Intrusion Detection, Snort, and Network Security Monitoring

Cybersecurity

Network Security Day 2

10.2 - Network Security - IDS, Snort, NSM

Class Preparation

1. Check into BCS
2. Update your git repository with `` `git pull` ``
3. Login to Azure and start the *Network Security* lab
   - Login/RDP when up (`azadmin/p4ssw0rd*`)
   - In your Windows VM, launch Hyper-V Manager and start the *Security Onion* VM
   - Login to the VM (`sysadmin/cybersecurity`)

Homeworks Due

- Unit 9 (Networking 2): due Sunday December 6
- Unit 10 (Network Security): due Sunday December 13

Upcoming Units

- Week 11: Cloud Sec. & Virtualization (12/05 - 12/12)
- Week 12: Project Week (12/14 - 12/19)
- Week 13: Cryptography (1/04 - 1/09)

Schedule Notes

Project 1 (Individual; Required)

- Mon 12/14 - Sat 12/19

Winter Break - No Class

- Last class on Sat 12/19
- Off: Mon 12/21 - Sat 1/02
- Return on Monday 1/04

Schedule Change

- Crypto delayed until after Winter Break

Class Objectives

By the end of class, you will be able to:

- Interpret and define Snort rules and alerts.
- Explain how intrusion detection systems work and how they differ from firewalls.
- Explain how intrusion detection systems work and how they differ from firewalls.
- Collect and analyze indicators of attack and indicators of compromise using NSM tools.
- Apply knowledge of NSM, Snort rules, and Security Onion to establish situational awareness within a network.

Before we get started, we need to launch an instance of **Security Onion**.

This will generate alert data that we’ll use to complete the labs.

Activity: Security Onion Setup (01_Security_Onion_Setup)

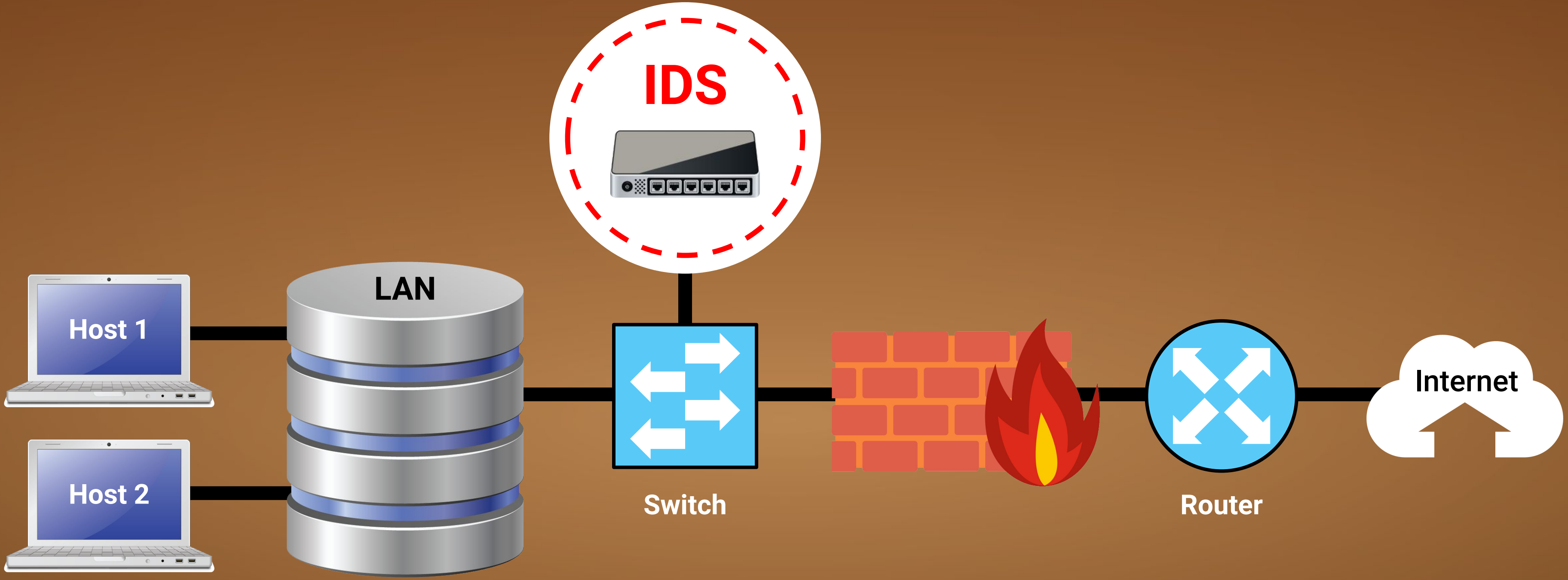
Follow along as we set up Security Onion to generate alert data.

Suggested Time:
10 Minutes

An **intrusion detection system (IDS)** both analyzes traffic *and* looks for malicious signatures.

Overview: Intrusion Detection Systems

An IDS is like a firewall that reads the data in the packets it inspects, logs information, and issues alerts



Overview: IDS and NSM

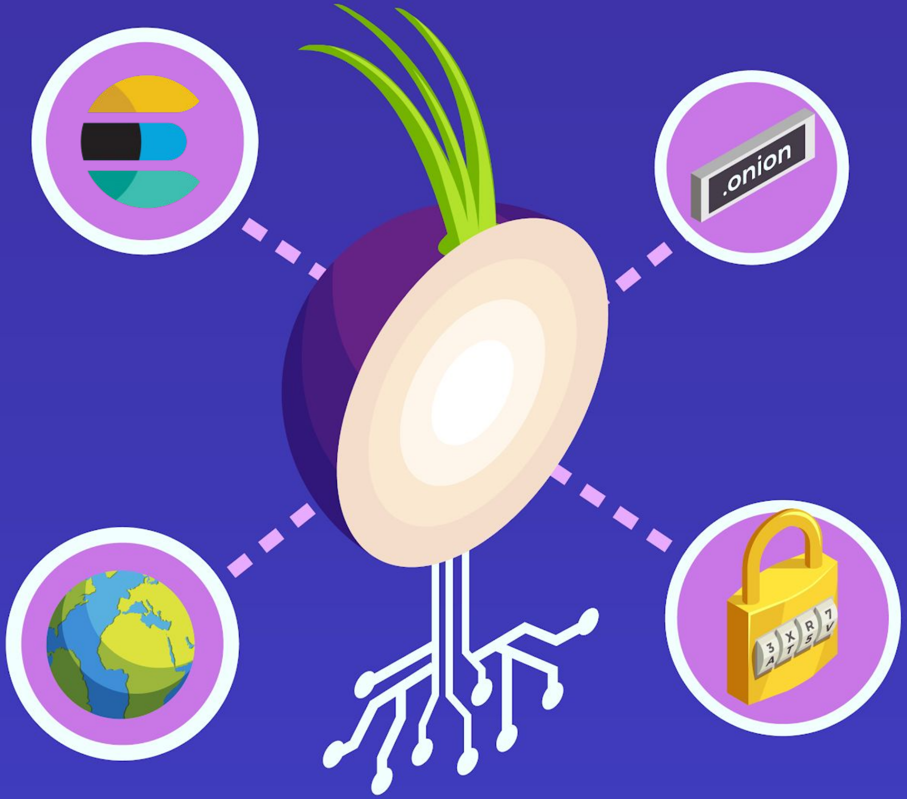
There are many varieties of intrusion detection systems, but today's class will focus on **Snort**, the world's most popular open-source solution.

- **Network security monitoring (NSM)** is the process of identifying weaknesses in a network's defense.
- It also provides organizations with situational awareness of their network.

Overview: Security Onion

Security Onion is a Linux distribution that contains many NSM tools.

Security Onion uses the Snort IDS engine as its event-driven mechanism.



Introduction to Intrusion Detection and Snort

Intrusion Detection Systems

Unlike firewalls, an IDS detects and alerts of an attack.

- IDS are usually *passive*. They do not generally respond to attacks; they only log and document information for future analysis.
- IDS helps organizations establish situational awareness of attackers, allowing them to harden defenses.

IDS Types

There are two types of IDS:

01 Signature-based IDS

A signature-based IDS compares patterns of traffic to predefined signatures.

- Good for identifying well-known attacks.
- Can be updated as new attack signatures are released.
- Vulnerable to attacks through packet manipulation.
- Unable to detect zero-day attacks.

02 Anomaly-based IDS

An anomaly-based IDS compares patterns of traffic against a well-known baseline.

- Good for detecting suspicious traffic that deviates from well-known baselines.
- Excellent at detecting when attackers probe and sweep a network.
- Prone to false alerts.
- Assumes network behavior does not deviate from well-known baselines.

Intrusion Detection Architecture

Intrusion detection systems have two basic architectures:

NIDS

Network intrusion detection (NIDS) filters an entire subnet on a network.

