Network scanning

NETMET Lab Exercises 12

Introduction

Now we have seen some tools to monitor a network (ping, traceroute, iperf, …) , it can be interesting to find out more information about what are the hosts composing these networks. As a network engineer, the more information we get, the more we can be proactive about potential attacks.

Disclaimer : Using a network scanner on an unauthorized network can lead to serious legal issues (see https://nmap.org/book/legal-issues.html).

Nmap

Nmap (https://nmap.org/) is a free and open-source network scanner. This utility can be used to scan opened ports on a target and try to guess the OS. You can use it on your own laptop or via the EdgeNet nodes.
We will use the public /24 network of nmap to do the experiments (**scanme.nmap.org/24)**.

Host discovery

Documentation: https://nmap.org/book/host-discovery-techniques.html

The first step of a security audit is usually to find out the host connected to the network.

- Use Nmap to discover the hosts of the network **scanme.nmap.org/24**.
- Explain how nmap finds the hosts up in a network by studying it with Wireshark.

Port scanning

Documentation: https://nmap.org/book/port-scanning-tutorial.html

Now we have our network targets, we can try to find out what services they are hosting by performing port scans and service detection.

- Use Nmap to a **scanme.nmap.org** to check the open ports using different scanning options (-sS, -sT, -sA, -sU, …). Explain the differences between them by using Wireshark.
- Use Nmap and your knowledge to find out what services are running on this target.

Remote OS guessing

Documentation: https://nmap.org/book/osdetect-methods.html

- Try to guess the OS of this **scanme.nmap.org** while capturing the traffic on Wireshark.
- Try to spot some fingerprinting methods in the wireshark capture and explain them.

Code one technique of your choice

- Implement *one* technique seen during this session (host discovery, port scan, OS detection fingerprint technique, …) in Python. During your tests, use a target you own or **scanme.nmap.org.**