Northwest State Community College

Nmap Basics

Made possible through support from the National Science Foundation (NSF) award number 1800929

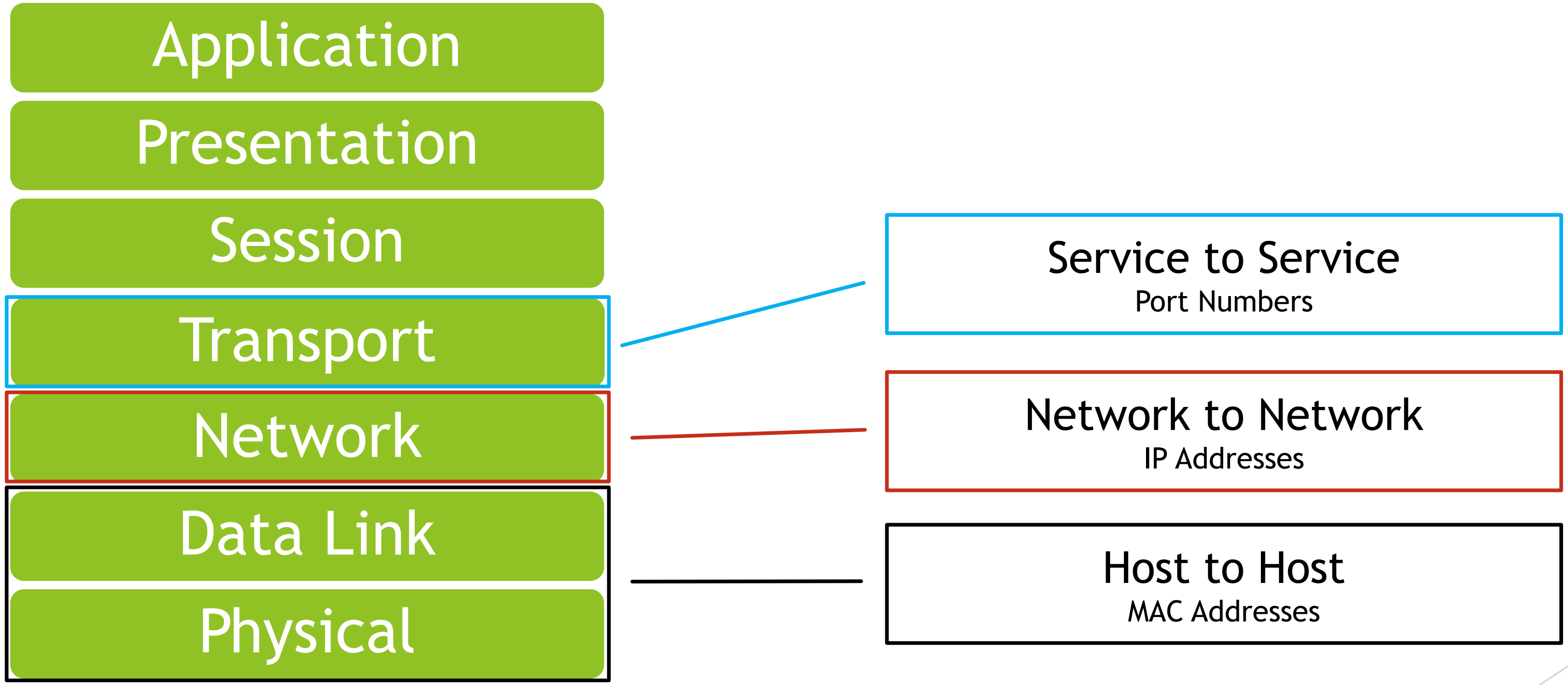
Objectives

- Describe TCP/IP Network Communications.
- Discuss Nmap Host Discovery.
- Discuss Nmap Port Mapping.
- Discuss Using Nmap to Identify Target Service and Operating System Data.
- Use Nmap to Perform Network Mapping.

