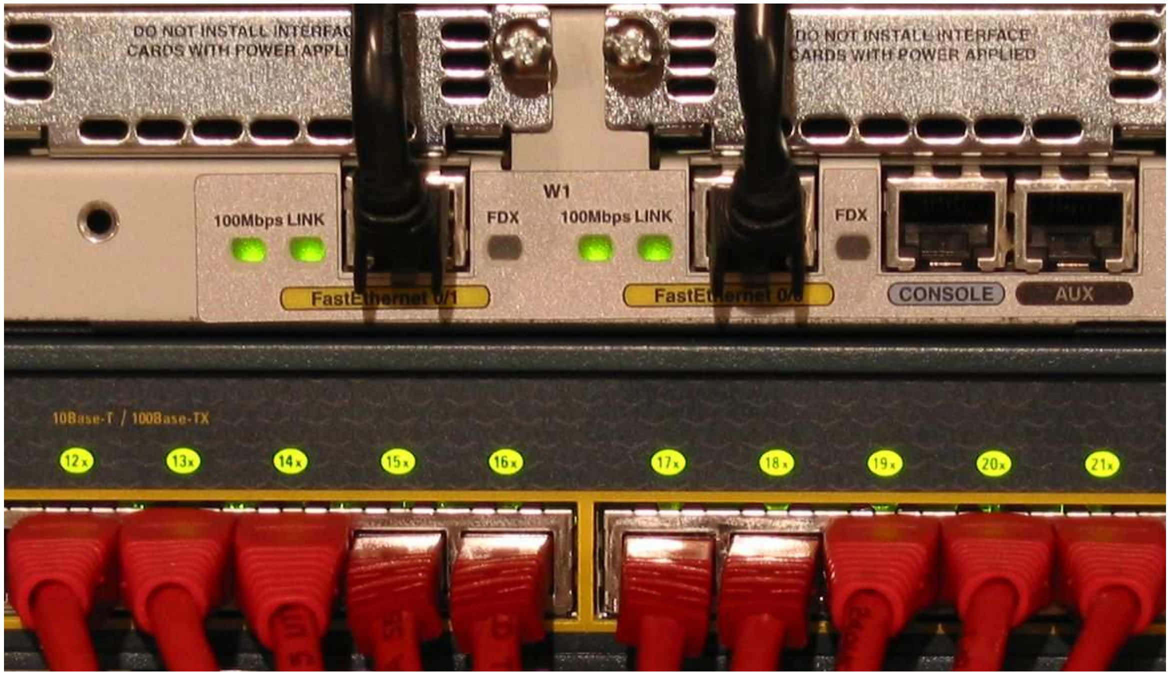
Traditional IDS Should Be Dead

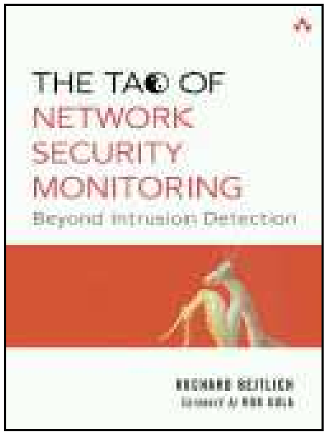


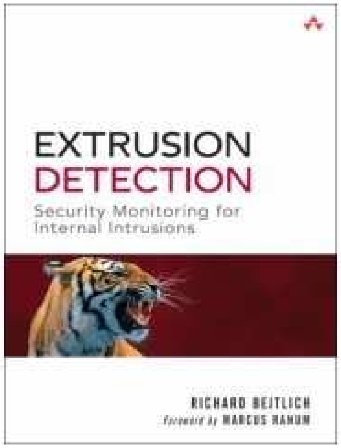
TAOSECURITY
THE WAY OF DIGITAL SECURITY

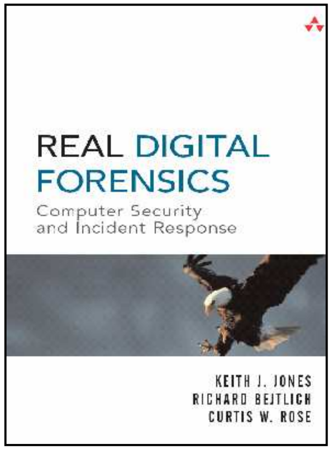
Richard Bejtlich
richard@taosecurity.com
www.taosecurity.com / taosecurity.blogspot.com

Introduction

- Bejtlich ("bate-lik") biography
  - TaoSecurity (05-present)
    - ManTech (04-05)
    - Foundstone (02-04)
    - Ball Aerospace (01-02)
    - Captain at US Air Force CERT (98-01)
    - Lt at Air Intelligence Agency (97-98)
  - Author
    - Tao of Network Security Monitoring: Beyond Intrusion Detection (solo, Addison-Wesley, Jul 04)
    - Extrusion Detection: Security Monitoring for Internal Intrusions (solo, Addison-Wesley, Nov 05)
    - Real Digital Forensics (co-author, Addison-Wesley, Sep 05)
    - Contributed to Incident Response, 2nd Ed and Hacking Exposed, 4th Ed







Argument

- Security environment has changed during the past ten years
- Prevention always eventually fails somewhere, yet most people focus on it exclusively and ignore detection
- "Intrusion Detection" must be an investigative process; "Intrusion Prevention" does not require investigation
- "Intrusion Detection" as currently practiced is actually managing attack or suspicious behavior inferences
- True intrusion detection requires investigating facts, not managing alerts based on inferences
- Traffic-centric forensics provides trustworthy evidence although details may be obfuscated

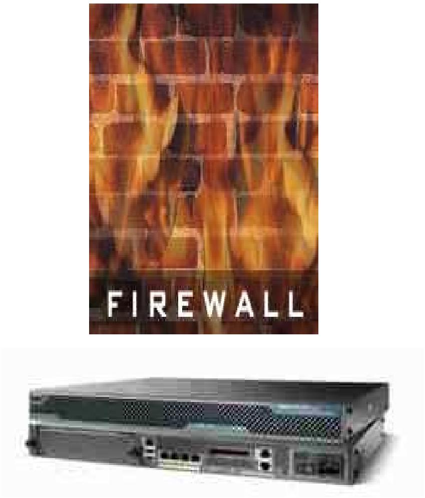
Changing Security Environment

1997	2007
Intruders obtain remote host control by abusing, subverting, or breaking unnecessary services and/or exposed services	Intruders gain remote host control via 1) client-side breaches; 2) abusing or subverting exposed and necessary applications; 3) breaking exposed services
Majority of malicious traffic is caused by humans interacting with targets	Majority of malicious traffic is caused by automated code operating on behalf of humans
Goal of exploitation is often control of target	Goal of exploitation is often theft of sensitive data
Defense involves preventing intrusions by applying patches for necessary services and disabling unnecessary services	Defense involves properly designing, coding, and deploying complex individualistic applications for which no commodity "patch" is available
Buffer overflows, SYN floods, and misconfiguration were the big problems	Web application abuse/subversion, root kits, bot nets, exploiting consumer data, etc. are huge

- Too many managers still live in 1997, along with their defensive strategies

Prevention Eventually Fails

- Risk environment changes faster than prevention system



Threats are exceptionally creative, numerous, determined, and always changing

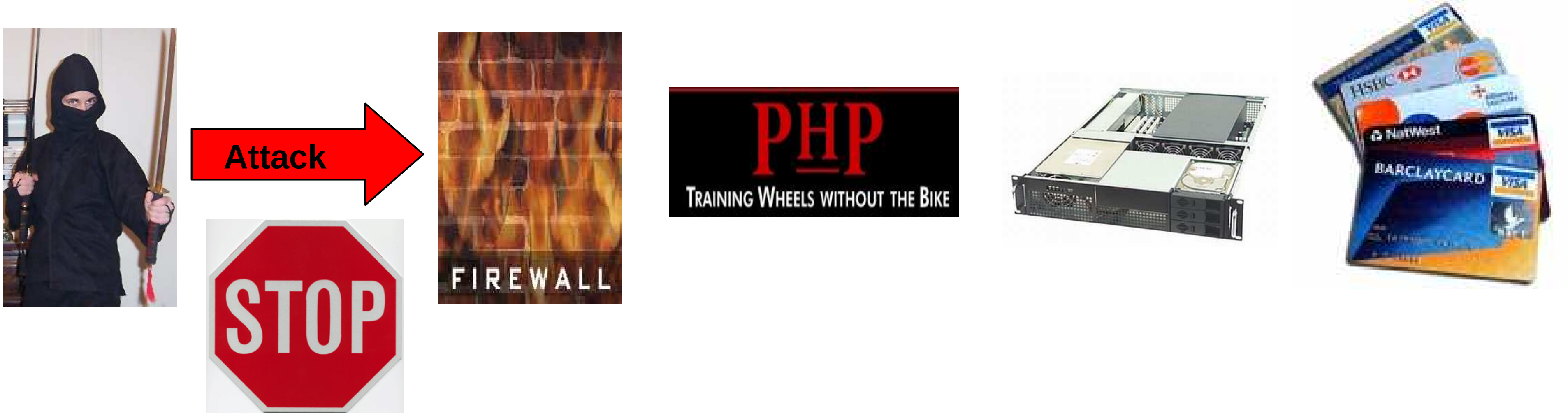
Defenses usually focus on attacks from the outside and cannot understand everything that happens

New devices with various services and applications are always being introduced, often out of the control of the enterprise

Assets are stored anywhere and everywhere

Prevention vs Detection

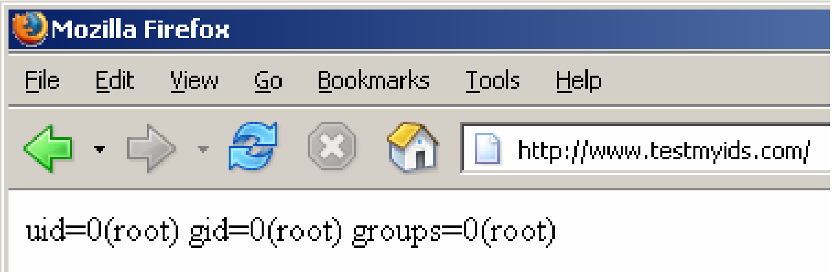
- When prevention succeeds, investigation is not required
  - Nothing about the target changed because traffic was denied



- All other scenarios require investigation
  - Prevention system doesn't recognize attack, permits traffic
  - Passive detection system recognizes attack, triggers alert
  - Passive detection system doesn't recognize attack, ignores it
- Investigation requires having data to analyze

What Do Alerts Really Mean?

- "Intrusion Detection" systems are at best "incident indication" systems providing inferences based on observed events



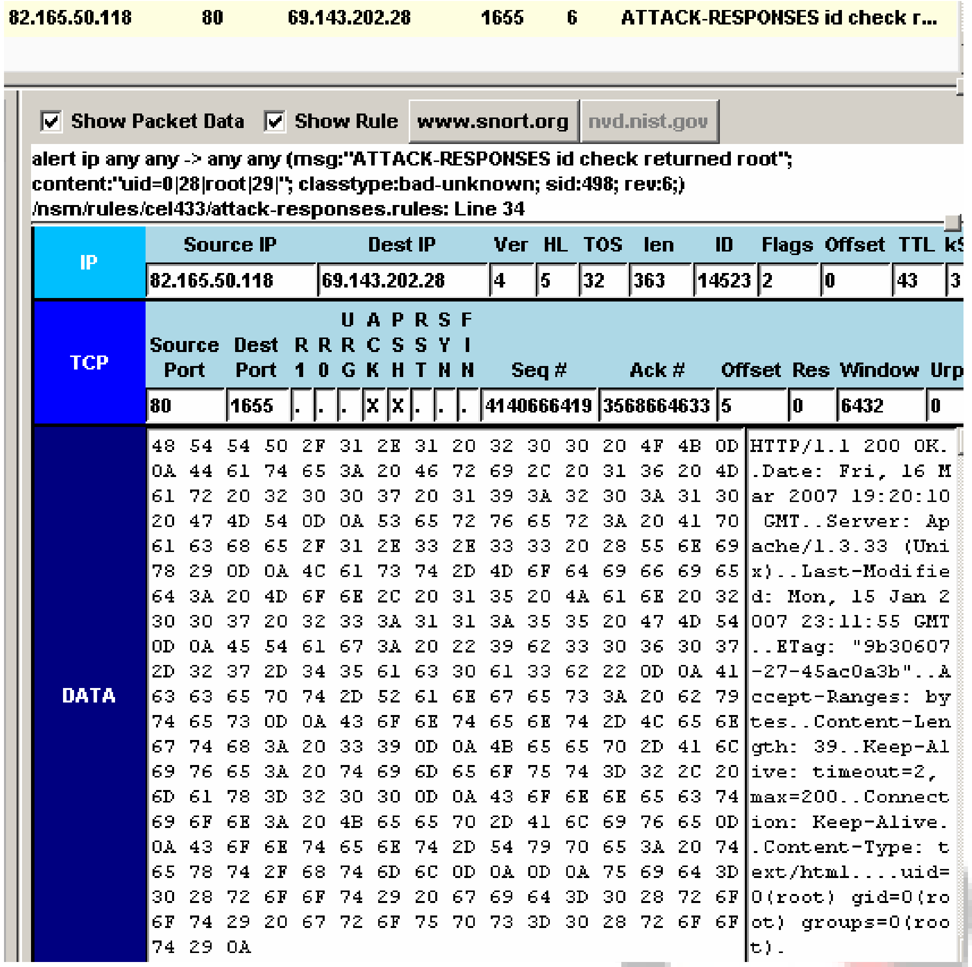
http://www.testmyids.com/

```
uid=0(root) gid=0(root) groups=0(root)
```

User visits www.testmyids.com.

IDS says "I think I saw traffic that I've been programmed to report as the result of running the Unix id command as root. I need to alert."

Replace this example with any of the thousands of alerts that have little to do with the intent of the detection system programmer



```
82.165.50.118     80     69.143.202.28     1655     6     ATTACK-RESPONSES id check r...
```

```
alert ip any any -> any any (msg:"ATTACK-RESPONSES id check returned root";
content:"uid=0|28|root|29|"; classtype:bad-unknown; sid:498; rev:6;)
/nsm/rules/cel433/attack-responses.rules: Line 34
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	k
	82.165.50.118	69.143.202.28	4	5	32	363	14523	2	0	43	3

TCP	Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res	Window	Urp
	80	1655	.	.	.	X	X	.	.	.	4140666419	3568664633	5	0	6432	0

DATA

```
48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D HTTP/1.1 200 OK.
0A 44 61 74 65 3A 20 46 72 69 2C 20 31 36 20 4D .Date: Fri, 16 M
61 72 20 32 30 30 37 20 31 39 3A 32 30 3A 31 30 ar 2007 19:20:10
20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41 70  GMT..Server: Ap
61 63 68 65 2F 31 2E 33 2E 33 33 20 28 55 6E 69 ache/1.3.33 (Uni
78 29 0D 0A 4C 61 73 74 2D 4D 6F 64 69 66 69 65 x)..Last-Modifie
64 3A 20 4D 6F 6E 2C 20 31 35 20 4A 61 6E 20 32 d: Mon, 15 Jan 2
30 30 37 20 32 33 3A 31 31 3A 35 35 20 47 4D 54 007 23:11:55 GMT
0D 0A 45 54 61 67 3A 20 22 39 62 33 30 36 30 37 ..ETag: "9b30607
2D 32 37 2D 34 35 61 63 30 61 33 62 22 0D 0A 41 -27-45ac0a3b"..A
63 63 65 70 74 2D 52 61 6E 67 65 73 3A 20 62 79 ccept-Ranges: by
74 65 73 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E tes..Content-Len
67 74 68 3A 20 33 39 0D 0A 4B 65 65 70 2D 41 6C gth: 39..Keep-Al
69 76 65 3A 20 74 69 6D 65 6F 75 74 3D 32 2C 20 ive: timeout=2,
6D 61 78 3D 32 30 30 0D 0A 43 6F 6E 6E 65 63 74 max=200..Connect
69 6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D ion: Keep-Alive.
0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 .Content-Type: t
65 78 74 2F 68 74 6D 6C 0D 0A 0D 0A 75 69 64 3D ext/html....uid=
30 28 72 6F 6F 74 29 20 67 69 64 3D 30 28 72 6F 0(root) gid=0(ro
6F 74 29 20 67 72 6F 75 70 73 3D 30 28 72 6F 6F ot) groups=0(roo
74 29 0A                                        t).
```

Inferences vs Facts

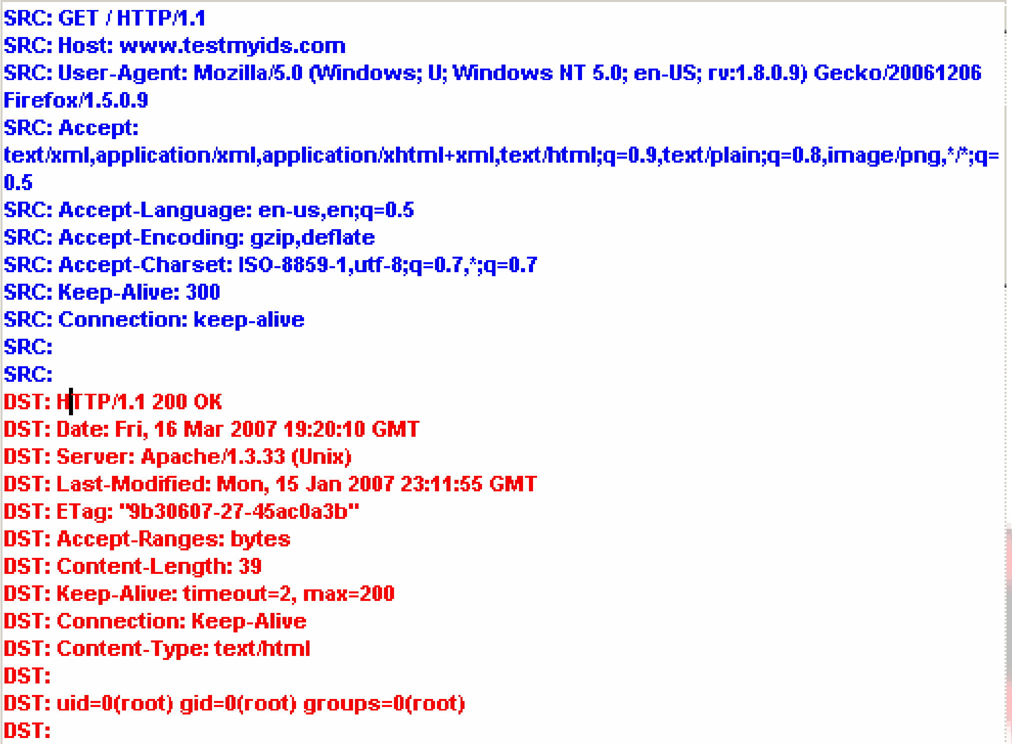
- This alert is an inference

```
------------------------------------------------------------------------
Count:1 Event#1.200816 2007-03-16 19:20:07
ATTACK-RESPONSES id check returned root
82.165.50.118 -> 69.143.202.28
IPVer=4 hlen=5 tos=32 dlen=363 ID=14523 flags=2 offset=0 ttl=43 chksum=33003
Protocol: 6 sport=80 -> dport=1655

Seq=4140666419 Ack=3568664633 Off=5 Res=0 Flags=***AP*** Win=6432 urp=44738 chksum=0
```

- This transcript is a fact

Real intrusion detection implies identifying facts

Which is better: conclusions based on facts or guesses based on assumptions?



