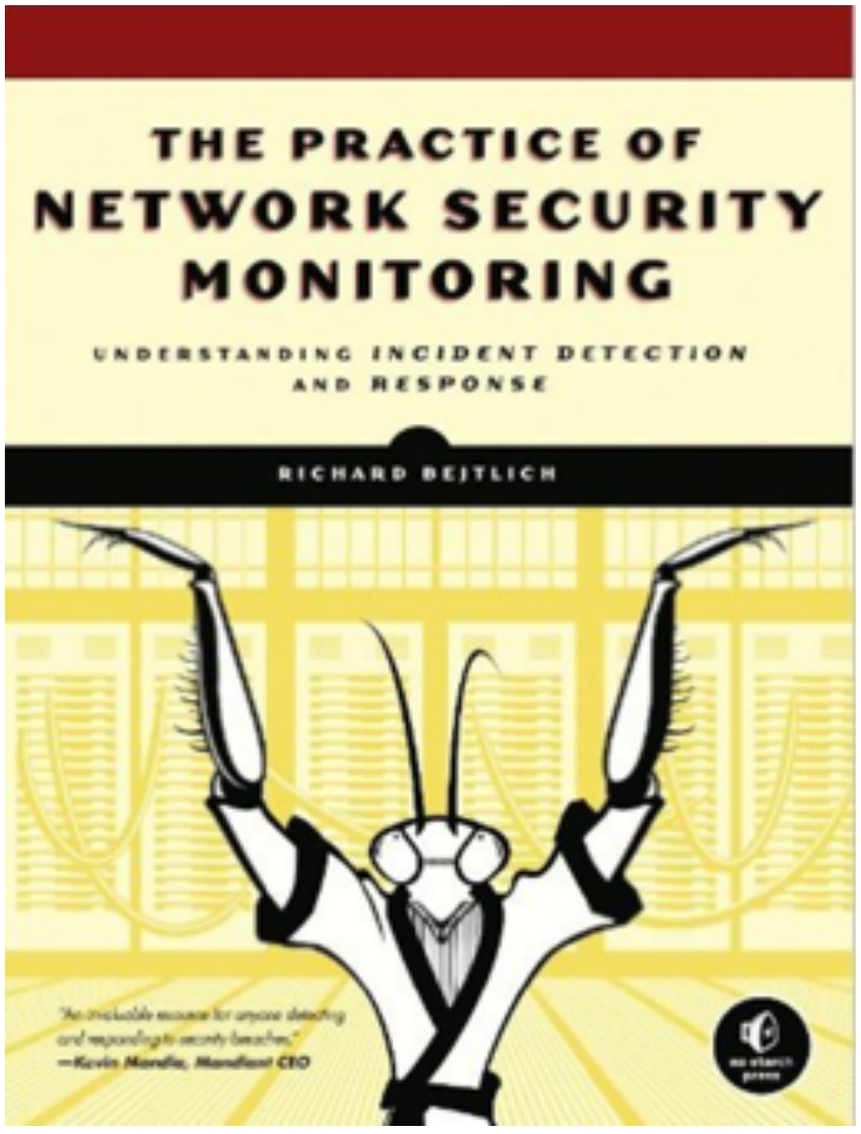
CNIT 50:
Network Security Monitoring

1. Network Security Monitoring Rationale



Rev. 12-11-17

Aurora Attack
December 2009

(not in textbook)

"Aurora" Attack on Google

- In December, 2009, Google discovered that confidential materials were being sent out of their network to China
- Google hacked into the Chinese server and stole data back, discovering that dozens of other companies had also been exploited, including Adobe and Intel

Aurora Attack Sequence

- Attacks were customized for each target based on vulnerable software and antivirus protection
  1. A user is tricked into visiting a malicious website
  2. Browser exploited to load malware on target PC
  3. Malware calls home to a control server
  4. Local privilege escalation

Aurora Attack Sequence

5. Active Directory password database stolen and cracked
6. Cracked credentials used to gain VPN Access
7. Valuable data is sent to China

New Recommendations

- Links Ch 13z1, 13z2

Here is a few short-term recommendations, as given by iSEC:

1. Log and inspect DNS traffic
2. Establish internal network surveillance capability
3. Control inbound and outbound network traffic
4. Expand log aggregation
5. Expand Windows endpoint control
6. Audit VPN access and enrollment.
7. Test malware scanning against known rootkits.

As regards long-term goals, companies should:

1. Build a security operations team
2. Secure your overseas offices
3. Classify and catalog sensitive data
4. Secure their Active Directory network (smartcard logins, steering clear of shared local accounts, using read-only domain controllers in overseas offices, and more).

The main lesson to be learned from these attacks is that times have changed. Anti-virus solutions and patching are no longer enough

Topics

- **Introduction to NSM**
- **A Sample NSM Test**
- **The Range of NSM Data**
- **NSM Drawbacks**

Introduction to NSM

Network Security Monitoring (NSM)

- **The collection, analysis, and escalation of indications and warnings to detect and respond to intrusions**

- **A way to find intruders on your network and do something about them before they cause damage**

Incident Response

- **Discovering adversaries**

- **A continuous business process**

- **NSM is one of the best ways to mature from zero defenses to some defensive capability**

Computer Incident Response Team (CIRT)

- **One person or more**
- **Responsible for handling computer intrusions**

CIRTs with NSM: Capabilities

- **Collect rich network-derived data**
- **Analyze data to find compromised assets**
- **Work with owners to contain and frustrate the enemy**
- **Use NSM data for damage assessment**