TCP/IP Network Communications

OSI Reference Model

- The OSI Reference Model



Application

Presentation

Session

Transport

Network

Data Link

Physical

Service to Service
Port Numbers

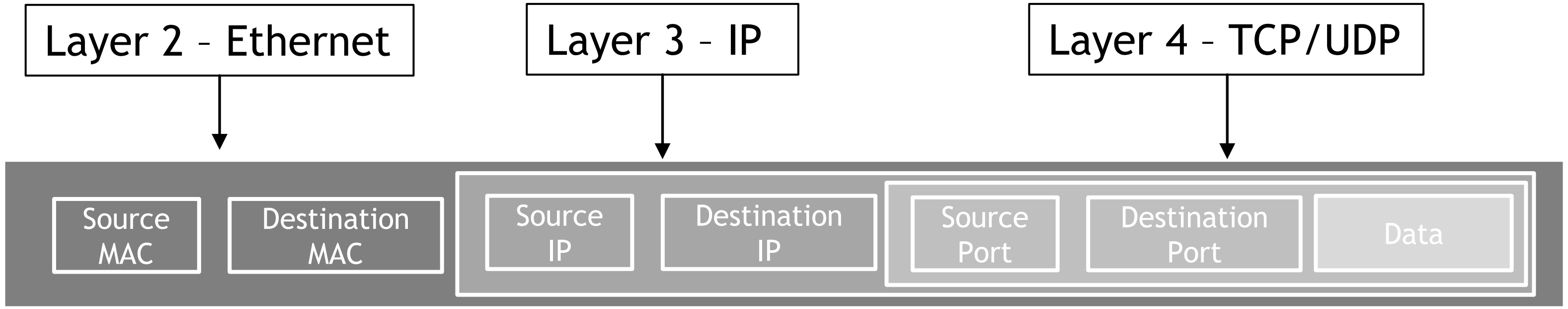
Network to Network
IP Addresses

Host to Host
MAC Addresses

TCP/IP Network Communications

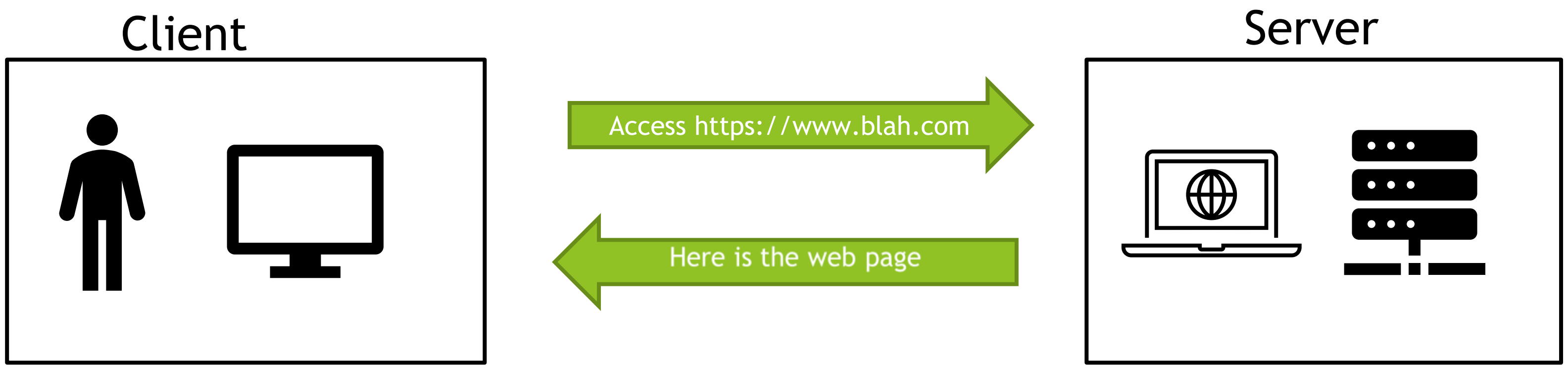
Data Headers

- The data to be transferred is broken down into smaller units known as segments, packets or frames
  - This is done to reduce congestion and to make error recovery faster
- Headers will be added before the data is transmitted so that it can properly be processed when it is received



