

Information Security Operations Center

Prepared by
Dr. Ibrahim Gomaa

جامعة الجميع الذكية

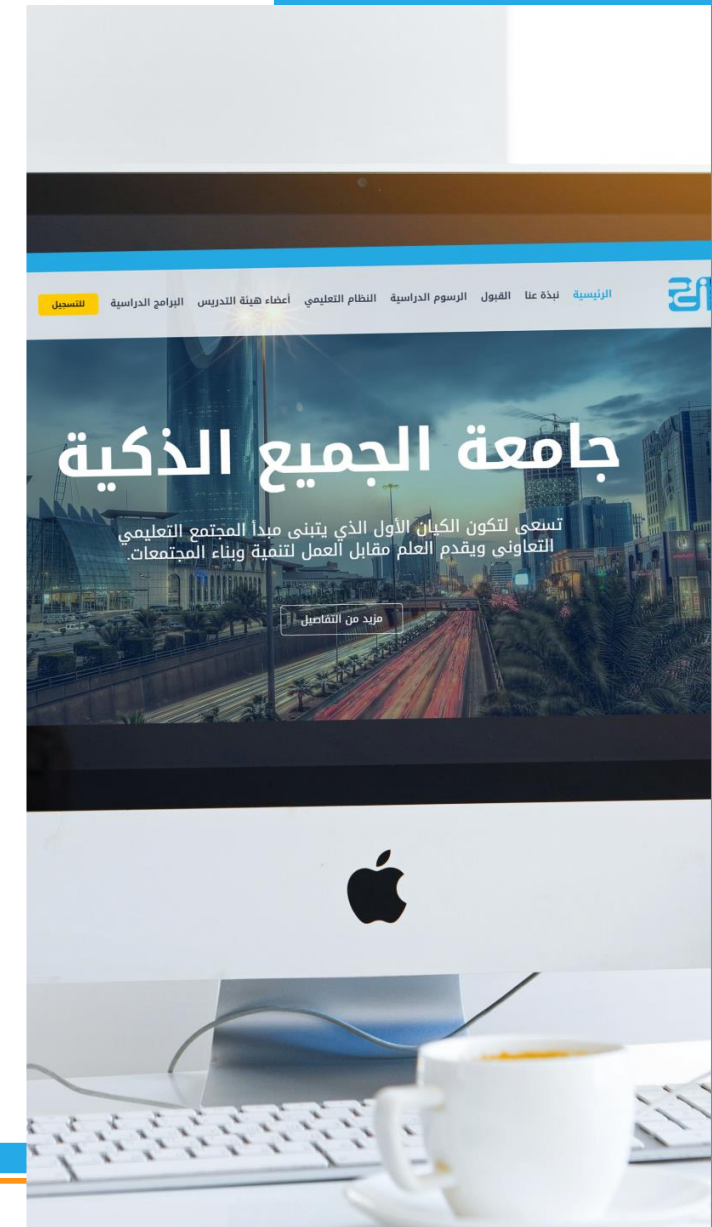
تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

Lecture 9: Analyze network intrusion data to
identify compromised hosts and vulnerabilities



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

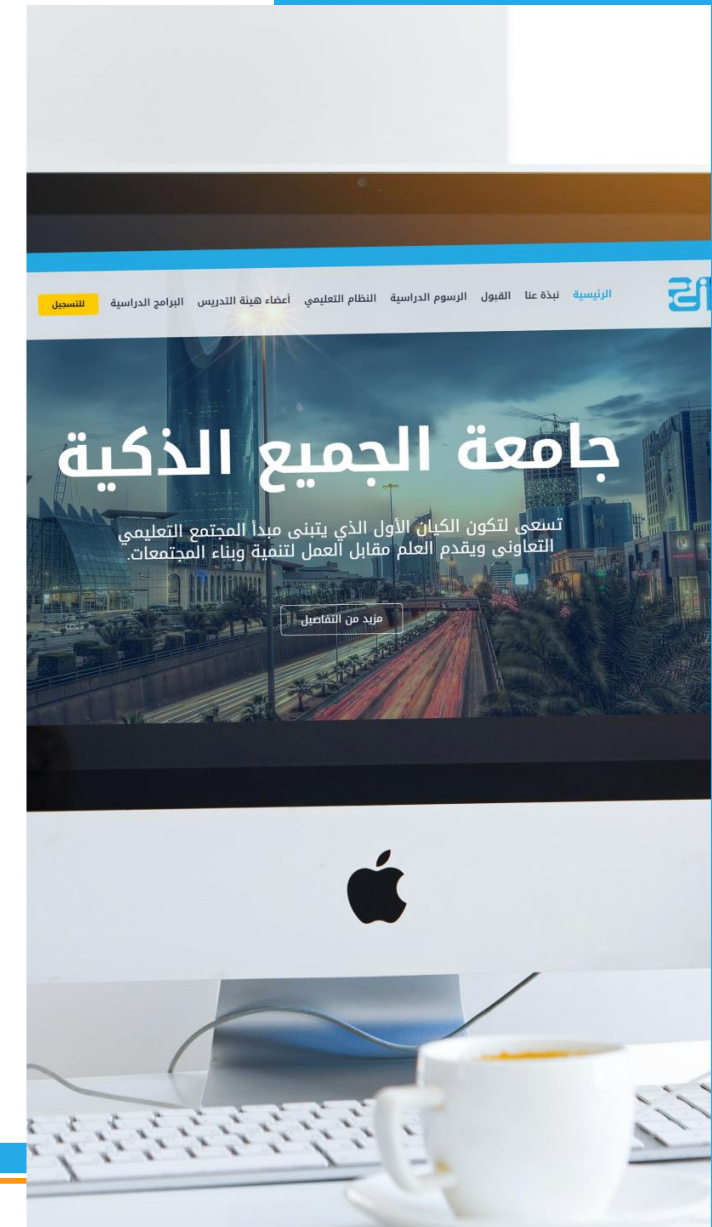
Topic Title	Topic Objective
A Common Data Platform	Explain how data is prepared for use in a Network Security Monitoring (NSM) system.
Investigating Network Data	Use Security Onion tools to investigate network security events.
Enhancing the Work of the CyberSecurity Analyst	Describe network monitoring tools that enhance workflow management.



