**Cyber Security Task 2 Report**

## Security Alert Monitoring & Incident Response Simulation

By CHITIRALA SA MADHU KEERTHI  
Future Interns Program – 7/July/2025



# FUTURE INTERNS

**Objective**

The goal of this internship task is to simulate the real-world responsibilities of a Security Operations Center (SOC) analyst by monitoring and investigating security alerts using a SIEM tool. This includes detecting suspicious behaviors, analyzing malware-related events, classifying threats, and recommending appropriate responses.

Through hands-on experience with log data, this task aims to:

* Identify and investigate malware detection alerts (e.g., Trojan, Worm, Ransomware, Rootkit, Spyware)
* Perform incident classification based on severity and potential impact
* Practice security alert triage using a SIEM tool (Splunk)
* Generate dashboards for threat visibility
* Draft incident response reports based on log evidence

**Tools Used**

* **Splunk Free Trial**  
  Used as the SIEM platform to ingest, search, and visualize system logs. Queries were run to identify security threats and generate incident timelines.
* **Google Docs / MS Word**  
  Used for preparing the incident response report and compiling findings.

**Dataset Details**

* **Log Source:** future intern task 2 logs
* **Splunk Index:** future\_intern\_task\_2\_main\_1
* **Sourcetype:** future\_intern\_task\_log
* **Log Type:** Simulated malware and activity logs
* **Host:** kali
* **Time Range:** July 3, 2025

**Log Contents Included:**

* Malware detection alerts with IP, user, and threat type
* Event timestamps down to the second
* Variety of threats: Trojan, Worm, Rootkit, Ransomware, Spyware
* Simulated user activity across different endpoints

**Malware Detection Summary**

|  |  |  |  |
| --- | --- | --- | --- |
| **User** | **IP Address** | **Threats Detected** | **Count** |
| Alice | 198.51.100.42 | Rootkit, Spyware, Trojan | 3 |
| Bob | 172.16.0.3 | Ransomware, Worm | 3 |
| Charlie | 172.16.0.3 | Trojan | 1 |
| David | 172.16.0.3 | Trojan | 1 |
| Eve | 10.0.0.5,203.x | Rootkit, Trojan | 3 |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Incident Reports**

## ****Incident 1: Ransomware Behavior Detected on Internal Host****

## ****Details****

* **Threat Type:** Ransomware Behavior
* **User:** bob
* **IP Address:** 172.16.0.3
* **Date & Time:** 2025-07-03 09:10:14 AM
* **Host:** kali
* **Source Log:** future intern task 2 logs
* **Index:** future\_intern\_task\_2\_main\_1

### ****Impact****

* **High risk of data encryption and loss** due to potential ransomware execution.
* Possible **business disruption**, including locked files, system downtime, or ransom demands.
* Threat may spread laterally to other systems and compromise entire network segments.
* Any unpatched vulnerabilities could be exploited to reinfect the machine or bypass recovery.

### ****Analysis****

A ransomware behavior signature was triggered on an internal host assigned to user bob. The system (172.16.0.3) is also linked to other malware alerts (e.g., Trojan), suggesting a **multi-stage attack** or **post-compromise activity**. The ransomware signature indicates the presence of **file encryption patterns or C2 (Command-and-Control) callbacks**, which are typically associated with known ransomware families.

The involvement of an internal IP also points to **internal lateral movement** or **user-initiated file execution**.