TCP/IP Network Communications

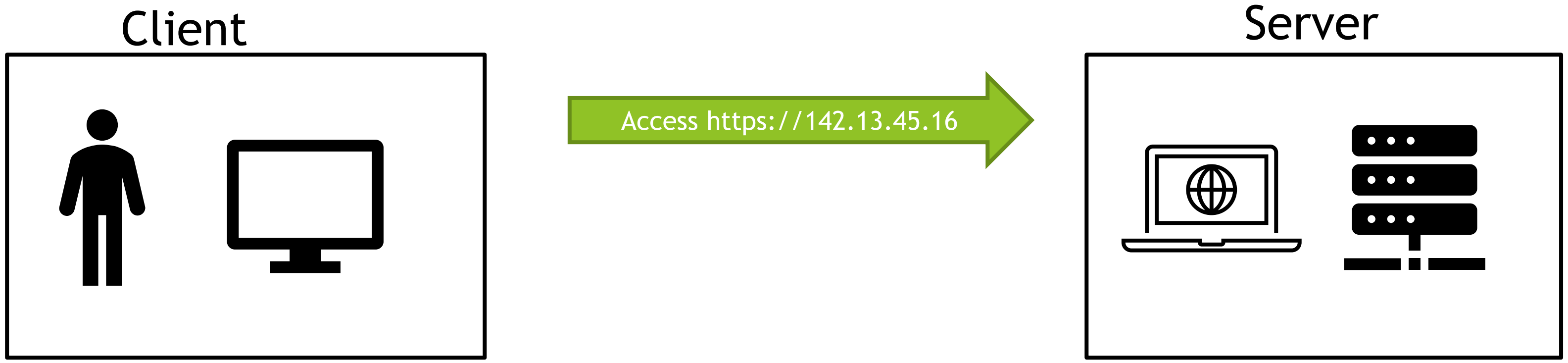
Simple connection



- A typical network connection is made up of many steps involving many different protocols.

TCP/IP Network Communications

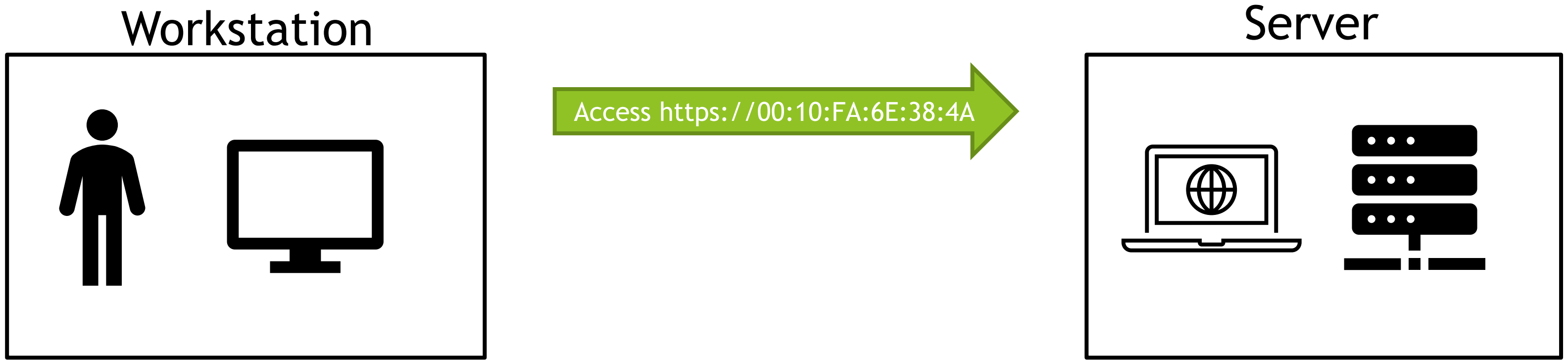
DNS



- DNS - Domain Name Service translates the name www.blah.com into the IP address needed to allow communication between TCP/IP networks.