Lecture – 9

Analyze network intrusion data to identify compromised hosts and vulnerabilities

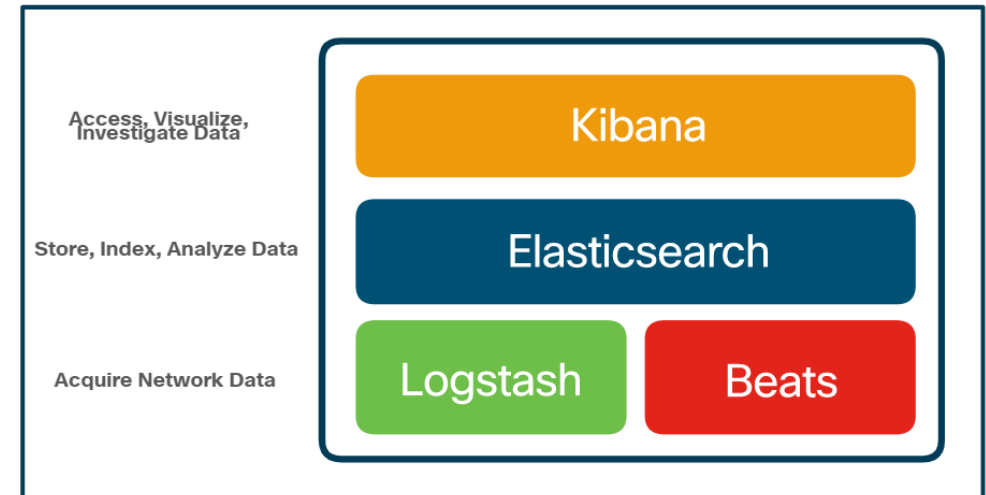
A Common Data Platform



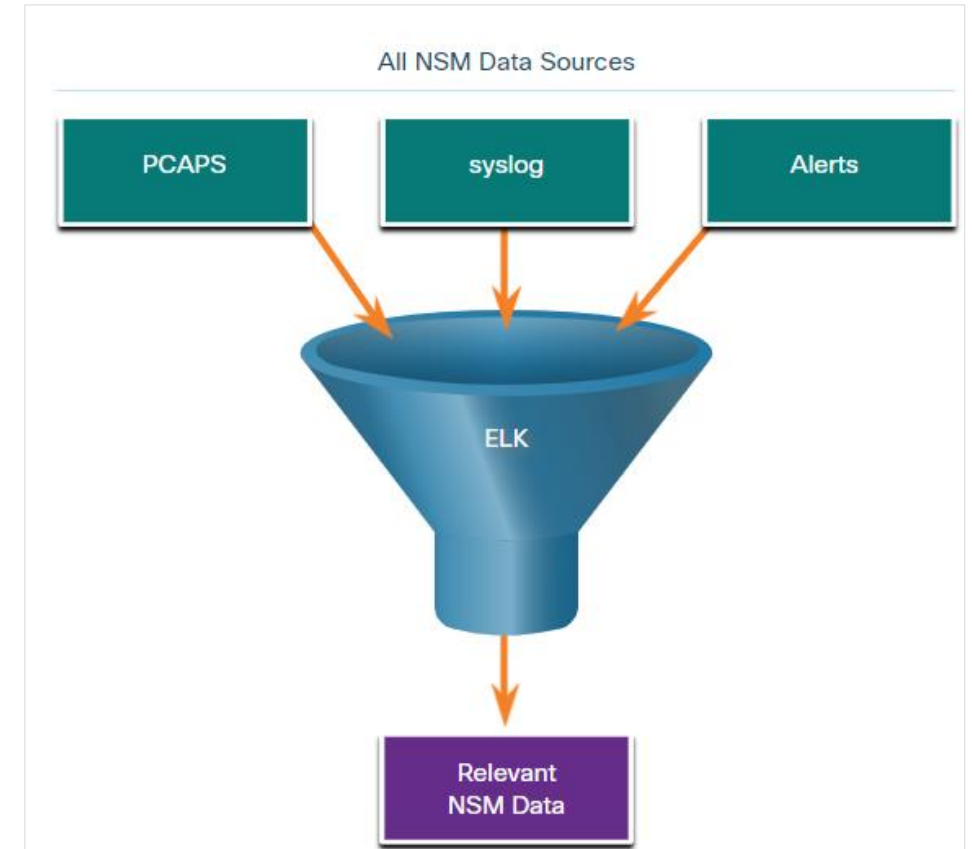
Security Onion includes [Elastic Stack](#) that consists of Elasticsearch, Logstash, and Kibana ([ELK](#)).

Core Components of ELK:

- **Elasticsearch**: An open-core platform for searching and analyzing an organization's data in near real time.
- **Logstash**: Enables collection and normalization of network data into data indexes that can be efficiently searched by Elasticsearch.
- **Kibana**: Provides a graphical interface to data that is compiled by Elasticsearch.
- **Beats**: Series of software plugins that send different types of data to the Elasticsearch data stores.



- To reduce data, it is essential to identify the network data that should be gathered and stored to reduce the burden on systems.
- By limiting the volume of data, tools like [Elasticsearch](#) will be far more useful.



Data Normalization

- **Data normalization** is the process of combining data from a number of sources into a common format.
- A common schema will specify the names and formats for the required data fields.
- For example, IPv6 addresses, MAC addresses, and date and time can be represented in varying formats:

IPv6 Address Formats	Mac Formats	Date Formats
2001:db8:acad:1111:2222::33	A7:03:DB:7C:91:AA	Monday, July 24, 2017 7:39:35pm
2001:DB8:ACAD:1111:2222::33	A7-03-DB-7C-91-AA	Mon, 24 Jul 2017 19:39:35 +0000
2001:DB8:ACAD:1111:2222:0:0:33	A70.3DB.7C9.1AA	2017-07-24T19:39:35+00:00

- Data normalization is also required to simplify searching for correlated events.