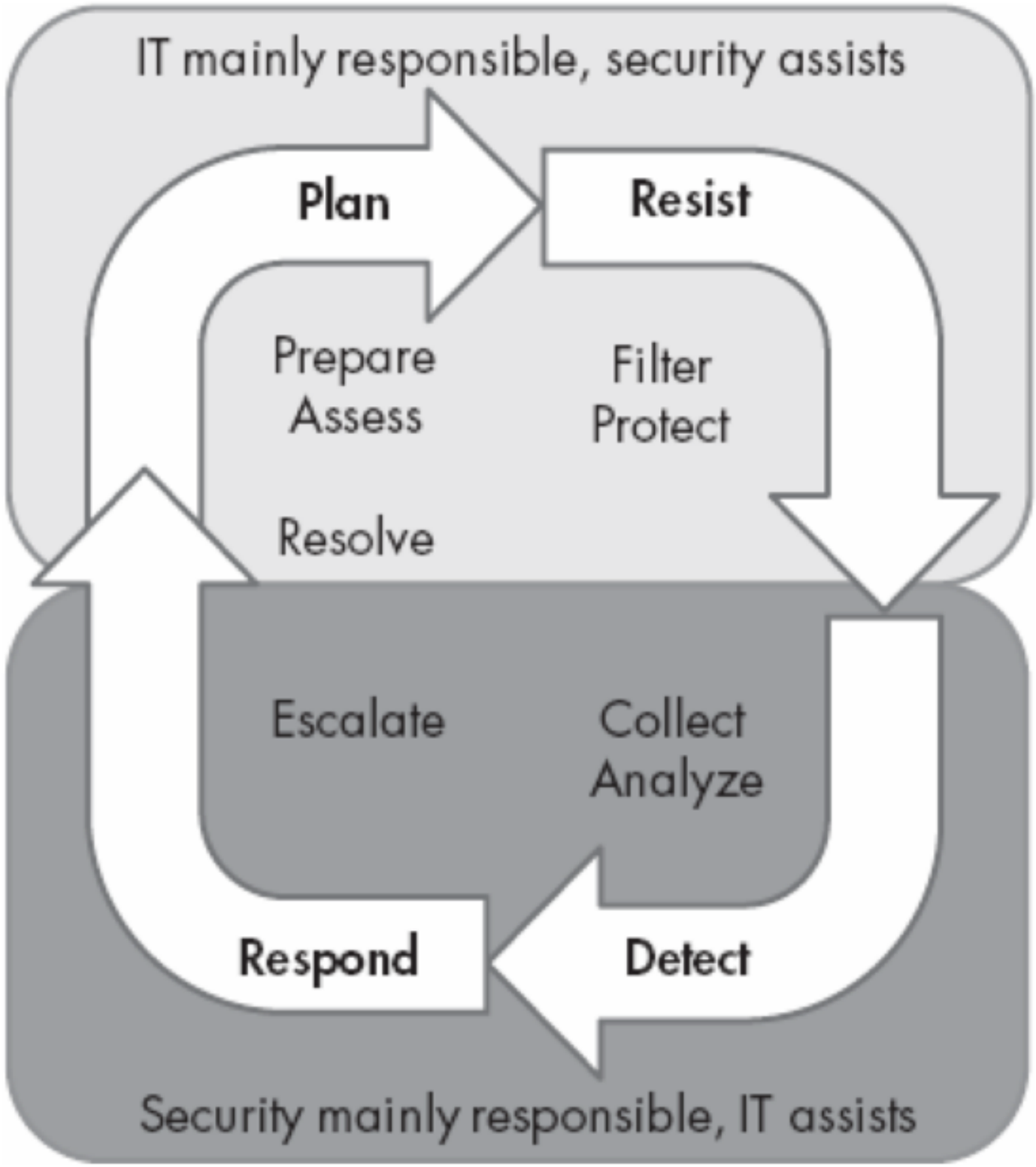


Figure 1-1. Enterprise security cycle

Preventing Intrusions

- **NSM does not prevent intrusions**
- **Prevention eventually fails**
- **Security breaches are inevitable**
- **Determined adversaries will inevitably breach your defenses**
- **But they may not achieve their objective**

Time

- **Time is the key factor**
- **Sophisticated attackers seek persistence**
- **This provides a window of time**
- **Between initial unauthorized access and ultimate mission accomplishment**

Why You Can't Prevent Intrusions

- **If you can detect it, why can't you prevent it?**
- **Protection can't keep up with new tactics**

Case Study

- **South Caroline Dept. of Revenue in 2012**
- **Attacker got in by phishing email**
- **Stole data 4 weeks later**
- **Four weeks later they called Mandiant**

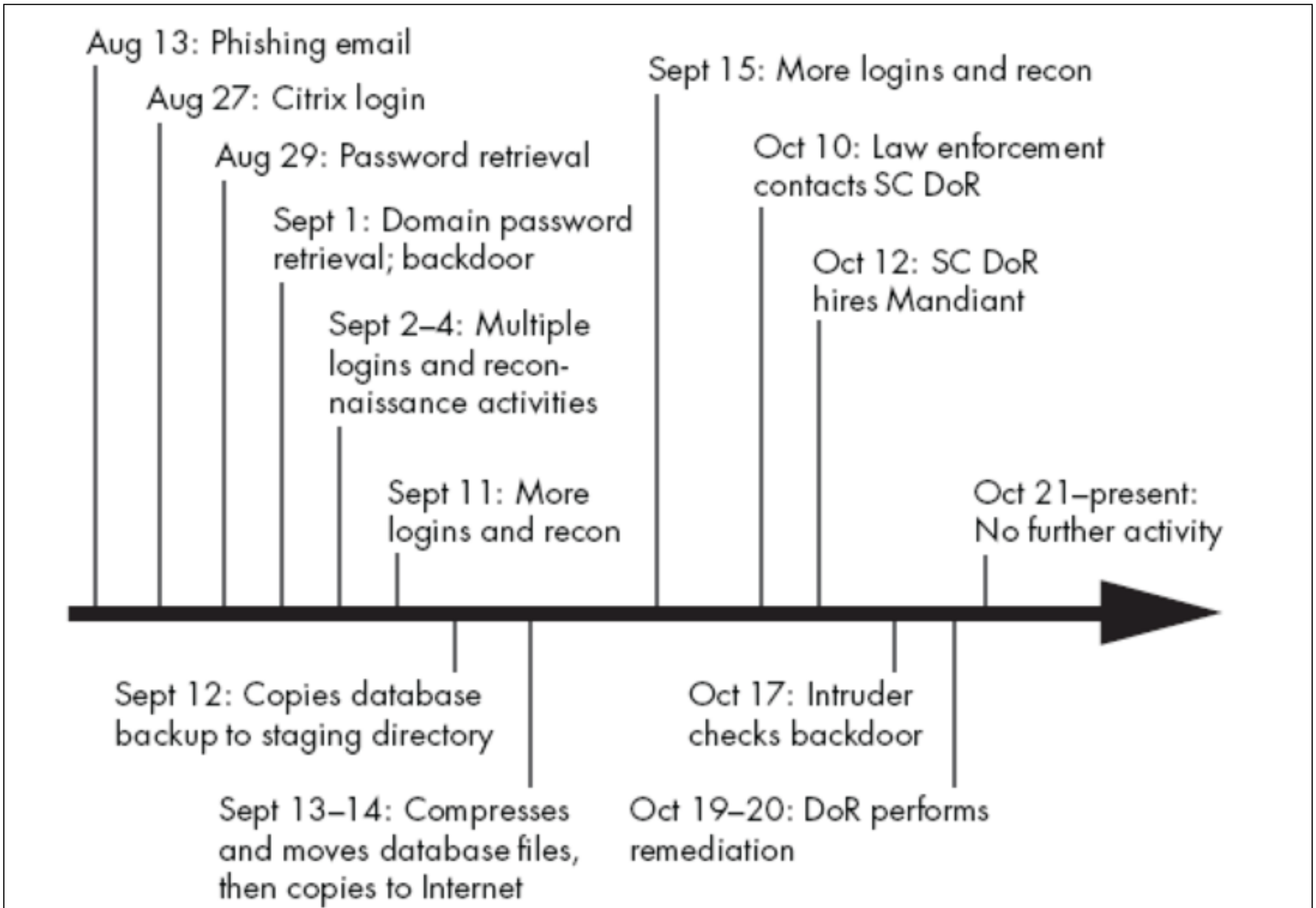


Figure 1-2. Edited timeline of South Carolina Department of Revenue incident

Lesson

- **This attack succeeded**
- **But the target had 4 weeks to stop it**
- **Would have saved $12 million**

Statistics

- **Median time between start of intrusion to incident response is > 240 days**

- **Only 1/3 of companies detected the intrusion themselves**

Continuous Monitoring (CM)

- **CM monitors vulnerabilities (compliance)**
- **Very different from NSM**
- **DHS & NIST promote CM in federal gov't**
- **An improvement over Certification & Accreditation**

Consider the differences in the ways that CM and NSM are implemented:

- A CM operation strives to find an organization's computers, identify vulnerabilities, and patch those holes, if possible.
- An NSM operation is designed to detect adversaries, respond to their activities, and contain them before they can accomplish their mission.

Other Defenses

- **Firewall, Intrusion Prevention System (IPS), Antivirus (AV), Whitelisting, Data Loss Prevention (DLP), Digital Rights Management (DRM)**