TCP/IP Network Communications

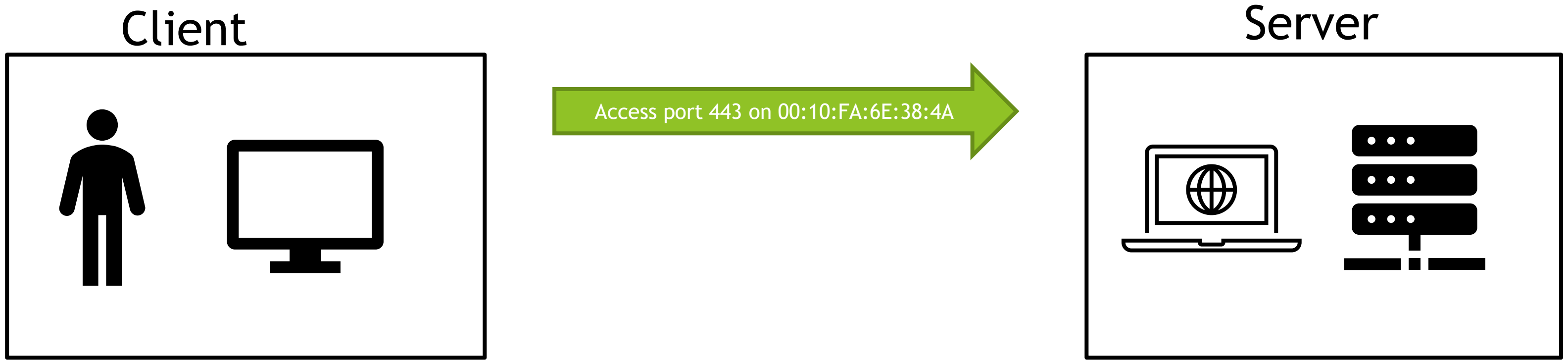
ARP



- ARP – Address Resolution Protocol translates the IP address into the MAC address needed for system-to-system communications on a local network.

TCP/IP Network Communications

Port Numbers

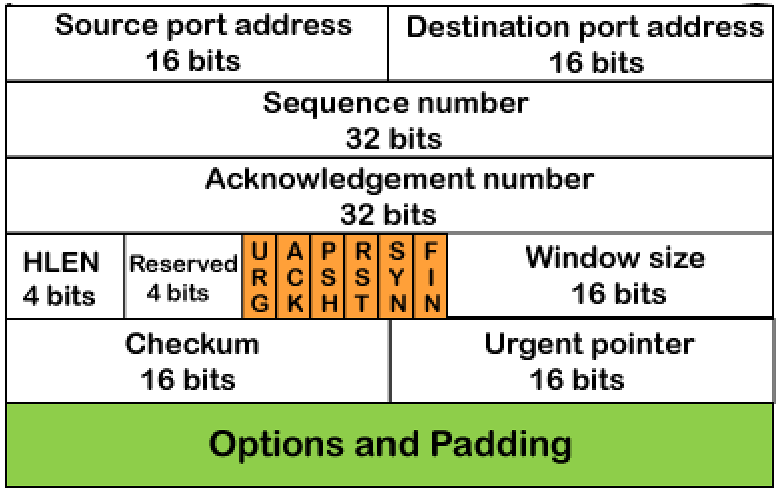


- Ports – Systems can establish communications with multiple systems and host multiple services. Port numbers are used to identify specific services and communication pathways.

TCP/IP Network Communications

TCP

- TCP – Protocol that offers session-oriented, acknowledged, reliable communication



<table>
<tr><td colspan="4">Source port address
16 bits</td><td colspan="5">Destination port address
16 bits</td></tr>
<tr><td colspan="9">Sequence number
32 bits</td></tr>
<tr><td colspan="9">Acknowledgement number
32 bits</td></tr>
<tr><td>HLEN
4 bits</td><td>Reserved
4 bits</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>Window size
16 bits</td></tr>
<tr><td colspan="4">Checkum
16 bits</td><td colspan="5">Urgent pointer
16 bits</td></tr>
<tr><td colspan="9">Options and Padding</td></tr>
</table>

TCP/IP Network Communications

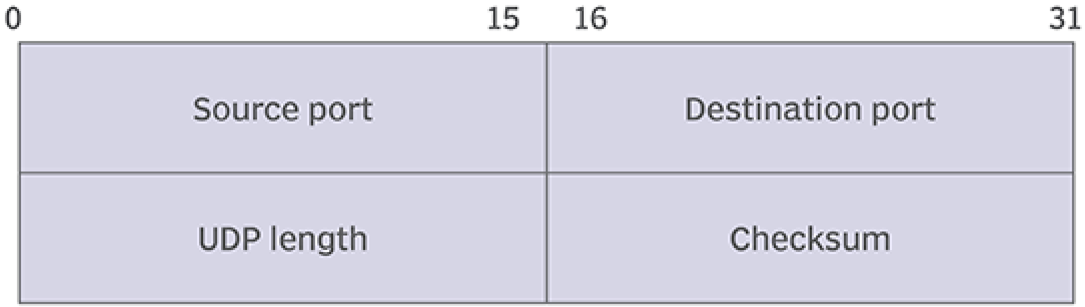
Flags

- TCP flags are used to communicate the state of the connection
  - SYN – Sync (Start)
  - ACK – Acknowledge
  - FIN – Finish
  - RST – Reset
  - PSH – Process data without delay
  - UGT – Urgent data