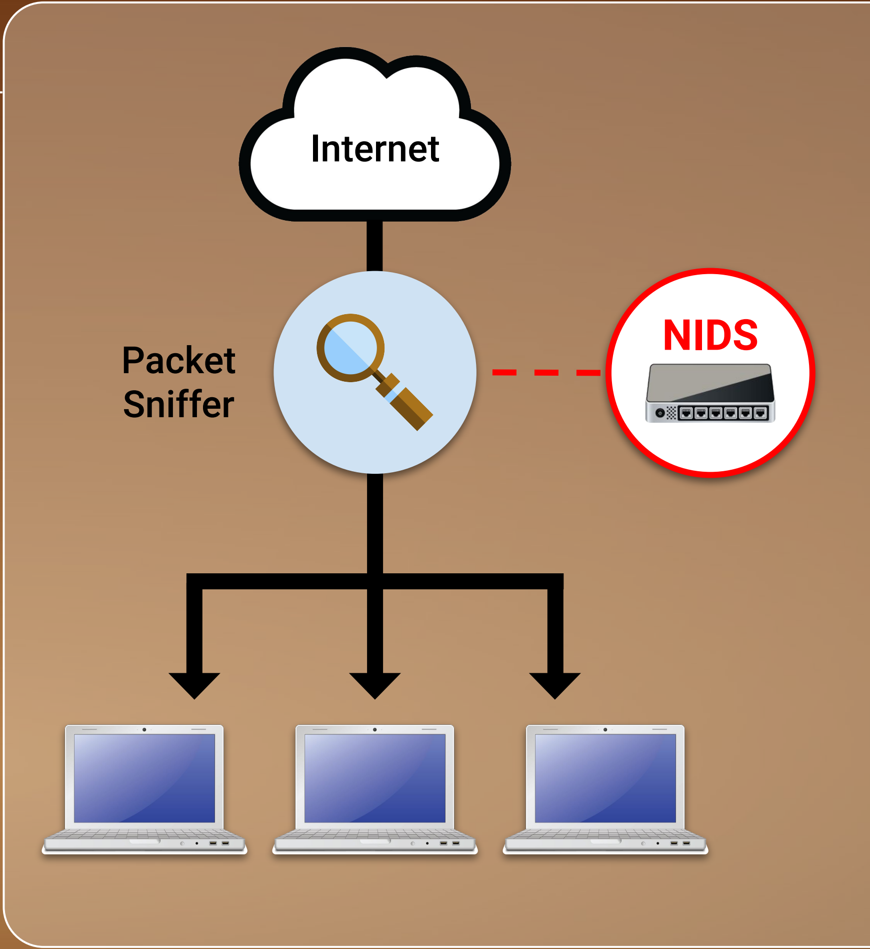
HIDS

Host-based intrusion detection (HIDS) runs locally on a host-based system or user’s workstation or server.

Intrusion Detection Architecture

Network intrusion detection (NIDS) filters an entire subnet on a network.

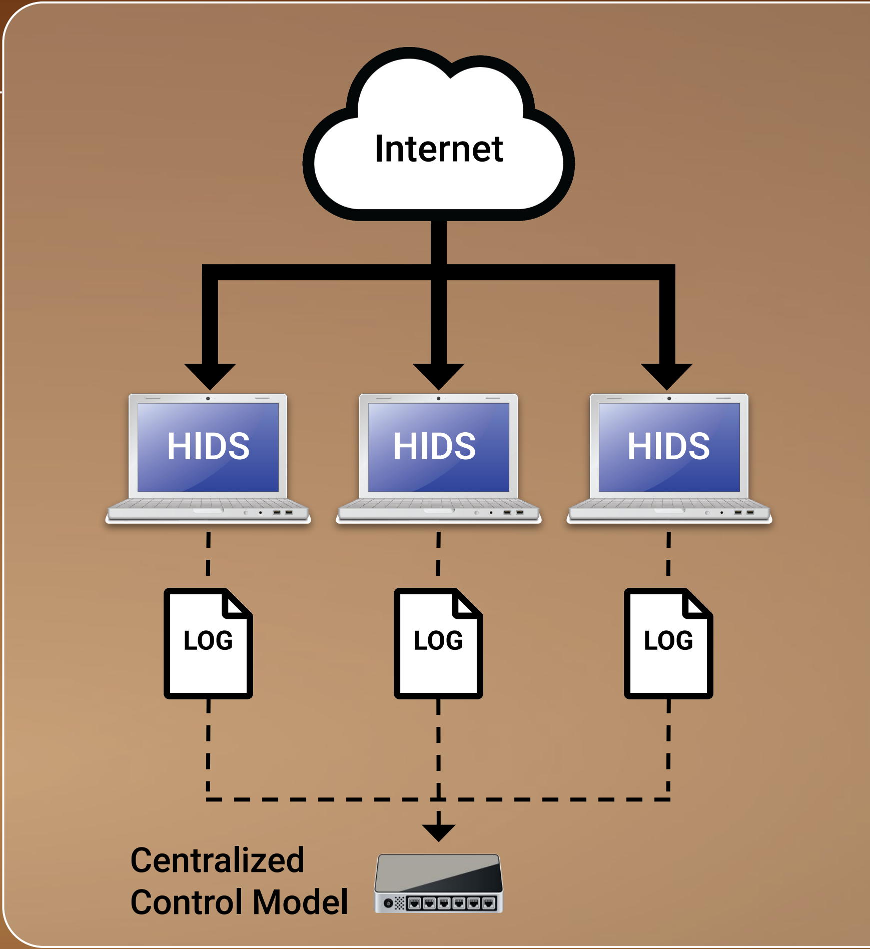
- Matches all traffic to a known library of attack signatures.
- Passively examines network traffic at points that it's deployed.
- Relatively easy to deploy and difficult to detect by attackers.



Intrusion Detection Architecture

Host-based intrusion detection (HIDS) runs locally on a host based system or user’s workstation or server.

- Acts as a second line of defense against malicious traffic that successfully gets past a NIDS.
- Examines entire file systems on a host, compares them to previous snapshots or baselines, and generates an alert if there are significant differences between the two.



Intrusion Prevention System

An **Intrusion Prevention System (IPS)** can do everything an IDS can, but can **also** respond to attacks.

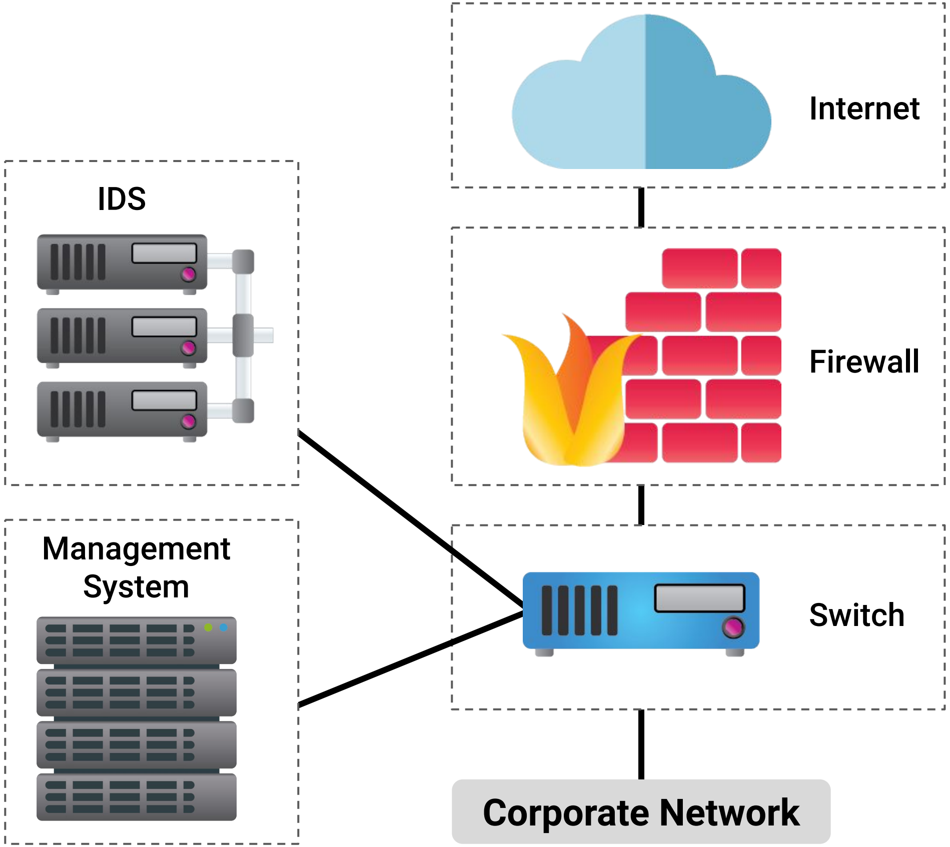
IPS can react to packets by blocking malicious traffic, preventing it from being delivered to a host on the network.

IDS vs. IPS

IDS connects via a network tap or mirrored SPAN port.