### ****Splunk Query:****

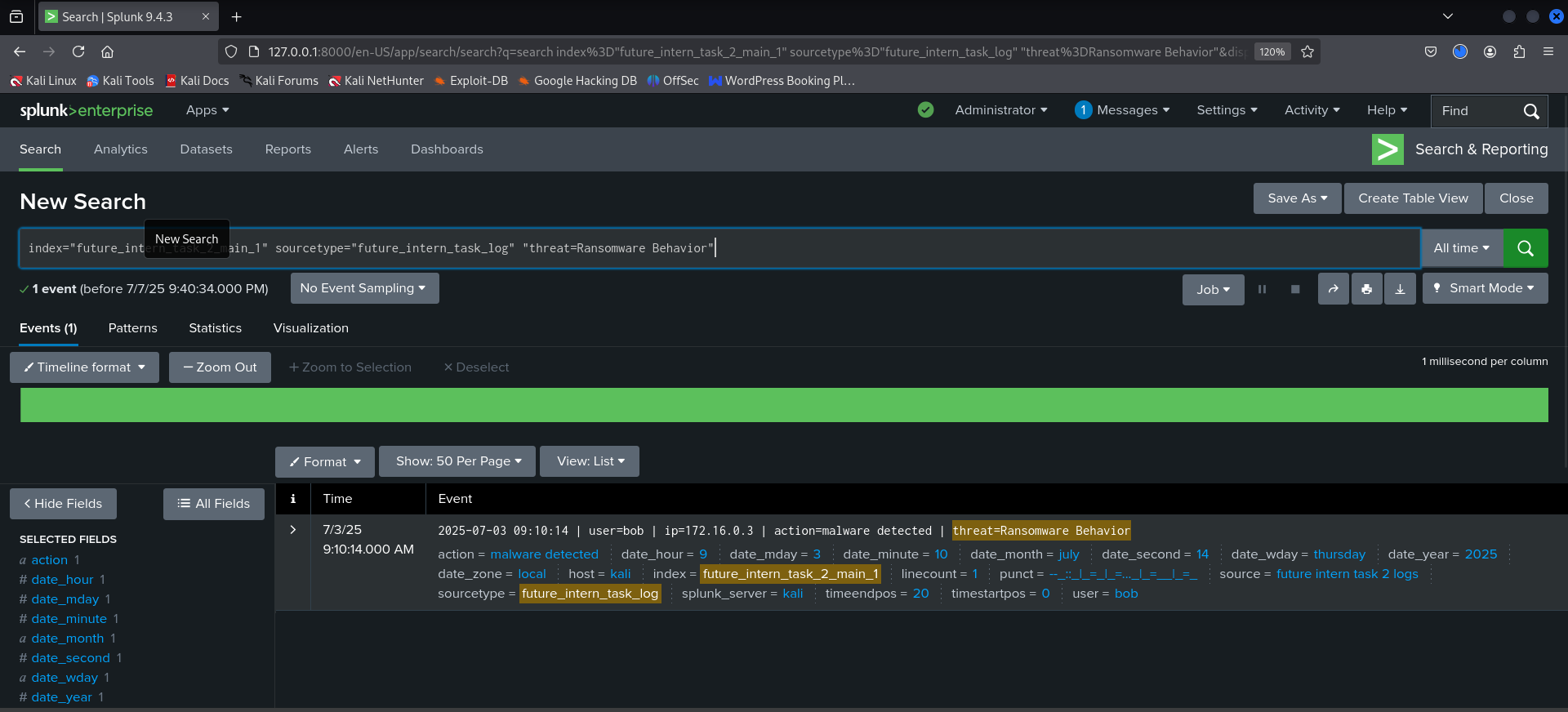
index="future\_intern\_task\_2\_main\_1" sourcetype="future\_intern\_task\_log" "threat=Ransomware Behavior"

### ****Severity:**** Critical

### ****Recommendations****

* Immediately **quarantine** the machine (172.16.0.3) to prevent further spread.
* Alert the user (bob) and disable account access temporarily.
* Conduct a **full disk backup and forensic imaging** before wiping the machine.
* Check for **exfiltration attempts** and any encrypted files or ransom notes.
* Conduct **network scans** to detect lateral movement.
* Review **system restore points** or backups for recovery.
* Patch all known vulnerabilities and harden endpoint defenses.

**Output:**



## ****Incident 2: Rootkit Signature Detected on Two Hosts****

### ****Details****

* **Threat Type:** Rootkit Signature
* **Users:** eve, alice
* **IP Addresses:**
  + 10.0.0.5 (user: eve @ 07:51 AM)
  + 198.51.100.42 (user: alice @ 04:19 AM)
* **Date:** 2025-07-03
* **Host:** kali
* **Index:** future\_intern\_task\_2\_main\_1

### ****Impact****

* Rootkits provide **stealth-level access** and can hide malware, processes, or user activity from the operating system.
* Systems infected with rootkits are often **fully compromised** and cannot be trusted.
* Potential **escalation of privileges** by attackers to maintain persistence.
* May require a **full system reinstallation**, as removal is difficult and unreliable.

### ****Analysis****

Two different IPs were flagged for Rootkit signatures within 4 hours:

* 10.0.0.5 (internal/private IP) – possibly a user endpoint or workstation.
* 198.51.100.42 (public IP) – might indicate **external exposure** or VPN-based access.

The detection across both users (eve and alice) raises concern for **widespread compromise** or malware propagation across networks. This also suggests that the rootkit may have been deployed via a **common attack vector**, such as a malicious email, removable media, or shared drive.

