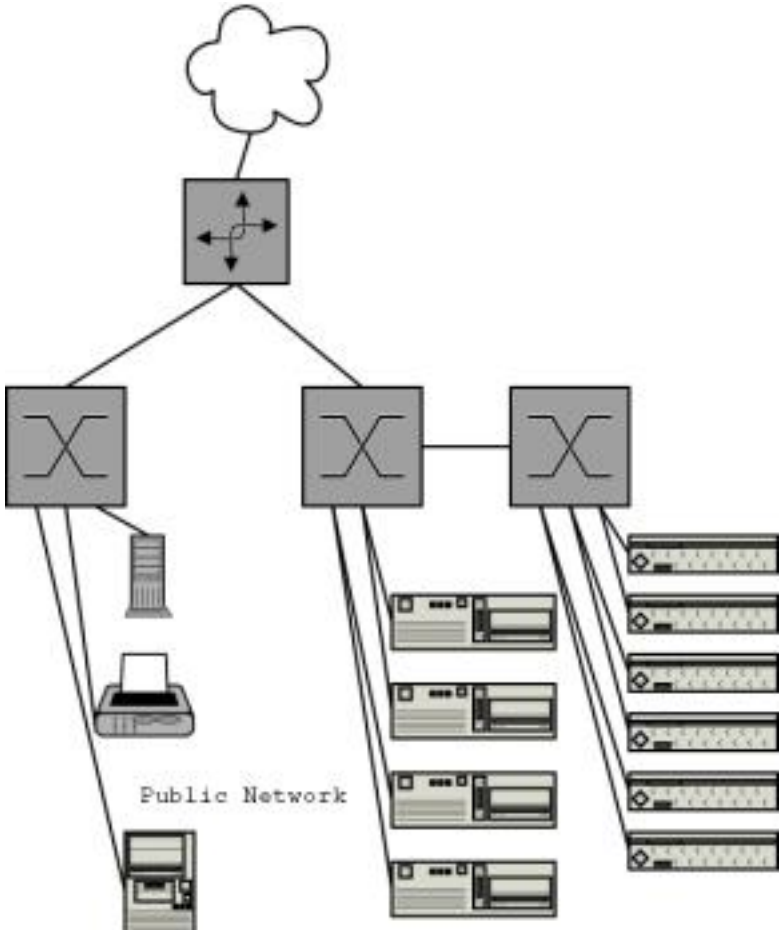
Network Security

Jon Hart & Muncus
Crew

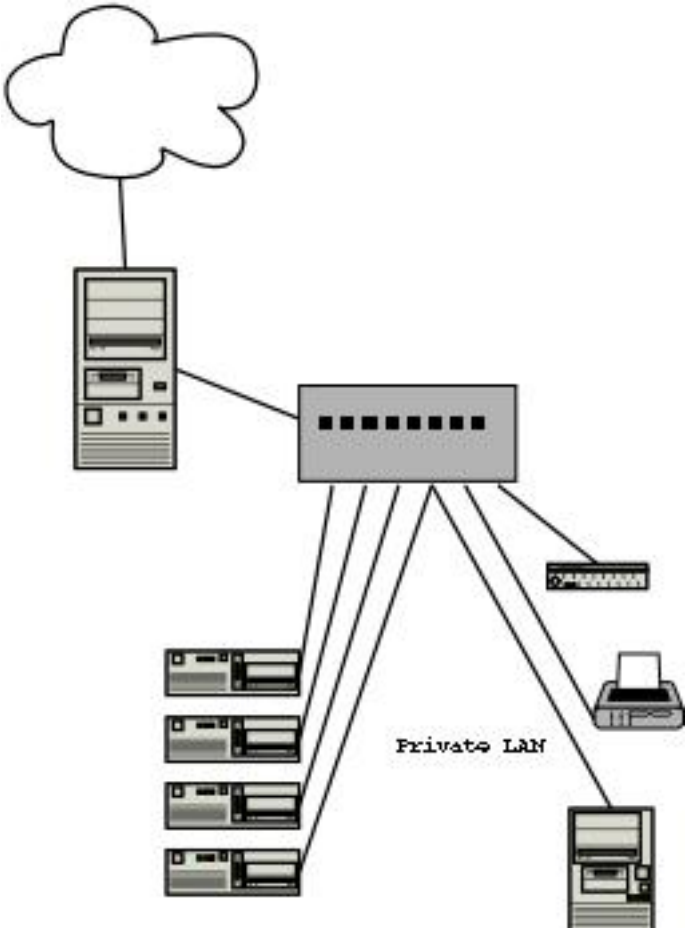
Disclaimer

- This talk:
  - Is not all inclusive
  - Will focus mostly on TCP/IP + Ethernet based networks
    - Much like the one used at CCS, CTF, home, etc
  - Many topics can be applied to other types of networks or security considerations
  - You will be punished and possibly serve jail time if you do this on networks that you don't own or otherwise have permission to poke at
  - Attacking, probing, or poking at CCS/NU networks will likely get you expelled.

