Identifying and Analyzing Network/Host Intrusion Detection System Alerts

The purpose of this lab is to introduce the concept of network and host monitoring using the Security Onion platform. The lab involves setting up Security Onion on a Kali machine and using Zenmap to perform an intense scan on multiple networks to identify common ports. In the second part of the lab, the command "sudo service nsm status" is used to monitor all networks for RealTime Events, and the packet data is analyzed for potential security incidents. A report is generated, highlighting potential security issues such as ET SCAN NMAP OS Detection. In the third part of the lab, Squert is used to apply filters to analyze traffic from a specific IP address (10.1.1.10) to the DVL Server on eth0 interface, enabling security analysts to identify potential threats and generate visual reports.

1. **Define IDS, Host-Based IDS and Network-Based IDS:**

IDS stands for Intrusion Detection System. It is a security technology that monitors network or system activities for malicious activities or policy violations. IDSs are designed to detect and respond to various types of attacks or unauthorized activities in real-time or near real-time.

Host-Based IDS (HIDS) is an IDS that focuses on monitoring and analyzing activities on individual hosts or endpoints within a network. It operates by installing software agents or sensors on the host systems to monitor and analyze local event logs, system files, and network connections. HIDS looks for signs of intrusion or suspicious behavior on a specific host, such as unauthorized access attempts, file modifications, or abnormal network traffic patterns. It provides a more detailed view of the host's security status and helps in detecting attacks targeting a specific system.

Network-Based IDS (NIDS), on the other hand, monitors network traffic and analyzes it for signs of malicious activities or policy violations. It operates by capturing and inspecting network packets flowing through network devices, such as routers, switches, or dedicated sensors. NIDS examines packet headers and payloads, looking for patterns or signatures of known attacks or anomalous behavior. It can identify various types of network-based attacks, including network scanning, denial-of-service (DoS) attacks, and intrusion attempts targeting specific services or protocols. NIDS provides a broader view of the network's security posture and helps in detecting attacks targeting multiple hosts or network segments.

2. **What is Security Onion and what is it used for?**

Security Onion is a free and open-source platform for network security monitoring and intrusion detection. It is a Linux distribution that integrates several security tools and components into a unified system. Security Onion provides a complete solution for network security monitoring, log management, and analysis.

The primary purpose of Security Onion is to assist in detecting and responding to security incidents within a network. It combines various components and tools to provide comprehensive network security capabilities.

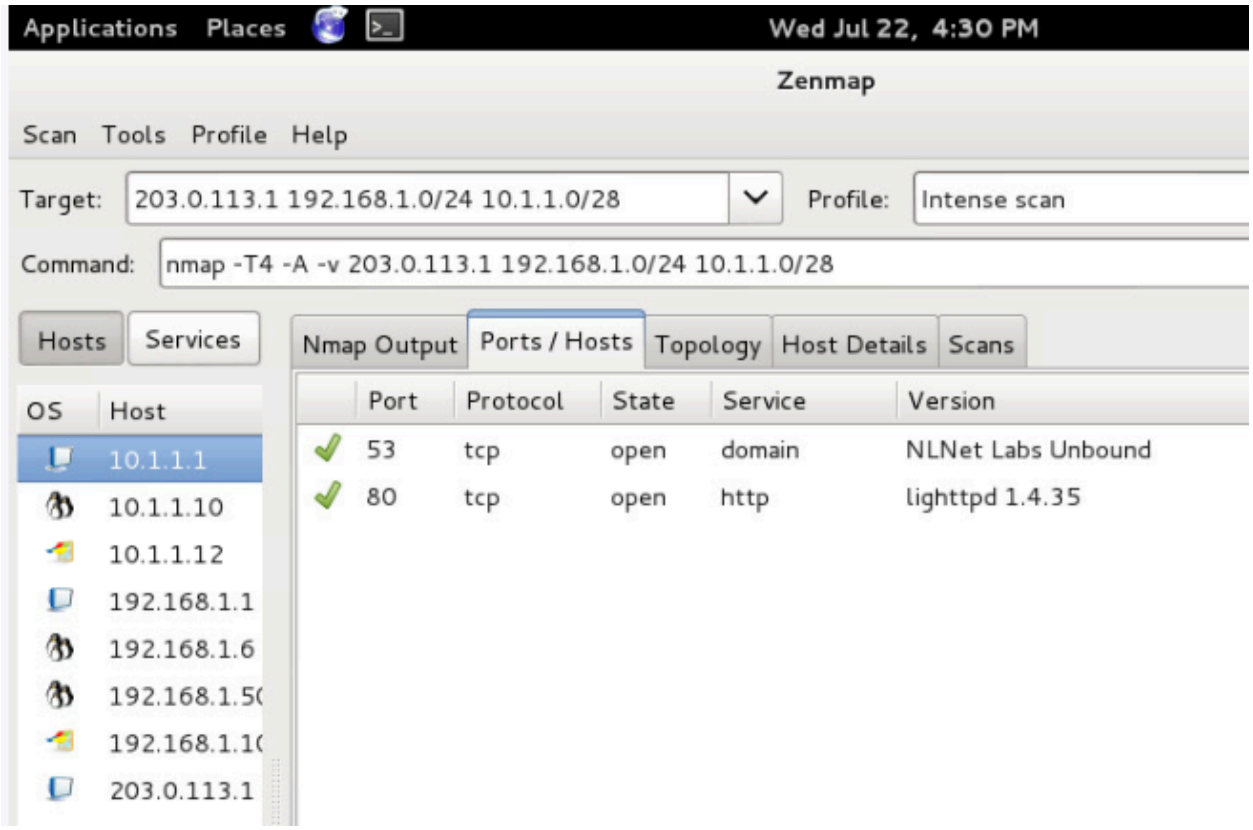
3. **Define Sguil and Squert and how they relate to one another:**

