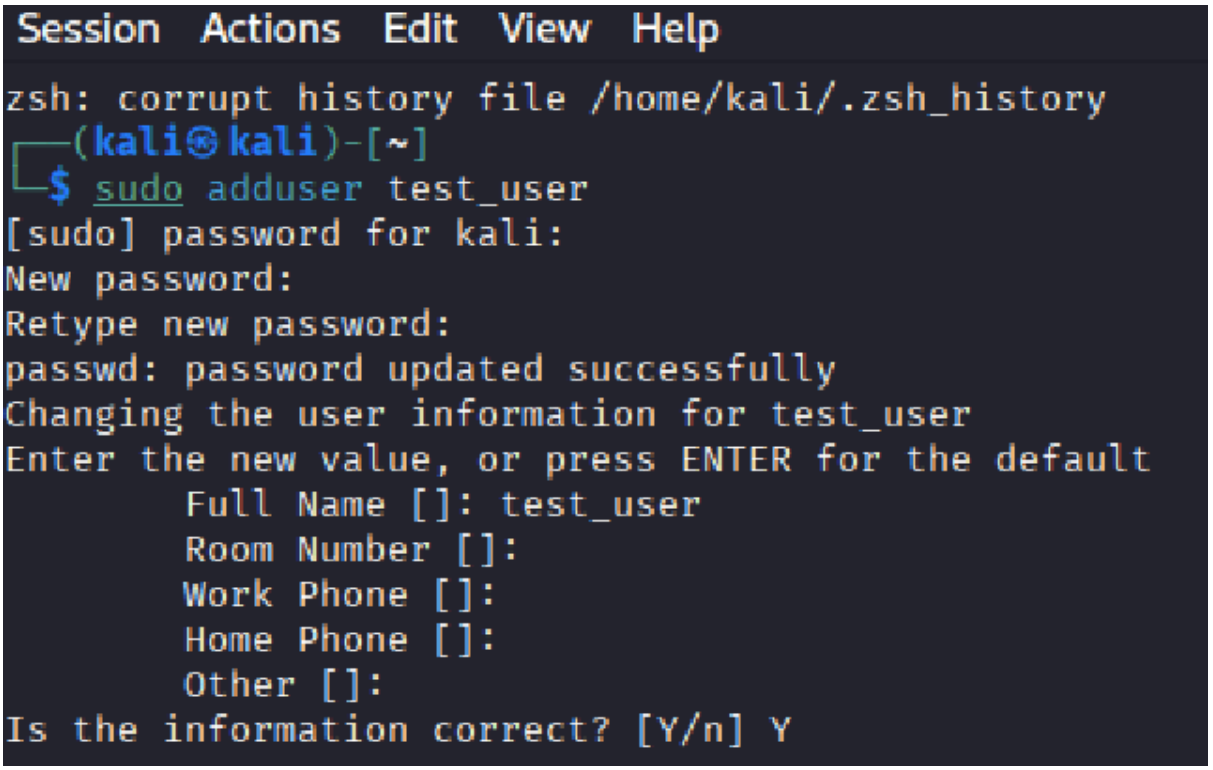
L'attività è stata suddivisa in quattro passaggi sequenziali: configurazione del target, attivazione del servizio, preparazione dell'attaccante ed esecuzione dell'attacco.

2.1 Configurazione del Target (Creazione Utente)

Come primo passo, è stato preparato l'ambiente target. È stato creato un nuovo utente non privilegiato sul sistema operativo Kali Linux, destinato a essere l'obiettivo del test di autenticazione.

- **Comando Eseguito:** sudo adduser test_user
- **Credenziali Impostate:**
  - **Username: test_user**
  - **Password: testpass** (password debole scelta deliberatamente per l'esercizio).

Questa operazione è fondamentale per simulare uno scenario reale in cui un attaccante ha già identificato un nome utente valido (tramite *enumeration* o *information gathering*) e intende scoprirne la password.



“ho lasciato le impostazioni dopo Full Name di default premendo invio ed infine confermando che le informazioni erano corrette“

2.2 Attivazione e Verifica del Servizio SSH

Successivamente, è stato attivato il servizio **Secure Shell (SSH)** sul target. SSH è un protocollo di rete crittografato che opera sulla porta TCP 22 e consente un accesso amministrativo remoto sicuro. L'attivazione del servizio è il prerequisito per un attacco di tipo *online*, in cui lo strumento di cracking interagisce attivamente con il servizio in ascolto.