Data Normalization

- **Data normalization** is the process of combining data from a number of sources into a common format.
- A common schema will specify the names and formats for the required data fields.
- For example, IPv6 addresses, MAC addresses, and date and time can be represented in varying formats:

IPv6 Address Formats	Mac Formats	Date Formats
2001:db8:acad:1111:2222::33	A7:03:DB:7C:91:AA	Monday, July 24, 2017 7:39:35pm
2001:DB8:ACAD:1111:2222::33	A7-03-DB-7C-91-AA	Mon, 24 Jul 2017 19:39:35 +0000
2001:DB8:ACAD:1111:2222:0:0:33	A70.3DB.7C9.1AA	2017-07-24T19:39:35+00:00

- Data normalization is also required to simplify searching for correlated events.

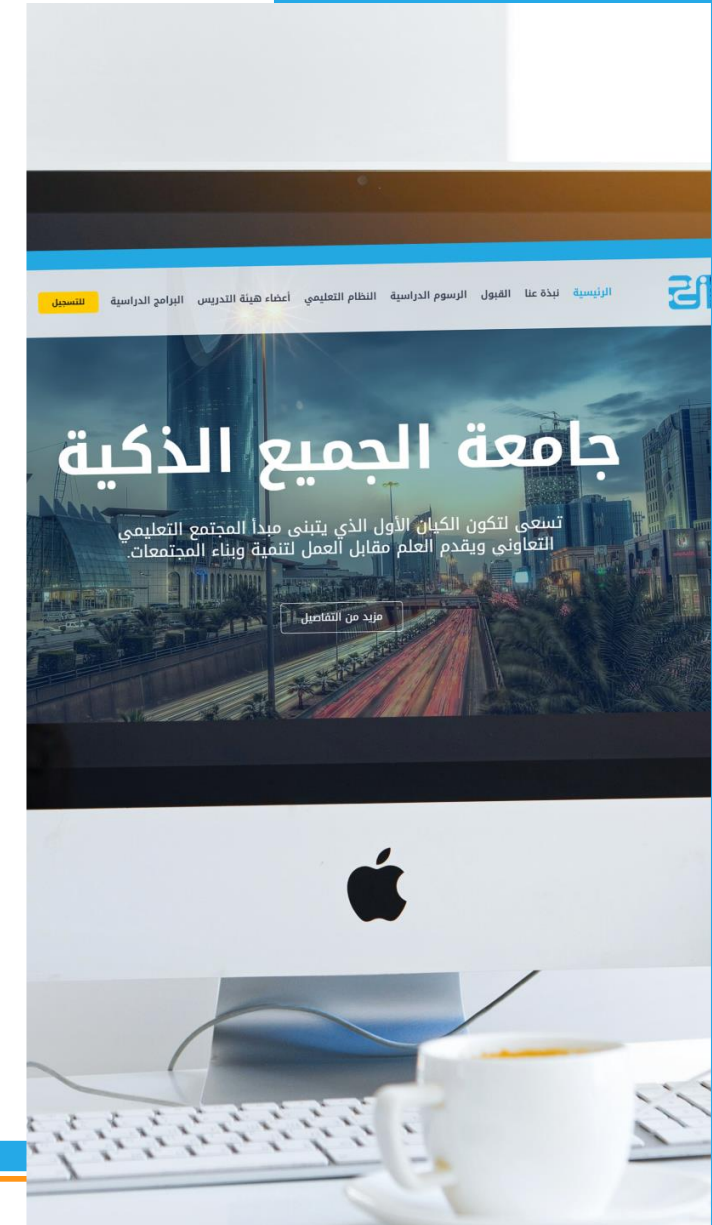
Lecture – 9

Activity 1

Lab - Convert Data into a Universal Format

In this lab, you will complete the following objectives:

- **Part 1:** Use command line tools to manually normalize log entries.
- **Part 2:** The timestamp field must be normalized.



Data Archiving

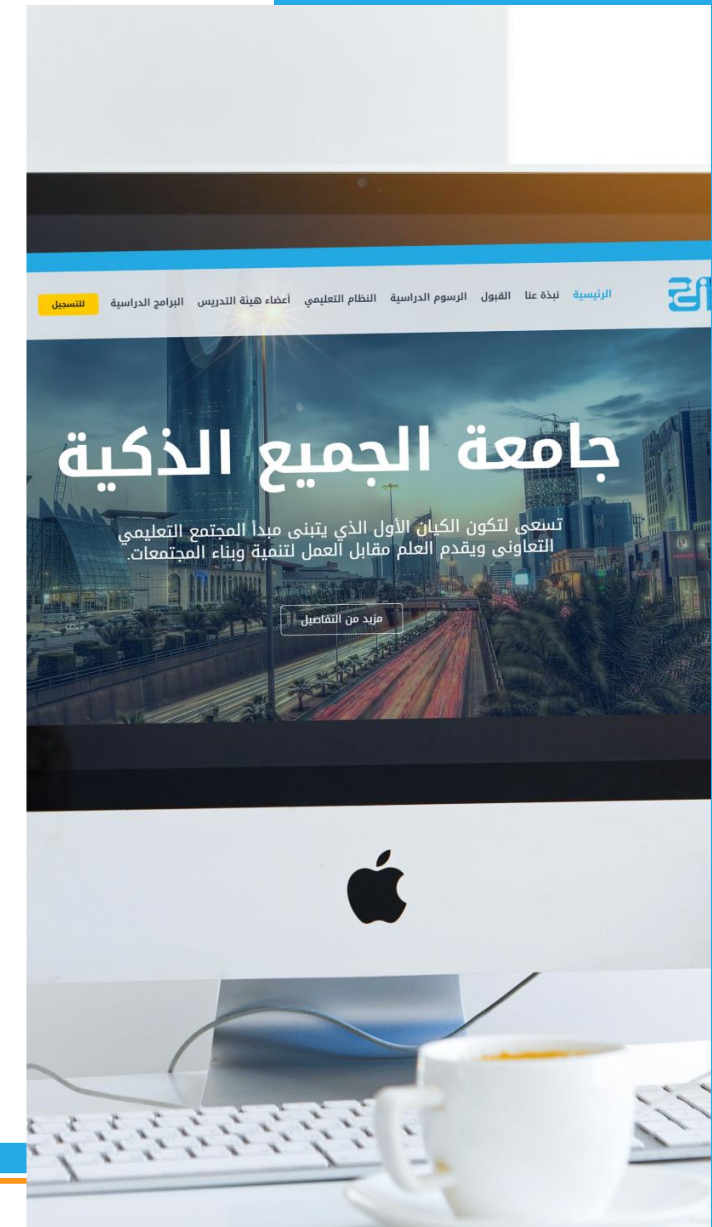
- Retaining Network Security Monitoring (NSM) data indefinitely is not feasible due to storage and access issues.
- The retention period for certain types of network security information may be specified by compliance frameworks.
- Sguil alert data is retained for 30 days by default. This value is set in the **securityonion.conf** file.
- Security Onion data can always be archived to external storage by a data archive system, depending on the needs and capabilities of the organization.