- **Network TAP** (Test Access Port) is a hardware device that provides access to a network. Network taps transit both inbound and outbound data streams on separate channels at the same time, so all data will arrive at the monitoring device in real time.
- **SPAN** (Switched Port Analyzer), also known as **port mirroring,** sends a mirror image of all network data to another physical port, where the packets can be captured and analyzed.
- IDS requires an administrator to react to an alert by examining what was flagged.

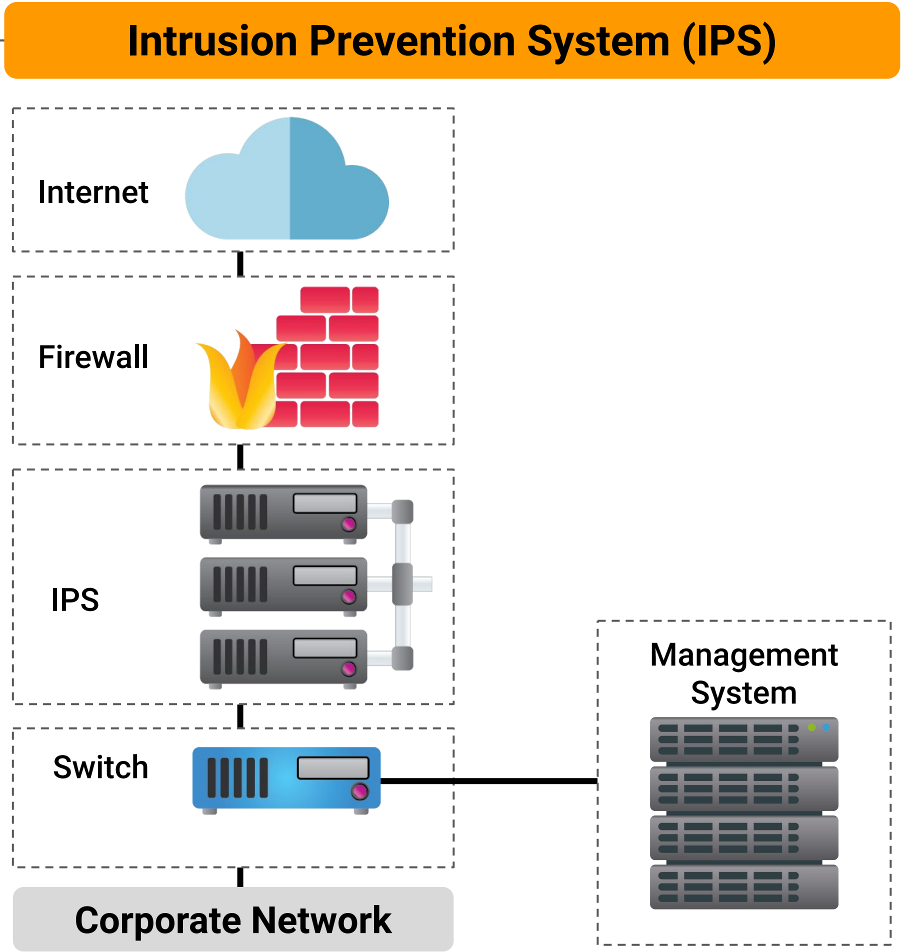
Intrusion Detection System (IDS)



IDS vs. IPS

IPS connects **inline** with the flow of data, typically between the firewall and network switch.

- Requires more robust hardware due to the amount of traffic flowing through it.
- IPS will automatically take action by blocking and logging a threat, thus it doesn't require administrative intervention.



IDS Alerts

An **alert** is a message that is sent to an analyst’s console as an indicator of attack (IOA).

An IDS system generates alerts when a **Snort rule** detects malicious traffic that matches a signature.

```
alert ip any any -> any any {msg: "IP Packet Detected";}
```

IDS Alerts

Indicators can be either:

01 Indicator of Attack (IOA)

Indicators of attack indicate attacks happening in real time.

- Proactive approach to intrusion attempts.
- Indicate that an attack is currently in progress but a full breach has not been determined.
- Focus on revealing the intent and end goal of an attacker, regardless of the exploit or malware used in the attack.

02 Indicator of Compromise (IOC)

Indicators of compromise indicate previous malicious activity.

- Indicate that an attack has occurred, resulting in a breach.
- Used to establish an adversary's techniques, tactics, and procedures (TTPs).
- Expose all the vulnerabilities used in an attack, giving network defenders the opportunity to revamp their defense as part of their mitigation strategy.

Snort

There are many varieties of intrusion detection systems, but today’s class will focus on **Snort**, the world’s most popular open-source solution.

- **Network security monitoring (NSM)** is the process of identifying weaknesses in a network’s defense.
- It also provides organizations with situational awareness of their network.

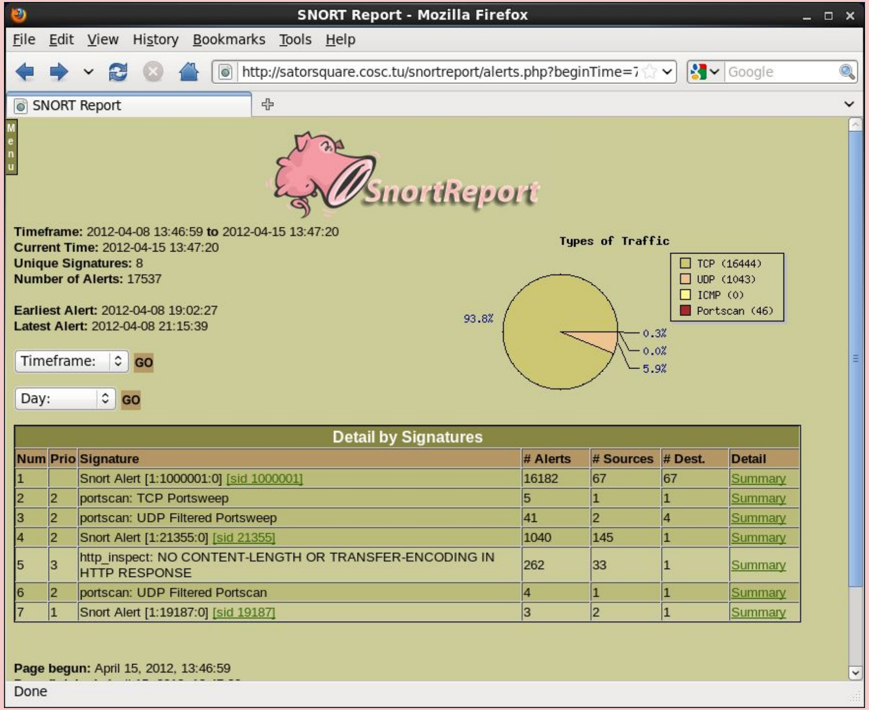
Snort is a free, open source network IDS/IPS.

Snort

Snort is a free, open source network IDS/IPS. It can perform real-time traffic analysis and can log packets on a network.

Snort adds additional layers of defense that can be applied at various layers of the defense in depth model, including:

- Perimeter IDS and IPS architecture
- Network IDS and IPS architecture
- Host IDS and IPS architecture


SNORT Report - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://satorsquare.cosc.tu/snortreport/alerts.php?beginTime=7
Google
SNORT Report
Menu
SnortReport
Types of Traffic
TCP (16444)
UDP (1043)
ICMP (0)
Portscan (46)
93.8%
0.3%
0.0%
5.9%
Timeframe:
GO
Day:
GO
Done

Timeframe: 2012-04-08 13:46:59 **to** 2012-04-15 13:47:20
Current Time: 2012-04-15 13:47:20
Unique Signatures: 8
Number of Alerts: 17537

Earliest Alert: 2012-04-08 19:02:27
Latest Alert: 2012-04-08 21:15:39

Detail by Signatures

Num	Prio	Signature	# Alerts	# Sources	# Dest.	Detail
1		Snort Alert [1:1000001:0] [sid 1000001]	16182	67	67	Summary
2	2	portscan: TCP Portsweep	5	1	1	Summary
3	2	portscan: UDP Filtered Portsweep	41	2	4	Summary
4	2	Snort Alert [1:21355:0] [sid 21355]	1040	145	1	Summary
5	3	http_inspect: NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	262	33	1	Summary
6	2	portscan: UDP Filtered Portscan	4	1	1	Summary
7	1	Snort Alert [1:19187:0] [sid 19187]	3	2	1	Summary

Page begun: April 15, 2012, 13:46:59

Snort Configuration Modes

Snort can operate in three modes:

01

Sniffer Mode
Reads network packets and displays them on screen.

02

Packet Logger Mode
Performs packet captures by logging all traffic to disk.

03

Network IDS Mode
Monitors network traffic, analyzes it, and performs specific actions based on administratively defined rules.

