Lab 2 - Mapping Network and Services

References:

- Wireshark tutorial, from HowtoGeek
- LifeWire has a more recent Tutorial, but HowtoGeek has more details.
- Nmap reference guide
- Target Specification
- Wireshark, Ethernet Capture Setup relevant for understanding the capture in switched networks, but not needed to perform the exercises

NOTE: For this class you should use the Host network configuration that was provided/configured in previous class. Commands below that start with # should be run as `root` (you can also use `sudo`).

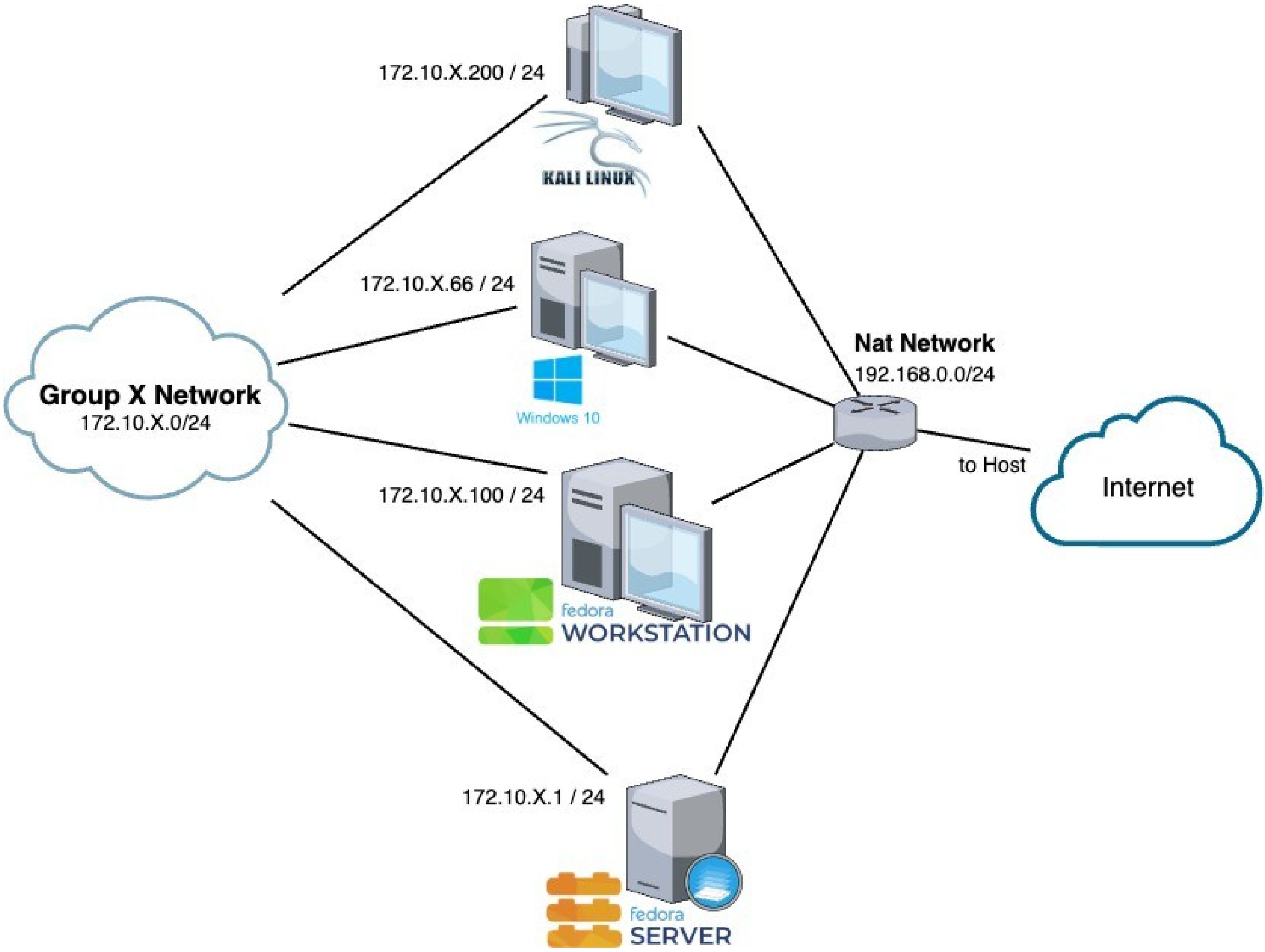

Figure 1 - Network Organization

Initial Network setup (see previous class)

Configure a static IP address for the group private LAN on the machines Kali, Win7, Fedora Desktop and workstation as described in previous class.

Wireshark setup (Exercise 0)

When running Wireshark, you need to run it as `root` (or `Administrator` in Windows). As running applications as `root` is a security risk, you should enable non-root users to capture packets (there are options to restrict or only enable specific users to capture packets). You can use this link for additional information.

Exercise 1 - Using Wireshark

Run Wireshark in one of the machines. Familiarize yourself with the interface (or recall if you have already used it). Through the help system or the Wireshark tutorial study the basic of the filtering expressions.

