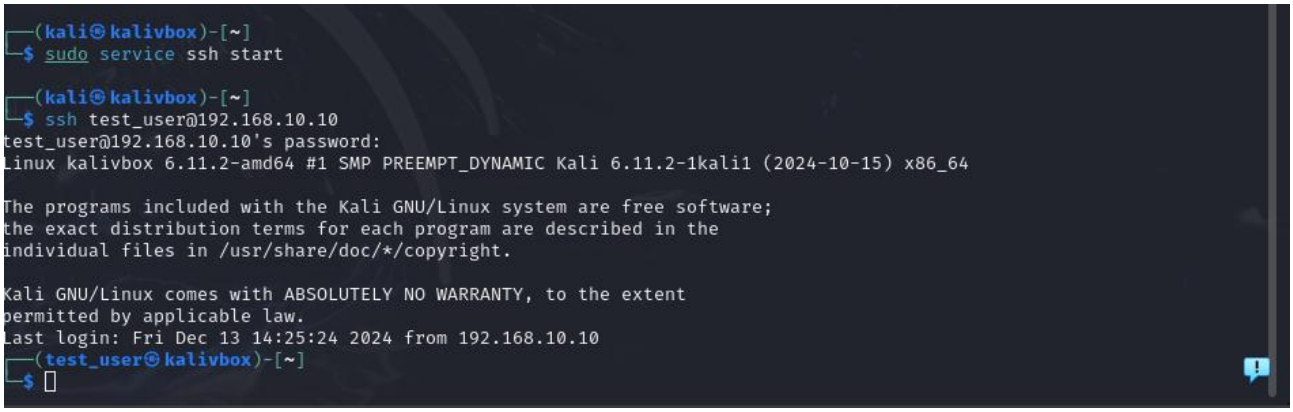
Relazione S6/L5

Lo scenario vede un utente ipotetico (test_user) con una password associata (testpass) subire un attacco di cracking. L'obbiettivo dell'attaccante era trovare l'username e password per l'accesso senza sapere quali fossero.

Aprendo un primo terminale si effettua l'accesso come l'utente x, in esempio rinominato test_user (bersaglio dell'attacco). In precedenza, sono stati impostati tutti i dati riguardanti l'utente come nome, numero di telefono e altre informazioni.



Nel frattempo, si è impostata un'altra shell per simulare l'attaccante il quale userà il tool "Hydra" per tentare una sessione di cracking ai danni del mal capitato. Tenterà di scoprire l'username e la relativa password d'accesso

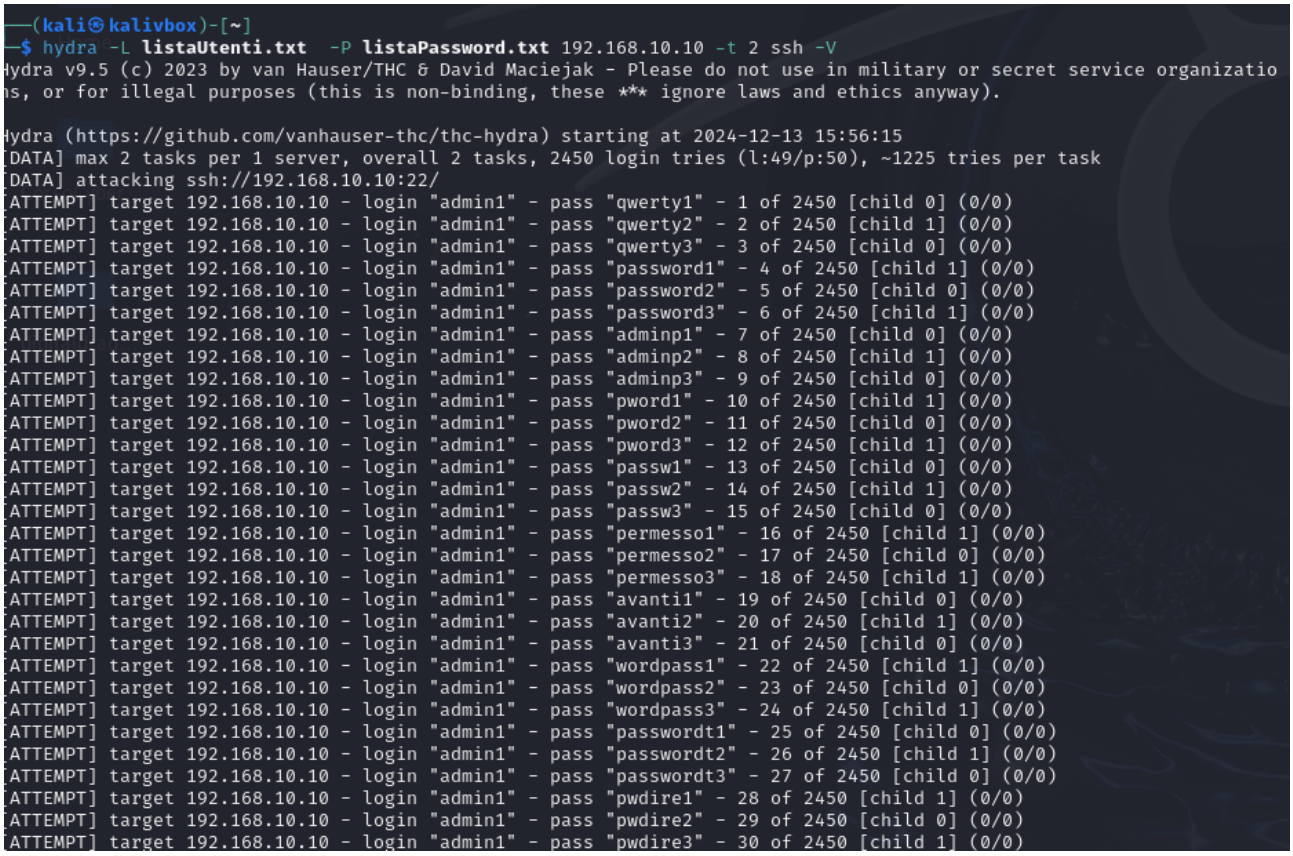
Con Hydra si è usato il comando "hydra –L listaUtenti.txt –P listaPassword.txt 192.168.10.10 -t 2 ssh -V" per tentare l'attacco di cracking.