```
SRC: GET / HTTP/1.1
SRC: Host: www.testmyids.com
SRC: User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.8.0.9) Gecko/20061206
Firefox/1.5.0.9
SRC: Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=
0.5
SRC: Accept-Language: en-us,en;q=0.5
SRC: Accept-Encoding: gzip,deflate
SRC: Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
SRC: Keep-Alive: 300
SRC: Connection: keep-alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Fri, 16 Mar 2007 19:20:10 GMT
DST: Server: Apache/1.3.33 (Unix)
DST: Last-Modified: Mon, 15 Jan 2007 23:11:55 GMT
DST: ETag: "9b30607-27-45ac0a3b"
DST: Accept-Ranges: bytes
DST: Content-Length: 39
DST: Keep-Alive: timeout=2, max=200
DST: Connection: Keep-Alive
DST: Content-Type: text/html
DST:
DST: uid=0(root) gid=0(root) groups=0(root)
DST:
```

This Is Alert Management, Not Security Investigation

1. Dashboard shows alert
2. Analyst looks at alert
3. Alert does not reveal if attack succeeded
4. Analyst looks for related alerts
5. If any related alerts exist, none reveal if attack succeeded
6. Repeat for next alert starting with Step 1

Analyst sees original alert

ALERT

Queries database for alerts

Database returns single alert

ALERT

Investigation ends

This Is Security Investigation, Not Alert Management

- Investigations with data present many more options

Analyst sees original alert

ALERT

Queries database for alerts

Database returns single alert

ALERT

Queries database for sessions

Analyst sees FTP to retrieve tools

SESSIONS

Reconstructs FTP control and data channels

FULL CONTENT

FTP data channel allows analysis of intruder back door

Queries database for sessions

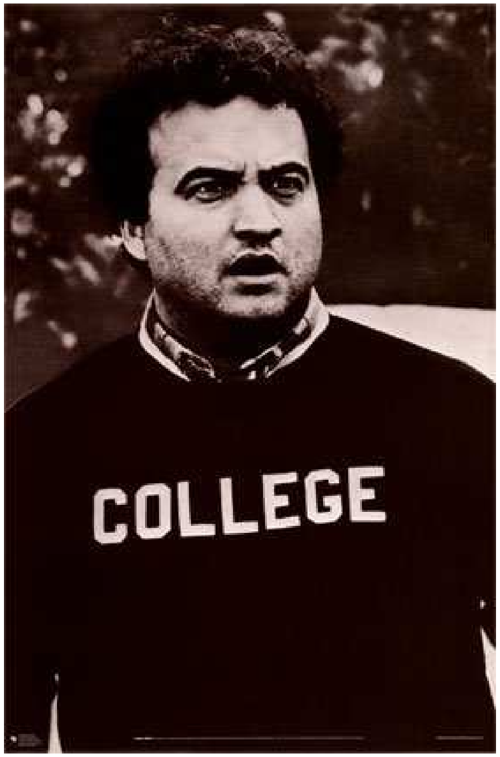
Analyst sees connections to other IPs

SESSIONS

...and the analyst was enlightened

Security Investigation Examples

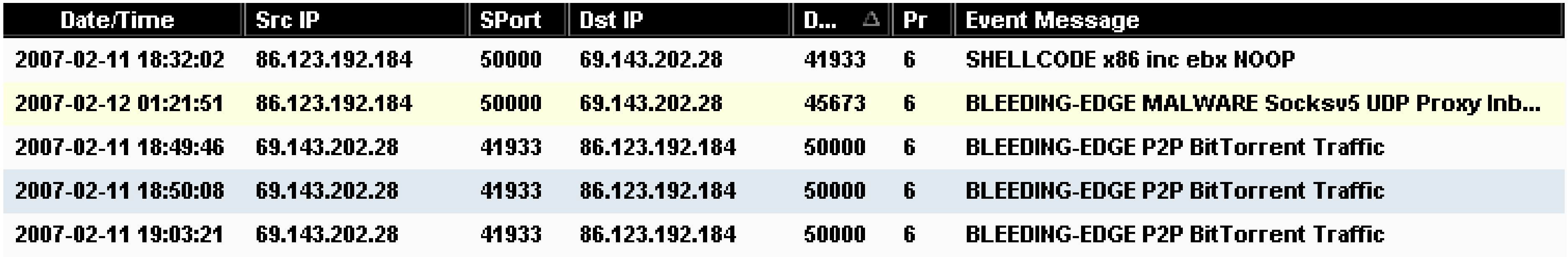
- The following represent cases taken from a network for which I can fully authorize disclosing all event details
- Therefore, it does not represent the latest and greatest, uber-elite hax0r activity I may or may not see elsewhere
- The idea is to demonstrate an investigative methodology where network data is available for investigation



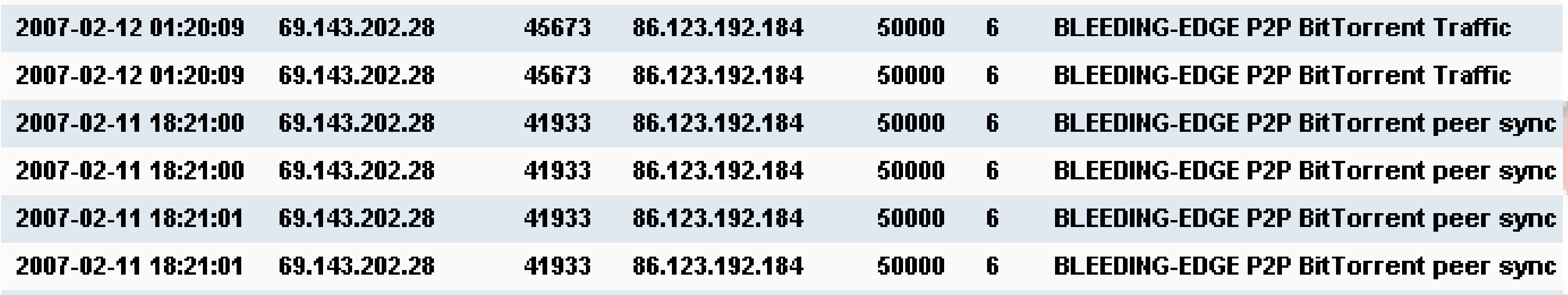
Example 1: Alerts Are Enough

- In this example, other alerts imply the nature of the original alert

```
------------------------------------------------------------------------
Count:1 Event#1.161790 2007-02-12 01:21:51
BLEEDING-EDGE MALWARE Socksv5 UDP Proxy Inbound Connect Request (Linux Source)
86.123.192.184 -> 69.143.202.28
IPVer=4 hlen=5 tos=32 dlen=78 ID=5907 flags=2 offset=0 ttl=37 chksum=6040
Protocol: 6 sport=50000 -> dport=45673

Seq=1162437692 Ack=2046273927 Off=11 Res=0 Flags=***AP*** Win=16022 urp=45361 chksum=0
Payload:
00 00 00 01 03 00 00 00 05 04 00 00 03 0B       ..............
```



Date/Time	Src IP	SPort	Dst IP	D... △	Pr	Event Message
2007-02-11 18:32:02	86.123.192.184	50000	69.143.202.28	41933	6	SHELLCODE x86 inc ebx NOOP
2007-02-12 01:21:51	86.123.192.184	50000	69.143.202.28	45673	6	BLEEDING-EDGE MALWARE Socksv5 UDP Proxy Inb...
2007-02-11 18:49:46	69.143.202.28	41933	86.123.192.184	50000	6	BLEEDING-EDGE P2P BitTorrent Traffic
2007-02-11 18:50:08	69.143.202.28	41933	86.123.192.184	50000	6	BLEEDING-EDGE P2P BitTorrent Traffic
2007-02-11 19:03:21	69.143.202.28	41933	86.123.192.184	50000	6	BLEEDING-EDGE P2P BitTorrent Traffic



2007-02-12 01:20:09	69.143.202.28	45673	86.123.192.184	50000	6	BLEEDING-EDGE P2P BitTorrent Traffic
2007-02-12 01:20:09	69.143.202.28	45673	86.123.192.184	50000	6	BLEEDING-EDGE P2P BitTorrent Traffic
2007-02-11 18:21:00	69.143.202.28	41933	86.123.192.184	50000	6	BLEEDING-EDGE P2P BitTorrent peer sync
2007-02-11 18:21:00	69.143.202.28	41933	86.123.192.184	50000	6	BLEEDING-EDGE P2P BitTorrent peer sync
2007-02-11 18:21:01	69.143.202.28	41933	86.123.192.184	50000	6	BLEEDING-EDGE P2P BitTorrent peer sync
2007-02-11 18:21:01	69.143.202.28	41933	86.123.192.184	50000	6	BLEEDING-EDGE P2P BitTorrent peer sync

Example 2: Alerts Are Not Enough

- Here the alert looks bad and no other alerts exist

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"BLEEDING-EDGE VIRUS
    Win32.Bagle.f (.AH,.AJ,Trojan.Lodear.D) Trojan Activity - download attempt";
    flow:established,to_server; uricontent:"/z.php"; nocase; classtype:trojan-activity;
    reference:url,www.trendmicro.com.au/consumer/vinfo/encyclopedia.php?LYstr=VMAINDATA
    &vNav=3&VName=TROJ_BAGLE.AH;
    reference:url,symantec.com/avcenter/venc/data/trojan.lodear.d.html; sid:2002699;
    rev:2;)
```

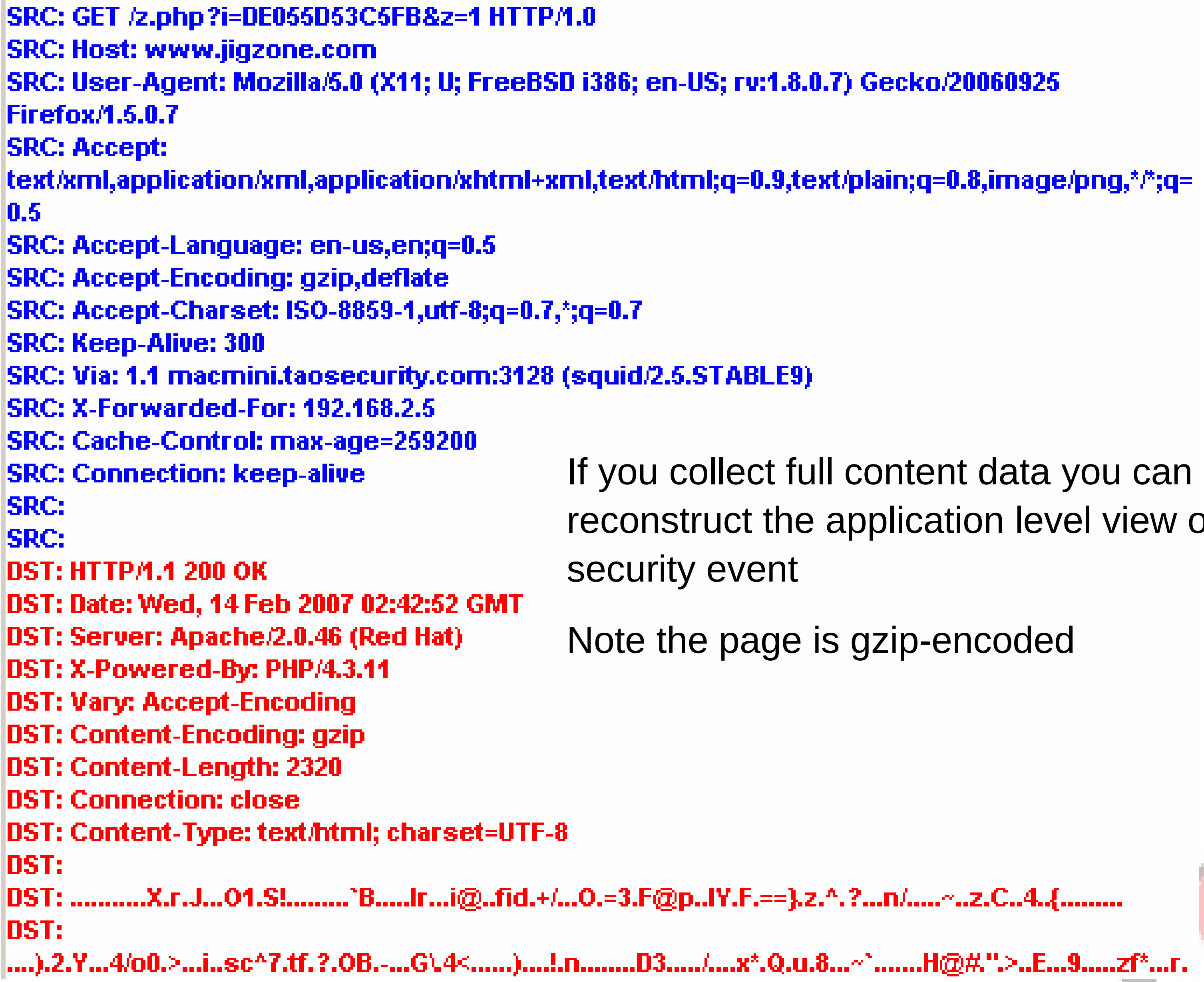
```
------------------------------------------------------------------------
Count:1 Event#1.166468 2007-02-14 02:42:45
BLEEDING-EDGE VIRUS Win32.Bagle.f (.AH,.AJ,Trojan.Lodear.D) Trojan Activity - download
    attempt
69.143.202.28 -> 72.3.247.18
IPVer=4 hlen=5 tos=0 dlen=597 ID=45433 flags=2 offset=0 ttl=63 chksum=14696
Protocol: 6 sport=39684 -> dport=80

Seq=485697299 Ack=4282992985 Off=8 Res=0 Flags=***AP*** Win=5840 urp=31333 chksum=0
Payload:
47 45 54 20 2F 7A 2E 70 68 70 3F 69 3D 44 45 30 GET /z.php?i=DE0
35 35 44 35 33 43 35 46 42 26 7A 3D 31 20 48 54 55D53C5FB&z=1 HT
54 50 2F 31 2E 30 0D 0A 48 6F 73 74 3A 20 77 77 TP/1.0..Host: ww
77 2E 6A 69 67 7A 6F 6E 65 2E 63 6F 6D 0D 0A 55 w.jigzone.com..U
73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C ser-Agent: Mozil
6C 61 2F 35 2E 30 20 28 58 31 31 3B 20 55 3B 20 la/5.0 (X11; U;
46 72 65 65 42 53 44 20 69 33 38 36 3B 20 65 6E FreeBSD i386; en
2D 55 53 3B 20 72 76 3A 31 2E 38 2E 30 2E 37 29 -US; rv:1.8.0.7)
20 47 65 63 6B 6F 2F 32 30 30 36 30 39 32 35 20  Gecko/20060925
46 69 72 65 66 6F 78 2F 31 2E 35 2E 30 2E 37 0D Firefox/1.5.0.7.
...continued...
```

Example 2: Alerts Are Not Enough

```
...continued...
0A 41 63 63 65 70 74 3A 20 74 65 78 74 2F 78 6D .Accept: text/xm
6C 2C 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78 6D l,application/xm
6C 2C 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78 68 l,application/xh
74 6D 6C 2B 78 6D 6C 2C 74 65 78 74 2F 68 74 6D tml+xml,text/htm
6C 3B 71 3D 30 2E 39 2C 74 65 78 74 2F 70 6C 61 l;q=0.9,text/pla
69 6E 3B 71 3D 30 2E 38 2C 69 6D 61 67 65 2F 70 in;q=0.8,image/p
6E 67 2C 2A 2F 2A 3B 71 3D 30 2E 35 0D 0A 41 63 ng,*/*;q=0.5..Ac
63 65 70 74 2D 4C 61 6E 67 75 61 67 65 3A 20 65 cept-Language: e
6E 2D 75 73 2C 65 6E 3B 71 3D 30 2E 35 0D 0A 41 n-us,en;q=0.5..A
63 63 65 70 74 2D 45 6E 63 6F 64 69 6E 67 3A 20 ccept-Encoding: 
67 7A 69 70 2C 64 65 66 6C 61 74 65 0D 0A 41 63 gzip,deflate..Ac
63 65 70 74 2D 43 68 61 72 73 65 74 3A 20 49 53 cept-Charset: IS
4F 2D 38 38 35 39 2D 31 2C 75 74 66 2D 38 3B 71 O-8859-1,utf-8;q
3D 30 2E 37 2C 2A 3B 71 3D 30 2E 37 0D 0A 4B 65 =0.7,*;q=0.7..Ke
65 70 2D 41 6C 69 76 65 3A 20 33 30 30 0D 0A 56 ep-Alive: 300..V
69 61 3A 20 31 2E 31 20 6D 61 63 6D 69 6E 69 2E ia: 1.1 macmini.
74 61 6F 73 65 63 75 72 69 74 79 2E 63 6F 6D 3A taosecurity.com:
33 31 32 38 20 28 73 71 75 69 64 2F 32 2E 35 2E 3128 (squid/2.5.
53 54 41 42 4C 45 39 29 0D 0A 58 2D 46 6F 72 77 STABLE9)..X-Forw
61 72 64 65 64 2D 46 6F 72 3A 20 31 39 32 2E 31 arded-For: 192.1
36 38 2E 32 2E 35 0D 0A 43 61 63 68 65 2D 43 6F 68.2.5..Cache-Co
6E 74 72 6F 6C 3A 20 6D 61 78 2D 61 67 65 3D 32 ntrol: max-age=2
35 39 32 30 30 0D 0A 43 6F 6E 6E 65 63 74 69 6F 59200..Connectio
6E 3A 20 6B 65 65 70 2D 61 6C 69 76 65 0D 0A 0D n: keep-alive...
0A
```

- What are you supposed to do now?

