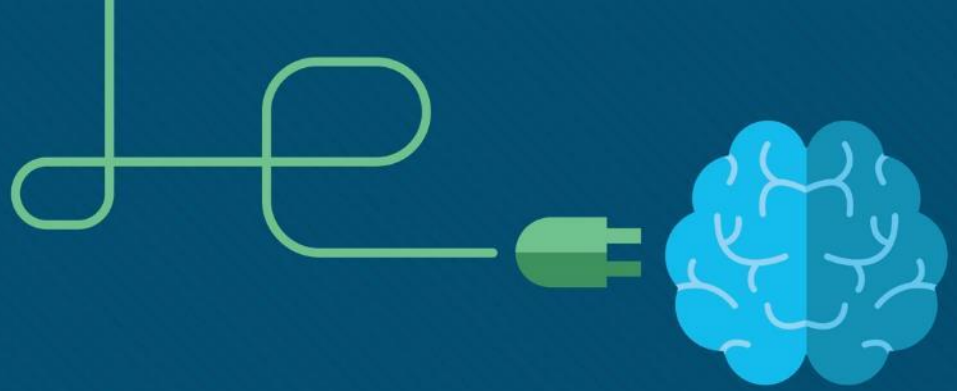


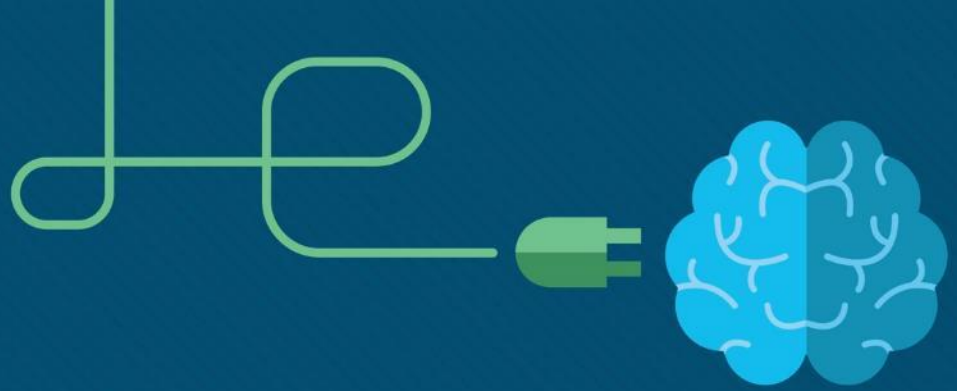
Chapter 12: Intrusion Data Analysis

Instructor Materials

CCNA Cybersecurity Operations V1.1

Chapter 12: Intrusion Data Analysis

CCNA Cybersecurity Operations v1.1 Planning Guide



Chapter 12: Intrusion Data Analysis

CCNA Cybersecurity Operations v1.1

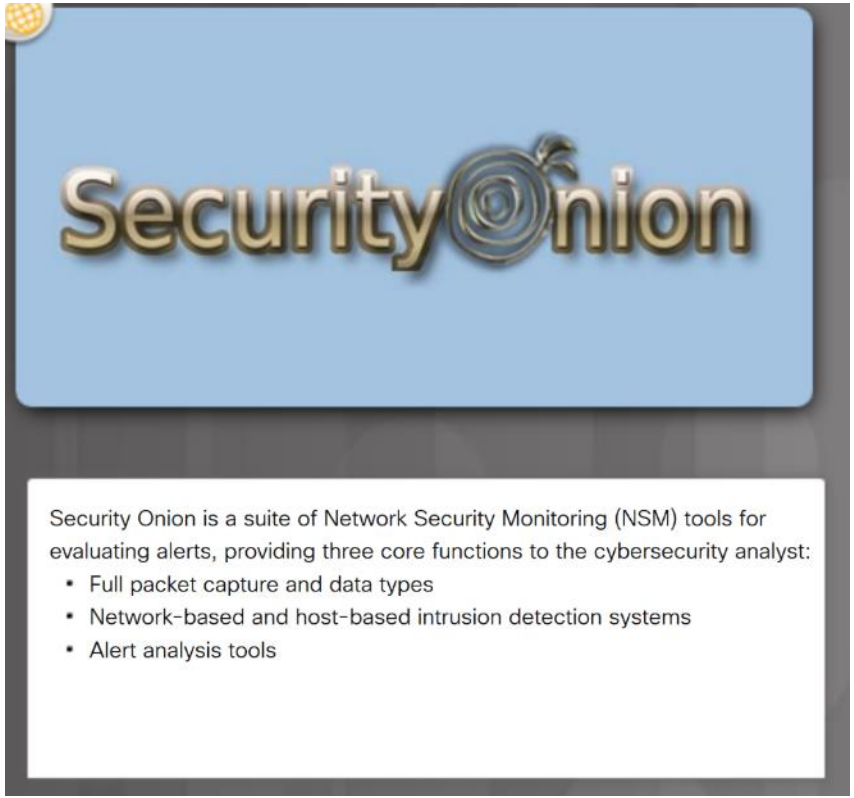
Chapter 12 - Sections & Objectives

- 12.1 Evaluating Alerts
  - Explain the process of evaluating alerts.
    - Identify the structure of alerts.
    - Explain how alerts are classified.
- 12.2 Working with Network Security Data
  - Interpret data to determine the source of an alert.
    - Explain how data is prepared for use in a Network Security Monitoring (NSM) system.
    - Use Security Onion tools to investigate network security events.
    - Describe network monitoring tools that enhance workflow management.
- 12.3 Digital Forensics
  - Explain how the cybersecurity analyst handles digital forensics and evidence to ensure proper attack attribution.
    - Explain the role of digital forensic processes.

12.1 Evaluating Alerts

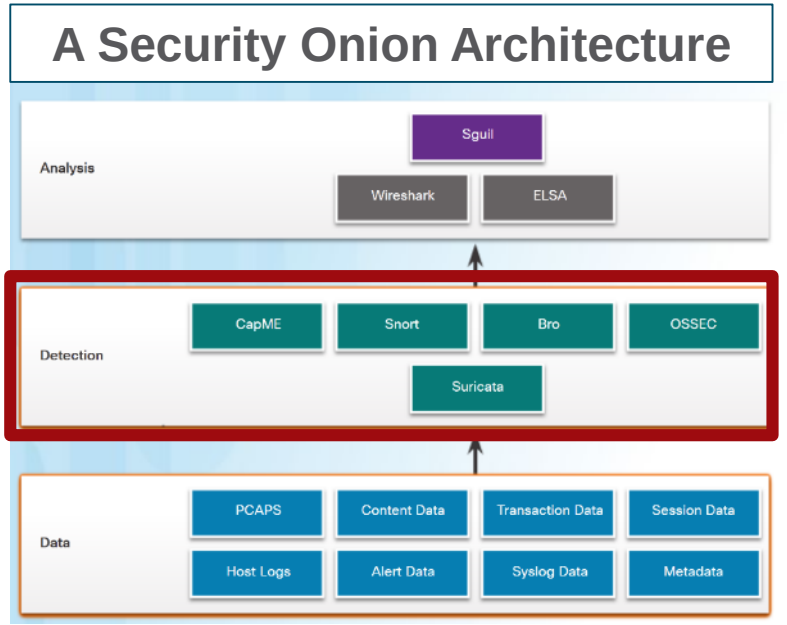
Security Onion

- Security Onion is an open-source suite of Network Security Monitoring (NSM) tools that run on an Ubuntu Linux distribution.
- Some components of Security Onion are owned and maintained by corporations, such as Cisco and Riverbend Technologies, but are made available as open source.