Prendendo in esame il comando presentato gli switch -L e -P servono per utilizzare un attacco a dizionario per una scansione su tutti i componenti presenti nella lista degli utenti confrontandoli con tutta la lista delle password fino a trovare un accesso valido. Notiamo anche che il -t è impostato a 2 per poter testare tutto con una bassa probabilità di essere scoperti dalla macchina attaccata e che venga arrestato il processo di ricerca. Lo switch "-V" serve invece a monitorare "live" i tentativi di brute force in corso.

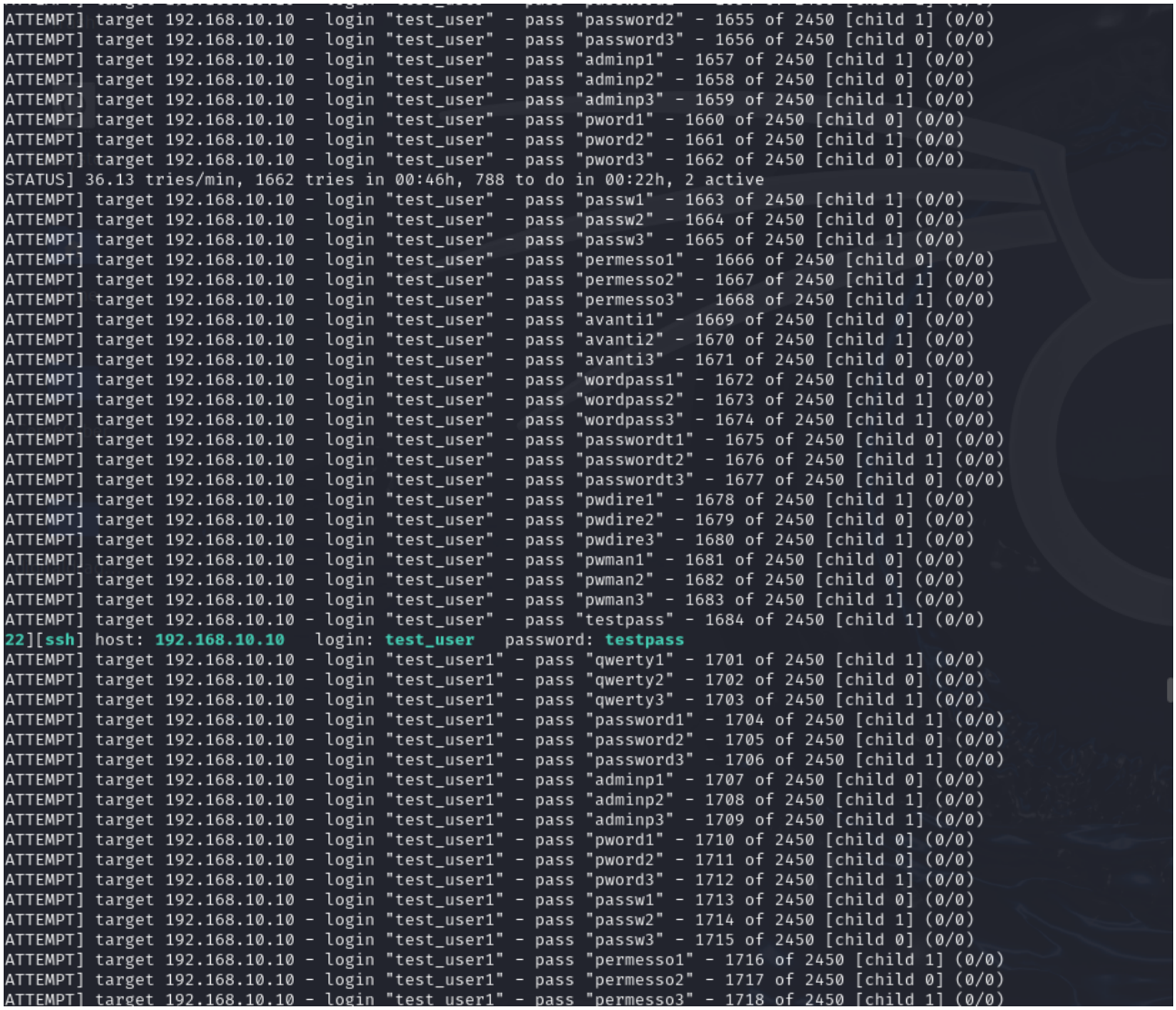
Le liste utilizzate nell'attacco a dizionario sono state create a posta per velocizzare il processo che, pur avendo pochi dati su cui lavorare (dalle 30 alle 40 per ogni lista), ci ha messo un tempo relativamente lungo per completare tutta la scansione dato il settaggio in -t 2. Se si volesse tentare un'attacco più veloce si potrebbe campiare l'impostazione di "-t" con la conseguenza che il sistema riveli troppi tentativi di accesso e blocchi la sessione di login per un tot di tempo o che faccia partire un avviso a chi si occupa della sicurezza, un responsabile, oppure che scriva nel report di elevati tentativi falliti in poco tempo sulla macchina attaccata.