Note: The storage locations for the different types of Security Onion data will vary based on the Security Onion implementation.

Lecture – 9

Analyze network intrusion data to identify compromised hosts and vulnerabilities

Investigating Network Data



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.
- To understand what is happening in the network, it may be useful to sort the **CNT** column to display the alerts with the highest frequency.

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2 2020-05-29 20:06:11 GMT

RealTime Events Escalated Events 7.1998 Event Query 1

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1059	seconion...	1.3	2020-04-29 15:26:36	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 packets in designated time interval (defined in os...
RT	881	seconion...	1.2	2020-04-29 15:22:36	0.0.0.0		0.0.0.0		0	[OSSEC] Listened ports status (netstat) changed (new port opened or c...
RT	647	seconion...	7.1	2020-04-29 16:08:59	209.165.201.17		209.165.201.21		1	GPL ICMP_INFO PING *NIX
RT	View Correlated Events		5.1	2020-04-29 16:55:12	209.165.201.17		209.165.200.235		1	GPL ICMP_INFO PING *NIX
RT	296	seconion...	5.792	2020-05-10 21:20:28	209.165.201.17	52206	209.165.200.235	80	6	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Atte...
RT	296	seconion...	7.1105	2020-05-10 21:20:28	209.165.201.17	52206	209.165.200.235	80	6	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Atte...
RT	252	seconion...	3.1	2020-04-29 16:44:19	192.168.0.11		192.168.0.1		1	GPL ICMP_INFO PING *NIX
RT	123	seconion...	5.466	2020-05-10 21:20:26	209.165.201.17	52174	209.165.200.235	80	6	ET WEB_SERVER Possible CVE-2014-6271 Attempt
RT	123	seconion...	5.467	2020-05-10 21:20:26	209.165.201.17	52174	209.165.200.235	80	6	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers
RT	123	seconion...	7.779	2020-05-10 21:20:26	209.165.201.17	52174	209.165.200.235	80	6	ET WEB_SERVER Possible CVE-2014-6271 Attempt
RT	123	seconion...	7.780	2020-05-10 21:20:26	209.165.201.17	52174	209.165.200.235	80	6	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers
RT	76	seconion...	7.691	2020-05-10 21:20:25	209.165.201.17	52158	209.165.200.235	80	6	ET INFO Executable Download from dotted-quad Host
RT	76	seconion...	5.378	2020-05-10 21:20:25	209.165.201.17	52158	209.165.200.235	80	6	ET INFO Executable Download from dotted-quad Host
RT	66	seconion...	7.1672	2020-05-10 21:20:42	209.165.201.17	52206	209.165.200.235	80	6	ET WEB_SERVER Executable Connected D4D Injection Attack (remote)

IP Resolution Agent Status Snort Statistics System Msgs User Msgs

☐ Reverse DNS ☒ Enable External DNS

Src IP:

Src Name:

Dst IP:

Dst Name:

Whois Query: ☐ None ☐ Src IP ☐ Dst IP

☒ Show Packet Data ☒ Show Rule

alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"GPL ICMP_INFO PING *NIX", rtype:8, content:"10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F", depth:32, classtype:misc-activity, sid:2100366, rev:8, metadata:created_at 2010_09_23,

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
ICMP	209.165.201.17	209.165.201.21	4	5	0	84	13326	2	0	64	53544
	Type	Code	ChkSum	ID	Seq #						
	8	0	23684	1110	1						
DATA	<pre> 03 A5 A9 5E 00 00 00 24 4E 07 00 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 01234567 </pre>										

Search Packet Payload ☐ Hex ☐ Text ☐ NoCase

Sguil Alerts Sorted on CNT

Sguil Queries

- Queries can be constructed in Sguil using the **Query Builder**. It simplifies constructing queries to a certain degree.
- **Cybersecurity analyst** must know the field names and some issues with field values to effectively build queries in Sguil.
- For example, Sguil stores IP addresses in an integer representation.

The screenshot displays the Sguil 0.9.0 interface. The top section shows a query result table with columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. The bottom section shows a packet capture view with a table of IP addresses and a detailed view of a packet (Source IP: 209.165.201.17, Dest IP: 209.165.200.235, Ver: 4, HL: 5, TOS: 0, Len: 268, ID: 33065, Flags: 2, Offset: 0, TTL: 63, ChkSum: 33914).

