Cyber Security Technologies

Session 12 – IDS/IPS

Shawn Davis
ITMS 448 – Spring 2016

Slides contain original content from Davis, S. and may contain content from Ch.8 and 9 of Stallings, W. and Brown, B, Computer Security 2ed; Pearson Education, Inc. 2012

Today

- We will be using RADISH for the hand's on portion of this lecture

Overview

Part I – IDS Introduction

Part II – Host Based IDS (HIDS)

Part III – Network Based IDS (NIDS)

Part IV – SecurityOnion

Part V – SecurityOnion Hands On Lab

Part I

IDS Introduction

Intrusion

- A significant issue in organizations is hostile or unwanted trespass by users or software
- User trespass:
  - Unauthorized logon
  - Authorized logon but acquisition of privileges or activities performed outside of user authorization
- Software trespass:
  - Malware

Examples of Intrusion

- Remote root compromise
- Web server defacement
- Guessing / cracking passwords
- Copying databases containing credit card numbers
- Viewing sensitive data without authorization

Examples of Intrusion (Cont.)

- Running a packet sniffer
- Distributing pirated software
- Using an unsecured modem to access internal network
- Impersonating an executive to get information
- Using an unattended workstation

Common Intruders

- Hackers
  - Attack for thrill and notoriety
- Criminal Enterprises
  - Attack for financial gains
- Internal Threats
  - Attack for financial gains, revenge, inadvertently, etc.

Hacker - Example

- Select target from reconnaissance
- Scan network with Nmap
- ID vulnerable services (Let's say pcAnywhere)
- Brute force attack on pcAnywhere password
- Install RAT called DameWare
- Wait for admin to log on so that his/her password can be captured
- Use that password to pivot across network systems

Criminal - Example

- Rents exploit kit servers
- Sends phishing email to targeted organization
- Waits for victims to be exploited and receive malware keylogger payload
- Victim's visit banking sites and their typed in credentials are sent to the criminal organization

Internal Threat - Example

- Employee receives escalated access for a project months back
- Admins don't audit access regularly and did not revoke the access after the project completed
- Employee is now disgruntled and decides to use access to view confidential proprietary source code
- Employee sets up FTP account and uploads source code to remote server

Intrusion Detection

- A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warnings of a wide variety of attacks

- Intrusion Detection System = IDS

Terminology

- Host-based IDS (HIDS):
  - Monitors events between single host and network gateway
- Network-based IDS (NIDS):
  - Monitors network traffic for particular network segment
- Sensors:
  - Responsible for collecting data such as packets, log files, etc.
  - Data is then sent to the analyzer

Terminology

- Analyzers:
  - Receive input from one or more sensors or from other analyzers
  - Is responsible for determining if an intrusion has occurred
- User Interface:
  - Allows analyst to view output from IDS and/or control the behavior of the system
- Intrusion Prevention System (IPS):
  - Ability to not only detect but also prevent an attack

Basic Principles

- IDS is simply another layer of defense
  - (Aside from firewalls, access control, authentication mechanisms, etc.)
- If intrusion is detected quickly, intruder can be identified quickly and ejected from system before too much damage occurs
- Effective IDS can act as a deterrent
- Information collected from IDS can assist in strengthening future intrusion prevention measures

Basic Principles (Cont.)

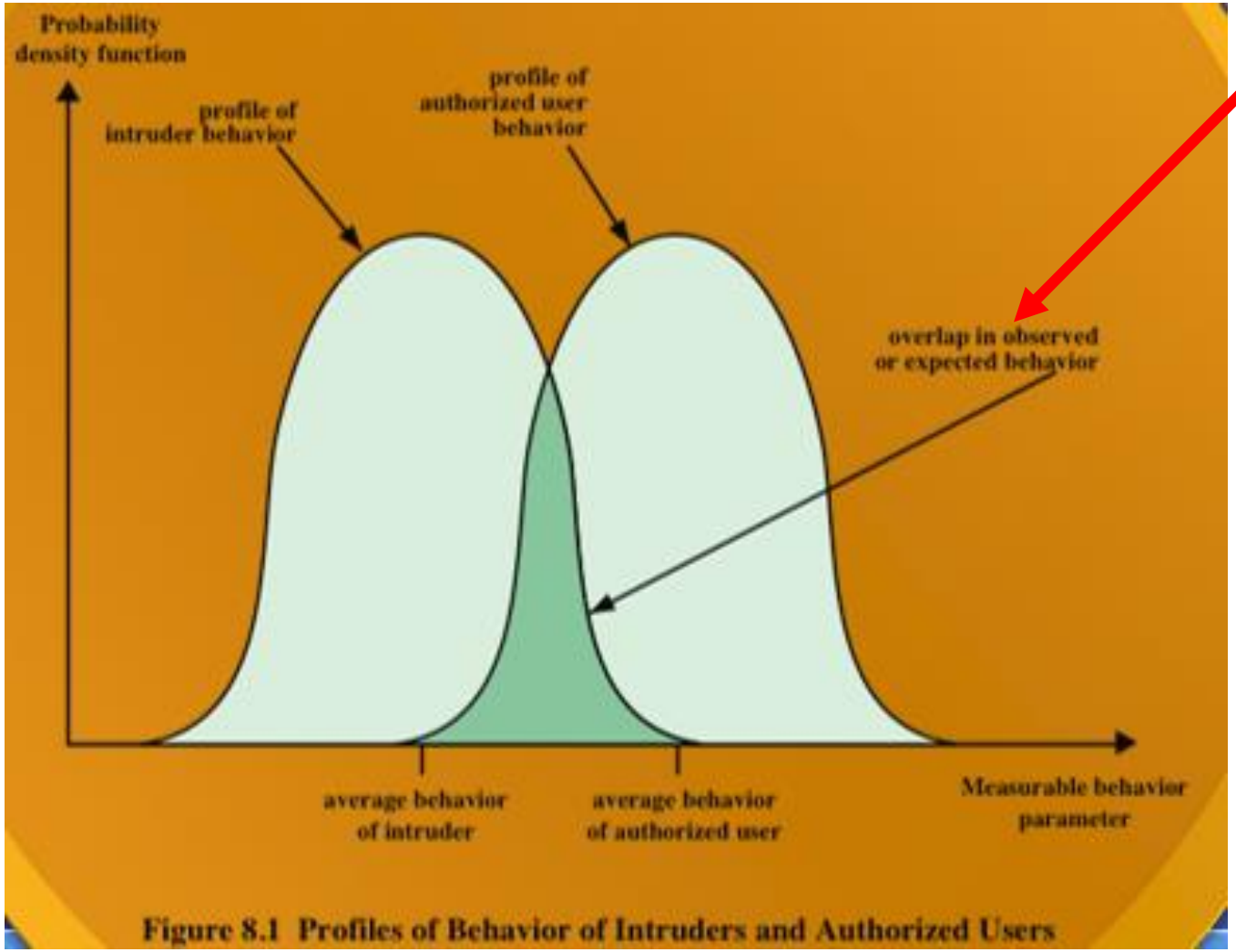


Figure 8.1 Profiles of Behavior of Intruders and Authorized Users

- Leads to:
  - False Positives (Authorized Users ID'd as intruders)
  - False Negatives (Intruders ID'd as Authorized Users)

General IDS Requirements

- Runs continually
- Fault tolerant
- Resists modification from attackers
- Imposes minimal overhead
- Configured according to security policies
- Should adapt to system and user behavior changes over time
- Scalable in number of hosts that it can monitor

General IDS Requirements (Cont.)

- If some components of IDS fail, rest should run unaffected
- Allow dynamic reconfiguration without requiring restart

Part II

Host-Based IDS (HIDS)

HIDS

- Installed on a host to monitor that specific host
  - Host = Workstation, Server, etc.
- Does not monitor hosts on a network
- Can be added to vulnerable or sensitive systems

HIDS (Cont.)

- Primary purpose is to:
  - Detect intrusions
  - Log suspicious events
  - Send alerts
- Can detect external and internal intrusions
  - (NIDS cannot detect internal intrusions)

Audit Records for HIDS

- Audit Records provide input data for the IDS
- Types of Records:
  - Native audit records
    - OS generated
    - Too verbose
  - Detection-specific audit records
    - Narrows down native audit records to only contain information required by HIDS

HIDS Detection Techniques

- Anomaly detection
  - Threshold detection (Frequency of event occurrence)
  - Profile based (Profile of user activity developed)
- Signature detection
  - Applies sets of rules from observing events on system

HIDS – Anomaly Detection Measures

- What do you think are some anomalies an IDS might detect???
  - Login frequency
  - Time since last login
  - Quantity of output
  - Session resource utilization
  - Password failures at local login and remote logins
  - Command execution frequency

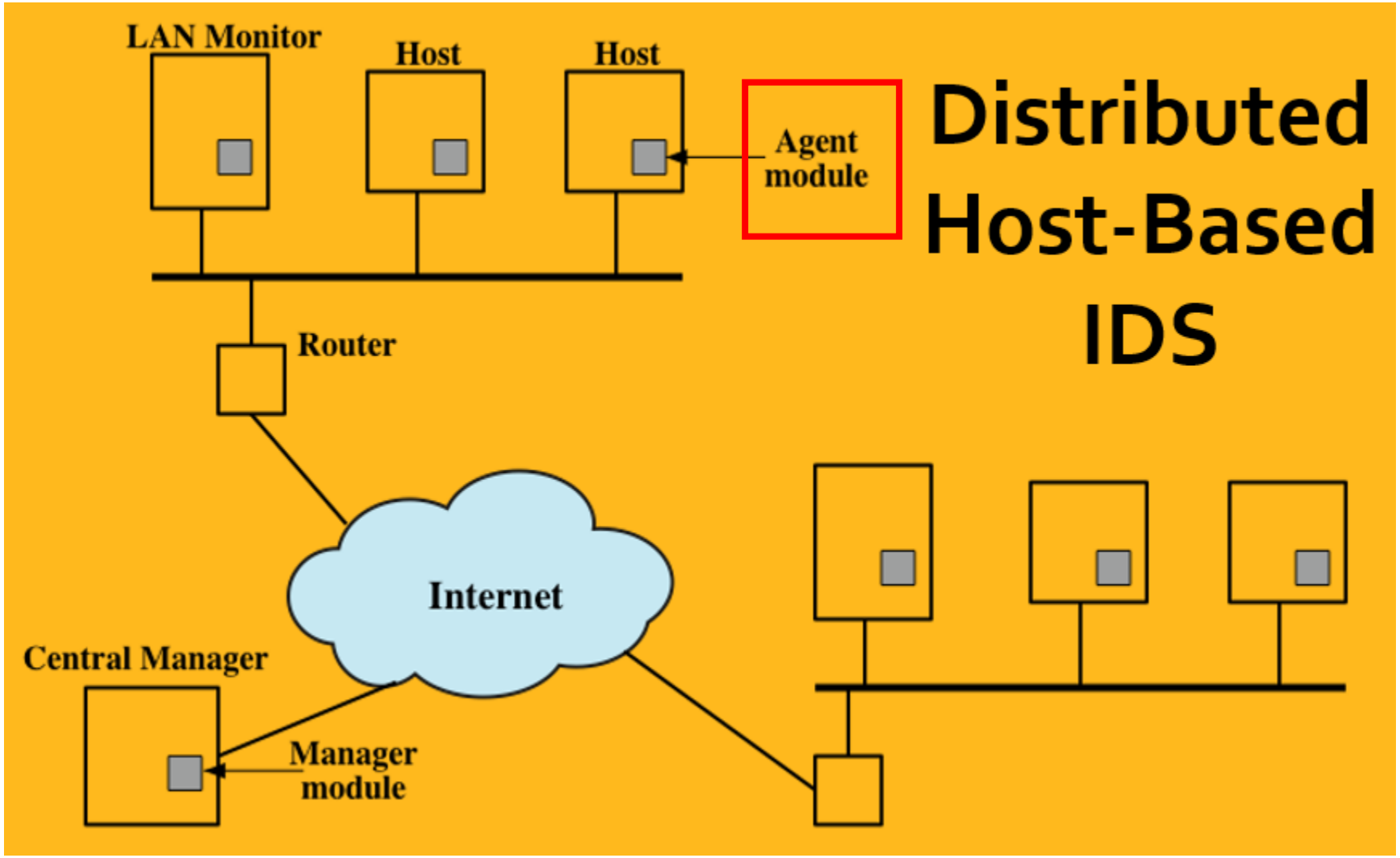
HIDS – Anomaly Detection Measures (Cont.)