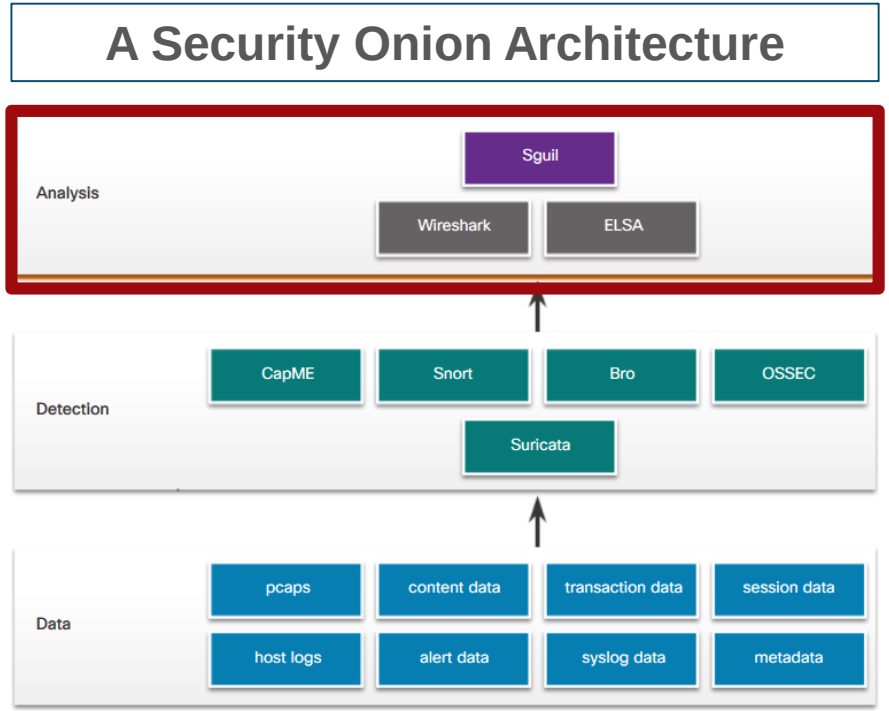


Detection Tools for Collection

- **CapME** provides the cybersecurity analyst with an easy-to-read means of viewing an entire Layer 4 session.
- **Snort** uses rules and signatures to generate alerts.
- **Bro** uses policies, in the form of scripts that determine what data to log and when to issue alert notifications.
- **OSSEC** actively monitors host system operations, including conducting file integrity monitoring, local log monitoring, system process monitoring, and rootkit detection.
- **Suricata** uses native multithreading, which allows the distribution of packet stream processing across multiple processor cores.



Analysis Tools

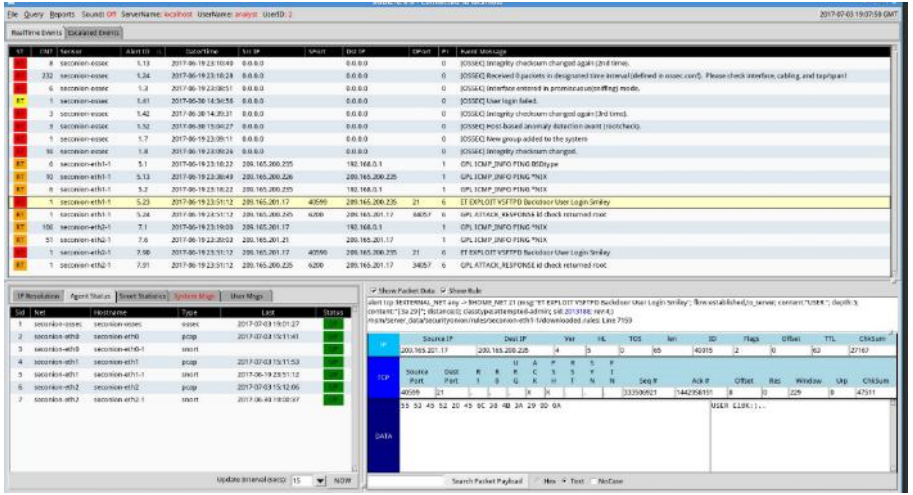


- **Sguil** – This provides a high-level cybersecurity analysts' console for investigating security alerts from a wide variety of sources.
- **ELSA** – Logging sources such as HIDS, NIDS, firewalls, syslog clients and servers, domain services, and others can be configured to make their logs available to ELSA databases.
- **Wireshark** – This is a packet capture application that is integrated into the Security Onion suite.

Alert Generation

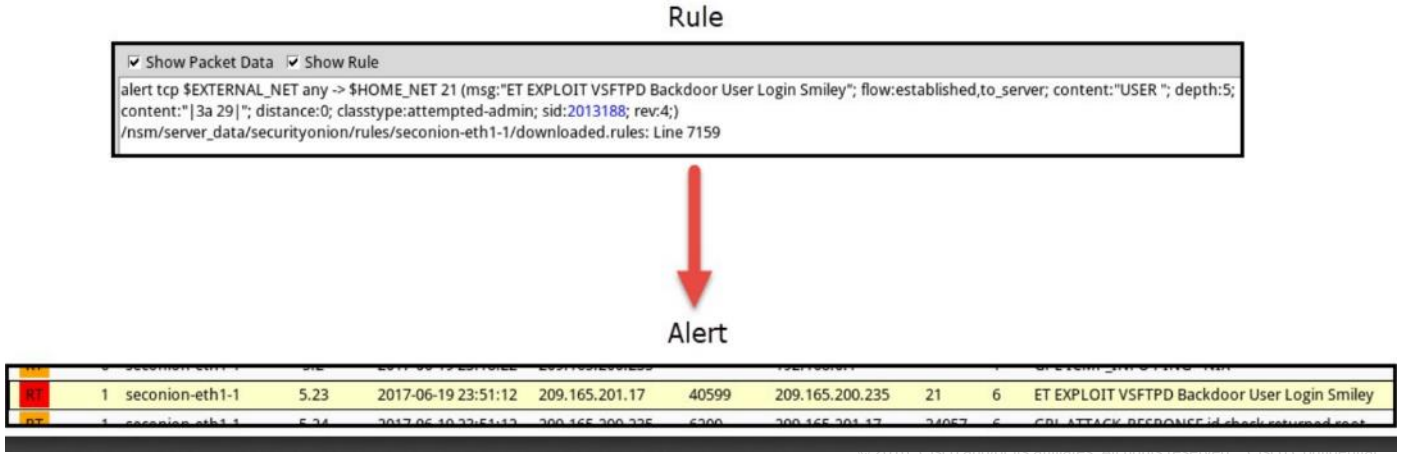
- Alerts are generated in Security Onion by many sources including Snort, Bro, Suricata, and OSSEC, among others.
- Sguil provides a console that integrates alerts from multiple sources into a timestamped queue.
- Alerts will generally include the following five-tuples information:
  - SrcIP - the source IP address for the event.
  - SPort - the source (local) Layer 4 port for the event.
  - DstIP - the destination IP for the event.
  - DPort - the destination Layer 4 port for the event.
  - Pr - the IP protocol number for the event.

Sguil Window



Rules and Alerts

- Alerts can come from a number of sources:
  - NIDS - Snort, Bro and Suricata
  - HIDS – OSSEC
  - Asset management and monitoring - Passive Asset Detection System (PADS)
  - HTTP, DNS, and TCP transactions - Recorded by Bro and pcaps
  - Syslog messages - Multiple sources



Snort Rule Structure

- Snort rules consist of the rule header and rule options.
  - Rule header contains the action, protocol, addressing, and port information
  - Rule options include the text message that identifies the alert also metadata about the alert.
- Snort rules come from a variety of sources including Emerging Threats (ET), SourceFire, and Cisco Talos.
- PulledPork is a Security Onion component that can download new rules automatically from snort.org.

```
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;)
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692
```

