Corporate Network Spying

Andrew Whitaker
Director of Enterprise InfoSec
InfoSec Academy / Training Camp

Who is this guy?

• Director of security course offerings for InfoSec Academy (division of Training Camp)
• Teaches ethical hacking / pentesting courses
• Co-author of *Penetration Testing and Network Defense* ( Cisco Press, 2005)
• Author of other books/articles relating to security / networking
• Pentester of numerous financial and healthcare institutions
• M.Sc., Computer Science; CISSP, CEH, CCSP, CCNP, CCNA, CCDA, MCSE, CNE, A+, Network+, Security+, CTP, et al.
Training Camp

- InfoSec Academy division is world leader in teaching information security
  - Authorized CISSP
  - Certified Ethical Hacker
  - Licensed Penetration Tester
  - Sarbanes Oxley
  - HIPAA Compliance Training
  - Certified Information Systems Auditor (CISA)
  - Much, much more…
What this is / What this is not

• What this is
  – Training on corporate network spying
  – Designed for those with beginner to intermediate skills

• What this is not
  – Discussion of hot new exploit (which may only be theoretical or work in a lab environment)
  – An overly technical discussion that only 1% of the techie world can understand
Agenda

• What the heck is this network spying thing?
• Who does it?
• Legal cases (to scare the begeezes out of ya)
• How to get past those darn switches
• General tools of the trade: Windump / TCPdump, Ethereal
• Analyzing common protocols
  – FTP, MSN IM, Web, SMTP/POP
• Demos to make you druel
What is Network Spying?

- Wiretapping
- Targeted packet capturing
Who Spies on Networks?

• Legitimate: Law enforcement
  – FBI
  – NSA
• Legitimate: Corporations with consent
  – Admins
  – Your boss
• Illegitimate: The "bad" guys
  – Hacker hobbyists
  – Corporate espionage
Who Spies on Networks?

• Law Enforcement
  – Patent #5,937,422 "Semantic Forests"
    • NSA solution
    • Captures voice conversation
    • Automatic speech transcription
  – Carnivore
    • Abandoned in 2005
    • Part of DragonWare suite
      – Carnivore – packet capturing
      – Packeteer – reassembles packets
      – Coolminer – searching captured packets
Who Spies on Networks?

• Corporations
  – PC Magazine reported 77% of companies spy on employees
  – Typically e-mail and web surfing
  – Justifications:
    • To ensure employee productivity
    • To ensure company is void of illegal activity
    • To protect trade secrets
Who Spies on Networks?

- Hacker hobbyists
  - Hey, look Ma, a wireless network!
- Corporate espionage
  - Tech companies especially at risk
  - Example: Oracle & Microsoft
Legal and Ethical Considerations

• 4th Amendment
• 1994 Communications Assistance for Law Enforcement
• Federal Electronic Communications Privacy Act (18 U.S.C. § 2511)
• PATRIOT Act
Cases

- Katz vs. United States, 1967
- 2004 Nicodemo Scarfo ("Little Nicky")
What You Need To Begin

• Commercial: Network Forensics Analysis Tools (NFAT)
• Packet capturing tool
  – Open-source vs. commercial
  – General vs. targeted
  – remote-vs. local
  – switched vs. shared
Sniffing on Switched Networks
Hubs...mmm...good

Frame from UserA is always propagated to UserB & UserC
How Switches Work
How Switches Work

User A sends a frame to user B.

MAC Table

<table>
<thead>
<tr>
<th>Port</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>01C9:44BB:00A1 (USER A)</td>
</tr>
<tr>
<td>Fa0/2</td>
<td>??</td>
</tr>
<tr>
<td>Fa0/3</td>
<td>??</td>
</tr>
</tbody>
</table>
How Switches Work

MAC Table

<table>
<thead>
<tr>
<th>Port</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>01C9:44BB:00A1 (USER A)</td>
</tr>
<tr>
<td>Fa0/2</td>
<td>???</td>
</tr>
<tr>
<td>Fa0/3</td>
<td>???</td>
</tr>
</tbody>
</table>

Frame is duplicated out to UserB and UserC.
How Switches Work

MAC Table
FA 0/1 01C9:44BB:00A1 (USER A)
FA 0/2 0BB0:0E44:2221 (USER B)
FA0/3 ???