- Program resource utilization
- Execution denials.
- Read, write, create, delete frequency and failures
- Read, write of sensitive data locations

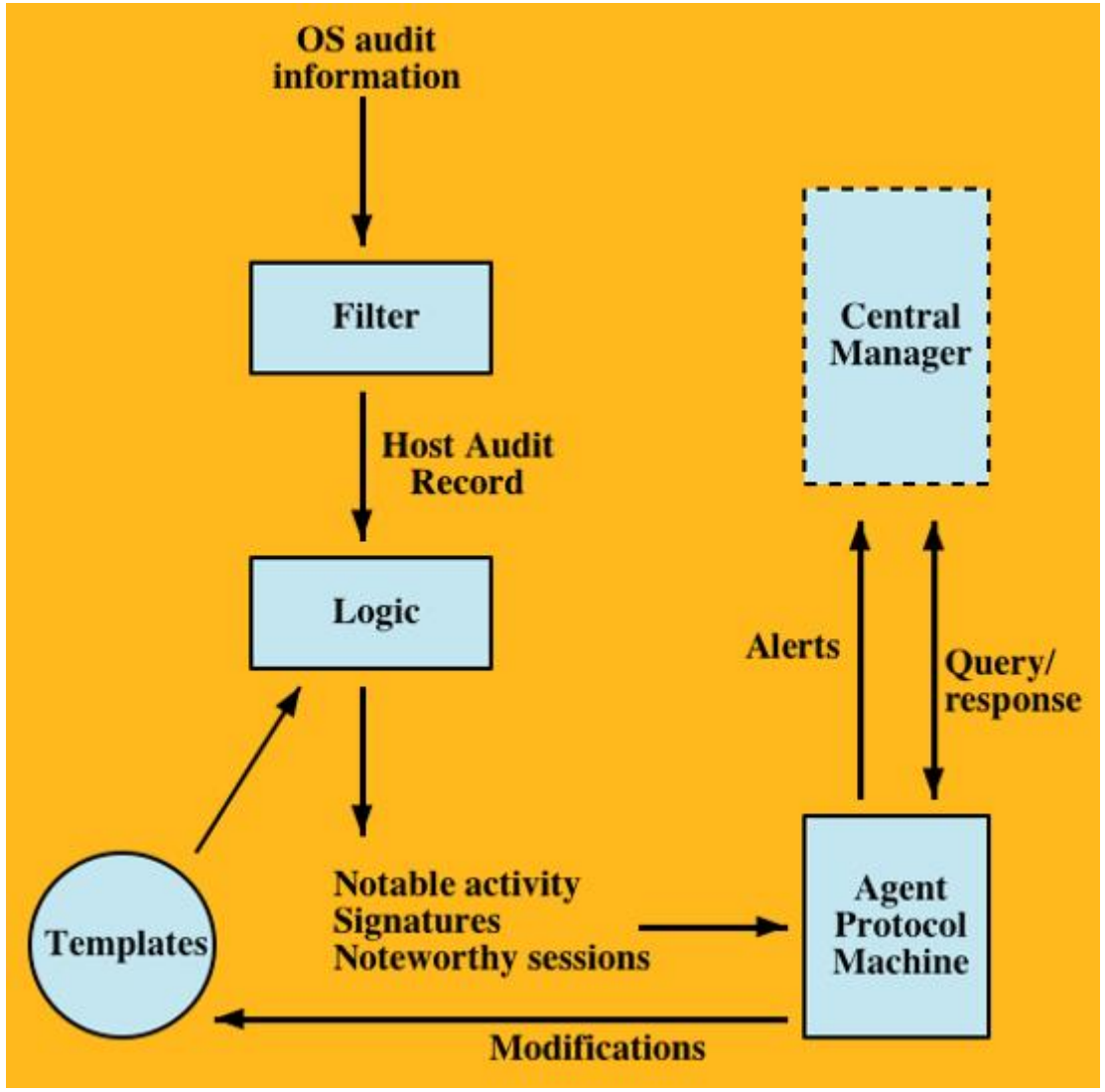
HIDS – Signature Detection Measures

- Rule-based anomaly detection
  - Current behavior is matched against set of rules
  - Large database of rules is needed
  - Historical audit records analyzed to identify usage patterns
- Rule-based penetration identification
  - Uses rules that ID known penetrations
  - Uses rules that ID suspicious behavior
  - Rules are generally specific to the system and its OS

Architecture for Distributed HIDS



Agent Module Architecture



Popular HIDS

- Tripwire
- OSSEC (We will use in the lab)
- Verisys

Part III

Network-Based IDS (NIDS)

NIDS

- Monitors traffic at selected points on a network
- Examines packets in real or close to real time
- May examine network, transport, and/or application-level protocol activity
- Comprised of:
  - Sensors
  - NIDS management server
  - User interface
- Analysis of traffic patterns may be done at sensor and/or management server

NIDS Deployment

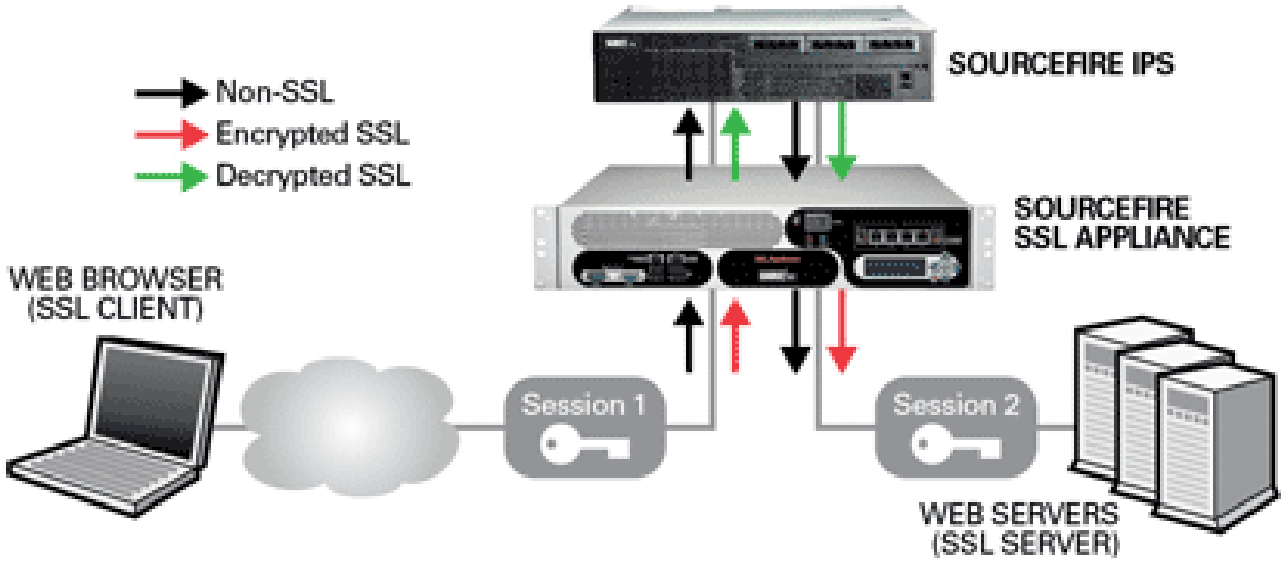
- You have several choices when deploying a NIDS

1. Do I want a single NIDS that includes one sensor or do I do I want to deploy multiple sensors to monitor traffic?
2. Where do I place the single NIDS or the multiple sensors?

Sensor Types

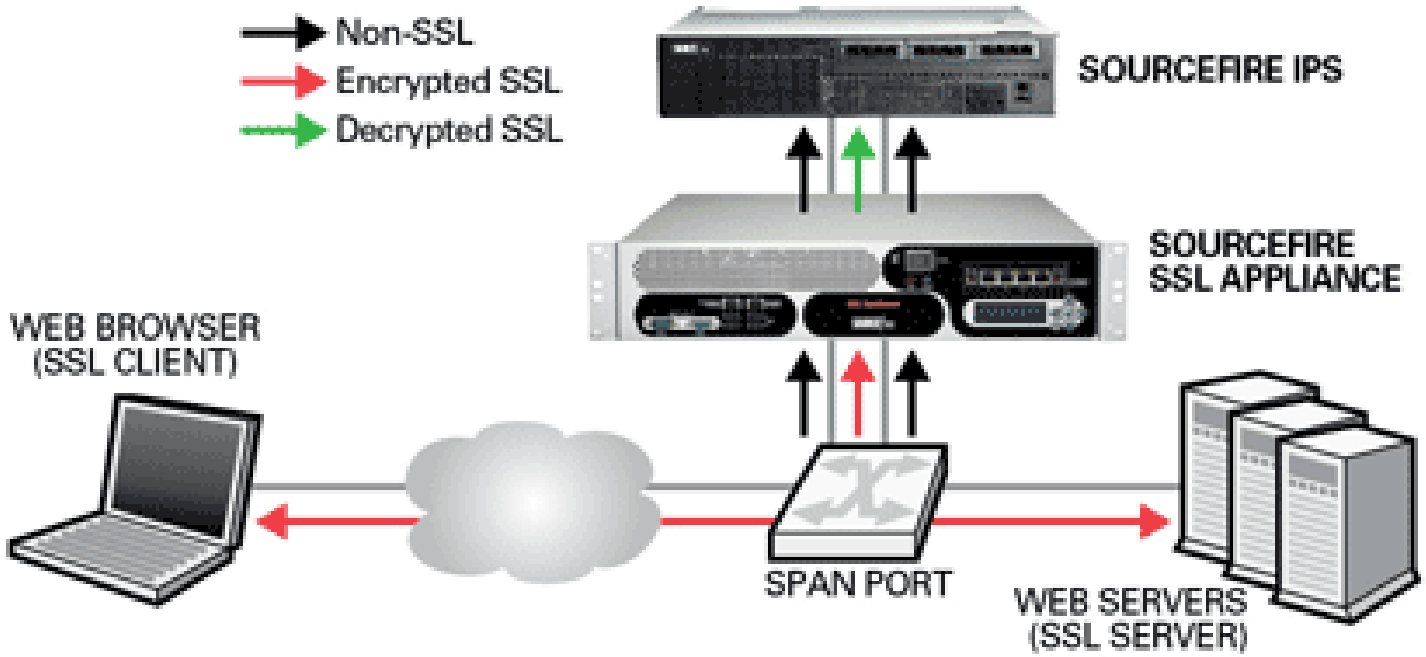
- Inline Sensor
  - Traffic passed through the sensor
- Passive Sensor
  - Traffic does not pass through the sensor
  - Monitors copy of traffic
- Sensor Server usually needs 3 interfaces
  - Ingress
  - Egress
  - Monitor