Example 2: Alerts Are Not Enough



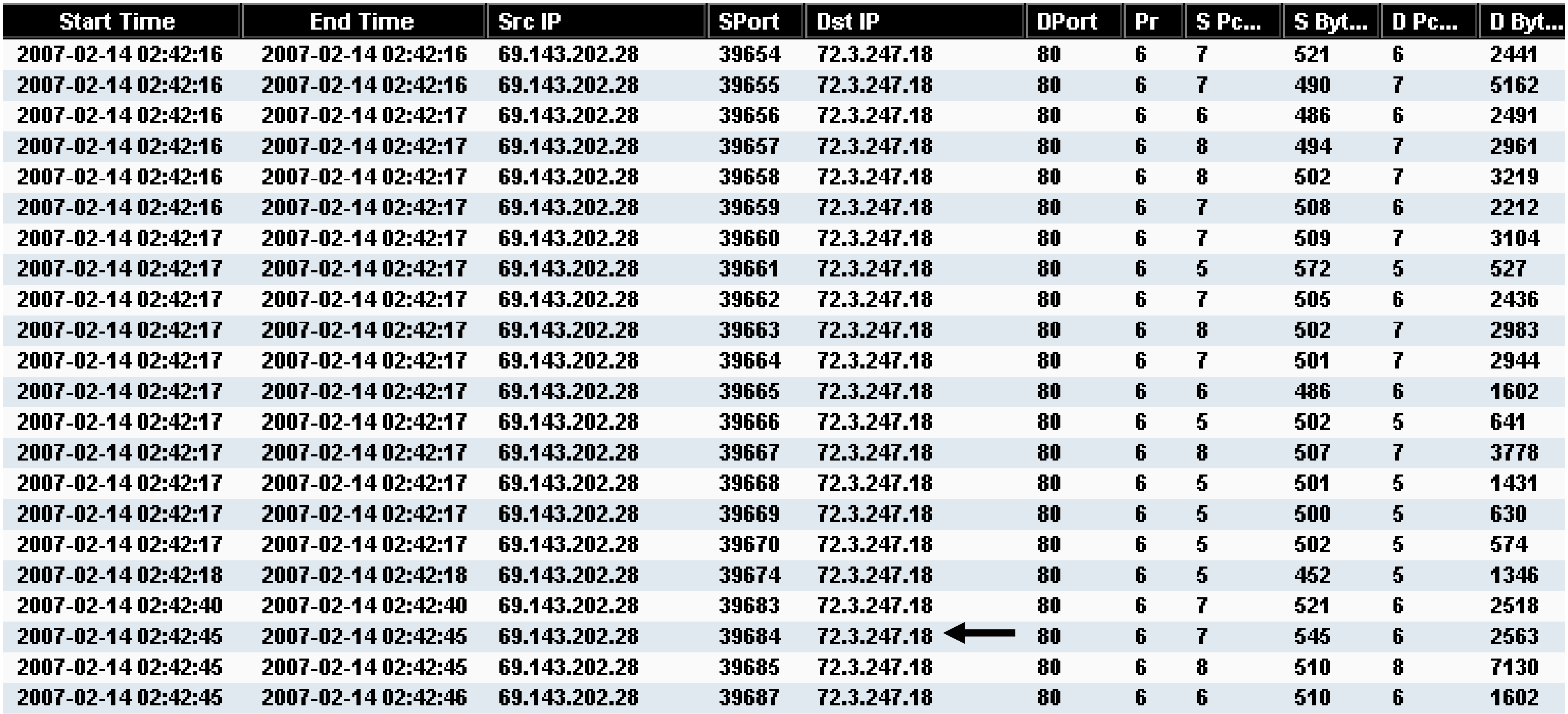
```
SRC: GET /z.php?i=DE055D53C5FB&z=1 HTTP/1.0
SRC: Host: www.jigzone.com
SRC: User-Agent: Mozilla/5.0 (X11; U; FreeBSD i386; en-US; rv:1.8.0.7) Gecko/20060925
Firefox/1.5.0.7
SRC: Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=
0.5
SRC: Accept-Language: en-us,en;q=0.5
SRC: Accept-Encoding: gzip,deflate
SRC: Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
SRC: Keep-Alive: 300
SRC: Via: 1.1 macmini.taosecurity.com:3128 (squid/2.5.STABLE9)
SRC: X-Forwarded-For: 192.168.2.5
SRC: Cache-Control: max-age=259200
SRC: Connection: keep-alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Wed, 14 Feb 2007 02:42:52 GMT
DST: Server: Apache/2.0.46 (Red Hat)
DST: X-Powered-By: PHP/4.3.11
DST: Vary: Accept-Encoding
DST: Content-Encoding: gzip
DST: Content-Length: 2320
DST: Connection: close
DST: Content-Type: text/html; charset=UTF-8
DST:
DST: ..........X.r.J...01.S!.........`B.....lr...i@..fid.+/...0.=3.F@p..lY.F.==}.z.^.?...n/.....~..z.C..4.{.........
DST:
....).2.Y...4/o0.>...i..sc^7.tf.?.OB.-...G\.4<......)....!.n........D3...../....x*.Q.u.8...~`.......H@#.".>..E...9.....zf*...r.
```

If you collect full content data you can reconstruct the application level view of the security event

Note the page is gzip-encoded

Example 2: Alerts Are Not Enough

- If you collect session data you can see other sessions beyond the one indicated by the IDS alert

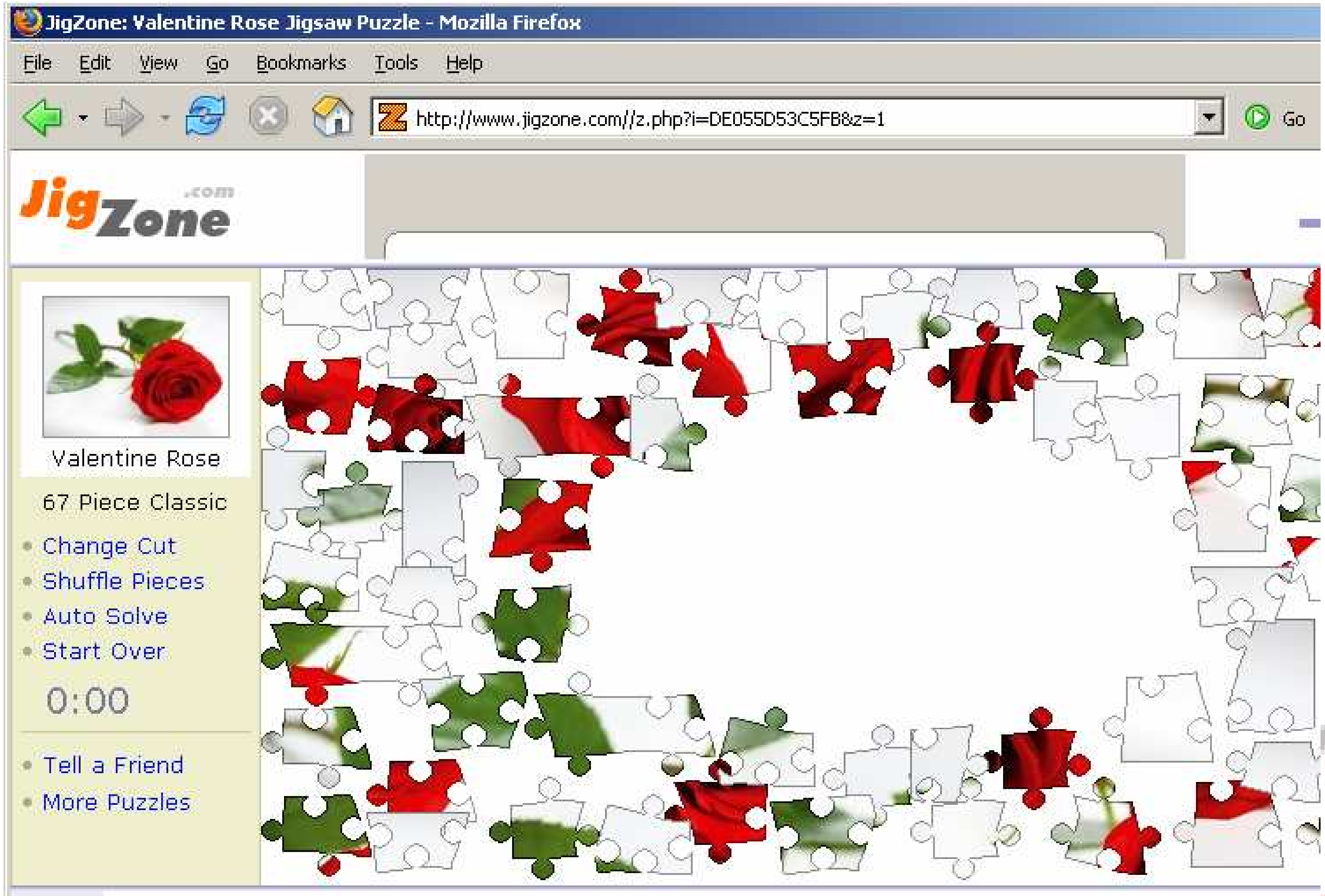


Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pc...	S Byt...	D Pc...	D Byt...
2007-02-14 02:42:16	2007-02-14 02:42:16	69.143.202.28	39654	72.3.247.18	80	6	7	521	6	2441
2007-02-14 02:42:16	2007-02-14 02:42:16	69.143.202.28	39655	72.3.247.18	80	6	7	490	7	5162
2007-02-14 02:42:16	2007-02-14 02:42:17	69.143.202.28	39656	72.3.247.18	80	6	6	486	6	2491
2007-02-14 02:42:16	2007-02-14 02:42:17	69.143.202.28	39657	72.3.247.18	80	6	8	494	7	2961
2007-02-14 02:42:16	2007-02-14 02:42:17	69.143.202.28	39658	72.3.247.18	80	6	8	502	7	3219
2007-02-14 02:42:16	2007-02-14 02:42:17	69.143.202.28	39659	72.3.247.18	80	6	7	508	6	2212
2007-02-14 02:42:17	2007-02-14 02:42:17	69.143.202.28	39660	72.3.247.18	80	6	7	509	7	3104
2007-02-14 02:42:17	2007-02-14 02:42:17	69.143.202.28	39661	72.3.247.18	80	6	5	572	5	527
2007-02-14 02:42:17	2007-02-14 02:42:17	69.143.202.28	39662	72.3.247.18	80	6	7	505	6	2436
2007-02-14 02:42:17	2007-02-14 02:42:17	69.143.202.28	39663	72.3.247.18	80	6	8	502	7	2983
2007-02-14 02:42:17	2007-02-14 02:42:17	69.143.202.28	39664	72.3.247.18	80	6	7	501	7	2944
2007-02-14 02:42:17	2007-02-14 02:42:17	69.143.202.28	39665	72.3.247.18	80	6	6	486	6	1602
2007-02-14 02:42:17	2007-02-14 02:42:17	69.143.202.28	39666	72.3.247.18	80	6	5	502	5	641
2007-02-14 02:42:17	2007-02-14 02:42:17	69.143.202.28	39667	72.3.247.18	80	6	8	507	7	3778
2007-02-14 02:42:17	2007-02-14 02:42:17	69.143.202.28	39668	72.3.247.18	80	6	5	501	5	1431
2007-02-14 02:42:17	2007-02-14 02:42:17	69.143.202.28	39669	72.3.247.18	80	6	5	500	5	630
2007-02-14 02:42:17	2007-02-14 02:42:17	69.143.202.28	39670	72.3.247.18	80	6	5	502	5	574
2007-02-14 02:42:18	2007-02-14 02:42:18	69.143.202.28	39674	72.3.247.18	80	6	5	452	5	1346
2007-02-14 02:42:40	2007-02-14 02:42:40	69.143.202.28	39683	72.3.247.18	80	6	7	521	6	2518
2007-02-14 02:42:45	2007-02-14 02:42:45	69.143.202.28	39684	72.3.247.18 ←	80	6	7	545	6	2563
2007-02-14 02:42:45	2007-02-14 02:42:45	69.143.202.28	39685	72.3.247.18	80	6	8	510	8	7130
2007-02-14 02:42:45	2007-02-14 02:42:46	69.143.202.28	39687	72.3.247.18	80	6	6	510	6	1602

- Is this enough to decide if there is a security problem?

Example 2: Alerts Are Not Enough

- Visiting the URL in the original alert shows a Valentine Rose jigsaw puzzle
- Sometimes solving a case requires reproducing the suspicious activity in a controlled environment

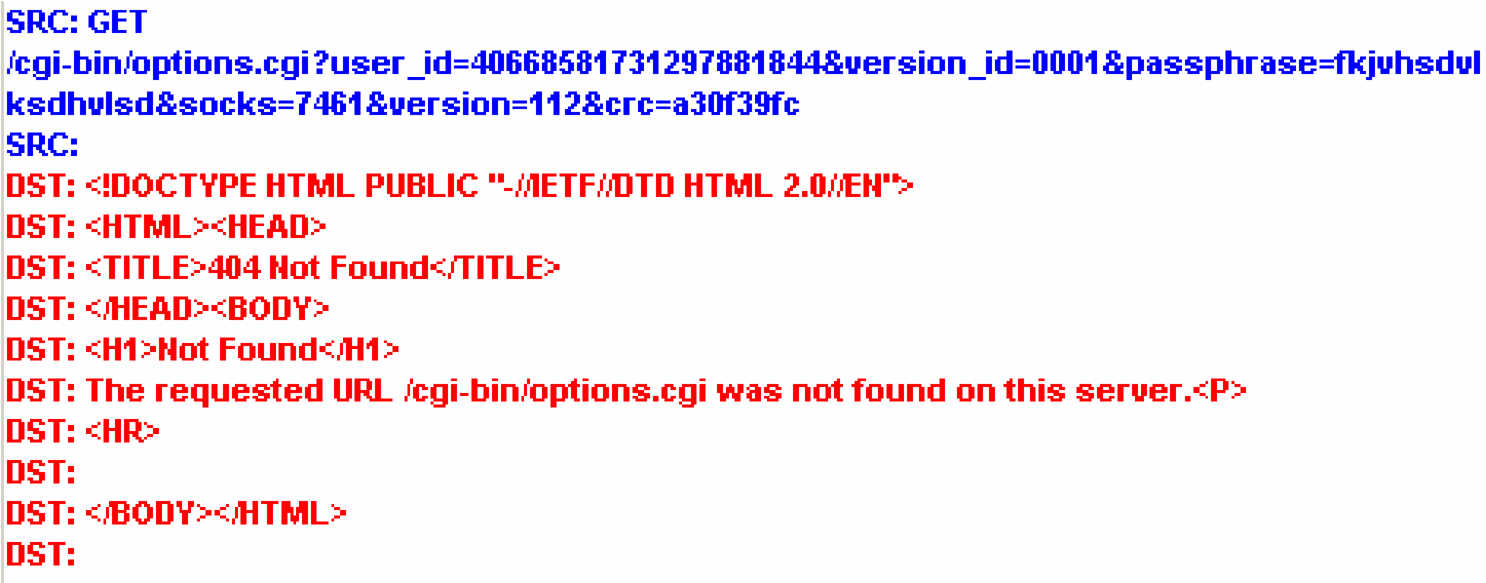


Example 3: What Happened Next?