- **All perform blocking, filtering, or denying**

- **Recognize malicious activity and stop it**

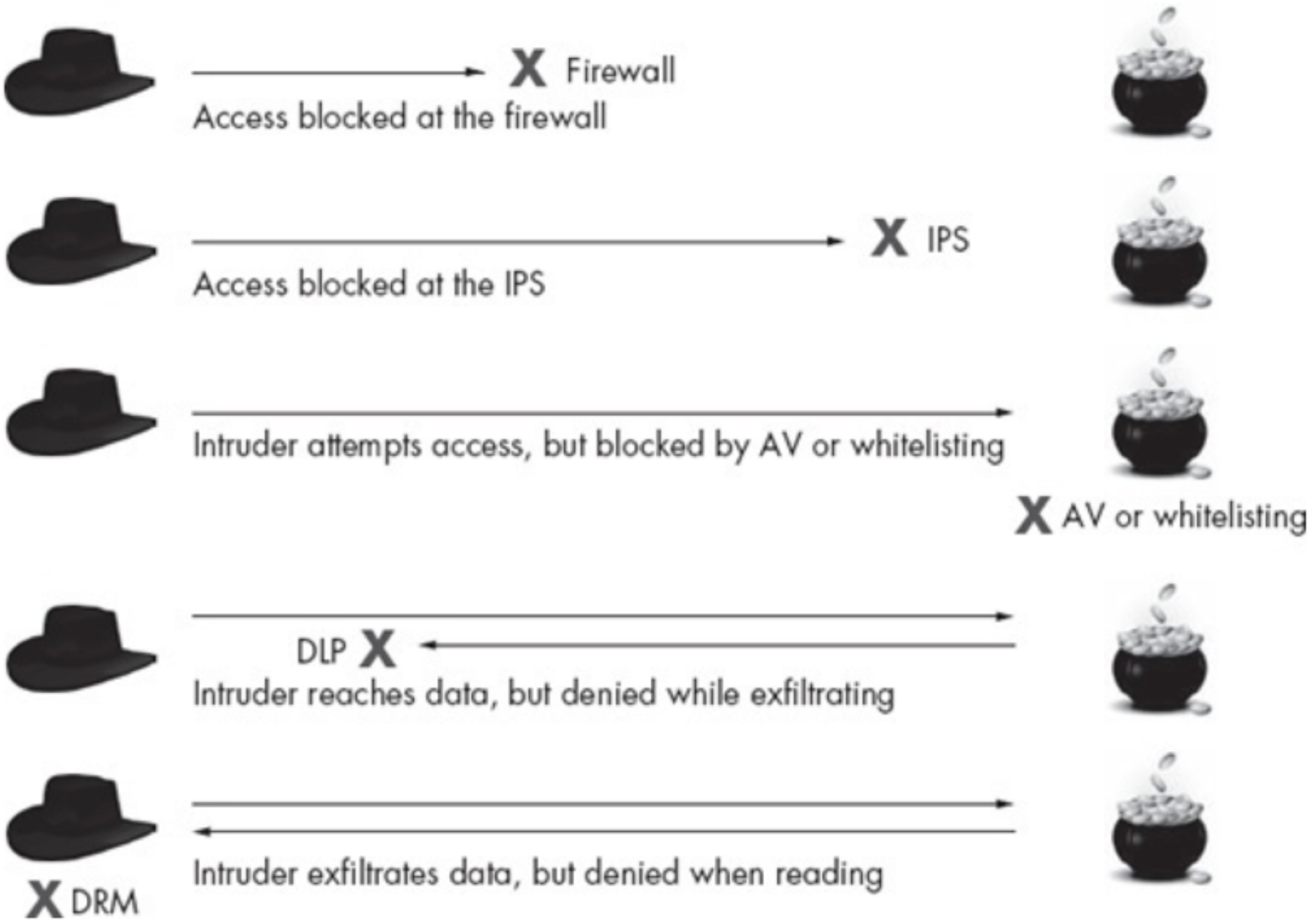


Figure 1-3. Blocking, filtering, and denying mechanisms

Role of NSM

- **NSM provides *visibility*, not control**
- **Makes failure of security controls more visible**

Why Does NSM Work?

- **Controls stop some attacks**
  - **Hit-and-run attacks**
- **But not determined attackers who want to gain persistence and remain in the system**
  - **They will find a way in**
  - **Then NSM and IR are needed**

Setting Up NSM

- **Select a suitable location to achieve network visibility**
- **Configure a switch to export copies of traffic**
- **Use a dedicated server as an NSM platform**

