IT-ADVENTURES

MAKING IT FUN

Network & Vulnerability Scanning

Module 10

Module 10 Agenda

➢ Network Scanning

➢ Port Scanning

➢ Vulnerability Scanning

Network Scanning

Network Scanning

- As we learned in Module 8, we can perform a penetration test to check for vulnerabilities within a computer system.
- Recall, passive reconnaissance is the first step of the pen test.
- The next step of a pen test is network scanning

- **Network scanning** is the process of finding what devices are on a network to discover potential entry points and weaknesses in the network.

Network Scanning

- Hackers commonly use network scanning to gain access to a computer system within a network.
  - Hence it is the second step of a penetration test
- Network scanning is not only used by hackers but large companies to try and keep their systems secure and protected.
  - They can be used to find vulnerabilities before hackers do and patch them up.

Network Scanning

Network Scanning is broken down into three parts…

- **Network/Host Scanning**
- **Port Scanning**
- **Vulnerability Scanning**

to gather sensitive information

Network/Host Scanning

Network/Host Scanning

Network/Host Scanning:

What is it:

- Lists all the potential IP addresses within a network

Why: Helps discover and manage devices being used on a network

Network/Host Scanning

How it works:

- Send out pings or packet to all the potential IP addresses in the network. A response will be send back to determine if the device in active or dead.
- Therefore, collecting all the active hosts and mapping out their IP addresses.

Port Scanning

Port Scanning

Port Scanning:

What is it:

- Lists all the open ports and services in a network

Why: Identifies open ports where attackers can easily hack a system

Port Scanning

How it works:

- Ports are where information flows in and out of to and from the internet or other computers.
- Port scans are just like network/host scans. After finding out all the IP addresses, port scans sends out either a ping or a packet to the ports within a network.
- They then get a response back that includes detailed information about the port.

Vulnerability Scanning

Vulnerability Scanning

Vulnerability Scanning

What is it:

- Discovers the presence of known vulnerabilities

Why:

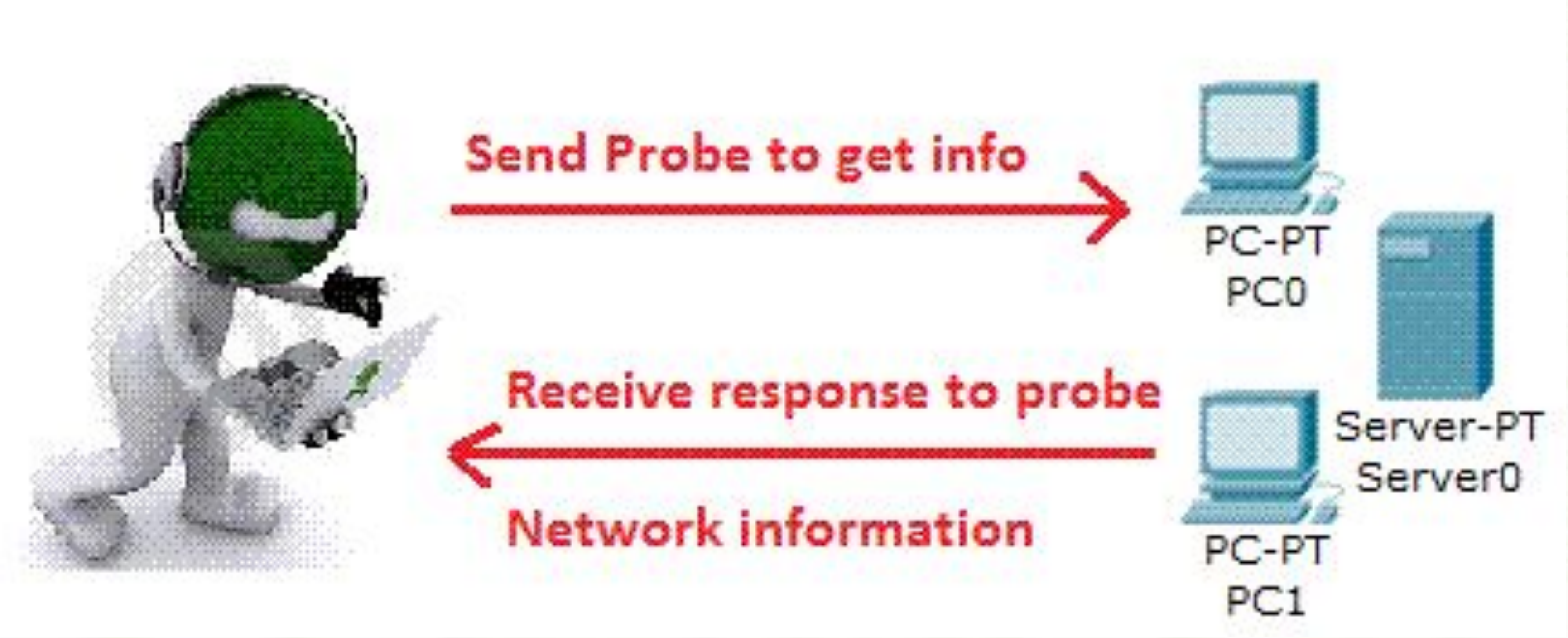
- Vulnerabilities within a network are a tremendous threat to the systems within the network and the data is holds.

Vulnerability Scanning

How it works:

- Once again, pings or packets are used to find the possible vulnerabilities of a network.
- This will result in a response given by the devices on the network.
- The results are then compared to a database that defines flaws, poor programs, misconfiguration, bugs, and defaults.

Network Scanning



Copyright 2021 Iowa State University

Types of Network Scanning Tools

- Nmap
- Nikto
- Nessus
- Armitage
- Metasploit

- We will be testing out how to use, Nmap, Armitage, and Metasploit in Activity 1 and Activity 2

To Do

❏ Complete Module 10 Activity 1

❏ Complete Module 10 Activity 2

End of Module 10!

What questions do you have?

Next Module Topic:

Auditing and Remediation!

Questions?

Contact IT-Adventures support staff!

email:

ita@iastate.edu

Your school’s IP-Range can be found at:

http://www.it-adventures.org/ip-ranges/