Report Laboratorio: Network Service Authentication Cracking

Data: 16 Gennaio 2026
Operatore: Gerald
Ambiente: Kali Linux (Virtual Machine)
Tool Utilizzati: Hydra, SSH, VSFTPD, Bash

---

1. Introduzione e Obiettivi

L'esercitazione ha avuto lo scopo di analizzare la vulnerabilità dei protocolli di accesso remoto (**SSH**) e trasferimento file (**FTP**) quando protetti da credenziali deboli. Attraverso la configurazione dei servizi e l'utilizzo del tool di audit **Hydra**, abbiamo dimostrato come un attaccante possa compromettere un sistema in pochi secondi.

La sicurezza di un'infrastruttura informatica dipende in larga misura dalla robustezza dei meccanismi di autenticazione dei suoi servizi. In questo scenario di laboratorio, l'obiettivo è analizzare la vulnerabilità dei protocolli di rete più comuni (come **SSH** e **FTP**) di fronte ad attacchi di tipo **Dictionary Attack** e **Brute-Force**.

L'esercitazione si focalizza su due pilastri fondamentali della Cybersecurity:

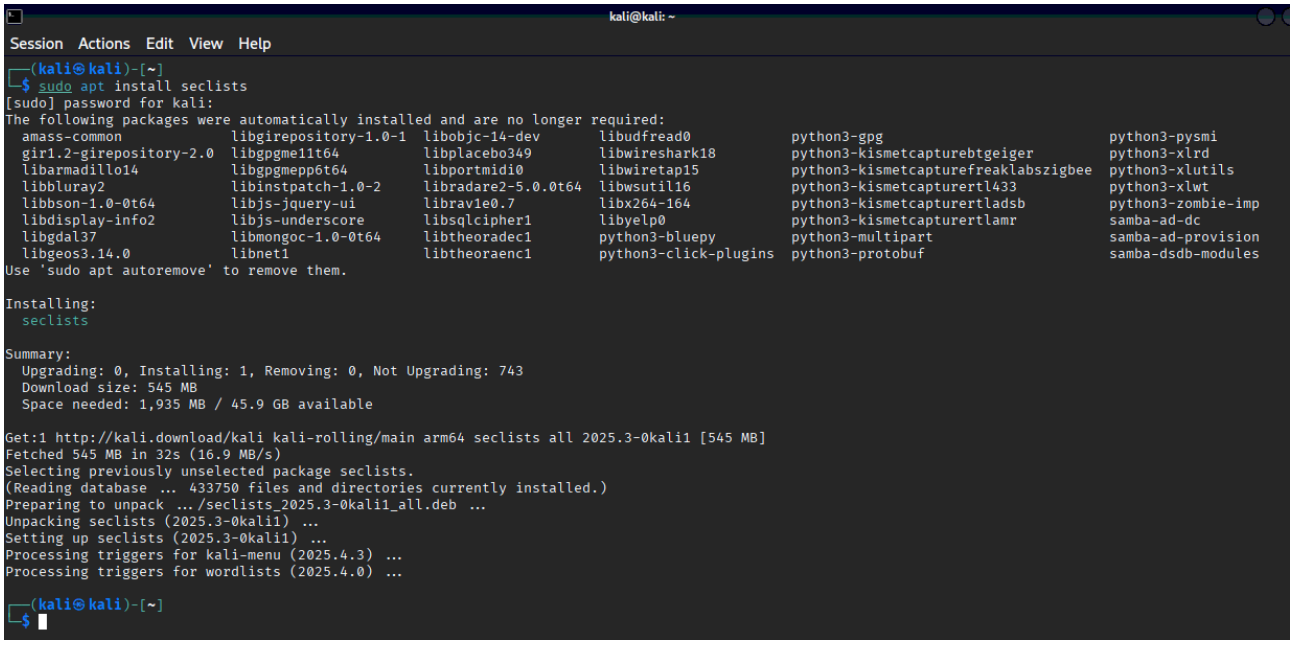
1. **Configurazione e Hardening dei Servizi:** La gestione dei demoni di sistema (come `sshd` e `vsftpd`), la creazione di utenti e la comprensione dei file di configurazione presenti in `/etc/`.
2. **Valutazione della Vulnerabilità tramite Hydra:** L'utilizzo di uno dei tool di cracking più potenti e parallelizzati del settore per testare la resistenza delle credenziali di accesso.