Snort Rules

Snort uses rules to detect and prevent intrusions. It operates by:

01 Reading a configuration file.

02 Loading the rules and plugins.

03 Capturing packets and monitoring traffic for patterns specified in rules.

04 When traffic matches a rule pattern, generating an alert and logging the matching packet for later inspection.

Snort Rules

Rules can direct Snort to monitor the following information:

01

OSI Layer

We can watch for IP and TCP data.

02

Source and Destination Address

Where the traffic is flowing from and to.

03

Byte Sequences

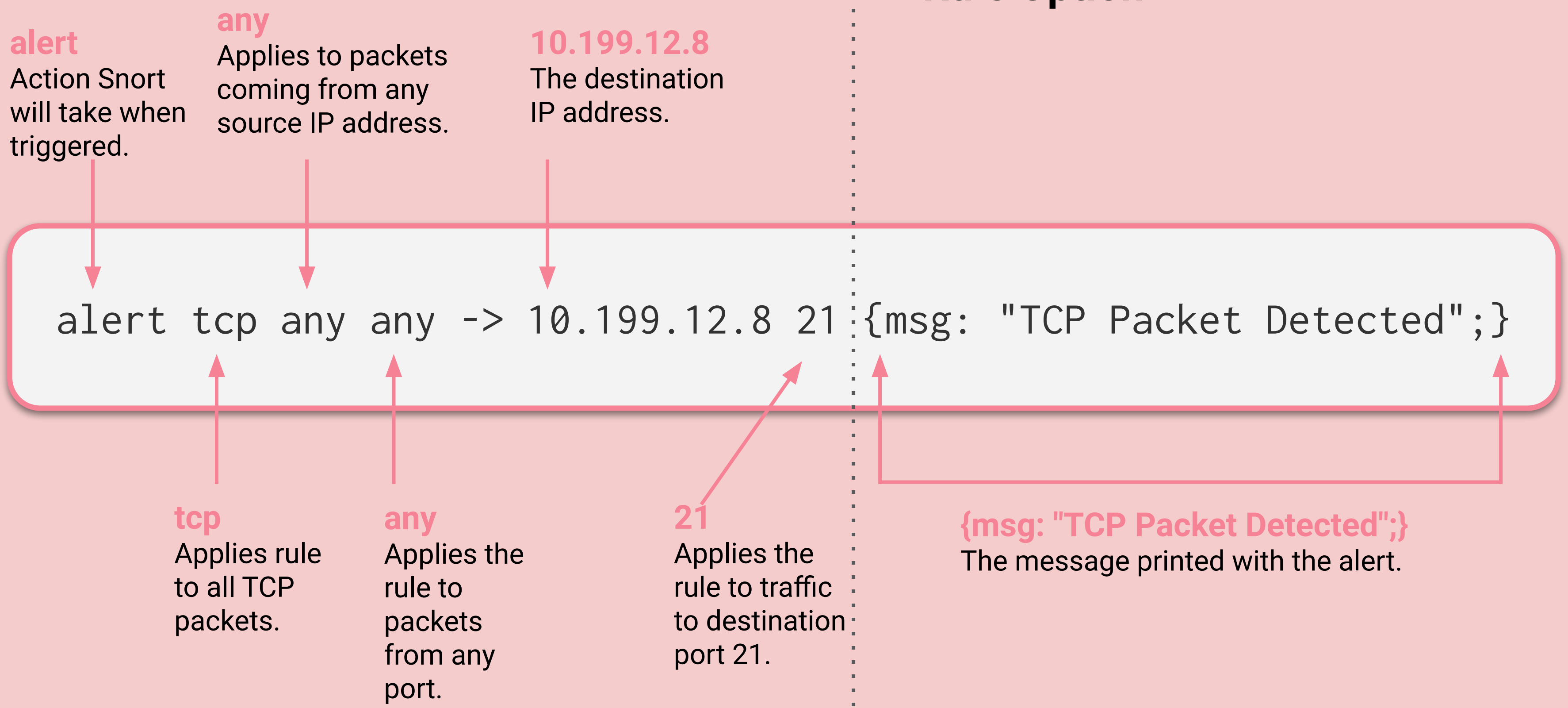
Patterns contained in data packets that might indicate malware, etc.

Snort Rules

```
alert ip any any -> any any {msg: "IP Packet Detected";}
```

This rule logs the message **“IP Packet Detected”** when it detects an IP packet.

Snort Rules



Rule Header

alert
Action Snort will take when triggered.

any
Applies to packets coming from any source IP address.

10.199.12.8
The destination IP address.

```
alert tcp any any -> 10.199.12.8 21 {msg: "TCP Packet Detected";}
```

tcp
Applies rule to all TCP packets.

any
Applies the rule to packets from any port.

21
Applies the rule to traffic to destination port 21.

Rule Option

{msg: "TCP Packet Detected";}
The message printed with the alert.

Activity: IDS and Snort (04_IDS_and_Snort)

Today, you will play the role of an SOC analyst for the California Department of Motor Vehicles (DMV).

In this activity, you will strengthen your knowledge of concepts related to Snort and intrusion detection systems.

Suggested Time:
10 Minutes

Networking Security Monitoring and Security Onion

Network Security Monitoring Case Study

On November 24, 2014, a hacker group released confidential information from Sony Pictures that contained personally identifiable information (PII) for all employees, including full names, home addresses, social security numbers, and financial information.

It was discovered that assailants had lurked on Sony’s network for 17 months.

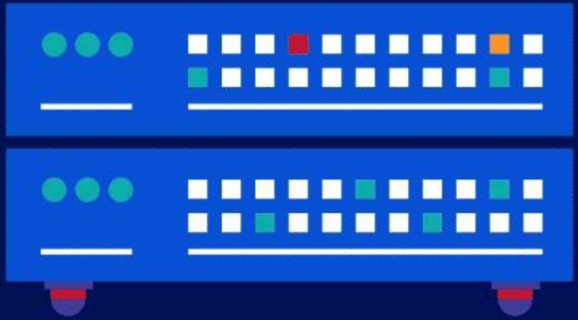
- A number of executives and upper management were fired.
- PII of all employees was exposed.
- Sony suffered massive damage to its reputation.
- Sony had to pay massive fines for violating federal regulations.

(thenextweb.com)

If Sony had a strong **network security monitoring** program, they might have discovered the attack much sooner, stopped it, and gotten a better understanding of the TTPs of the attacker.

Network Security Monitoring

Network security monitoring use a variety of data analysis tools to detect and stop threats after most front-end layers are compromised.



(Source)

NSM Strengths

NSM allows organizations to:

- Track adversaries through a network and determine intent.
- Acquire intelligence and situational awareness.
- Be proactive by identifying vulnerabilities.
- Be reactive through incident response and network forensics.
- Provide insights about advanced persistent threats.
- Uncover and track malware.

NSM Weaknesses

NSM has its limitations:

- Cannot read encrypted traffic (directly)
- Powerful hardware and CPU requirements mean higher costs.
- Difficulty reading radio transmissions, meaning attackers can use mobile radio communications to obfuscate attacks.
- NSM is an invasive process that monitors and records all network data.
- Placement of an NSM can be limited at certain areas of the network.

NSM Stages and Processes

NSM operates in two stages, each involving two processes:

01 **Detection**

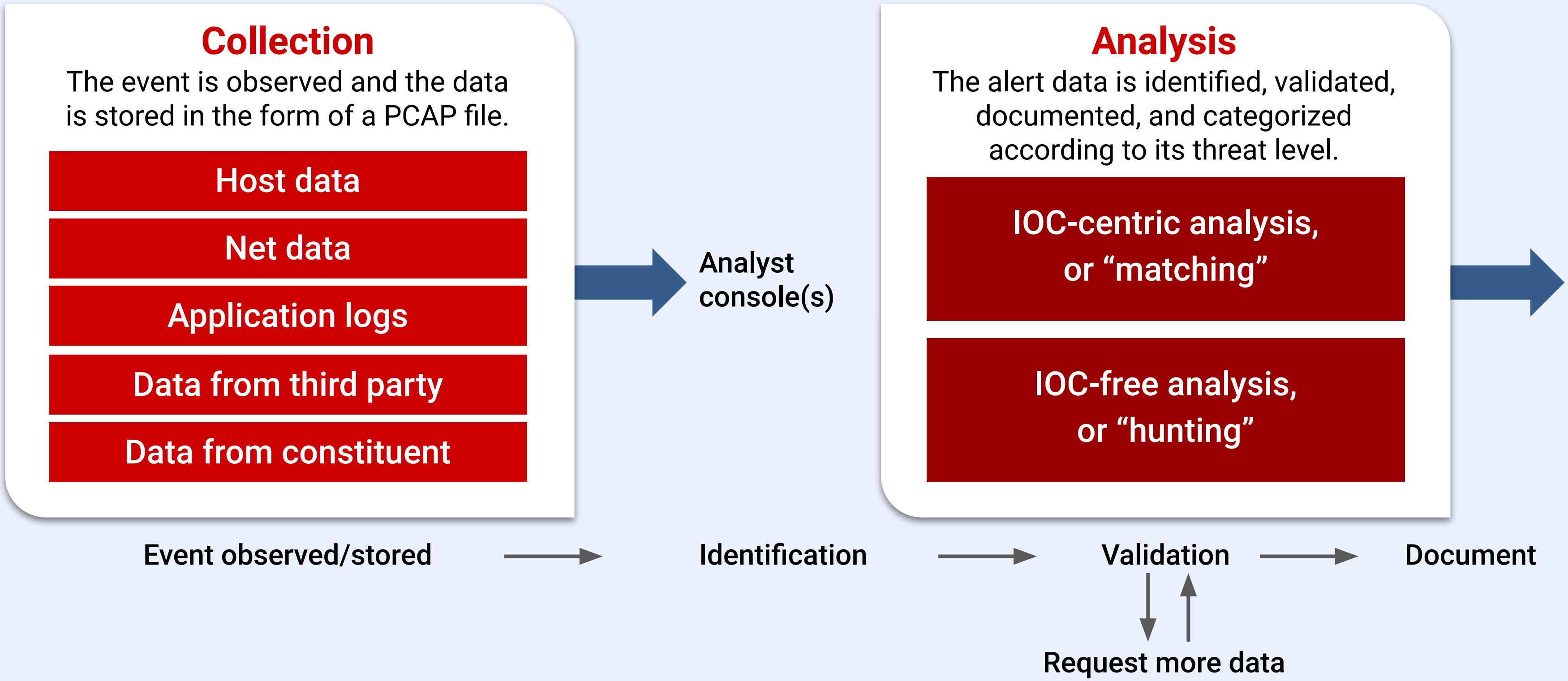
An alert is generated in the Sguil analyst console.

