A. The Internet, TCP/IP, and LANs
B. Ping sweeps, port scans, traceroutes, & OS fingerprinting
C. An introduction to security issues
   a. Attack Points
      – *Human access*
      – *Physical access*
      – *LAN access*
      – *Wireless access*
      – *Remote (Internet) access*
   b. Scanning your site
   c. The law
The Anatomy of an Attack

**Introductory Labs**

- **Lab #1**: Survey the University of the Pacific
- **Lab #2**: Survey Dave, UOP’s IT security officer
- **Lab #3**: Use Nmap to ping sweep/port scan your own computer (or the lab’s LAN)
- **Lab #4**: Use Nbtenum to capture user data from your own computer (or from the lab’s LAN)
- **Lab #5**: Use SAMInside to capture your own password hashes. Use SamInside and John to crack the passwords
- **Lab #6**: Use Nessus to vulnerability test your own computer (or the lab’s LAN)
- **Lab #7**: Use Ethereal to capture packets on the lab’s LAN
The Internet Infrastructure
The Internet, TCP/IP, and LANs

Traceroute to Finland

24 Hops (Routers)

Traceroute counts routers.
Each router is a “hop.”
The Internet, TCP/IP, and LANs

Traceroute to Pakistan

16 Hops (Routers)
Everything you must absolutely positively know about TCP/IP

TCP = Transport Control Protocol
IP = Internet Protocol

TCP and IP control the vast majority of traffic that moves over the Internet!

What is a protocol?
Compare meeting someone! Using the telephone!
Internet Addressing - it’s all about:

**IP Addresses and Port Numbers**

- **IP Address**: Identifies your network and your computer. Every computer that uses the Internet must have a unique IP address.

- **Port Number**: Identifies your application (or “service”). Every application (e.g. browser, email) that uses the Internet must have a port number.

- **COMPARE**: It’s like a Post Office that delivers only post cards. All messages are broken up into numbered post cards (packets), each sent to an address (IP address) and a person at that address (port number). Every packet is labeled with a **TO & FROM** IP address and **TO & FROM** port number.
IP Addresses - Identify networks and computers

- IPv4 (version 4) is by far the most used (IPv6 is next).
- IPv4 addresses are 32 bits long (four 8-bit bytes).
  - Therefore, the Internet can accommodate up to $2^{32}$ (4,294,967,296) IP addresses (not enough).
- They are displayed in 4-byte “dotted decimal” form.
- Addresses range from 0.0.0.0 to 255.255.255.255.
  - In decimal, a byte ranges from 0 to 255 (11111111)
- Therefore, the IP address 192.200.5.130 is really:
  1100 0000 1100 1000 0000 0101 1000 0010
  (spaces added for clarity)
- They are part network address, part computer address.
- Routers move packets based on their IP addresses.
  - *See next slide…*
The Internet, TCP/IP, and LANs

The Internet is a giant network of networks!

Routers move packets between networks.

Switches move packets (frames) within networks.
IPv4 Addresses

- Non-routable IP addresses
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255
  - Internet routers drop any packets addressed to these address spaces; therefore, we can use them in labs and LANs without fear of our packets “escaping” into the Internet

- Routable IP addresses
  - Every address that is not non-routable
Port Numbers – Identify applications (services)
Port numbers are 16 bits long.
- Therefore, a computer can accommodate up to $2^{16}$ (65,536) port numbers.
- They are always displayed in decimal form.
- Addresses range from 0 to 65,535.
- 0 to 1023 = server application port numbers.
  - See next slide…
- 1024 to 65,535 = client application port numbers.
- Client apps are browsers, email programs, etc.
- Therefore, the port number 80 (web site) is really:
  0000 0000 0101 0000
  (spaces added for clarity)
Server application port numbers (0 to 1023)
- 21 – ftp (file transfer protocol)
- 22 – ssh (secure shell)
- 23 – telnet (remote login)
- 25 – smtp (simple mail transport protocol)
- 53 – dns (domain name service)
- 69 – tftp (trivial file transfer protocol)
- 80 – http (hypertext transfer protocol - web pages)
- 110 – pop3 (post office protocol)
- 135, 139, 445 – netbios (network basic input output system - printer/file sharing)
- 443 – https (encrypted web pages; s = secure)

Server apps are web servers, email servers, etc.
Servers “listen,” clients connect, then the two “talk.”
Use `netstat -an` to find out what ports are open on your machine (a = all, n = numbers only = do not determine the services associated with port numbers).

You’re listening, so you’re a server.
Most Microsoft LAN exploits take advantage of the following protocols in some way:

- **NetBIOS (TCP Ports 137, 138, 139)** – used for Windows networking to connect clients to file and print servers. Should never be allowed through the Firewall except through an encrypted tunnel (as in a VPN).

- **RPC Locator (TCP Port 135)** – used by Windows networking to locate network services that use the RPC protocol. Should never be allowed through the Firewall.
One more address you need to know about – the LAN address

- Every NIC (Network Interface Card) has a **unique** address called the **MAC** (Media Access Control) address.
- MAC vs. IP: It’s like a housing community that delivers mail based on lot number vs. the world-based postal address.
- MAC addresses (48 bits) are given in **hexadecimal**.
  Hexadecimal represents binary numbers in 4-bit groups:

  0000 = 0 0100 = 4 1000 = 8 1100 = C
  0001 = 1 0101 = 5 1001 = 9 1101 = D
  0010 = 2 0110 = 6 1010 = A 1110 = E
  0011 = 3 0111 = 7 1011 = B 1111 = F

- An example MAC address is: 00–0E–35–56–60–FA
  = 0000 0000 0000 1110 0011 0101 0101 0110 0110 0000 1111 1010
- The first 24 bits (00–0E–35) identifies the manufacturer.
  The second 24 bits (56–60–FA) represents the NIC card.
- **Switches move packets based on their MAC addresses.**
  - See next slide…
The final word on addresses!

