

Air Force Association's CyberPatriot

The National High School Cyber Defense Competition



Network Fundamentals

Module 6





Objectives

- Identify Common Network Devices
- Define Protocols
- Fundamentals of DNS
- Network Configuration Tools



Common Network Devices

- Network Interface Card (NIC)
 - Allows computer to talk to a network
- Hub
 - Allows multiple network devices to connect. A signal comes in one port and is transmitted to all other ports.
- Switch
 - Allows multiple network devices to connect, but does not distribute signals without verifying whether it really needs to propagate to a given port or ports





Common Network Devices

- **Wireless Access Point (WAP)**
 - Allows users to connect to a network without 'wires'
 - RF signals are used to communicate instead of physical wires
 - Wireless access standards are broadly divided into 802.11a, 802.11b, and 802.11g
- **Router**
 - Forwards data packets between networks; used to connect different networks and transfer packets between them
- **Gateway**
 - Used to connect two different types of networks
- **Modem**
 - Translates digital signals from a computer into analog signals



Protocols

- Protocols

- A set of rules that governs the communications between computers on a network
- Not hardware (cable, routers, etc.); rather what makes all the hardware function together and allows it communicate

- Internet Protocol (IP)

- A set of related network protocols (TCP, UDP, HTTP, FTP, ARP, ICMP) used to move data around the Internet and other networks

- Protocols allow the following to occur

- Streaming video or music online (UDP)
- Changes www.google.com to 74.125.45.99 (DNS)
- Safely perform transactions online (SSL)
- Chat online (IRC)





Protocols

- TCP/IP – Transmission Control Protocol/Internet Protocol
 - Most commonly used protocol for Internet communication
- IP Addressing
 - The IP address uniquely identifies computers on a TCP/IP network
 - Every “node” (client, server, router) on a network has to have a unique IP address (192.168.1.15 for example)
- UDP - User Datagram Protocol
 - A connectionless service
 - Main alternative to TCP
- DNS - Domain Name System
 - Translates network address (such as IP addresses) into terms understood by humans (such as Domain Names) and vice-versa



Protocols

- DHCP - Dynamic Host Configuration Protocol
 - Can automatically assign Internet addresses to computers and users
- FTP - File Transfer Protocol
 - A protocol that is used to transfer and manipulate files over the network
- HTTP - HyperText Transfer Protocol
 - An Internet-based protocol for sending and receiving web pages
- HTTPS - HyperText Transfer Protocol Secure
 - An Internet-based protocol for sending and receiving WebPages securely
- IMAP - Internet Message Access Protocol
 - A protocol for e-mail messages on the Internet





Protocols

- IRC - Internet Relay Chat
 - A protocol used for Internet chat and other communications
- POP3 - Post Office protocol Version 3
 - A protocol used by e-mail clients to retrieve messages from remote servers
- SMTP - Simple Mail Transfer Protocol
 - A protocol for e-mail messages on the Internet
- ARP – Address Resolution Protocol
 - Converts an IP address to its corresponding physical network address





Protocols

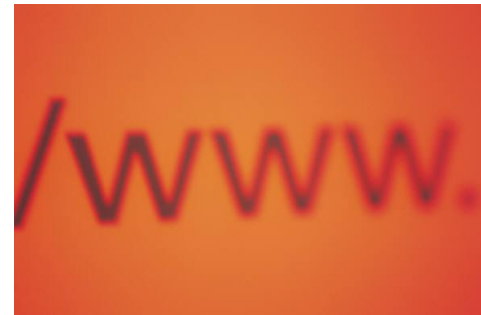
- **SNMP - Simple Network Management Protocol**
 - A standard TCP/IP protocol used to monitor and map network availability, performance, and error rates
- **Telnet**
 - A remote terminal access protocol
- **SSH – Secure Shell**
 - A secure remote terminal access protocol
- **SSL - Secure Sockets Layer**
 - A security protocol to enable Web sites to pass sensitive information securely in an encrypted format
- **LDAP - Lightweight Directory Access Protocol**
 - A network protocol and a standard architecture for organizing the directory data