Inline IDS Sensor



http://www.ipsworks.com/SSL-Appliance.asp

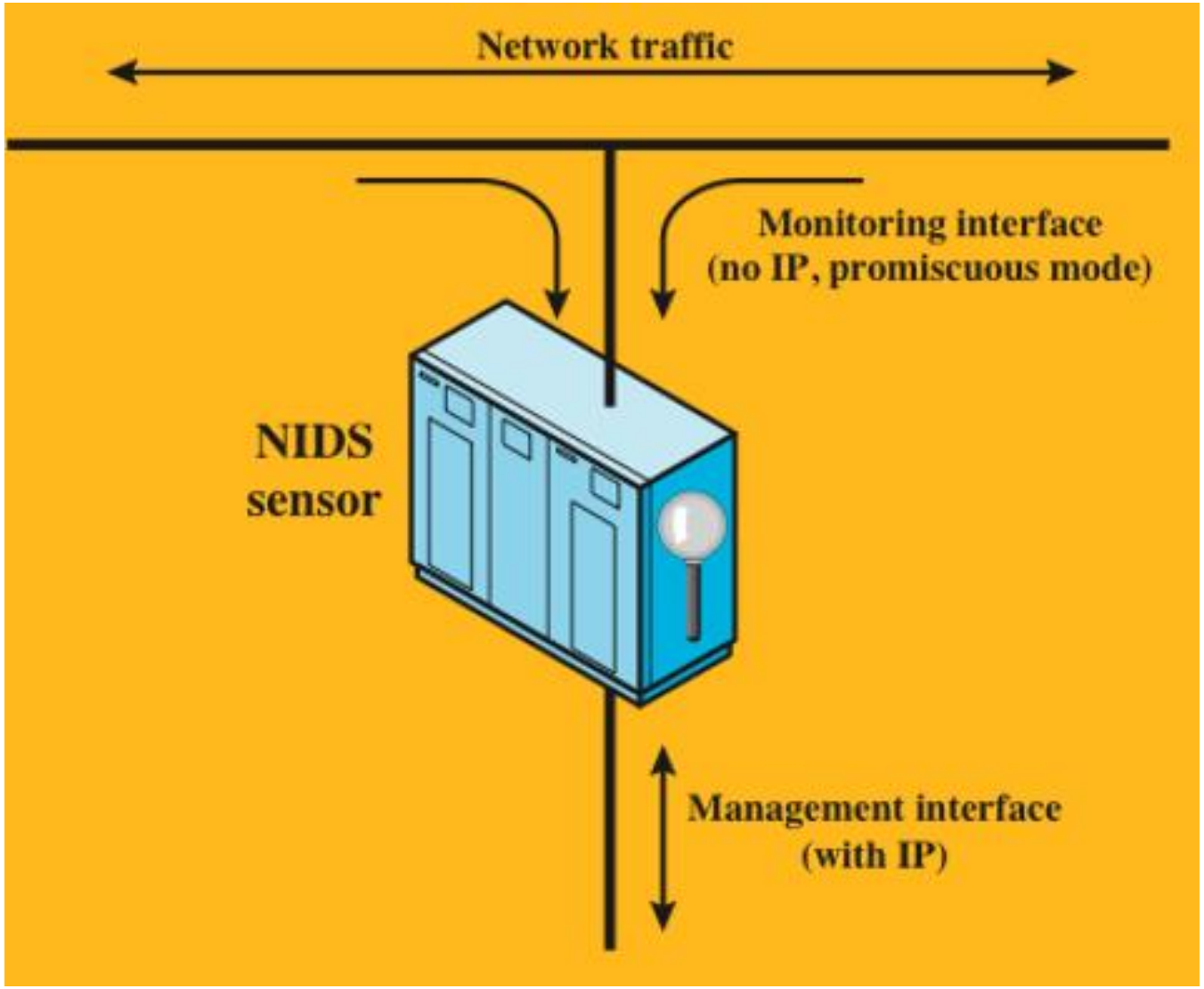
Passive IDS Sensor



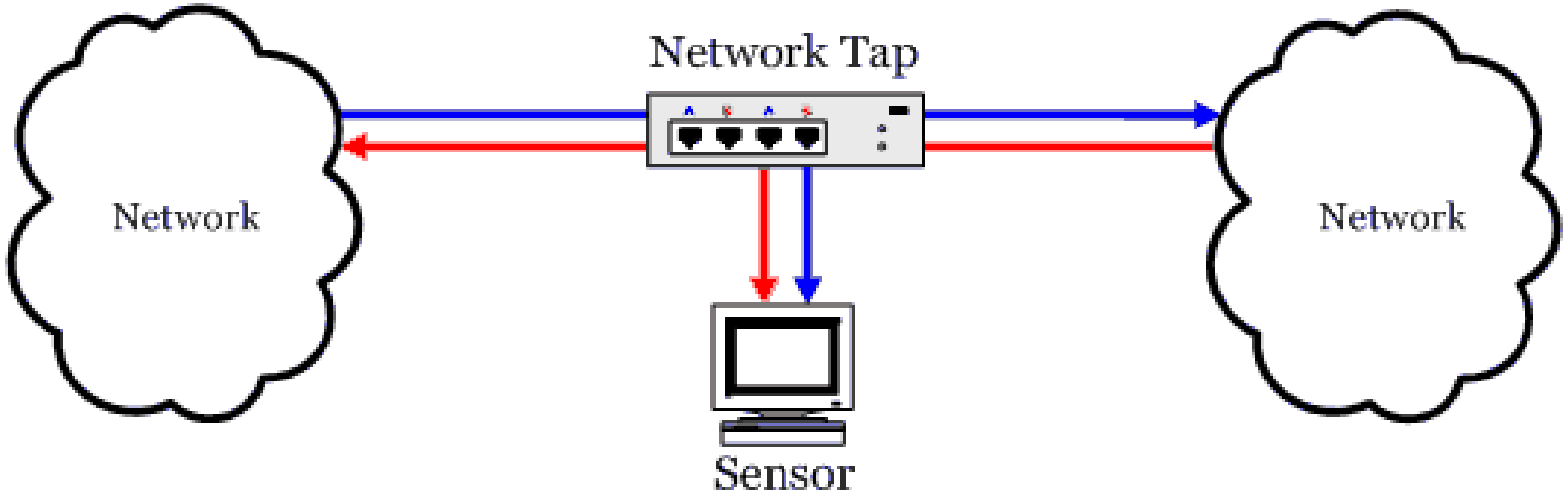
http://www.ipsworks.com/SSL-Appliance.asp

Passive Sensor

- May use:
  - Network TAP
  - Switch SPAN port

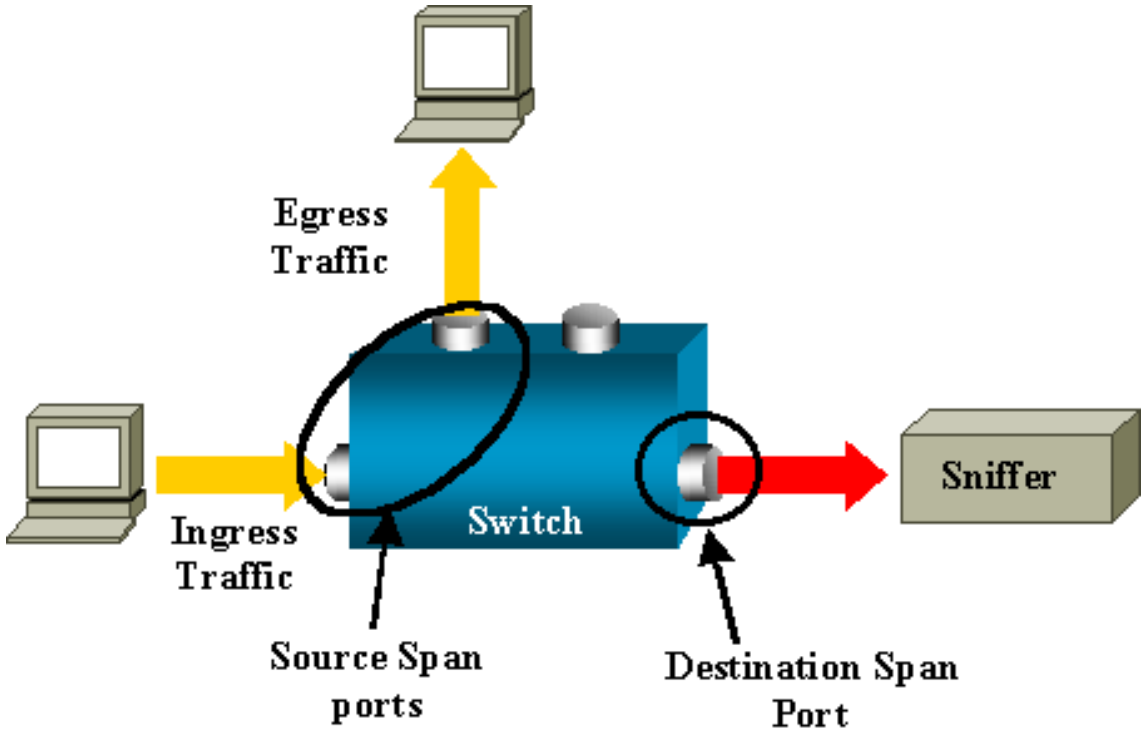


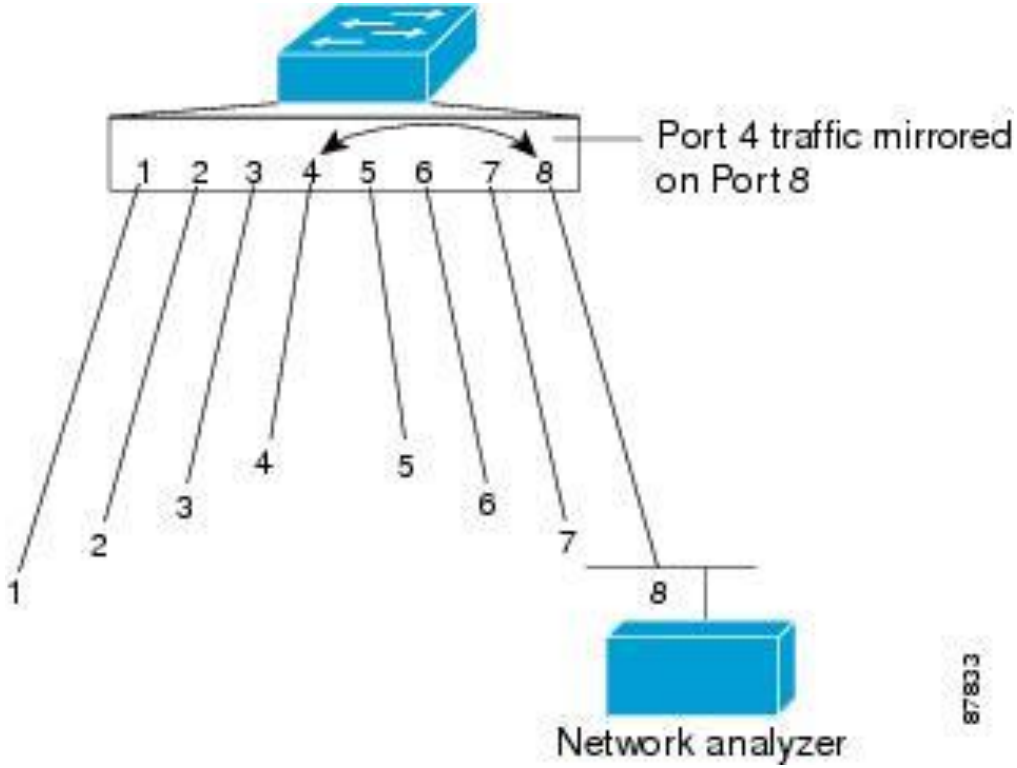
Network TAP



http://www.infosecwriters.com/hhworld/hh9/roc/node4.html

SPAN Port





http://www.cisco.com/c/dam/en/us/support/docs/switches/catalyst-6500-series-switches/10570-41d.gif
http://www.cisco.com/c/dam/en/us/td/i/000001-100000/85001-90000/87001-88000/87833.ps/_jcr_content/renditions/87833.jpg