CCS Network Diagram



CTF Network Diagram



Where do I start?

- Read. Learn. Do.
- Know your network
- Think like the attacker
- "How to Secure Your Network by Breaking Into it"

Know your network

- Info/Recon Gathering
  - Scan, Poke, Prod, which gets you...
    - A list of services
    - Network layout
    - And, with any luck, avenues of attack
  - Not everything has to be intrusive or malicious:
    - WHOIS records
    - DNS records
    - Website dredging
    - Google
  - The squeaky wheel gets the grease
- Physical Security
  - Is extremely important
  - If an attacker has physical access, its only a matter of time before its game over

Know your network (cont.)

- Tools you can't live without:
  - nmap
  - nessus
  - MBSA
  - nc/telnet
  - firewalk
  - packet crafting tool

Network scanning

- Aka "mapping"
- More of an information gathering process
- Figure out how a network is configured:
  - Network topology
  - Access Control Lists (ACLs)
  - What devices are in use, and how
- May allow you to discover misconfigurations

Network scanning: Defensive

- A good firewall ruleset, ACL, etc:
  - pf, ipf, ipchains, iptables, PIX, Cisco ACL, etc
  - Ingress and Egress filtering, bogon blocking
- Rate-limiting and monitoring:
  - cricket, mrtg
- Anomaly Detection:
  - Snort, Spade
- Know your network. What is 'normal'?

Network scanning: Offensive

- bypassing firewalls
  - SYN flags
  - packet reassembly bugs
- Open proxies
  - allows masking of source
- Tools
  - Fragroute(r)
  - nmap
  - Firewalk
  - traceroute
- Protocols

```
$  nmap -sO blah
Protocol   State       Name
1          open        icmp
2          open        igmp
6          open        tcp
17         open        udp
```

Host scanning

- Aka "portscanning"
- Again, mostly an information gathering process
- Figure out how a host is configured:
  - OS Type and version, maybe even specific options
  - Open Ports (services offered)
  - Allowed protocols

Host scanning

- Aka "portscanning"
- Again, mostly an information gathering process
- Figure out how a host is configured:
  - OS Type and version, maybe even specific options
  - Open Ports (services offered)
  - Allowed protocols
- Example: this laptop

```
$ nmap -O localhost

Starting nmap V. 3.10ALPHA4 ( www.insecure.org/nmap/ )
Interesting ports on cuba (127.0.0.1):
(The 1602 ports scanned but not shown below are: closed)
Port       State       Service
22/tcp     open        ssh
25/tcp     open        smtp
111/tcp    open        sunrpc
Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20
Uptime 0.036 days (since Thu Apr 10 05:28:12 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 6 seco
```

Host scanning: Defensive

- A good firewall:
  - Block everything, allow only whats needed
  - Stateful
  - Windows: ZoneAlarm, built-in
  - Linux: ipchains or iptables
  - *BSD, Solaris: pf, ipf
- Logging:
  - Logwatch, logsurfer

Host scanning: Offensive

- nmap
- nmap
- nessus
- Xprobe
- nc/telnet
- Google
- Pen and paper
- nmap

Specific Examples...

Specific Examples...

- Target: yournethere.com

Specific Examples...

- Target: yournethere.com
- MegaCorp Misconfiguration

Specific Examples...

- Target: yournethere.com
- MegaCorp Misconfiguration
- Arp spoofing

Specific Examples...