Sguil and Squert are two components of the Security Onion platform that work together to provide enhanced network security monitoring and analysis capabilities.

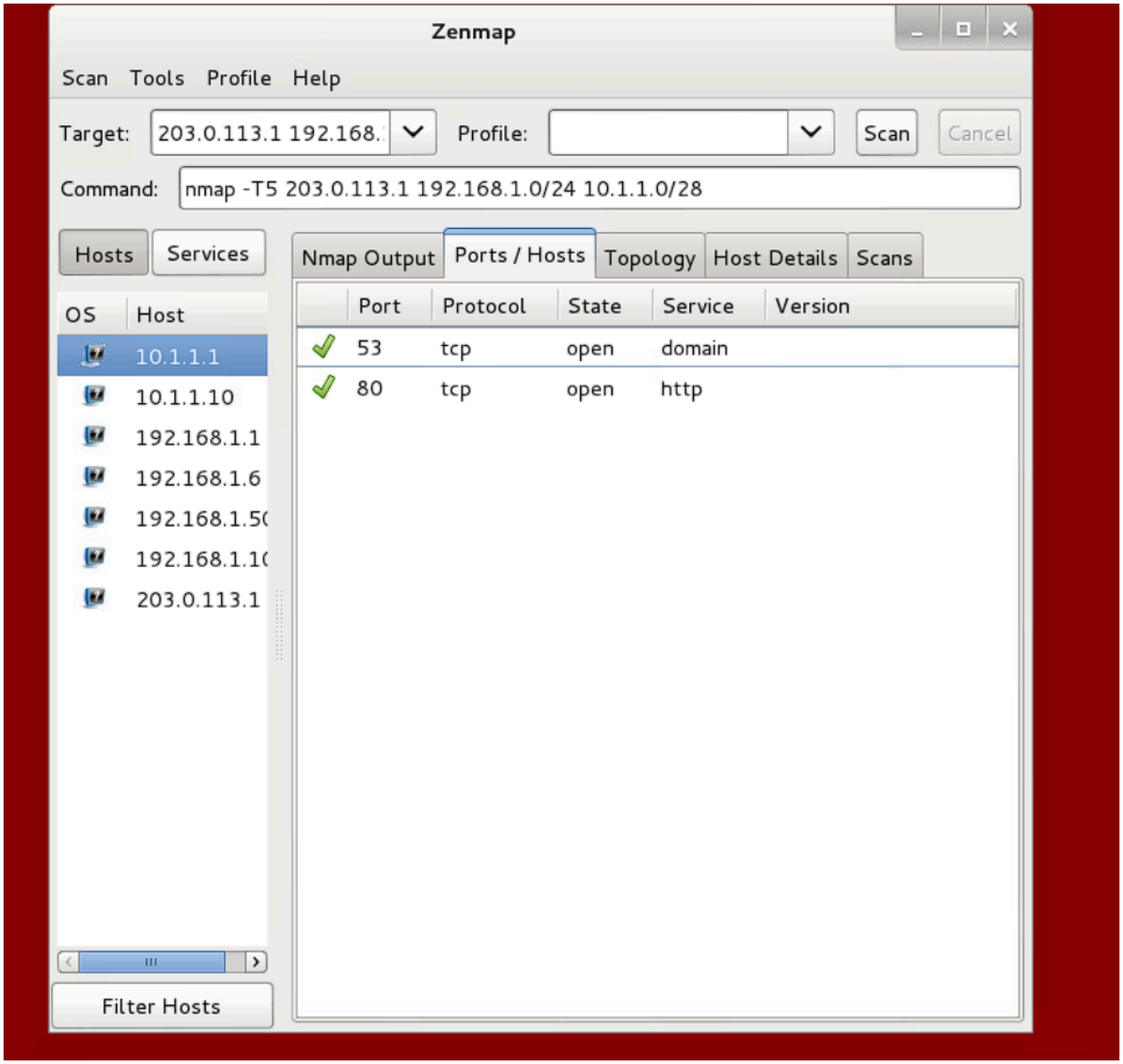
Sguil is a graphical user interface (GUI) that serves as a central management console for Security Onion. It integrates various security tools, including intrusion detection systems (IDS), packet capture tools, and log management systems, into a unified interface. Sguil provides a single pane of glass for security analysts to monitor and investigate security events in real-time.