### ****Splunk Query:****

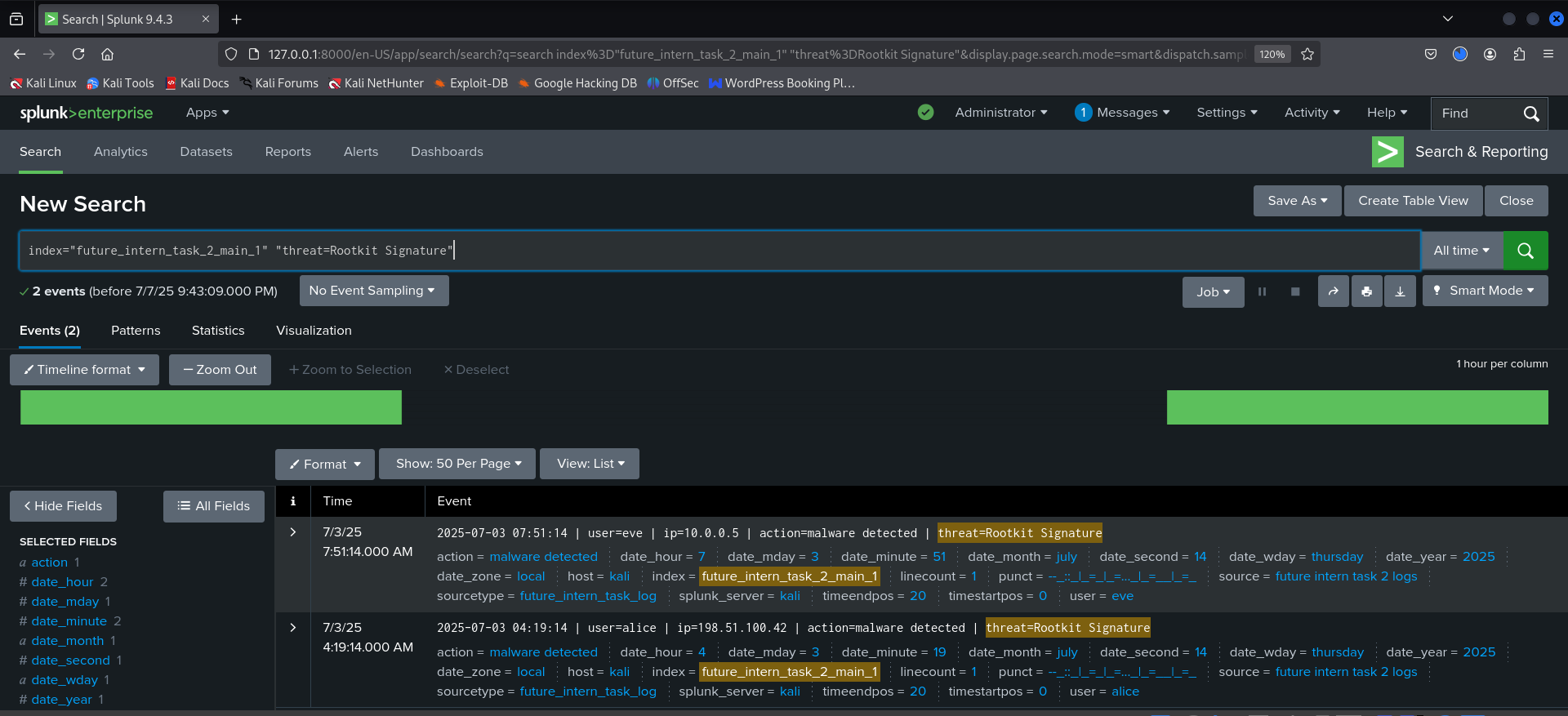
index="future\_intern\_task\_2\_main\_1" "threat=Rootkit Signature"

### ****Severity:**** High

### ****Recommendations****

* Immediately **disconnect affected systems** from the network.
* Perform **offline malware scans** using rootkit-specific tools (e.g., chkrootkit, GMER).
* Initiate **forensic analysis** to determine the rootkit’s origin and timeline.
* **Reimage systems** if rootkit presence is confirmed.
* Block suspicious IP addresses or domains associated with external communications.
* Review firewall and VPN logs for additional anomalies.
* Implement **application whitelisting** and enable secure boot to prevent reinstallation.

**Output:**



## ****Incident 3: Repeated Trojan Detection on Single Host****

### ****Details****

* **Threat Type:** Trojan Detected
* **IP Address:** 172.16.0.3
* **Users Affected:**
  + charlie (07:45 AM)
  + david (05:45 AM)
* **Date:** 2025-07-03
* **System Host:** kali
* **Index:** future\_intern\_task\_2\_main\_1

### ****Analysis****

This internal host was flagged **twice within two hours** for **Trojan malware infections** by **two separate users**. The recurrence indicates:

* **Persistent malware** infection surviving across sessions.
* A **compromised shared system** possibly acting as a pivot point.
* Increased risk of **credential harvesting**, **data exfiltration**, or **lateral movement** within the network.

### ****Impact****

* **Security Breach Risk:** The host may be used as a **launchpad for internal attacks** or **external command-and-control (C2)** connections.
* **Credential Compromise:** Both users (charlie and david) may have had their credentials **harvested by the Trojan**.
* **Operational Disruption:** The infected machine poses a risk to ongoing business functions and must be taken offline, affecting system availability.
* **Reputation & Compliance Risk:** If sensitive data is leaked, this could lead to **regulatory violations** and reputational damage.