NIDS/Sensor Placement Choices

- Behind the firewall
  - Records all traffic that passes **successfully** through the firewall
  - Requires dedicated server for NIDS sensor

NIDS/Sensor Placement Choices

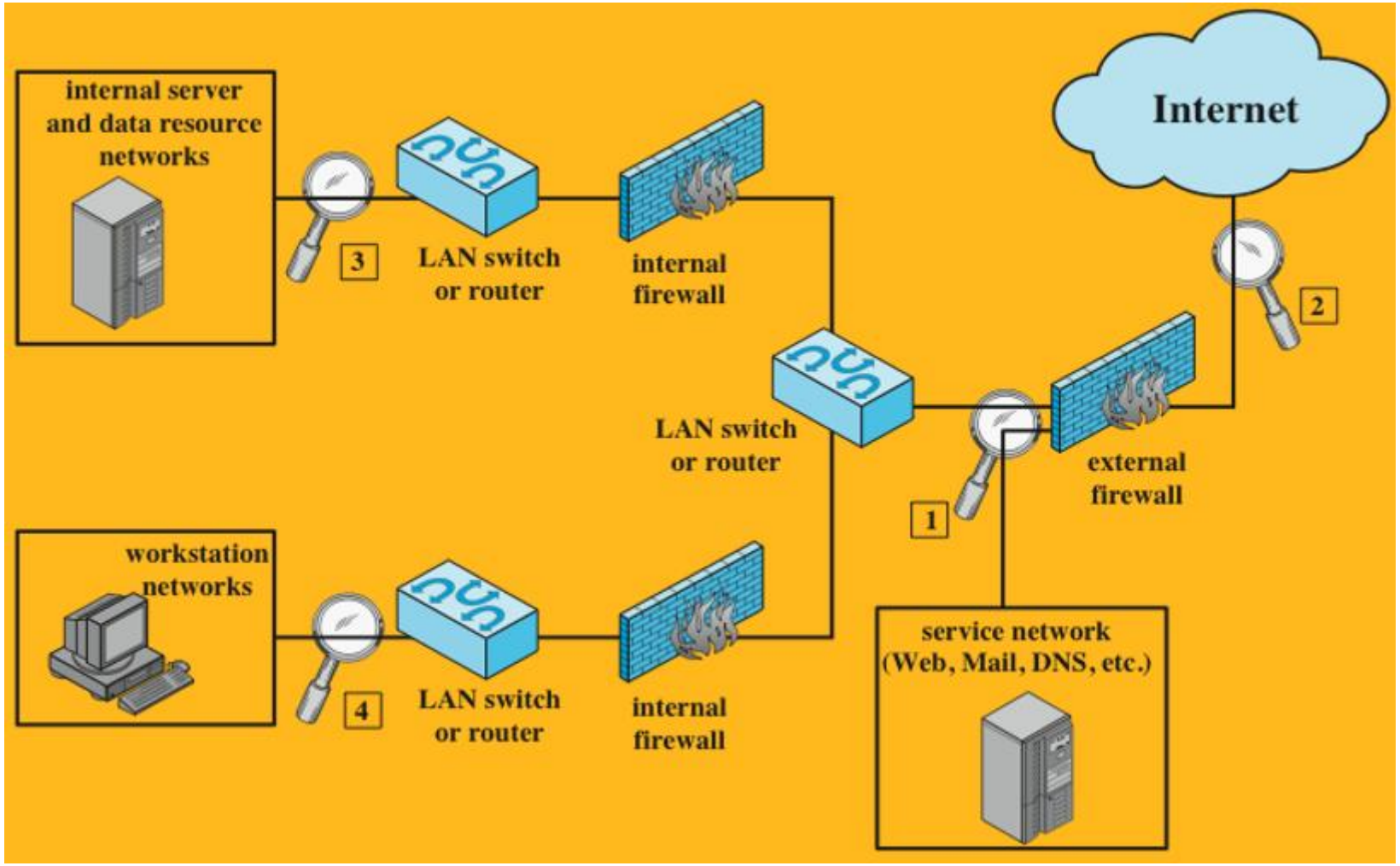
1. In front of the firewall
   - Records **all** inbound traffic
2. What are some disadvantages of in front placement?
   - Noisy since records all inbound traffic
   - Hard to tell if an intrusion is successful as the firewall may block the attempt
   - Requires dedicated server for NIDS sensor

NIDS/Sensor Placement Choices (Cont.)

3. In front of server networks
   - Can set specific rules for server OS
4. In front of workstation networks
   - Can set specific rules for workstation OS

NIDS Sensor Placement Examples

1. Behind the firewall
2. In front of the firewall
3. In front of server networks
4. In front of workstation networks



NIDS Intrusion Detection Techniques

- Sensors detect violations and send alerts/logs to analyst based on:
  - Signature detection
    - At application, transport, network layers
    - Unexpected application services
    - Policy violations
  - Anomaly detection
    - DoS/DDoS attacks
    - Scanning
    - Worms

Popular NIDS

- IBM
- Juniper
- Cisco

- We will use all of these popular open source NIDS in the lab:
  - Snort
  - Suricata
  - Bro

Security Information and Event Management (SIEM)

- Tool that aggregates as security data (IDS, A/V, Proxy, Firewall, System Logs, etc.
- Popular Commercial tools:
  - HP ArcSight
  - Splunk
  - AlienVault
  - Trustwave
  - Tenable
  - Novell
  - IBM Security
  - McAfee
  - LogRhythm
  - NetIQ
  - SolarWinds

Security Information and Event Management (SIEM)

- We will use an open source SIEM called ELSA in the lab.

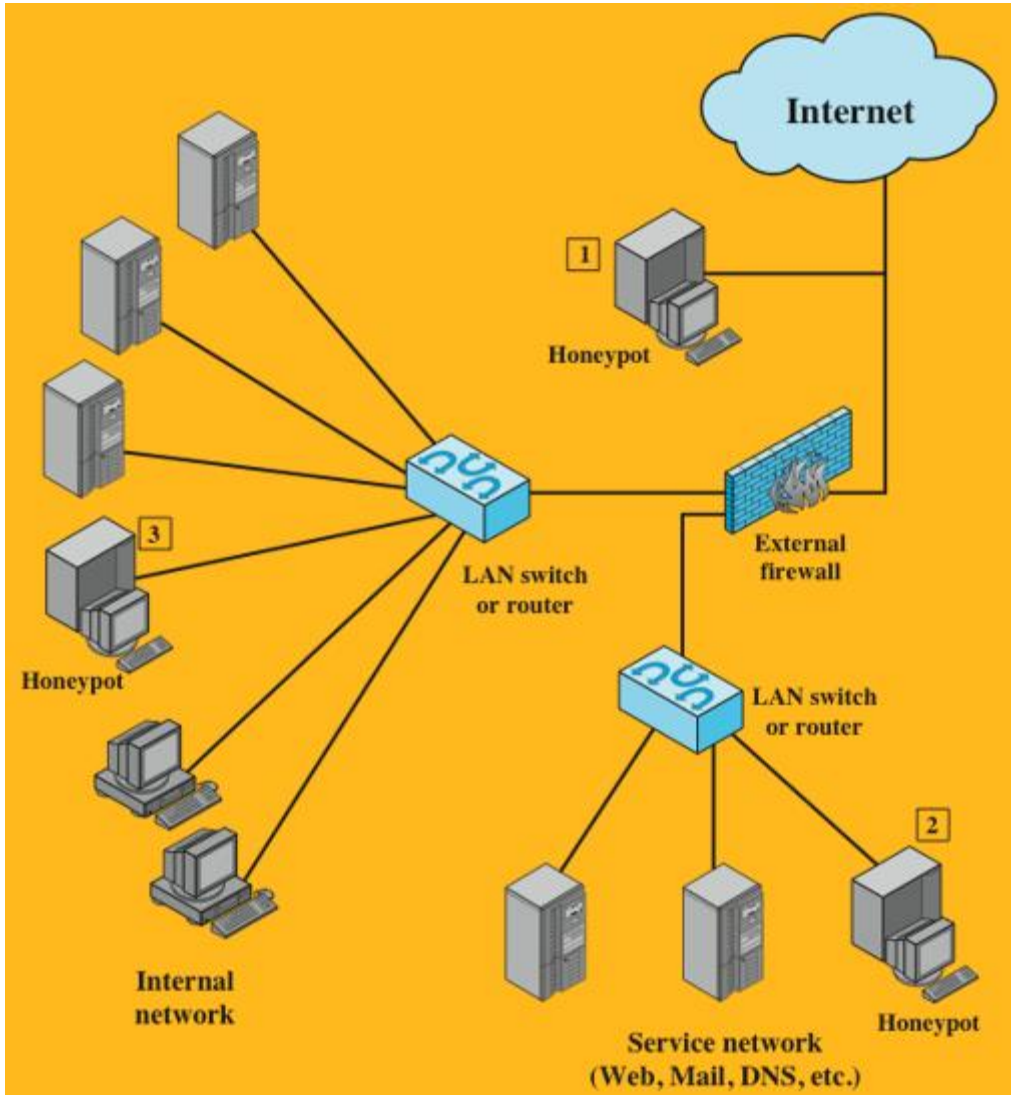
Question:

- An attack observed by a traditional IDS/IPS could be stopped manually or automatically.
- What is another option a security administrator can take to deal with impending attacks???
  - A Honeypot!

Honeypot

- Decoy system designed to:
  - Lure a potential attacker away from critical systems
  - Collect information about the attacker's activity
  - Encourage the attacker to stay on the system long enough for administrators to respond
- Filled with fabricated information that appears valuable
- One attackers are in the honeypot, administrators can observe their behavior to figure out defenses

Honeypot Deployment



- Note:
  - It can be dangerous to place a honeypot outside of the firewall
  - Why???
    - Could be used as a launching pad for attacks on other organizations
  - Why can't a honeypot inside the firewall attack other organizations???
    - The firewall can stop outbound traffic from the honeypot

Building your own Honey Pot

- Workstation or Server
- OS (Usually Linux)
- Sniffer

Honey Pot Systems

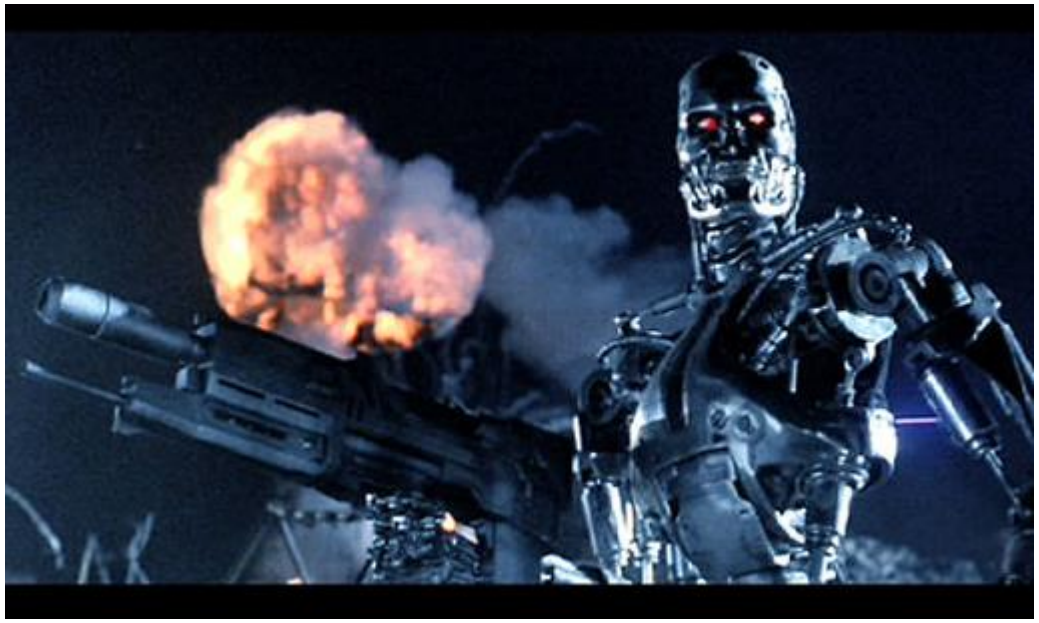
- Cybercop Sting
- Tripwire
- Deception Toolkit
- ManTrap
- Glastopf
- Specter
- Ghost USB
- KFSensor

