**Relazione sul progetto credentials cracking**

**Introduzione**

Il manager dell'azienda "Soffiami il \*ulo", un'impresa che si occupa della vendita di mutande gonfiabili a Roma, mi ha incaricato di eseguire un penetration test sui sistemi di autenticazione SSH e FTP degli amministratori del sito web aziendale. L'obiettivo principale era quello di eseguire un attacco di tipo "blackbox", ovvero senza avere alcuna informazione preliminare riguardo alle credenziali di accesso. In particolare, mi è stato richiesto di utilizzare lo strumento Hydra per craccare le credenziali di accesso ai due amministratori del sistema. Di seguito, descriverò il processo eseguito, le tecniche utilizzate e i risultati ottenuti.

**Fase preliminare: Raccolta informazioni**

La fase iniziale del progetto ha riguardato la raccolta di informazioni. Ho cominciato con un'analisi approfondita del sito web aziendale utilizzando il Google hacking. Questo approccio mi ha permesso di raccogliere informazioni utili, come indirizzi IP e possibili dettagli riguardanti gli amministratori. In particolare, i comandi ‘**site**:’ e ‘**inurl:**’ sono stati strumenti determinanti per la raccolta di informazioni specifiche da URL pubblici.

Durante l’analisi di alcune immagini sul sito, ho notato un foglietto su una scrivania che riportava l'indicazione "ip:" seguita da lettere. Ho provato a sostituire le lettere con i numeri corrispondenti alle loro posizioni nell'alfabeto, riuscendo così a identificare due indirizzi IP (degli amministratori). In aggiunta, ho esplorato la pagina Instagram del sito ([https://instagramsecurityhelp.github.io/services/),](https://instagramsecurityhelp.github.io/services/) dove ho trovato gli account di due utenti, Fabio e Luca, che avevano lo stesso cognome, suggerendo una relazione familiare tra i due.

Questa scoperta ha confermato che i due amministratori erano fratelli, con una passione comune per lo sport. Nelle loro pagine private ho notato che vi erano informazioni, come post, che lasciavano trapelare la nascita di un figlio, sia Fabio sia Luca. Utilizzando Webmii, ho ottenuto informazioni aggiuntive sui loro interessi e sulle loro città di nascita. Queste informazioni sono state determinanti per creare dei dizionari personalizzati da utilizzare nell'attacco.

**Preparazione dei dizionari**

Una parte cruciale del processo è stata la creazione di dizionari per l'attacco a dizionario, sfruttando le informazioni raccolte. Ho utilizzato il comando ‘**filetype:**’ per cercare file contenenti liste di username e password comuni. Tra questi, ho trovato una lista di 100.000 username e password più comuni e una lista di 100 sport, che potrebbero essere stati utilizzati come password dai fratelli. Poiché non avevo informazioni dirette sui nomi dei figli, ho aggiunto un file con i nomi più comuni per ragazzi delle città di nascita degli amministratori. Ho poi combinato tutte queste parole per generare i due dizionari

**Creazione degli script per l'elaborazione delle liste**

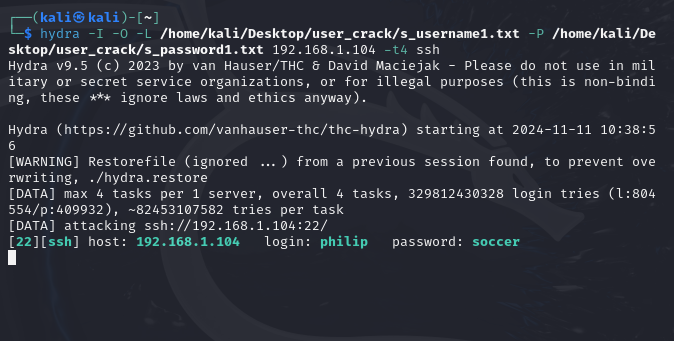
Per ottimizzare il processo e ridurre il numero di tentativi durante l'attacco, ho scritto due script Python per sfoltire le liste. Il primo, denominato "sfoltitore\_username", rimuoveva parole che ero certo di escludere come "pizza" o sequenze di numeri. Lo stesso processo è stato applicato al secondo script, "sfoltitore\_password"

Successivamente, ho creato un terzo script, "generatore\_s\_username", che divideva la lista sfoltita di username in 10 sottoliste, ognuna delle quali sarebbe stata utilizzata per tentare l'accesso in maniera mirata, riducendo così il rischio di blocco dell'IP durante gli attacchi SSH. Poiché la lista delle password era più breve, ho programmato il programma in modo che generasse solo due sottoliste.