### ****Splunk Query:****

index="future\_intern\_task\_2\_main\_1" "threat=Trojan Detected" "ip=172.16.0.3"

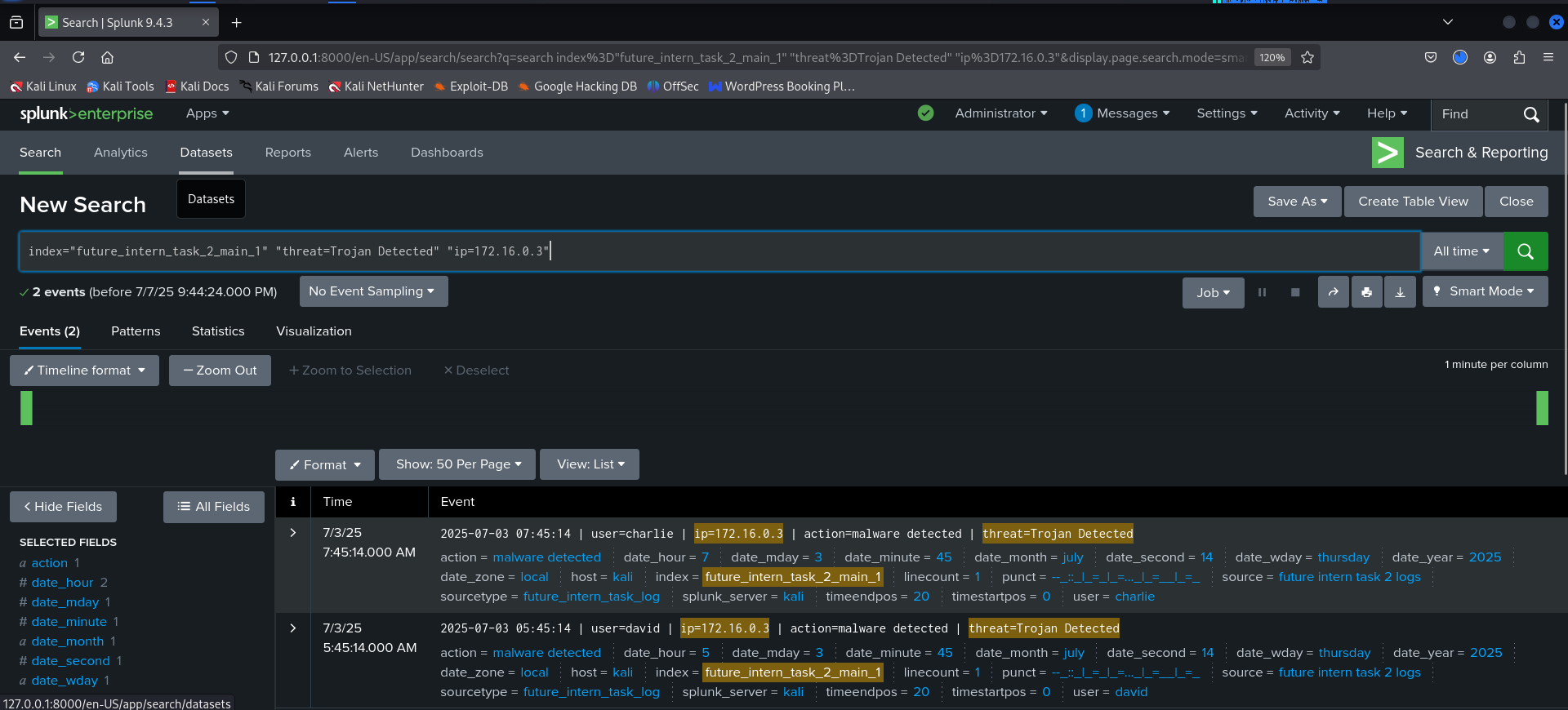
### ****Severity:**** High

Repeated infections on a single internal IP from multiple users is a critical red flag in SOC operations.

### ****Recommendations****

* Immediately **isolate the system (172.16.0.3)** from the network.
* Perform **forensic imaging** of the host for offline investigation.
* Scan all drives for **malware persistence techniques** (registry keys, startup scripts, scheduled tasks).
* Enforce a **password reset** for both users.
* Audit lateral connections from this host to identify any spread.

**Output:**



### ****Incident Report – Vulnerability 4****

**Threat Type:** Worm Infection Attempt  
**Detected Action:** malware detected  
**User Involved:** Bob  
**IP Address:** 203.0.113.77  
**Detection Time:** 2025-07-03 05:06:14 AM  
**Splunk Query:**

index="future\_intern\_task\_2\_main\_1" "threat=Worm Infection Attempt"

### ****Description:****

A **Worm Infection Attempt** was detected originating from user **Bob** on IP **203.0.113.77**. Worms are self-replicating malware that can spread across systems without user interaction. This type of malware typically exploits vulnerabilities in the operating system or network configuration to move laterally across the network.