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"BLEEDING-EDGE TROJAN
    Orderjack Reporting User Activity"; flow:established,to_server;
    uricontent:"options.cgi?user_id="; nocase; uricontent:"&version_id="; nocase;
    uricontent:"&passphrase="; nocase;
    reference:url,www.avira.com/en/threats/section/fulldetails/id_vir/1724/tr_dldr.orde
    rjack.a.html; classtype:trojan-activity; sid:2002854; rev:1;)
/nsm/rules/cel433/bleeding-virus.rules: Line 354

------------------------------------------------------------------------
Count:1 Event#1.175382 2007-02-21 17:32:47
BLEEDING-EDGE TROJAN Orderjack Reporting User Activity
69.143.202.28 -> 81.95.147.107
IPVer=4 hlen=5 tos=0 dlen=187 ID=8939 flags=2 offset=0 ttl=62 chksum=9436
Protocol: 6 sport=58307 -> dport=80

Seq=2867320777 Ack=3541503528 Off=8 Res=0 Flags=***AP*** Win=33304 urp=48386 chksum=0
Payload:
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 6F 70 74 GET /cgi-bin/opt
69 6F 6E 73 2E 63 67 69 3F 75 73 65 72 5F 69 64 ions.cgi?user_id
3D 34 30 36 36 38 35 38 31 37 33 31 32 39 37 38 =4066858173129 78
38 31 38 34 34 26 76 65 72 73 69 6F 6E 5F 69 64 81844&version_id
3D 30 30 30 31 26 70 61 73 73 70 68 72 61 73 65 =0001&passphrase
3D 66 6B 6A 76 68 73 64 76 6C 6B 73 64 68 76 6C =fkjvhsdvlksdhvl
73 64 26 73 6F 63 6B 73 3D 37 34 36 31 26 76 65 sd&socks=7461&ve
72 73 69 6F 6E 3D 31 31 32 26 63 72 63 3D 61 33 rsion=112&crc=a3
30 66 33 39 66 63 0A                            0f39fc.
```

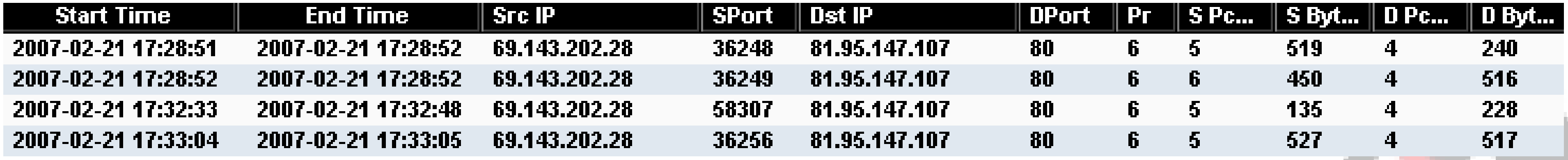
Example 3: What Happened Next?

- Full content data shows the response from the Web server that options.cgi is unavailable, so the victim *may not* have reported its status



```
SRC: GET
/cgi-bin/options.cgi?user_id=40668581731297881844&version_id=0001&passphrase=fkjvhsdvl
ksdhvlsd&socks=7461&version=112&crc=a30f39fc
SRC:
DST: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
DST: <HTML><HEAD>
DST: <TITLE>404 Not Found</TITLE>
DST: </HEAD><BODY>
DST: <H1>Not Found</H1>
DST: The requested URL /cgi-bin/options.cgi was not found on this server.<P>
DST: <HR>
DST:
DST: </BODY></HTML>
DST:
```

- Session data reveals the extent of the network-based evidence

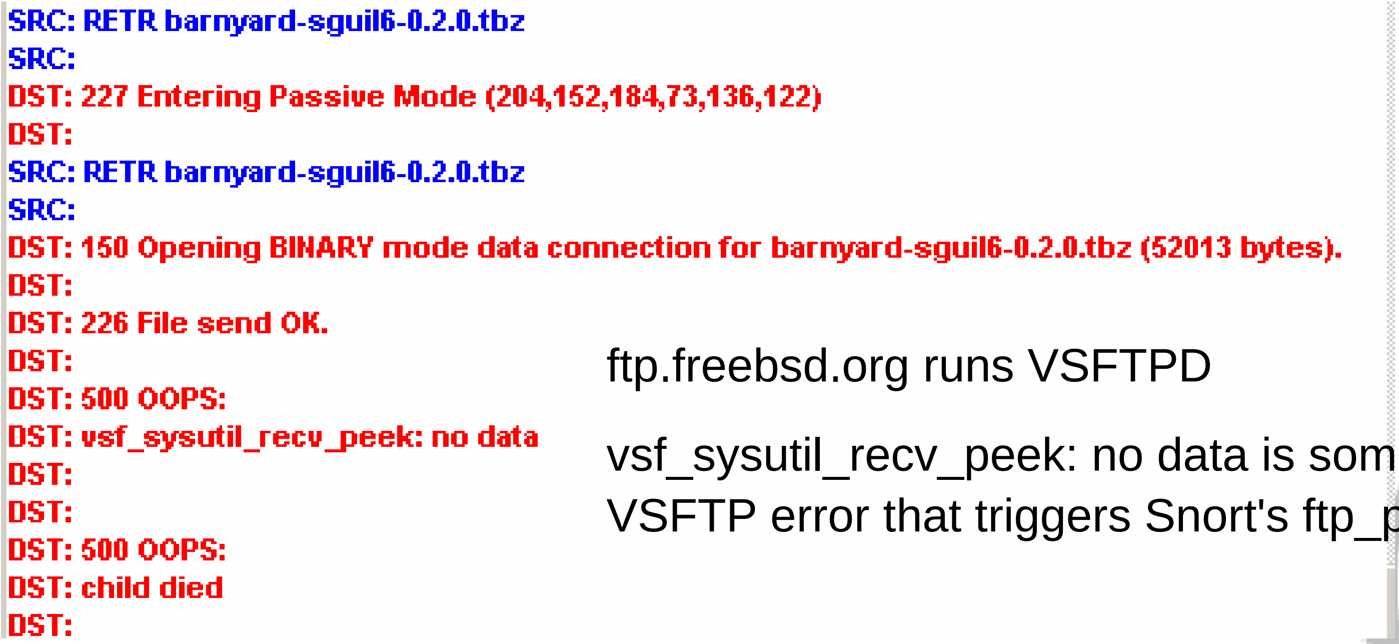


Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pc...	S Byt...	D Pc...	D Byt...
2007-02-21 17:28:51	2007-02-21 17:28:52	69.143.202.28	36248	81.95.147.107	80	6	5	519	4	240
2007-02-21 17:28:52	2007-02-21 17:28:52	69.143.202.28	36249	81.95.147.107	80	6	6	450	4	516
2007-02-21 17:32:33	2007-02-21 17:32:48	69.143.202.28	58307	81.95.147.107	80	6	5	135	4	228
2007-02-21 17:33:04	2007-02-21 17:33:05	69.143.202.28	36256	81.95.147.107	80	6	5	527	4	517

Example 4: Protocol Analysis Preprocessors

```
-----------------------------------------------------------------------
Count:1 Event#1.167160 2007-02-14 18:08:07
ftp_pp: FTP command channel encrypted
204.152.184.73 -> 69.143.202.28
IPVer=4 hlen=5 tos=32 dlen=82 ID=44797 flags=2 offset=0 ttl=38 chksum=4347
Protocol: 6 sport=21 -> dport=57229

Seq=3439200498 Ack=3554780672 Off=8 Res=0 Flags=***AP*** Win=65535 urp=57883 chksum=0
Payload:
76 73 66 5F 73 79 73 75 74 69 6C 5F 72 65 63 76 vsf_sysutil_recv
5F 70 65 65 6B 3A 20 6E 6F 20 64 61 74 61       _peek: no data
```

- Full content data shows a normal FTP retrieval of a FreeBSD package



```
SRC: RETR barnyard-sguil6-0.2.0.tbz
SRC:
DST: 227 Entering Passive Mode (204,152,184,73,136,122)
DST:
SRC: RETR barnyard-sguil6-0.2.0.tbz
SRC:
DST: 150 Opening BINARY mode data connection for barnyard-sguil6-0.2.0.tbz (52013 bytes).
DST:
DST: 226 File send OK.
DST:
DST: 500 OOPS:
DST: vsf_sysutil_recv_peek: no data
DST:
DST:
DST: 500 OOPS:
DST: child died
DST:
```

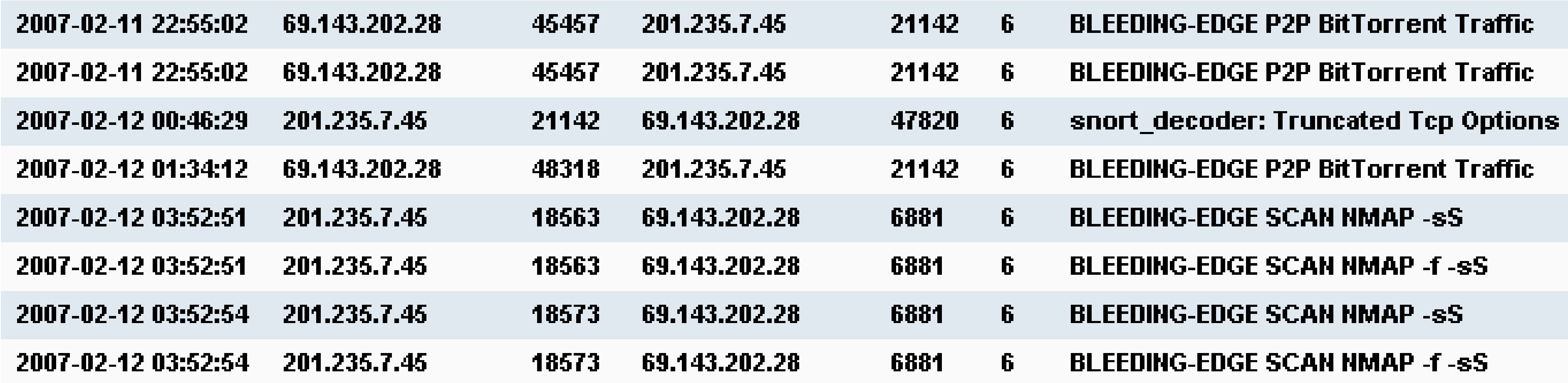
ftp.freebsd.org runs VSFTPD

vsf_sysutil_recv_peek: no data is some VSFTP error that triggers Snort's ftp_pp

Example 5: So You Like TCP Options...

```
------------------------------------------------------------------------
Count:1 Event#1.161610 2007-02-12 00:46:29
snort_decoder: Truncated Tcp Options
201.235.7.45 -> 69.143.202.28
IPVer=4 hlen=5 tos=32 dlen=64 ID=55026 flags=2 offset=0 ttl=103 chksum=23521
Protocol: 6 sport=21142 -> dport=47820

Seq=3375965127 Ack=557227574 Off=11 Res=0 Flags=***A**** Win=17520 urp=25587 chksum=0
Payload:
None.
```

- A check for other alerts involving the same source show P2P activity

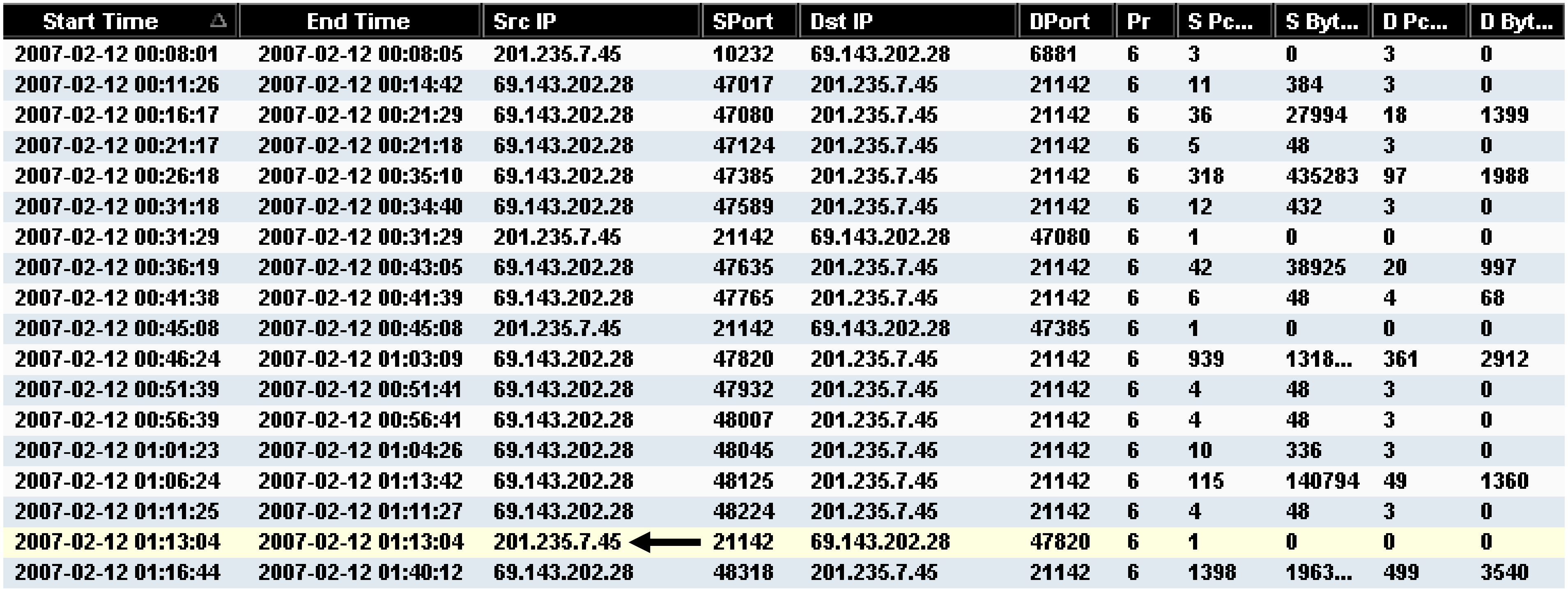


2007-02-11 22:55:02	69.143.202.28	45457	201.235.7.45	21142	6	BLEEDING-EDGE P2P BitTorrent Traffic
2007-02-11 22:55:02	69.143.202.28	45457	201.235.7.45	21142	6	BLEEDING-EDGE P2P BitTorrent Traffic
2007-02-12 00:46:29	201.235.7.45	21142	69.143.202.28	47820	6	snort_decoder: Truncated Tcp Options
2007-02-12 01:34:12	69.143.202.28	48318	201.235.7.45	21142	6	BLEEDING-EDGE P2P BitTorrent Traffic
2007-02-12 03:52:51	201.235.7.45	18563	69.143.202.28	6881	6	BLEEDING-EDGE SCAN NMAP -sS
2007-02-12 03:52:51	201.235.7.45	18563	69.143.202.28	6881	6	BLEEDING-EDGE SCAN NMAP -f -sS
2007-02-12 03:52:54	201.235.7.45	18573	69.143.202.28	6881	6	BLEEDING-EDGE SCAN NMAP -sS
2007-02-12 03:52:54	201.235.7.45	18573	69.143.202.28	6881	6	BLEEDING-EDGE SCAN NMAP -f -sS

- The so-called Nmap alerts are P2P-related too

Example 5: So You Like TCP Options...

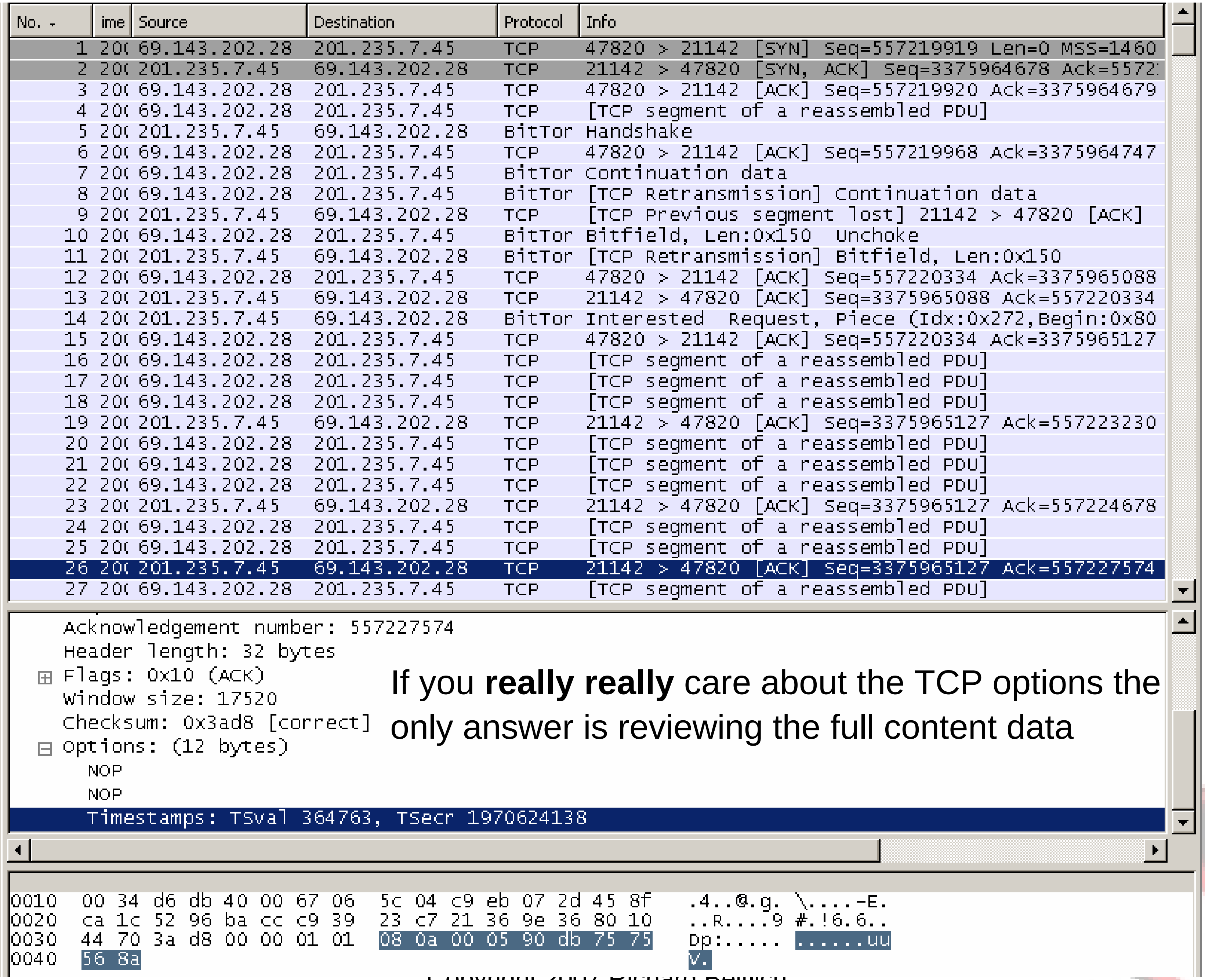
- If you are really paranoid you can look for other sessions involving the source IP



Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pc...	S Byt...	D Pc...	D Byt...
2007-02-12 00:08:01	2007-02-12 00:08:05	201.235.7.45	10232	69.143.202.28	6881	6	3	0	3	0
2007-02-12 00:11:26	2007-02-12 00:14:42	69.143.202.28	47017	201.235.7.45	21142	6	11	384	3	0
2007-02-12 00:16:17	2007-02-12 00:21:29	69.143.202.28	47080	201.235.7.45	21142	6	36	27994	18	1399
2007-02-12 00:21:17	2007-02-12 00:21:18	69.143.202.28	47124	201.235.7.45	21142	6	5	48	3	0
2007-02-12 00:26:18	2007-02-12 00:35:10	69.143.202.28	47385	201.235.7.45	21142	6	318	435283	97	1988
2007-02-12 00:31:18	2007-02-12 00:34:40	69.143.202.28	47589	201.235.7.45	21142	6	12	432	3	0
2007-02-12 00:31:29	2007-02-12 00:31:29	201.235.7.45	21142	69.143.202.28	47080	6	1	0	0	0
2007-02-12 00:36:19	2007-02-12 00:43:05	69.143.202.28	47635	201.235.7.45	21142	6	42	38925	20	997
2007-02-12 00:41:38	2007-02-12 00:41:39	69.143.202.28	47765	201.235.7.45	21142	6	6	48	4	68
2007-02-12 00:45:08	2007-02-12 00:45:08	201.235.7.45	21142	69.143.202.28	47385	6	1	0	0	0
2007-02-12 00:46:24	2007-02-12 01:03:09	69.143.202.28	47820	201.235.7.45	21142	6	939	1318...	361	2912
2007-02-12 00:51:39	2007-02-12 00:51:41	69.143.202.28	47932	201.235.7.45	21142	6	4	48	3	0
2007-02-12 00:56:39	2007-02-12 00:56:41	69.143.202.28	48007	201.235.7.45	21142	6	4	48	3	0
2007-02-12 01:01:23	2007-02-12 01:04:26	69.143.202.28	48045	201.235.7.45	21142	6	10	336	3	0
2007-02-12 01:06:24	2007-02-12 01:13:42	69.143.202.28	48125	201.235.7.45	21142	6	115	140794	49	1360
2007-02-12 01:11:25	2007-02-12 01:11:27	69.143.202.28	48224	201.235.7.45	21142	6	4	48	3	0
2007-02-12 01:13:04	2007-02-12 01:13:04	201.235.7.45	21142	69.143.202.28	47820	6	1	0	0	0
2007-02-12 01:16:44	2007-02-12 01:40:12	69.143.202.28	48318	201.235.7.45	21142	6	1398	1963...	499	3540

- Port 21142 TCP and 6881 TCP indicate P2P activity

Example 5: So You Like TCP Options...