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
1	1	seconion-eth1-1	5.521	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
1	1	seconion-eth1-1	5.522	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Nmap SQL Spider Scan
1	1	seconion-eth1-1	5.523	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Possible Nmap User-Agent Observed
1	1	seconion-eth2-1	7.587	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
1	1	seconion-eth2-1	7.588	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Nmap SQL Spider Scan
1	1	seconion-eth2-1	7.589	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Possible Nmap User-Agent Observed

Sid	Net	Hostname	Type	Last
1	seconion-sssec	seconion-sssec	ossec	2017-07-19 21:05:17
2	seconion-eth0	seconion-eth0	pcap	2017-07-19 13:44:58
3	seconion-eth0	seconion-eth0-1	snort	
4	seconion-eth1	seconion-eth1	pcap	2017-07-19 13:45:11
5	seconion-eth1	seconion-eth1-1	snort	2017-07-05 18:53:42
6	seconion-eth2	seconion-eth2	pcap	2017-07-19 13:45:22
7	seconion-eth2	seconion-eth2-1	snort	2017-07-05 18:53:42

Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
209.165.201.17	209.165.200.235	4	5	0	268	33065	2	0	63	33914

Source Port	Dest Port	R R R C S S Y I	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
40754	80	 X X	1692715185	667712887	8	0	229	0	50943

Update Interval (secs): 15 NOW

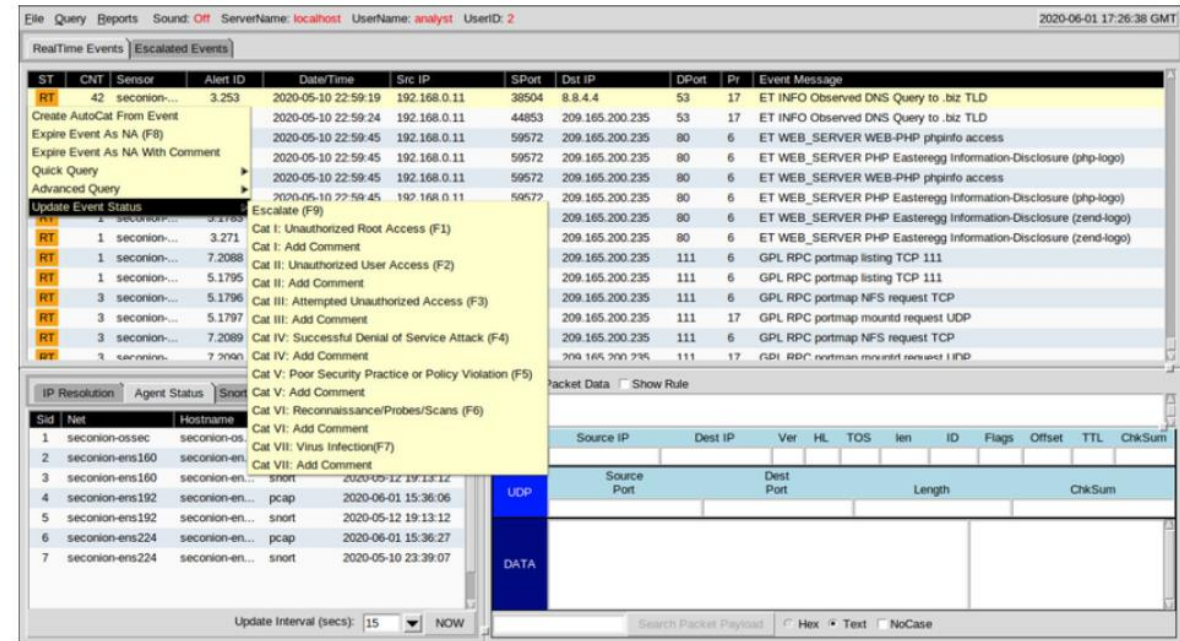
Pivoting from Sguil

- Sguil provides the ability for the **cybersecurity analyst** to pivot to other information sources and tools.
- **Log files** are available in Elasticsearch.
- Relevant packet captures can be displayed in Wireshark.

The screenshot displays the Sguil interface. The top section shows a list of events with columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. A red box highlights the 'Event History' section, which includes 'Transcript', 'Transcript (force new)', 'Wireshark', and 'Wireshark (force new)'. Below this, the 'IP Resolution' section shows a table of IP addresses and their corresponding hostnames. The bottom section shows a packet capture view with columns for IP, Source IP, Dest IP, Ver, HL, TOS, Len, ID, Flags, Offset, TTL, and ChkSum. The packet capture view is currently showing a TCP packet with source port 80 and destination port 80.