2. Preparazione dell'Ambiente di Analisi

Preparazione dell'Arsenale: Download delle Wordlist (Seclists): per condurre con successo un attacco a dizionario, non basta avere il software di attacco, ma serve anche il dizionario stesso. Prima di iniziare le configurazioni, abbiamo scaricato il pacchetto **Seclists**.

- **Comando:** `sudo apt install seclists`

Approfondimento: Che cos'è SecLists? SecLists non è un programma eseguibile, ma è la più famosa "biblioteca" di file di testo utilizzata dagli esperti di sicurezza. È un repository che aggrega milioni di password realmente utilizzate dagli utenti e trapelate in passati data breach (come la famosa lista *rockyou.txt*). Mentre Hydra è il "motore" dell'attacco, SecLists fornisce le "munizioni". Questo ci permette di trasformare un attacco *Brute-Force* puro (che richiederebbe anni) in un *Dictionary Attack* mirato, provando prima le password che gli esseri umani usano più spesso.



3. Implementazione e Cracking del Servizio SSH

In questa prima fase, il focus è rivolto al protocollo **SSH (Secure Shell)**, lo standard per l'amministrazione remota dei sistemi Linux. Nonostante SSH sia intrinsecamente sicuro grazie alla cifratura del traffico, rimane vulnerabile se protetto da password deboli.

Attraverso la creazione di un utente personalizzato **(test_user)** e l'attivazione del demone SSH, simuleremo un attacco esterno utilizzando **Hydra**. L'obiettivo è dimostrare come, partendo da una collezione di password note (**SecLists**), un attaccante possa guadagnare l'accesso al sistema in pochi secondi se non vengono implementate politiche di password robuste o sistemi di blocco automatico (come Fail2Ban).

3.1 Cos'è il servizio SSH? (In parole povere)

Immagina che il tuo computer sia una casa. Il servizio **SSH** è come una **porta sul retro** che permette al proprietario (l'amministratore) di entrare in casa da remoto (tramite internet) per fare lavori di manutenzione. Questa porta è protetta da un lucchetto: per entrare servono un **Nome Utente** e una **Password**. È un protocollo di rete che permette di accedere e controllare un computer a distanza (remoto) in modo totalmente criptato.

A cosa serve?

Principalmente viene usato per:

- **Amministrazione remota:** Gestire server, router o altri dispositivi tramite riga di comando (terminale).
- **Trasferimento file sicuro:** Spostare file tra computer usando protocolli basati su SSH (come SCP o SFTP).
- **Tunneling:** Creare un "tunnel" protetto per far passare altri dati in modo che non siano visibili dall'esterno.

Il "Lucchetto" Digitale (La Crittografia)

Prima di SSH, si usava un servizio chiamato **Telnet**. Il problema di Telnet era che tutto ciò che scrivevi (inclusi username e password) viaggiava sulla rete in **testo in chiaro**. Chiunque si trovasse nel mezzo poteva leggere le tue credenziali.

SSH risolve questo problema:

- **Cripta tutto il traffico:** Dal momento in cui premi il tasto "Invio", i dati vengono mescolati e diventano illeggibili per chiunque non abbia la chiave corretta.
- **Autenticazione:** Si assicura che tu stia parlando con il server giusto e che tu sia chi dici di essere (tramite password o, meglio ancora, **chiavi SSH**).

Come funziona (In parole semplici)

Quando ti connetti via SSH (solitamente sulla **porta 22**), avvengono tre fasi:

1. **Handshake (Stretta di mano):** Il tuo PC e il server si mettono d'accordo su come criptare la conversazione.
2. **Verifica del Server:** Il server invia una "impronta digitale" per dimostrare che è lui e non un impostore.
3. **Autenticazione:** Tu inserisci la password (o usi la tua chiave privata). Se è corretta, il server ti apre una "shell" (il terminale).

3.2 Cos'è il servizio Ftp? (In parole povere)

L'**FTP** è uno dei protocolli più vecchi di Internet (nato negli anni '70). Il suo unico scopo è il **trasferimento di file** tra un client (il tuo computer) e un server (il computer remoto).

Quando ti connetti via FTP, puoi:

1. **Download:** Prendere file dal server e portarli sul tuo PC.
2. **Upload:** Inviare file dal tuo PC al server.
3. **Gestione:** Rinominare, cancellare o creare cartelle sul server.

