Network Discovery with Port Scanning Module (20-25 mins)

Learning Outcomes

- Learn how an attacker uses port scanning to gather information that can be used later for an attack.
- Be able to discover what hosts are alive on a network and what services are running on them.

About Port Scanning:

Port Scanning is the process of making connection attempts to another networked computing device in order to gain information about what services are running on the machine.

Procedure:

Step 1: Ping Scan

When scanning a network, the first thing to do is to determine which hosts are "alive" on a network. This process is known as host discovery and can be done using the tool **nmap**.

Nmap has a vast amount of methods for performing host discovery. In this module, we will discuss only one, the basic "ping" scan.
Basic command - `nmap -sn host_ip_address`

Your Turn

Open "**team#_wadc-adversary**" VM console

Username: root
Password: root

Open the terminal in the machine to execute the commands.

Use the following commands to discover which hosts are alive on the corp, control center, and substation networks:

Control Center: `nmap -sn 52.135.80.1/24`
Substation 1: `nmap -sn 6.87.151.1/24`
Substation 2: `nmap -sn 6.87.152.1/24`
Substation 3: `nmap -sn 6.87.153.1/24`
Create a list of IP addresses in a text file (name it `hosts`) for these networks.

Step 2: Service Scan

After you have discovered which hosts are alive on the various networks of interest, we then want to interrogate those machines with a deeper scan. This is where the *nmap service scan* comes into play.

To do a service scan against the IP addresses in a file called `hosts`, issue the following command:

```
nmap -iL hosts -sV
```

Your Turn

Now do the same for the list of IP addresses that you collected from the ping scan by creating a text file. Write all the discovered IP addresses in that file separated by line breaks (“Enter”) and name the file as “hosts” and run the aforementioned command in the terminal.
Note: The directory in which the command is executed should be the same as that of the file “hosts”.

Take note of key services that are running on each host on your **worksheet.**

Report

1. Note down the command you used and the corresponding information collected.
2. Analyze the information that you get and comment on what potential attacks could happen to your fleet.