LAB: scanning

Lab Environment

The workshop WiFi:

- SSID: `workshop`
- PASS: `iij/2497`

Hosts - Virtual machines (Ubuntu 18.04LTS/LXC)

- Hostname: `nsXX.workshop`
- IPv6: `fd00:2497:1::X`
- IPv4: `10.0.0.X`

Where `X` and `XX` is yoru group ID. For group 1, hostname is `ns01.workshop`, IPv6 address is `fd00:2497:1::1`, and IPv4 is `10.0.0.1`.

Install Nmap

`ssh` to your virtual server and install the Nmap software.

```
$ sudo apt install nmap
```

Host detection

Detect online hosts using ping.

```
$ nmap -sn 10.0.0.0/24
```

```
$ nmap -sn 10.0.255.0/24
```

Scan one host

Scan a specific node by specifying its IP addrss.

```
$ sudo nmap -A IP_ADDRESS
```

Scan yourself

Scan your local node to check what kind of services you are using.

> Warning: Do not scan others

```
$ sudo nmap IP_OF_YOUR_NOTEBOOK
```

OS detection

Try to guess the operating system of the scan target.

```
$ sudo nmap -O IP_ADDRESS
```

Version detection

Try to guess the software version of the services of the scan target.

```
$ sudo nmap -sV IP_ADDRESS
```

Try to scan our hosts

Scan our testbed servers.

Scan our border gateway.

```
$ sudo nmap -A 10.0.255.1
```

Q: What is the Operating System of the target?

Q: What are the SSH host keys of the target?

Q: What is the MAC address of the target?

Q: What kind of services does the border gateway provie?

Q: What are the version numbers of the service software?

Scan our own Root DNS server.

```
$ sudo nmap -A 10.0.255.10
```

See what is happening

Capture the network traffic using wireshark to see how `nmap` scans the targets.