02 **Response**

A security team responds to a security incident.

NSM Stages and Processes

Detection An alert is generated in the Sguil analyst console.



Collection

The event is observed and the data is stored in the form of a PCAP file.

- Host data
- Net data
- Application logs
- Data from third party
- Data from constituent

Analyst console(s)

Analysis

The alert data is identified, validated, documented, and categorized according to its threat level.

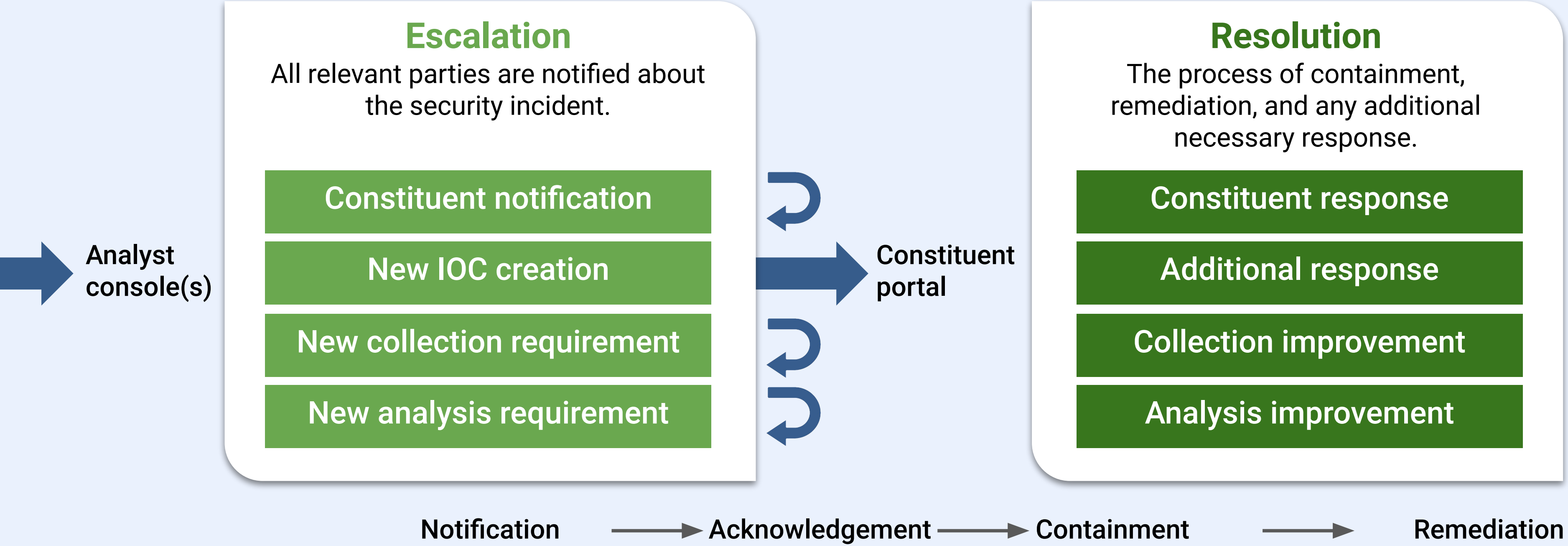
- IOC-centric analysis, or “matching”
- IOC-free analysis, or “hunting”

Event observed/stored → Identification → Validation → Document

Validation ↔ Request more data

NSM Stages and Processes

Response A security team responds to a security incident.



Analyst console(s)

Escalation

All relevant parties are notified about the security incident.

- Constituent notification
- New IOC creation
- New collection requirement
- New analysis requirement

Constituent portal

Resolution

The process of containment, remediation, and any additional necessary response.

- Constituent response
- Additional response
- Collection improvement
- Analysis improvement

Notification → Acknowledgement → Containment → Remediation

Intrusion detection systems are generally placed at strategic points in a network where traffic is most vulnerable.

These devices are typically placed next to a router or switch that filters traffic.

NSM Sensor Connectivity

IDS can be physically connected to a network in two ways:

01 SPAN or Mirrored Port

A SPAN port is a function of an enterprise-level switch that allows you to mirror one or more physical switch ports to another port.

A mirror image of all data will flow across both ports equally.

02 Network TAP

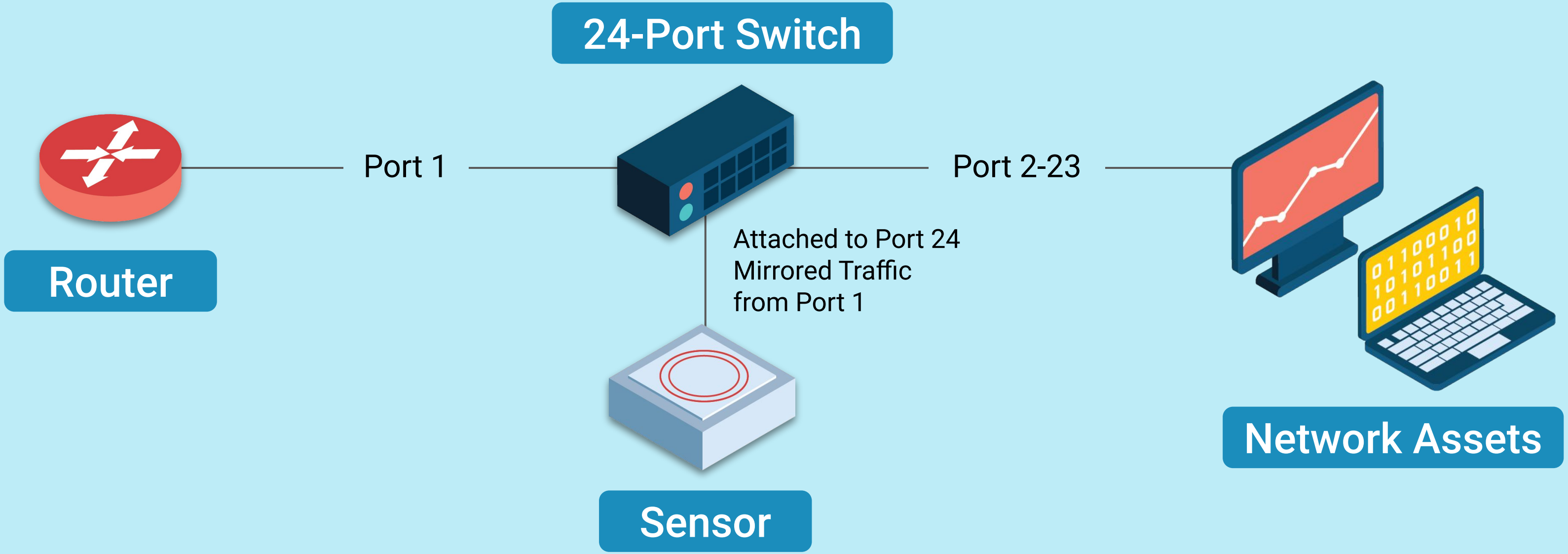
The most common type of TAP is an aggregated TAP, in which a cable connects the TAP monitor port with the NIC on the sensor. This specific placement allows traffic to be monitored between the router and switch.

NSM Sensor Connectivity

01

SPAN or Mirrored Port

A SPAN port is a function of an enterprise-level switch allowing you to mirror one or more physical switch ports to another port. A mirror image of all data flows across both ports equally. This allows the IDS to perform packet captures on all inbound and outbound traffic within a network.