TCP/IP Network Communications

UDP

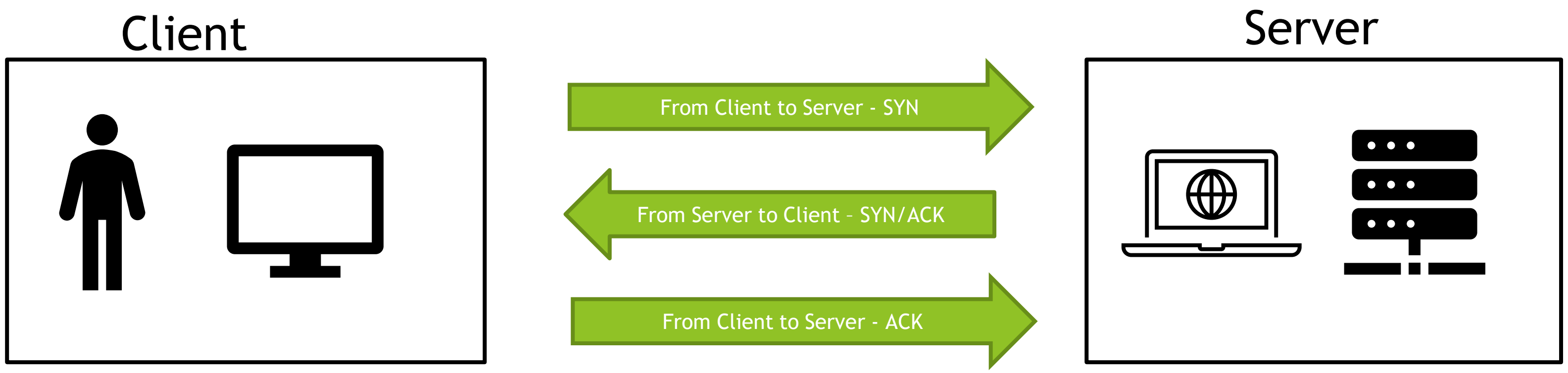
- UDP – Alternate to TCP that offers simpler unacknowledged communication



0 15	16 31
Source port	Destination port
UDP length	Checksum

TCP/IP Network Communications

TCP Three Way Handshake


Client
Server
From Client to Server - SYN
From Server to Client - SYN/ACK
From Client to Server - ACK

- The client sends a packet to the server with the SYN (synchronize) flag set indicating that it wants to establish a connection.
- The server responds to the client with a packet containing the SYN and ACK (acknowledge) flags set indicating that it acknowledges the client and wishes to establish a connection.
- The client sends a packet back to the server with the ACK flag set indicating that it acknowledges the server.

TCP/IP Network Communications

ICMP

- ICMP (Internet Control Message Protocol) – A support protocol designed to allow devices to communicate regarding issues such as router or general system reachability.
  - ICMP Echo Request/Reply– Also known as a ping this communications is designed to determine if a system is reachable
    - A small data packet (echo request) is sent from the source to the destination and the destination then responds (echo reply)
  - ICMP Timestamp Request/Reply – A request for a timestamp so that time synchronization can be achieved

Nmap Host Discovery

Warning

- nmap can DAMAGE or DISABLE network systems and equipment, use with CAUTION!!

Nmap Host Discovery

Basics

- Basic use: nmap host(s)
  - Examples:
    - nmap 192.168.1.1
    - nmap 192.168.1.0/24
    - nmap 192.168.1.1-254
    - nmap www.domainname.com

Nmap Host Discovery

Options

Basic use: nmap option host(s)

Option	Explanation
-sn	No port scan, host discovery only
-Pn	No host discovery
-PR	ARP Scan - Only works if target is on same LAN as source
-PS	Perform a TCP SYN scan on port 80
-PA	Perform a TCP ACK scan on port 80 (Note: Superuser only) - Some firewalls block incoming SYN but not ACK
-PU	Perform a UDP scan on port 40125 - May generate ICMP unreachable if port is closed - If port is not closed responses vary

Nmap Port Mapping

Options

Basic use: nmap option host(s)