- **Comando di Avvio:** `sudo service ssh start`
- **Comando di Verifica:** `sudo service ssh status`

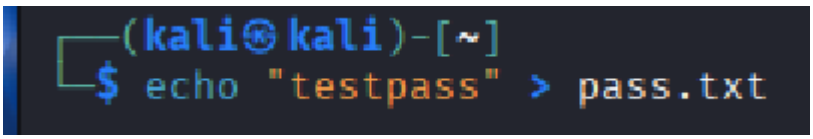
La verifica ha confermato che il servizio **sshd** (il demone di SSH) era **active (running)**, e quindi pronto ad accettare connessioni in ingresso.

```
┌──(kali㉿kali)-[~]
└─$ sudo service ssh start
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
     Active: active (running) since Fri 2025-10-31 07:12:34 EDT; 28s ago
 Invocation: 8fe6d38860994a69b5836558386aed38
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 10064 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 10067 (sshd)
      Tasks: 1 (limit: 9369)
     Memory: 2.1M (peak: 2.8M)
        CPU: 23ms
     CGroup: /system.slice/ssh.service
             └─10067 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 31 07:12:34 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server ...
Oct 31 07:12:34 kali sshd[10067]: Server listening on 0.0.0.0 port 22.
Oct 31 07:12:34 kali sshd[10067]: Server listening on :: port 22.
Oct 31 07:12:34 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

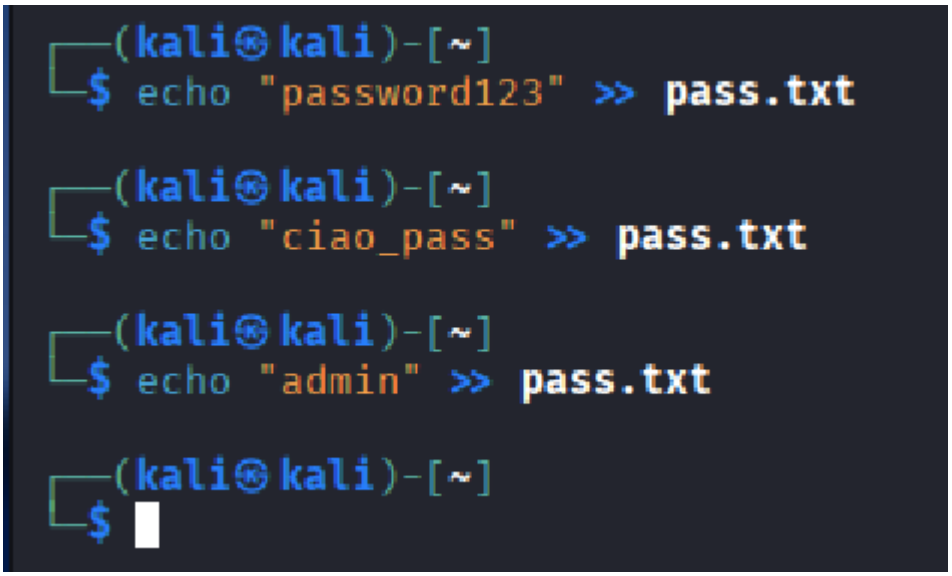
2.3 Preparazione dell'Attaccante (Creazione Wordlist)

Dalla postazione attaccante (nello stesso terminale, in questo caso), è stato preparato un "dizionario" o ***wordlist***. Un attacco a dizionario, a differenza di un **brute-force puro**, testa solo le password presenti in una lista predefinita.

Per garantire l'efficacia e la rapidità del test, è stata creata una wordlist personalizzata **pass.txt** contenente la password corretta e altri comuni "esche".



Comandi Eseguiti:
echo "testpass" > pass.txt
echo "password123" >> pass.txt
echo "admin" >> pass.txt



Contenuto finale di `pass.txt`:
testpass
password123
admin
ciao_pass

2.4. Esecuzione dell'Attacco con Hydra

Con il target configurato e la wordlist pronta, è stato lanciato l'attacco utilizzando Hydra.

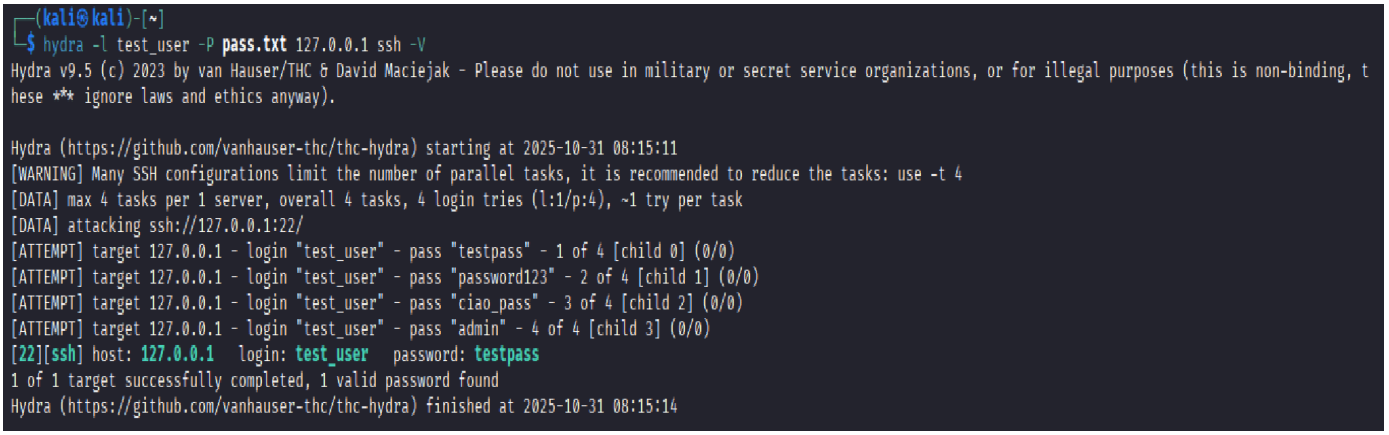
- **Comando Eseguito: hydra -l test_user -P pass.txt 127.0.0.1 ssh -V**
- **Analisi del Comando:**
  - hydra: Avvia lo strumento.
  - -l test_user: Specifica un singolo **l**ogin (utente) da testare.
  - -P pass.txt: Indica il percorso del file contenente le **P**assword.
  - 127.0.0.1: Specifica l'IP del target (localhost).

- `ssh`: Indica il protocollo da attaccare.
- `-V`: Abilita la modalità **V**erbose per visualizzare tutti i tentativi.

3 Risultati Ottenuti