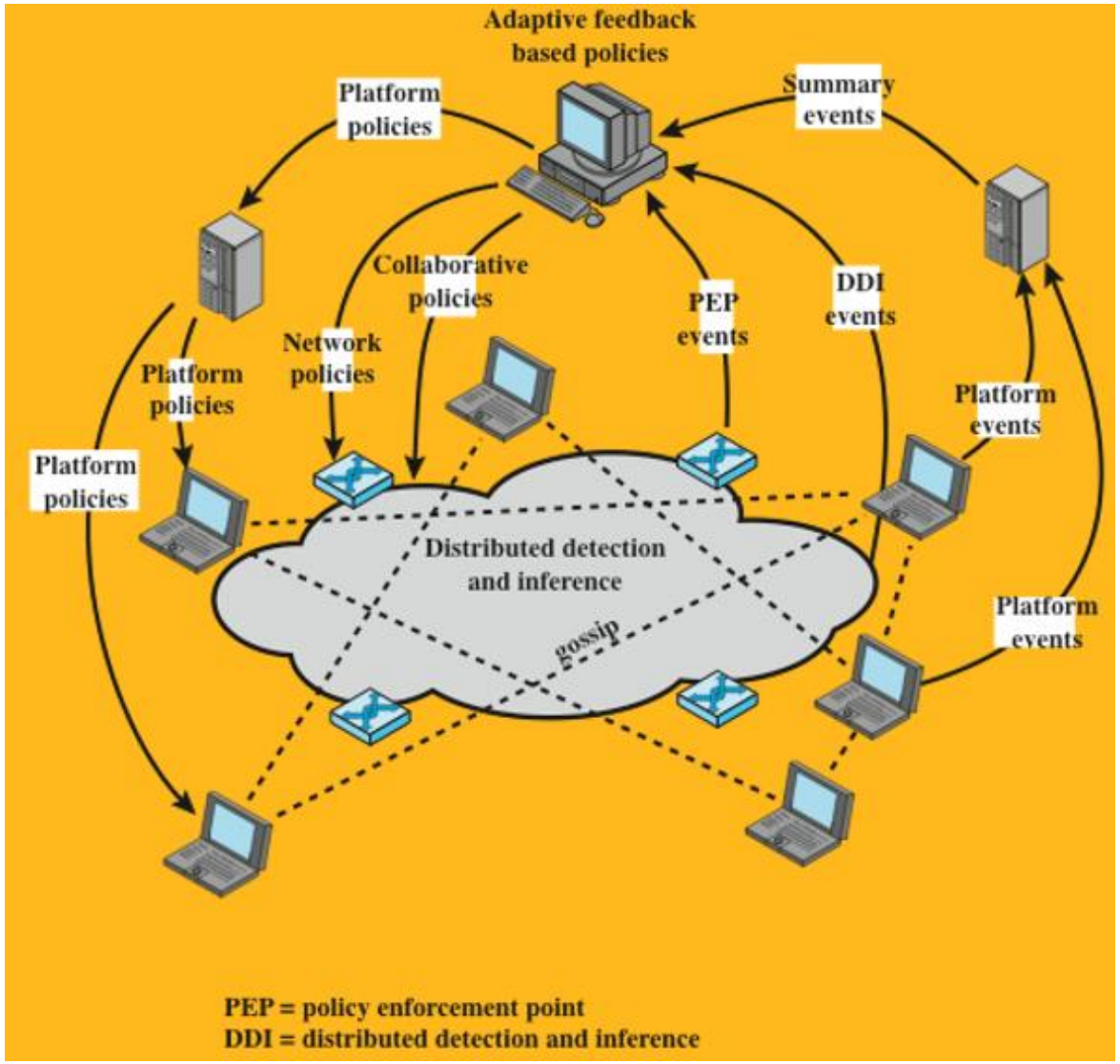
- Good resource:
  - http://www.honeynet.org/project

Autonomic Enterprise Security Systems

- Lastly, the concept of IDS inter-communication has evolved recently which involve:
  - Distributed systems that cooperate to identify intrusions
  - Adapt to changing attack profiles
- Anomaly detectors look for evidence of unusual activity
  - Detector uses P2P protocol to inform other machines about the unusual activity
  - If threshold exceeded, machine may defend itself!

Example: Autonomic Enterprise Security System





Part IV

SecurityOnion

SecurityOnion

- Linux Distro for:
  - IDS (Intrusion Detection System)
  - NSM (Network Security Monitoring)
  - Log Management
- Can also take and analyze packet captures of all data.
  - This can take up a lot of space per day so a huge SAN or daily rotation is necessary

Core Components

- NIDS (Network Intrusion Detection System)
  - Rule-Driven NIDS (Compares traffic to known signatures)
    - **Snort**
    - **Suricata**
  - Analysis-Driven NIDS (Logs data and provides framework for analysis
    - **Bro**

https://code.google.com/p/security-onion/wiki/IntroductionToSecurityOnion

Core Components

- HIDS (Host Intrusion Detection System)
  - Provides visibility from client endpoint to network gateway
    - **OSSEC**

Analysis Tools – **Sguil** (Main SecOnion Tool)

- GUI analyst console that provides visibility into collected event data and context to validate the detection
- For viewing:
  - Snort or Suricata alerts
  - OSSEC alerts
  - Bro HTTP events
  - Passive Real-Time Asset Detection System (PRADS) alerts
- Can pivot from alert directly into packet capture to drill into event
- Can conduct reverse DNS and perform WHOIS lookups of involved hosts
- Analysts can comment on and escalate alerts

Analysis Tools - **Squert**

- Web application interface to the Sguil database
- Allows querying of the Sguil database for visualizations such as geo-IP mapping and time series representations

Analysis Tools - **Snorby**

- Web application interface to view, search, and classify Snort and Suricata alerts
- Generates reports such as:
  - Most active IDS signatures
  - Most active sensors
  - Top src/dest IP addresses
- Can be used to pivot into a transcript of the entire session that involves the packet that triggered the alert

Analysis Tools - **ELSA**

- Enterprise Log Search and Archive
- Built on Syslog-NG, MySQL, and Sphinx full text searching
- Web based query interface that can quickly search a tremendous amount of logs for arbitrary strings
- Combs through most all data collected by SecurityOnion as well as any other syslog sources forwarded to it
- Powerful charting and graphing ability
- Similar to Splunk but free

More Snort Details

- Snort can be used as an IDS or IPS
- Many rulesets with intrusion definitions available
  - Registered Account:
    - Free, just sign up for an Oinkcode here:
      - https://www.snort.org/users/sign_in
    - 30 day delay before you receive new rules
  - Subscription Based Account:
    - Get new rules right away
    - Personal, Business, Integrators
- Can write your own rules!!
  - http://manual.snort.org/node27.html

pulledpork

- Script that automatically downloads latest snort rules
- https://code.google.com/p/pulledpork/

Snort's Two Modes (and Sub-modes)

- Active
  - Inline: Acts as IPS and forwards/denies all traffic based on ruleset
  - Offline: Acts as pseudo IPS and monitors traffic but has ability to deny some traffic through sending RST or ICMP error messages
- Passive
  - Inline: Acts as IDS and allows all traffic to pass through
  - Offline: Acts as IDS and watches copy of traffic from switch SPAN port or network TAP. **Most popular deployment**

http://searchitchannel.techtarget.com/tip/Tips-and-tricks-for-using-Snort-and-its-limitations

Part V

SecurityOnion Hands On Lab

Hands On

- Now, we are going to have a hands on lab with SecurityOnion
- The VM I created is ready to use but SecurityOnion is not configured
- We will be setting up the services and the network interfaces:
  - eth0: Management Interface
  - eth1: Monitoring Interface for traffic

Hands On

- The management interface will have connectivity to the internet and has an IP address.
- The monitoring interface has no connectivity to the internet and has no IP address.
  - Normally, this interface would have an Ethernet cable going to our switch SPAN port or network TAP monitor port
  - For this lab, we will simply be injecting traffic into the monitoring interface with tcpreplay which can reply any packet capture (PCAP file)

Hands On

- Open the M: Drive / Students folder
- Open your personal folder and double click on the SecurityOnion VNC file to access your VM
- If it is not already logged in, the credentials are:

- Login: **admin1**
- Password: **$ecOnion22.**

Hands On

- Double click on the “Terminal Emulator” on your desktop
- Run **ifconfig** and confirm that eth0 shows an address in the 10 network and eth1 does not show an IP address

Hands On

- Double-click on the “Setup” icon
- Enter the $ecOnion22. password
- “Yes, Continue!”
- “Yes, configure /etc/network/interfaces!”
- Select “eth0” for our management interface, “OK”
- Select DHCP, “OK”

Hands On

- "Yes, configure monitor interfaces"
- Place a check in "eth1" and hit "OK"
- "Yes, make changes!"
- "Yes, reboot!"
- If after reboot, you see a black screen, click in the Window to pull the GUI up.
  - If the GUI still doesn't come up after about 30 secs, close VNC and open the link again
- If asked, log back in with admin1 / $ecOnion22.

Hands On

- Now, we need to continue the SecurityOnion configuration
- Double-click the “Setup” icon again
- Password: **$ecOnion22.**
- “Yes, Continue!”
- “Yes, skip network configuration!”
- Select “Advanced Setup” and click “OK”

Hands On

- Select the “Standalone” option since we want to deploy both the server and sensor components
- Select “Yes, enable Snorby!”
- Set the Snorby email as **test@iit.edu** and click “OK”
- Set the Sguil username to be **sguiladmin1** and click “OK”
- Set the services password as **Servicespass22** and click “OK”
- Confirm the prior password again and click “OK”

Hands On

- Keep default of 30 days for data retention
- Keep default of 7 days for Sguil database repair
- Select “Snort” for IDS Engine to use
- Select “Emerging Threats GPL” as the IDS ruleset
  - If we had registered for Snort, we could have selected a different option that required an oinkcode
- Keep 4096 as the default for PF_RING slots
- eth1 should be selected as the monitored interface

Hands On

- Select “Yes, enable the IDS Engine!”
- Select “3” for IDS engine processes
- Select “Yes, enable Bro!”
- Select “Yes, enable file extraction!”
- Select “1” for Bro process to run
- Select “Yes, enable http_agent!”
- Select “No, disable Argus.”

Hands On

- Select “Yes, enable Prads!”
- Select “Yes, enable full packet capture!”
- Keep default as 150MB for pcap file size
- Select “No, use default scatter/gather I/O.”
- Keep 64MB default for PCAP ring buffer
- Change disk usage percentage to begin purging old logs to 70

Hands On

- Select “No, disable Salt”
- Select “Yes, enable ELSA!”
- Keep disk space option for ELSA logs as 6
- Select “Yes, proceed with the changes!”