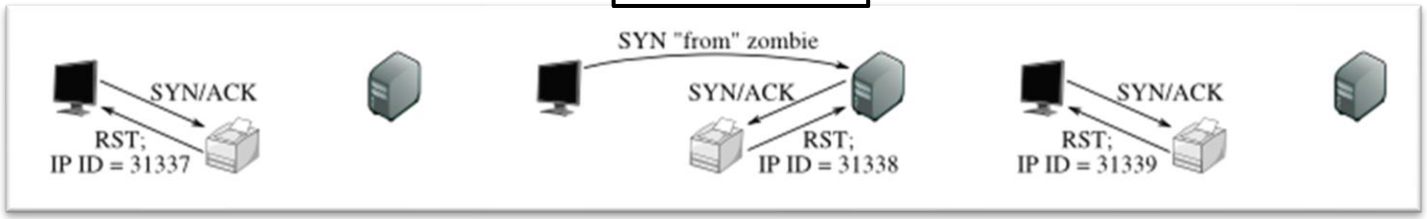
Option	Explanation
-p port_num	Scan port port_num - Use – (-p-) to scan all ports
-sS	Stealth Scan (Note: Superuser only) - SYN->SYN/ACK->RST
-sT	Performs full handshake
-sU	Perform a UDP scan
-sF –sN -sX	FIN scan, NULL scan and an Xmas scan - TCP rules state that RST should be sent if port is closed, and invalid flag(s) are present

Nmap Port Mapping

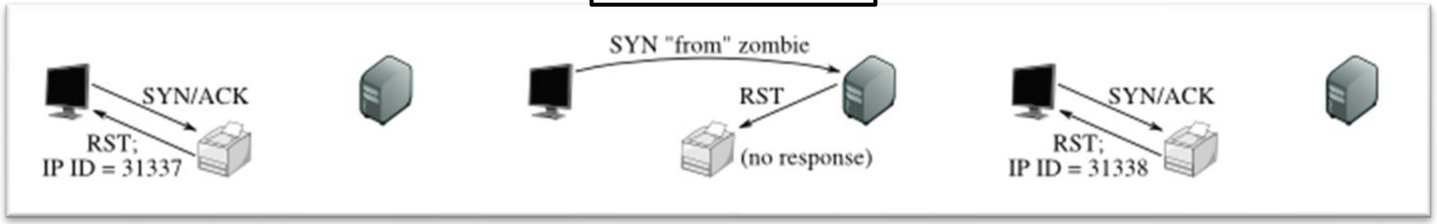
Idle Scan

- An Idle scan (-sI) can perform a blind, difficult to trace port mapping

Open Port



Closed Port



Nmap Port Mapping

Port Status

Basic use: nmap option host(s)

State	Explanation
Open	Port is open
Closed	Port is closed
Filtered	A firewall is blocking the port
Unfiltered	A firewall is not blocking the port
Open | Filtered	The port is either open or filtered
Closed | Filtered	The port is either closed or filtered

Nmap Port Mapping

Timing

Basic use: nmap option host(s)

Option	Explanation
-T0	Paranoid – 5 minute delay
-T1	Sneaky – 15 second delay
-T2	Polite – .4 second delay
-T3	Normal
-T4	Aggressive – 10 ms delay
-T5	Insane – 5 ms delay
--max-hostgroup --min-hostgroup	Maximum or minimum number of hosts to scan in parallel
--max-parallelism --min-parallelism	Maximum or minimum number of probes to perform in parallel

Nmap Target Identification

- Using the –A switch will tell nmap to attempt to identify the specific programs and operating system in use by the target
  - Will also attempt to identify version numbers
  - Uses techniques such as header signatures and banner grabbing
  - Very noisy
- Nmap also supports scripting to allow even more complex version detection or vulnerability scanning

Export Nmap Results

Option	Explanation
-oN filename	Export data to a text file
-oG filename	Export data to a text file in grepable (searchable) format
-oX filename	Export data as an XML file

Summary

- Describe TCP/IP Network Communications.
- Discuss Nmap Host Discovery.
- Discuss Nmap Port Mapping.
- Discuss Using Nmap to Identify Target Service and Operating System Data.
- Use Nmap to Perform Network Mapping.

For More Information

- For further information go to https://www.nl.northweststate.edu/camo or contact:
  - Tony Hills – thills@northweststate.edu – 419-267-1354
  - Mike Kwiatkowski – mkwiatkowski@northweststate.edu – 419-267-1231

Made possible through support from the National Science Foundation (NSF) award number 1800929