PROGETTO S6L5

Per il progetto di oggi, lo scopo era simulare un authentication cracking utilizzando il programma **Hydra** sui servizi **SSH** e **FTP**. In questa relazione, forniremo un breve cenno teorico su ciò che è stato svolto durante il progetto.

**Introduzione al Penetration Test**

Durante un **penetration test**, l’etical hacker si occupa di trovare, testare e mitigare tutte le vulnerabilità presenti all’interno di una rete. Una volta identificate le informazioni e scannerizzate le vulnerabilità della rete, è necessario verificarne la veridicità, dando prova concreta che queste vulnerabilità esistano effettivamente; ed è possibile farlo nella la fase di exploit, che consiste nell’attacco vero e proprio.

Le principali tipologie di attacco durante la fase di exploit sono tre:

* Exploit per le web app
* Exploit per i sistemi operativi
* Exploit per le reti

Nel progetto odierno, l’attacco simulato rientra nella categoria degli attacchi alle password, che fanno parte della macro area degli attacchi alle web app.

**Gli Attacchi alle Password**

Questo tipo di attacchi sono molto comuni tra i black hat, poiché le password sono un elemento fondamentale per proteggere dati sensibili e l'accesso ai sistemi. Gli attaccanti cercano quindi, di ottenere un accesso non autorizzato a dati o sistemi che potrebbero compromettere la sicurezza.

Tra le principali tipologie di attacchi alle password, possiamo trovare:

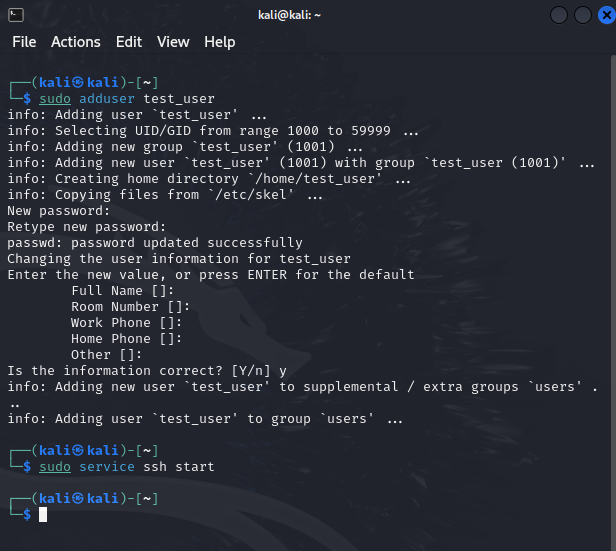
* Attacchi a forza bruta
* Attacchi al dizionario
* Phishing
* Keylogging
* Man in the middle
* Pass the hash
* Rainbow tables

Nel progetto odierno, la tipologia di attacco simulato è un **attacco a dizionario**, uno degli attacchi alle password più comuni. In un attacco a dizionario, l'attaccante utilizza un file che contiene una lista di password comuni, cercando di farle confrontare con quelle presenti nel sistema target. Il software di cracking, come **Hydra**, confronta ogni password del dizionario con quella utilizzata dal sistema, fino a trovare una corrispondenza.

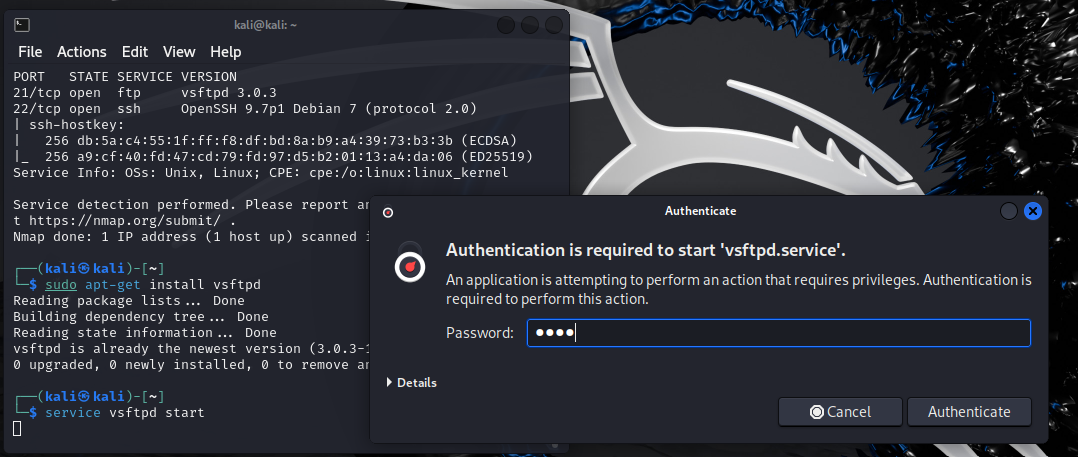
Ovviamente, non sempre la password cercata è presente nel dizionario. In questi casi, se l'attacco a dizionario fallisce, gli attaccanti possono ricorrere all'**attacco a forza bruta**, che prova tutte le combinazioni possibili di caratteri per trovare la password corretta. Per ottimizzare il tempo e migliorare l’efficacia dell'attacco, è utile raccogliere informazioni sull'utente e sulle sue abitudini, poiché molti utenti associano le loro credenziali a elementi familiari.