```
No. ▾   ime Source          Destination     Protocol Info
    1 20( 69.143.202.28   201.235.7.45    TCP      47820 > 21142 [SYN] Seq=557219919 Len=0 MSS=1460
    2 20( 201.235.7.45    69.143.202.28   TCP      21142 > 47820 [SYN, ACK] Seq=3375964678 Ack=5572:
    3 20( 69.143.202.28   201.235.7.45    TCP      47820 > 21142 [ACK] Seq=557219920 Ack=3375964679
    4 20( 69.143.202.28   201.235.7.45    TCP      [TCP segment of a reassembled PDU]
    5 20( 201.235.7.45    69.143.202.28   BitTor   Handshake
    6 20( 69.143.202.28   201.235.7.45    TCP      47820 > 21142 [ACK] Seq=557219968 Ack=3375964747
    7 20( 69.143.202.28   201.235.7.45    BitTor   Continuation data
    8 20( 69.143.202.28   201.235.7.45    BitTor   [TCP Retransmission] Continuation data
    9 20( 201.235.7.45    69.143.202.28   TCP      [TCP Previous segment lost] 21142 > 47820 [ACK]
   10 20( 69.143.202.28   201.235.7.45    BitTor   Bitfield, Len:0x150  Unchoke
   11 20( 201.235.7.45    69.143.202.28   BitTor   [TCP Retransmission] Bitfield, Len:0x150
   12 20( 69.143.202.28   201.235.7.45    TCP      47820 > 21142 [ACK] Seq=557220334 Ack=3375965088
   13 20( 201.235.7.45    69.143.202.28   TCP      21142 > 47820 [ACK] Seq=3375965088 Ack=557220334
   14 20( 201.235.7.45    69.143.202.28   BitTor   Interested  Request, Piece (Idx:0x272,Begin:0x80
   15 20( 69.143.202.28   201.235.7.45    TCP      47820 > 21142 [ACK] Seq=557220334 Ack=3375965127
   16 20( 69.143.202.28   201.235.7.45    TCP      [TCP segment of a reassembled PDU]
   17 20( 69.143.202.28   201.235.7.45    TCP      [TCP segment of a reassembled PDU]
   18 20( 69.143.202.28   201.235.7.45    TCP      [TCP segment of a reassembled PDU]
   19 20( 201.235.7.45    69.143.202.28   TCP      21142 > 47820 [ACK] Seq=3375965127 Ack=557223230
   20 20( 69.143.202.28   201.235.7.45    TCP      [TCP segment of a reassembled PDU]
   21 20( 69.143.202.28   201.235.7.45    TCP      [TCP segment of a reassembled PDU]
   22 20( 69.143.202.28   201.235.7.45    TCP      [TCP segment of a reassembled PDU]
   23 20( 201.235.7.45    69.143.202.28   TCP      21142 > 47820 [ACK] Seq=3375965127 Ack=557224678
   24 20( 69.143.202.28   201.235.7.45    TCP      [TCP segment of a reassembled PDU]
   25 20( 69.143.202.28   201.235.7.45    TCP      [TCP segment of a reassembled PDU]
   26 20( 201.235.7.45    69.143.202.28   TCP      21142 > 47820 [ACK] Seq=3375965127 Ack=557227574
   27 20( 69.143.202.28   201.235.7.45    TCP      [TCP segment of a reassembled PDU]
```

```
    Acknowledgement number: 557227574
    Header length: 32 bytes
 ⊞ Flags: 0x10 (ACK)
    Window size: 17520
    Checksum: 0x3ad8 [correct]
 ⊟ Options: (12 bytes)
      NOP
      NOP
      Timestamps: TSval 364763, TSecr 1970624138
```

```
0010  00 34 d6 db 40 00 67 06  5c 04 c9 eb 07 2d 45 8f   .4..@.g. \....-E.
0020  ca 1c 52 96 ba cc c9 39  23 c7 21 36 9e 36 80 10   ..R....9 #.!6.6..
0030  44 70 3a d8 00 00 01 01  08 0a 00 05 90 db 75 75   Dp:..... ......uu
0040  56 8a                                              V.
```

If you **really really** care about the TCP options the only answer is reviewing the full content data

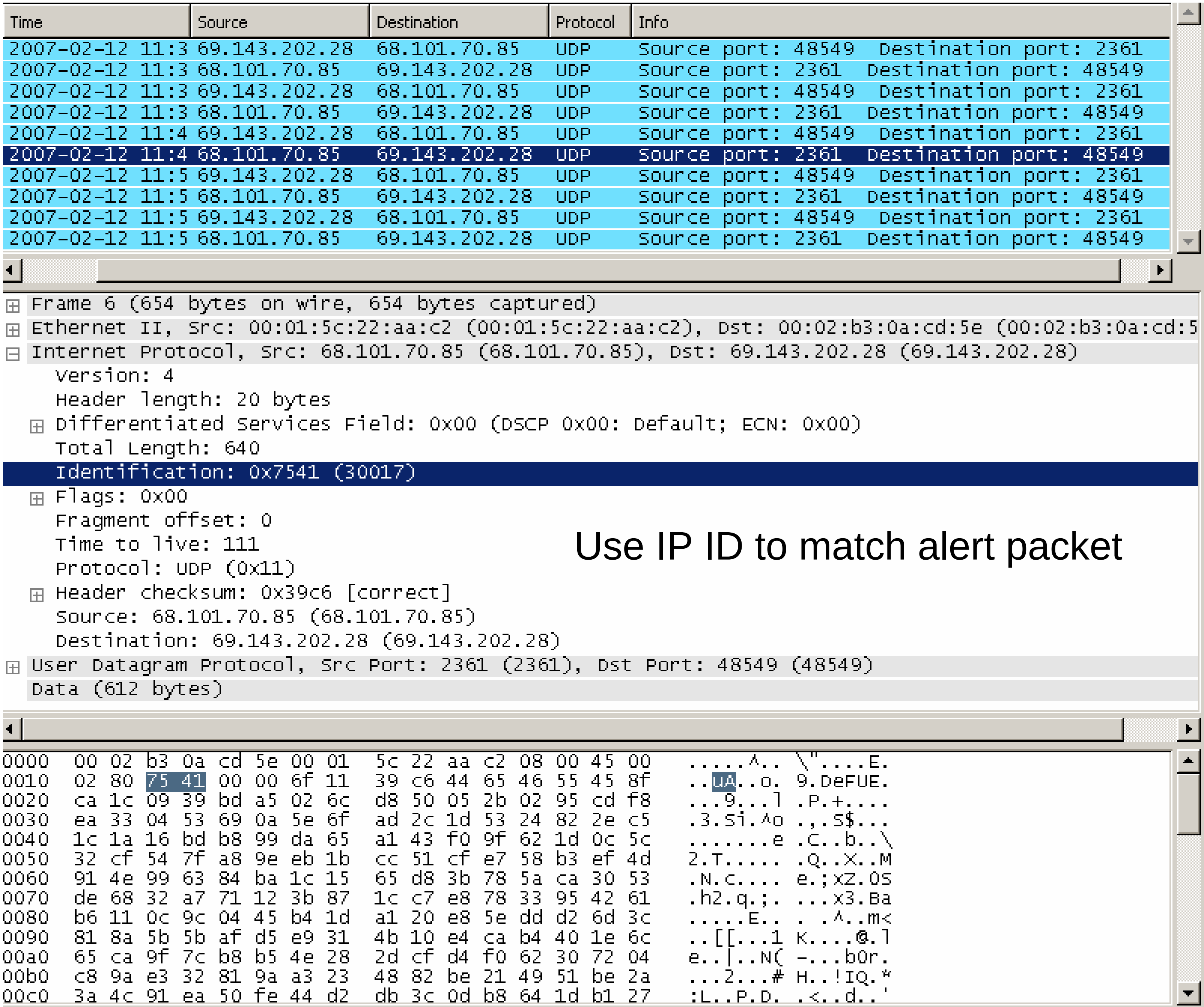
Example 6: Odd UDP Traffic

```
alert udp $EXTERNAL_NET any -> $SQL_SERVERS any (msg:"MS-SQL probe response overflow
    attempt"; content:"|05|"; depth:1; byte_test:2,>,512,1; content:"|3B|"; distance:0;
    isdataat:512,relative; content:!"|3B|"; within:512; reference:bugtraq,9407;
    reference:cve,2003-0903; reference:nessus,11990;
    reference:url,www.microsoft.com/technet/security/bulletin/MS04-003.mspx;
    classtype:attempted-user; sid:2329; rev:7;)
/nsm/rules/cel433/sql.rules: Line 66

------------------------------------------------------------------------
Count:1 Event#1.164746 2007-02-12 16:44:49
MS-SQL probe response overflow attempt
68.101.70.85 -> 69.143.202.28
IPVer=4 hlen=5 tos=0 dlen=640 ID=30017 flags=0 offset=0 ttl=111 chksum=14790
Protocol: 17 sport=2361 -> dport=48549

len=620 chksum=55376
Payload:
05 2B 02 95 CD F8 EA 33 04 53 69 0A 5E 6F AD 2C .+.....3.Si.^o.,
1D 53 24 82 2E C5 1C 1A 16 BD B8 99 DA 65 A1 43 .S$..........e.C
F0 9F 62 1D 0C 5C 32 CF 54 7F A8 9E EB 1B CC 51 ..b..\2.T......Q
CF E7 58 B3 EF 4D 91 4E 99 63 84 BA 1C 15 65 D8 ..X..M.N.c....e.
3B 78 5A CA 30 53 DE 68 32 A7 71 12 3B 87 1C C7 ;xZ.0S.h2.q.;...
E8 78 33 95 42 61 B6 11 0C 9C 04 45 B4 1D A1 20 .x3.Ba.....E...
E8 5E DD D2 6D 3C 81 8A 5B 5B AF D5 E9 31 4B 10 .^..m<..[[...1K.
E4 CA B4 40 1E 6C 65 CA 9F 7C B8 B5 4E 28 2D CF ...@.le..|..N(-.
D4 F0 62 30 72 04 C8 9A E3 32 81 9A A3 23 48 82 ..b0r....2...#H.
BE 21 49 51 BE 2A 3A 4C 91 EA 50 FE 44 D2 DB 3C .!IQ.*:L..P.D..<
0D B8 64 1D B1 27 22 91 B6 54 2C E1 0E B0 AF 2E ..d..'"..T,.....
...continued...
```

Example 6: Odd UDP Traffic

```
...continued...
A9 15 4E 51 FC E6 63 59 8E BA 96 E2 34 AE BE AD ..NQ..cY....4...
68 A1 8A F3 AB D7 A4 E5 FC EC 09 1E 7C FF 1C 92 h...........|...
4B 70 D0 FB 18 30 61 DB 6F AE 89 4F AA 33 29 50 Kp...0a.o..O.3)P
0C 4A DC 42 4A BC FB 38 70 D5 75 2D B2 4F A6 5E .J.BJ..8p.u-.O.^
76 06 6F 03 17 86 C2 BA 83 9B 90 91 6F E4 23 BF v.o.........o.#.
B3 51 A2 17 6F 59 1E A1 E7 0C 5C 9B BF 5D 1D 45 .Q..oY....\..].E
7A 45 30 EA 8E E6 9E FA 02 BD 9F 4F 44 9A 64 CC zE0........OD.d.
2A C2 8C 4B A9 17 E0 04 33 13 FE B0 8F F2 3A CD *..K....3.....:.
FC 45 98 F8 64 17 5D D2 1D 5F 76 9E 53 E9 CA AA .E..d.].._v.S...
6D 84 2B 98 87 8A 9F 72 FD C4 84 C4 27 15 45 42 m.+....r....'.EB
B1 27 54 5A 99 E7 C1 43 81 4C F1 64 70 20 BB 02 .'TZ...C.L.dp ..
4B 4D F6 CE DC 64 69 71 2A 79 5D F3 30 D4 DD DB KM...diq*y].0...
68 D9 DD 8A 62 A1 EB 17 1B B1 82 A5 B8 8D EA F6 h...b...........
4C 4C 99 AB 2E BC 33 CB 89 B0 4F 0F 30 E6 E1 6B LL....3...O.0..k
1A 5B D1 CC 8A 0A D1 25 00 77 EB 11 EF 9F 0E AC .[.....%.w......
95 AC 78 16 7E 86 92 F8 1A D6 22 09 B6 8F 1D 72 ..x.~....."....r
01 D4 8F 43 CF 17 53 5E 70 64 7C 7E 27 5B B1 AD ...C..S^pd|~'[..
A3 02 7D D7 58 7A AC CD E2 1B 11 00 CC 0E 08 AF ..}.Xz..........
40 B7 36 E5 61 12 50 8C 36 D4 1E A8 58 81 58 54 @.6.a.P.6...X.XT
D9 8C F5 B6 44 95 D7 A2 34 CE 0C 89 DD 06 2B 6A ....D...4.....+j
E2 F9 34 28 26 31 21 D5 D6 0B 60 CD 5B 28 A3 8B ..4(&1!...`.[(..
7C AF 41 52 AB 11 C4 72 FB C8 26 A5 E0 0D 89 84 |.AR...r..&.....
18 99 93 5C CC 5E 52 51 1C 29 CC 68 A2 86 F1 41 ...\.^RQ.).h...A
C6 F4 37 23 E0 5F B9 89 E0 C1 AB F2 1E 04 1A D7 ..7#._..........
FA 78 4D AC 39 A2 2F CE CB BF 99 B7 5A 2E E8 75 .xM.9./.....Z..u
E0 75 3E 04 F2 12 08 A4 43 EB 42 9A 44 DD 3A 37 .u>.....C.B.D.:7
58 4D FA 19 E1 E8 E5 F7 26 F4 CD 6D BB CA F9 10 XM......&..m....
1B 62 2B A4                                     .b+.
```

Example 6: Odd UDP Traffic



Time	Source	Destination	Protocol	Info
2007-02-12 11:3	69.143.202.28	68.101.70.85	UDP	Source port: 48549 Destination port: 2361
2007-02-12 11:3	68.101.70.85	69.143.202.28	UDP	Source port: 2361 Destination port: 48549
2007-02-12 11:3	69.143.202.28	68.101.70.85	UDP	Source port: 48549 Destination port: 2361
2007-02-12 11:3	68.101.70.85	69.143.202.28	UDP	Source port: 2361 Destination port: 48549
2007-02-12 11:4	69.143.202.28	68.101.70.85	UDP	Source port: 48549 Destination port: 2361
2007-02-12 11:4	68.101.70.85	69.143.202.28	UDP	Source port: 2361 Destination port: 48549
2007-02-12 11:5	69.143.202.28	68.101.70.85	UDP	Source port: 48549 Destination port: 2361
2007-02-12 11:5	68.101.70.85	69.143.202.28	UDP	Source port: 2361 Destination port: 48549
2007-02-12 11:5	69.143.202.28	68.101.70.85	UDP	Source port: 48549 Destination port: 2361
2007-02-12 11:5	68.101.70.85	69.143.202.28	UDP	Source port: 2361 Destination port: 48549

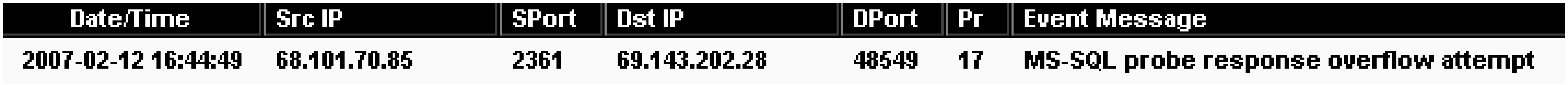
```
⊞ Frame 6 (654 bytes on wire, 654 bytes captured)
⊞ Ethernet II, Src: 00:01:5c:22:aa:c2 (00:01:5c:22:aa:c2), Dst: 00:02:b3:0a:cd:5e (00:02:b3:0a:cd:5
⊟ Internet Protocol, Src: 68.101.70.85 (68.101.70.85), Dst: 69.143.202.28 (69.143.202.28)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 640
    Identification: 0x7541 (30017)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 111
    Protocol: UDP (0x11)
  ⊞ Header checksum: 0x39c6 [correct]
    Source: 68.101.70.85 (68.101.70.85)
    Destination: 69.143.202.28 (69.143.202.28)
⊞ User Datagram Protocol, Src Port: 2361 (2361), Dst Port: 48549 (48549)
  Data (612 bytes)
```

Use IP ID to match alert packet