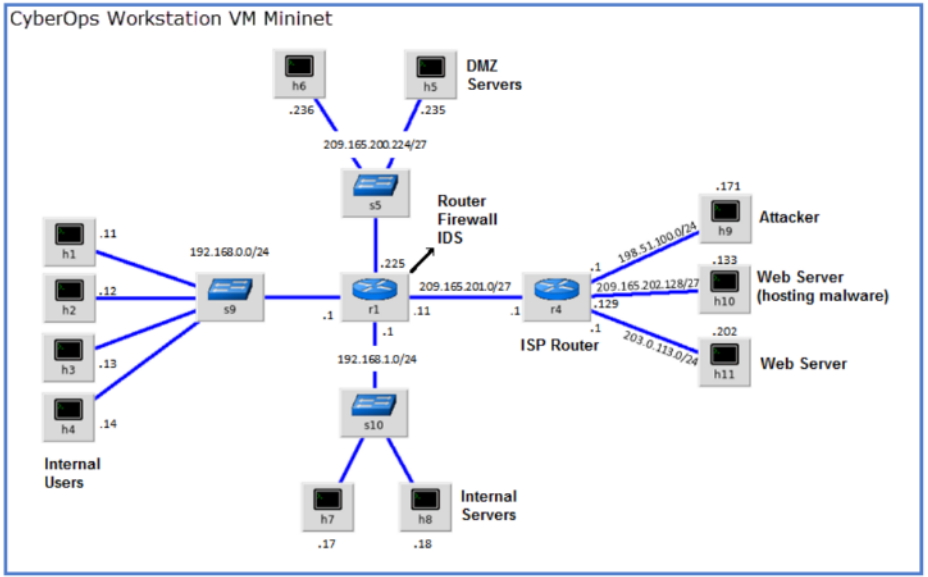
Component	Explanation
rule header	contains the action to be taken, source and destination addresses and ports, and the direction of traffic flow
rule options	includes the message to be displayed, details of packet content, alert type, source ID, and additional details, such as a reference for the rule or vulnerability
rule location	added by Sguil to indicate the location of the rule in the Security Onion file structure and in the specified rule file

Lab – Snort and Firewall Rules

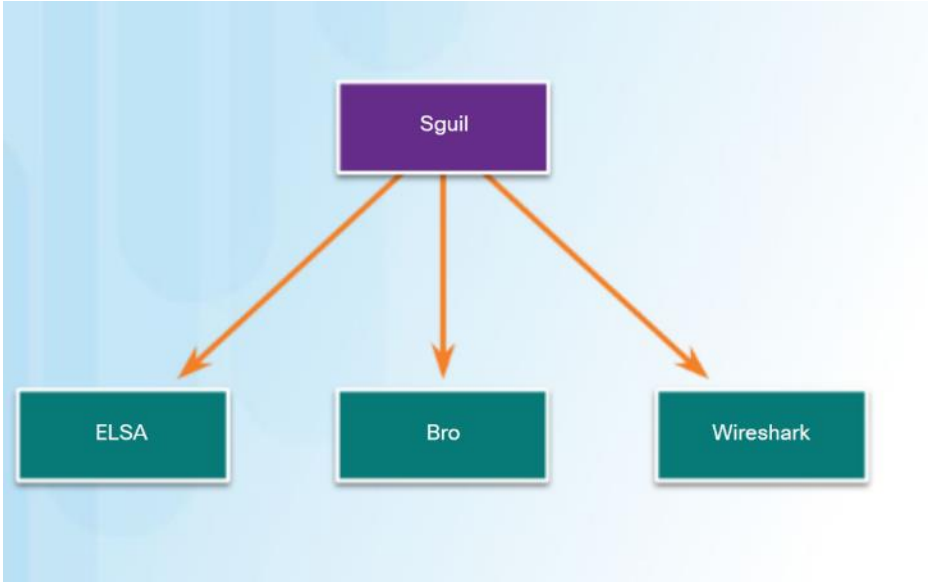
Networking Academy

Lab – Snort and Firewall Rules

Topology



The Need for Alert Evaluation



- Exploits will inevitably evade protection measures, no matter how sophisticated they may be.
- Detection rules should be overly conservative.
- It is necessary to have skilled cybersecurity analysts investigate alerts to determine if an exploit has actually occurred.
- Tier 1 cybersecurity analysts will work through queues of alerts in a tool like Sguil, pivoting to tools like Bro, Wireshark, and ELSA .

Evaluating Alerts

- Alerts can be classified as follows:
  - **True Positive**: The alert has been verified to be an actual security incident.
  - **False Positive**: The alert does not indicate an actual security incident.
  - **True Negative**: No security incident has occurred.
  - **False Negative**: An undetected incident has occurred.

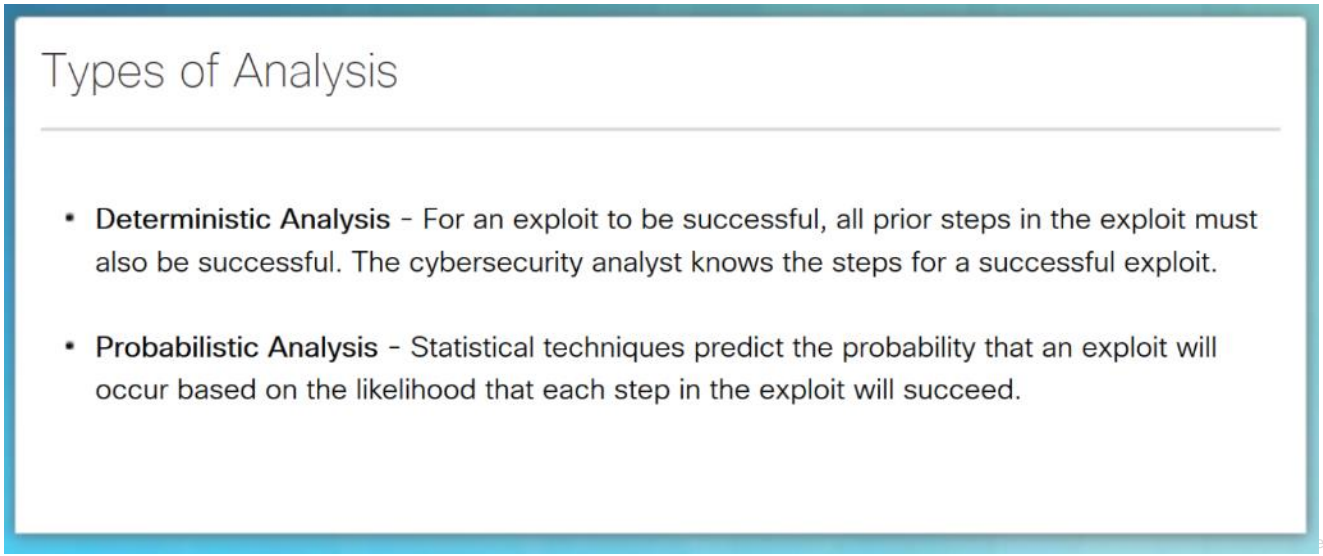
When an alert is issued, it will receive one of four possible classifications

	True	False
Positive (Alert exists)	Incident occurred	No incident occurred
Negative (No alert exists)	No incident occurred	Incident occurred

Events classified as 'true" are desired.