Sguil and Squert are complementary components of the Security Onion platform. Sguil serves as the central management console for security monitoring and investigation, while Squert provides a visual representation and analysis of security events. Together, they enhance the capabilities of Security Onion by enabling real-time monitoring, event correlation, investigation, collaboration, and visual analysis for network security incidents.

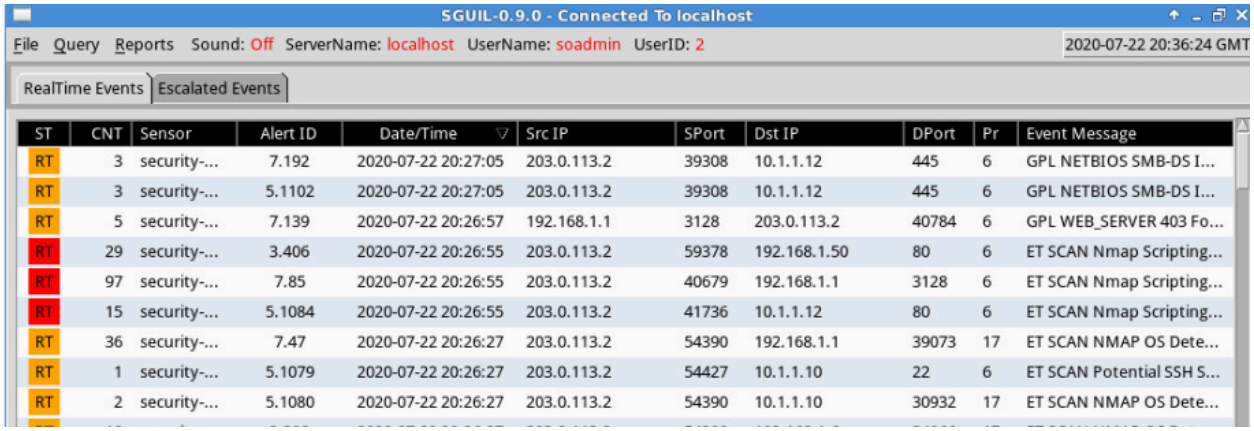
On page 7, import the snapshot equivalent to Figure 10. Include the list of various hosts that were scanned by Zenmap. See the example below:



4. **Import your snapshot (similar to example above) here:**

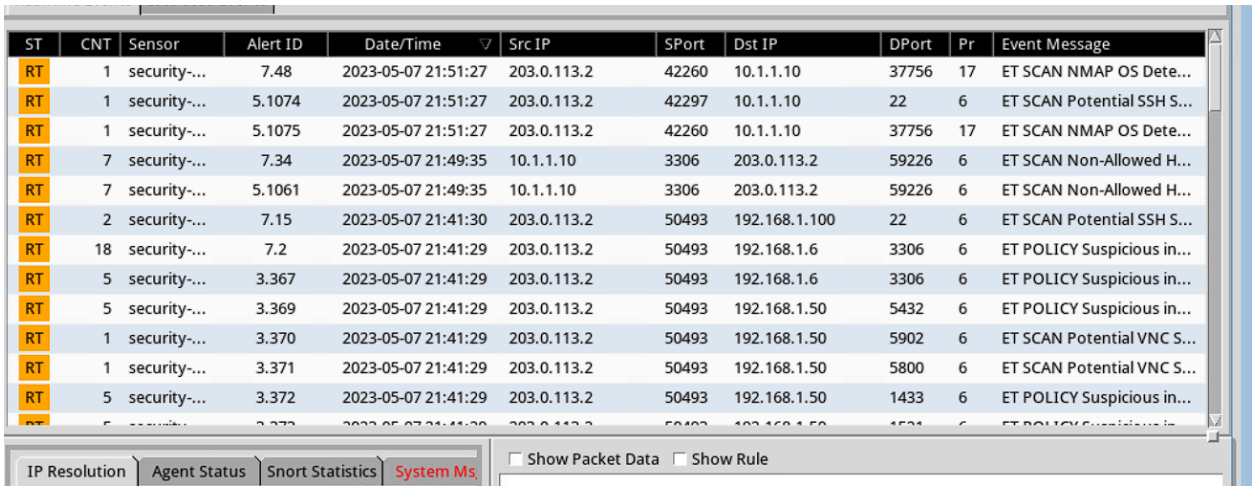

Zenmap
Scan Tools Profile Help
Target: 203.0.113.1 192.168.
Profile:
Scan
Cancel
Command: nmap -T5 203.0.113.1 192.168.1.0/24 10.1.1.0/28
Hosts
Services
OS
Host
10.1.1.1
10.1.1.10
192.168.1.1
192.168.1.6
192.168.1.5(
192.168.1.1(
203.0.113.1
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Port
Protocol
State
Service
Version
53
tcp
open
domain
80
tcp
open
http

On page 9, import the snapshot equivalent to Figure 5. See the example below:



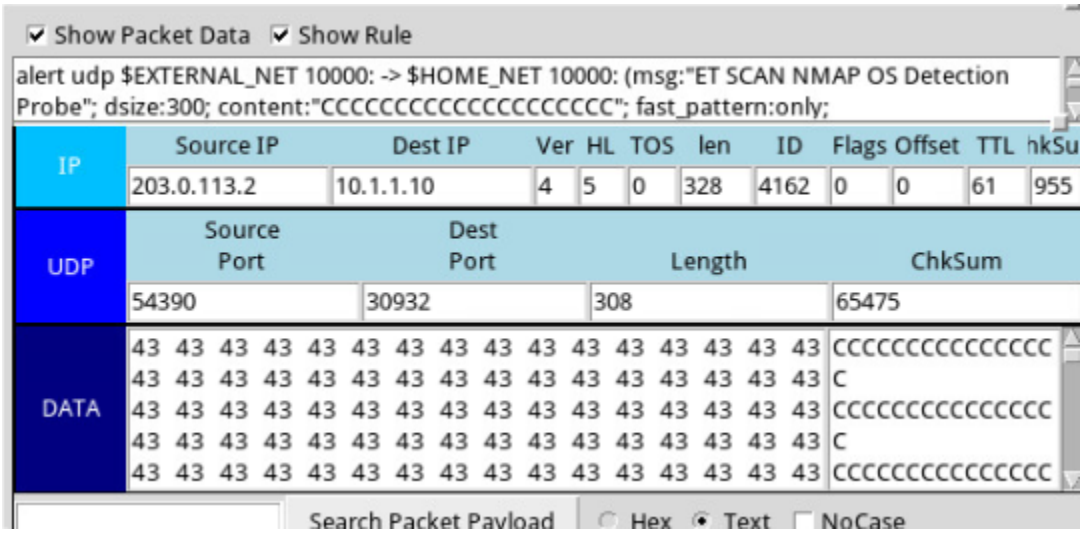
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	3	security-...	7.192	2020-07-22 20:27:05	203.0.113.2	39308	10.1.1.12	445	6	GPL NETBIOS SMB-DS I...
RT	3	security-...	5.1102	2020-07-22 20:27:05	203.0.113.2	39308	10.1.1.12	445	6	GPL NETBIOS SMB-DS I...
RT	5	security-...	7.139	2020-07-22 20:26:57	192.168.1.1	3128	203.0.113.2	40784	6	GPL WEB_SERVER 403 Fo...
RT	29	security-...	3.406	2020-07-22 20:26:55	203.0.113.2	59378	192.168.1.50	80	6	ET SCAN Nmap Scripting...
RT	97	security-...	7.85	2020-07-22 20:26:55	203.0.113.2	40679	192.168.1.1	3128	6	ET SCAN Nmap Scripting...
RT	15	security-...	5.1084	2020-07-22 20:26:55	203.0.113.2	41736	10.1.1.12	80	6	ET SCAN Nmap Scripting...
RT	36	security-...	7.47	2020-07-22 20:26:27	203.0.113.2	54390	192.168.1.1	39073	17	ET SCAN NMAP OS Dete...
RT	1	security-...	5.1079	2020-07-22 20:26:27	203.0.113.2	54427	10.1.1.10	22	6	ET SCAN Potential SSH S...
RT	2	security-...	5.1080	2020-07-22 20:26:27	203.0.113.2	54390	10.1.1.10	30932	17	ET SCAN NMAP OS Dete...