```
0000  00 02 b3 0a cd 5e 00 01  5c 22 aa c2 08 00 45 00   .....^.. \"....E.
0010  02 80 75 41 00 00 6f 11  39 c6 44 65 46 55 45 8f   ..uA..o. 9.DeFUE.
0020  ca 1c 09 39 bd a5 02 6c  d8 50 05 2b 02 95 cd f8   ...9...l .P.+....
0030  ea 33 04 53 69 0a 5e 6f  ad 2c 1d 53 24 82 2e c5   .3.Si.^o .,.S$...
0040  1c 1a 16 bd b8 99 da 65  a1 43 f0 9f 62 1d 0c 5c   .......e .C..b..\
0050  32 cf 54 7f a8 9e eb 1b  cc 51 cf e7 58 b3 ef 4d   2.T..... .Q..X..M
0060  91 4e 99 63 84 ba 1c 15  65 d8 3b 78 5a ca 30 53   .N.c.... e.;xZ.0S
0070  de 68 32 a7 71 12 3b 87  1c c7 e8 78 33 95 42 61   .h2.q.;. ...x3.Ba
0080  b6 11 0c 9c 04 45 b4 1d  a1 20 e8 5e dd d2 6d 3c   .....E.. . .^..m<
0090  81 8a 5b 5b af d5 e9 31  4b 10 e4 ca b4 40 1e 6c   ..[[...1 K....@.l
00a0  65 ca 9f 7c b8 b5 4e 28  2d cf d4 f0 62 30 72 04   e..|..N( -...b0r.
00b0  c8 9a e3 32 81 9a a3 23  48 82 be 21 49 51 be 2a   ...2...# H..!IQ.*
00c0  3a 4c 91 ea 50 fe 44 d2  db 3c 0d b8 64 1d b1 27   :L..P.D. .<..d..'
```

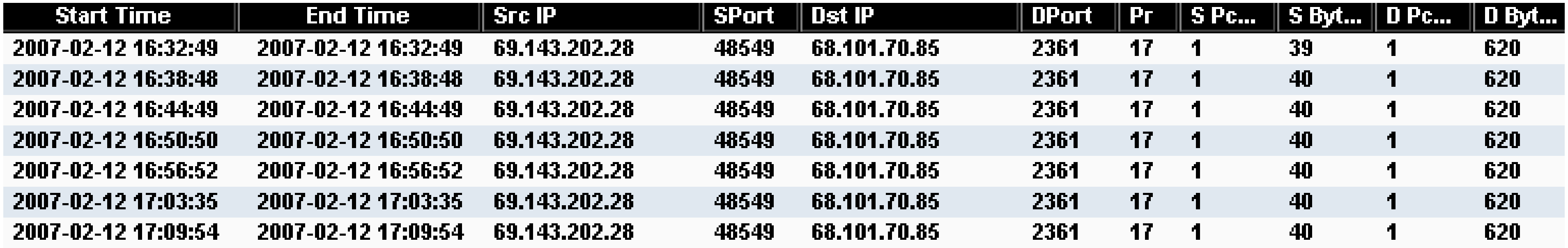
Example 6: Odd UDP Traffic

- Only one alert involved source IP



Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
2007-02-12 16:44:49	68.101.70.85	2361	69.143.202.28	48549	17	MS-SQL probe response overflow attempt

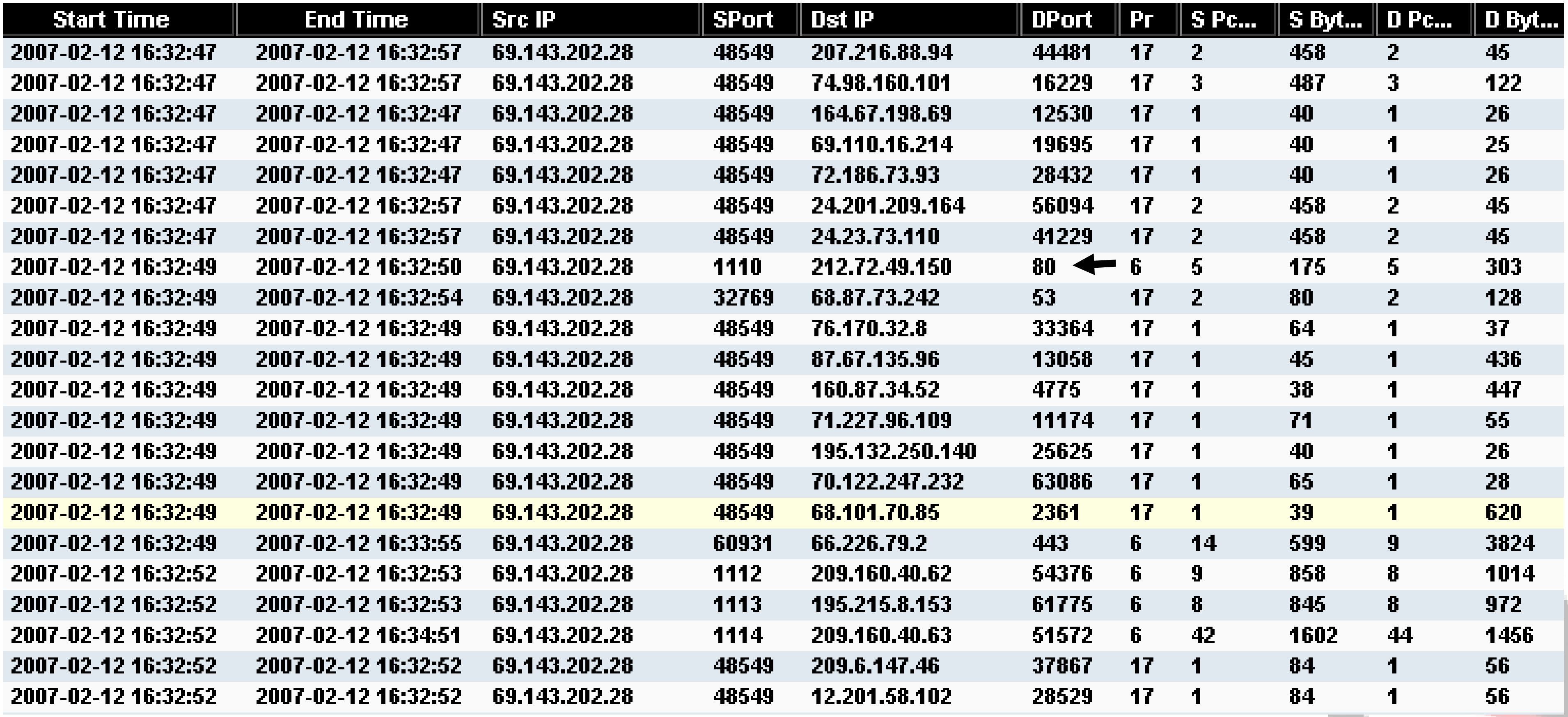
- Seven similar UDP sessions involving source IP



Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pc...	S Byt...	D Pc...	D Byt...
2007-02-12 16:32:49	2007-02-12 16:32:49	69.143.202.28	48549	68.101.70.85	2361	17	1	39	1	620
2007-02-12 16:38:48	2007-02-12 16:38:48	69.143.202.28	48549	68.101.70.85	2361	17	1	40	1	620
2007-02-12 16:44:49	2007-02-12 16:44:49	69.143.202.28	48549	68.101.70.85	2361	17	1	40	1	620
2007-02-12 16:50:50	2007-02-12 16:50:50	69.143.202.28	48549	68.101.70.85	2361	17	1	40	1	620
2007-02-12 16:56:52	2007-02-12 16:56:52	69.143.202.28	48549	68.101.70.85	2361	17	1	40	1	620
2007-02-12 17:03:35	2007-02-12 17:03:35	69.143.202.28	48549	68.101.70.85	2361	17	1	40	1	620
2007-02-12 17:09:54	2007-02-12 17:09:54	69.143.202.28	48549	68.101.70.85	2361	17	1	40	1	620

Example 6: Odd UDP Traffic

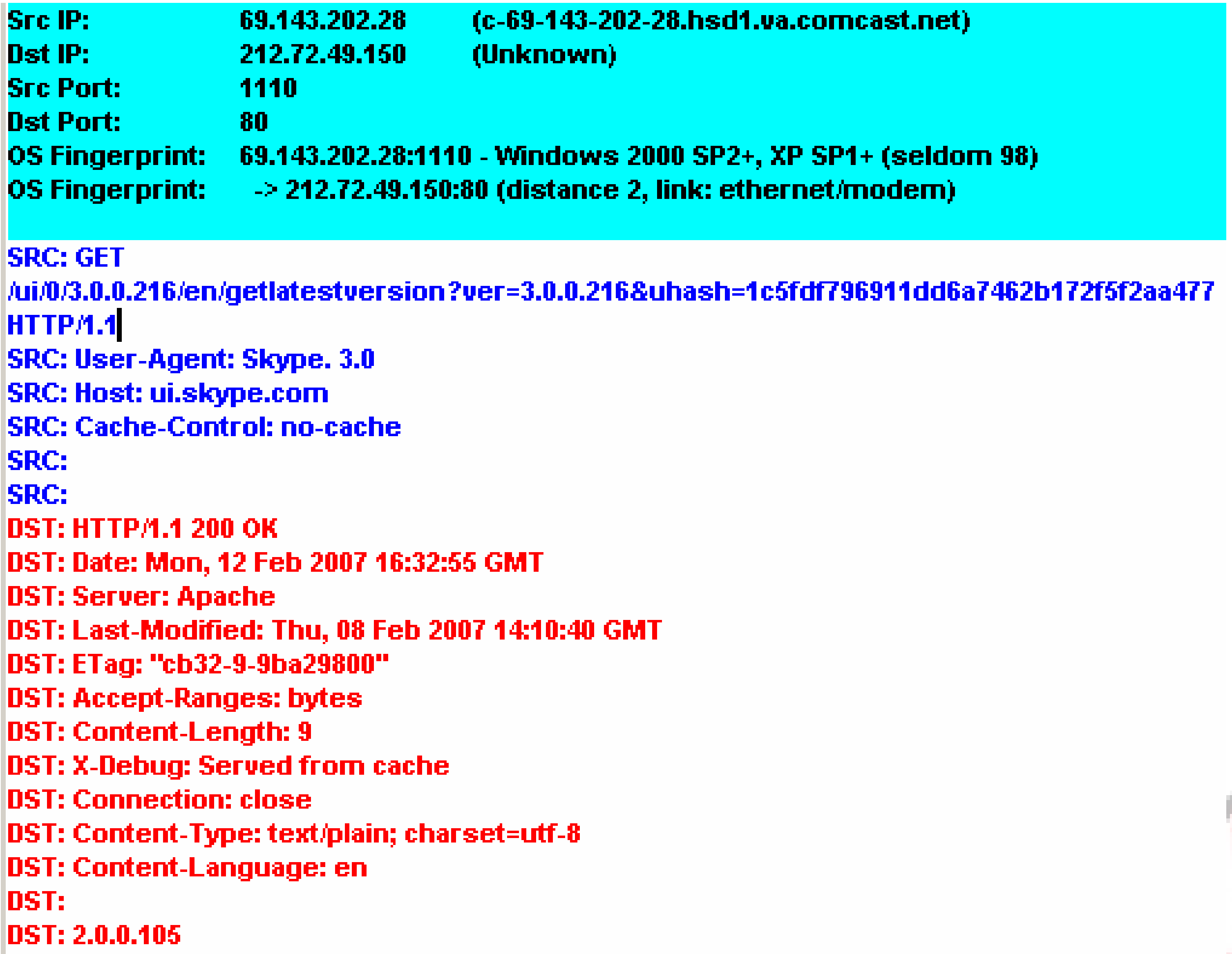
- Query for sessions involving our IP around the time of the original alert
- Investigating this Web session might be interesting



Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pc...	S Byt...	D Pc...	D Byt...
2007-02-12 16:32:47	2007-02-12 16:32:57	69.143.202.28	48549	207.216.88.94	44481	17	2	458	2	45
2007-02-12 16:32:47	2007-02-12 16:32:57	69.143.202.28	48549	74.98.160.101	16229	17	3	487	3	122
2007-02-12 16:32:47	2007-02-12 16:32:47	69.143.202.28	48549	164.67.198.69	12530	17	1	40	1	26
2007-02-12 16:32:47	2007-02-12 16:32:47	69.143.202.28	48549	69.110.16.214	19695	17	1	40	1	25
2007-02-12 16:32:47	2007-02-12 16:32:47	69.143.202.28	48549	72.186.73.93	28432	17	1	40	1	26
2007-02-12 16:32:47	2007-02-12 16:32:57	69.143.202.28	48549	24.201.209.164	56094	17	2	458	2	45
2007-02-12 16:32:47	2007-02-12 16:32:57	69.143.202.28	48549	24.23.73.110	41229	17	2	458	2	45
2007-02-12 16:32:49	2007-02-12 16:32:50	69.143.202.28	1110	212.72.49.150	80 ←	6	5	175	5	303
2007-02-12 16:32:49	2007-02-12 16:32:54	69.143.202.28	32769	68.87.73.242	53	17	2	80	2	128
2007-02-12 16:32:49	2007-02-12 16:32:49	69.143.202.28	48549	76.170.32.8	33364	17	1	64	1	37
2007-02-12 16:32:49	2007-02-12 16:32:49	69.143.202.28	48549	87.67.135.96	13058	17	1	45	1	436
2007-02-12 16:32:49	2007-02-12 16:32:49	69.143.202.28	48549	160.87.34.52	4775	17	1	38	1	447
2007-02-12 16:32:49	2007-02-12 16:32:49	69.143.202.28	48549	71.227.96.109	11174	17	1	71	1	55
2007-02-12 16:32:49	2007-02-12 16:32:49	69.143.202.28	48549	195.132.250.140	25625	17	1	40	1	26
2007-02-12 16:32:49	2007-02-12 16:32:49	69.143.202.28	48549	70.122.247.232	63086	17	1	65	1	28
2007-02-12 16:32:49	2007-02-12 16:32:49	69.143.202.28	48549	68.101.70.85	2361	17	1	39	1	620
2007-02-12 16:32:49	2007-02-12 16:33:55	69.143.202.28	60931	66.226.79.2	443	6	14	599	9	3824
2007-02-12 16:32:52	2007-02-12 16:32:53	69.143.202.28	1112	209.160.40.62	54376	6	9	858	8	1014
2007-02-12 16:32:52	2007-02-12 16:32:53	69.143.202.28	1113	195.215.8.153	61775	6	8	845	8	972
2007-02-12 16:32:52	2007-02-12 16:34:51	69.143.202.28	1114	209.160.40.63	51572	6	42	1602	44	1456
2007-02-12 16:32:52	2007-02-12 16:32:52	69.143.202.28	48549	209.6.147.46	37867	17	1	84	1	56
2007-02-12 16:32:52	2007-02-12 16:32:52	69.143.202.28	48549	12.201.58.102	28529	17	1	84	1	56

Example 6: Odd UDP Traffic

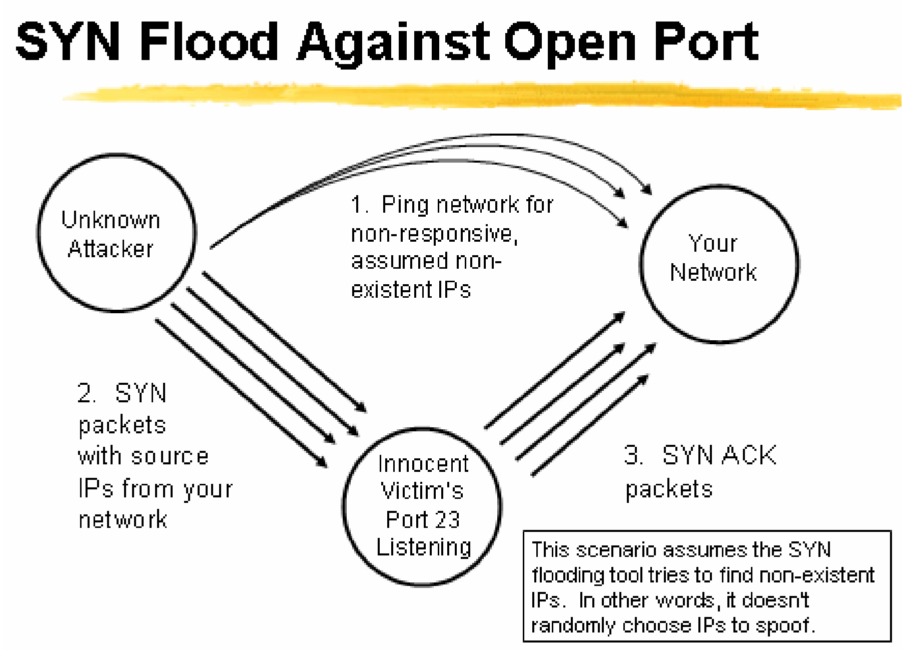
- Port 80 TCP traffic shows Skype download