Un altro metodo per ottimizzare i tempi di scansione è **limitare** il campo della ricerca, restringendo il dizionario alle password più probabili. In alternativa, è possibile **creare un dizionario personalizzato,** basato su criteri specifici (ad esempio, lunghezza o tipo di caratteri), per migliorare l'efficienza dell'attacco.

**Descrizione dell’attacco simulato**

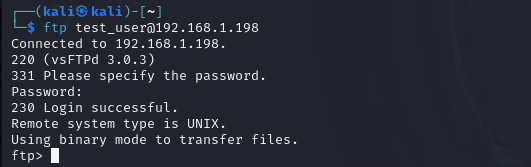
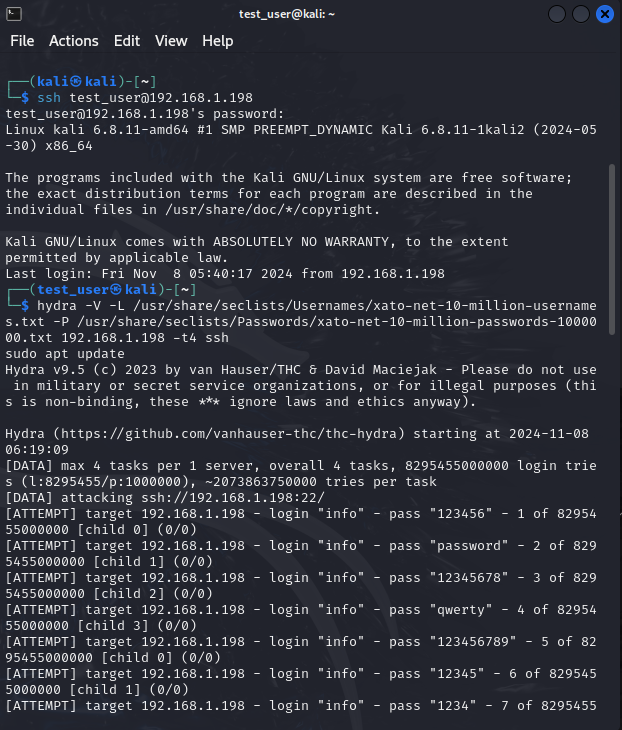
Passiamo ora a descrivere le operazioni effettuate durante il progetto di oggi.

Creazione dell’utente: Come prima cosa, su una macchina Kali Linux, abbiamo creato un nuovo utente, denominato **test\_user**, utilizzando il comando adduser e impostando la password **testpass** Successivamente, abbiamo avviato il servizio SSH;

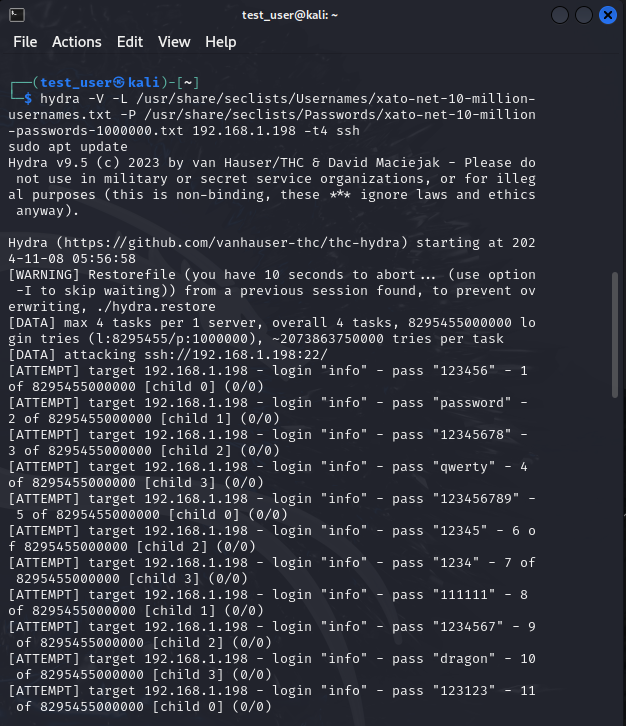


La stessa operazione è stata eseguita per il protocollo FTP, che però, a differenza di SSH, richiede un’autenticazione