Deterministic Analysis and Probabilistic Analysis

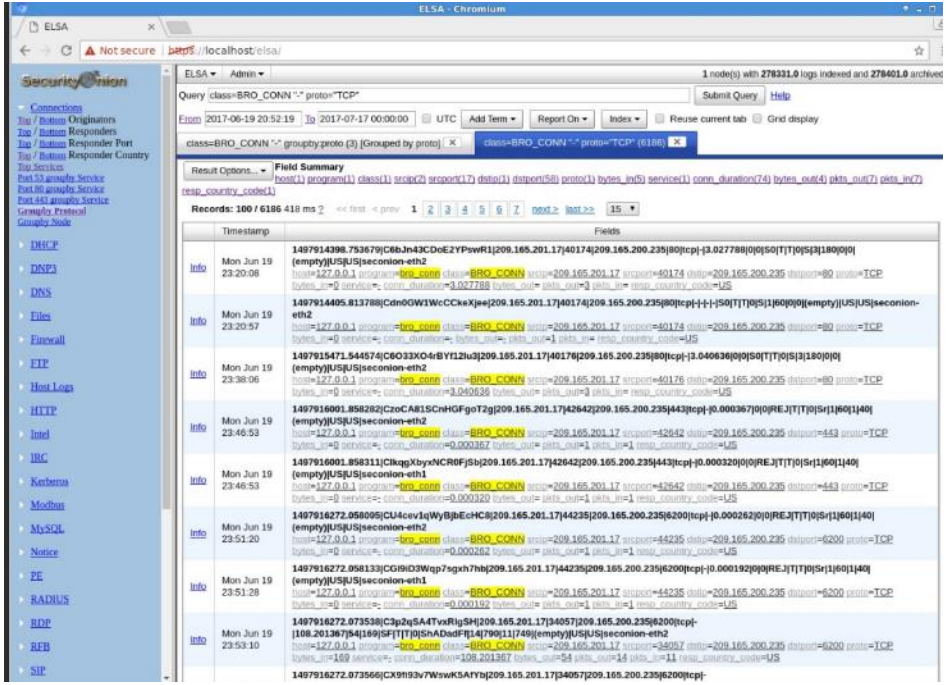
- Statistical techniques can be used to evaluate the risk that exploits will be successful in a given network.
  - **Deterministic Analysis** – evaluates risk based on what is known about a vulnerability.
  - **Probabilistic Analysis** – estimates the potential success of an exploit by estimating the likelihood that if one step in an exploit has successfully been completed that the next step will also be successful.



12.2 Working with Network Security Data

A Common Data Platform

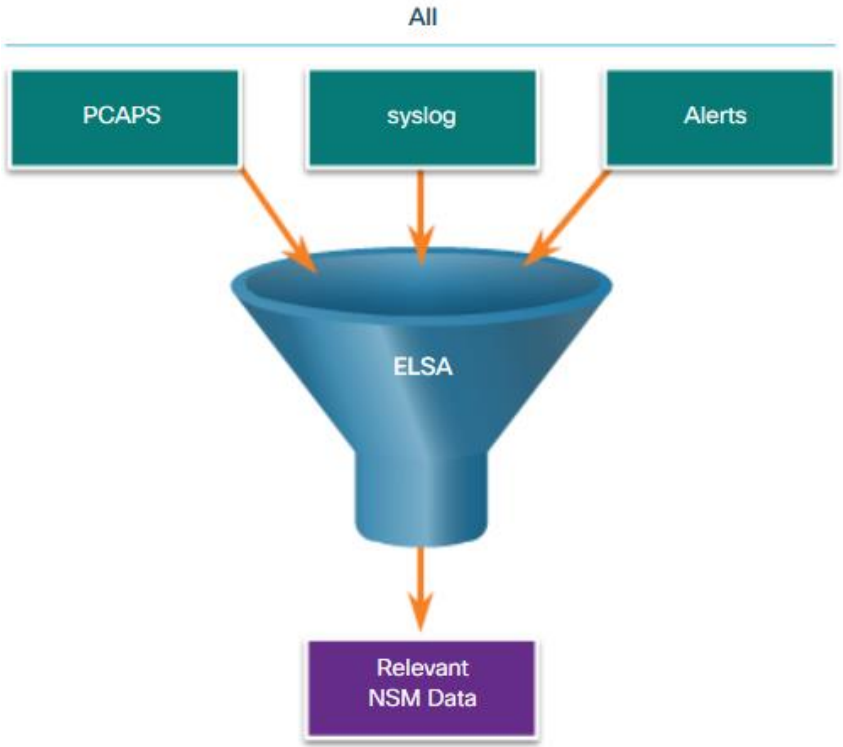
ELSA



- Enterprise Log Search and Archive (ELSA) is an enterprise-level tool for searching and archiving NSM data that originates from multiple sources.
- ELSA is able to normalize log file entries into a common schema that can then be displayed in the ELSA web interface.
- ELSA receives logs over Syslog-NG, stores logs in MySQL databases, and indexes using Sphinx Search.

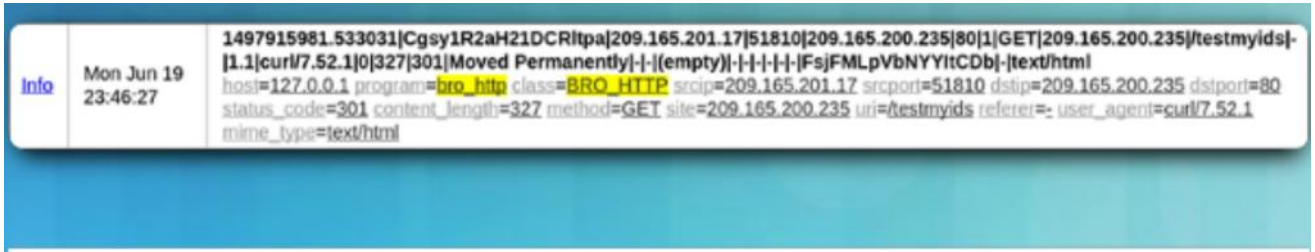
Data Reduction

- Data reduction is the identification of data that should be gathered and stored to reduce the burden on systems.
- By limiting the volume of data, tools like ELSA will be far more useful.



Data Normalization

- Data normalization is the process of combining data from a number of sources into a common format for indexing and searching.



Bro Log Format Fields	Normalized and Labelled ELSA Log Format Fields
1497915981.533031	Mon Jun 19 23:46:27
|209.165.201.17|51810|209.165.200.235|80|	srcip=209.165.201.17 srcport=51810 dstip=209.165.200.235 dstport=80
|327|301|	status_code=301 content_length=327
|GET|209.165.200.235|/testmyids|	method=GET site=209.165.200.235 uri=/testmyids

Data Archiving

- Retaining NSM data indefinitely is not feasible due to storage and access issues.
- Compliance frameworks may require storage of data for a specified period of time.
- ELSA can be configured to retain data for a period of time. The default is 90 days.
- Sguil alert data is retained for 30 days by default.

Lab – Convert Data Into a Universal Format

Networking Academy

Lab - Convert Data into a Universal Format

Objectives

Part 1: Normalize Timestamps in a Log File

Part 2: Normalize Timestamps in an Apache Log File

Part 3: Log File Preparation in Security Onion

Background / Scenario

Log entries are generated by network devices, operating systems, applications, and various types of programmable devices. A file containing a time-sequenced stream of log entries is called a *log file*.

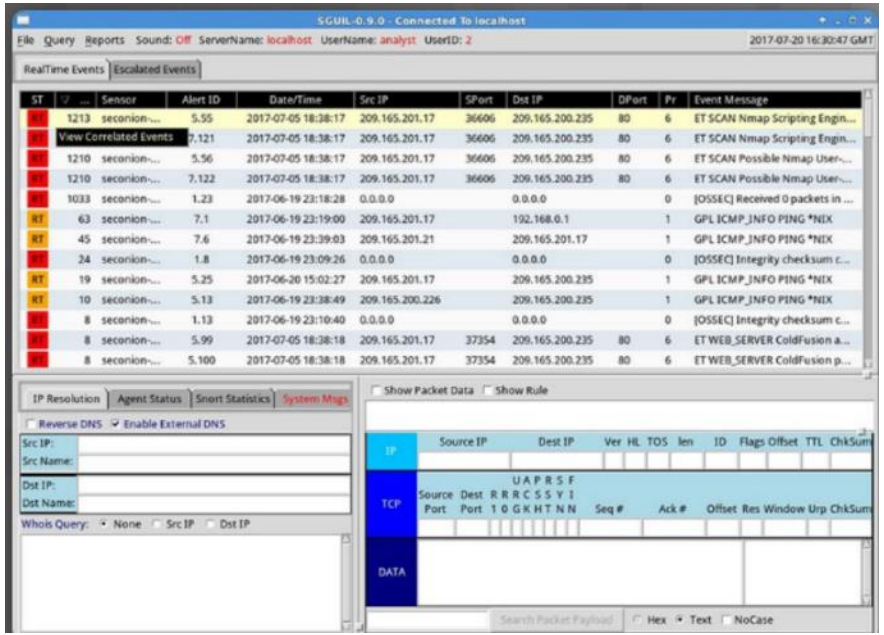
By nature, log files record events that are relevant to the source. The syntax and format of data within log messages are often defined by the application developer.