```
Src IP:          69.143.202.28     (c-69-143-202-28.hsd1.va.comcast.net)
Dst IP:          212.72.49.150     (Unknown)
Src Port:        1110
Dst Port:        80
OS Fingerprint:  69.143.202.28:1110 - Windows 2000 SP2+, XP SP1+ (seldom 98)
OS Fingerprint:    -> 212.72.49.150:80 (distance 2, link: ethernet/modem)

SRC: GET
/ui/0/3.0.0.216/en/getlatestversion?ver=3.0.0.216&uhash=1c5fdf796911dd6a7462b172f5f2aa477
HTTP/1.1
SRC: User-Agent: Skype. 3.0
SRC: Host: ui.skype.com
SRC: Cache-Control: no-cache
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Mon, 12 Feb 2007 16:32:55 GMT
DST: Server: Apache
DST: Last-Modified: Thu, 08 Feb 2007 14:10:40 GMT
DST: ETag: "cb32-9-9ba29800"
DST: Accept-Ranges: bytes
DST: Content-Length: 9
DST: X-Debug: Served from cache
DST: Connection: close
DST: Content-Type: text/plain; charset=utf-8
DST: Content-Language: en
DST:
DST: 2.0.0.105
```

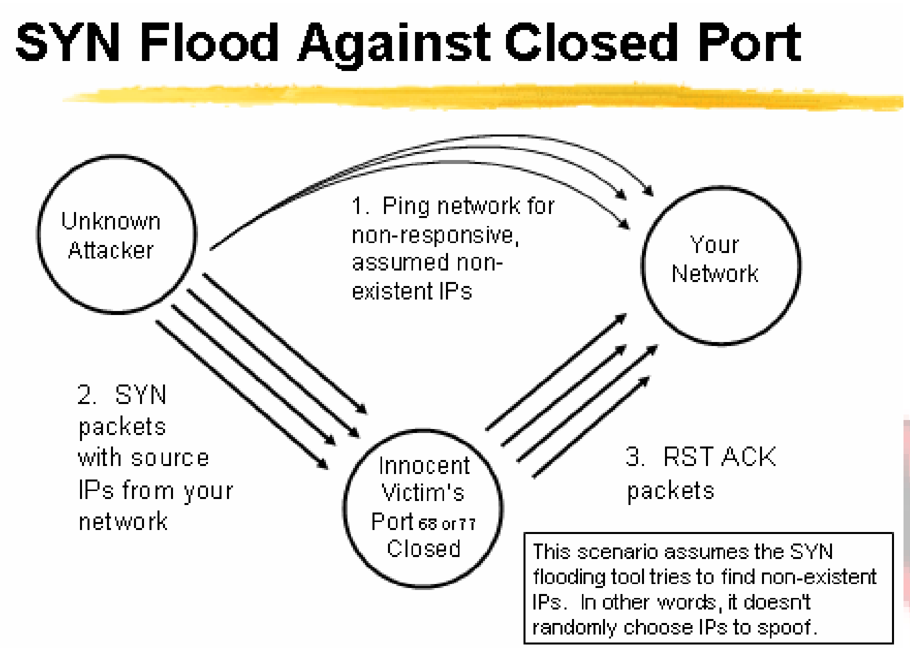
Example 7: SANS ISC TCP Options

- Sometimes the best investigative method is to step away from Wireshark and talk to a human
- 2 March 2007: SANS ISC reports "generally" seeing SYN ACK traffic from sources "80, 6667, 6666, and 443" from 129.250.128.21 (compton.ameri.ca)
- I wrote about this in 1999 and taught it at SANS in 2000


SYN Flood Against Open Port

Unknown Attacker
1. Ping network for non-responsive, assumed non-existent IPs
Your Network
2. SYN packets with source IPs from your network
Innocent Victim's Port 23 Listening
3. SYN ACK packets

This scenario assumes the SYN flooding tool tries to find non-existent IPs. In other words, it doesn't randomly choose IPs to spoof.


SYN Flood Against Closed Port

Unknown Attacker
1. Ping network for non-responsive, assumed non-existent IPs
Your Network
2. SYN packets with source IPs from your network
Innocent Victim's Port 68 or 77 Closed
3. RST ACK packets

This scenario assumes the SYN flooding tool tries to find non-existent IPs. In other words, it doesn't randomly choose IPs to spoof.

Example 7: SANS ISC TCP Options

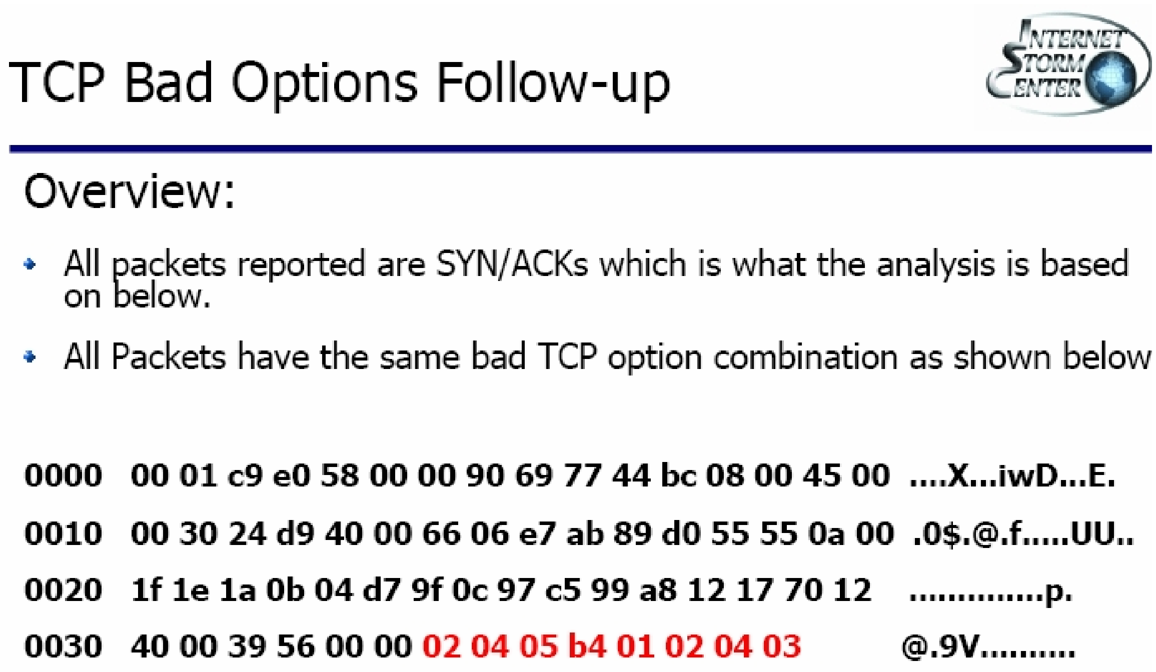
- SANS basically ignores me, so I contact the owner of compton.ameri.ca (Brad Dreisbach) who says:
  - "*i have been getting tcp syn attacked for about 3 weeks now. i have re-installed the OS on the host just to be safe, but im fairly sure my systems are secure. i have also taken measures with my upstream, whom i also work for, to migitate the attack. some stuff is still getting through but at this point im just waiting for the attackers to give up...* "
- Brad sends me a trace that also shows an ACK flood against his host from other parties
- SANS still ignores me, never posts additional details on isc.sans.org

Example 7: SANS ISC TCP Options

- ShadowServer project sends me bot net C&C traffic

```
Feb 26 16:59:16 xx.xx.xx.xx (xx.xx.xx.xx:6667) :ESP|846305!njhvef@xx.xx.xx.xx
PRIVMSG ##r0x## :nzm
(tcp.plg) »» Done with ack flood to IP: 129.250.128.21. Sent: 19186 packet(s) @
2KB/sec (1MB).

Feb 26 16:59:16 xx.xx.xx.xx:6667 :ESP|846305!njhvef@xx.xx.xx.xx PRIVMSG ##r0x##
:nzm (tcp.plg) »» Done
with ack flood to IP: 129.250.128.21. Sent: 19186 packet(s) @ 2KB/sec (1MB).

Feb 26 16:59:23 xx.xx.xx.xx:6667 :ESP|187844!guwcpbmq@xx.xx.xx.xx PRIVMSG ##r0x##
:nzm (tcp.plg) »»
Done with ack flood to IP: 129.250.128.21. Sent: 49633 packet(s) @ 7KB/sec (2MB).

Feb 26 16:59:24 xx.xx.xx.xx (xx.xx.xx.xx:6667) :ESP|187844!guwcpbmq@xx.xx.xx.xx
PRIVMSG ##r0x## :nzm
(tcp.plg) »» Done with ack flood to IP: 129.250.128.21. Sent: 49633 packet(s) @
7KB/sec (2MB).

Feb 26 16:59:52 xx.xx.xx.xx:6667 :PRT|113722!owfxzrp@xx.xx.xx.xx.rev.xxximus.pt
PRIVMSG ##r0x## :nzm
(tcp.plg) »» Done with ack flood to IP: 129.250.128.21. Sent: 47952 packet(s) @
7KB/sec (2MB).

Feb 26 16:59:52 xx.xx.xx.xx (xx.xx.xx.xx:6667)
:PRT|113722!owfxzrp@xx.xx.xx.xx.rev.xxximus.pt PRIVMSG
##r0x## :nzm (tcp.plg) »» Done with ack flood to IP: 129.250.128.21. Sent: 47952
packet(s) @ 7KB/sec (2MB).
```

Example 7: SANS ISC TCP Options



TCP Bad Options Follow-up

Overview:

- All packets reported are SYN/ACKs which is what the analysis is based on below.
- All Packets have the same bad TCP option combination as shown below

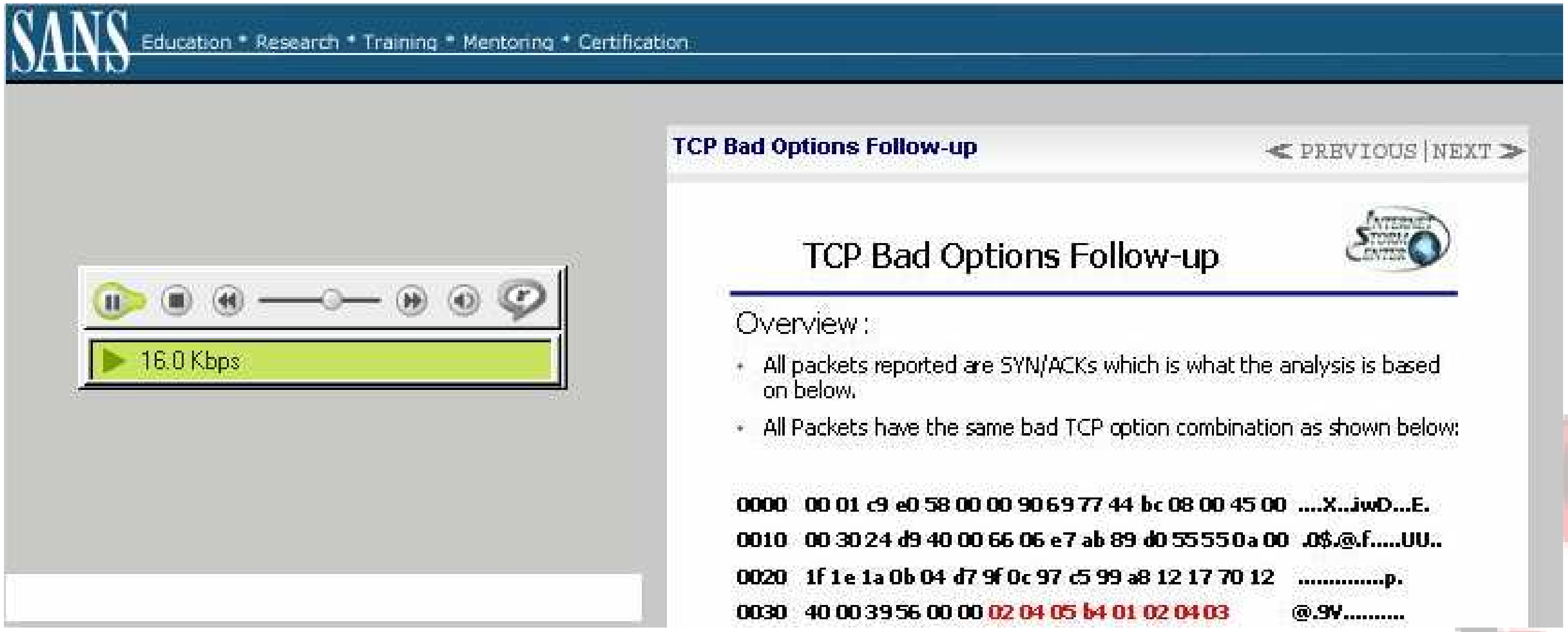
```
0000   00 01 c9 e0 58 00 00 90 69 77 44 bc 08 00 45 00  ....X...iwD...E.
0010   00 30 24 d9 40 00 66 06 e7 ab 89 d0 55 55 0a 00  .0$.@.f.....UU..
0020   1f 1e 1a 0b 04 d7 9f 0c 97 c5 99 a8 12 17 70 12   .............p.
0030   40 00 39 56 00 00 02 04 05 b4 01 02 04 03         @.9V.........
```

- Michal Zalewski's Museum of Broken Packets shows traffic caused by juno-z DoS tool
  - http://packetstormsecurity.org/DoS/juno-z.101f.c

```
0000 XX XX XX XX XX XX XX XX XX XX XX XX 08 00 45 00 ..............E.
0010 00 30 6f bb 40 00 7f 06 63 b6 40 be 19 30 XX XX .0o.@...c.@.....
0020 XX XX 04 59 01 ea 10 10 02 39 00 00 00 00 70 02 ...Y.....9....p.
0030 40 00 02 3b 00 00 02 04 05 b4 01 02 04 03 .. .. @..;...........
```

Example 7: SANS ISC TCP Options

- At the end of the day we have...
  - Backscatter traffic seen by various sites, reported to SANS ISC
  - Report from the victim of a DoS attack that he was flooded by multiple methods (including IPv6!) for three weeks
  - Traffic from DoS victim showing an ACK flood
  - Botnet C&C traffic showing bots attacking victim via ACK flood
  - Correlation with other traffic and identification of juno-z DoS tool



TCP Bad Options Follow-up

TCP Bad Options Follow-up

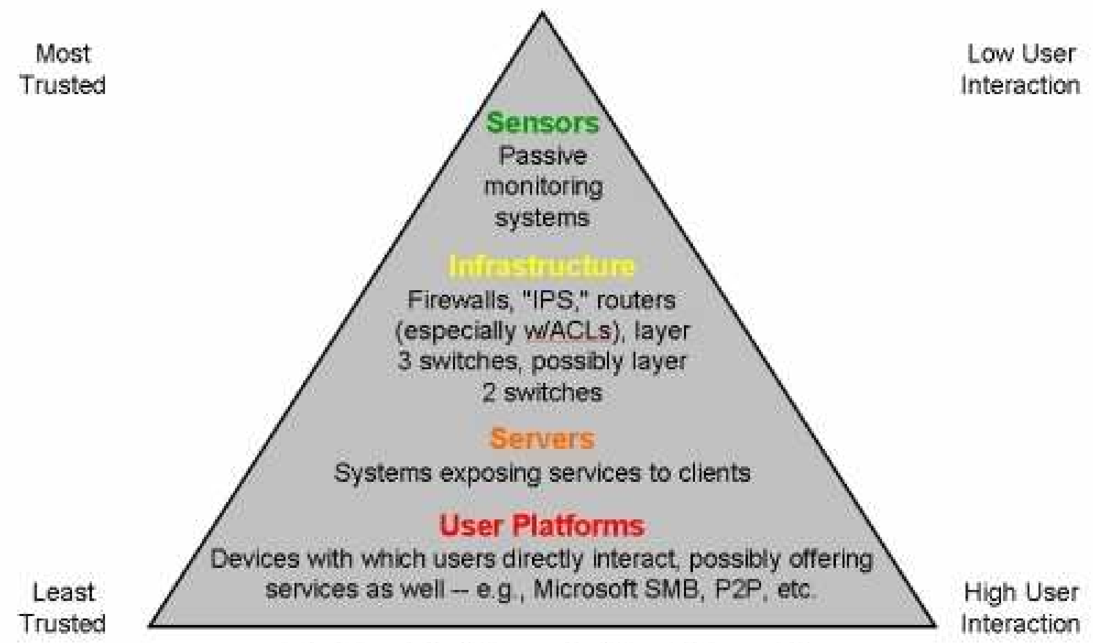
Overview:

- All packets reported are SYN/ACKs which is what the analysis is based on below.
- All Packets have the same bad TCP option combination as shown below:

```
0000   00 01 c9 e0 58 00 00 90 69 77 44 bc 08 00 45 00   ....X..iwD...E.
0010   00 30 24 d9 40 00 66 06 e7 ab 89 d0 55 55 0a 00   .0$.@.f.....UU..
0020   1f 1e 1a 0b 04 d7 9f 0c 97 c5 99 a8 12 17 70 12   ..............p.
0030   40 00 39 56 00 00 02 04 05 b4 01 02 04 03         @.9V.........
```

Conclusion

- If you're not stopping absolutely everything that's malicious, you're either blindly permitting it or perhaps alerting on some of it
- Investigating those suspicious events requires trusted data, and the network can provide one (not "the") independent source


Most Trusted
Low User Interaction
Sensors
Passive monitoring systems
Infrastructure
Firewalls, "IPS," routers (especially w/ACLs), layer 3 switches, possibly layer 2 switches
Servers
Systems exposing services to clients
User Platforms
Devices with which users directly interact, possibly offering services as well -- e.g., Microsoft SMB, P2P, etc.
Least Trusted
High User Interaction

TaoSecurity Enterprise Trust Pyramid

If You Thought I Was Going to Mention Gartner...

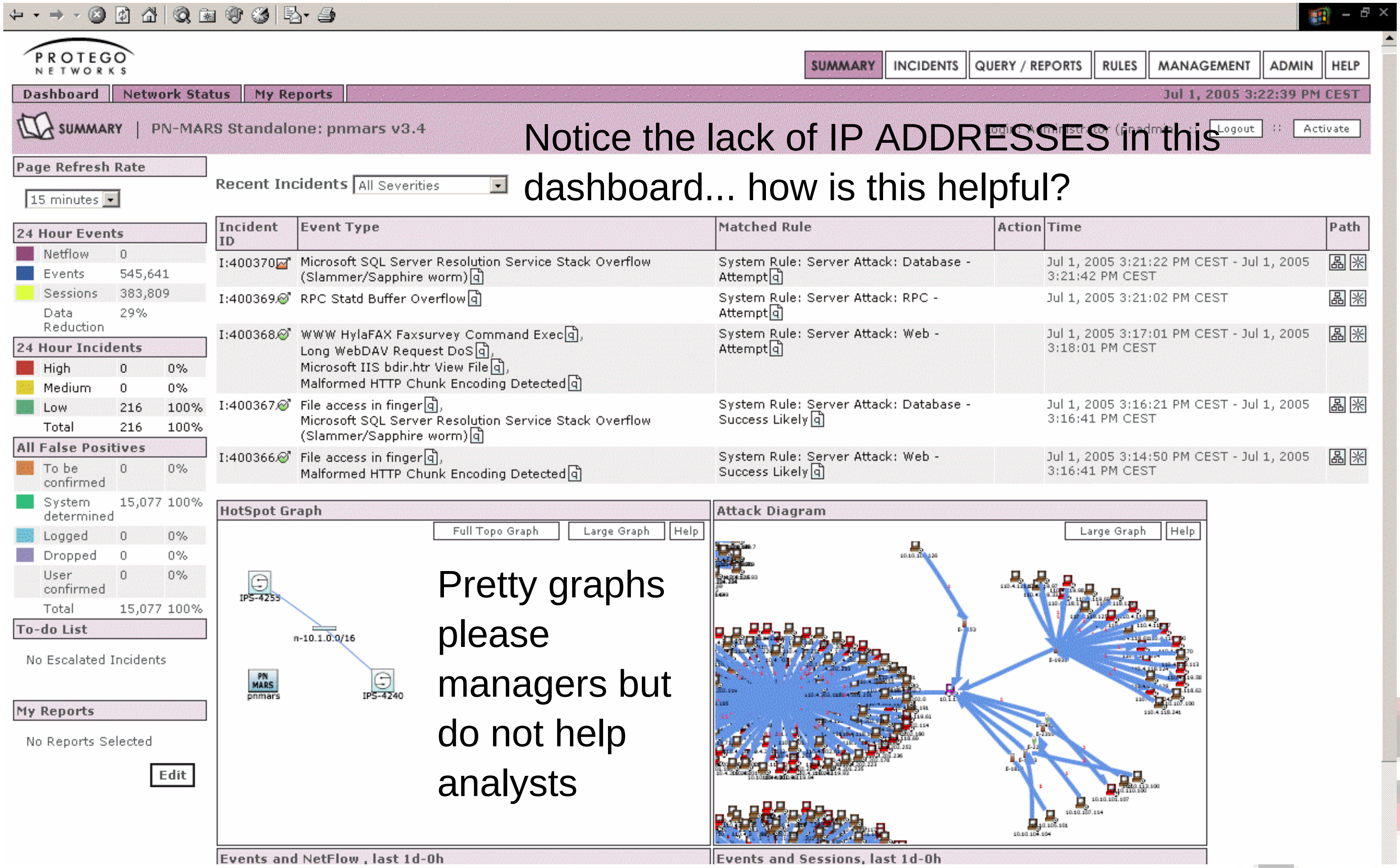
- 2003 Gartner Press Release
  - “IDSs have failed to provide value relative to its costs and **will be obsolete by 2005**.” **(*didn't happen*)**
  - “The Gartner Information Security Hype Cycle shows that **IDS** technology **does not add an additional layer of security** as promised by vendors. In many cases IDS implementation has proven to be **costly** and an **ineffective** investment.” (*probably true*)
  - Gartner recommends that enterprises redirect the money they would have spent on IDS toward defense applications such as those offered by thought-leading **firewall vendors** that offer both network-level and application-level firewall capabilities in an integrated product.” (*going to happen, eventually*)

2003 Gartner Press Release, cont.

- "According to the Gartner Information Security Hype Cycle research, some of the problems associated with IDSs are:
  1) False positives and negatives
  2) An increased burden on the IS organization by requiring full-time monitoring (24 hours a day, seven days a week, 365 days a year)
  3) A taxing incident-response process
  4) An inability to monitor traffic at transmission rates greater than 600 megabits per second"
- **Comment:** "Deep packet inspection firewalls" don't help
  1) False positives and negatives are unavoidable
  2) Constant vigilance is a requirement for any enterprise
  3) Incident response is always a PITA
  4) High rates is a technology issue common to any platform

Gratuitous Critique of Commercial Products

- This is Cisco MARS -- please see taosecurity.blogspot.com/2007/02/earth-to-mars.html



Notice the lack of IP ADDRESSES in this dashboard... how is this helpful?

24 Hour Events

🟪	Netflow	0
🟦	Events	545,641
🟨	Sessions	383,809
	Data Reduction	29%

24 Hour Incidents

🟥	High	0	0%
🟨	Medium	0	0%
🟩	Low	216	100%
	Total	216	100%

All False Positives

🟧	To be confirmed	0	0%
🟩	System determined	15,077	100%
🟦	Logged	0	0%
🟪	Dropped	0	0%
	User confirmed	0	0%
	Total	15,077	100%

To-do List

No Escalated Incidents

My Reports

No Reports Selected

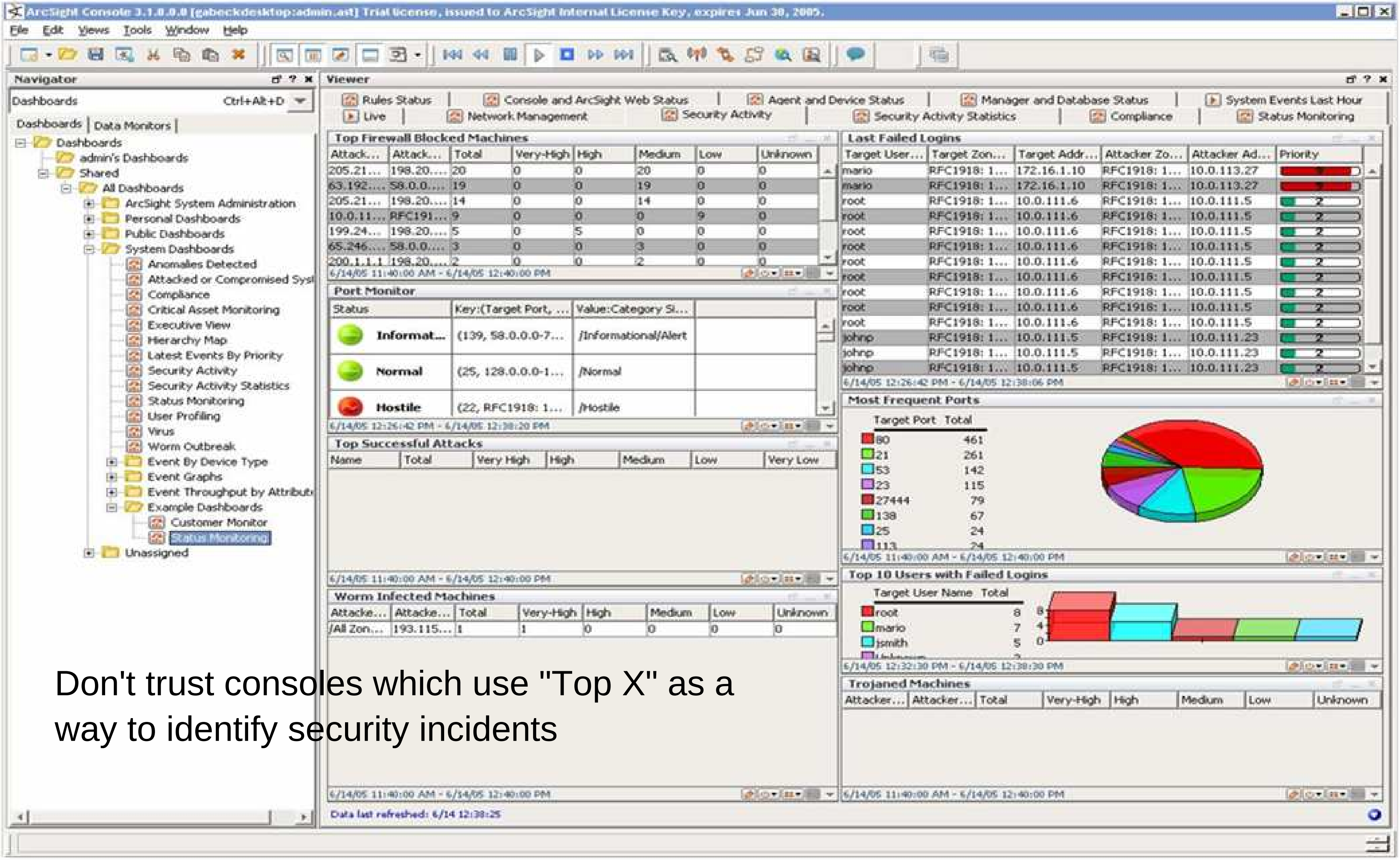
Edit

Incident ID	Event Type	Matched Rule	Action	Time	Path
I:400370	Microsoft SQL Server Resolution Service Stack Overflow (Slammer/Sapphire worm)	System Rule: Server Attack: Database - Attempt		Jul 1, 2005 3:21:22 PM CEST - Jul 1, 2005 3:21:42 PM CEST	
I:400369	RPC Statd Buffer Overflow	System Rule: Server Attack: RPC - Attempt		Jul 1, 2005 3:21:02 PM CEST	
I:400368	WWW HylaFAX Faxsurvey Command Exec, Long WebDAV Request DoS, Microsoft IIS bdir.htr View File, Malformed HTTP Chunk Encoding Detected	System Rule: Server Attack: Web - Attempt		Jul 1, 2005 3:17:01 PM CEST - Jul 1, 2005 3:18:01 PM CEST	
I:400367	File access in finger, Microsoft SQL Server Resolution Service Stack Overflow (Slammer/Sapphire worm)	System Rule: Server Attack: Database - Success Likely		Jul 1, 2005 3:16:21 PM CEST - Jul 1, 2005 3:16:41 PM CEST	
I:400366	File access in finger, Malformed HTTP Chunk Encoding Detected	System Rule: Server Attack: Web - Success Likely		Jul 1, 2005 3:14:50 PM CEST - Jul 1, 2005 3:16:41 PM CEST	

Pretty graphs please managers but do not help analysts

Gratuitous Critique of Commercial Products

- This is ArcSight -- how do you avoid GIGO?



Top Firewall Blocked Machines

Attack...	Attack...	Total	Very-High	High	Medium	Low	Unknown
205.21...	198.20....	20	0	0	20	0	0
63.192....	58.0.0....	19	0	0	19	0	0
205.21...	198.20....	14	0	0	14	0	0
10.0.11...	RFC191...	9	0	0	0	9	0
199.24...	198.20....	5	0	5	0	0	0
65.246....	58.0.0....	3	0	0	3	0	0
200.1.1.1	198.20....	2	0	0	2	0	0

6/14/05 11:40:00 AM - 6/14/05 12:40:00 PM

Port Monitor

Status	Key:(Target Port, ...	Value:Category Si...
Informat...	(139, 58.0.0.0-7...	/Informational/Alert
Normal	(25, 128.0.0.0-1...	/Normal
Hostile	(22, RFC1918: 1...	/Hostile

6/14/05 12:26:42 PM - 6/14/05 12:38:20 PM

Top Successful Attacks

Name	Total	Very High	High	Medium	Low	Very Low

6/14/05 11:40:00 AM - 6/14/05 12:40:00 PM

Worm Infected Machines

Attacke...	Attacke...	Total	Very-High	High	Medium	Low	Unknown
/All Zon...	193.115...	1	1	0	0	0	0

6/14/05 11:40:00 AM - 6/14/05 12:40:00 PM

Last Failed Logins

Target User...	Target Zon...	Target Addr...	Attacker Zo...	Attacker Ad...	Priority
mario	RFC1918: 1...	172.16.1.10	RFC1918: 1...	10.0.113.27	7
mario	RFC1918: 1...	172.16.1.10	RFC1918: 1...	10.0.113.27	7
root	RFC1918: 1...	10.0.111.6	RFC1918: 1...	10.0.111.5	2
root	RFC1918: 1...	10.0.111.6	RFC1918: 1...	10.0.111.5	2
root	RFC1918: 1...	10.0.111.6	RFC1918: 1...	10.0.111.5	2
root	RFC1918: 1...	10.0.111.6	RFC1918: 1...	10.0.111.5	2
root	RFC1918: 1...	10.0.111.6	RFC1918: 1...	10.0.111.5	2
root	RFC1918: 1...	10.0.111.6	RFC1918: 1...	10.0.111.5	2
root	RFC1918: 1...	10.0.111.6	RFC1918: 1...	10.0.111.5	2
root	RFC1918: 1...	10.0.111.6	RFC1918: 1...	10.0.111.5	2
root	RFC1918: 1...	10.0.111.6	RFC1918: 1...	10.0.111.5	2
johnp	RFC1918: 1...	10.0.111.5	RFC1918: 1...	10.0.111.23	2
johnp	RFC1918: 1...	10.0.111.5	RFC1918: 1...	10.0.111.23	2
johnp	RFC1918: 1...	10.0.111.5	RFC1918: 1...	10.0.111.23	2

6/14/05 12:26:42 PM - 6/14/05 12:38:06 PM

Most Frequent Ports

Target Port	Total
🟥 80	461
🟩 21	261
🟦 53	142
🟪 23	115
🟥 27444	79
🟩 138	67
🟦 25	24
🟪 113	24

6/14/05 11:40:00 AM - 6/14/05 12:40:00 PM

Top 10 Users with Failed Logins

Target User Name	Total
🟥 root	8
🟩 mario	7
🟦 jsmith	5

6/14/05 12:32:30 PM - 6/14/05 12:38:30 PM

Trojaned Machines

Attacker...	Attacker...	Total	Very-High	High	Medium	Low	Unknown

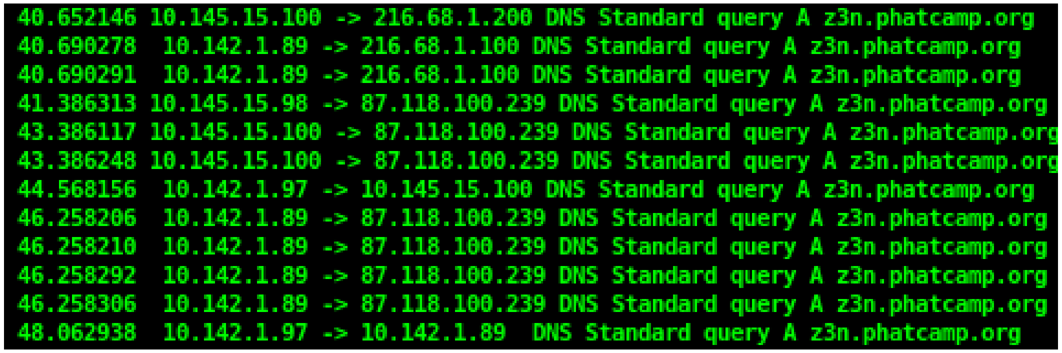
6/14/05 11:40:00 AM - 6/14/05 12:40:00 PM

Data last refreshed: 6/14 12:38:25

Don't trust consoles which use "Top X" as a way to identify security incidents

Questions?

KNOW YOUR NETWORK BEFORE AN INTRUDER DOES



```
40.652146 10.145.15.100 -> 216.68.1.200 DNS Standard query A z3n.phatcamp.org
40.690278  10.142.1.89 -> 216.68.1.100 DNS Standard query A z3n.phatcamp.org
40.690291  10.142.1.89 -> 216.68.1.100 DNS Standard query A z3n.phatcamp.org
41.386313 10.145.15.98 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
43.386117 10.145.15.100 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
43.386248 10.145.15.100 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
44.568156  10.142.1.97 -> 10.145.15.100 DNS Standard query A z3n.phatcamp.org
46.258206  10.142.1.89 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
46.258210  10.142.1.89 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
46.258292  10.142.1.89 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
46.258306  10.142.1.89 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
48.062938  10.142.1.97 -> 10.142.1.89  DNS Standard query A z3n.phatcamp.org
```

Richard Bejtlich
richard@taosecurity.com
www.taosecurity.com
9532 Liberia Ave Suite 141
Manassas VA 20110
202.409.8045