Authentication cracking con Hydra

Introduzione

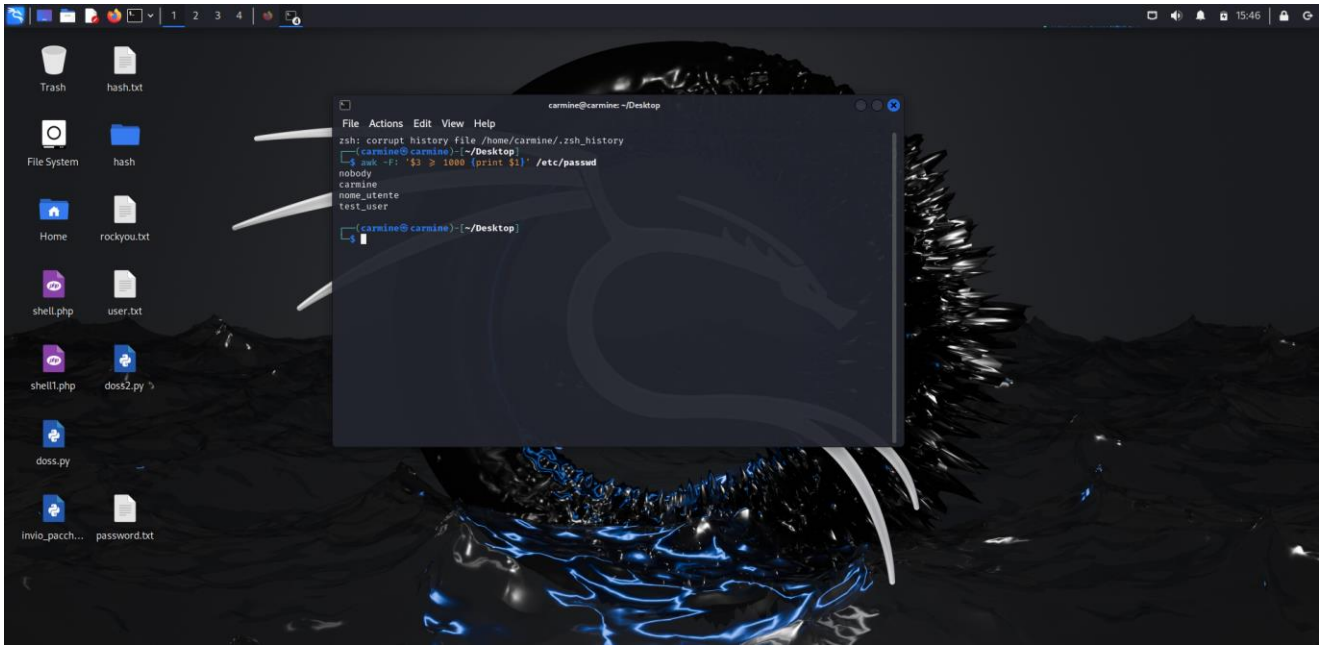
La presente relazione ha lo scopo di analizzare la vulnerabilità di sistemi remoti sfruttando i protocolli SSH e FTP mediante l'utilizzo dello strumento Hydra su una distribuzione Kali Linux. Attraverso una serie di test di penetrazione, si è cercato di valutare l'efficacia di attacchi di forza bruta volti a compromettere le credenziali di accesso e, di conseguenza, ottenere un accesso non autorizzato ai sistemi target. L'obiettivo principale è stato quello di evidenziare le criticità legate alla sicurezza informatica e proporre delle contromisure efficaci

Procedimento

Creazione dell'utente:

Comando: adduser `test_user` Questo comando crea un nuovo utente chiamato "**test_user**" sul sistema.

Configurazione password: Durante la creazione dell'utente, verrà richiesto di impostare una password. In questo caso, è stata impostata la password **“testpass**".



Monitoraggio dei tentativi di brute force con Hydra

Hydra è un programma che viene utilizzato per eseguire attacchi di forza bruta su vari tipi di servizi di rete. In pratica, Hydra tenta di indovinare le password di un account provando una vasta gamma di combinazioni di caratteri, fino a quando non ne trova una che funziona.

Come funziona Hydra?

Hydra supporta un'ampia varietà di protocolli, tra cui:

- **SSH:** Utilizzato per accedere in modo sicuro a sistemi remoti.
- **FTP:** Utilizzato per trasferire file tra computer.
- **Telnet:** Un protocollo di rete non sicuro per la connessione remota a dispositivi.
- **HTTP:** Utilizzato per la navigazione web.
- **E molti altri...**

L'utente fornisce a Hydra un elenco di nomi utente e una lista di possibili password (o un dizionario di parole). Hydra proverà tutte le combinazioni possibili fino a quando non troverà una coppia valida di nome utente e password.