UserA
UserB
UserC
How Switches Work

MAC Table
FA 0/1 01C9:44BB:00A1 (USER A)
FA 0/2 0BB0:0E44:2221 (USER B)
FA0/3 ???
How To Get Around This Problem

• Five Solutions:
  1. ARP Poisoning method 1
  2. ARP Poisoning method 2
  3. MAC Duplicating
  4. MAC Flooding
  5. Port Mirroring
ARP Poisoning Method 1

- A.K.A. ARP spoofing
- Sending crafted replies to ARP requests

What is the MAC address for UserB?

I'm here!
Here's my MAC

I heard that.
Here's the same MAC.

MAC Table
FA 0/1 01C9:44BB:00A1 (USER A)
FA 0/2 0BB0:0E44:2221 (USER B)
FA0/3 0BB0:0E44:2221 (spoofed)
ARP Poisoning Method 2

MAC Table
- FA 0/1 01C9:44BB:00A1 (USER A)
- FA 0/2 0BB0:0E44:2221 (USER B)
- FA0/3 0040:5B50:387E (spoofed)
- Fa0/4 0040:5B50:387E (Router)

UserA 10.0.0.11
UserB 10.0.0.12
UserC 10.0.0.13

Router 10.0.0.1

ARP Reply
ARP Reply
ARP Reply
MAC Duplicating

- Used to target traffic sent to a single host (such as a server)
- ARP for a host you want to target to get its MAC address

What is the MAC address of 10.0.0.11?

New spoofed MAC address: 01C9:44BB:00A1
MAC Flooding

- MAC addresses are stored in CAM table
- Content Addressable Memory (CAM) table
  - Switch must find an exact binary match
  - Information to do a lookup is called a key
  - Key is fed into a hashing algorithm to produce a pointer into the table
MAC Flooding

- CAM is limited on switches (typically 64k)
- If filled up, switch can no longer store new addresses
- Switch effectively turns into a hub
MAC Flooding

- MACOF (part of Dsniff)
- http://www.monkey.org/~dugsong/dsniff/
Port Mirroring

- Port mirroring is a legitimate method of mirroring one port to another port
- Cisco calls this *switched port analyzer* (SPAN)
  - Remote SPAN (RSPAN) can send traffic from one or more ports or an entire VLAN to another port on a different switch
  - There can be more than one source and more than one destination (up to 64 destination ports!)
- SPAN can copy traffic in one of three ways:
  - Rx SPAN
  - Tx SPAN
  - Rx/Tx SPAN
Port Mirroring

1) Specify source

```bash
monitor session session_number source
  {interface interface-id | vlan vlan-id} [, | -] [both | rx | tx]
```

2) Specify destination

```bash
monitor session session_number destination
  {interface interface-id [, | -] [encapsulation replicate]
```
Port Mirroring

Switch(config)#monitor session 1 source interface fastethernet 0/1, 0/2 both
Switch(config)#monitor session 1 destination fastethernet 0/3
Packet Capturing Software

• Tons!!
• PacketStorm Security (http://packetstormsecurity.org/sniffers/) has almost 200 different sniffers
• Most popular freeware utilities:
  – Windump / Tcpdump
  – Ethereal (Now Wireshark)
Windump / TCPDump

- Developed by Loris Degioanni, Gianluca Varenni, Fulvio Risso, John Bruno, Piero Viano
- Requires winpcap / libpcap library
Using WinDump / TCPDump

- `tcpdump [ -ABdDefIlnNOpqRStuUvxX ] [ -c count ]`

  - `-C file_size`
  - `-F file`
  - `-i interface`
  - `-m module`
  - `-M secret`
  - `-r file`
  - `-s snaplen`
  - `-T type`
  - `-w file`