Hands On

- Now, just wait a bit for the changes to complete
- Once complete, you will receive a window that states “Security Onion Setup is now complete!”
- Click OK
- Now there will be several information windows.
- Read each one and click “OK”
- Once, you click the last one (which mentions training) you are done and SecurityOnion is ready to go

Note (Don't do this now)

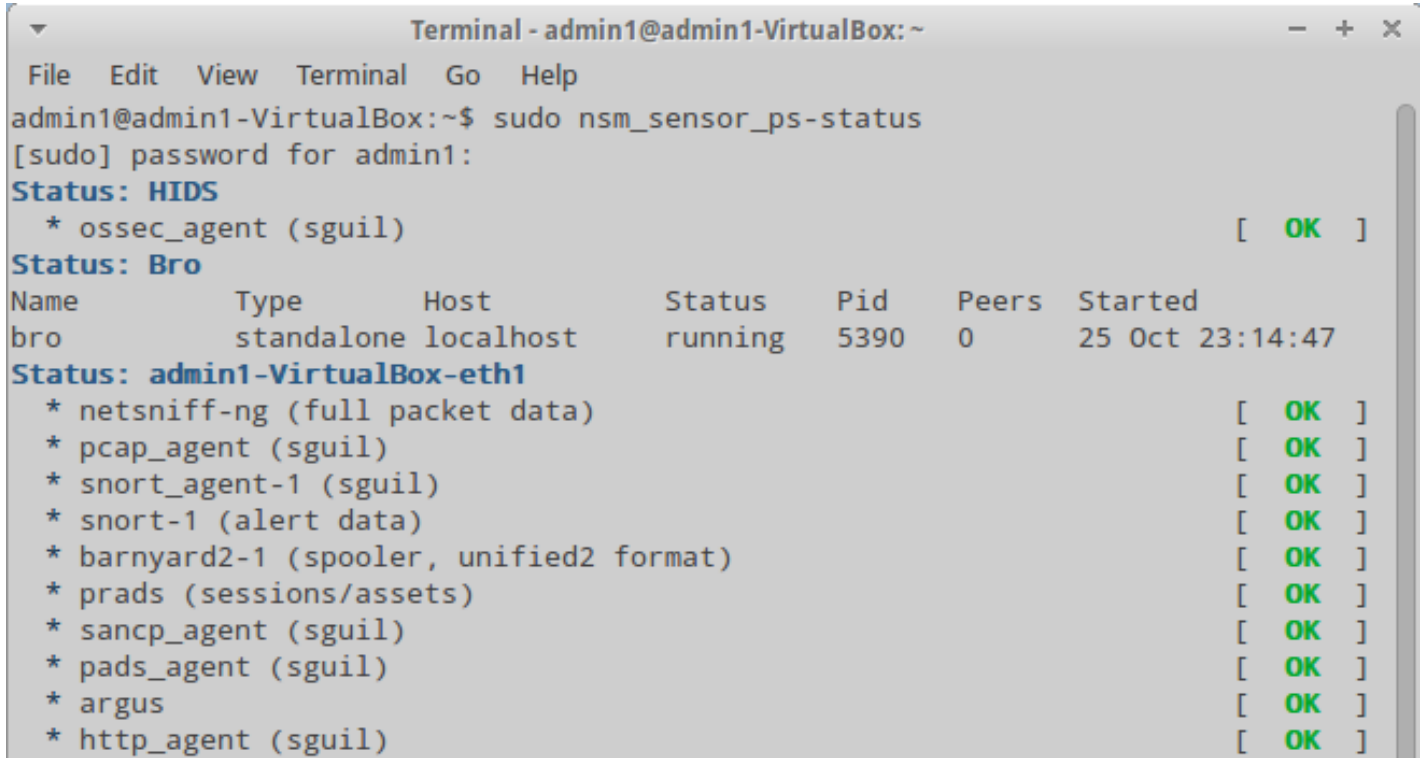
- SecurityOnion is now performing full packet capture
- If you would like to turn that feature off temporarily in the future:
  - sudo nsm_sensor_ps-stop --only-pcap
- To restart full packet capture:
  - sudo nsm_sensor_ps-start --only-pcap
- To permanently turn that feature off in the future:
  - sudo chmod 0 /usr/sbin/netsniff-ng

Hands On

- Now, let's make sure all of the SecurityOnion components are working properly
- Double-click on the "Terminal Emulator"

Hands On

- **sudo nsm_sensor_ps-status**
- Password: **$ecOnion22.**



Hands On

- Now, let's check out Sguil
- Double-click Sguil icon on desktop of VM
- Username = **sguiladmin1**
- Password = **Servicespass22**
- Choose "Select All" to Monitor both the eth1 interface and any OSSEC events
- Choose "Start SGUIL"
- Maximize Sguil

Hands On

- You should see a few OSSEC events listed in a few secs
- Select one of the events and put a check in “Display Detail”
  - You should notice some are related to integrity changes of system files
- Right click and hold under “CNT” for the top line and drag down to “View correlated events” and release
- You should now see several events.
- Select the “RealTime Events” tab to go back where you were

Hands On

- Now, we are going to use tcpreplay to replay an attack from a packet capture.
- Go back to your terminal
- **cd /home/admin1/Desktop/Malicious\ PCAPs**
- **ls** and you should see three packet captures in there
- We are only going to replay pcap_a.pcap for now

Hands On

- **sudo tcpreplay –i eth1 –M10 pcap_a.pcap**
  - Password is $ecOnion22. if asked
- You should see a message that 5201 packets were successfully injected into the eth1 interface
- Now go back to the RealTime Events Tab of Sguil
- It takes the sensor awhile the first time to show the results so it may take a couple of minutes

Hands On

- Maximize Sguil
- Drag the right edge of the Sensor tab to the right so that you can see the entire values
- Take a quick look through the eth1 events
- Does this malicious traffic look familiar???

Hands On

- This is the crimeboss pcap from earlier in the semester
- Click on the “ET CURRENT_EVENTS Possible CrimeBoss Generic URL Structure”
- Place a check in “Show Packet Data” and “Show Rule”

Hands On

- Snort Rule:

☑ Show Packet Data ☑ Show Rule

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Possible CrimeBoss Generic URL Structure"; flow:established,to_server; content:".php?action=jv&h="; http_uri; classtype:bad-unknown; sid:2016558; rev:3;)
/nsm/server_data/securityonion/rules/admin1-VirtualBox-eth1-1/downloaded.rules: Line 1849

- Detected Traffic:

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	192.168.1.133	173.254.28.55	4	5	0	458	60067	2	0	128	33319

TCP	Source Port	Dest Port	R 1	R 0	URG	ACK	PSH	RST	SYN	FIN	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	2581	80	.	.	.	X	X	.	.	.	383730025	2708941523	5	0	63649	0	10278

DATA

```
47 45 54 20 2F 2F 63 62 2E 70 68 70 3F 61 63 74   GET //cb.php?act
69 6F 6E 3D 6A 76 26 68 3D 36 30 38 32 39 39 33   ion=jv&h=6082993
34 33 20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63   43 HTTP/1.1..Acc
65 70 74 3A 20 2A 2F 2A 0D 0A 52 65 66 65 72 65   ept: */*..Refere
72 3A 20 68 74 74 70 3A 2F 2F 61 62 72 61 68 61   r: http://abraha
6D 73 70 61 74 68 2E 6F 72 67 2E 75 6B 2F 63 62   mspath.org.uk/cb
2E 70 68 70 0D 0A 41 63 63 65 70 74 2D 4C 61 6E   .php..Accept-Lan
67 75 61 67 65 3A 20 65 6E 2D 75 73 0D 0A 55 73   guage: en-us..Us
65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C   er-Agent: Mozill
61 2F 34 2E 30 20 28 63 6F 6D 70 61 74 69 62 6C   a/4.0 (compatibl
```

Hands On

- Notice on that event that the “CNT” column shows a “2”
- Right click on the “2” and drag down to “View Correlated Events” and release
- You should see the signature of the first rule which was “.php?action=jv&h” which was saw in the previous slide
- What is the signature of the other rule???

Hands On

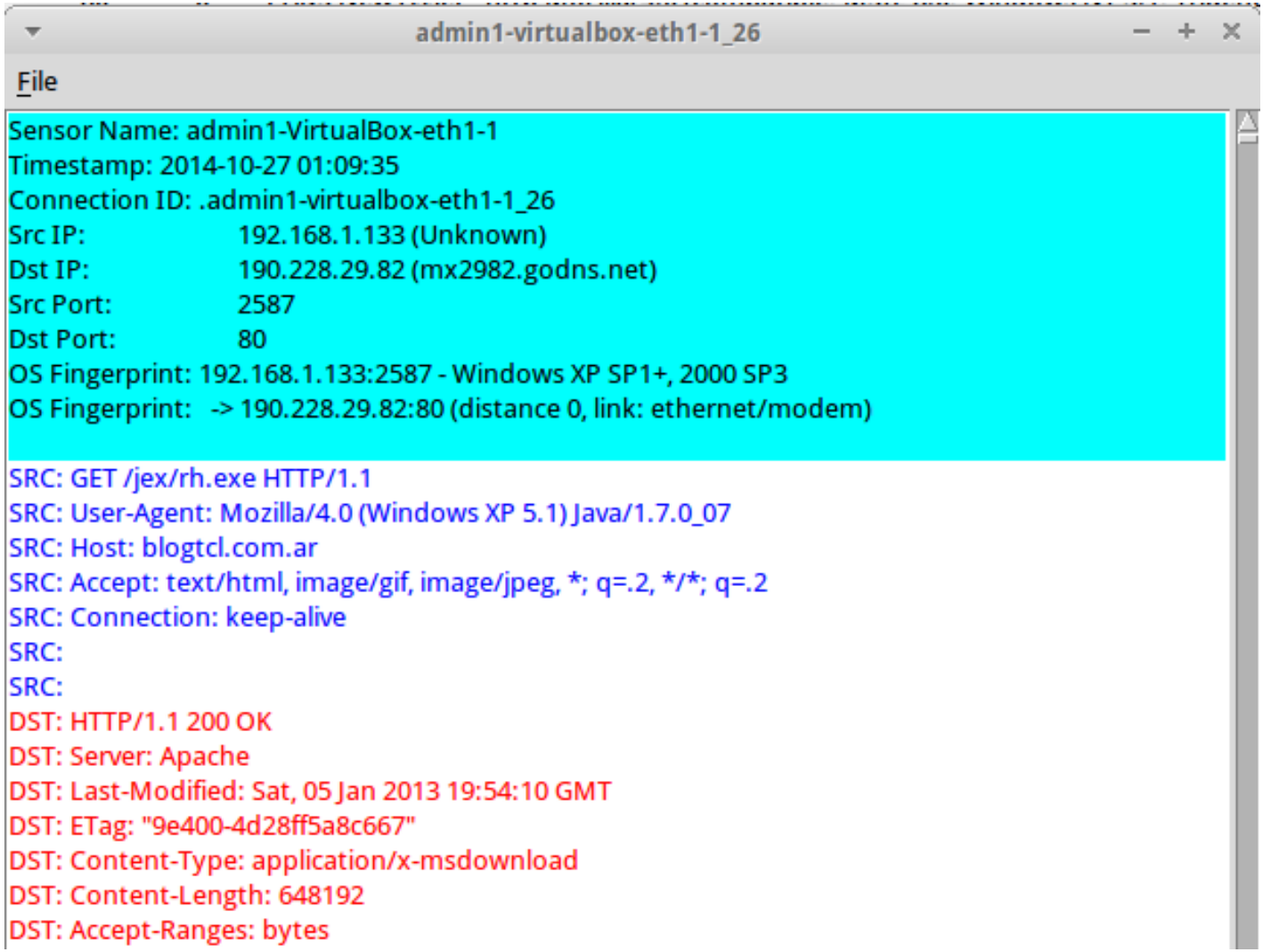
- The second rule's signature was "/cb.php?action="
- Click back to the RealTime Events tab
- Go ahead and take some time to click on the other "ET" events and notice how the snort rules are written
- See anything interesting?