### ****Severity Level:**** High

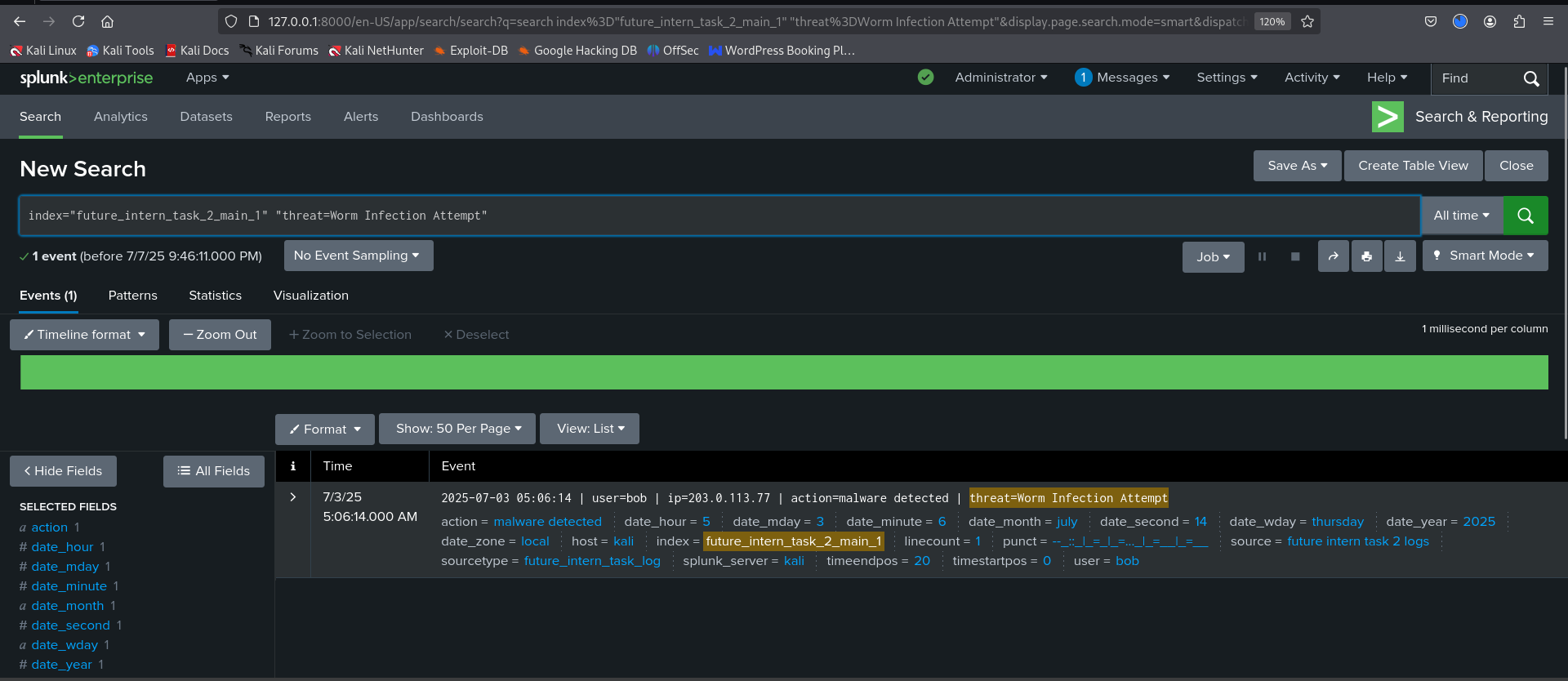
### ****Technical Impact:****

* Worms can **self-replicate** and **infect multiple systems** within minutes, causing rapid infection across the network.
* They often open **backdoors** for further exploitation or use the host as a bot in a larger botnet.
* Can severely impact **network performance**, and may **leak data** or cause **service disruption**.
* Risk of malware **spreading laterally** across critical infrastructure, especially if network segmentation is weak.

### ****Recommended Response Actions:****

* **Isolate the Affected System Immediately** to prevent the worm from spreading.
* **Perform a Full Malware Scan** on the device using endpoint security tools.
* **Block the Source IP** from network communication if it's not an internal asset.
* **Audit Network Logs** for signs of lateral movement or replication attempts.
* **Apply Security Patches** to vulnerable systems that the worm might exploit.
* **Conduct a Forensic Investigation** to determine the worm’s origin and payload.