  - `-W filecount`

  - `-E spi@ipaddr algo:secret,...`

  - `-y datalinktype`
  - `-Z user`
  - `[ expression ]`
Using WinDump / tcpdump

- **Display interfaces**: `windump –D`
- **Use interface**: `windump –i <interface # or identifier>`
- **Print out in Ascii**: `windump –A`
- **Log to file**: `windump –w file.log`
- **Read from log**: `windump –r file.log`
- **Verbose output**: `windump –vvv`
Windump Example

23:23:52.991879 IP (tos 0x0, ttl 128, id 11231, offset 0, flags [DF], proto: TCP (6), length: 48)
   A152B.2436 > www.defcon.org.80: S, cksum 0x86d6 (correct), 916679930:916679930(0) win 16384 <mss 1460,nop,nop,sackOK>
E..0+.@.....
..9..(.....P6.l.....p.@............

23:23:53.116681 IP (tos 0x0, ttl 47, id 35735, offset 0, flags [none], proto: TCP (6), length: 44)
   www.defcon.org.80 > A152B.2436: S, cksum 0x2304 (correct), 451321314:451321314(0) ack 916679931 win 65535 <mss 1460>
E,.../.../]..(.
..9.P.....6.l.`........

23:23:53.116738 IP (tos 0x0, ttl 128, id 11232, offset 0, flags [DF], proto: TCP (6), length: 40)
   A152B.2436 > www.defcon.org.80: ., cksum 0xf650 (correct), 1:1(0) ack 1 win 17520
E...(+.@.....

23:23:53.117616 IP (tos 0x0, ttl 128, id 11233, offset 0, flags [DF], proto: TCP (6), length: 495)
   A152B.2436 > www.defcon.org.80: P 1:456(455) ack 1 win 17520
E...+(.@....P
Ethereal / Wireshark

- Packet analyzer
- Original author was Gerald Combs
- Now supported by over 100 programmers
- Can 'dissect' 759 protocols
- Linux & Windows friendly
- Now licensed through CACE Technologies
  http://www.wireshark.org/
### Ethereal / Wirehsark

**GET SNMPv2-SMI::MIB-2.25.3.2.1.5.1 SNMPv2-SMI::MIB-2.25.3.5.1.1.1**

**Standard query A www.defcon.org**

**Standard query response A 216.231.40.180**

**Standard query A mirror.toolbar.netcraft.com**

2552 > http [SYN] Seq=0 Len=0 MSS=1460

**Standard query response CNAME p.mii.instacontent.net A 64.191.208.114**

2553 > http [SYN] Seq=0 Len=0 MSS=1460

http > 2552 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460

2552 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0

GET /html/defcon-14/html/dc-css/defconbluestyles.css HTTP/1.1

http > 2553 [SYN, ACK] Seq=0 Ack=1 Win=6144 Len=0 MSS=1460

2553 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0

GET /check_url/http://www.defcon.org/3639027892 HTTP/1.1

HTTP/1.1 302 Redirect (text/html)
Ethereal / Wireshark

- To view entire conversation, right-click and choose **Follow TCP Stream**
Ethereal / Wireshark

Follow TCP stream

Stream Content

GET /html/defcon-14/html/dc-css/defconbluestyles.css HTTP/1.1
Host: www.defcon.org
User-Agent: Mozilla/5.0 (windows; u; windows nt 5.1; en-us; rv:1.8.0.4) gecko/20060508
Firefox/1.5.0.4
Accept: text/css, */*;q=0.1
Accept-Language: en-us, en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1, utf-8;q=0.7, *,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.defcon.org/
If-Modified-Since: Fri, 26 Mar 2004 16:31:58 GMT