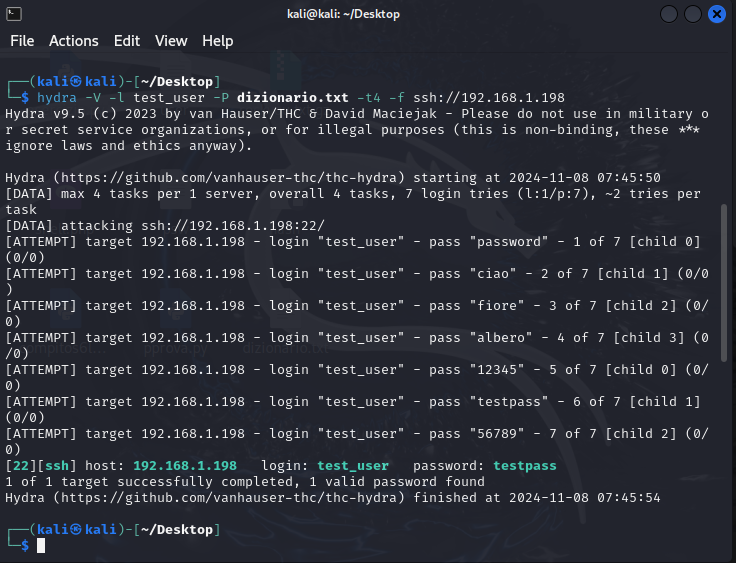
**Accesso con l'utente creato**: Una volta configurati i servizi, ci siamo autenticati sulla macchina remota con indirizzo IP inserito utilizzando l'utente test\_user tramite il protocollo **SSH** e, successivamente, tramite **FTP**.



**Avvio dell’attacco con Hydra**: Con l’utente autenticato, abbiamo avviato l’attacco vero e proprio utilizzando **Hydra.** Abbiamo fornito al programma un dizionario, prelevato dalla **Seclist**, per tentare il cracking della password. Essendo il dizionario molto ampio, la scansione richiederà diverse ore per completarsi;

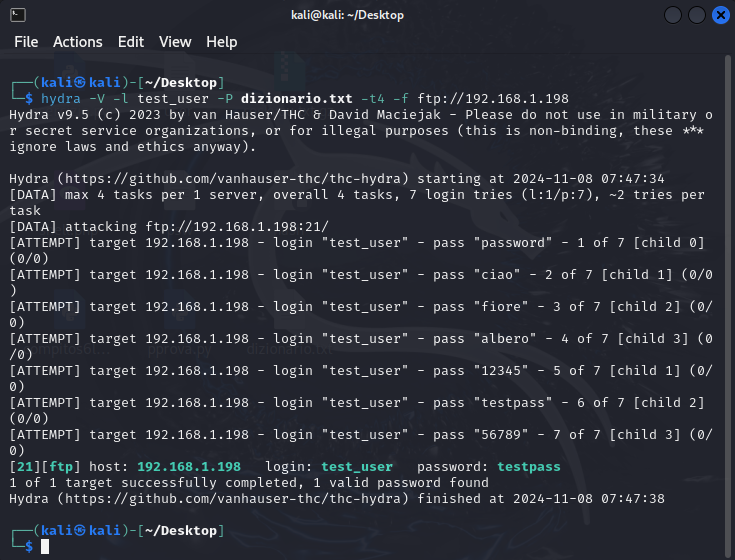


come detto precedentemente, si è optato per una soluzione che abbreviasse i tempi di scansione: ovvero quella di **ridurre il dizionario** a una lista più contenuta, che contenesse solo le password più comuni o quelle ritenute più probabili.



La password presente nella lista **dizionario.txt** creata precedentemente, è stata trovata con successo

Lo stesso lavoro è stato svolto per il protocollo FTP ed anche in questo caso la password presente nella lista è stata trovata con successo.



Con il comando utilizzato

-V ci permette di visionare i vari passaggi del nostro scan

-l indica l’user di cui ci interessa la password

-P indica la lista da dove Hydra dovrà scannerizzare le varie password

-t4 la veloicità di scansione

-f gli diciamo di fermarsi quando trova corrispondenza

Poi inseriamo il protocollo e l’IP della macchina