5. Import your snapshot (similar to example above) here:

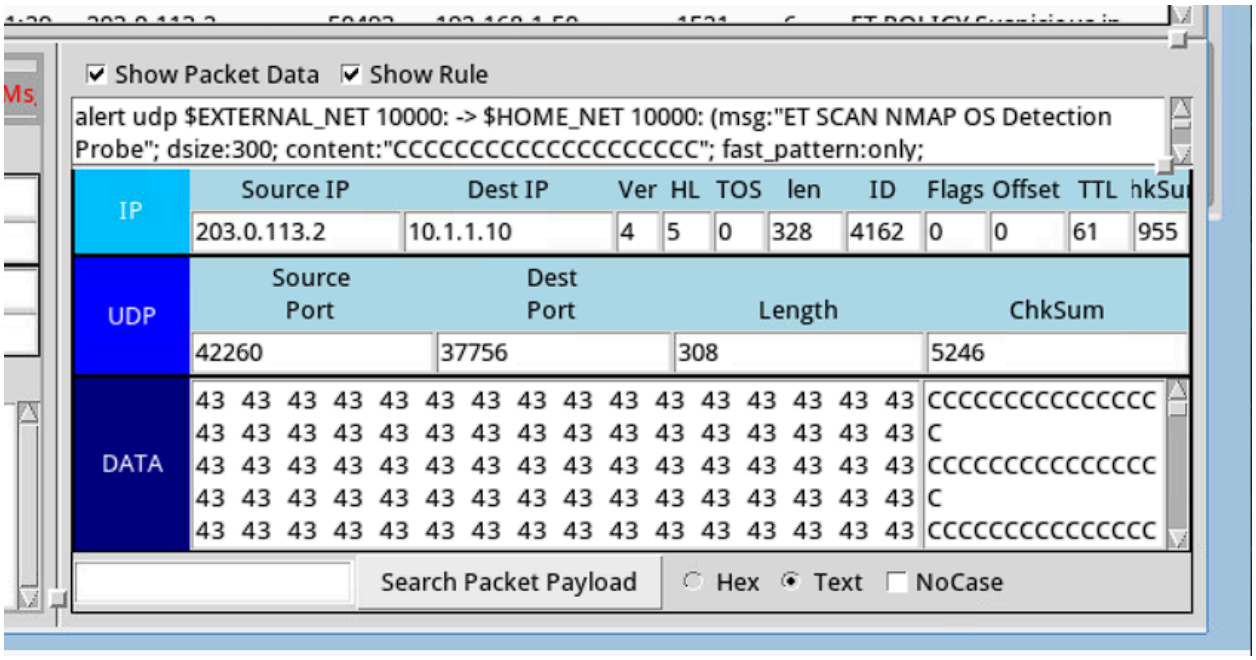


ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	security-...	7.48	2023-05-07 21:51:27	203.0.113.2	42260	10.1.1.10	37756	17	ET SCAN NMAP OS Dete...
RT	1	security-...	5.1074	2023-05-07 21:51:27	203.0.113.2	42297	10.1.1.10	22	6	ET SCAN Potential SSH S...
RT	1	security-...	5.1075	2023-05-07 21:51:27	203.0.113.2	42260	10.1.1.10	37756	17	ET SCAN NMAP OS Dete...
RT	7	security-...	7.34	2023-05-07 21:49:35	10.1.1.10	3306	203.0.113.2	59226	6	ET SCAN Non-Allowed H...
RT	7	security-...	5.1061	2023-05-07 21:49:35	10.1.1.10	3306	203.0.113.2	59226	6	ET SCAN Non-Allowed H...
RT	2	security-...	7.15	2023-05-07 21:41:30	203.0.113.2	50493	192.168.1.100	22	6	ET SCAN Potential SSH S...
RT	18	security-...	7.2	2023-05-07 21:41:29	203.0.113.2	50493	192.168.1.6	3306	6	ET POLICY Suspicious in...
RT	5	security-...	3.367	2023-05-07 21:41:29	203.0.113.2	50493	192.168.1.6	3306	6	ET POLICY Suspicious in...
RT	5	security-...	3.369	2023-05-07 21:41:29	203.0.113.2	50493	192.168.1.50	5432	6	ET POLICY Suspicious in...
RT	1	security-...	3.370	2023-05-07 21:41:29	203.0.113.2	50493	192.168.1.50	5902	6	ET SCAN Potential VNC S...
RT	1	security-...	3.371	2023-05-07 21:41:29	203.0.113.2	50493	192.168.1.50	5800	6	ET SCAN Potential VNC S...
RT	5	security-...	3.372	2023-05-07 21:41:29	203.0.113.2	50493	192.168.1.50	1433	6	ET POLICY Suspicious in...