HTTP/1.1 404 file does not exist
X-xxxx:xxxxxxxxxxxx
Date: Sun, 09 Jul 2006 04:15:41 GMT
Last-Modified: Fri, 26 Mar 2004 16:31:58 GMT
Content-Type: text/html
Transfer-Encoding: chunked

564
<!doctype html public "-//w3c//dtd html 4.0 transitional//en">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<meta name="GENERATOR" content="vi">
<meta name="Author" content="web master">
<meta name="Description" content="html error 404 code">
<meta name="Keywords" content="html error 404 code">
<meta name="copyright" content="Copyright . 1996-2004 by DatAmerica. All rights reserved." />
<meta name="robots" content="index, follow, noarchive" />
</head>

Save As  Print  Entire conversation (2039 bytes)  
ASCII  EBCDIC  Hex Dump  C Arrays  Raw
Password Capturing

• The following protocols send passwords in plain text
  – Telnet
  – FTP
  – POP
  – SMTP
  – Just to name a few!

• Even if password is not in plain text, it is often easily cracked
Tool: Cain and Abel

- Developed by Massimiliano Montoro
- [http://www.oxid.it/index.html](http://www.oxid.it/index.html)
- Password recovery tool that supports packet capturing
- Can even capture & replay voice conversations
<table>
<thead>
<tr>
<th>Timestamp</th>
<th>POP3 server</th>
<th>Client</th>
<th>Username</th>
<th>Password</th>
<th>AuthType</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/07/2006 - 23:58:17</td>
<td>38.113.3.22</td>
<td>10.4.1.19</td>
<td>victim14</td>
<td>defcon14</td>
<td>ClearText</td>
</tr>
<tr>
<td>08/07/2006 - 23:58:18</td>
<td>38.113.3.22</td>
<td>10.4.1.19</td>
<td>victim14</td>
<td>defcon14</td>
<td>ClearText</td>
</tr>
</tbody>
</table>
Cain and Abel
Cain and Abel
Cain and Abel

Password: A3B2C1D0 E4F5G6H7 I8J9K0L1

***Welcome to the DefCon Router***

***Authorized access only***

Defcon>

View

Remove  Delete

Remove All
### Cain and Abel

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>aWBgtLLqW-c6wSmCrX</td>
<td>defcon14</td>
<td><a href="http://www.hotpop.com/lo">http://www.hotpop.com/lo</a></td>
</tr>
<tr>
<td>victim14</td>
<td>xxxxxxxxxx</td>
<td><a href="http://registration.excite.co">http://registration.excite.co</a></td>
</tr>
</tbody>
</table>
Cain and Abel
Tool: Dsniff

- [Link to Dsniff](http://www.monkey.org/~dugsong/dsniff/)
- Dsniff can be used to listen only for passwords
Tool: Ettercap

- Can be used to sniff passwords
- Active and passive capturing capabilities
- Content filtering
## Tool: Ettercap

### Host List

<table>
<thead>
<tr>
<th>Host</th>
<th>Port</th>
<th>Host</th>
<th>Port</th>
<th>Proto</th>
<th>State</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.1.3</td>
<td>53286</td>
<td>T</td>
<td>killed</td>
<td>510</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.1.3</td>
<td>53222</td>
<td>T</td>
<td>idle</td>
<td>123</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.1.3</td>
<td>53222</td>
<td>T</td>
<td>idle</td>
<td>123</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Group 1: ANY (all the hosts in the list)

### Group 2: ANY (all the hosts in the list)

Starting Unified sniffing...