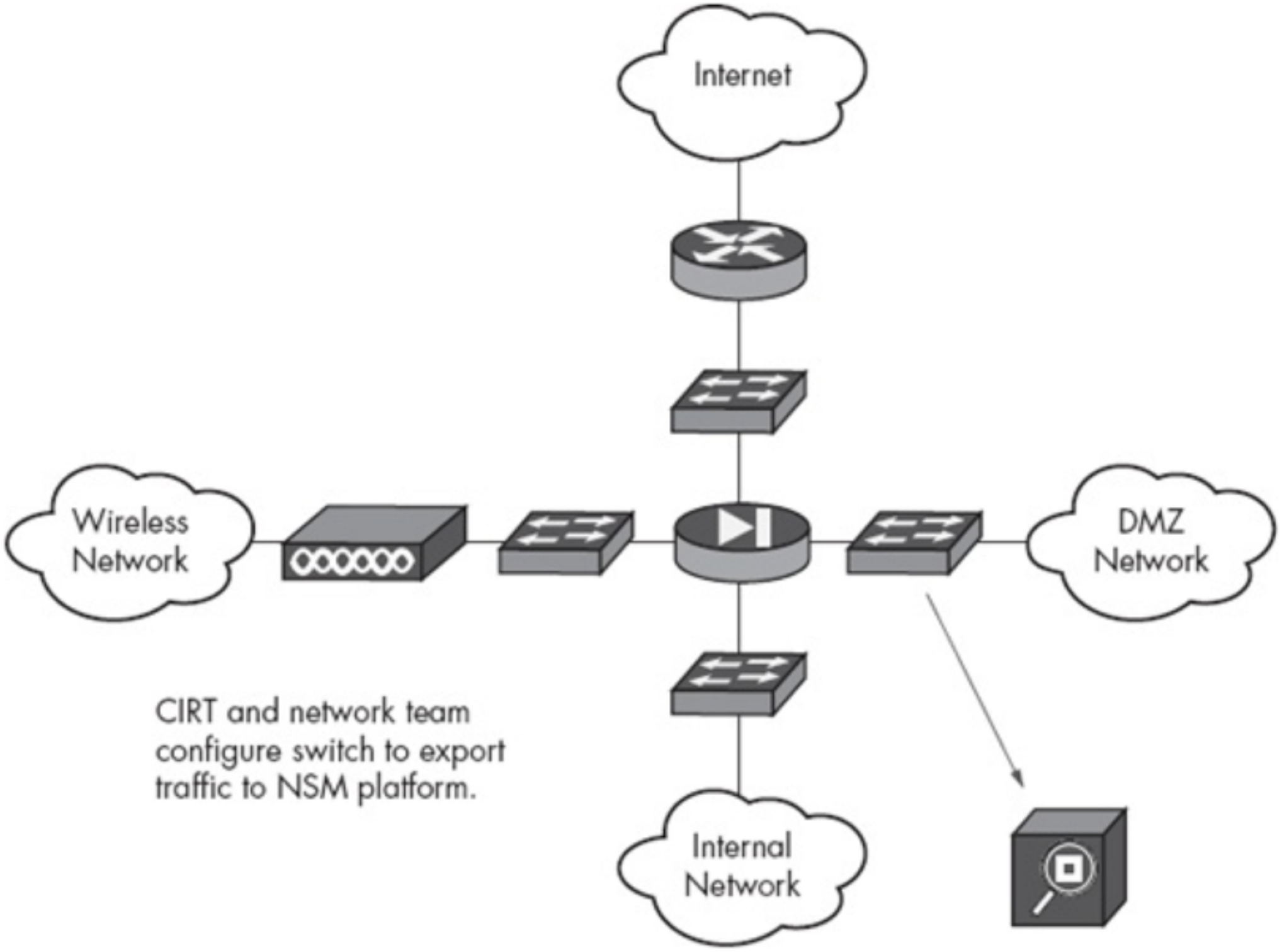


Figure 1-4. Simple network diagram and NSM platform

Installing a Tap

- **Better way**

- **Dedicated hardware to access network traffic**

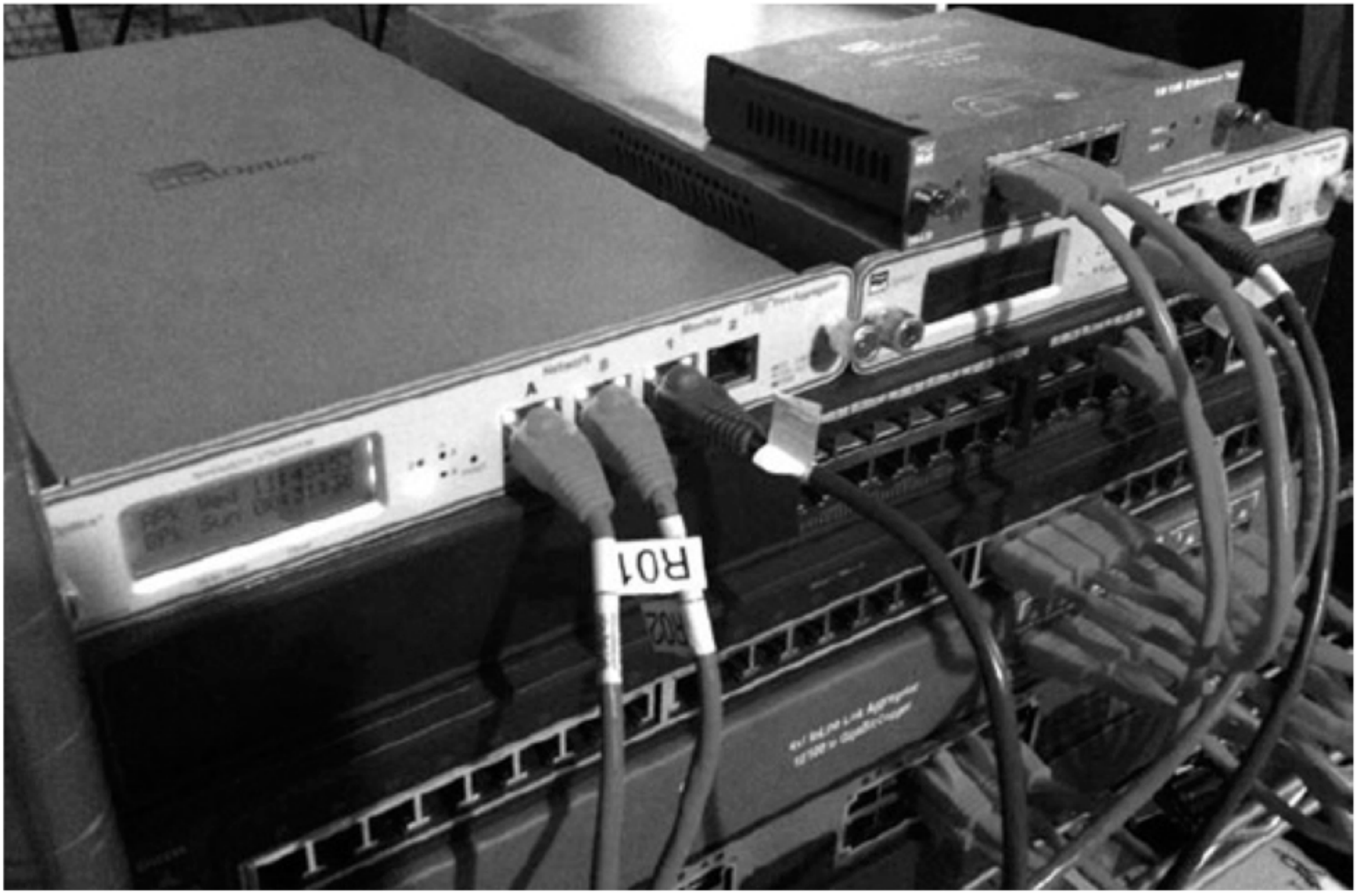


Figure 1-5. Network taps and switches

When NSM Won't Work

- **Wireless traffic difficult to monitor, because it's encrypted**
- **Wireless traffic between wireless devices won't be monitored**
- **If it goes through the wired LAN, it will be detected**
- **Cellular traffic also difficult to monitor**

Cloud or Hosted Environments

- **Service provider owns infrastructure**
- **They may monitor network, but customers can't access the data**
- **Similar situation with ISPs and telcos**

Is NSM Legal?

- **Get legal advice**
- **Wiretap Act: U.S. Code 18 § 2511**
  - **Company is allowed to monitor traffic when necessary to provide service or to protect their rights or property**
  - **Also OK if one party has given consent for monitoring**
- **State laws also may apply**

Protecting User Privacy

- **CIRTs should focus on external threats**
- **Forensics professionals focus on internal threats**

Sample NSM Test

- **Looks like someone got a root shell and ran the id command**

Network Traffic

- **DNS request and reply for *www.test,yids.com***
- **HTTP request from browser and reply**
- **Browser requests favicon and server replies**


Kahoot!

The Range of NSM Data

May Include

- Full content
- Extracted content
- Session data
- Transaction data
- Statistical data
- Metadata
- Alert data

Full Content Data

- **Exact copies of all network traffic**
- **Reviewed in two stages**
  - **Summary of data headers**
  - **Inspection of individual packets**

Headers from Wireshark

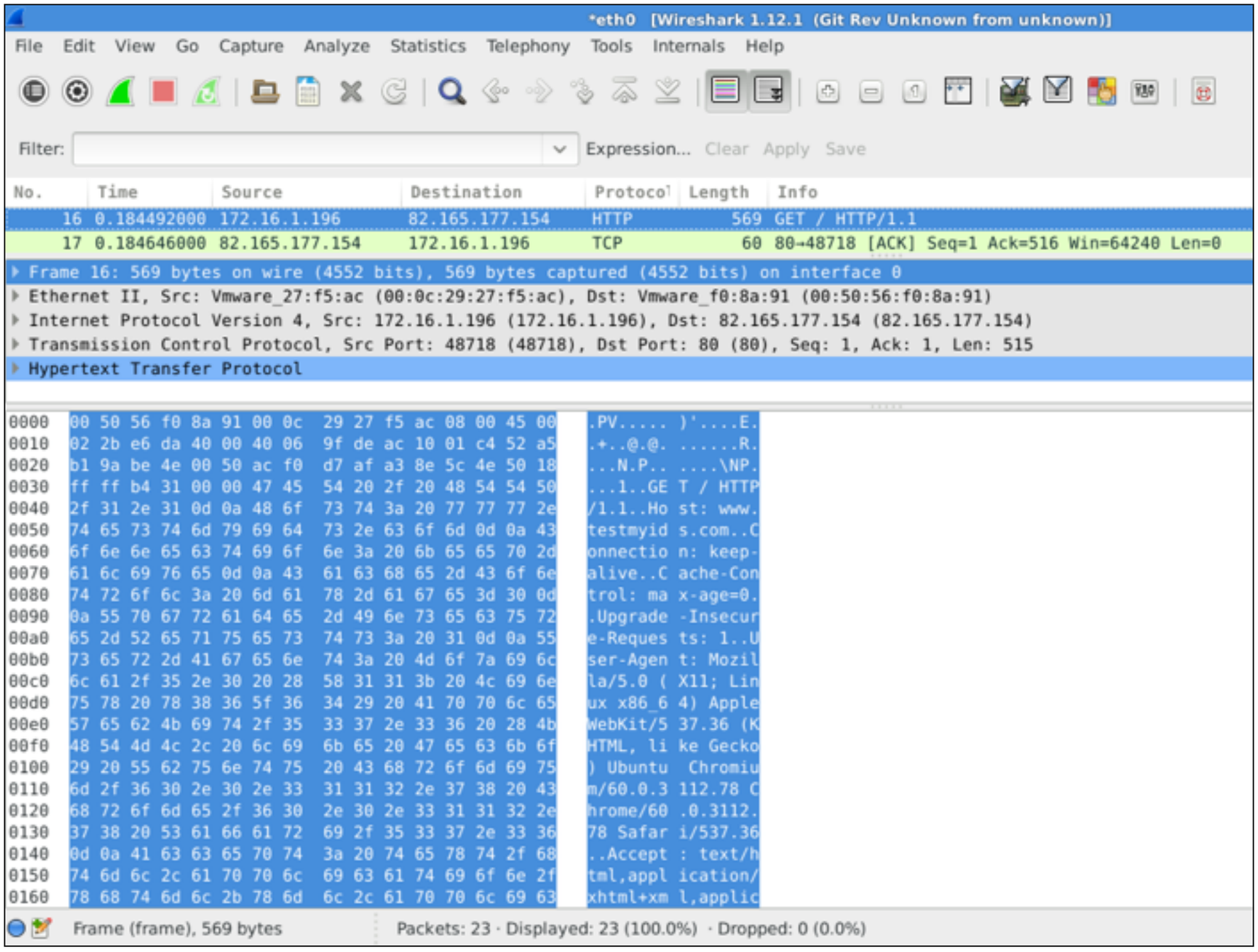
No.	Time	Source	Destination	Length	Protocol	Info
1	0.000000000	172.16.1.1	224.0.0.251	82	MDNS	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
2	6.160324284	172.16.1.188	172.16.1.2	77	DNS	Standard query 0xf18e A www.testmyids.com
3	6.160388273	172.16.1.188	172.16.1.2	77	DNS	Standard query 0x4237 AAAA www.testmyids.com
4	6.192605470	172.16.1.2	172.16.1.188	93	DNS	Standard query response 0xf18e A www.testmyids.com A 82.165.177.15
5	6.194689720	172.16.1.2	172.16.1.188	124	DNS	Standard query response 0x4237 AAAA www.testmyids.com CNAME www.te
6	6.194889965	172.16.1.188	82.165.177.1…	74	TCP	43656 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=
7	6.380027648	82.165.177.154	172.16.1.188	60	TCP	80 → 43656 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
8	6.380074715	172.16.1.188	82.165.177.1…	54	TCP	43656 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
9	6.380271638	172.16.1.188	82.165.177.1…	382	HTTP	GET / HTTP/1.1
10	6.380408693	82.165.177.154	172.16.1.188	60	TCP	80 → 43656 [ACK] Seq=1 Ack=329 Win=64240 Len=0
11	6.567109047	82.165.177.154	172.16.1.188	360	HTTP	HTTP/1.1 200 OK (text/html)
12	6.567160106	172.16.1.188	82.165.177.1…	54	TCP	43656 → 80 [ACK] Seq=329 Ack=307 Win=30016 Len=0
13	8.568233174	172.16.1.188	82.165.177.1…	54	TCP	43656 → 80 [FIN, ACK] Seq=329 Ack=307 Win=30016 Len=0
14	8.568455079	82.165.177.154	172.16.1.188	60	TCP	80 → 43656 [ACK] Seq=307 Ack=330 Win=64239 Len=0
15	8.568993657	82.165.177.154	172.16.1.188	60	TCP	80 → 43656 [FIN, PSH, ACK] Seq=307 Ack=330 Win=64239 Len=0
16	8.569017749	172.16.1.188	82.165.177.1…	54	TCP	43656 → 80 [ACK] Seq=330 Ack=308 Win=30016 Len=0