- Target: yournethere.com
- MegaCorp Misconfiguration
- Arp spoofing
- DNS spoofing

Target: yournethere.com

```
$ host yournethere.com
yournethere.com has address 192.168.0.51
$ whois 192.168.0.51
<snip>
Address:    36 Main St.
City:       Boston
StateProv:  MA
PostalCode: 02115
Country:    US

NetRange:   192.168.0.0 - 192.168.255.255
CIDR:       192.0.0/16
NetName:    YOURNETHERE-COM
NetHandle:  NET-192-0-0-0-1
Parent:     NET-192-0-0-0-0
NetType:    Direct Assignment
NameServer: bogus.yournethere.com
NameServer: bogus2.yournethere.com
Comment:
RegDate:    1988-07-18
Updated:    2000-09-07

TechHandle: FYTR-ARIN
TechName:   YOURNETHERE
TechPhone:  +1-555-555-1212
TechEmail:  hostmaster@yournethere.com
```

Target: yournethere.com (cont.)

```
$  host -t mx yournethere.com
yournethere.com mail is handled by 10 mail.yournethere.com.
yournethere.net mail is handled by 25 backup.net.
$  host -t ns yournethere.com
yournethere.com name server ns1.yournethere.com.
yournethere.com name server foo.blah.net.
$  traceroute yournethere.com
traceroute to yournethere.com (192.168.0.51), 64 hops max, 40 by
1  bstnma1-ar1-1-35-053-001.bstnma1.elnk.dsl.genuity.net (1.35.5
2  somehost1 (1.25.53.93)  18.174 ms  18.598 ms  15.482 ms
3  somehost2 (1.24.189.161)  15.902 ms  19.512 ms  16.342 ms
4  somehost3 (1.24.8.161)  20.743 ms  19.395 ms  15.602 ms
5  somehost4 (1.24.10.210)  18.448 ms  19.75 ms  15.839 ms
6  otherhost1 (2.24.6.49)  22.109 ms  25.551 ms  23.562 ms
7  otherhost2 (2.24.10.217)  24.665 ms  21.659 ms  22.404 ms
8  otherhost3 (2.24.5.221)  24.958 ms  26.769 ms  21.916 ms
9  littlepipe.net (192.24.246.6)  24.477 ms  26.701 ms  30.288 m
10  phatpipe.net (192.24.2.14)  27.224 ms  26.6 ms  23.114 ms
11  wehaveanOCxx.net (192.24.6.11)  25.931 ms  26.24 ms  25.67 m
12  woot.net (192.24.6.26)  26.127 ms  22.806 ms  23.751 ms
13  * * *
14  yournethere.com (192.168.0.51) 29.96 ms 27.84 ms 26.394 ms
```

Target: yournethere.com (cont.)

```
$  host -t mx yournethere.com
yournethere.com mail is handled by 10 mail.yournethere.com.
yournethere.net mail is handled by 25 backup.net.
$  host -t ns yournethere.com
yournethere.com name server ns1.yournethere.com.
yournethere.com name server foo.blah.net.
$  traceroute yournethere.com
traceroute to yournethere.com (192.168.0.51), 64 hops max, 40 by
1  bstnma1-ar1-1-35-053-001.bstnma1.elnk.dsl.genuity.net (1.35.5
2  somehost1 (1.25.53.93)  18.174 ms  18.598 ms  15.482 ms
3  somehost2 (1.24.189.161)  15.902 ms  19.512 ms  16.342 ms
4  somehost3 (1.24.8.161)  20.743 ms  19.395 ms  15.602 ms
5  somehost4 (1.24.10.210)  18.448 ms  19.75 ms  15.839 ms
6  otherhost1 (2.24.6.49)  22.109 ms  25.551 ms  23.562 ms
7  otherhost2 (2.24.10.217)  24.665 ms  21.659 ms  22.404 ms
8  otherhost3 (2.24.5.221)  24.958 ms  26.769 ms  21.916 ms
9  littlepipe.net (192.24.246.6)  24.477 ms  26.701 ms  30.288 m
10  phatpipe.net (192.24.2.14)  27.224 ms  26.6 ms  23.114 ms
11  wehaveanOCxx.net (192.24.6.11)  25.931 ms  26.24 ms  25.67 m
12  woot.net (192.24.6.26)  26.127 ms  22.806 ms  23.751 ms
13  * * *
14  yournethere.com (192.168.0.51) 29.96 ms 27.84 ms 26.394 ms
```

- What useful information does an attacker now have?

MegaCorp Misconfiguration

- You are trying to get inside the MegaCorp network, but they only seem to have a few webservers up and thats it
- After browsing through the pages of a few hosts, you check out server1.megacorp.net and notice a link titled "Documents".
- Following the link seems to bring you to another, unfamiliar machine
- Reading the source, you see a comment in the HTML:

```
<!-- Uses Apache's reverse-proxy to access 192.168.0.2 -->
<a href="/documents">Documents</a>
```

- You now have partial access inside their network, **and** have an idea of how the network is configured:
  - RFC1918 space of 192.168.0.0/24

MegaCorp Misconfiguration

- You are trying to get inside the MegaCorp network, but they only seem to have a few webservers up and thats it
- After browsing through the pages of a few hosts, you check out server1.megacorp.net and notice a link titled "Documents".
- Following the link seems to bring you to another, unfamiliar machine
- Reading the source, you see a comment in the HTML:

```
<!-- Uses Apache's reverse-proxy to access 192.168.0.2 -->
<a href="/documents">Documents</a>
```

- You now have partial access inside their network, **and** have an idea of how the network is configured:
  - RFC1918 space of 192.168.0.0/24
- How could this have been prevented?