TCP

- Most communications are handled using TCP
- TCP is reliable
 - Acknowledgements indicate delivery of data
 - Checksums are used to detect corrupted data
 - Sequence numbers detect missing, or mis-sequenced data
 - Corrupted data is retransmitted after a timeout
 - Mis-sequenced data is re-sequenced
 - Flow control prevents over-run of receiver
 - Uses *congestion control* to share network capacity among users
 - TCP is *connection-oriented*
- Commonly used for
 - World Wide Web
 - E-mail
 - File transfer





UDP

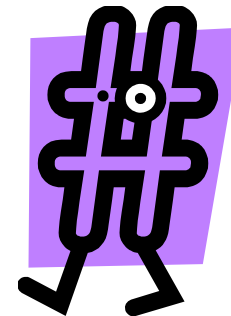
- UDP is not reliable
 - Not guaranteed that packets will be received
 - No acknowledgements to indicate delivery of data
 - Data may arrive out of sequence
 - Data may be duplicate or go missing
 - Congestion of data is common
 - Checksums are used to detect tampering or corruption
- Commonly used for
 - Streaming music or video
 - Voice over IP (VoIP)
 - Gaming
 - DNS





File Integrity

- Network data transmissions often produce errors, such as toggled, missing or duplicated bits
 - The data received might not be identical to the data transmitted
- Checksums are used
 - Ensures the integrity of data portions for data transmission or storage
- Hash functions
 - A hash value is generated for each given message
 - Used for data comparison and detecting duplicated data
 - Commonly used to check data integrity





File Integrity

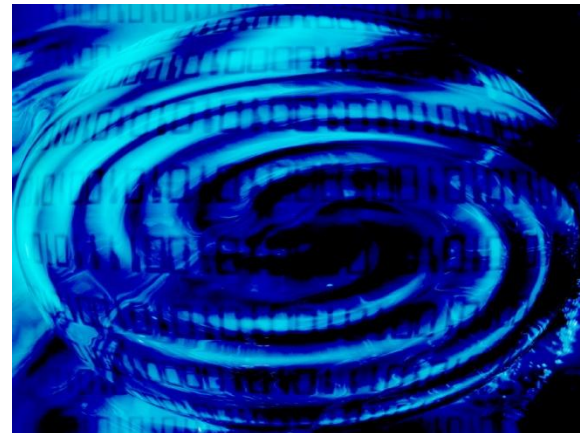
- Md5
 - A command line utility usable on either Unix or MS-DOS/Windows which generates and verifies message digests using the MD5 algorithm
 - Security has been compromised as an encryption protocol, however, used mostly to provide some assurance that a transferred file has arrived intact and uncorrupted
 - How to use md5
 - http://www.openoffice.org/dev_docs/using_md5sums.html





Ports

- Port
 - A virtual connection point that allows software applications to share hardware resources without interfering with each other
 - Computers and routers automatically manage network traffic traveling via their virtual ports
 - Used in protocols to name the ends of logical connections which carry long term conversations
- Well known (privileged) ports
 - 1-1023
- Registered ports
 - 1024-49151
- Dynamic or private ports
 - 49152-65535





CommonPorts

- A service contact port is defined for providing services to unknown callers
- These are common ports that are easily targeted
 - TCP port 21 - FTP (File Transfer Protocol)
 - TCP port 23 - Telnet
 - TCP port 25 - SMTP (Simple Mail Transfer Protocol)
 - TCP and UDP port 53 - DNS (Domain Name System)
 - TCP ports 80 and 443 - HTTP (Hypertext Transport Protocol) and HTTPS (HTTP over SSL)
 - TCP port 110 - POP3 (Post Office Protocol version 3)
 - TCP and UDP port 135 – Windows RPC
 - TCP and UDP ports 137–139 - Windows NetBIOS over TCP/IP
- On a Unix/Linux system, ports and associated service names are listed in the /etc/services file
- For a complete list of ports and services, see <http://packetlife.net/media/library/23/common-ports.pdf>