Headers from Tcpdump

```
03:11:53.031231 IP 172.16.1.188.38998 > 172.16.1.2.53: 65532+ A? www.testmyids.com. (35)
03:11:53.031292 IP 172.16.1.188.38998 > 172.16.1.2.53: 46799+ AAAA? www.testmyids.com. (35)
03:11:53.063962 ARP, Request who-has 172.16.1.188 tell 172.16.1.2, length 46
03:11:53.063978 ARP, Reply 172.16.1.188 is-at 00:0c:29:52:bb:35, length 28
03:11:53.064085 IP 172.16.1.2.53 > 172.16.1.188.38998: 65532 1/0/0 A 82.165.177.154 (51)
03:11:53.088789 IP 172.16.1.2.53 > 172.16.1.188.38998: 46799*- 2/0/0 CNAME www.testmyids.com., A 82.165.177.154 (82)
03:11:53.088991 IP 172.16.1.188.43658 > 82.165.177.154.80: Flags [S], seq 1034088282, win 29200, options [mss 1460,sackOK,TS val 9867151 ecr 0,nop,
03:11:53.269935 IP 82.165.177.154.80 > 172.16.1.188.43658: Flags [S.], seq 3493996192, ack 1034088283, win 64240, options [mss 1460], length 0
03:11:53.269967 IP 172.16.1.188.43658 > 82.165.177.154.80: Flags [.], ack 1, win 29200, length 0
03:11:53.270194 IP 172.16.1.188.43658 > 82.165.177.154.80: Flags [P.], seq 1:329, ack 1, win 29200, length 328: HTTP: GET / HTTP/1.1
03:11:53.270340 IP 82.165.177.154.80 > 172.16.1.188.43658: Flags [.], ack 329, win 64240, length 0
03:11:53.451877 IP 82.165.177.154.80 > 172.16.1.188.43658: Flags [P.], seq 1:307, ack 329, win 64240, length 306: HTTP: HTTP/1.1 200 OK
03:11:53.451896 IP 172.16.1.188.43658 > 82.165.177.154.80: Flags [.], ack 307, win 30016, length 0
03:11:55.449654 IP 82.165.177.154.80 > 172.16.1.188.43658: Flags [FP.], seq 307, ack 329, win 64240, length 0
03:11:55.449781 IP 172.16.1.188.43658 > 82.165.177.154.80: Flags [F.], seq 329, ack 308, win 30016, length 0
03:11:55.449994 IP 82.165.177.154.80 > 172.16.1.188.43658: Flags [.], ack 330, win 64239, length 0
```