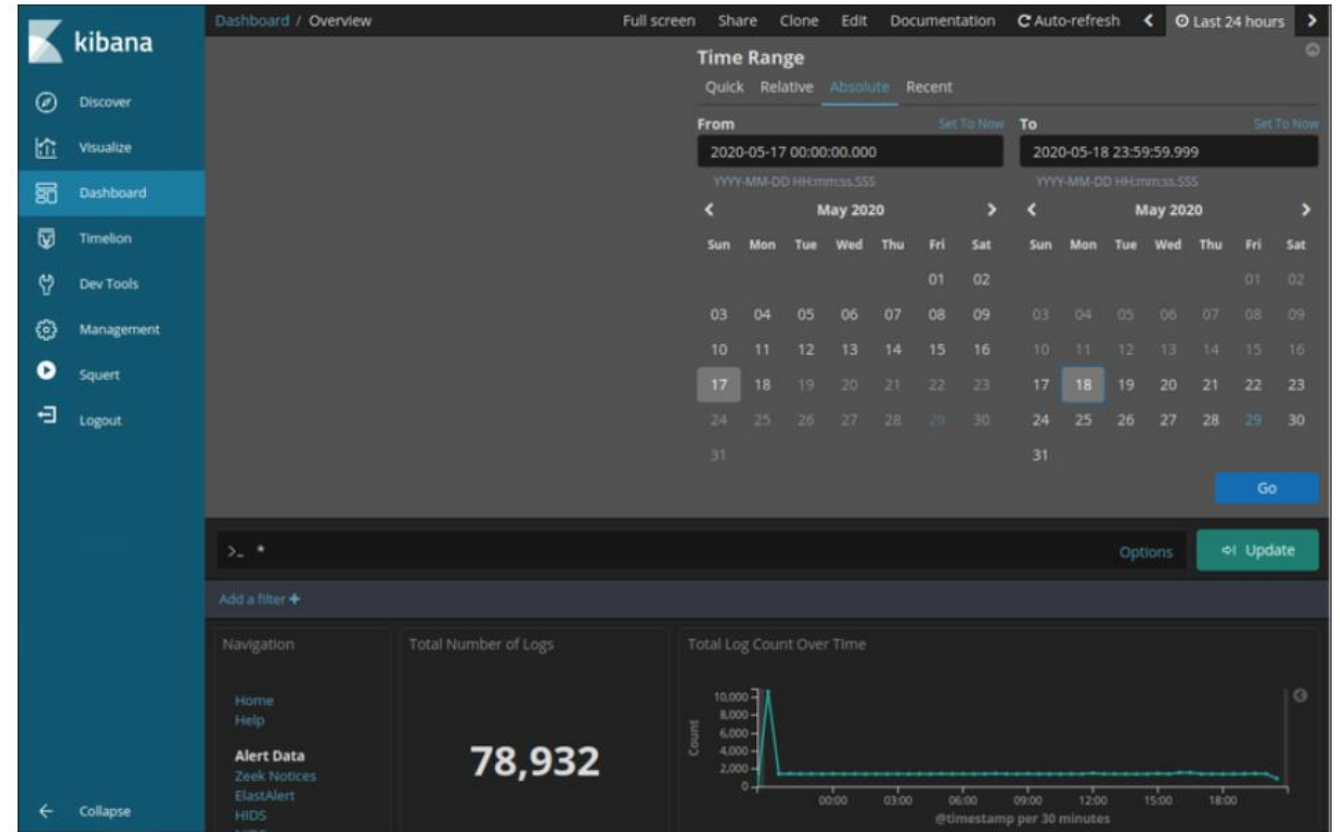
Event Handling in Sguil

- Sguil is a console that enables a cybersecurity analyst to investigate, verify, and classify security alerts.
- 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.



- Sguil includes seven pre-built categories that can be assigned by using a menu or by pressing the corresponding function key.

- **Logstash and Beats** are used for data ingestion in the Elastic Stack.
- Kibana, which is the visual interface into the logs, is configured to show the **last 24 hours** by default.
- Logs are ingested into Elasticsearch into separate indices or databases based on a configured range of time.
- The best way to monitor the data in Elasticsearch is to build customized visual dashboards.

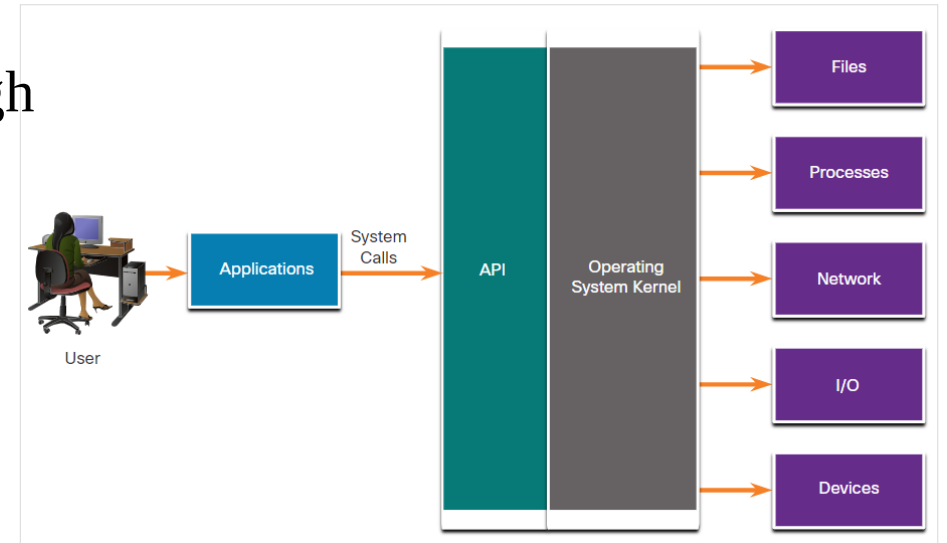


Queries in ELK

- Elasticsearch is built on [Apache Lucene](#), an open-source search engine software library featuring full text indexing and searching capabilities.
- Using Lucene software libraries, Elasticsearch has its own query language based on JSON called [Query Domain Specific Language](#) (QDSL).
- Along with JSON, Elasticsearch queries make use of elements such as Boolean operators, Fields, Ranges, Wildcards, Regex, Fuzzy Search, and Text Search.
- Elasticsearch was designed to interface with users using web-based clients that follow the HTTP REST framework.
- Methods used for executing the queries are URI, cURL, JSON and Dev Tools.