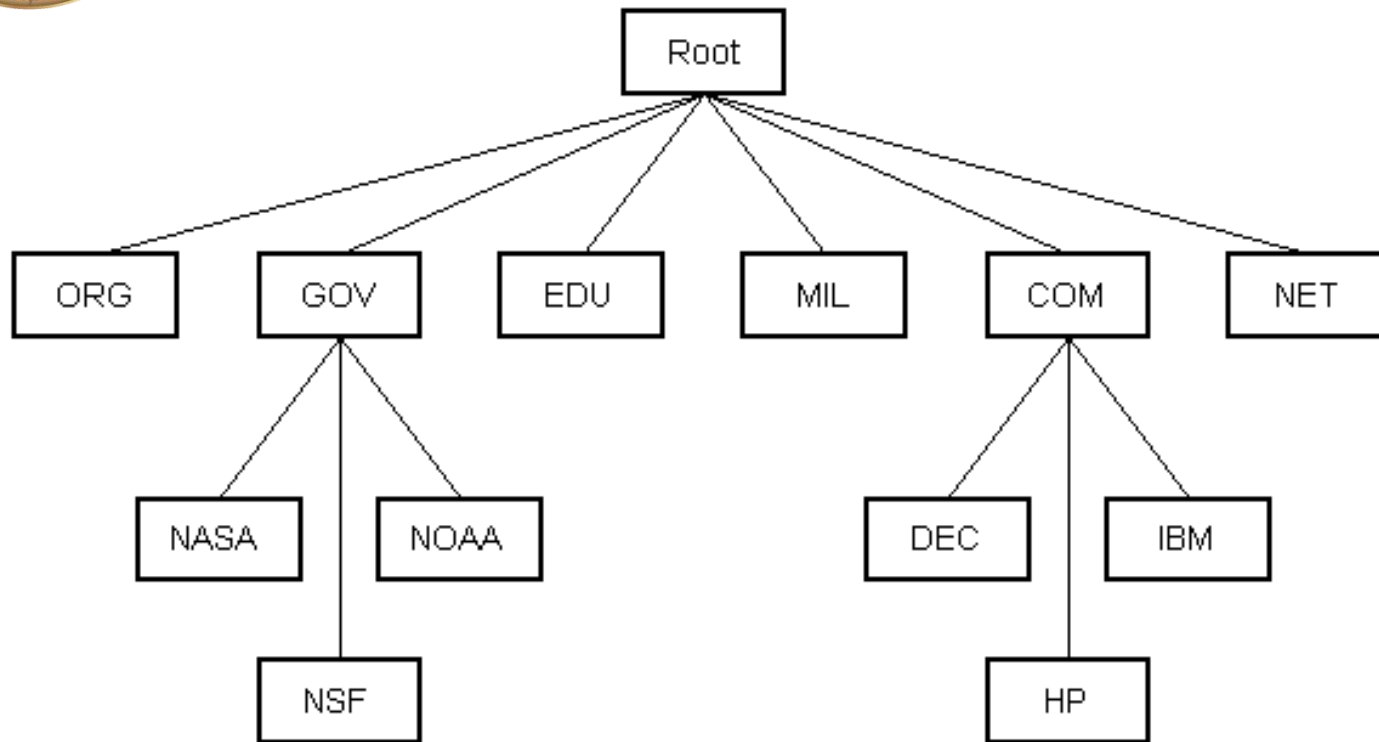


DNS

- Domain Name System (DNS)
 - Associates information with domain names
 - It translates human-readable computer hostnames (e.g., *ww.wikipedia.org*) into the IP address
 - Requests and responses are normally sent as UDP packets (to port 53)
- DNS is a distributed database: parts of the tree (called "zones") are held in different servers
 - DNS servers do not contain the entire database, but rather a subset
- Each zone has two or more authoritative nameservers
 - These authoritative DNS servers publish information about that domain and the nameservers of any domains "beneath" it
(See next slide for illustration)
- Every caching nameserver is seeded with a list of root servers
- Currently there are only 13 root servers



DNS



DNS is structured as a hierarchy similar to the IP routing hierarchy. The computer requesting a name resolution will be re-directed 'up' the hierarchy until a DNS server is found that can resolve the domain name in the request.