- **Demo: tcpdump -n > foo**

Whole Packet in Wireshark

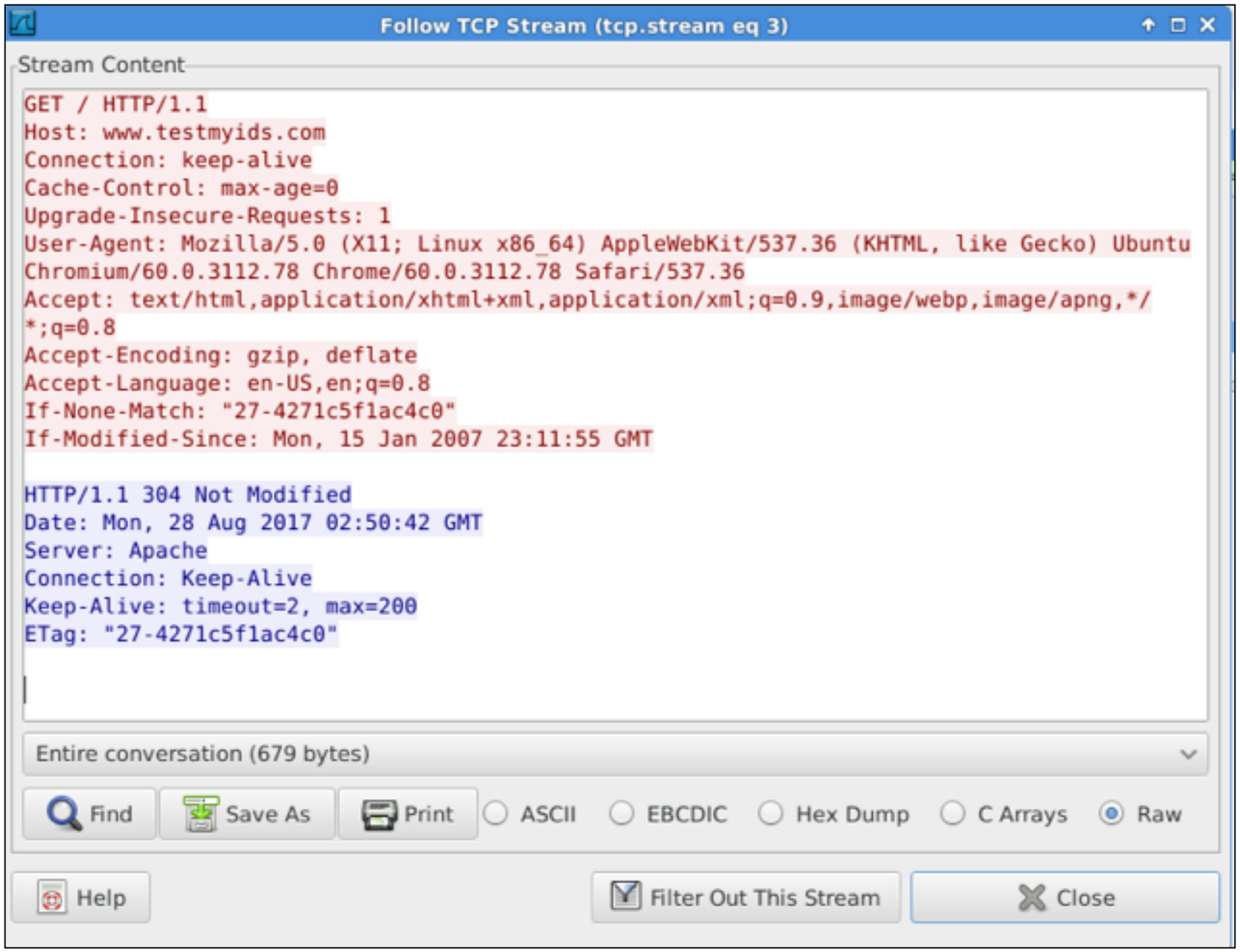


Complete Packet in Tcpdump

```
03:15:02.934696 IP 172.16.1.188.43660 > 82.165.177.154.80: Flags [P.], seq 1:397, ack 1, win 29200, length 396: HTTP: GET / HTTP/1.1
        0x0000:  4500 01b4 5e00 4000 4006 2938 ac10 01bc  E...^.@.@.)8....
        0x0010:  52a5 b19a aa8c 0050 80eb 153a 640c 8c66  R......P...:d..f
        0x0020:  5018 7210 61bf 0000 4745 5420 2f20 4854  P.r.a...GET./.HT
        0x0030:  5450 2f31 2e31 0d0a 486f 7374 3a20 7777  TP/1.1..Host:.ww
        0x0040:  772e 7465 7374 6d79 6964 732e 636f 6d0d  w.testmyids.com.
        0x0050:  0a55 7365 722d 4167 656e 743a 204d 6f7a  .User-Agent:.Moz
        0x0060:  696c 6c61 2f35 2e30 2028 5831 313b 204c  illa/5.0.(X11;.L
        0x0070:  696e 7578 2069 3638 363b 2072 763a 3435  inux.i686;.rv:45
        0x0080:  2e30 2920 4765 636b 6f2f 3230 3130 3031  .0).Gecko/201001
        0x0090:  3031 2046 6972 6566 6f78 2f34 352e 300d  01.Firefox/45.0.
        0x00a0:  0a41 6363 6570 743a 2074 6578 742f 6874  .Accept:.text/ht
```

- **Demo: tcpdump -nX > foo**

TCP Stream in Wireshark



- **Right-click packet, Follow TCP Stream**

Save PCAP File

- **In Wireshark, save as .pcap**
  - **NOT .pcapng**

Start Xplico

- **Connect to http://172.16.1.196:9876/**
  - **Using the IP of your Security Onion VM**
- **Log in as**
  - **xplico**
  - **xplico**

Make a PCAP

- **On host system, open Wireshark**
- **Surf some non-encrypted sites in a Browser**
  - **ad.samsclass.info**
  - **www.testmyids.com**
  - **http://www.kittenwar.com/**
- **Save in WIreshark/tcpdump pcap format**

Xplico Demo Steps

- **Make a new case and a new session**
- **Upload the PCAP**
- **Wait for decoding**

172.16.1.196:9876/sols/view/1

Xplico Interface

User: xplico

Help | Forum | Wiki | CapAnalysis | Change password | Licenses | Logout

- Case
  - Cases
  - Sessions
  - Session
- Graphs
- Web
- Mail
- Voip
- Share
- Chat
- Shell
- Undecoded

CapAnalysis

Follow @xplico

Session Data

Case and Session name	d -> d
Cap. Start Time	2017-08-28 21:11:08
Cap. End Time	2017-08-28 21:11:54
Status	DECODING COMPLETED
Hosts	

Filter

Pcap set

PCAP-over-IP TCP port: 30001.

Add new pcap file.

Choose File | No file chosen

Upload

List of all pcap files.

HTTP

Post	0
Get	33
Video	0
Images	10

MMS

Number	0
Contents	0
Video	0
Images	0

Emails

Received	0
Sent	0
Unreaded	0/0

FTP - TFTP - HTTP file

Connections	0 - 0
Downloaded	0 - 0
Uploaded	0 - 0
HTTP	0

Web Mail

Total	0
Received	0
Sent	0

Facebook Chat / Paltalk

Users	0
Chats	0/0

IRC/Paltalk Exp/Msn/Yahoo!

Server	0
Channels	0/0/0/0

Dns - Arp - Icmpv6

DNS res	8
ARP/ICMPv6	7/0

RTP/VoIP

Video	0
Audio	0

NNTP

Groups	0
Articles	0

Feed & Printed files

Number	0
Pdf	0

WhatsApp

Connection	0

Telnet / Syslog

Connections	0/0

SIP

Calls	0

Undecoded

Text flows	3/18
Dig	0

172.16.1.196:9876/webs/index

Xplico Interface

User: xplico

Help Forum Wiki CapAnalysis Change password Licenses Logout

- Case
- Graphs
- Web
  - Site
  - Feed
  - Images
- Mail
- Voip
- Share
- Chat
- Shell
- Undecoded

CapAnalysis

Follow @xplico

For a complete view of html page set your browser to use Proxy, and point it to Web server.

Web URLs: (•) Html ( ) Image ( ) Flash ( ) Video ( ) Audio ( ) JSON ( ) All

Search: [ ] Go

Date	Url	Size	Method	Info
2017-08-28 14:11:50	www.kittenwar.com/	2377	GET	info.xml
2017-08-28 14:11:44	www.kittenwar.com/	2380	GET	info.xml
2017-08-28 14:11:42	www.kittenwar.com/	2378	GET	info.xml
2017-08-28 14:11:39	www.kittenwar.com/	2381	GET	info.xml
2017-08-28 14:11:36	www.kittenwar.com/	2375	GET	info.xml
2017-08-28 14:11:32	www.testmyids.com/	39	GET	info.xml
2017-08-28 14:11:32	www.testmyids.com/favicon.ico			nfo.xml
2017-08-28 14:11:30	www.testmyids.com/favicon.ico			nfo.xml
2017-08-28 14:11:23	ad.samsclass.info/			nfo.xml
2017-08-28 14:11:23	ad.samsclass.info/teal_leaf.gif			nfo.xml
2017-08-28 14:11:23	ad.samsclass.info/favicon.ico			nfo.xml
2017-08-28 14:11:21	ad.samsclass.info/			nfo.xml
2017-08-28 14:11:21	ad.samsclass.info/teal_leaf.gif			nfo.xml
2017-08-28 14:11:21	ad.samsclass.info/favicon.ico	292	GET	info.xml

Previous 1 of 1 Next

Vulnerable Pages

172.16.1.196:9876/webs/resBody/6

Sam Bowne

Vulnerable Pages

172.16.1.196:9876/webs/images

Xplico Interface

User: xplico

Help Forum Wiki CapAnalysis Change password Licenses Logout

- Case
- Graphs
- Web
  - Site
  - Feed
  - Images
- Mail
- Voip
- Share
- Chat
- Shell
- Undecoded

CapAnalysis

Follow @xplico

Search: Go

 www.kittenwar.com Image or Page	 www.kittenwar.com Image or Page	 www.kittenwar.com Image or Page	 www.kittenwar.com Image or Page
 www.kittenwar.com Image or Page	 www.kittenwar.com Image or Page	 www.kittenwar.com Image or Page	 www.kittenwar.com Image or Page
 www.kittenwar.com Image or Page	 www.kittenwar.com Image or Page		

Previous 1 of 1 Next

Extracted Content Data

- **High-level data streams**
- **Like files, images, media**
- **Without IP or MAC addresses, etc.**
- **Wireshark is good at extracting files**
- **Xplico and other tools can do it too**