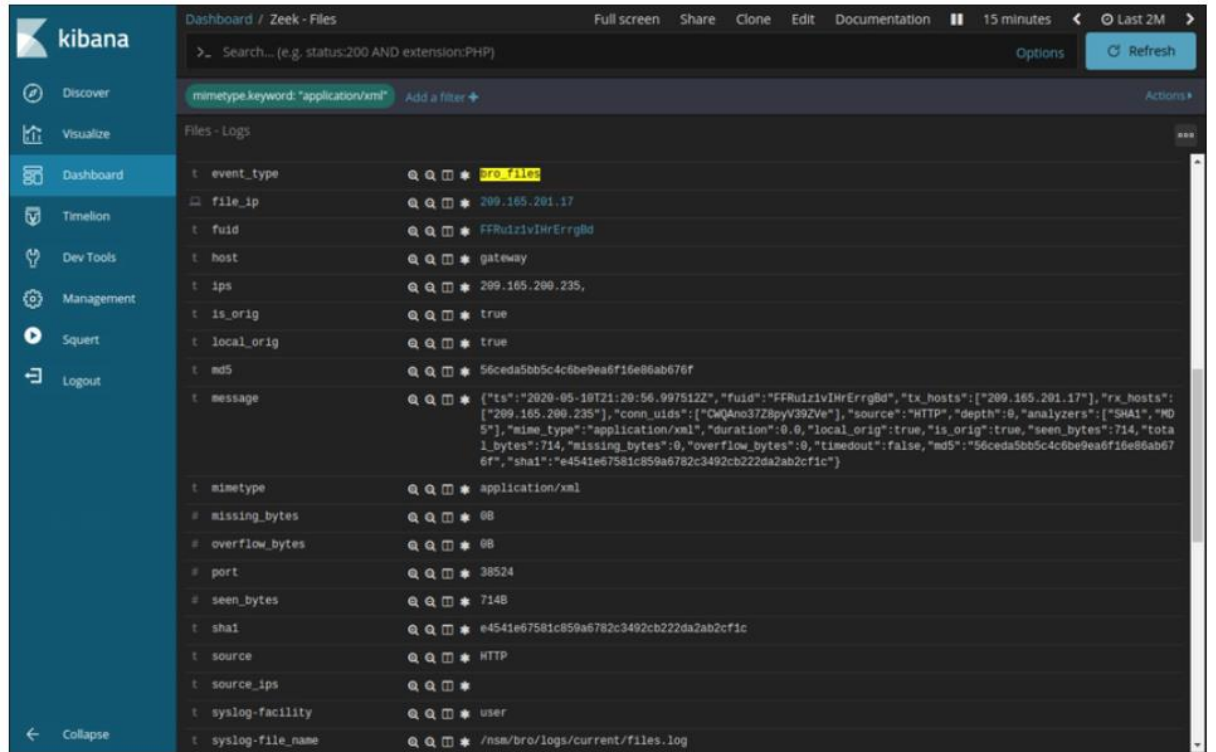
Investigating Process or API Calls

- Applications interact with an Operating System (OS) through system calls to the OS Application Programming Interface (API).
- 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.
- OSSEC rules will trigger an alert in Sguil.
- Pivoting to Kibana on the host IP address allows you to choose the type of alert based on the program that created it.
- Filtering for **OSSEC** indices results in a view of the OSSEC events that occurred on the host, including indicators that **malware may have interacted with the OS kernel**

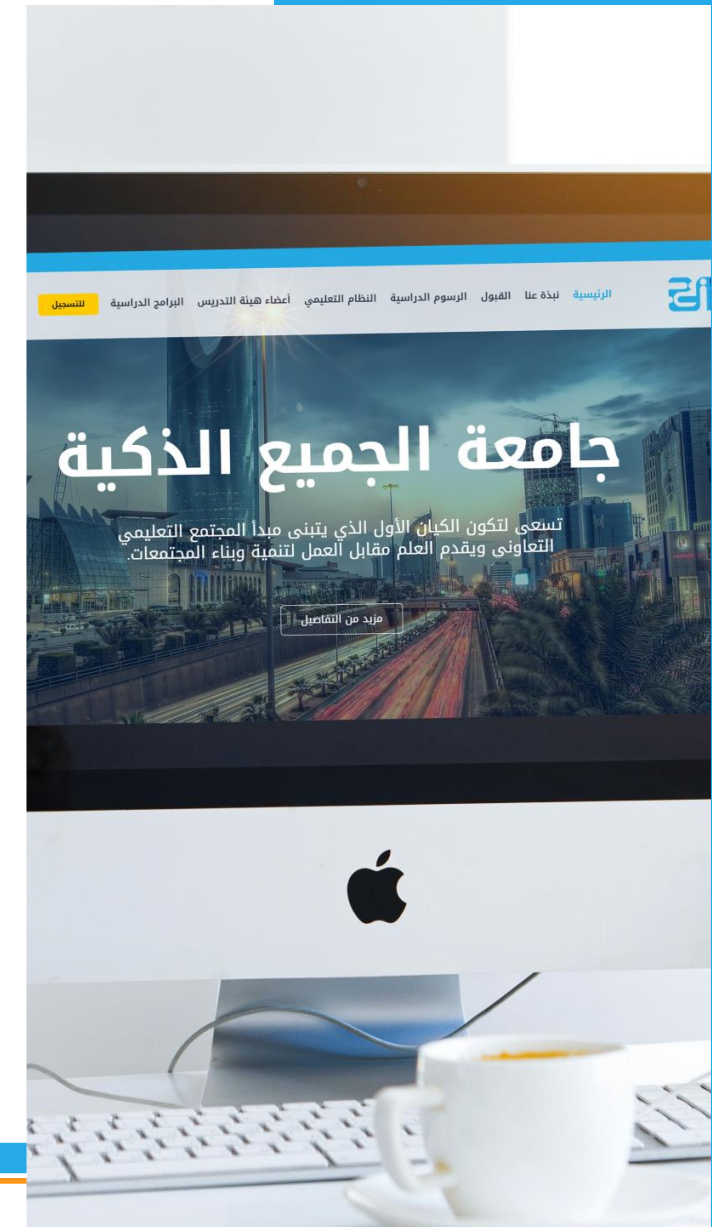


Investigating File Details

- In Sguil, if the cybersecurity analyst is suspicious of a file, the hash value can be submitted to an online site to determine if the file is a known malware.
- In [Kibana](#), [Zeek Hunting](#) can be used to display information regarding the files that have entered the network.
- Note that in Kibana, the event type is shown as [bro_files](#), even though the new name for Bro is Zeek.