Therefore, the terminology used in the log entries often varies from source to source. For example, depending on the source, the terms login, logon, authentication event, and user connection, may all appear in log entries to describe a successful user authentication to a server.

It is often desirable to have a consistent and uniform terminology in logs generated by different sources. This is especially true when all log files are being collected by a centralized point.

The term *normalization* refers to the process of converting parts of a message, in this case a log entry, to a common format.

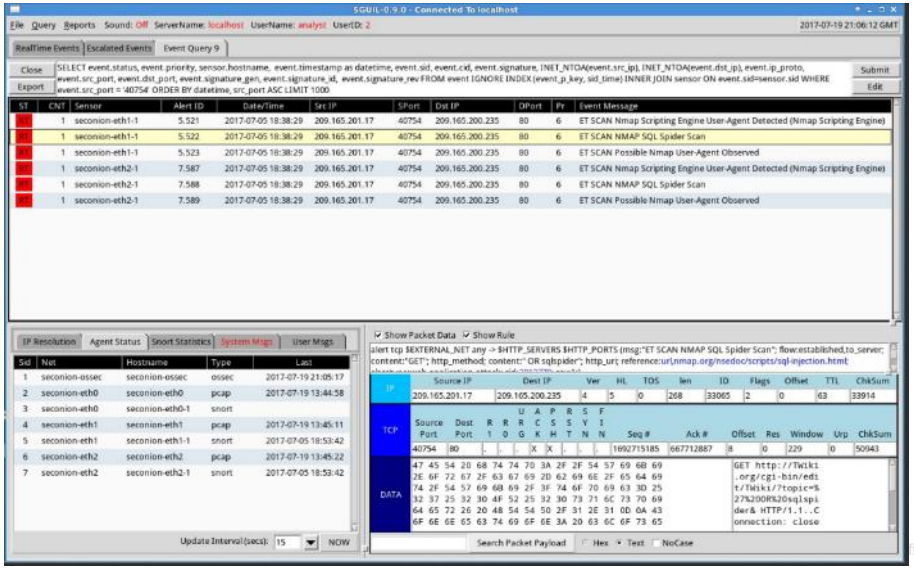
Working in Sguil



- In Security Onion, the first place that a cybersecurity analyst will go to verify alerts is Sguil.
- Sguil automatically correlates similar alerts into a single line and provides a way to view correlated events represented by that line.

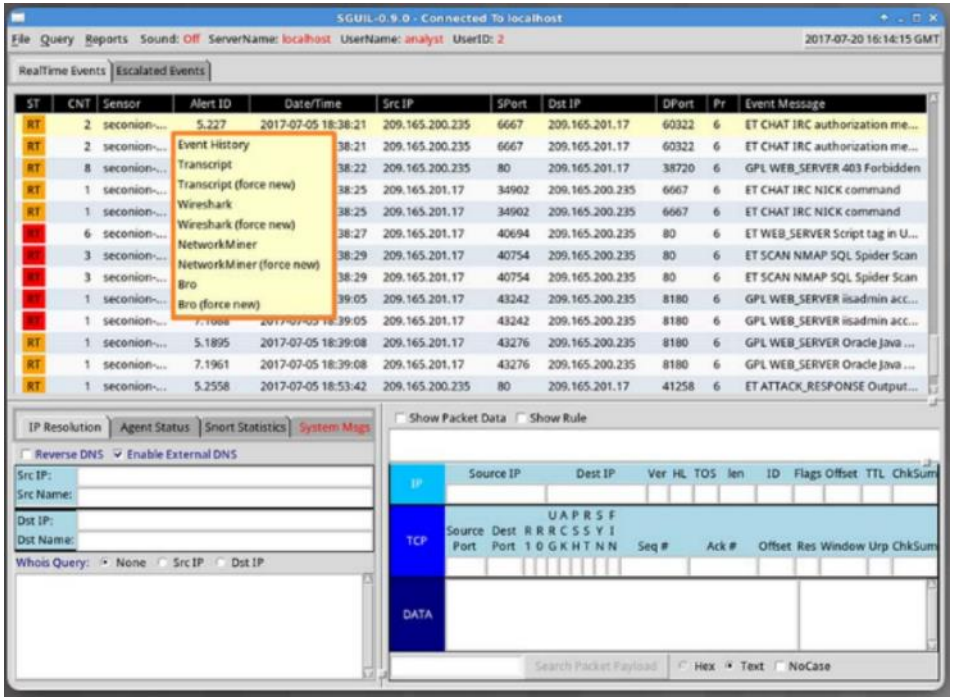
Sguil Queries

- Queries can be constructed in Sguil using the Query Builder, which simplifies constructing queries.
- Cybersecurity analyst must know the field names and some issues with field values.

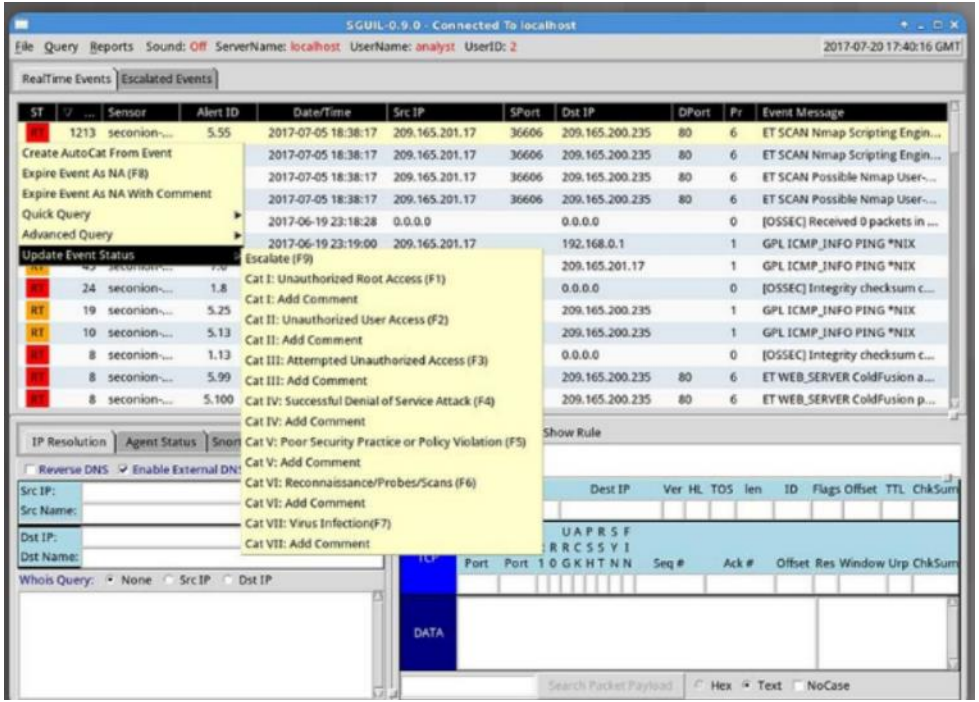


Pivoting from Sguil

- Sguil provides the ability to “pivot” the investigation to other tools such as ELSA, Wireshark, or Bro.
- Log files are available in ELSA, relevant packet captures can be displayed in Wireshark, and transcripts of TCP sessions and Bro information are also available.