Session Data

- **Record of the conversation between two nodes**
- **Bro can generate session data logs**
  - **Sample data from link Ch 1a**

```
$ gzcat 2013-01-01/conn.00\:00\:00-00\:00\:00.log.gz | head
#separator \x09
#set_separator ,
#empty_field (empty)
#unset_field -
#path conn
#open 2013-01-01-00-00-01
#fields ts uid id.orig_h id.orig_p id.resp_h id.resp_p proto service dura
#types time string addr port addr port enum string interval count count s
1357016390.095574 qfuVcja4nb9 43.45.3.9 46137 93.191.121.39 53 udp dns 0.
1357016390.255919 mW8KwF7YXSb 43.45.3.9 22314 204.212.170.189 53 udp dns
```

Session Data

- **Session data is much smaller than full content data (PCAPs)**
- **Easier to store and search through**
- **Cannot reconstruct files and web pages from session data**

Transaction Data

- **Similar to session data**
- **Focuses on requests and replies**
- **Example: Bro http.log (link Ch 1b)**

```
# ts           uid           orig_h         orig_p  resp_h          resp_p
1311627961.8   HSH4uV8KVJg   192.168.1.100  52303   192.150.187.43  80
```

```
# method   host        uri  referrer  user_agent
GET        bro.org     /    -         <...>Chrome/12.0.742.122<...>
```

Statistical Data

- **Summaries of data**
- **Examples from Wireshark**
  - **Statistics, Capture File Properties**
  - **Statistics, Protocol Hierarchy**
  - **Statistics, Packet Lengths**

Wireshark · Capture File Properties · demo2pm

Details

First packet:	2017-08-28 14:11:08
Last packet:	2017-08-28 14:11:54
Elapsed:	00:00:46

Capture

Hardware:	Unknown
OS:	Unknown
Application:	Unknown

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
Unknown	Unknown	Unknown	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	6102	6102 (100.0%)	N/A
Time span, s	46.304	46.304	N/A
Average pps	131.8	131.8	N/A
Average packet size, B	821.5	821.5	N/A
Bytes	5015645	5015645 (100.0%)	0
Average bytes/s	108 k	108 k	N/A
Average bits/s	866 k	866 k	N/A

Wireshark · Protocol Hierarchy Statistics · demo2pm

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packet
Frame	100.0	6102	100.0	5015645	866 k	0
Ethernet	100.0	6102	1.7	85428	14 k	0
Internet Protocol Version 6	0.1	4	0.0	160	27	0
User Datagram Protocol	0.1	4	0.0	32	5	0
Multicast Domain Name System	0.1	4	0.0	160	27	4
Internet Protocol Version 4	99.9	6093	2.4	121860	21 k	0
User Datagram Protocol	2.7	167	0.0	1336	230	0
Simple Service Discovery Protocol	0.1	4	0.0	700	120	4
QUIC (Quick UDP Internet Connections)	2.1	127	0.5	25673	4435	127
Network Time Protocol	0.2	10	0.0	480	82	10
Multicast Domain Name System	0.1	4	0.0	160	27	4
Dropbox LAN sync Discovery Protocol	0.1	4	0.0	520	89	4
Domain Name System	0.3	18	0.0	1129	195	18
Transmission Control Protocol	97.1	5926	95.3	4777597	825 k	4870
Secure Sockets Layer	19.1	1165	98.7	4948048	854 k	988
Malformed Packet	0.1	4	0.0	0	0	4
Hypertext Transfer Protocol	1.0	64	4.1	205039	35 k	39
Line-based text data	0.2	15	2.1	105504	18 k	15
JPEG File Interchange Format	0.2	10	2.7	137065	23 k	10
Address Resolution Protocol	0.1	5	0.0	140	24	5

Wireshark · Packet Lengths · demo2pm

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
▼ Packet Lengths	6102	821.97	42	1514	0.1318	100%	3.3200	16.181
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	2255	65.48	42	79	0.0487	36.96%	1.2100	16.154
80-159	191	96.42	80	159	0.0041	3.13%	0.7100	16.292
160-319	131	233.33	160	313	0.0028	2.15%	0.0900	43.411
320-639	209	467.88	323	636	0.0045	3.43%	0.0600	18.710
640-1279	587	1029.45	652	1258	0.0127	9.62%	0.1700	16.065
1280-2559	2729	1508.59	1280	1514	0.0589	44.72%	2.2900	16.181
2560-5119	0	-	-	-	0.0000	0.00%	-	-
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

Metadata

- **Data about data**
- **Extract key elements from network traffic**
- **Use external tools to learn more about them**
- **Ex: whois, robtex (link Ch 1c)**

```
Sams-MacBook-Pro-3:proj sambowne$ whois testmyids.com
   Domain Name: TESTMYIDS.COM
   Registry Domain ID: 555360075_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.123-reg.co.uk
   Registrar URL: http://www.meshdigital.com
   Updated Date: 2016-08-08T23:52:59Z
   Creation Date: 2006-08-15T11:54:28Z
   Registry Expiry Date: 2018-08-15T11:54:28Z
   Registrar: 123-Reg Limited
   Registrar IANA ID: 1515
   Registrar Abuse Contact Email:
   Registrar Abuse Contact Phone:
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS59.1AND1.CO.UK
   Name Server: NS60.1AND1.CO.UK
   DNSSEC: unsigned
```

Robtex LTD [CY] | https://www.robtex.com/dns-lookup/testmyids.com

testmyids.com

Robtex>>>DNS>>>com>>>testmyids

Follow 612 followers

testmyids.com GO

Try our chrome extension!

ANALYSIS | RECORDS | SEO | WOT | SHARED | GRAPH | HISTORY | WHOIS | DNSBL | GRAPH(old)

ANALYSIS

Testmyids.com has two name servers, one mail server and one IP number.

1and1 name servers

The name servers are ns59.**1and1**.co.uk (used by 86,800 domains) and ns60.**1and1**.co.uk (used by 86,800 domains).

The combination is used by 86,800 domains.

Example: **univ3rsity.com**, **appletreecardiff.co.uk**, **givingonline.org.uk** and **ttf-management.com**.