**Output:**



## Summary Dashboard

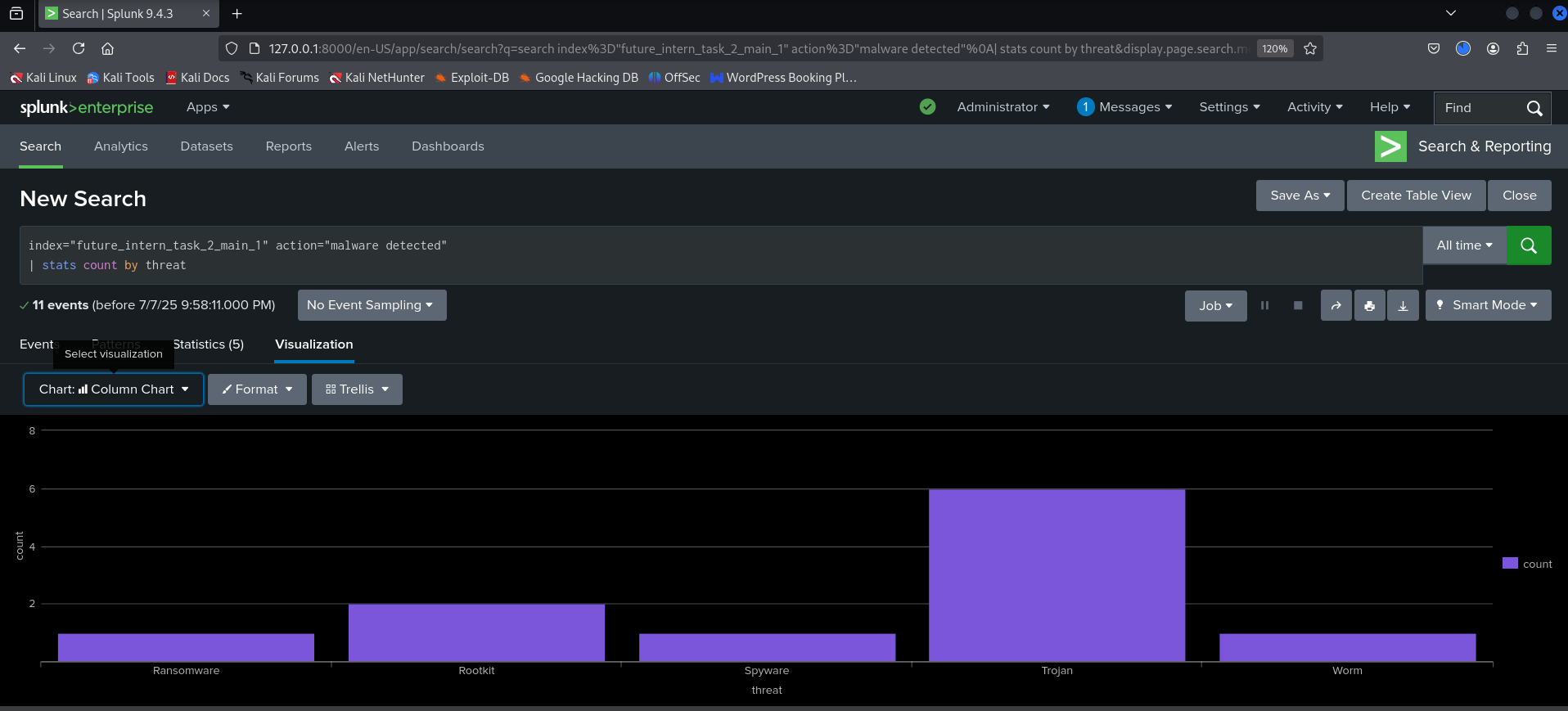
* Title: Malware Detection Summary – Task 2

### Added panels:

#### ****Panel: Threat Type Count****

index="future\_intern\_task\_2\_main\_1" action="malware detected"