Arp spoofing

- Aka "arp poisoning"
- Sending specially crafted malicious responses to ARP requests:
  - Traffic snooping
  - MITM attacks
  - DoS

Arp spoofing

- Aka "arp poisoning"
- Sending specially crafted malicious responses to ARP requests:
  - Traffic snooping
  - MITM attacks
  - DoS
- Q: If I ask the room how to send mail to Fred, how can you get me to send my mail to you?

Arp spoofing

- Aka "arp poisoning"
- Sending specially crafted malicious responses to ARP requests:
  - Traffic snooping
  - MITM attacks
  - DoS
- Q: If I ask the room how to send mail to Fred, how can you get me to send my mail to you?
- A: Keep telling me that Fred's address is yours

Arp spoofing

- Aka "arp poisoning"
- Sending specially crafted malicious responses to ARP requests:
  - Traffic snooping
  - MITM attacks
  - DoS
- Q: If I ask the room how to send mail to Fred, how can you get me to send my mail to you?
- A: Keep telling me that Fred's address is yours
- Successful sustained Arp spoofing often requires you to DoS one or more machines

Arp spoofing (cont.)

- Offensive Techniques
  - arpspoof (from Dug Song's dsniff)
  - ettercap
  - hunt
  - arp-tk, arp-sk
- Defensive Techniques
  - Port Security, MAC Locking
  - Static arp entries:

```
$  cat /etc/ethers
00:11:22:33:44:55 estonia
$ arp -f /etc/ethers
$ arp -a
estonia (192.168.0.1) at 00:11:22:33:44:55 [ether] PERM on eth0
```

DNS spoofing

- Sending specially crafted malicious responses to DNS requests (hostname -> IP queries):
  - Traffic snooping
  - MITM attacks
  - Trust attacks
  - DoS
- As effective as arp spoofing, but difficult to detect
- Offensive Techniques
  - dnsspoof (from Dug Song's dsniff)
- Defensive Techniques
  - Combination of:
    - /etc/hosts
    - /etc/nsswitch.conf
    - /etc/resolv.conf
    - nscd
    - Arp spoofing defensive techniques...

Page 'o links

- arp-sk - http://www.arp-sk.org/
- arp-tk - http://spoofed.org/files/
- arpspoof - http://naughty.monkey.org/~dugsong/dsniff/
- bugtraq - http://securityfocus.com/bid/vendor/
- cricket -
- default passwords - http://www.phenoelit.de/dpl/dpl.html
- dnsspoof - http://naughty.monkey.org/~dugsong/dsniff/
- dsniff - http://naughty.monkey.org/~dugsong/dsniff/
- ettercap - http://ettercap.sourceforge.net/
- firewalk - http://www.packetfactory.net/projects/firewalk
- fragroute - http://naughty.monkey.org/~dugsong/fragroute/

Page 'o links (cont.)

- hunt-
- ingress/egress filtering-
- ipchains - http://www.netfilter.org/ipchains/
- ipf - http://coombs.anu.edu.au/~avalon/
- iptables - http://www.netfilter.org/
- libnet - http://www.packetfactory.net/libnet/
- logwatch - http://www.logwatch.org/
- logsurfer - http://www.cert.dfn.de/eng/logsurf/
- mailing list archives - http://marc.theaimsgroup.com/
- mbsa- http://www.microsoft.com/TechNet/Security/tools/tools/MBSAHo
- mrtg - http://people.ee.ethz.ch/~oetiker/webtools/mrtg/

Page 'o links (cont.)

- nc - http://www.atstake.com/research/tools/network_utilities/
- nemesis - http://www.packetfactory.net/projects/nemesis
- nessus - http://nessus.org/
- nmap - http://www.insecure.org/nmap/
- pf - http://www.benzedrine.cx/pf.html
- snort - http://www.snort.org
- spade - http://www.silicondefense.com/products/freesoftware/spade/
- xprobe - http://www.sys-security.com/html/projects/X.html
- zonealarm - http://www.zonelabs.com