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
How Others Scan You!
What the Bad Guys Can Find Out

Others can scan **YOU** remotely. More on this in your homework (www.grc.com). To determine your local (LAN) IP address, use `ipconfig` if you’re using Windows, `ifconfig` if you’re using Linux.

Your LAN IP address

Your “edge router” – a cable or DSL modem
What the Bad Guys Can Find Out

Use `netstat -an` to find out what ports are open on your machine (a = all, n = numbers only). Look for “Established” and “Listening.”

```
C:\Documents and Settings\Name>netstat -an

Active Connections

Proto  Local Address        Foreign Address         State
TCP    10.33.18.127:139    0.0.0.0:0             LISTENING
TCP    10.33.18.127:1107   64.233.161.99:80      ESTABLISHED
TCP    127.0.0.1:1026      0.0.0.0:0             LISTENING
TCP    127.0.0.1:1241      0.0.0.0:0             LISTENING
TCP    127.0.0.1:1242      0.0.0.0:0             LISTENING

“There’s no place like 127.0.0.1.”
```
A normal netstat output...

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>0.0.0.0:135</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:445</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:2869</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>127.0.0.1:1028</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>127.0.0.1:1241</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>127.0.0.1:62514</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>192.168.1.100:139</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>192.168.1.100:9515</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>192.168.1.100:14749</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:445</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:500</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:1051</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:1200</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:1353</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:1359</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:4500</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>127.0.0.1:123</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>127.0.0.1:1900</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>127.0.0.1:2791</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>127.0.0.1:2974</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>127.0.0.1:2979</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>127.0.0.1:2993</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>127.0.0.1:62514</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>192.168.1.100:123</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>192.168.1.100:137</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>192.168.1.100:138</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>192.168.1.100:1900</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>192.168.1.100:13173</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>192.168.1.100:44537</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
</tbody>
</table>

A connection to my edge router

0.0.0.0 = NetBIOS
or no connection

UDP ports do not show “Listening,” etc., but they are

127.0.0.1 = home
(listening to myself)
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
      ✈ Still Here!
   c. The law
What the Bad Guys Can Find Out

Surveying networks with remote access: **Nmap**
- Voted #1 by White Hats!
- Ping sweeps, port scans, OS fingerprinting
- Works on wireless networks!
- A very useful tool with advanced scanning capabilities
- Download from [www.insecure.org/nmap](http://www.insecure.org/nmap)
Nmap plays with the 6 TCP flags.
What the Bad Guys Can Find Out

TCP Header

- 16-bit origin port number
- 16-bit destination port number
- 32-bit sequence number
- 32-bit acknowledgement number
- 4-bit length (Header)
  - 6-bit Reserved
  - URG, ACK, PSH, RST, SYN, FIN
- 16-bit window size
- 16-bit TCP checksum
- 16-bit urgent pointer
- Option fields (if any)
- Data (if any)
What the Bad Guys Can Find Out

Nmap options
usage: nmap [Scan Type(s)] [Options] <host or net #1… [#N]>
63 options!
Scan type options
- **-sP**  ✅ Scan with pings - Find “up” hosts, but do no port scanning
- **-sT**  ✅ Scan, full-connect TCP – not stealthy!
- **-sS**  ✅ Scan TCP SYN only – stealthy!
- **-sU**  ✅ Scan for open UDP ports
- **-sN, -sF, -sX**  ✅ no flags set, FIN flag set, all flags set
- **-p n-m** ✅ Scan ports n to m

Example: Scan ports 1 to 3389 on ten boxes
> nmap -p 1-3389 192.168.0.1-10
What the Bad Guys Can Find Out

More Nmap options

- `sV` ➔ Scan versions – Determine the particular service and, if possible, its version number
- `O` ➔ OS identification - use TCP/IP fingerprinting
- `P0` ➔ Don't ping hosts (some firewalls block pings)
- `v` ➔ Verbose. Use twice for greater effect (-vv)
- `h` ➔ Help, print the help menu
- `f` ➔ Fragment the scan packets, avoiding IDSs
- `g <port>` ➔ Spoof your (source) port - 53 is good because it looks like a DNS response!
- `S <IP>` ➔ Spoof your (source) IP address – but someone else gets the response!
More Nmap options

-D \( \Rightarrow \) Decoy scan - creates decoys (using spoofed IP addresses) along with your IP address - even if the target detects the scan, they are unlikely to know which IP is really scanning them and which are decoys

-sA \( \Rightarrow \) ACK scan - test firewall rule-bases - an ACK packet will always receive a RST packet in response, which does NOT tell you if the port is opened or closed. However, it does tell you if the packet got through the firewall, which is the goal of this scan.