Immagina l'FTP come un sistema a due canali:

- **Canale di Controllo (Porta 21):** È dove passano i comandi. Qui tu dici al server: "Ehi, sono l'utente *test_user*, la mia password è *testpass* e vorrei vedere la cartella Documenti".
- **Canale Dati (Porta 20):** È il tubo separato dove passano effettivamente i bit del file che stai scaricando.

---

4. Configurazione dello Scenario (Il Target)

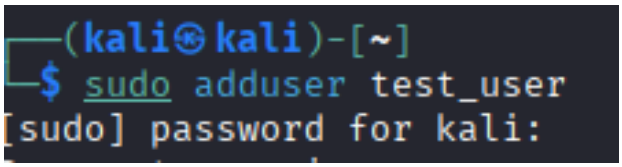
Per simulare un ambiente reale, è stato necessario configurare una macchina "vittima" con un utente specifico.

4.1 Creazione dell'Utente

Abbiamo creato un nuovo "abitante" nel sistema Linux per fungere da bersaglio.

- **Comando:** `sudo adduser test_user`
- **Password scelta:** `testpass`

Abbiamo scelto intenzionalmente una password debole (`testpass`) per dimostrare come una singola configurazione errata possa compromettere l'intero sistema.



---

5 Entra in scena Hydra: Il "Martello Pneumatico"

Hydra non è un virus, ma un software che simula un ladro molto veloce. Invece di provare a scassinare la serratura con la forza, Hydra prova a inserire **migliaia di chiavi diverse** in pochissimi secondi.

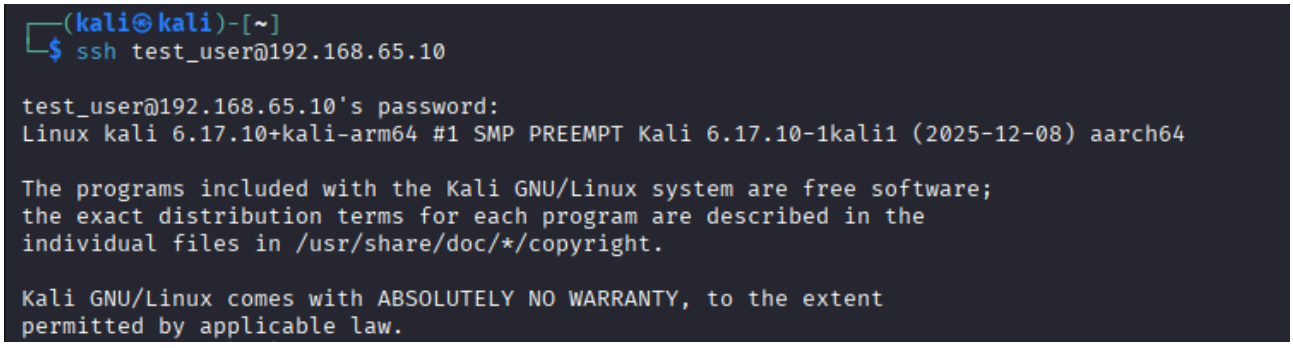
Nel nostro esercizio, abbiamo dato a Hydra due liste (chiamate **Wordlist**):

- Una lista di possibili nomi (tra cui il nostro `test_user`).
- Una lista di password comuni (tra cui la nostra `testpass`).

5 .1 Configurazione e Cracking del Servizio SSH

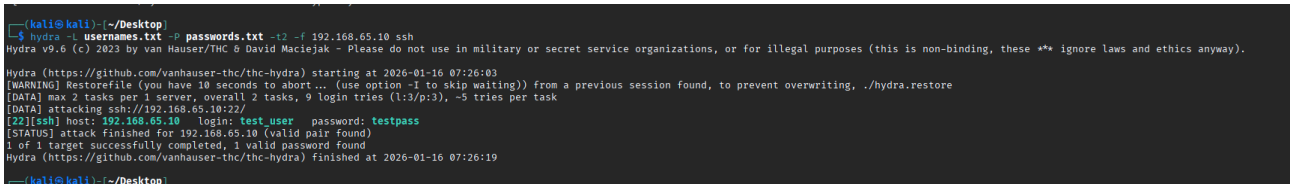
I passaggi effettuati:

- **Abilitazione del Servizio:** Abbiamo attivato il server SSH (Secure Shell), già presente su Kali Linux, utilizzando il comando `sudo service ssh start`.
- **Configurazione Utente:** Abbiamo preparato il target creando l'utente `test_user` con password `testpass` tramite il comando `adduser`.