POP: [censored]:110 -> USER: quicksilr PASS: [censored]

IMAP: [censored]:143 -> USER: dcwilliams PASS: [censored]

FTP: [censored]:21 -> USER: dwilliams2 PASS: [censored]

---

**TRAINING CAMP**

Accelerated Learning. Education Evolved.
## Analysis of E-mail Traffic

### SMTP Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HELO</td>
<td>Used to initiate communication to an SMTP server</td>
</tr>
<tr>
<td>EHLO</td>
<td>Same as HELO</td>
</tr>
<tr>
<td>MAIL FROM:</td>
<td>Address you are sending e-mail from (easy to spoof!)</td>
</tr>
<tr>
<td>RCPT TO:</td>
<td>Destination of e-mail</td>
</tr>
<tr>
<td>SIZE=#### of bytes</td>
<td>Not necessary. Specifies size of e-mail in bytes.</td>
</tr>
<tr>
<td>DATA</td>
<td>The message body. Terminated with a single period (.) on a line by itself.</td>
</tr>
<tr>
<td>QUIT</td>
<td>Terminates the SMTP session</td>
</tr>
<tr>
<td>VRFY username</td>
<td>Verify that a username is valid. Excellent way to enumerate users.</td>
</tr>
<tr>
<td>EXPN name</td>
<td>Like VRFY, can verify a username. EXPN can also list out all usernames in a distribution list.</td>
</tr>
</tbody>
</table>
Analysis of E-mail Traffic

- POP Commands (RFC 1225)
  - USER
  - PASS
  - QUIT
  - STAT
  - LIST
  - RETR
  - DELE
  - LAST
  - RSET
Analysis of E-mail Traffic

Response: +OK
Request: USER victim14
pop3 > 1819 [ACK] Seq=6 Ack
Response: +OK
Request: PASS defcon14
Response: +OK
Request: STAT
Analysis of E-mail Traffic
Analysis of E-mail Traffic

Ethereal capture of SMTP email exchange:

```plaintext
smtp > 1815 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0
1815 > smtp [ACK] Seq=1 Ack=1 win=64240 Len=0
Response: 220 smtp-2.hotpop.com ESMTP Postfix
Command: HELO TTCQ7VTQEOB0C
smtp > 1815 [ACK] Seq=38 Ack=22 win=5840 Len=0
Response: 250 smtp-2.hotpop.com
Command: MAIL FROM: <victim14@PunkAss.com>
Response: 250 Ok
Command: RCPT TO: <attacker14@PunkAss.com>
smtp > 1815 [ACK] Seq=69 Ack=92 win=5840 Len=0
Response: 250 Ok
Command: DATA
smtp > 1815 [ACK] Seq=77 Ack=98 win=5840 Len=0
Response: 354 End data with <CR><LF>.<CR><LF>
Message Body
Message Body
smtp > 1815 [ACK] Seq=114 Ack=1558 win=8760 Len=0
```
The DefCon conference is coming up. Can we send some feds to it?
Analysis of E-mail Traffic: Ettercap

10.0.1.3:53396
USER quiksirr.
PASS
STAT.
Tool: Mailsnarf

- Part of Dsniff: http://www.monkey.org/~dugsong/dsniff/
- Dug Song
- Listens only for e-mail
Tool: Mailsnarf

root@1[ettercap]# mailsnarf
mailsnarf: listening on eth0

Mime-Version: 1.0 (Apple Message framework v752.2)
To: David Williams
Message-Id: <E7819150-6632-42A5-870B-F447CF313500@trainingcamp.net>
Content-Type: multipart/alternative; boundary=Apple-Mail-4-218664851
From: David Williams
Subject: Defcon 14 Mailsnarf
Date: Sun, 9 Jul 2006 15:07:20 -0400
X-Mailer: Apple Mail (2.752.2)

Testing Mail Snarf

David Williams
Information Systems Support Specialist

Tech Train | The Training Camp | Infosec Academy
Visit our website at http://www.trainingcamp.net
Analysis of FTP Traffic
Analysis of FTP Traffic

..r... Z)....E.
.Y.o@... *....
...j...i...Y...
...i... F...
..331 Pa ssword r
quired for defc
on14...