- **Every computer** connected to the Internet must have a unique **IP address**.
  - For example, every website’s URL must map to a unique (to the Internet) IP address.
  - DNS performs this mapping - *See next slide*.

- **Every program** that communicates over the Internet must have a unique (to the computer) **port number**.
  - Most services (web, email, etc.) have an assigned port number (web servers use port 80).

- **Every computer** on a LAN (whether the LAN is connected to the Internet or not) must have a unique **MAC address**.
The Internet is a giant network of networks!

**Routers** move packets between networks – they read IP addresses.

**Switches** move packets (frames) within networks – they read MAC addresses.
The Internet, TCP/IP, and LANs

- **DNS** - Domain Name Service
  - Converts **URLs** (e.g. www.uop.edu) into **IP addresses**
  - Browsers request the conversion from DNS servers
- DNS servers query each other to resolve names into addresses
- To lower traffic requirements, DNS servers cache answers

![Diagram showing the DNS resolution process]

**Resolve:**
www.uop.edu

- **Client**
- **Local NS**
  - Configured with all 13 Root NS IP addresses
- **Root NS**
  - Each root NS stores IP addresses of 100s of TLD NSs
- **TLD NS**
  - Top Level Domain name servers, e.g. .com, .edu, .net
- **Company NS**
  - Local authoritative name servers, e.g. cs.uop.edu
DNS – Domain Name Service

- Converts the URL (Uniform Resource Locator) you type into a browser’s **Address** field into an IP address
- This is the DOS *traceroute* command – *More on it in later…*

The tracert program made a DNS request!
**The Internet, TCP/IP, and LANs**

**ARP – Address Resolution Protocol**

- Similar to the way DNS (Domain Name Service) maps URLs (Uniform Resource Locator) to IP addresses, ARP maps IP addresses to LAN MAC addresses.

- Browsers need IP addresses (e.g. 64.233.161.99), not URLs (e.g. www.google.com) to connect to a website.

  \[ \text{www.google.com} = 64.233.161.99 \]

- Ethernet LAN applications need MAC addresses, not IP addresses, to connect to a computer on a LAN.

  - MAC vs. IP: It’s like a housing community that delivers mail based on lot number vs. the world-based postal address.

- Often, however, the application knows only the IP address of the destination. **Solution**: ARP

  \[ 192.168.0.23 = 00-0E-35-56-60-FA \] -- *See next slide…*

- This will be an important concept later, when we talk about ARP cache poisoning!
The Internet, TCP/IP, and LANs

ARP – Address Resolution Protocol

- In DOS, to view (all of) the ARP cache, enter:
  \texttt{arp \ -a}

\begin{verbatim}
C:\> arp -a
Interface: 192.168.1.100 --- 0x10004
          Internet Address Physical Address
  192.168.1.1          00-14-bf-ec-b2-6f
C:\>
\end{verbatim}

\begin{itemize}
\item IP address
\item MAC address = NIC address = Physical Address
\end{itemize}
The Internet is a giant network of networks!

**Packets** have IP addresses.

**Frames** have MAC addresses.

**ARP** returns a MAC address when sent an IP address.
Internet Sockets

- Networkers are always talking about sockets.
- Some define a socket as an IP address/Port number pair.
- A better definition is that it’s a “connection” between an application and the TCP/IP stack.
- In any event, at both ends of every Internet communications channel is a socket, through which two machines “talk” via the Internet.
- So, a socket is equivalent to a telephone, interfacing the user to the communications network.
- An attacker who “owns” a remote box, will have his attack code open a socket on the victim box. This socket connects to a socket on attacker’s box – or vice versa.
REMEMBER THIS!

1. **Nothing** moves over the Internet (or LAN or WAN) unless there is a connection through which it flows.

2. **All** connections start with a server listening
   - We call this an open port.

3. **Therefore, if a box has no open ports, it is invulnerable to a (direct) remote attack!** Well, sort of…
   - An attacker cannot connect to it - and can exploit it **only** via a vulnerability.
   - An attacker’s only options are (1) human access (e.g. send the human a Trojan email attachment or trick him into visiting your website) or (2) physical access.

4. If you are running a Peer-to-Peer service (AIM, ICQ, Napster, Kazaa, Morpheus, etc.), your computer **is** a server!

5. If you are running Windows, your computer is a server, but…
The Internet, TCP/IP, and LANs

- Packets travel the Internet
  - Every packet has 32-bit TO/FROM IP addresses
  - And TO/FROM port numbers

- Frames travel LANs
  - Every frame has 48-bit TO/FROM MAC addresses

ARP returns this when sent this

More on the TCP and IP headers in a minute....
Routers look at IP addresses.
Switches look at MAC addresses.
Computers look at port numbers.

Frames move within networks.
Packets move between networks.
Frame = packet + MAC header
Your "edge" router's address that the world sees could be a cable modem, a DSL modem, or a phone modem.
Use `ipconfig` to determine your LAN IP address, and the IP address of your “edge” router.

Your computer’s LAN IP address

Your “edge” router’s LAN IP address

Your ISP’s network

The INTERNET
Your ISP’s network

Your router’s LAN IP address
This ISP gives routable IP addresses
The Internet, TCP/IP, and LANs

The TCP/IP Protocol Stack

Application (IE, etc.)
Transport (TCP, UDP)
Network (IP)
Data Link (Ethernet)

Port number
IP address
MAC address
MAC = Media Access Control

Data
Segment
Packet
Frame
Physical Layer (the cable)