- **L'Attacco con Hydra:** Utilizzando le wordlist scaricate precedentemente (SecLists), abbiamo configurato Hydra per puntare alla porta 22 (quella standard del protocollo SSH).

Il Risultato: Una volta lanciato il comando, Hydra ha iniziato a testare le combinazioni presenti nelle liste a una velocità impressionante. In meno di un secondo, il tool ha restituito un risultato positivo, evidenziato in verde nel terminale:



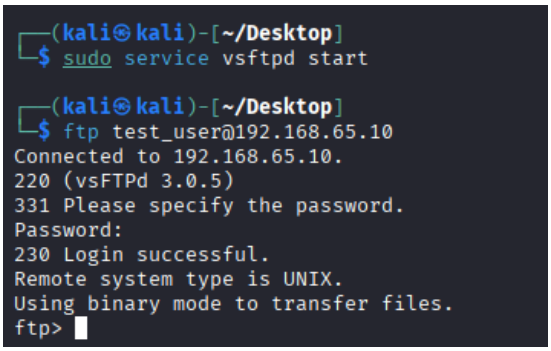
[22][ssh] host: 192.168.65.10 login: test_user password: testpass

Questo dimostra che, nonostante la crittografia di SSH protegga i dati durante il transito, l'autenticazione è stata compromessa istantaneamente a causa della debolezza della password scelta.

5.2 Configurazione e Cracking del Servizio FTP

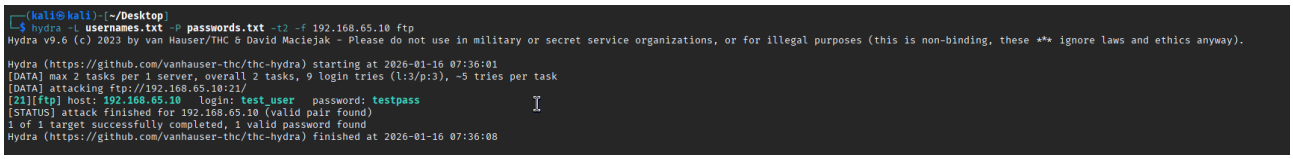
I passaggi effettuati:

- **Installazione del Servizio:** Abbiamo installato il server FTP chiamato `vsftpd` (Very Secure FTP Daemon) utilizzando il comando `sudo apt install vsftpd`.
- **Attivazione:** Abbiamo avviato il servizio rendendolo disponibile sulla rete con il comando `sudo service vsftpd start`.
- **L'Attacco con Hydra:** Utilizzando le stesse wordlist della fase precedente, abbiamo riconfigurato Hydra per puntare alla porta 21 (quella standard del protocollo FTP).



Il Risultato: Proprio come per l'SSH, Hydra ha analizzato il dizionario di password trovando immediatamente la corrispondenza. Poiché l'utente è un account di sistema, le credenziali sono risultate valide anche per questo servizio:

[21][ftp] host: 192.168.65.10 login: test_user password: testpass



Questo risultato evidenzia un ulteriore rischio di sicurezza: se un utente utilizza la stessa password debole per più servizi (SSH e FTP), l'attaccante ottiene il controllo totale su ogni punto di accesso del server.

---

6. Conclusioni e Strategie di Difesa (Mitigazione)

Questo laboratorio ha messo in luce una verità fondamentale della Cybersecurity: **la sicurezza di un sistema è forte quanto il suo anello più debole.** In questo caso, l'anello debole era la password.

Cosa abbiamo imparato:

- **SSH vs FTP:** Anche se usiamo protocolli sicuri come SSH, se la "chiave" d'ingresso (la password) è banale, il protocollo non può proteggerci.
- **Automazione:** Gli strumenti come Hydra permettono agli attaccanti di provare migliaia di password al minuto senza fatica.

Come proteggersi (Hardening): Per evitare che un attacco reale di questo tipo abbia successo, un amministratore di sistema dovrebbe:

1. **Imporre Password Complesse:** Obbligare gli utenti a usare password lunghe, con numeri e caratteri speciali, che non siano presenti nei dizionari comuni.
2. **Usare Fail2Ban:** Installare software che bloccano automaticamente l'indirizzo IP di chi sbaglia la password troppe volte consecutive (es. 3 tentativi errati = ban per 1 ora).
3. **Autenticazione a Chiavi (SSH Keys):** Abbandonare le password e utilizzare le coppie di chiavi crittografiche (Pubblica/Privata), che sono impossibili da indovinare con un attacco Brute-Force.