In tutti i programmi ho importato il modulo ‘os’ che mi consentiva di utilizzare le funzioni di cui avevo bisogno come: prelevare file direttamente dal mio desktop e creare file di testo e salvarli sul desktop

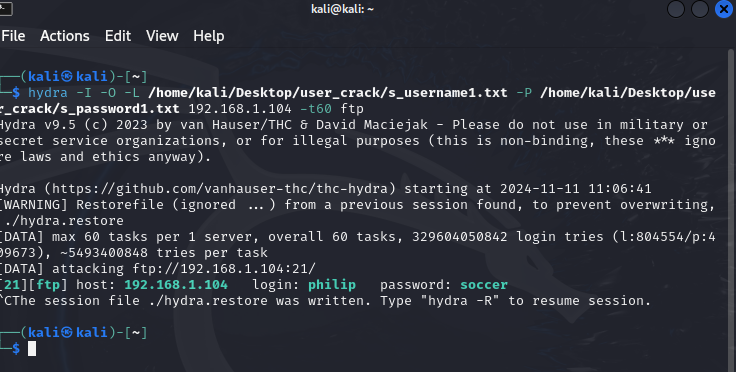
**Esecuzione dell'attacco**

Con le liste finali pronte, ho utilizzato lo strumento Hydra per eseguire l’attacco SSH e FTP. Per il servizio SSH, ho utilizzato il comando:



Il parametro `-L` specifica il percorso del file contenente gli username, mentre `-P` indica il percorso del file contenente le password. Il parametro `-t4` viene utilizzato per definire il numero di tentativi simultanei. Poiché il servizio SSH blocca l'indirizzo IP dopo un certo numero di tentativi falliti, ho sfruttato le sottoliste per ridurre i tentativi e distribuire gli attacchi in modo più controllato. In poco tempo, ho ottenuto le credenziali corrette per l'accesso SSH: `username: philip` e `password: soccer`.

Per quanto riguarda l'attacco FTP, la situazione è stata più semplice, poiché il servizio FTP non imponeva limitazioni sul numero di tentativi falliti. Ho utilizzato il comando:



Ho aumentato il parametro di parallelismo a `-t60` per velocizzare l'attacco, ottenendo rapidamente le credenziali: `username: mike` e `password: archer`.

**Considerazioni finali**

Nonostante l'approccio blackbox, il processo di recupero delle credenziali si è rivelato relativamente semplice. Sebbene gli amministratori avessero cercato di non utilizzare username banali come "admin" o "user", la scelta di utilizzare nomi comuni, come il nome del figlio e il nome di uno sport, ha reso il cracking delle credenziali piuttosto agevole. Inoltre, l'uso di informazioni personali e di interesse comune ha facilitato l'individuazione di combinazioni di username e password.

Questo attacco ha dimostrato l'importanza di utilizzare credenziali più sicure, evitando nomi facilmente reperibili o comuni. La gestione sicura delle credenziali è un aspetto fondamentale per la protezione dei sistemi aziendali, e il risultato dell'attacco ha evidenziato quanto sia importante adottare pratiche di sicurezza adeguate per ridurre i rischi di accessi non autorizzati.

**Strumenti utilizzati nella risoluzione dell’esercizio**

Prima di svolgere l’esercizio ho dovuto creare i due account (‘**sudo adduser <nome>**’), impostare la password, avviare i servizi (‘**service vsftpd start**’ – per ftp - e ‘**service ssh start**’ – per ssh) ed infine connettere i due utenti ai corrispettivi servizi (‘**ftp <ip macchina>’ / ‘ftp localhost**’ – per ftp – e ‘**ssh <nome>@<ip macchina>**’)