Hands On

- Select the "ET POLICY PE EXE or DLL Windows file download" event
- What caused this to fire as a Windows EXE in the snort signature???
  - The "MZ" and "PE" in the content of the packet
- One problem we have is, we don't know what the file name of the file was that was downloaded
- Right click on the Alert ID value of that event and drag to "Transcript" and release

Hands On

- What is the file name?
  - rh.exe
- Go ahead and close the transcript window



Hands On

- When right clicking on “Alert ID” there are several other options:
  - Wireshark
  - Network Miner
- Select and check out each of those options
- What does Network Miner show you?

Hands On

- Once, you have looked at an event, you can do the following
  - F8 to dismiss as NA
  - F9 to escalate
  - Right click on “ST” column and select “Update Event Status” and you can choose a category which will tag that event and remove it from your queue

Hands On

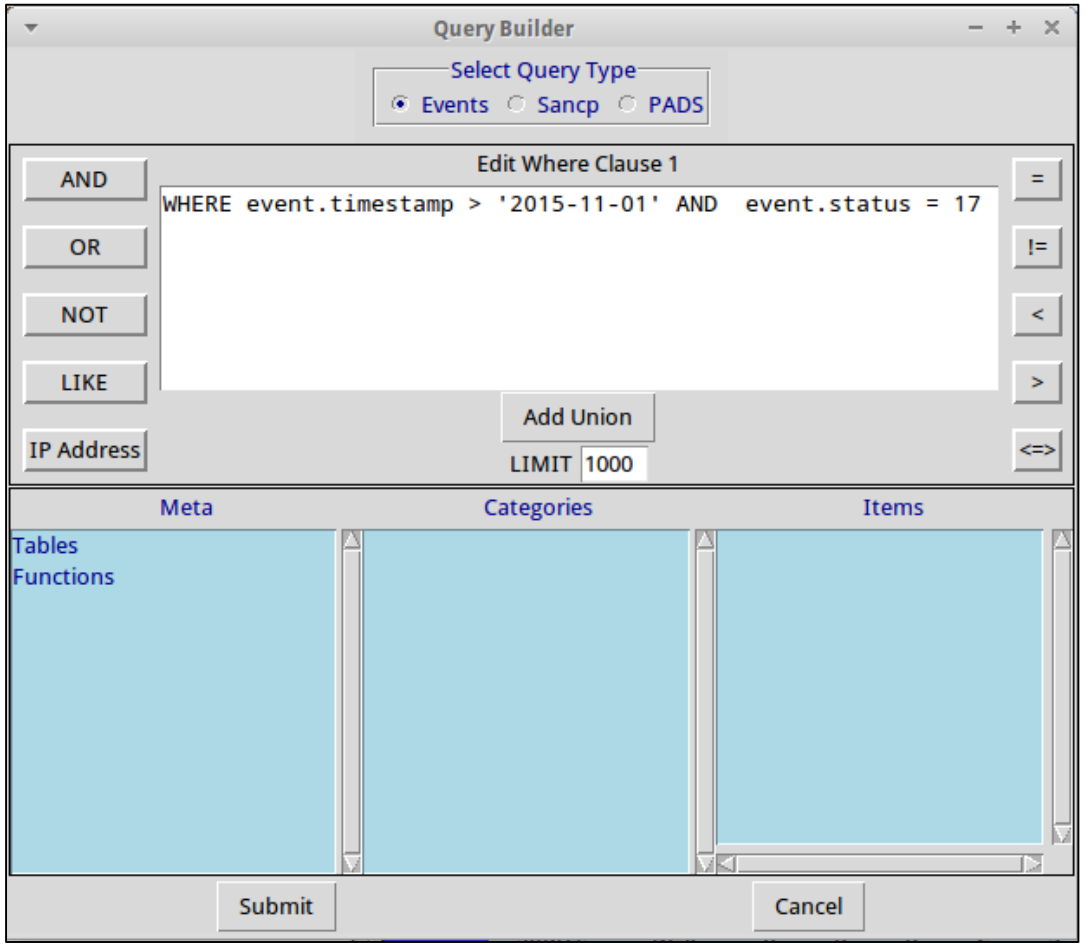
- Let's categorize the "Windows file download" as a "Cat VII: Virus Infection"
- Right click on the "ST" column value for it and choose "Update Event Status" and "Cat VII: Virus Infection"
- Classify the two Java Exploit events as "Cat VII: Virus Infection" as well by selecting each event and hitting F7

Hands On

- Now let's look at what we have categorized
- Go to Query / Query by Category / CAT VII: Virus Infection

Hands On

- Select Submit at the bottom:



Hands On

- Now you can see that Category's Events:

RealTime Events | Escalated Events | Event Query Cat VII

Close

Export

(SELECT event.status, event.priority, sensor.hostname, event.timestamp as datetime, event.sid, event.cid, event.signature, INET_NTOA(event.src_ip), INET_NTOA(event.dst_ip), event.ip_proto, event.signature_rev FROM event IGNORE INDEX (event_p_key, sid_time) INNER JOIN sensor ON event.sid=sensor.sid WHERE event.timestamp > '2015-11-01' AND event.status = 17) UNION (SELECT event.status, event.priority, sensor.hostname, event.timestamp as datetime, event.sid, event.cid, event.signature, INET_NTOA(event.src_ip), INET_NTOA(event.dst_ip), event.ip_proto, event.src_port, event.dst_port, event.signature_gen, event.signature_id, event.sig

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
C7	1	admin1-V...	3.25	2015-11-07 23:07:30	173.236.175.34	80	192.168.1.133	2586	6	ET INFO JAVA - Java Archive Download By Vulnerable Client
C7	1	admin1-V...	3.16	2015-11-07 23:07:30	173.236.175.34	80	192.168.1.133	2585	6	ET INFO JAVA - Java Archive Download By Vulnerable Client
C7	1	admin1-V...	3.23	2015-11-07 23:07:30	173.236.175.34	80	192.168.1.133	2586	6	ET INFO JAVA - Java Archive Download By Vulnerable Client
C7	1	admin1-V...	3.14	2015-11-07 23:07:30	173.236.175.34	80	192.168.1.133	2585	6	ET INFO JAVA - Java Archive Download By Vulnerable Client
C7	1	admin1-V...	3.21	2015-11-07 23:07:30	173.236.175.34	80	192.168.1.133	2586	6	ET CURRENT_EVENTS Crimeboss - Java Exploit - Recent Jar (3)
C7	1	admin1-V...	3.12	2015-11-07 23:07:30	173.236.175.34	80	192.168.1.133	2585	6	ET CURRENT_EVENTS Crimeboss - Java Exploit - Recent Jar (3)
C7	1	admin1-V...	3.19	2015-11-07 23:07:30	173.236.175.34	80	192.168.1.133	2586	6	ET CURRENT_EVENTS Crimeboss - Java Exploit - Recent Jar (3)
C7	1	admin1-V...	3.10	2015-11-07 23:07:30	173.236.175.34	80	192.168.1.133	2585	6	ET CURRENT_EVENTS Crimeboss - Java Exploit - Recent Jar (3)
C7	1	admin1-V...	3.17	2015-11-07 23:07:30	173.236.175.34	80	192.168.1.133	2585	6	ET INFO JAVA - Java Archive Download By Vulnerable Client

Hands On

- Go back to the “RealTime Events” tab
- Now, see if you can figure out how to run a query that will only show the traffic to the destination IP of 187.45.240.67
- Once you figure that out, play around with any other features in Sguil

Hands On

- Go ahead and close out of Sguil
- Now we are going to check out ELSA but first let's generate an event
- Open the terminal
- **sudo useradd testuser1**
  - Might have to enter sudo password of $ecOnion22.
- **sudo passwd testuser1**
- Enter the password as **asdfasdf**

Hands On

- **su testuser1**
- Enter the **asdfasdf** password
- **sudo cat /etc/shadow**
- Enter the **asdfasdf** password
- You should get a denied message since testuser1 is not in the sudoers file
- This is an example of a failed access elevation attempt which an IDS can detect

Hands On

- Double click on ELSA on the desktop
- You will receive a “connection is not private” issue
- Select “Advanced”
- Select “Proceed to localhost “
- User Name: **sguiladmin1**
- Password: **Servicespass22**
- Maximize ELSA

Hands On

- ELSA is similar to Splunk and indexes the various data coming in and allows for detailed searching
- Now perform a query on testuser1
- What do you see???
- Now, in the “Query” box, enter sudoers and hit “Submit Query
- You should see the error about testuser1’s unauthorized attempt to try to access the shadow file

Hands On

- Now's let look at our Crimeboss details with ELSA
- On the left side, scroll down and expand "Snort/Suricata" and click on "Top NIDS Alerts"
- Click on the …Recent Jar (1) event
- Now let's say we want to see what other traffic this user has been involved in
- Notice the 173.236.175.34 under dstip in the event
- Clear the Query window

Hands On

- Enter 173.236.175.34 and hit “Submit Query” to see all events that involve that IP
- Let’s say now we want to know what other hosts did DNS lookups for the malicious domain hosting the java exploits
- Enter BRO_DNS.hostname=danieldelaney.com
- Hit “Submit Query”
- Only the 192.168.133 host is shown but this is useful in an enterprise where there could be many hosts that were potentially infected from clicking on the same phishing email

Hands On

- Sometimes you might want to know if someone who hit an exploit kit actually got infected with a payload.
- The crimeboss pcap we analyzed showed the infected host visited tecnologiadesecundaria.com/grand/index.php and posted the hostname of the infected computer to the attacker's server there
- Enter grand/index.php in ELSA and submit the query

Hands On

- You should see that the 192.168.1.133 host did in fact visit that address and is therefore infected
- Click on some of the other ELSA hot links on the left side in categories such as:
  - Host Logs
  - HTTP
  - Files
  - Etc.
- Close ELSA

Hands On

- Double click on Squert on the desktop
- You will receive a “connection is not private” issue
- Select “Advanced”
- Select “Proceed to localhost “
- User Name: **sguiladmin1**
- Password: **Servicespass22**

Hands On

- Offers different visualization of data from Sguil database
- Main screen shows top dangerous events
- Click on the different tabs at the top (EVENTS, SUMMARY, VIEWS)
- What do you see???

Hands On

- Close Squert
- Double click on Snorby on the desktop
- You will receive a “connection is not private” issue
- Select “Advanced”
- Select “Proceed to localhost “
- User Name: **test@iit.edu**
- Password: **Servicespass22**

Hands On

- Take a few minutes to click around in the Dashboard to see the visualizations and drill down on some items
- Check out the Events Tab as well
- What countries have received transmissions from the network?

Hands On

- Close Snorby
- Lastly, we'll write our own Snort rule to detect upon the grand/index.php infection signature
- First let's learn a little about how the syntax for Snort rules
- Snort rules are broken into two sections
  - Rule Header
  - Rule Options

Snort Rule Syntax

- Rule Header
- Rule Options

alert tcp 192.168.1.15 5858 -> 121.14.1.2 80 (msg: "Info here"; reference: url,http://whateversite.com; content: "cb.php"; flow:to_server; nocase; sid: 1000001; rev:1)

Snort Rule Syntax - Header

- alert: Generate an alert and then log the packet
- tcp: Protocol (TCP, UDP, ICMP, IP)

alert tcp 192.168.1.15 5858 -> 121.14.1.2 80

SrcIP SrcPort DestIP DstPort

*$HOME_NET can also be used as the SrcIP and is a variable in Snort for all private network ranges (Class A, B, and C)

Snort Rule Syntax –Rule Options

- General Rule Options:
  - Provide information during the rule but don't affect detection
    - Msg, reference, priority, etc.
- Payload Detection Rules:
  - Detects within the payload of a packet
    - Base64 data and then decode it, data at a certain offset, content in a packet, etc.