Tools



- Nslookup
 - Tool used to query DNS for a domain name or IP address
- At a command line, type 'nslookup <hostname>' and hit enter.

```
C:\Users\mel>nslookup utsa.edu
Server:    clinton1604.utsarr.net
Address:   129.115.102.165

Non-authoritative answer:
Name:      utsa.edu
Address:   129.115.102.107
```



- Whois

- Command returns information about a domain name or IP address such as domain name, registrant, contacts, nameservers, and domain name dates (i.e., activation, expiration)
- To perform a Whois search online go to <http://www.internic.net/whois.html>

Domain Name: UTSA.EDU

Registrant:

University of Texas at San Antonio
6900 North Loop 1604 West
San Antonio, TX 78249
UNITED STATES

Name Servers:

JULIET.IT.UTSA.EDU	129.115.102.150
BERRY.IT.UTSA.EDU	129.115.102.151

Domain record activated: 14-Dec-1990

Domain record last updated: 29-Jun-2011

Domain expires: 31-Jul-2012



- Traceroute
 - Command that shows the path a network packet takes from origination to destination
- The command displays how many 'hops' from router to router it takes for the packet to reach its destination
- Also displayed are the addresses of each router and the time it takes for a packet to go from router to router
- If a router is not reachable, you will see a request timeout
- In UNIX machines the command is 'traceroute', in MS Windows machines it is called 'tracert'.
 - This command is not always effective as many sites block ICMP to minimize DDoS issues
- The next slide shows an example of running the command



Tools

- Traceroute
 - See results for 'tracert www.yahoo.com'

```
C:\Users\mel>tracert www.yahoo.com

Tracing route to any-fp3-real.wa1.b.yahoo.com [209.191.122.70]
over a maximum of 30 hops:

  1      1 ms      1 ms      1 ms      rrcs-24-173-46-81.sw.biz.rr.com [24.173.46.81]
  2      2 ms      2 ms      2 ms      rrcs-24-73-242-153.sw.biz.rr.com [24.73.242.153]

  3      6 ms      *          6 ms      24.73.242.30
  4      *          6 ms      6 ms      gig3-0-0.snantx5000-m-rtr01.texas.rr.com [24.93.
60.144]
  5      7 ms      6 ms      7 ms      gig2-0-1.hstntxl3-pe-rtr01.texas.rr.com [24.93.3
5.22]
  6      7 ms      6 ms      7 ms      gig3-0-1.hstntxl3-p-rtr01.texas.rr.com [24.93.35
.20]
  7     14 ms     12 ms     10 ms     gig4-2-0.hstntxl3-rtr1.texas.rr.com [24.93.60.66
]
  8      6 ms     12 ms      6 ms      ae-4-0.cr0.hou30.tbone.rr.com [66.109.6.54]
  9     11 ms     11 ms     10 ms     107.14.17.141
 10     13 ms     10 ms     10 ms     66.109.9.191
 11     11 ms     12 ms     11 ms     ae-1-d111.msr2.mud.yahoo.com [216.115.104.103]
 12     11 ms     11 ms     11 ms     te-8-1.fab2-a-gdc.mud.yahoo.com [209.191.78.141]

 13     28 ms     11 ms     12 ms     te-8-2.bas-c1.mud.yahoo.com [209.191.78.173]
 14     11 ms     11 ms     11 ms     ir1.fp.vip.mud.yahoo.com [209.191.122.70]

Trace complete.
```