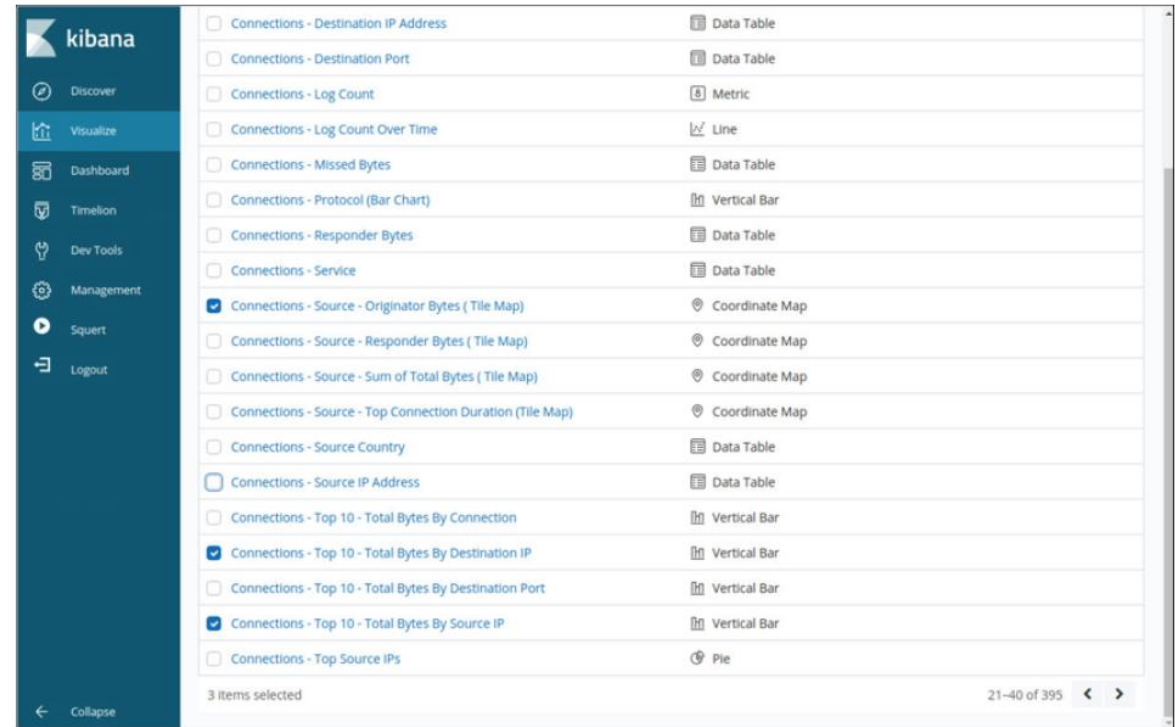


Enhancing the Work of the Cybersecurity Analyst



Dashboards and Visualizations

- **Dashboards** provide a combination of data and visualizations which allows cybersecurity analysts to focus on specific details and information.
- Dashboards are usually interactive.
- **Kibana** includes the capability of designing **custom dashboards**.
- In addition, tools such as **Squert** in Security Onion provide a **visual interface** to NSM data.



Workflow Management

- **Workflows** are the sequence of processes and procedures through which work tasks are completed.
- **Managing the SOC workflows:**
 - Enhances the efficiency of the cyberoperations team
 - Increases the accountability of the staff
 - Ensures that all potential alerts are treated properly
- **Sguil** provides a **basic workflow management** but **not a good choice for large operations**. There are third party systems available that can be customized.
- Automated queries add efficiency to the cyberoperations workflow. These queries automatically search for complex security incidents that may evade other tools.



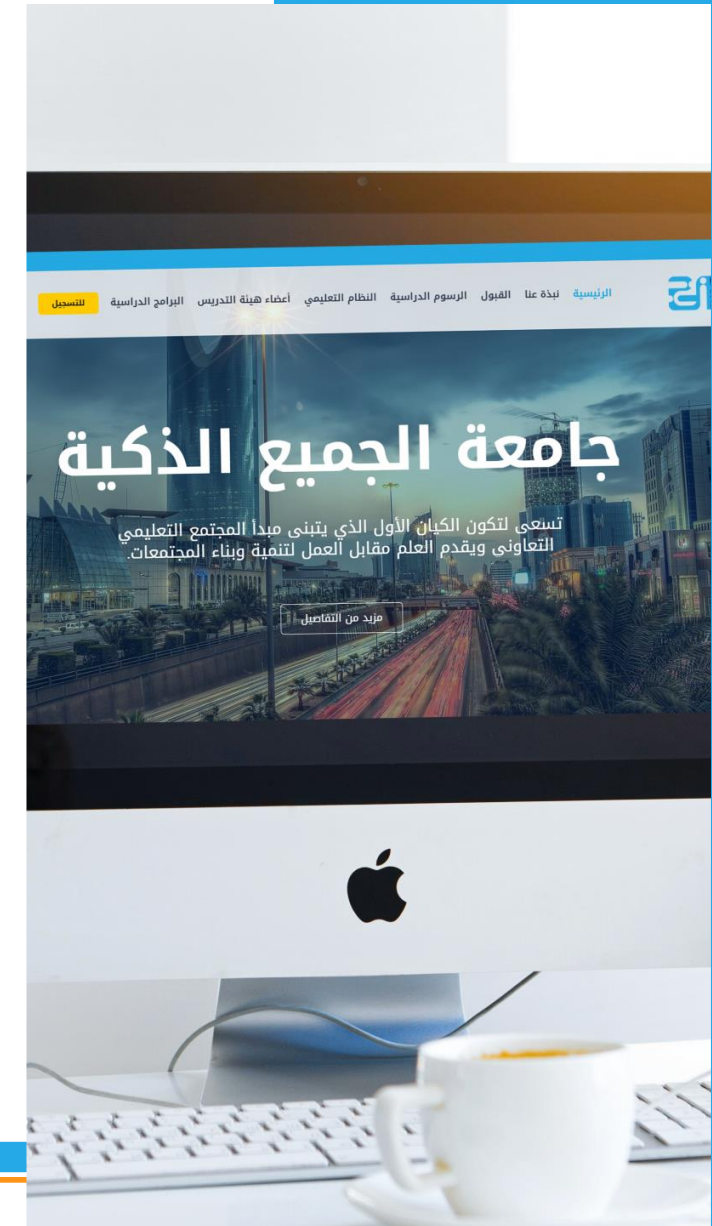
Lecture – 9

Activity 2

Lab - Isolate Compromised Host Using 5-Tuple

In this lab, you will complete the following objective:

- Use Security Onion tools to investigate an exploit.



Lecture – 9

Analyze network intrusion data to identify compromised hosts and vulnerabilities

Thanks