Esempio di comando Hydra:

```
hydra -V -L percorso del file/username_list -P percorso del file/password_list 192.168.101.201 t1 ssh
```

- **-V:** L'aggiunta dello switch `-V` al comando Hydra permette di visualizzare in tempo reale i tentativi di login effettuati. Questo è particolarmente utile per monitorare eventuali attacchi di brute force.

- **`-L username_list`**: Specifica un file contenente una lista di nomi utente da provare.
- **`-P password_list`**: Specifica un file contenente una lista di password da provare.

- **`192.168.101.201`**: L'indirizzo IP del sistema Kali.
- **`ssh:`** Indica che l'attacco è diretto al servizio SSH.

SSH

SSH (Secure Shell) è un protocollo di rete crittografato che permette di stabilire una connessione remota sicura con un altro computer. È come avere un tunnel sicuro attraverso il quale puoi accedere e controllare un altro sistema, anche se si trova dall'altra parte del mondo.

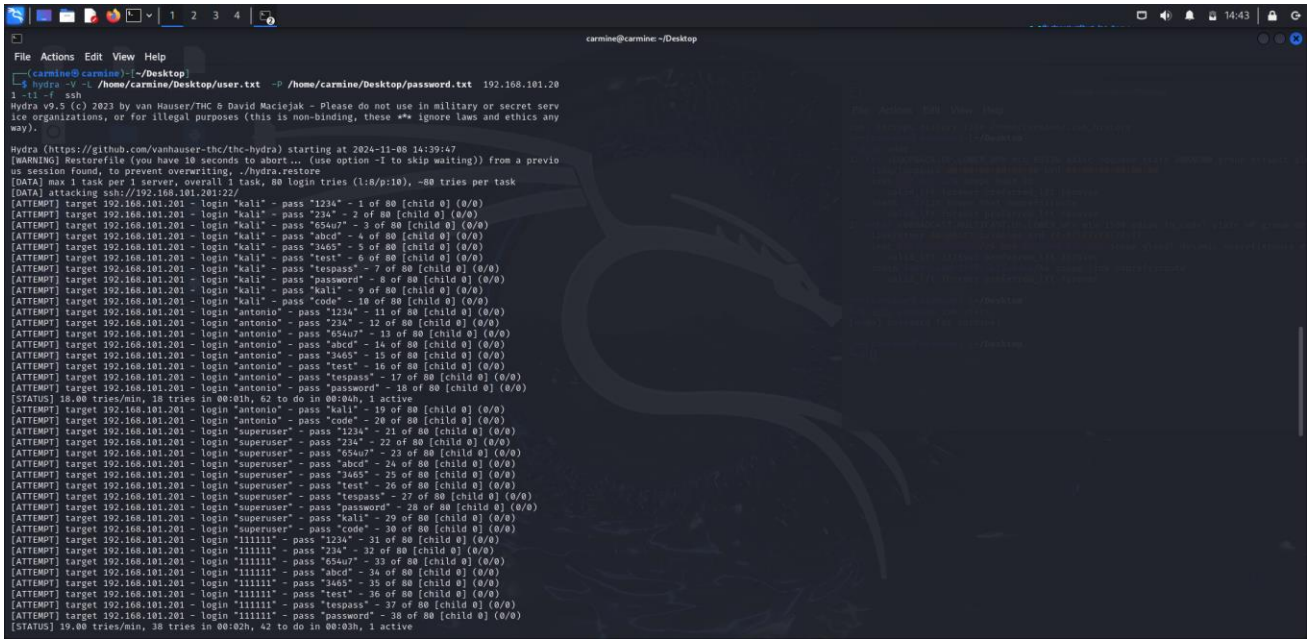
Attivazione del servizio SSH:

-Comando: `sudo systemctl start ssh` Questo comando avvia il servizio SSH, consentendo le connessioni remote al sistema.

Test della connessione SSH:

-Comando: `ssh test_user@192.168.101.201` questo comando tenta di stabilire una connessione SSH in qualità dell'utente "test_user".

Il Comando che andiamo ad usare per attaccare il servizio ssh è: `hydra -V -L percorso del file/username_list -P percorso del file/password_list 192.168.101.201 t1 ssh.` E abbiamo usato il dizionario seclist.



FTP

FTP, acronimo di **File Transfer Protocol**, è un protocollo di rete utilizzato per trasferire file da un computer ad un altro attraverso una rete, come Internet. In pratica, l'FTP permette di copiare file da un server (un computer che fornisce il servizio) al tuo computer (il client) e viceversa.

