Network Scanning
Beau Bikakis, Guang Jin Liu, Tue Le
Advisor: Dr. Melissa Danforth  Assistant: Alfonso Puga

Partial support for this work was provided by the National Science Foundation’s Federal Cyber Service: Scholarship for Service (SFS) program under Award No. 1241636.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Department of CEE/ Computer Science

Background

How does the Internet work?

The Internet is the interaction of many connected devices across the world. It is a combination of hardware (computers, routers, servers, etc.) and protocols (a common set of rules for all internet devices to follow). All devices on the Internet can speak to each other because they all follow the same set of protocols (TCP/IP).

When a device is connected to the Internet through a local area network, it is given a special IP address to differentiate it from all the other devices that are also connected to the Internet. The IP address has two main functions: network identification and location addressing.

Client computers send requests to an Internet server in order to open web pages, watch videos, etc. The request goes through a series of routers to reach the Internet server, the server searches its database for data that matches the request and then sends back its response. The client is the input and the server is the output.

What is Network Scanning?

Network scanning is the use of scanning software to identify servers, devices, and clients on the network. It can be done by administrators looking to secure their network or hackers looking to exploit vulnerabilities.

How does Network Scanning work?

By using the correct programs and knowing how to use them, scanning networks can become quite easy. Those programs can scan network vulnerabilities, capture packets, and detect incoming threats. Keep this in mind when you are on the Internet as anyone can scan your web activity to quickly find unencrypted passwords and determine what websites you have been on.

Network Scanning Programs

Wireshark

- Scans network traffic.
- Analyzes packets (data that can be transferred over a network).
- Filters through packets to find specific criteria.
- Is graphics-based instead of terminal-based.
- Monitor data coming in and out of your network.

TCPdump

- Acts similar to Wireshark but has a different interface.
- Terminal-based.
- You type in command for which filter you want to apply.

Nmap

- Shows all hosts and devices connected to your network.
- Creates a virtual “map”.
- Can determine the operating system of the target.
- Discovers hosts by sending a packet and analyzing the response.

Snort

- Detect the intrusion of computers from outside world.
- Detect the intrusion in and out from the computer.
- Can choose between different types of alerts and actions for different inputs.
- Has three settings: sniffer, packet logger, and Network intrusion detection.

Network

- Network is a subnet of links that get data to destination IP
- A Network is two or more computers linked together in order to share resources
- Data is organized into packets.
- There are series of headers for the different tasks within the packet.
- Host to network is physical connection between two machines, such as WiFi, Ethernet, etc.

Network Vulnerabilities

- Bugs in server programs, client programs, websites or web programs.
  - Mistake in program code.
  - Exploitable feature of program.
  - Malicious code.

- No default encryption that protects from packet sniffing.
- No verification of addresses and infrastructure servers.

Additional Info.

- Most programs shown here are totally free to download.
- It is illegal to scan other people’s network without proper clearance.
- Permission is needed to scan other people’s network.

References

- Wireshark: http://www.wireshark.org/
- TCPdump: http://www.tcpdump.org/
- Nmap: http://nmap.org/
- Snort: https://www.snort.org/
- IP protocol: https://www.ietf.org/rfc/rfc791.txt