# Lab 4 - Port scanning

1. Run a ping scan in the 192.168.56.1/24 subnetwork. List all hosts that are reported as up.

   Command used:
   ```
   nmap -sn 192.168.56.0/24
   ```
   Result:
   3 hosts up:
   192.168.56.2 (network interface)
   192.168.56.5 (kali vm)
   192.168.56.6 (metasploitable2 vm)
   Explanation:
   The flag `-sn` is used to scan a network in order to find which hosts are up.

2. Scan all ports of the target host (the Metaesploitable2 machine) using two different methods.

   Commands used:
   - TCP Stealth (SYN) scan:
   ```
   sudo nmap -v -sS 192.168.56.6 -p-
   ```
   - TCP FIN scan:
   ```
   sudo nmap -v -sF 192.168.56.6 -p-
   ```
   Result:
   ```
   30 open/filtered ports
   ```
   Explanation:
   I used two of the different TCP scans to get the ports that are open on the Metasploitable2 machine with a higher level of verbosity, as TCP FIN scan did not output the open ports by default.

3. Find the device type, OS and version of the target host.

   Command used:
   ```
   sudo nmap -sV -O 192.168.56.6
   ```
   Result:
   ```
   Device type: general purpose
   OS: Linux 2.6.X
   Version: 2.6.9 - 2.6.33
   ```
   Explanation:
   I ran nmap with the -O flag to get the OS information needed (device type, OS and OS version).

4. Run a service detection only for those ports determined as open in step (2). Run it again using all service probes and compare the result with the default service detection.

   Command used:

Default service probes:

```
sudo nmap -sV -p
21,22,23,25,53,80,111,139,445,512,513,514,1099,1524,2049,2121
,3306,3632,5432,5900,6000,6667,6697,8009,8180,8787,43387,4774
6,55487,56554 192.168.56.6
```

All service probes:

```
sudo nmap -sV --version-intensity 9 -p
21,22,23,25,53,80,111,139,445,512,513,514,1099,1524,2049,2121
,3306,3632,5432,5900,6000,6667,6697,8009,8180,8787,43387,4774
6,55487,56554 192.168.56.6
```

Result:

There is no difference between the default one and the one using all the probes. This could be due to the default version scan using `--version-intensity 7`

Explanation:

I ran the service version scan for a list of the ports that were reported as open in the second activity of the lab, both with the default level of intensity and with the highest (9) level of intensity (using all service probes).

5. Notice that the target machine is running a bindshell over some tcp port. Connect to it and check that this is a backdoor that gives you root access. Use the privileges to steal the password files from the target machine. Crack it and report as many passwords as you can.

Command used:

```
# Connect to the bind shell with netcat
nc -nv 192.168.56.6 1524
```

Result:

The cracked passwords are (cracked 6 out of 7):

```
user (user)
postgres (postgres)
msfadmin (msfadmin)
service (service)
123456789 (klog)
batman (sys)
```

Explanation:

I ran netcat specifying the port where the bind shell was running, connected to the metasploitable machine and copied the content of both "/etc/shadow" and "/etc/passwd" files into the kali virtual machine, then proceeded to unshadow them and run John the Ripper to crack 6 out of the 7 passwords in a few seconds.