File: /var/tmp/etherJChY4Iust 3755 Bytes 00:00:00 0
P: 40 D: 40 M: 1 Drops: 0
### Analysis of FTP Traffic

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.00600</td>
<td>10.0.1.2</td>
<td>10.0.1.4</td>
<td>TCP</td>
<td>54890 &gt; compressnet</td>
</tr>
<tr>
<td>2</td>
<td>0.01485</td>
<td>10.0.1.4</td>
<td>10.0.1.2</td>
<td>TCP</td>
<td>compressnet &gt; 54890</td>
</tr>
<tr>
<td>3</td>
<td>0.01490</td>
<td>10.0.1.2</td>
<td>10.0.1.4</td>
<td>TCP</td>
<td>54890 &gt; compressnet</td>
</tr>
<tr>
<td>5</td>
<td>0.01598</td>
<td>10.0.1.2</td>
<td>10.0.1.4</td>
<td>TCP</td>
<td>54890 &gt; compressnet</td>
</tr>
<tr>
<td>6</td>
<td>0.13952</td>
<td>10.0.1.2</td>
<td>10.0.1.4</td>
<td>TCP</td>
<td>54890 &gt; compressnet</td>
</tr>
<tr>
<td>7</td>
<td>0.14086</td>
<td>10.0.1.2</td>
<td>10.0.1.4</td>
<td>TCP</td>
<td>54890 &gt; compressnet</td>
</tr>
<tr>
<td>9</td>
<td>0.14071</td>
<td>10.0.1.2</td>
<td>10.0.1.4</td>
<td>TCP</td>
<td>54890 &gt; compressnet</td>
</tr>
<tr>
<td>10</td>
<td>0.14716</td>
<td>10.0.1.2</td>
<td>10.0.1.4</td>
<td>TCP</td>
<td>54890 &gt; compressnet</td>
</tr>
<tr>
<td>11</td>
<td>0.14735</td>
<td>10.0.1.2</td>
<td>10.0.1.4</td>
<td>TCP</td>
<td>54890 &gt; compressnet</td>
</tr>
<tr>
<td>12</td>
<td>0.14796</td>
<td>10.0.1.2</td>
<td>10.0.1.4</td>
<td>TCP</td>
<td>54890 &gt; compressnet</td>
</tr>
<tr>
<td>13</td>
<td>0.15260</td>
<td>10.0.1.2</td>
<td>10.0.1.4</td>
<td>TCP</td>
<td>54890 &gt; compressnet</td>
</tr>
</tbody>
</table>

Frame 4 (93 bytes on wire, 93 bytes captured)
Internet Protocol, Src: 10.0.1.4 (10.0.1.4), Dst: 10.0.1.2 (10.0.1.2)
Transmission Control Protocol, Src Port: compressnet (3), Dst Port: 54890 (54890)
Data (27 bytes)

```
..r.. Z)....E.
.O.n@... 5.....
..... j... i... Y...
............. E..
..220 Mi croscof
FTP Serv ice..
```

File: `/var/tmp/etherjCh4list` 3755 Bytes 00:00:00
Analysis of FTP Traffic

File: `/var/tmp/etherJtChY4lust` 3755 Bytes 00:00:00

P: 40 D: 40 H: 1 Drops: 0
Analysis of FTP Traffic
Analysis of FTP Traffic

Mark Packet (toggle)
Time Reference
Apply as Filter
Prepare a Filter
Follow TCP Stream

Decode As...
Print...
Show Packet in New Window

Internet Protocol, Src: 10.0.1.2 (10.0.1.2), Dst: 10.0.1.4 (10.0.1.4)
Transmission Control Protocol, Src Port: 54890 (54890), Dst Port: compressnet (3), Seq: 0, Ack: 0, Len: 0

0000 00 10 5a 29 a2 b7 00 0d 93 81 df 72 08 00 4f 00 ...z.......
0010 00 3c 2a 58 00 40 00 00 f0 ac 0a 00 00 01 02 0a 00 ....X.......
0020 01 04 46 6a 00 00 86 b9 5f 00 00 00 00 00 a0 02 ....J........
0030 ff ff ab 05 00 00 00 02 04 05 b4 01 03 03 03 01 01 ...........
0040 00 08 00 17 80 ba e1 00 00 00 00 ...........