L'attacco ha avuto successo immediato. L'output di Hydra (modalità Verbose) ha mostrato i tentativi falliti per le password "password123" , “ciao_pass” e "admin", nell’ordine in cui le ha provate, e ha poi identificato la password corretta.

L'output finale ha confermato il ritrovamento delle credenziali valide: **[22][ssh] host: 127.0.0.1 login: test_user password: testpass**



4 Conclusioni e Riflessioni (Fase 1)

Successo dell'Attacco: La Fase 1 è stata completata con successo, dimostrando l'efficacia di Hydra nell'eseguire attacchi a dizionario online contro servizi di autenticazione.

Riflessione sulla Sicurezza: Questo test evidenzia una vulnerabilità critica e molto comune: **l'uso di password deboli**. Sebbene il protocollo SSH sia robusto e crittografato (impedendo l'intercettazione o *sniffing* delle credenziali in transito), la sua sicurezza è vanificata se le credenziali stesse sono facilmente intuibili o presenti in dizionari comuni.

L'anello debole della catena non era il protocollo (SSH), ma il "fattore umano" (la scelta di una password debole).

Contromisure (Mitigazioni): Per prevenire questo tipo di attacco, un amministratore di sistema dovrebbe implementare:

1. **Password Policy Robuste:** Imporre requisiti di complessità (lunghezza, caratteri speciali, numeri, maiuscole/minuscole) e scadenza delle password.
2. **Account Lockout Policy:** Bloccare temporaneamente un account dopo un numero limitato di tentativi di login falliti (es. 3-5 tentativi), rendendo un attacco Hydra estremamente lento e rumoroso.
3. **Autenticazione a Due Fattori (MFA):** Richiedere un secondo fattore (es. un codice da un'app) oltre alla password.
4. **Accesso basato su Chiavi SSH:** Disabilitare l'autenticazione basata su password e consentire solo l'accesso tramite coppie di chiavi crittografiche (pubblica/privata).

1. Introduzione

Adesso descrivo la Fase 2 dell'esercizio di laboratorio "Authentication cracking con Hydra". In linea con la traccia. L' obiettivo era configurare un nuovo servizio di rete e testarne la sicurezza dell'autenticazione.

È stato scelto il **File Transfer Protocol (FTP)**, un servizio standard per il trasferimento di file che opera sulla porta TCP 21. Questa scelta è stata didatticamente significativa perché, a differenza di SSH (Fase 1), l'FTP è un protocollo **intrinsecamente insicuro** che trasmette le credenziali in chiaro. L'obiettivo era testare la sua vulnerabilità a un attacco a dizionario online tramite Hydra.

---

2. Svolgimento - Fase 2: Attacco a FTP

L'attività ha richiesto una sequenza di installazione,configurazione e attacco.