Attivazione del servizio FTP

-Aggiornare Kali: sudo apt-get updata. Con questo comando eseguiamo un aggiornamento su Kali.

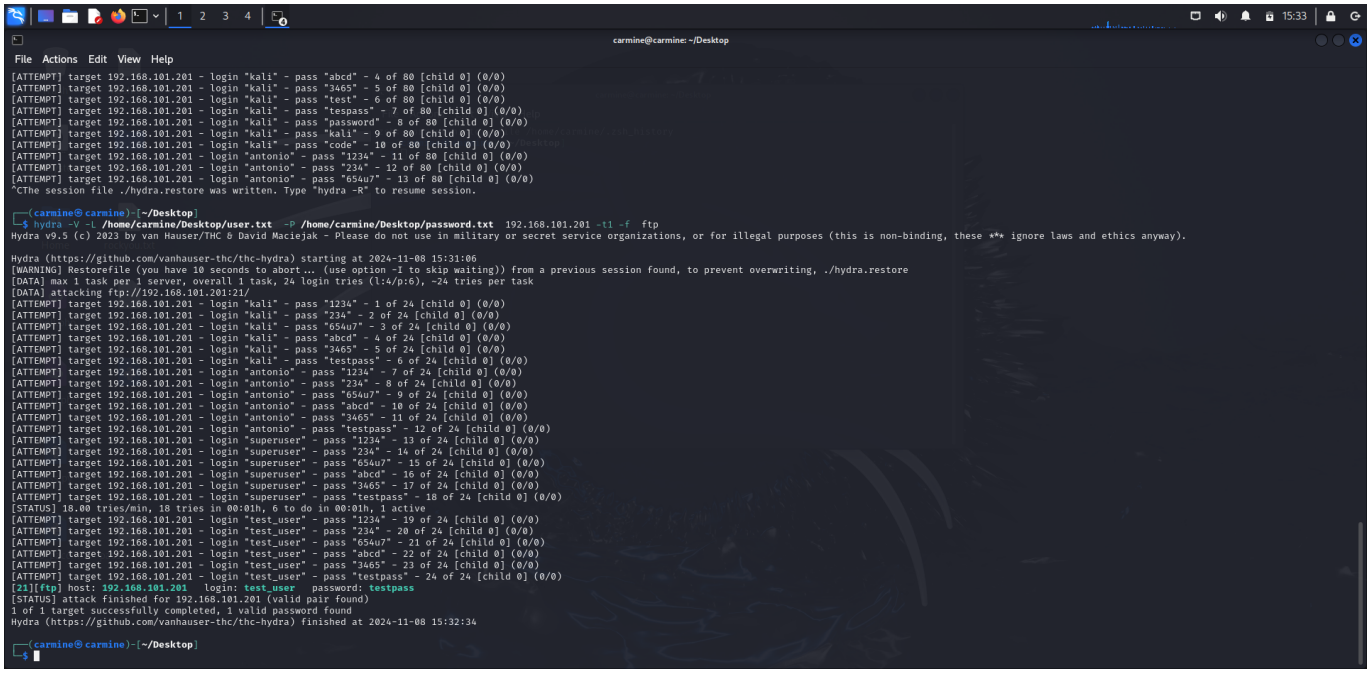
-**Comando installazione FTP: sudo apt install vsftpd**

-Comando di attivazione: `sudo systemctl start vsftpd` Questo comando avvia il servizio SSH, consentendo le connessioni remote al sistema.

Il comando che abbiamo usato è: `hydra -V -L percorso del file/username_list -P percorso del file/password_list 192.168.101.201 t1 ftp.` E abbiamo usato lo stesso dizionario di ssh.

Bonus

Il problema dell'usare il dizionario Speclist è che essendo una lista molto lunga i tempi di attesa del risultato saranno molto lunghi, quindi per velocizzare i tempi possiamo usare dei dizionari più piccoli e in questo modo sarà più veloce il processo di rilevamento dei dati richiesti.



Considerazioni sulla Sicurezza

- **Password forti:** È fondamentale utilizzare password complesse e uniche per ogni account.
- **Limitazione degli accessi:** Configura il firewall per consentire le connessioni SSH solo da indirizzi IP autorizzati.
- **Disabilita il login root:** Per motivi di sicurezza, è consigliabile disabilitare il login diretto come root.
- **Monitoraggio:** Utilizzare strumenti di monitoraggio per rilevare eventuali attività sospette.

Conclusioni

gli esperimenti condotti hanno dimostrato l'efficacia di Hydra nell'individuare vulnerabilità legate alle debolezze delle password in sistemi SSH e FTP. È evidente la necessità di rafforzare le politiche di gestione delle password e di implementare misure di autenticazione più robuste.