- . Write a wireshark filter that allows you to filter just the network traffic on the interface that connects to the Host network, originates on the that machine and is `http`. Look at the output from a session accessing the Museu Nacional do Azulejo website. Repeat for Sigarra, during and after authentication (you can do a bogus login). Can you see any password in transit? Why?
- . See the messages related to the `SSL` connection and inspect several field that have been explained in the previous lecture class. Also see the certificates that are announced by the web server.

Install an imap/pop server on your fedora server. See below how. Install an email client (ex.: Claws mail) on the workstation. You can use the email account for `auser` at the fedora server.

- . Create a filter in wireshark to capture the IMAP/POP sessions (ports: `143`, `110`) that your email client in the workstation machine establishes with the IMAP server. Can you see the password? (may need to decode from base64).
- . Solve the security problem by configuring an authentication mechanisms that do not imply plaint text authentication and recheck in Wireshark. Which version of `TLS` is being used (or stated by wireshark)?

Exercise 2 - Penetration testing

Before doing penetration tests you should survey the target network, for mapping and identifying potential targets. This can be done with scanning tools such as nmap. Check the nmap tutorial to get acquainted with the functionalities of this utility (the tutorial is archived but gives a feeling of the capabilities). See also the Port Scanning Techniques.

- Use the `-v` and `-n` options in `nmap` (check why using the `nmap` documentation).

- . Using `nmap`, discover which IP addresses of the `192.168.0.0/24` network are active.
    - . Use wireshark to determine which type of packets are being used for the discovery.
- . Use `nmap` to discover all VMs on your group (use the `172.10.X.0/24` network) identifying its Operating System's version and the active services in each.
    - Review with care the `nmap` syntax for specifying the targets accurately.
    - . Do the same for the `192.168.0.0/24` network.
- . See what the different types of scans do (`-sS`, `-sN`, `-sF`, `-sX`, `-sM`, `-sA` e `-sW`) and use them to obtain more information.

. Discover on the IP addresses, OSes, and net services versions for the machines (if any) that have the following protocols available `smtp`, `smtps`, `imap`, `imaps`, `http`, `https`, `telnet`, `nfs`, `netbios-ns`, `pop3` and `dns`.

  - You should specify the ports to scan and not do a port range (you can use strings as identifiers for the ports).

. Do a detailed scan of the services running on the local machine (the one running `nmap`), discovering its services (use the `loopack` address or the `172.10.X.0/24` address) and use wireshark to see the packets used on that detection.

  . If no service is running on the local machine (you should, at least find an SSH service).
  . Based on the analysis of the packet flow, how can `nmap` determine if a port is closed, open or filtered?
  . How does `nmap` it discover the service version running on a specific port?

. What is an `idle-scan`? You can performe one using the `172.10.X.0/24` network.

  . From the Kali machine discover if the Windows machine can be used as a *zombie* (may need to turn off Windows Firewall).
  . Add the following `iptables` rule on the Fedora Server using the correct NIC name (ens7 is used in the example):

```
iptables -I INPUT 1 -p tcp -i ens7 --tcp-flags SYN,ACK,FIN,RST SYN -j
LOG --log-prefix "port-scan? "
```

See on the `iptables` manual what the `--tcp-flags` option does. Using this we can "watch" on the log the start of a TCP connection (the `SYN`). To watch it, you should do:

```
tail -f /var/log/messages
```

With the `-f` option, `tail` monitors the file showing the "additions" to it.

  . Run an `idle-scan` targeting the Fedora Server from the Kali machine using Windows as the *zombie*. Compare the result with the one from a direct scan (both from the results obtained and the log entries).

. Repeat the previous question, but this time try using IP spoofing with "source Decoys" to help hide the origin of the scan (use the `172.10.X.0/24` network). Explore the manual to figure out how to use this option.

. On the Kali machine you can install zenmap, a graphical user interface for `nmap`. Test it and see/explain the options for the `Slow comprehensive scan`.

Exercise 3 & 4 - Installing an IMAP/POP server

In this exercise we will be using the imap/pop server dovecot (a server designed with security in mind).

. Install the server `dovecot` with `dnf` on the Fedora Server machine

. Change the following configuration files:

> `/etc/dovecot/conf.d/10-ssl.conf`: change the `ssl=required` to `ssl=yes`.

> `/etc/dovecot/conf.d/10-auth.conf`: by default `un-encrypted authentication` is not allowed. Change the configuration to allow it.

> `/etc/dovecot/conf.d/10-mail.conf`: configure the `mail_location` as follows: `mail_location=maildir:~/Maildir`.

. Start the `dovecot` service

- Using `#> systemctl start dovecot`

  . Check it is running

  > Using `#> systemctl status dovecot`

  . Save the `iptables` rules, using the `iptables-save` command (the rules can be restored with command `iptables-restore`).

    . Disable all firewall rules.

    . Also disable the `firewalld` service that can prevent remote access to the server:

  > Using: `#> systemctl stop firewalld.service`.

. You can test it by connecting with `telnet` to the `imap` port and loging in:

> `. LOGIN auser <password>` (note the initial "." (see test IMAP server).)

As there isn't an email server configured you do not have any email.

- You can check this by writing:

  > `. SELECT inbox`

- Logout with:

  > `. LOGOUT`

. Try to access this server via an email client (e.g. Claws Mail).

. Repeat the relevant parts of Exercise 2 and try to detect the newly created `IMAP`/`POP` services.