# OTLab 09

*Scanning Techniques with 'nmap'*

Prof. Dr. Luiz Fernando Freitas-Gutierres (a.k.a. substationworm)

`linkedin.com/in/lffreitas-gutierres`

`github.com/substationworm/OTLab`

`luiz.gutierres@ufsm.br`

## Problem Overview

### Containerized Hosts (Generic Corporate Systems)

- `server1`: `172.30.0.11`, `02:aa:bb:cc:dd:11`.
- `server2`: `172.30.0.12`, `02:aa:bb:cc:dd:12`.
- `server3`: `172.30.10.10`, `02:aa:bb:cc:dd:13`.
- `attacker`: `172.30.0.5` (`eth0`) and `172.30.10.5` (`eth1`), `02:aa:bb:cc:dd:01`.

### Networks

- `corp-net`: `172.30.0.0/24` (single `/24` broadcast domain).
- `corp-subnet`: `172.30.10.0/26` (subnet).

## Tasks

1. Issue three ICMP echo requests (`ping`) from the `attacker` workstation to `server1` while capturing ICMP traffic on `server1` using `tcpdump`. Analyze and describe the communication pattern.

2. Conduct a host discovery scan (no port scan, using `-sn`) on the `corp-net` from the `attacker` workstation while monitoring ARP traffic on `server1` using `tcpdump`. Analyze and describe the ARP-based communication.

3. Perform a TCP connect scan (`-sT`) from the `attacker` workstation against port 22 on `server1`, and monitor the resulting TCP traffic on `server1` using `tcpdump`.

4. Repeat Task 3, but use a SYN stealth scan (`-sS`) instead of a TCP connect scan.

5. Repeat Task 3 using the following TCP flag–based scans: Null scan (`-sN`), FIN scan (`-sF`), and Xmas scan (`-sX`).

6. Execute a UDP scan (`-sU`) from the `attacker` workstation targeting `server2` on ports 53 and 161 while monitoring UDP and ICMP traffic on `server2` using `tcpdump`.

7. Use `nmap` to perform service and version detection (`-sV`) against ports 22 and 80 on

`server1`.

8. Use `nmap` to conduct a cross-subnet scan (`-sS`) targeting port 9999 on `server3`.

## Tools

These are the tools available on the server1, server2, server3, and attacker hosts for completing OTLab 09: `ifconfig`, `nmap`, `ping`, and `tcpdump`.

## Nomenclature

- ARP: Address resolution protocol.
- ICMP: Internet control message protocol.
- IP: Internet protocol.
- MAC: Media access control.
- TCP: Transmission control protocol.
- UDP: User datagram protocol.