Qui vediamo la partenza del tentativo di cracking da parte del malintenzionato.

Come si può notare alla partenza del'attacco di brute force la prima cosa che viene stampata è un avviso di non utilizzare questo tool in ambiti militari o governativi come agenzie di servizi segreti con intenzioni illegali.

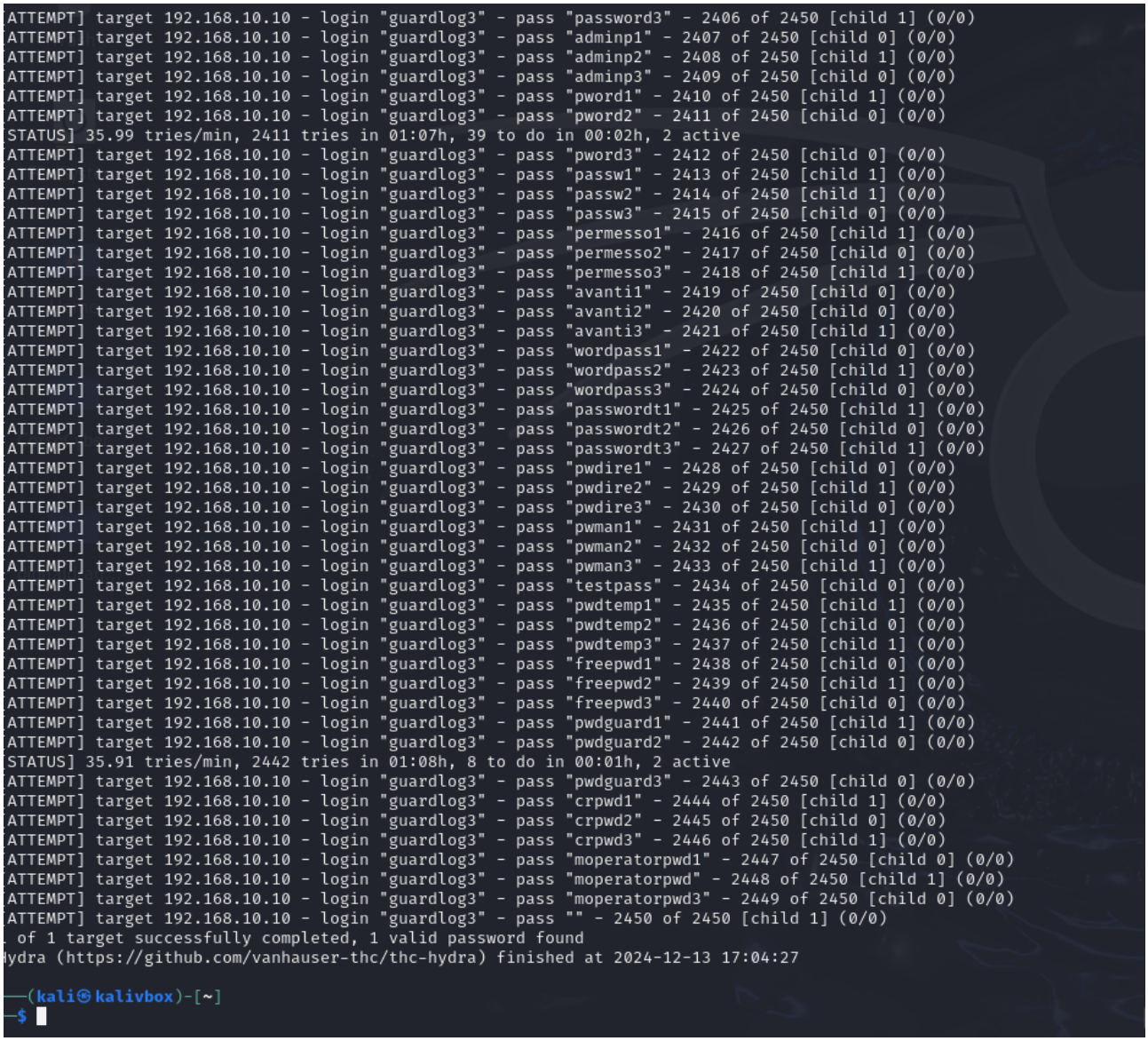


Oltre a questo avviso vengono evidenziate la data e l'ora di avvio, i numeri di task attivi massimi che può sopportare il server, il numero effettivo di task che stanno operando al momento, il numero di login che verranno eseguiti e anche l'IP target con la relativa porta.



La ricercha ha impiegato 1:07h per controllare tutte le combinazioni possibili trovando poi una corrispondenza ed evidenziandola. Ottenute le informazioni volute si potrebbe terminare l'attacco, ma in questo caso abbiamo deciso di far teminare tutta la scansione delle liste.

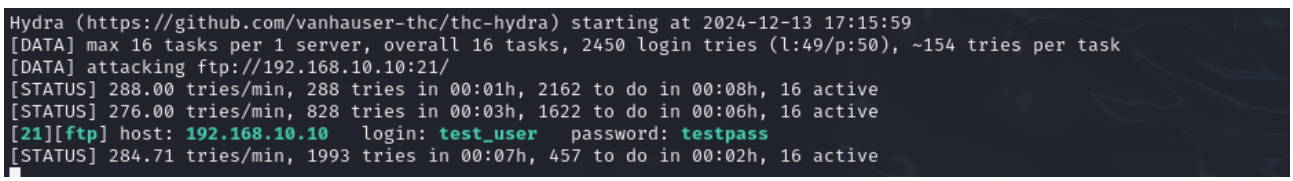
Alla fine conlude il servizio dicendo quante combinazioni funzionanti ha trovato.



Fase 2

Nella fase 2 abbiamo optato sempre per un attacco con Hydra ma utilizzando un altro servizio, il servizio in questione è l' FTP. Dopo aver installato il servizio abbiamo fatto partire il medesimo tipo di attacco ma tramite appunto il servizio di File Transfert Protocol.

Come si nota dallo script del comando in questo caso non è stato cambiato molto a parte il servizio impostato e il limite di thread non specificato, ma già al primo tentativo l'attacco al servizio FTP è riuscito dandoci in risposta username e password senza blocchi da parte della macchina attaccata. Il processo è stato molto rapido non avendo appunto settato un limite di thread, quindi di default arrivava fino a 16 combinazioni in simultanea riducendo drasticamente il tempo di ricerca.