Snort Rule Syntax –Rule Options

- Non-Payload Detection Rules:
  - Detects non-payload data
    - Sequence and Ack numbers, flow direction, flags, etc.
- Post-Detection Rule Options:
  - Triggers that can happen after a rule has been fired
    - Replace content, extract user data from TCP sessions, etc.

Snort Documentation

- Open a browser from your physical Lab computer
- Go to the full Snort documentation:
  - http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node1.html
- Scroll down to "3. Writing Snort Rules"
- Take five minutes to skim through some of the header info in 3.2 and the rule info in 3.4, 3.5, 3.6, and 3.7.

Snort Rule Syntax – Common Rule Options

- msg: Name of the event
- reference: Can add site you found signature or contains additional info
- content: Searches for specific content in the packet payload
  - The content keyword is one of the most important features of Snort.
- flow: Direction of the traffic
- nocase: Not case sensitive
- sid: Id of alert (Custom alerts must start at 1 Million+)
- rev: Revision number of alert

(msg: “Info here”; reference: url,http://whateversite.com; content: “cb.php”; flow:to_server; nocase; sid: 1000001; rev:1)

Snort Downloaded Rules

- Before we write our own rule, lets look at the rules Snort downloaded through PulledPork
- Open a terminal and change directories to /etc/nsm/rules
- **ls –l**
  - The last character above is a lowercase L
- The download.rules file has the most data and rules

Snort Downloaded Rules (Cont.)

- We can use **cat** to read the file and **grep** to search for specific rules
- Take a few minutes to look at some of the below types of rules:
- **cat downloaded.rules | grep –i crimeboss**
- **cat downloaded.rules | grep –i ddos**
- **cat downloaded.rules | grep –i cryptolocker**
- Search for rules for a different type of attack, malware, or exploit kit

- In your physical lab computer, browse to:
- https://www.snort.org/rules_explanation

- These are some of the categories of downloaded rules
- Take a few minutes to look through them

Hands On

- Now, let's write our first infection rule
- Snort's "content" keyword searches for anything in the payload of a packet
- For example, when the infection in pcap_a is successful, the victim will send a post to a server with a path of /grand/index.php
- We will write a rule to detect /grand/index.php

Hands On

```
5143 2…  67.219287  192.168.1.133   69.72.240.58   t…  HTTP 318 POST /grand/index.php HTTP/1.0

▷ Checksum: 0x8353 [validation disabled]
  Urgent pointer: 0
▷ [SEQ/ACK analysis]
  TCP segment data (264 bytes)

00  00 1c 10 b3 fb 0b 08 00  27 55 e9 b8 08 00 45 00   ........ 'U....E.
10  01 30 f5 cb 40 00 80 06  0c 4c c0 a8 01 85 45 48   .0..@... .L....EH
20  f0 3a 0a 20 00 50 7e 96  9a 28 3f a1 75 1b 50 18   .:. .P~. .(?.u.P.
30  fa f0 83 53 00 00 50 4f  53 54 20 2f 67 72 61 6e   ...S..PO ST /gran
40  64 2f 69 6e 64 65 78 2e  70 68 70 20 48 54 54 50   d/index. php HTTP
50  2f 31 2e 30 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   /1.0..Co nnection
60  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 6f   : keep-a live..Co
70  6e 74 65 6e 74 2d 54 79  70 65 3a 20 61 70 70 6c   ntent-Ty pe: appl
80  69 63 61 74 69 6f 6e 2f  78 2d 77 77 77 2d 66 6f   ication/ x-www-fo
90  72 6d 2d 75 72 6c 65 6e  63 6f 64 65 64 0d 0a 43   rm-urlen coded..C
a0  6f 6e 74 65 6e 74 2d 4c  65 6e 67 74 68 3a 20 38   ontent-L ength: 8
b0  36 0d 0a 48 6f 73 74 3a  20 74 65 63 6e 6f 6c 6f   6..Host:  tecnolo
c0  67 69 61 64 65 73 65 63  75 6e 64 61 72 69 61 2e   giadesec undaria.
d0  63 6f 6d 0d 0a 41 63 63  65 70 74 3a 20 74 65 78   com..Acc ept: tex
e0  74 2f 68 74 6d 6c 2c 20  2a 2f 2a 0d 0a 41 63 63   t/html,  */*..Acc
f0  65 70 74 2d 45 6e 63 6f  64 69 6e 67 3a 20 69 64   ept-Enco ding: id
00  65 6e 74 69 74 79 0d 0a  55 73 65 72 2d 41 67 65   entity.. User-Age
10  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 33 2e 30 20   nt: Mozi lla/3.0
20  28 63 6f 6d 70 61 74 69  62 6c 65 3b 20 49 6e 64   (compati ble; Ind
30  79 20 4c 69 62 72 61 72  79 29 0d 0a 0d 0a         y Librar y)....
```

Snort's "Content" keyword can detect anything in the payload data of a packet

Hands On

- Open the terminal
- Type exit to return to the admin1 user prompt
- **cd /etc/nsm/rules**
- **sudo vi local.rules**
  - $ecOnion22. if asked
- Hit i key to insert text into file with INSERT mode

Hands On

- Before you enter this, someone explain this rule:

alert tcp any any -> any 80 (msg: “Banking payload successful”; reference: url,http://whateversite.com; content: “grand/index.php”; flow:to_server; nocase; sid: 1000001; rev:1)

Go ahead and enter it in the file

***There can be no typos

Hands On

- Hit the ESC key and type :wq and then hit Enter
- Now, we need to restart Snort to take our new rule
- **sudo rule-update**
- Wait a bit, and the “warning bad line” msg is okay
- As long as you had no typos, this should be the last thing you see:

```
Restarting: seconion-eth1
  * starting: snort-1 (alert data)                    [  OK  ]
  * starting: snort-2 (alert data)                    [  OK  ]
  * starting: snort-3 (alert data)                    [  OK  ]
```

Hands On

- Now, we need to resend the Crimeboss packets
- In the terminal:
- **cd /home/admin1/Desktop/Malicious\ PCAPs**
- **sudo tcpreplay –i eth1 –M10 pcap_a.pcap**
- You should see a message that 5201 packets were successfully injected into the eth1 interface

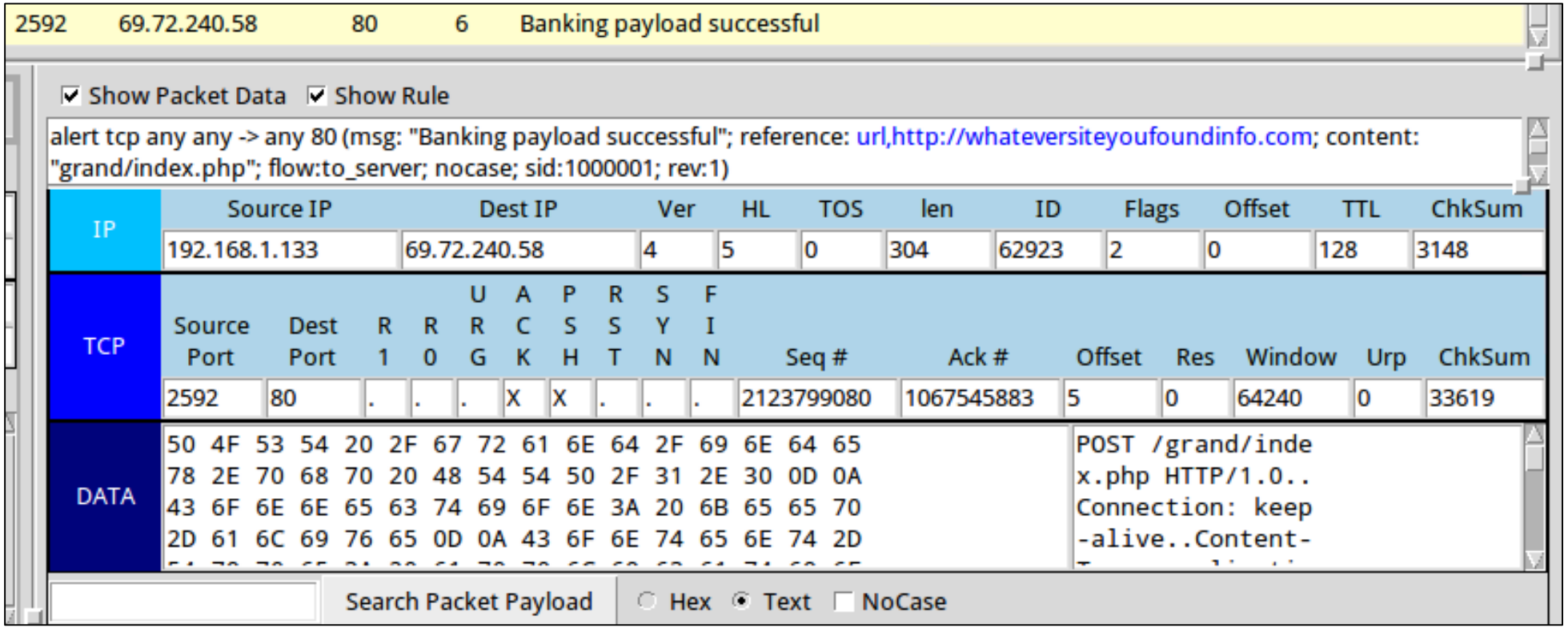
Hands On

- Now, open Sguil and we should have some more interesting traffic to look at
- Username = **sguiladmin1**
- Password = **Servicespass22**
- Choose “Select All” to Monitor both eth1 interface and any OSSEC events
- Choose “Start SGUIL”
- Maximize Sguil

Hands On

- Scroll to the bottom
- Click on the “Banking payload successful” event that you previously created
- Place a check in “Show Packet Data” and “Show Rule”
- You should now see your rule and the packet with the grand/index.php data

Hands On



- You just wrote your first Snort rule!

Individual Project

- I will review your submissions from Homework 9 as soon as possible and will put my feedback in Blackboard under that question
- The next stage of your project is to accomplish the tasks on the next two slides based on the feedback I will provide and upload the slides and video before class on April 11th
  - The slides and video should be uploaded in a zip file to the Project Info / Individual Project assignment on Blackboard

Individual Project Tasks Due Before 5:30pm on 4/11

- 5-10 PowerPoint slides in your own words explaining:
  1. What your service does
  2. Common default or non-default configuration options that led to a vulnerability and any other insecure issues you uncovered with the service
  3. Your methods to harden the service to defend against these attacks
  4. **Make sure you include a Bibliography slide with citations for any resources you used for the project.

Individual Project Tasks Due Before 5:30pm on 4/11

5. Short video (1 minute) showing at least one example of your running service being attacked by you and then showing your service resisting that same attack after being hardened. (I want to see a hand's on attack and do not want to simply see you mention your service is vulnerable to a software issue and then just show yourself fixing it by downloading a patch.)

- I will review the PowerPoints and videos shortly after April 11th and will provide feedback for any needed changes.
- On Apr 25th, each student will present their PowerPoint and video to the class. Each student will have around 7 minutes total to present.

Individual Project

- If your service is very secure and cannot be attacked, I may have you create a video showing how you could purposely make it insecure or something else
- Keep in mind, this is the first semester I have assigned this project (so you are the test class)
  - As long as you put good effort into the final presentation on 4/25, you will receive full credit for the project which is 5% of your grade

Homework

- Complete Homework12 located on Blackboard under "Homework Assignments"
  - Homework12 is due before midnight on Sunday, April 10th

**Remember that Homework11 (Stego/Firewalls) is due before midnight this Sunday, April 3rd