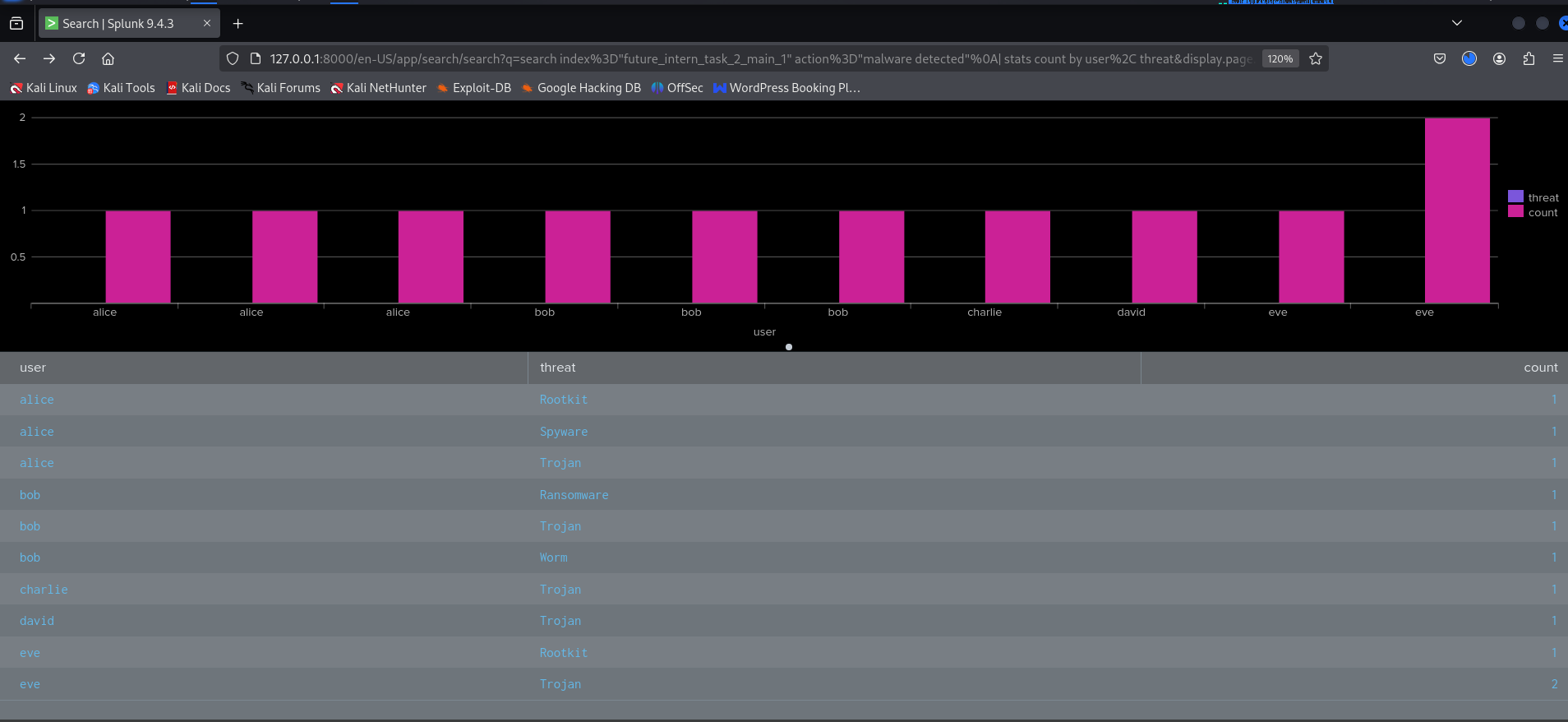
| stats count by threat



#### ****Panel: Malware per User****

index="future\_intern\_task\_2\_main\_1" action="malware detected"

| stats count by user, threat

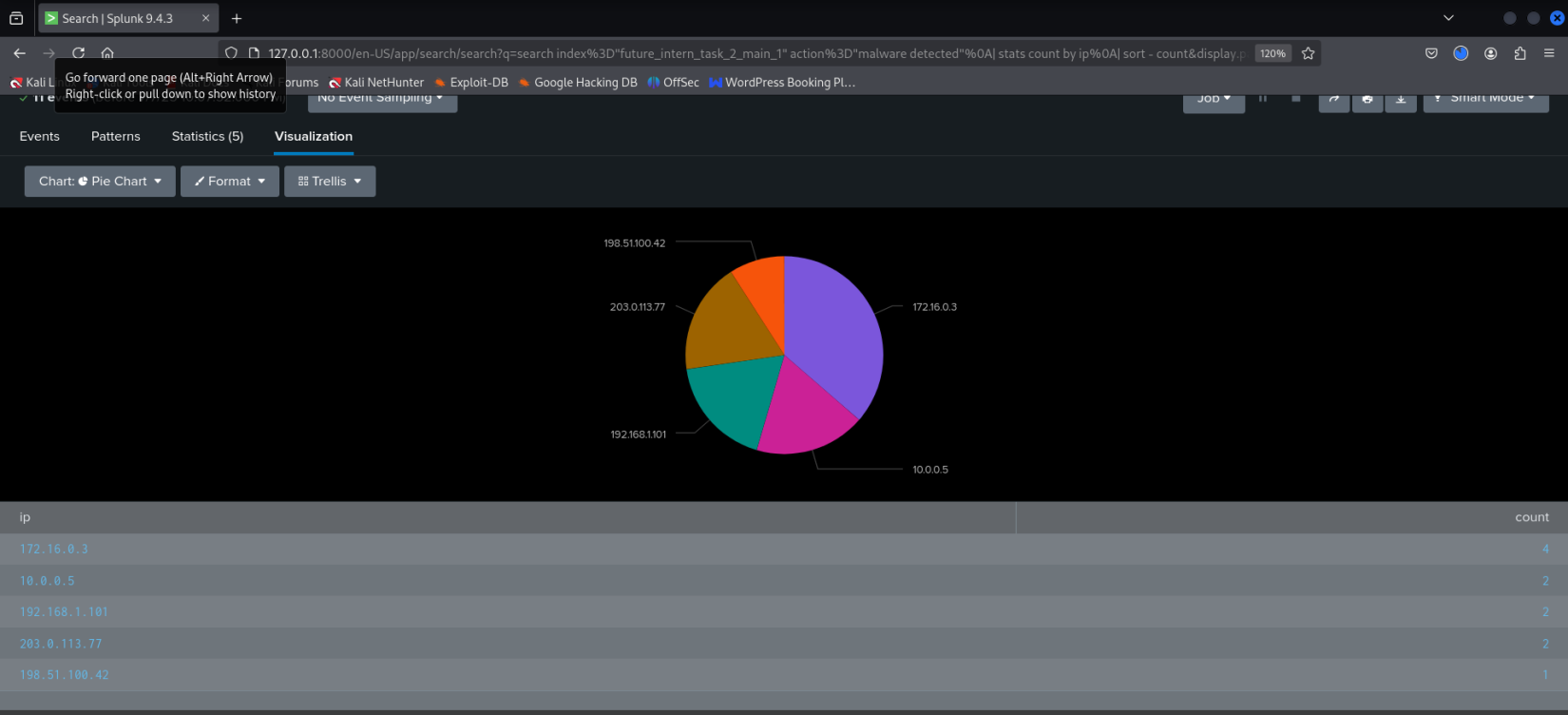


#### ****Panel: Most Affected IPs****

index="future\_intern\_task\_2\_main\_1" action="malware detected"