- Netstat

- A tool for checking network configuration and activity such as
 - All connections including what protocol and its current state
 - Display contents of the IP Routing table
 - Network interface statistics
- Displays different information by using different parameters or 'flags' with the command (e.g., 'netstat -a')

Note: Windows and Unix have different 'flags' and options available

- For Windows XP

- <http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/netstat.mspx?mfr=true>

- For Linux

- <http://tldp.org/LDP/nag2/x-087-2-iface.netstat.html>
- <http://www.thegeekstuff.com/2010/03/netstat-command-examples/>



Tools

- Netstat
 - Display all connections and current state using 'netstat -a'
 - (Windows XP)

```
C:\Users\mel> netstat -a
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	TRN44:0	LISTENING
TCP	0.0.0.0:445	TRN44:0	LISTENING
TCP	0.0.0.0:912	TRN44:0	LISTENING
TCP	0.0.0.0:17972	TRN44:0	LISTENING
TCP	0.0.0.0:49152	TRN44:0	LISTENING
TCP	0.0.0.0:49153	TRN44:0	LISTENING
TCP	0.0.0.0:49154	TRN44:0	LISTENING
TCP	0.0.0.0:49157	TRN44:0	LISTENING
TCP	0.0.0.0:49158	TRN44:0	LISTENING
TCP	0.0.0.0:57621	TRN44:0	LISTENING
TCP	127.0.0.1:4370	TRN44:0	LISTENING
TCP	127.0.0.1:4380	TRN44:0	LISTENING
TCP	127.0.0.1:5354	TRN44:0	LISTENING
TCP	127.0.0.1:5354	TRN44:49155	ESTABLISHED
TCP	127.0.0.1:27015	TRN44:0	LISTENING
TCP	127.0.0.1:27015	TRN44:49164	ESTABLISHED



- Netstat
 - Display contents of the IP Routing table using 'netstat -r '
 - (Linux)

```
# netstat -r
Kernel IP routing table
Destination      Gateway          Genmask          Flags      MSS Window  irtt  Iface
192.168.1.0      *               255.255.255.0    U          0  0        0  eth2
link-local       *               255.255.0.0      U          0  0        0  eth2
default          192.168.1.1     0.0.0.0          UG         0  0        0  eth2
```

<http://www.thegeekstuff.com/2010/03/netstat-command-examples/>



Tools

- Netstat

- Display interface statistics using 'netstat -i)
- Linux only