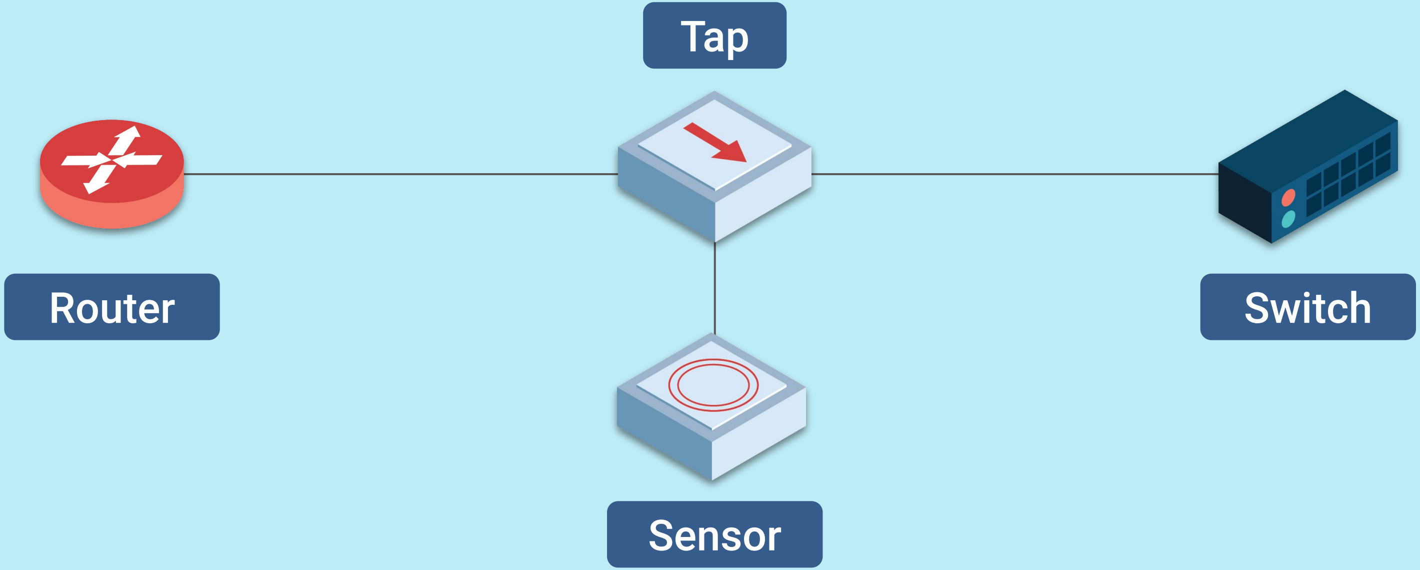


NSM Sensor Connectivity

02

Network Tap

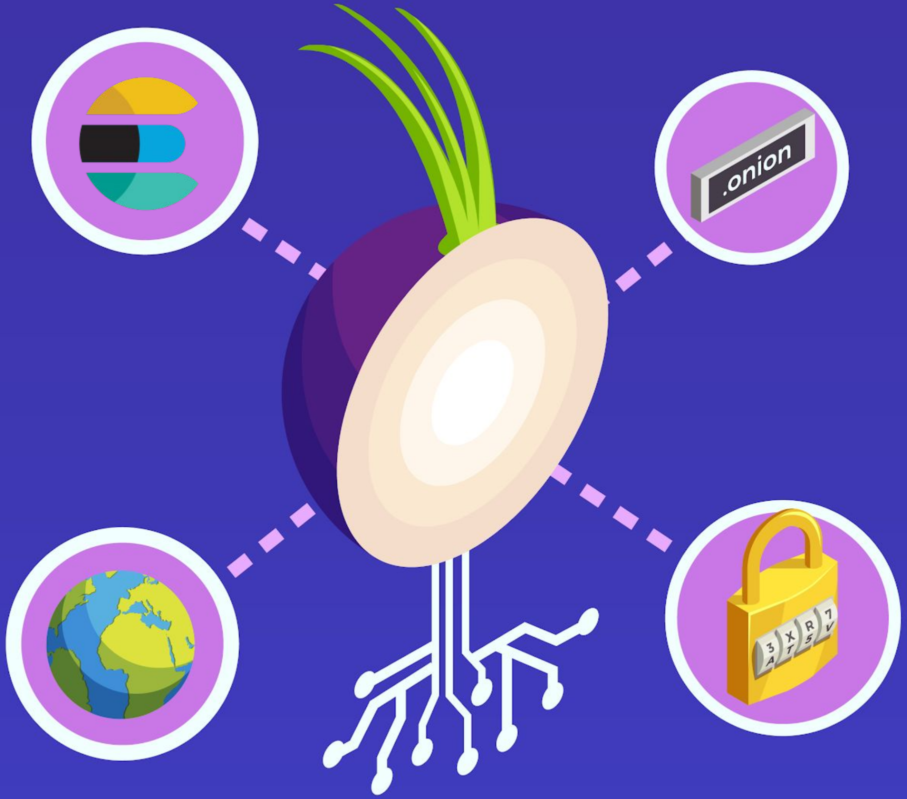
The most common type of TAP
is an aggregated TAP, in which a cable connects the TAP monitor port with the NIC on the sensor. This specific placement allows traffic to be monitored between the router and switch.



Security Onion

Today we'll work with Security Onion, a network security monitoring platform that provides context, intelligence, and situational awareness of a network.

Security Onion is an Ubuntu-based, open source Linux distribution that contains many NSM tools used to protect networks from attacks.



Security Onion and NSM

We'll also use a few NSM tools for incident detection and response:

01

Sguil

Pulls alert data from Snort, allowing us to more thoroughly analyze alerts.

02

Transcript

Provides a view of PCAP transcripts that are rendered with TCP flow.

03

NetworkMiner

Performs advanced network traffic analysis through extraction of artifacts contained in PCAP files.

Sguil (pronounced: “sgweel”)

Sguil has six key functions that help with analysis:

01 Performs simple aggregation of alert data records.

02 Makes available certain types of metadata.

03 Allows queries and review of alert data.

04 Allows queries and review of session data.

05 Allows easy transitions between alert or session data and full content data.

06 Counts and classifies events, enabling escalation and other incident response decisions.

Sguil

Sguil has four main sections:

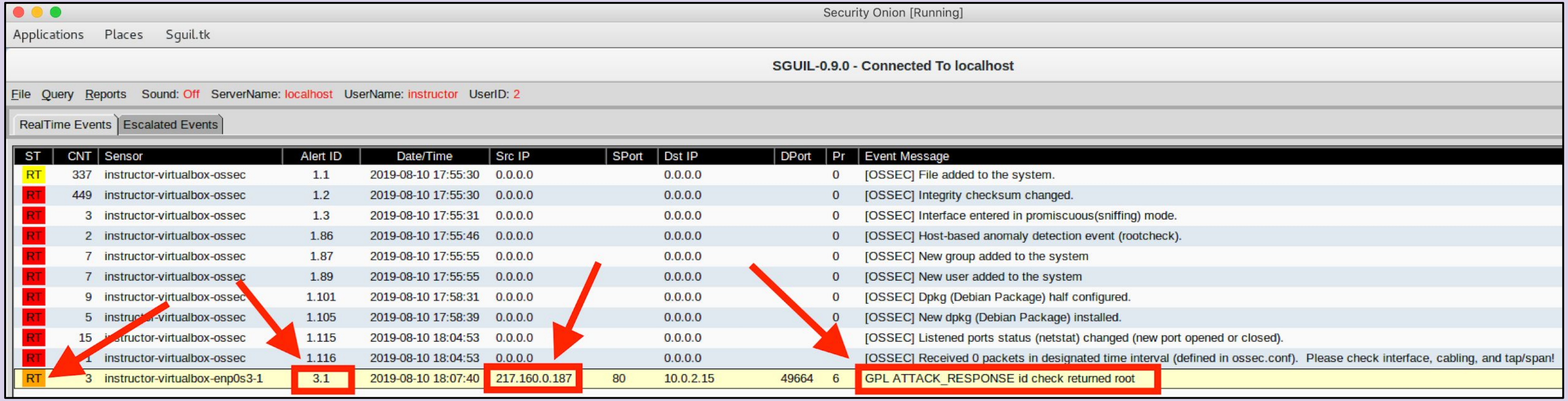
01 Alert Panel

02 Snort Rule

03 Packet Data

04 IP Resolution

Sguil Alert Panel



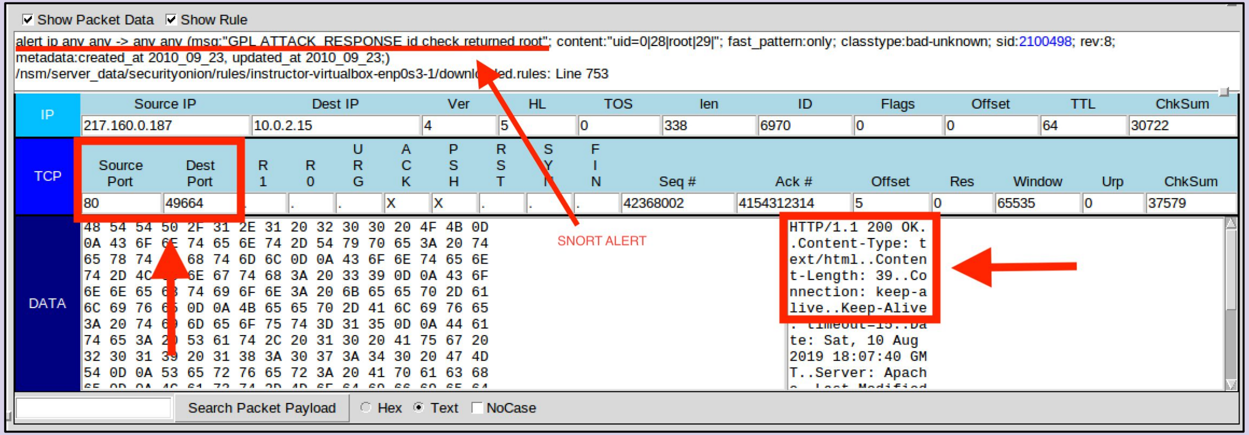
SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: instructor UserID: 2

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	337	instructor-virtualbox-ossec	1.1	2019-08-10 17:55:30	0.0.0.0		0.0.0.0		0	[OSSEC] File added to the system.
RT	449	instructor-virtualbox-ossec	1.2	2019-08-10 17:55:30	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum changed.
RT	3	instructor-virtualbox-ossec	1.3	2019-08-10 17:55:31	0.0.0.0		0.0.0.0		0	[OSSEC] Interface entered in promiscuous(sniffing) mode.
RT	2	instructor-virtualbox-ossec	1.86	2019-08-10 17:55:46	0.0.0.0		0.0.0.0		0	[OSSEC] Host-based anomaly detection event (rootcheck).
RT	7	instructor-virtualbox-ossec	1.87	2019-08-10 17:55:55	0.0.0.0		0.0.0.0		0	[OSSEC] New group added to the system
RT	7	instructor-virtualbox-ossec	1.89	2019-08-10 17:55:55	0.0.0.0		0.0.0.0		0	[OSSEC] New user added to the system
RT	9	instructor-virtualbox-ossec	1.101	2019-08-10 17:58:31	0.0.0.0		0.0.0.0		0	[OSSEC] Dpkg (Debian Package) half configured.
RT	5	instructor-virtualbox-ossec	1.105	2019-08-10 17:58:39	0.0.0.0		0.0.0.0		0	[OSSEC] New dpkg (Debian Package) installed.
RT	15	instructor-virtualbox-ossec	1.115	2019-08-10 18:04:53	0.0.0.0		0.0.0.0		0	[OSSEC] Listened ports status (netstat) changed (new port opened or closed).
RT	1	instructor-virtualbox-ossec	1.116	2019-08-10 18:04:53	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf). Please check interface, cabling, and tap/span!
RT	3	instructor-virtualbox-enp0s3-1	3.1	2019-08-10 18:07:40	217.160.0.187	80	10.0.2.15	49664	6	GPL ATTACK_RESPONSE id check returned root

ST or Status	Colors indicate severity levels of real-time"or "RT" events. Red Critical, possible data breach in progress. Must be resolved immediately. Orange Moderate, high potential for data breach. Requires immediate review. Yellow General, low potential for data breach. Requires review.
Alert ID	A randomly generated numerical ID created by Sguil.
Source IP	IP address of the source identified by the alert.
Event Message	The message generated by the Snort rule option.

Sguil Snort Rule and Packet Data



☑ Show Packet Data ☑ Show Rule

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;
metadata:created_at 2010_09_23, updated_at 2010_09_23;)
/nsm/server_data/securityonion/rules/instructor-virtualbox-enp0s3-1/downloaded.rules: Line 753
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	217.160.0.187	10.0.2.15	4	5	0	338	6970	0	0	64	30722

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	ChkSum
	80	49664	.	.	.	X	X	.	.	.	42368002	4154312314	5	0	65535	0	37579

DATA

```
48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D   HTTP/1.1 200 OK.
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 43 6F 6E 74 65 6E   ext/html..Conten
74 2D 4C 65 6E 67 74 68 3A 20 33 39 0D 0A 43 6F   t-Length: 39..Co
6E 6E 65 63 74 69 6F 6E 3A 20 6B 65 65 70 2D 61   nnection: keep-a
6C 69 76 65 0D 0A 4B 65 65 70 2D 41 6C 69 76 65   live..Keep-Alive
3A 20 74 69 6D 65 6F 75 74 3D 31 35 0D 0A 44 61   : timeout=15..Da
74 65 3A 20 53 61 74 2C 20 31 30 20 41 75 67 20   te: Sat, 10 Aug
32 30 31 39 20 31 38 3A 30 37 3A 34 30 20 47 4D   2019 18:07:40 GM
54 0D 0A 53 65 72 76 65 72 3A 20 41 70 61 63 68   T..Server: Apach
65 0D 0A 4C 61 73 74 2D 4D 6F 64 69 66 69 65 64   e..Last-Modified
```

Search Packet Payload ○ Hex ● Text □ NoCase

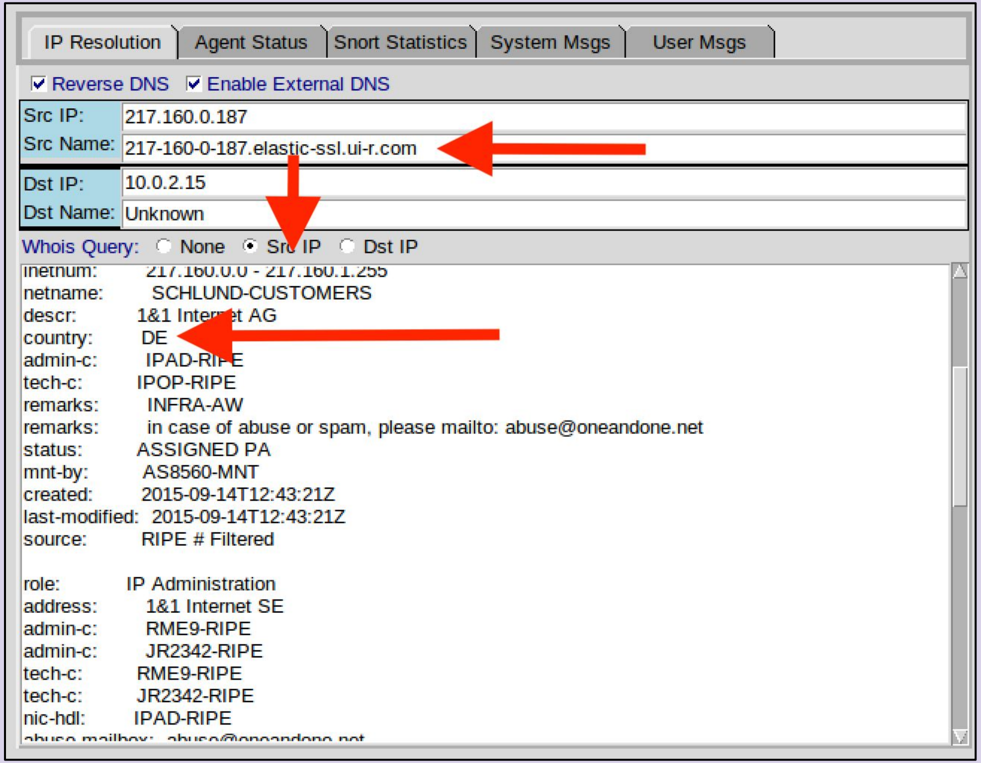
SNORT ALERT

Snort Rule	Packet Data
In the top portion of this window is the Snort NIDS engine that generated alert data when traffic matched one of its rules. • Alert data is an indicator of attack. An analyst may have to determine if it represents benign or malicious activity. • Alert data from the Snort NIDS stores entries in the Event Messages column that begin with text like “ET” (for Emerging Threats, an IDS rule source).	The lower, more colorful part of this window is the portion of Sguil that performs network packet analysis. • The packet analyzer presents a detailed view of the data capture that includes packet header information and data streams presented in hex and text form.

Sguil’s IP Resolution

This section of Sguil's analyst console provides reverse DNS lookup information.

- This information is used to reveal identifying information about the attacker, including domain name registries and IP addresses.
- Other information may include country of origin, and possibly the names, email addresses, and/or phone numbers of the DNS registrants.