| stats count by ip

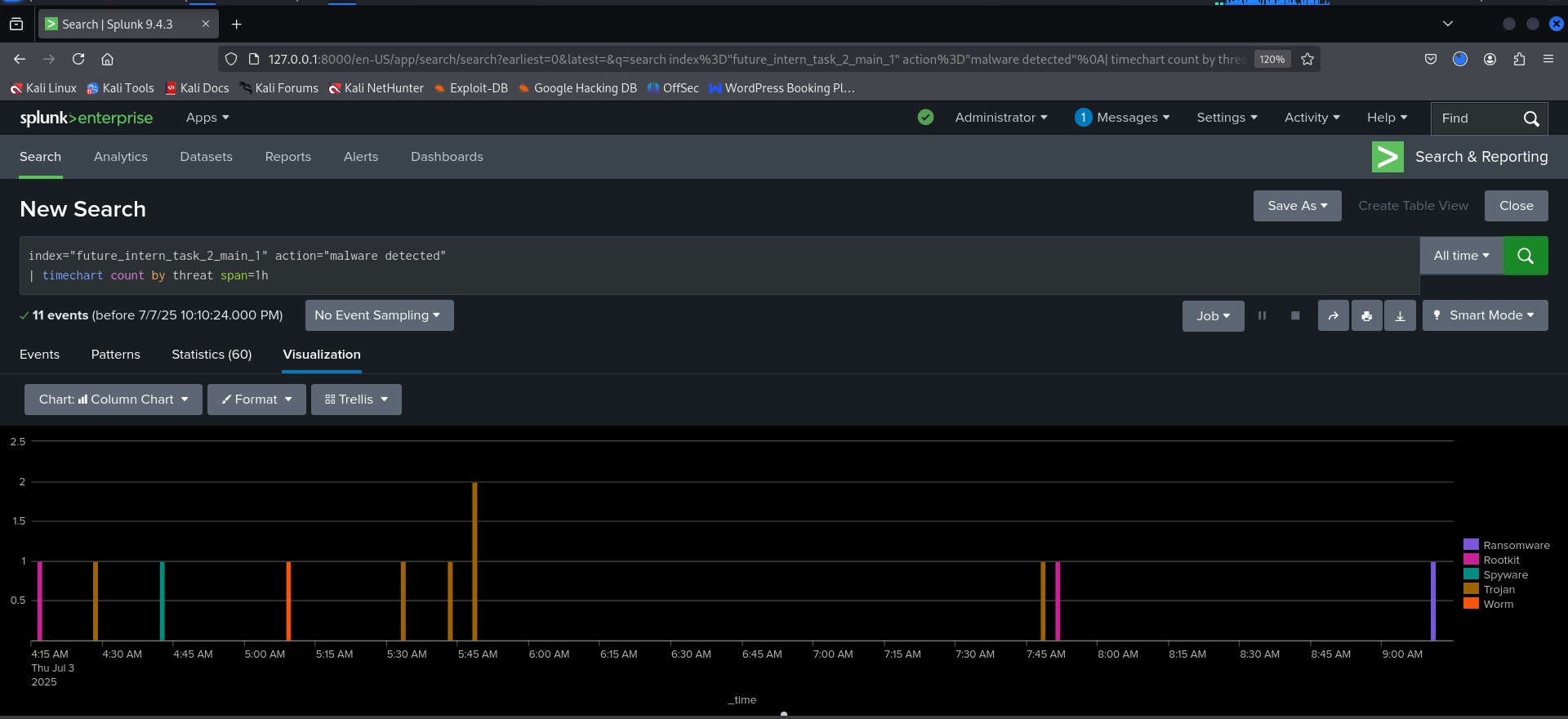
| sort - count



#### ****Panel: Timeline of Threats****

index="future\_intern\_task\_2\_main\_1" action="malware detected"

| timechart count by threat span=1h



**Final Dashboard Panel:**

## 

## 

## Dashboard pdf:

## 

## Email Draft for Final Report Submission

**Subject:** Final Malware Detection Report – SOC Internship Task 2

Respected Future Interns Team,

I hope you're doing well.

Please find attached my final report for Task 2 of the Future Interns Cybersecurity Program. The report documents malware incidents detected using Splunk, covering threats such as Trojan, Rootkit, Spyware, Ransomware, and Worms, along with impact assessment and remediation steps.

I have also included summary dashboards as visual evidence from Splunk to support the findings.

Thank you for your guidance throughout the internship.

Best regards,  
**Chitirala Sai Madhu Keerthi**  
Future Interns – Cybersecurity Track