File: `/var/tmp/etherJChY4Iust` 3755 Bytes 00:00:00
P: 40 D: 40 M: 1 Drops: 0
Analysis of FTP Traffic
Analysis Of FTP Traffic: Ettercap

220 ttcftp Microsoft FTP Service (Version 5.0)...
331 Password required for seaport...
230-Training Camp's FTP in Bushkill, PA. All Unauthorized access is prohibited!
230 User ___ logged in...
215 Windows_NT version 5.0.
500 'MACB ENABLE': command not understood.
257 "/" is current directory...
500 'FEAT': command not understood.
227 Entering Passive Mode ___ (9,76)...
125 Data connection already open; Transfer starting...
226 Transfer complete...

FTP: 216.113.232.131:21 -> USER ___ PASS ___
Analysis of FTP Traffic: Ettercap

Shows directory listing of FTP server

```
-rw-r--r-- 1 owner group 0 Jun 22 12:39 Images
-rw-r--r-- 1 owner group 0 Mar 17 14:26 Instruct
-rw-r--r-- 1 owner group 0 Sep 6 2004 Java.
-rw-r--r-- 1 owner group 17072239 Apr 7 2005 kernel-
```

```
-rw-r--r-- 1 owner group 0 Feb 26 2004 New Trainers Kits.
rw-r--r-- 1 owner group 0 Apr 22 2004 Novell.
rw-r--r-- 1 owner group 0 Apr 18 2005 Oracle.
rw-r--r-- 1 owner group 0 Mar 3 2005 Programs.
rw-r--r-- 1 owner group 0 Jun 23 11:43 Public.
rw-r--r-- 1 owner group 0 May 15 10:53 Rick.
rw-r--r-- 1 owner group 0 Jun 14 9:17 Solaris.
rw-r--r-- 1 owner group 0 Aug 10 2004 Test Materials.
rw-r--r-- 1 owner group 0 May 17 22:31 TestInstallation.
rw-r--r-- 1 owner group 0 Jun 19 12:07 Upload.
```

```
-rw-r--r-- 1 owner group 2025 May 4 12:07 upload.a
```
Victim14@PunkAss.com: "We need to send feds to the Defcon conference. Hackers are bad...very bad.

Attacker14@PunkAss.com: "No, there is no need to send a fed...I am sure nobody will do anything illegal there."
Analysis of MSN Messenger Traffic

- MSN Sniffer
- www.effetech.com
- Also have ICQ Sniffer, AIM Sniffer, HTTP Sniffer, ACE Password Sniffer, and much more
Analysis of MSN Messenger Traffic

#1, 2006-7-8 16:30:28
attacker14@punkass.com (attacker14@punkass.com) says:
No, you have nothing to worry about. Where do you live again?

#0, 2006-7-8 16:30:16
victim14@punkass.com (victim14@PunkAss.com) says:
Is it it ok to leave my wireless open? You don't think anyone will use it, do you?
Web Traffic: URLSnarf

- Part of dsniff, written by Dug Song
- http://www.monkey.org/~dugsong/dsniff/
- urlsnarf [-n] [-i interface] [[-v] pattern [expression]]
  - -n  Do not resolve IP to hostname
  - -i  Interface
  - -v  "versus mode"  Invert the pattern you are matching
  - pattern  Specify regular expression to match
  - Expression  Specify a tcpdump filter expression to select traffic to dump
Web Traffic: URLSnarf

```
root@1[ettercap]# urlsnarf
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
10.0.1.3 - - [09/Jul/2006:15:09:32 -0400] "GET http://www.apple.com/ HTTP/1.1" - - "Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en) AppleWebKit/418.8 (KHTML, like Gecko) Safari/419.3"
```

TRAINING CAMP
Accelerated Learning. Education Evolved.
Tool: Ettercap
Countermeasures

- Port Security
- IPSec
Demo Time