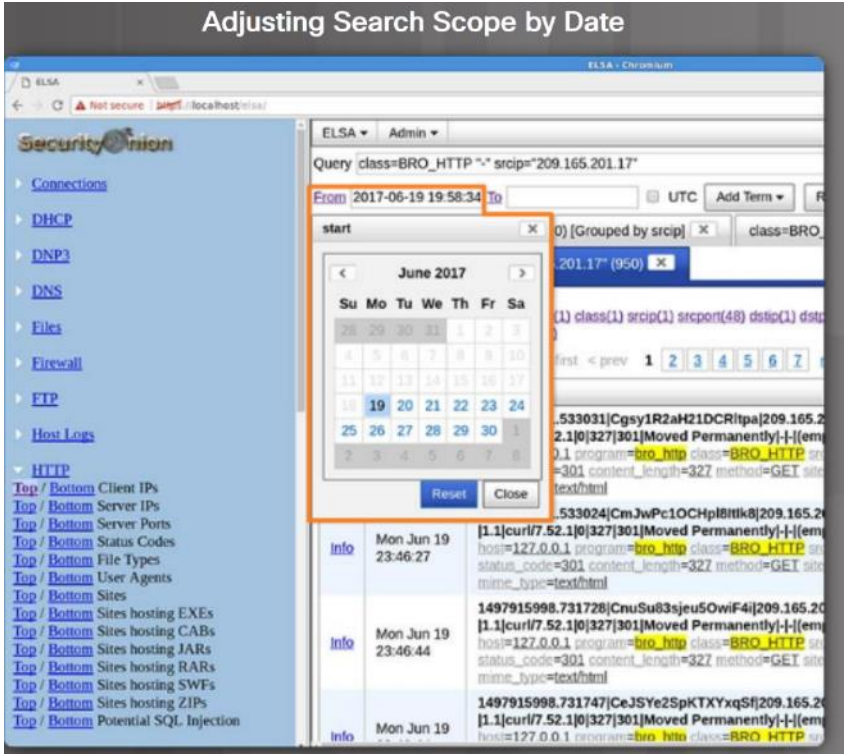
Event Handling in Sguil



- Three tasks can be completed in Sguil to manage alerts.
  - Alerts that have been found to be false positives can be expired.
  - An event can be escalated by pressing the F9 key.
  - An event can be categorized.

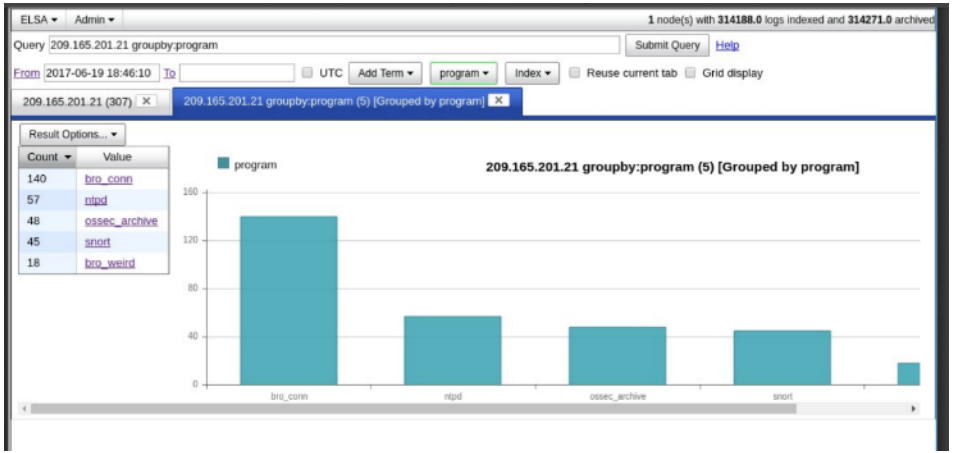
Working in ELSA

- ELSA provides access to a large number of log file entries.
- ELSA will only retrieve the first 100 records for the previous 48 hours.
- The easiest way to see information in ELSA is to issue the built-in queries that appear to the left of the ELSA window and then adjust the dates and resubmit the query using the Submit Query button.

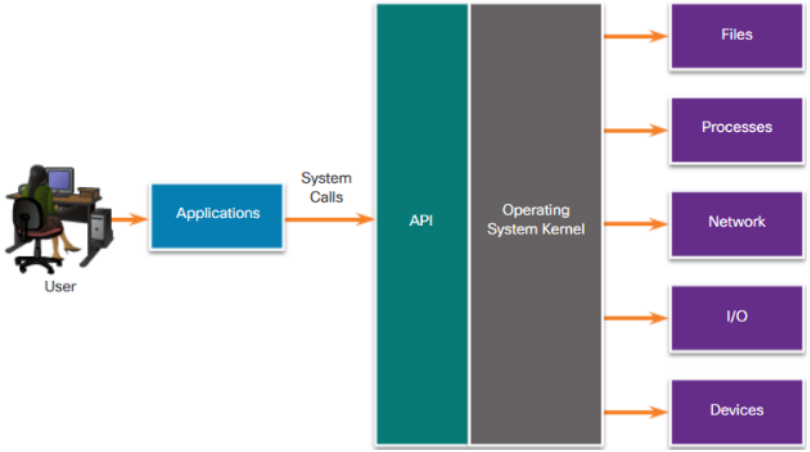


Queries in ELSA

- ELSA provides field summary and value information for every field that is indexed in the query results. This permits refining queries based on a wide range of values.
- Clicking an entry in the Value column will display the query with the value added to the previous query. This process can be repeated to narrow down search results easily.
- Regular expressions are executed in ELSA using the grep function.



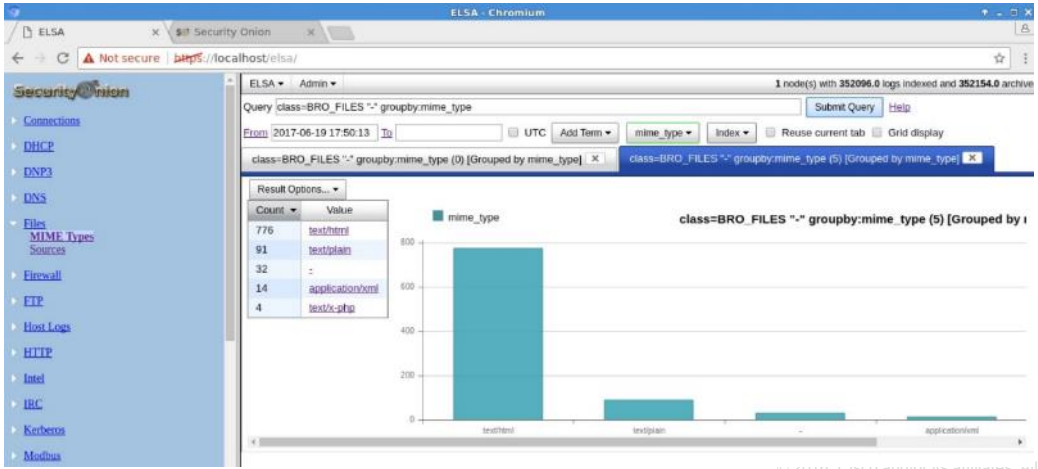
Investigating Process or API Calls



- If malware can fool an OS kernel into allowing it to make system calls, many exploits are possible.
- OSSEC rules detect changes in host-based parameters like the execution of software processes, changes in user privileges, and registry modifications, among others.
- OSSEC rules will trigger an alert in Sguil.
- Choosing OSSEC as the source program in ELSA results in a view of the OSSEC events that occurred on the host.

Investigating File Details

- When ELSA is opened directly, a query short cut exists for Files.
- Opening the Files queries and selecting Mime Types in the menu displays a list of the types of files that have been downloaded.
- MD5 and SHA-1 hashes for downloaded files are also available.
- File hash values can be submitted to online sites to determine if the file is known malware.



Lab – Regular Expression Tutorial

Networking Academy

Lab – Regular Expression Tutorial

Objectives

In this lab, you will learn how to use regular expressions to search for desired strings of information.

Background / Scenario

A regular expression (regex) is a pattern of symbols that describes data to be matched in a query or other operation. Regular expressions are constructed similarly to arithmetic expressions, by using various operators to combine smaller expressions. There are two major standards of regular expression, POSIX and Perl.

In this lab, you will use an online tutorial to explore regular expressions. You will also describe the information that matches given regular expressions.

Required Resources

- CyberOps Workstation VM
- Internet connection

Step 1: Complete the regexone.com tutorial.

a. Open a web browser and navigate to https://regexone.com/. Regex One is a tutorial that provides you with lessons to learn about regular expression patterns.