```
# netstat -i
Kernel Interface table
```

Iface	MTU	Met	RX-OK	RX-ERR	RX-DRP	RX-OVR	TX-OK	TX-ERR	TX-DRP	TX-OVR	Flg
eth0	1500	0	0	0	0	0	0	0	0	0	BMU
eth2	1500	0	26196	0	0	0	26883	6	0	0	BMRU
lo	16436	0	4	0	0	0	4	0	0	0	LRU

- The RX and TX columns show how many packets have been received or transmitted error-free (RX-OK/TX-OK) or damaged (RX-ERR/TX-ERR); how many were dropped (RX-DRP/TX-DRP); and how many were lost because of an overrun (RX-OVR/TX-OVR)
- The last column shows the flags that have been set for this interface



Patching

- Snort
 - An open source network intrusion prevention and detection system (IDS/IPS)
 - Can be configured in three main modes
 - Sniffer
 - Will read and display network packets
 - Packet logger
 - Records packets to disk
 - Network intrusion detection
 - Monitor and analyze network traffic according to a previously defined ruleset
 - Perform defined action based on what it found
 - Download at <http://www.snort.org/snort-downloads>
 - The Snort Manual - http://www.snort.org/assets/166/snort_manual.pdf

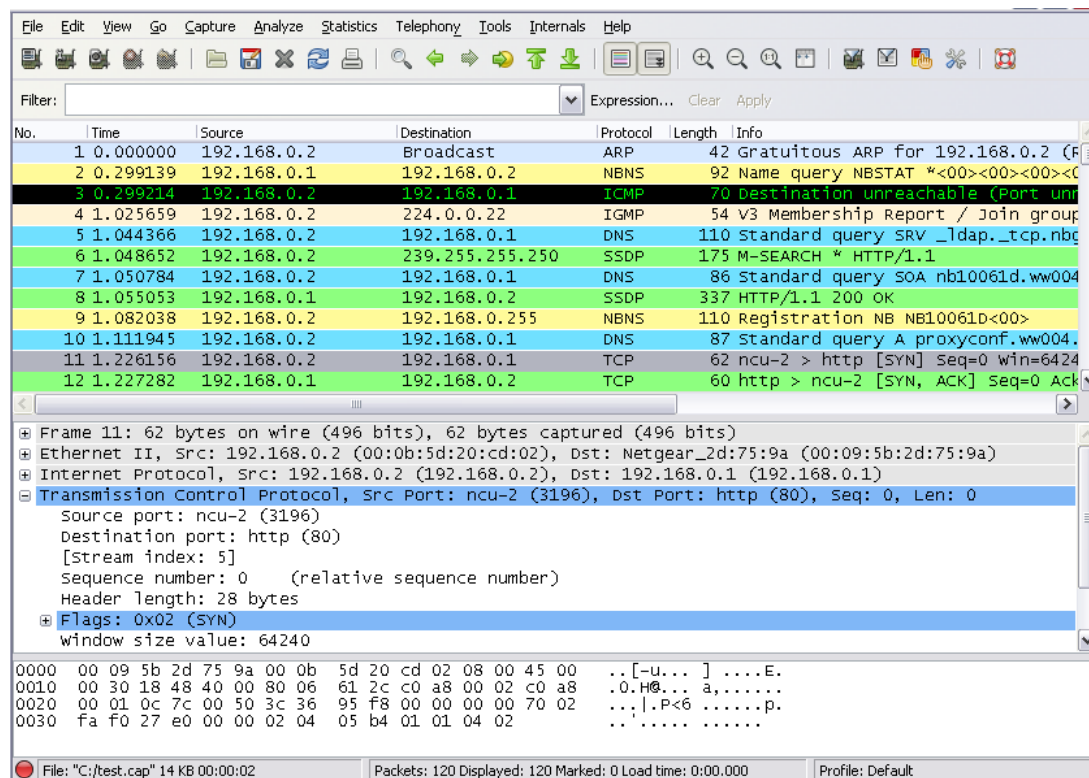


- Wireshark
 - A network packet analyzer that captures packets and displays that packet data for easier examination
 - Can be used to
 - Troubleshoot network problems
 - Examine security problems
 - Debug protocol implementations
 - Import and export packet data
 - Filter packets based on criteria
 - Makes it easy to differentiate protocols, traffic, etc. by color coding on screen
 - Download at <http://www.wireshark.org/download.html>
 - User guides and presentations at <http://www.wireshark.org/docs/>



Tools

- Screenshot of packets being captured using Wireshark
 - For more details, see http://www.wireshark.org/docs/wsug_html_chunked/ChUseMainWindowSection.html





Summary

- Identified common network devices
- Defined protocols
- Discussed the fundamentals of DNS
- Introduced some free network configuration tools



References

- http://www.starlancs.com/EducateMe/educate_network_devices.html
- <http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ap1.htm>
- http://www.theshulers.com/whitepapers/internet_whitepaper/index.html#http
- <http://fcit.usf.edu/network/chap2/chap2.htm>
- <http://www.comptechdoc.org/independent/networking/cert/netterms.html>
- <http://packetlife.net/media/library/23/common-ports.pdf>
- http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/3/html/Security_Guide/ch-ports.html
- <http://www.mediacollege.com/internet/troubleshooter/traceroute.html>
- <http://www.thegeekstuff.com/2010/03/netstat-command-examples>
- <http://www.wireshark.org/download.html>
- <http://www.wireshark.org/docs/>
- <http://www.snort.org/snort-downloads>
- http://www.openoffice.org/dev_docs/using_md5sums.html