2.1 Installazione del Servizio (`vsftpd`) e Troubleshooting

Il servizio scelto per erogare FTP è stato **vsftpd** (Very Secure FTP Daemon), un server FTP comune in ambiente Linux.

1. Tentativo di Installazione e Diagnosi: Il comando iniziale **`sudo apt install vsftpd`** è fallito. L'output del sistema (`E: Package 'vsftpd' has no installation candidate`) ha indicato che il gestore di pacchetti **`apt`** non riusciva a trovare il software.

- **Comando Eseguito** “per troubleshooting”**: sudo apt-get update**

2. Installazione (Successo): Dopo l'aggiornamento, il comando di installazione è stato rieseguito con successo.

- **Comando Eseguito: `sudo apt-get install vsftpd`**

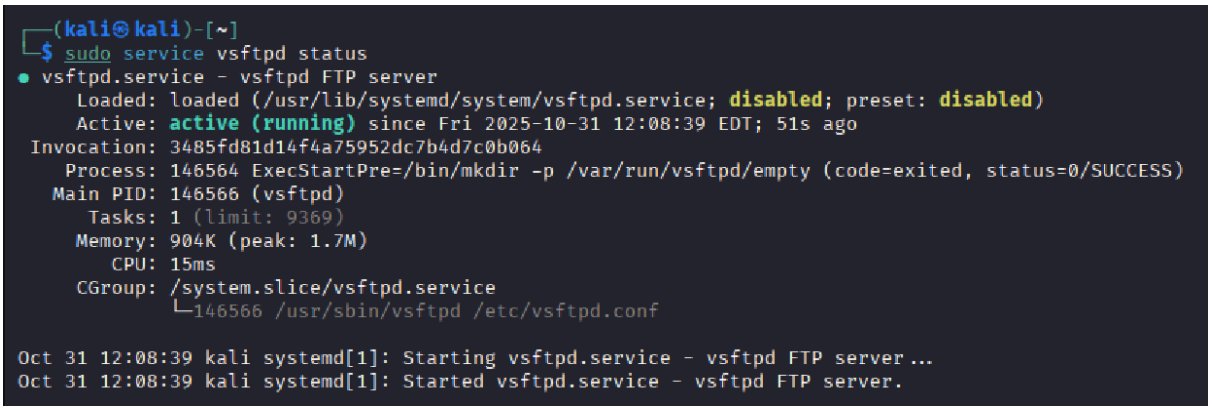
```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install vsftpd
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 943 not upgraded.
Need to get 151 kB of archives.
After this operation, 381 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.3 [151 kB]
Fetched 151 kB in 1s (130 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 421848 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0.3_amd64.deb ...
Unpacking vsftpd (3.0.5-0.3) ...
Setting up vsftpd (3.0.5-0.3) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.2) ...
```

2.2 Avvio e Verifica del Servizio

Successivamente, il servizio è stato avviato e il suo stato verificato per assicurarsi che fosse in esecuzione e in ascolto sulla porta 21.

- **Comando di Avvio: sudo service vsftpd start**
- **Comando di Verifica: sudo service vsftpd status**

Il comando di verifica ha confermato che il servizio era **`Active: active (running)`**.



2.4. Esecuzione dell'Attacco con Hydra

Con il server FTP attivo, è stato sferrato l'attacco a dizionario dalla postazione attaccante (localhost).

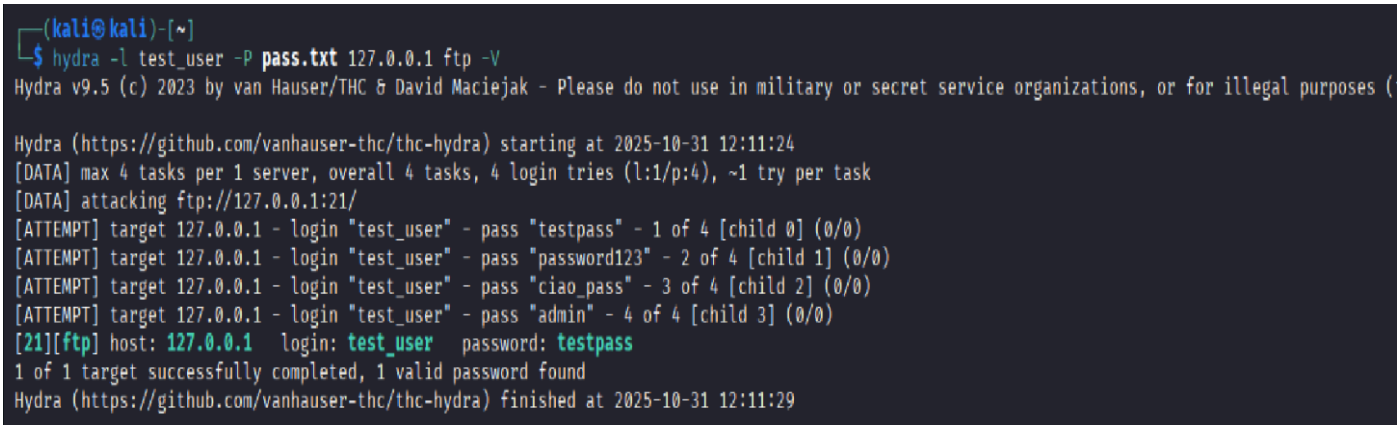
- **Comando Eseguito:** **`hydra -l test_user -P pass.txt 127.0.0.1 ftp -V`**
- **Analisi del Comando:**
  - `-l test_user`: Target (login).
  - `-P pass.txt`: Dizionario (password).
  - `127.0.0.1`: IP Target.
  - `ftp`: Protocollo da attaccare (Hydra si collega automaticamente alla porta 21).

---

3. Risultati Ottenuti

L'attacco ha avuto successo immediato. L'output di Hydra ha mostrato il tentativo con la password corretta (**`testpass`**) e ha immediatamente riportato il successo.

- **Credenziali Trovate:** **`[21][ftp] host: 127.0.0.1 login: test_user password: testpass`**



4. Conclusioni e Riflessioni (Fase 2)