☑ Reverse DNS ☑ Enable External DNS

Src IP: 217.160.0.187

Src Name: 217-160-0-187.elastic-ssl.ui-r.com

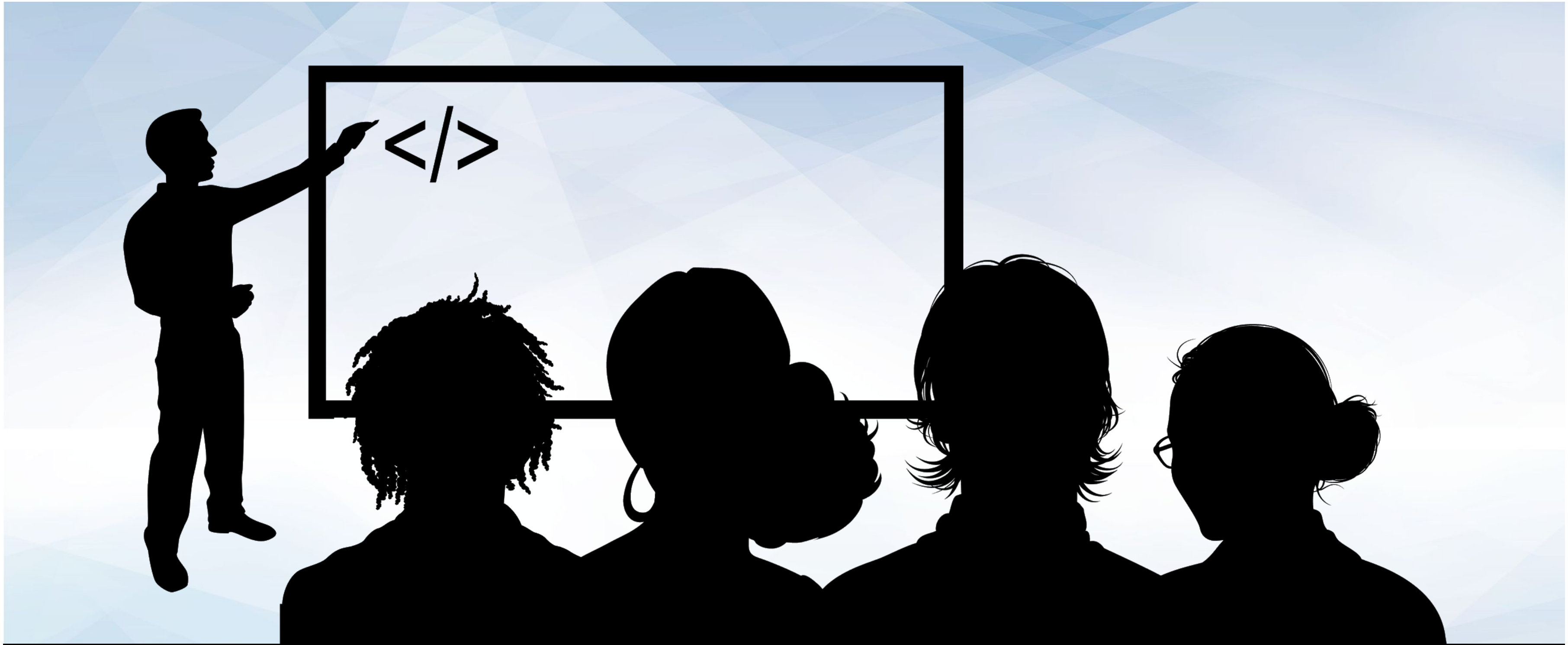
Dst IP: 10.0.2.15

Dst Name: Unknown

Whois Query: ○ None ● Src IP ○ Dst IP

```
inetnum:        217.160.0.0 - 217.160.1.255
netname:        SCHLUND-CUSTOMERS
descr:          1&1 Internet AG
country:        DE
admin-c:        IPAD-RIPE
tech-c:         IPOP-RIPE
remarks:        INFRA-AW
remarks:        in case of abuse or spam, please mailto: abuse@oneandone.net
status:         ASSIGNED PA
mnt-by:         AS8560-MNT
created:        2015-09-14T12:43:21Z
last-modified:  2015-09-14T12:43:21Z
source:         RIPE # Filtered

role:           IP Administration
address:        1&1 Internet SE
admin-c:        RME9-RIPE
admin-c:        JR2342-RIPE
tech-c:         RME9-RIPE
tech-c:         JR2342-RIPE
nic-hdl:        IPAD-RIPE
abuse-mailbox:  abuse@oneandone.net
```



Instructor Demonstration

Security Onion - Sguil

Activity: Security Onion and NSM (07_Security_Onion_NSM)

In this activity, you will reinforce your knowledge of Security Onion and network security monitoring.

Suggested Time:
20 Minutes

Alert:
FTP File Extraction

Security Onion Demo Setup

Sometimes, an alert requires an analyst to do some data mining.

- A security analyst must have a thorough understanding of how NSM tools are integrated.
- These skills help speed up incident and response efforts.

(Source)

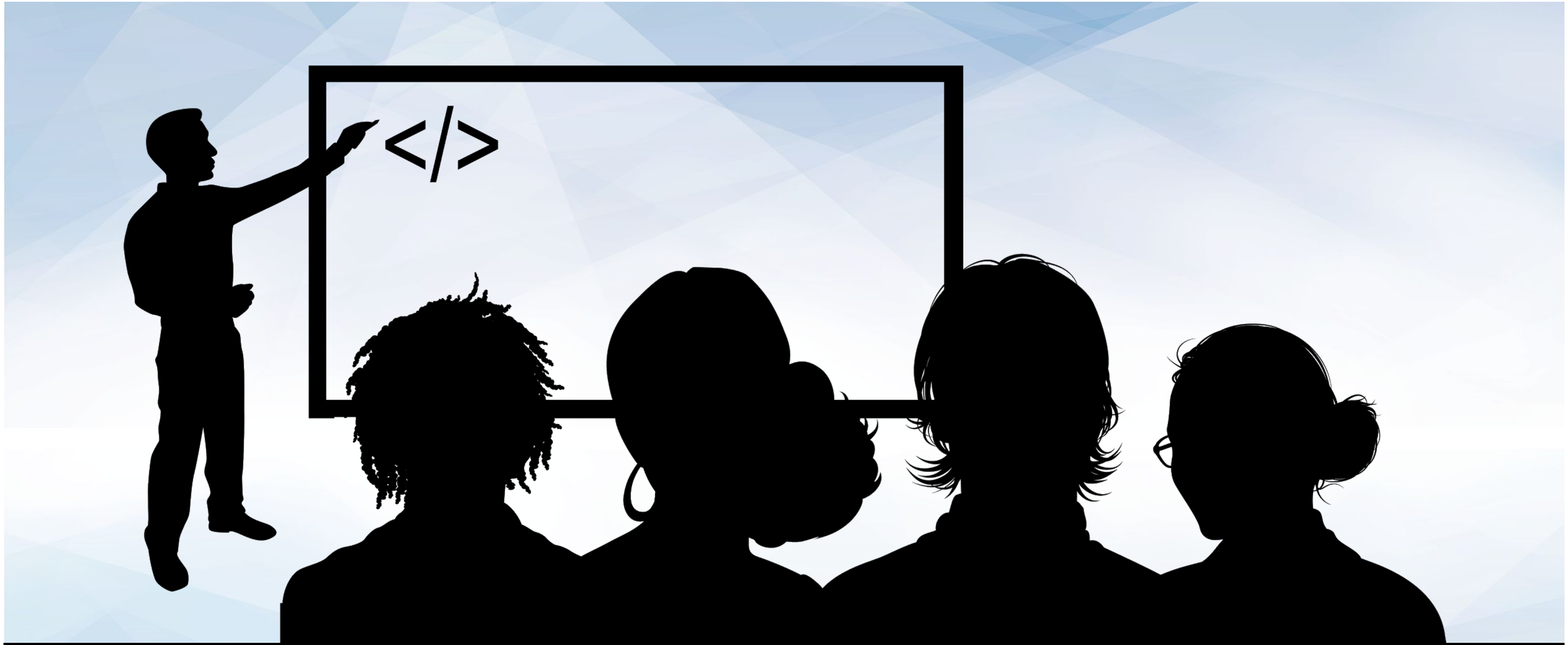
In the next walkthrough, we’ll use Sguil as the starting point for learning other NSM tools for security investigations.

Security Onion and NetworkMiner Demo

Now that we now know there was a drive-by attack, we must search for any files that were downloaded to the host.

We'll use a forensics tool called **NetworkMiner** to extract any files that were installed on the user's machine, and put together an attacker profile.

- Network Miner is an NSM tool that performs advanced Network Traffic Analysis (NTA) of extracted artifacts, presented through an intuitive interface.



Instructor Demonstration

Security Onion - NetworkMiner

Activity: Alert - FTP File Extraction (11_Alert_FTP_File_Extraction)

In this activity, you will examine an alert to determine if any systems were breached and if any data was supplanted or exfiltrated from the network.

Suggested Time:
20 Minutes