Lab – Extract an Executable from a PCAP

Networking Academy

Lab – Extract an Executable from a PCAP

Objectives

Part 1: Prepare the Virtual Environment

Part 2: Analyze Pre-Captured Logs and Traffic Captures

Background / Scenario

Looking at logs is very important but it is also important to understand how network transactions happen at the packet level.

In this lab, you will analyze the traffic in a previously captured pcap file and extract an executable from the file.

Required Resources

- CyberOps Workstation VM
- Internet connection

Part 1: Prepare the Virtual Environment

a. Launch Oracle VirtualBox. Right-click CyberOps Workstion > Settings > Network. Besides **Attached To**, select **Bridged Adapter**, if necessary, and click **OK**.

Dashboards and Visualizations

- Dashboards provide an interactive combination of data and visualizations designed to improve the value of large amounts of information.
- Allow analysts to focus on specific details and information
- ELSA capable of designing custom dashboards
- Squert provides a visual interface
- Cisco Talos provides an interactive dashboard

Workflow Management

- Network security monitoring requires workflows to be managed.
  - Enhances efficiency of the cyberoperations team
  - Increases the accountability of staff
  - Ensures that all potential alerts are treated properly
  - Each alert should be systematically assigned, processed, and documented
- Sguil provides basic workflow management but not a good choice for large operations, third party systems are available that can be customized
- Automated queries add efficiency to workflow
  - Search for complex security incidents that may evade other tools
  - ELSA query can be configured as an alert rule and run regularly
  - Can be created in a scripting language such as Python

12.3 Digital Forensics

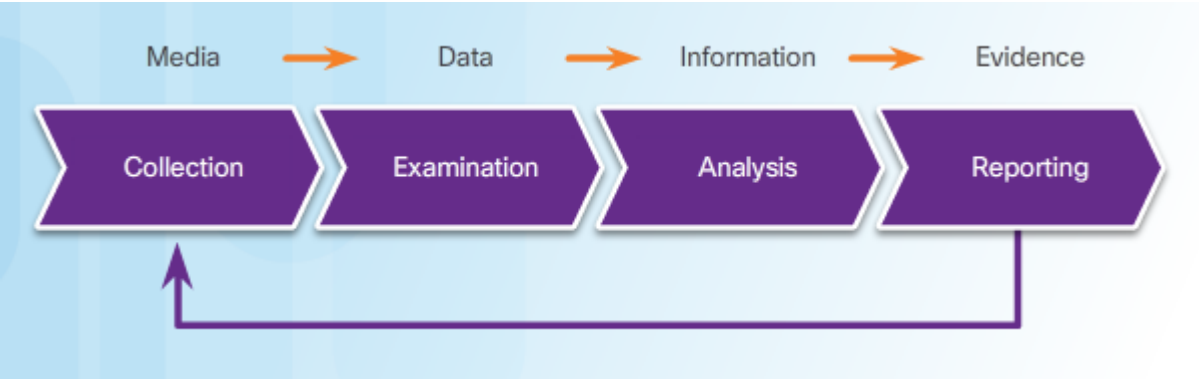
Digital Forensics

- Cybersecurity analyst will uncover evidence of criminal activity.
  - Must identify threat actors, report them to the appropriate authorities, and provide evidence to support prosecution.
  - Usually first to uncover wrong doing.
- Digital forensics is the recovery and investigation of information found on digital devices as it relates to criminal activity.
  - Could be data on storage devices, in volatile computer memory, or traces of cybercrime in network data such as pcaps and logs
- Cybercriminal activity can be characterized as origination from inside or outside of the organization.
- Under HIPAA, notification of breach must be made to the affected individuals.
- Analysts must know the requirements regarding the preservation and handling of evidence.

The Digital Forensics Process

- NIST describes the digital forensics process as involving four steps:

1. Collection – Identification of potential sources of forensic data and acquisition, handling, and storage of that data.
2. Examination – Assessing and extracting relevant information from the collected data. May involve decompression and decryption.
3. Analysis – Drawing conclusions from the data. (People, places, time, events, etc.)
4. Reporting – Preparing and presenting information. Suggestions for further investigation and next steps should be made.



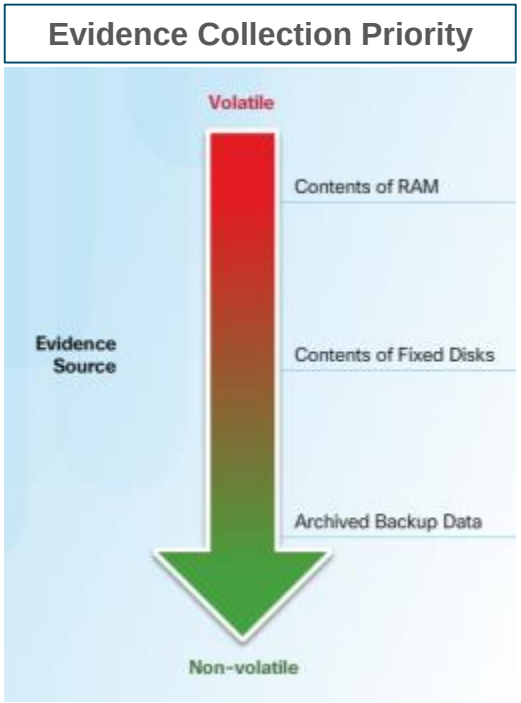
Types of Evidence

- In legal proceedings, evidence is broadly classified:
  - **Direct evidence** was indisputably in the possession of the accused, or is eyewitness evidence from someone who observed criminal behavior.
  - **Best evidence** is evidence that is in its original state.
  - **Corroborating evidence** supports an assertion that is developed from best evidence.
  - **Indirect evidence**, in combination with other facts, establishes a hypothesis. Also know as circumstantial evidence.

Evidence Collection Order

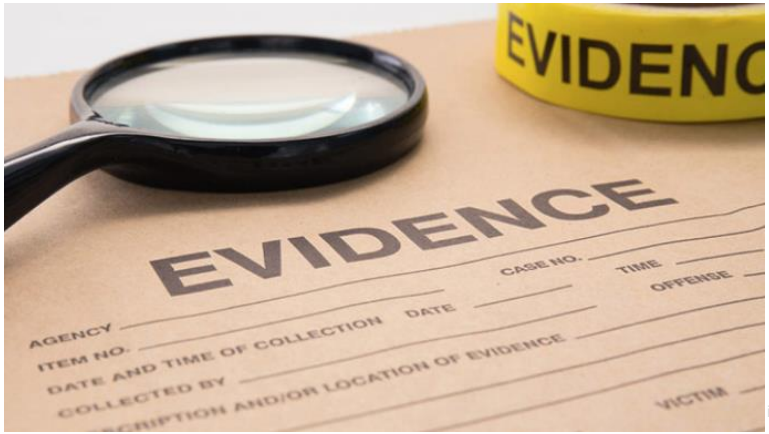
- Collection of digital evidence should begin in order from the most volatile evidence and proceed to the least volatile.
  - Data in RAM is most volatile.
- Example most volatile to least volatile:

1. Memory registers, caches
2. Routing table, ARP cache, process table, kernel statistics, RAM
3. Temporary files systems
4. Non-volatile media, fixed and removable
5. Remote logging and monitoring data
6. Physical interconnections and topologies
7. Archival media, tape or other backups



Chain of Custody

- Chain of custody involves the collection, handling, and secure storage of evidence.
  - Who discovered the evidence.
  - All details about the handling of evidence including times, places, and personnel involved.
  - Who has primary responsibility for the evidence, when responsibility was assigned, and when custody changed.
  - Who has physical access to the evidence while it was stored? Access should be restricted to only the most essential personnel.