More on the ACK (firewall) scans later…
More Nmap options

- `sI <spoofedIP_or_URL>` ➔ Idle scan - allows a completely blind scan (no packets sent to the target from your real IP) of a target - based on predictable IP fragment ID numbers (most OSs increment by 1 with each created packet); SYNPs the target while spoofing the source IP and then SYNPs the spoofed address to see if its IP ID has been incremented – if yes, a SYN/ACK was sent it by the target [the port is open!] so it must return a RST; if no, a RST was sent [the port is closed], which is ignored by the spoofed address.

  – Of course, an open (listening) port on the target returns a SYN-ACK in response to a SYN
  – The applicable RFC here dictates that a RST be returned when an unexpected SYN-ACK arrives (at the spoofed address), and RST packets are ignored

See http://www.insecure.org/nmap for more information.
**What the Bad Guys Can Find Out**

**Nmap scans**

- **-sP** ➙ Scan with pings only
  - Just reports what IP addresses are “up”
  - Uses ICMP (Internet Control Message Protocol)
  - Note: Some firewalls block pings

```bash
> nmap -sP 192.168.0.1-10
```
What the Bad Guys Can Find Out

**Nmap scans**

- `-sT` ➙ Completed-TCP scans
  - Uses the 3-way handshake, of course
  - Easily detected and **typically logged**

> nmap -sT -p 1-3389 192.168.0.1
Nmap scans

- `ss` SYN scans
  - Sends the SYN only
    - A returned SYN-ACK indicates an open port
  - Typically not logged – much less “noisy”
  - Faster than completed-TCP scans

```bash
> nmap -ss 192.168.0.1
```
What the Bad Guys Can Find Out

Of course…

You can see if a single box is up by simply pinging it

```
C:\>ping www.google.com

Pinging www.google.akadns.net [64.233.161.99] with 32 bytes of data:

Reply from 64.233.161.99:  bytes=32  time=8ms  TTL=248
Reply from 64.233.161.99:  bytes=32  time=7ms  TTL=248
Reply from 64.233.161.99:  bytes=32  time=7ms  TTL=248
Reply from 64.233.161.99:  bytes=32  time=7ms  TTL=248

Ping statistics for 64.233.161.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 8ms, Average = 7ms
```
What the Bad Guys Can Find Out

But you can use Nmap to ping sweep an entire network:

Scan with pings 10 boxes

```
C:\Tools\nmap>nmap -sP 192.168.0.1-10

Starting Nmap 4.03 (http://www.insecure.org/nmap) at 2006-05-30
Standard Time
Host 192.168.0.2 appears to be up.
MAC Address: 00:30:1B:B2:64:1A (Shuttle)
Host 192.168.0.3 appears to be up.
MAC Address: 00:30:1B:B2:64:1B (Shuttle)
Host 192.168.0.4 appears to be up.
MAC Address: 00:30:1B:B2:63:41 (Shuttle)
Host 192.168.0.5 appears to be up.
MAC Address: 00:30:1B:B2:6A:A7 (Shuttle)
Nmap finished: 10 IP addresses (4 hosts up) scanned in 13.479 seconds

C:\Tools\nmap>
```
What the Bad Guys Can Find Out

> nmap -O -p1-3389 192.168.0.2

Scan ports 1-3389

Scan this box

Attack these ports!