Successo dell'Attacco: La Fase 2 è stata completata con successo, dimostrando la capacità di configurare un servizio FTP e violarne l'autenticazione tramite un attacco a dizionario.

Riflessione sulla Sicurezza (SSH vs. FTP): Questo esercizio ha evidenziato una differenza cruciale tra SSH (Fase 1) e FTP (Fase 2):

1. **SSH** è un protocollo *sicuro* (crittografato), ma è risultato vulnerabile a causa di una **password debole**.
2. **FTP** non solo è risultato vulnerabile alla stessa **password debole**, ma è anche un protocollo *insicuro* per design. Se avessimo "sniffato" (intercettato) il traffico di rete durante il login di Hydra (ad esempio con Wireshark), avremmo visto la password `testpass` passare in chiaro (clear text).

La vulnerabilità è quindi duplice: debolezza delle credenziali e debolezza del protocollo.

Riflessione sul Processo (Troubleshooting): La difficoltà che ho incontrato nell'installazione (`Package 'vsftpd' has no installation candidate`) è stata una parte fondamentale dell'apprendimento. Ha dimostrato l'importanza di una corretta manutenzione del sistema (l'uso di `sudo apt-get update`) e ha rinforzato le capacità di diagnosi e risoluzione dei problemi, competenze essenziali per qualsiasi amministratore di sistema o penetration tester.

Contromisure (Mitigazioni): Per questo servizio, le mitigazioni includono:

1. **Policy Password Robuste** (come per SSH).
2. **Account Lockout Policy** (come per SSH).
3. **Abbandono del Protocollo:** La mitigazione più efficace è **non usare FTP**. Dovrebbe essere sostituito con protocolli sicuri che forniscono crittografia, come **SFTP** (che opera su SSH, porta 22) o **FTPS** (FTP su SSL/TLS).

Breve Conclusione Generale

Ho con successo l'esercizio, configurando e violando l'autenticazione di due servizi di rete fondamentali: **SSH** e **FTP**. Entrambi gli attacchi a dizionario con Hydra sono riusciti, portando alla scoperta della password `testpass`.

Riflessione Chiave

L'esercizio mi ha dimostrato in modo pratico due lezioni fondamentali:

1. **L'Anello Debole Umano:** Anche un protocollo robusto e crittografato come **SSH** è reso inutile se protetto da una **password debole**. La sicurezza del "fattore umano" è tanto importante quanto la sicurezza tecnica del protocollo.
2. **L'Importanza del Troubleshooting:** Le difficoltà incontrate nell'installazione di FTP (la gestione dei repository `apt`) non sono state un intoppo, ma una parte cruciale dell'esercizio. Un professionista della sicurezza deve prima di tutto saper configurare e diagnosticare e tenere aggiornati i sistemi che sta testando.