INR Lab 2 - IPv4 & IPv6

> **Note**: only scan the ports of the machines you own or is allowed to scan. You might break some stuff

Overview

In this lab, you will get familiar with some of the layers of the OSI model, mainly the layers from 3 (Networking) to 7 (Application). You will learn about some protocols relying on the IP protocol (version 4 and 6) and you will learn some of the skills required to troubleshoot your networks in the case of problems.

Task 1 - Ports and Protocols

> Using your network topology from the previous lab, you will be gathering some information about your machines.

1. Check the open ports and listening Unix sockets against ssh and http on *Admin* and *Web* respectively.

   Hint: use lsof, netstat

2. Scan your gateway from the outside. What are the known open ports?

   Hint: use nmap

3. A gateway has to be transparent, you should not see any port that is not specifically forwarded. Adjust your firewall rules to make this happen. Disable any unnecessary services and scan again.

4. It suppose that some scanners start by scanning the known ports and pinging a host to see if it is alive.

   4.1. Scan the *Worker VM* from *Admin*. Can you see any ports?

   4.2. Block ICMP traffic on *Worker* and change the port for SSH to one that is above 10000.

   4.3. Scan it without extra arguments.

   4.4. Now make necessary changes to the command to force the scan on all possible ports.

   > **Note**: *Nmap* doesn't only use ping for discovery but also other probes, you can read about this the documentation, Chapter 3: Host Discovery.

   4.5. Gather some information about your open ports on *Web* (`ssh` and `http`).

   > **Note**: Don't paste the scan results, summarize them in the answer and include them as an appendix of your submission in Moodle.

Task 2 - Traffic Captures & IPv6

In some cases, you might need to take a look at the traffic sent and received from your machines to understand what is going on. You will be sniffing the traffic of your External services. For this, you can use `Wireshark` which has an integration with GNS3 or `tcpdump` from the machines.

1. Access your *Web* Page from the outside and capture the traffic between the gateway and the bridged interface.

   Can you see what is being sent?

What kind of information can you get from this?

What do the headers mean?

2. SSH to the *Admin* from the outside and capture the traffic (make sure to start capturing before connecting to the server).

   Can you see what is being sent?

   What kind of information can you get from this?

   What are the names of the ciphers used?

3. Configure `Burp Suite` as a proxy on your machine and intercept your HTTP traffic.

   Show that you can modify the contents by changing something in the request.

   Why are you able to do this here and not in an SSH connection?

   Do you know any other tools that are analogues to `Burp suite`? List and give a one-line description of them.

4. Configure `IPv6` from the Web Server to the Worker. This includes IPs on the servers and the default gateways.
5. Access the *Web* Page using `IPv6` from *Admin* while capturing again. Can you see the difference? What's the difference?

   Attach you `IPv6` captures in a folder `captures` with your report.