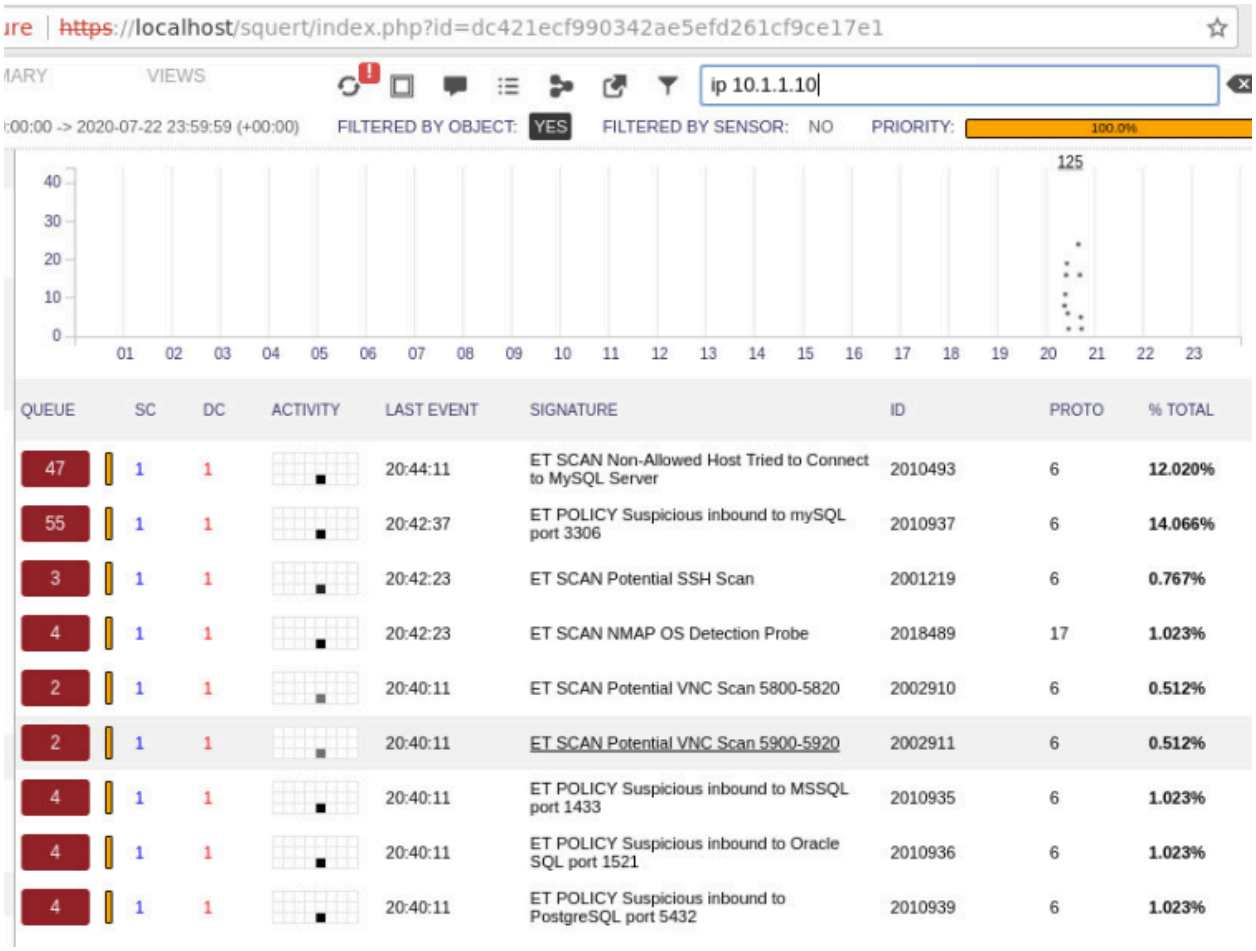
On page 11, import the snapshot equivalent to Figure 4. See the example below:



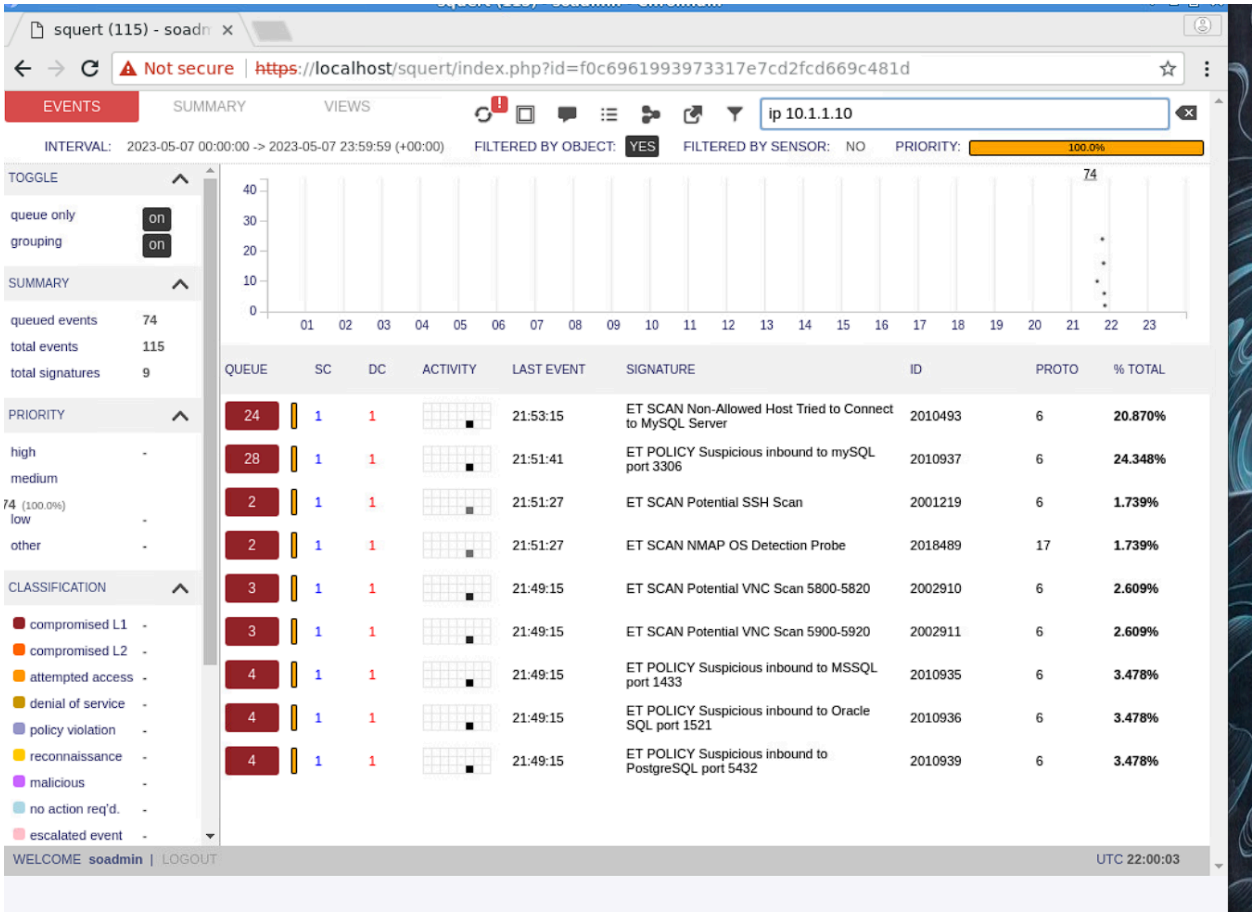
6. **Import your snapshot (similar to example above) here:**



On page 16, import the snapshot equivalent to Figure 9. See the example below:



7. **Import your snapshot (similar to example above) here:**


squert (115) - soadn
Not secure
https://localhost/squert/index.php?id=f0c6961993973317e7cd2fcd669c481d
EVENTS
SUMMARY
VIEWS
ip 10.1.1.10
INTERVAL: 2023-05-07 00:00:00 -> 2023-05-07 23:59:59 (+00:00)
FILTERED BY OBJECT: YES
FILTERED BY SENSOR: NO
PRIORITY: 100.0%
TOGGLE
queue only on
grouping on
SUMMARY
queued events 74
total events 115
total signatures 9
PRIORITY
high -
medium
74 (100.0%)
low -
other -
CLASSIFICATION
compromised L1 -
compromised L2 -
attempted access -
denial of service -
policy violation -
reconnaissance -
malicious -
no action req'd. -
escalated event -
74
40
30
20
10
0
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23
QUEUE SC DC ACTIVITY LAST EVENT SIGNATURE ID PROTO % TOTAL
24 1 1 21:53:15 ET SCAN Non-Allowed Host Tried to Connect to MySQL Server 2010493 6 20.870%
28 1 1 21:51:41 ET POLICY Suspicious inbound to mySQL port 3306 2010937 6 24.348%
2 1 1 21:51:27 ET SCAN Potential SSH Scan 2001219 6 1.739%
2 1 1 21:51:27 ET SCAN NMAP OS Detection Probe 2018489 17 1.739%
3 1 1 21:49:15 ET SCAN Potential VNC Scan 5800-5820 2002910 6 2.609%
3 1 1 21:49:15 ET SCAN Potential VNC Scan 5900-5920 2002911 6 2.609%
4 1 1 21:49:15 ET POLICY Suspicious inbound to MSSQL port 1433 2010935 6 3.478%
4 1 1 21:49:15 ET POLICY Suspicious inbound to Oracle SQL port 1521 2010936 6 3.478%
4 1 1 21:49:15 ET POLICY Suspicious inbound to PostgreSQL port 5432 2010939 6 3.478%
WELCOME soadmin | LOGOUT
UTC 22:00:03