Conclusioni

Hydra è uno strumento versatile capace di attacchi di vario genere, due di questi li abbiamo visti oggi.

Attacco SSH: protocollo di rete SH consente una connessione sicura tra due macchine, di solito sfrutta la porta 22, occorrono username e password per l'autenticazione. L'SSH cifra tutte le comunicazioni tra il client ed il server rendendo difficile la intercettare i dati, ma Hydra riesce ad eseguire attacchi di brute force cercando di indovinare le credenziali dell'utente (password e username), ma deve essere impostato con un basso numero di thread altrimenti la macchina vittima reagirà all'attacco bloccando i tentativi di log legati all'account o alla macchina.

Attacco FTP: il protocollo FTP è utilizzato per il trasferimento di file tra client e server, di solito sfrutta la porta 21 di default, ma sfrutta anche una gamma di di porte per il trasferimento in modalità passiva, gli occorono username e password per l'autenticazione. FTP non cifra i dati trasmessi, rendendo le comunicazioni vulnerabili ad intercettazioni. Hydra tenterà anche in questo caso di carpire username e password dell'utente sotto attacco.

In sintesi, mentre entrambi i servizi utilizzano nomi utente e password per l'autenticazione, SSH offre una maggiore sicurezza grazie alla crittografia dei dati trasmessi, mentre FTP non lo fa. Hydra può essere utilizzato per attaccare entrambi i servizi cercando di forzare le credenziali.