ID the OS
What the Bad Guys Can Find Out

> nmap -sV -p 1-111 192.168.0.2

Scan ports 1-11

Scan this box

ID the service version

C:\Tools\nmap>nmap -sV -p1-111 192.168.0.2

Starting Nmap 4.03 ( http://www.insecure.org/nmap ) at 2006-05-30
Standard Time
Interesting ports on 192.168.0.2:
(The 108 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE SERVICE VERSION
21/tcp open ftp vsftpd 2.0.4
22/tcp open ssh OpenSSH 4.3 (protocol 2.0)
111/tcp open rpcbind 2 (rpc #100000)
MAC Address: 00:30:1B:B2:64:1A (Shuttle)
Service Info: OS: Unix
Nmap finished: 1 IP address (1 host up) scanned in 19.348 seconds
C:\Tools\nmap>
Another Nmap command line example:

```
> nmap  -sS  -O  -P0  www.uop.edu
```

- `-sS = scan with SYN packets`
- `-O = OS fingerprint`
- `-P0 = Don’t ping (the border routers/firewalls of some secure networks will not pass a ping – without P0, Nmap will skip any IP address that does not respond to a ping)`
- `Nmap will do a DNS lookup when given a URL.`

- This will often scan well-locked down networks, including UOP’s.
What the Bad Guys Can Find Out

In the Nmap lab…
- Assume the target owns the IP address space: 192.168.0.2 to 192.168.0.199
- The only ports you are interested in are the server ports, 1 to 1023 (the standard server ports)

To find out who’s up…
Open a DOS window and Enter:
> cd c:\tools\nmap
> nmap -sP 192.168.0.2-199
  -sP = scan Pings (no port scanning yet)
  All you want right now are the server IP addresses
  Record addresses on the Server Info Sheets!
The command below does it all!
This speeds things up a lot: --max-retries 0
In your DOS window, enter:

```
> nmap --max-retries 0 -O -p 1-3389
192.168.0.1-10
```

-zero capital oh

You’re really only interested in ports 1-1023; however, one of the Windows servers is running Terminal Server, and it listens on port 3389.
Matrix Reloaded: Trinity uses Nmap to find a vulnerable SSH server. She then exploits the server using the SSH1 CRC32 exploit from 2001.
Nmap against Apple Computers

Nmap won’t find any open ports when scanning a client Apple box in a default configuration – not even when the firewall is OFF.

Due to the MAC address (first 3 bytes indicate the manufacturer), it knows the computer is an Apple.

However, Nmap cannot identify the specific OS.

C:\Tools\Nmap> nmap  -O  -p 1-5000 192.168.1.106
Starting Nmap 4.03 ( http://www.insecure.org/nmap ) at 2007-02-16 12:24 Pacific Standard Time
Warning:  OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 5000 scanned ports on 192.168.1.106 are: closed
MAC Address: 00:11:24:7B:95:2A (Apple Computer)
Too many fingerprints match this host to give specific OS details
Nmap finished: 1 IP address (1 host up) scanned in 69.660 seconds
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

← We’re Here!
A Word About the Law

Danger, Will Robinson!  Danger, Sherman!
According to the FBI, unauthorized use of computers generally takes one of the following forms:

1. File browsing
2. File alteration
3. File deletion
4. Service denial
The following federal laws have been used to convict persons of computer-related crimes:

- **15 USC 1644** (1995 Truth in Lending Act)
  - i.e. United States Code Title 15 Section 1644
  - Prohibits fraudulent use of credit cards.

  - Prohibits transfer or use of the identity documentation of another person without the legal authority and with the intent to commit, aid, or abet any unlawful activity.

- **18 USC § 1029**
  - Prohibits fraudulent acquisition of telecommunications services.
Federal Law (cont.)

• **18 USC 1030** (1986 Computer Fraud and Abuse Act)
  – Prohibits unauthorized access to any computer operated by the U.S. Government, financial institution insured by the U.S. Government, federally registered securities dealer, or foreign bank.

• **18 USC § 1343**
  – Prohibits wire fraud.

• **18 USC § 1361-2**
  – Prohibits malicious mischief.

• **18 USC § 1831**
  – Prohibits stealing of trade secrets.
Federal Law (cont.)

• **18 USC § 2314**
  - Prohibits interstate transport of stolen, converted, or fraudulently obtained material; *U.S. v. Riggs*, 739 F.Supp. 414 (N.D.Ill 1990) applied this law to computer data files.

• **18 USC § 2319 and 17 USC § 506(a)**
  - Prohibits criminal violations of copyright law

• **18 USC § 2510-11**
  - Prohibits interception of electronic communications

• **18 USC § 2701**
  - Prohibits access to communications stored on a computer (addresses e-mail privacy)