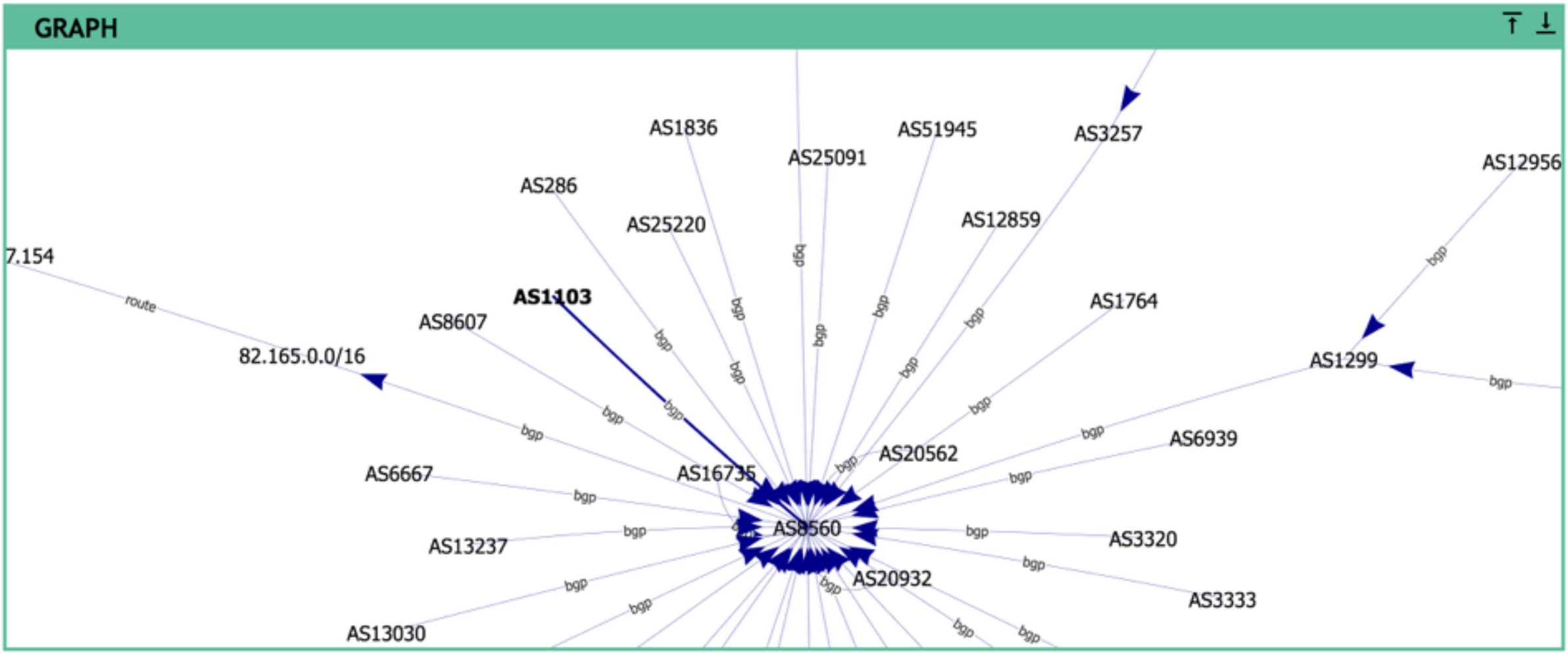
Ovh mail server

The mail server is vps30662.vps.**ovh**.ca (used by three domains).

Three domains use **only** the mail server vps30662.vps.**ovh**.ca.

Example: **hut7.org** and **wiul.org**.

GRAPH


AS1836
AS51945
AS3257
AS25091
AS12956
AS286
AS25220
AS12859
7.154
route
AS1103
AS1764
AS8607
82.165.0.0/16
AS1299
bgp
AS6939
AS20562
AS6667
AS16735
AS8560
AS3320
AS13237
AS20932
AS3333
AS13030

Alert Data

- **Event that triggers an Intrusion Detection System**
  - **Such as Snort or Suricata**
  - **Squil is a graphical console to view alert data**
  - **Image on next slide from link Ch 1d**

SGUIL-0.9.0 - Connected To 192.168.8.250

File | Query | Reports Sound: Off ServerName: 192.168.8.250 UserName: bamm UserID: 2 2014-11-07 02:02:09 GMT

RealTime Events | Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	fin-ext	1.313990	2014-11-07 00:44:43	222.186.21.55	4270	97.95.102.96	22	6	ET SCAN LibSSH Based SSH Connection - Often used as a BruteForce Tool
RT	1	fin-ext	1.313991	2014-11-07 00:45:55	213.136.94.87	5071	97.95.102.96	5060	17	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)
RT	1	fin-ext	1.313992	2014-11-07 00:45:55	213.136.94.87	5071	97.95.102.96	5060	17	ET SCAN Sipvicious Scan
RT	1	fin-int	7.1033042	2014-11-07 00:50:06	23.235.46.133	80	192.168.8.77	55300	6	ET SHELLCODE Excessive Use of HeapLib Objects Likely Malicious Heap Spray Attempt
RT	1	fin-ext	1.313993	2014-11-07 00:50:06	23.235.46.133	80	97.95.102.96	55300	6	ET SHELLCODE Excessive Use of HeapLib Objects Likely Malicious Heap Spray Attempt
RT	10	fin-int	7.1033043	2014-11-07 00:50:20	192.168.8.77	55435	208.85.40.20	80	6	ET POLICY Pandora Usage
RT	10	fin-ext	1.313994	2014-11-07 00:50:20	97.95.102.96	55435	208.85.40.20	80	6	ET POLICY Pandora Usage
RT	2	fin-int	7.1033052	2014-11-07 00:54:11	192.168.8.77	51775	192.168.8.253	53	17	ET CURRENT_EVENTS DNS Query to a .tk domain - Likely Hostile
RT	18	fin-int	7.1033054	2014-11-07 00:54:12	192.168.8.77	55671	66.6.44.4	80	6	ET CURRENT_EVENTS HTTP Request to a *.tk domain
RT	18	fin-ext	1.314003	2014-11-07 00:54:12	97.95.102.96	55671	66.6.44.4	80	6	ET CURRENT_EVENTS HTTP Request to a *.tk domain
RT	16	fin-ext	1.314022	2014-11-07 00:59:23	122.225.109.100	50117	97.95.102.96	22	6	ET SCAN LibSSH Based SSH Connection - Often used as a BruteForce Tool
RT	16	fin-int	7.1033080	2014-11-07 00:59:23	122.225.109.100	50117	192.168.8.8	22	6	ET SCAN LibSSH Based SSH Connection - Often used as a BruteForce Tool
RT	8	fin-ext	1.314031	2014-11-07 01:03:40	122.225.109.100	34787	97.95.102.96	22	6	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack!
RT	8	fin-int	7.1033089	2014-11-07 01:03:40	122.225.109.100	34787	192.168.8.8	22	6	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack!
RT	1	fin-ext	1.314059	2014-11-07 01:31:02	221.229.162.150	6000	97.95.102.96	3306	6	ET POLICY Suspicious inbound to mySQL port 3306
RT	2	fin-ext	1.314060	2014-11-07 01:40:46	97.95.102.96	44752	192.30.252.129	22	6	ET SCAN Potential SSH Scan OUTBOUND
RT	1	fin-int	7.1033117	2014-11-07 01:41:31	192.168.8.72	64916	192.30.252.131	22	6	ET SCAN Potential SSH Scan OUTBOUND

IP Resolution | Agent Status | Snort Statistics | System Msgs | User Msgs

Reverse DNS Enable External DNS

Src IP:
Src Name:

Dst IP:
Dst Name:

Whois Query: None Src IP Dst IP

```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '122.225.109.0 - 122.225.109.127'

inetnum:        122.225.109.0 - 122.225.109.127
netname:        DINGQI-NETWORK-TECHNOLOGY
country:        CN
descr:          Shaoxing Dingqi Network Technology Co., Ltd.
descr:
admin-c:        JS2095-AP
tech-c:         CH119-AP
mnt-irt:        IRT-CHINANET-ZJ
```

Show Packet Data Show Rule

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack!";
flow:established,to_server; content:"SSH-"; content:"libssh"; within:20; threshold: type both, count 5, seconds 30, track by_src;
reference:url,doc.emergingthreats.net/2006546; classtype:attempted-admin; sid:2006546; rev:5;)
/sguild_data/rules/fin-int/emerging-scan.rules: Line 490
```

IP

Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
122.225.109.100	192.168.8.8	4	5	40	63	20152	2	0	103	5091

TCP

Source Port	Dest Port	R1	R0	URG	ACK	PSH	RST	SYN	FIN	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
34787	22	.	.	.	X	X	.	.	.	4171882588	3428280706	5	0	65535	0	21499

DATA

```
53 53 48 2D 32 2E 30 2D 6C 69 62 73 73 68 32 5F    SSH-2.0-libssh2_
31 2E 34 2E 32 0D 0A                               1.4.2..
```

Search Packet Payload Hex Text NoCase

What's the Point of All this Data?

- **Equips CIRTs to detect, respond to, and contain intruders**
- **Complements efforts of other tools and systems**
- **Analysts can discover and act on intrusions early**

Retrospective Security Analysis (RSA)

- **Applies newly discovered threat intelligence**
- **To previously collected data**
- **Hoping to find intruders who evaded earlier detection**

Postmortem Analysis

- **Examination following incident resolution**

NSM Drawbacks

Difficult Situations

- **Encrypted traffic such as VPNs, which conceal data, and also source and destination addresses**
- **Network Address Translation (NAT) conceals source and destination addresses**
- **Mobile devices use networks that are not monitored**
- **High traffic volume may overwhelm NSM platform**
- **Privacy concerns may limit access to traffic**


Kahoot!