Data Integrity and Preservation

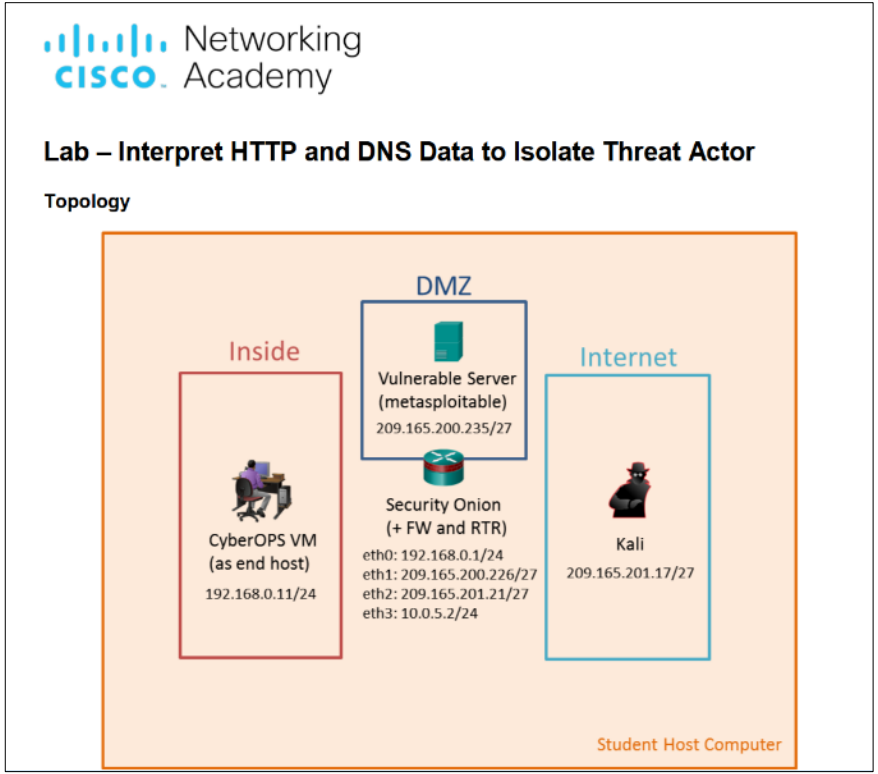
- Digital evidence should be preserved in its original condition.
  - Original evidence should be copied, and analysis should only be conducted on copies.
  - Timestamps may be part of evidence so opening files from the original media should be avoided.
- Process used to create copies of evidence should be recorded.
- Special tools should be used to preserve forensic evidence before the device is shut down and evidence is lost.
- Users should not disconnect, unplug, or turn off infected machine unless told to by security personnel.

Attack Attribution

- Threat attribution is the act of determining the individual, organization, or nation responsible for a successful intrusion or attack incident.
- Identification of threat actors should occur through principled and systematic investigation of evidence.
- In an evidence-based investigation, the incident response team correlates the tactics, techniques, and procedures (TPP) that were used in the incident with other known exploits to identify threat actors.
- Aspects of a threat that can aid in attribution are the location of originating hosts or domains, features of the codes used in malware, the tools used, and other techniques.

12.4 Chapter Summary

Lab – Interpret HTTP and DNS Data to Isolate Threat Actor

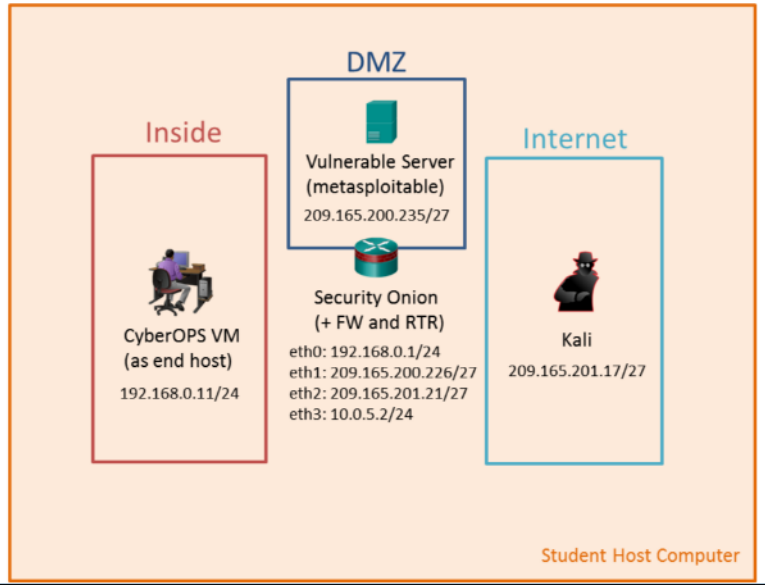


Lab – Isolate Compromised Host Using 5-Tuple

Networking Academy

Lab – Isolated Compromised Host Using 5-Tuple

Topology



Summary

- Security Onion provides an integrated NSM environment for investigating security events that are created by diverse systems.
- A Tier 1 cybersecurity analyst evaluates security alerts to verify whether actual security incidents have occurred.
- ELSA provides a common data platform for the aggregation of log files from many sources.
- Sguil provides an analyst's console that enables the investigation of alerts through pivots to other tools.
- Tier 1 analysts may discover illegal activity on the network and be required to handle, preserve, and analyze digital forensic evidence.
- Digital forensic evidence can lead to the attribution of cybersecurity events to threat actors.

New Terms and Commands

- Attack attribution
- Best evidence
- CapME
- chain of custody
- Corroborating evidence
- Dashboard
- Data normalization
- Deterministic analysis
- Digital Forensics
- ELSA
- False Negative
- False Positive
- Indirect evidence
- OSSEC
- Probabilistic analysis
- Suricata
- True Negative
- True Positive

Cybersecurity Operations Certification

- This chapter covers the following areas in the Cybersecurity Operations Certification:
- From 210-250 SECFND - Understanding Cisco Cybersecurity Fundamentals:
- **Domain 5: Security Monitoring**
  - 5.2 Describe the following types of data used in security monitoring:
    - Full packet capture
    - Session Data
    - Transaction Data
    - Statistical Data
    - Extracted content
    - Alert Data

Cybersecurity Operations Certification

- This chapter covers the following areas in the Cybersecurity Operations Certification:
- From 210-255 SECFND - Implementing Cisco Cybersecurity Operation:
- **Domain 2: Network Intrusion Analysis**
  - 2.8 Compare and contrast impact and no impact for the following:
    - False Positive
    - False Negative
    - True Positive
    - True Negative
- **Domain 4: Data and Event Analysis**
  - 4.1 Describe the process of data normalization
  - 4.2 Interpret common data values into a universal format
  - 4.3 Describe 5-tuple correlation
  - 4.4 Apply the 5-tuple approach to isolate a compromised host in a grouped set of logs

Cybersecurity Operations Certification

- This chapter covers the following areas in the Cybersecurity Operations Certification:
- From 210-255 SECFND - Implementing Cisco Cybersecurity Operation:
- **Domain 4: Data and Event Analysis**
  - 4.1 Describe the process of data normalization
  - 4.2 Interpret common data values into a universal format
  - 4.3 Describe 5-tuple correlation
  - 4.4 Apply the 5-tuple approach to isolate a compromised host in a grouped set of logs
  - 4.9 Compare and contrast deterministic and probabilistic analysis

Cybersecurity Operations Certification

- This chapter covers the following areas in the Cybersecurity Operations Certification:
- From 210-255 SECFND - Implementing Cisco Cybersecurity Operation:
- **Domain 5: Incident Handling**
  - 5.2 Apply the NIST.SP800-61 r2 incident handling process to an event
  - 5.3 Define the following activities as they relate to incident handling:
    - Identification
    - Scoping
    - Containment
    - Remediation
    - Lessons based hardening
    - Reporting

Cybersecurity Operations Certification

- This chapter covers the following areas in the Cybersecurity Operations Certification:
- From 210-255 SECFND - Implementing Cisco Cybersecurity Operation:
- **Domain 5: Incident Handling**
  - 5.4 Describe the following concepts as they are documented in NIST SP800-86:
    - Evidence collection order
    - Data integrity
    - Data preservation
    - Volatile data collection


CISCO