Soc Analyst Lab-Navjot Singh and Safa Sultany

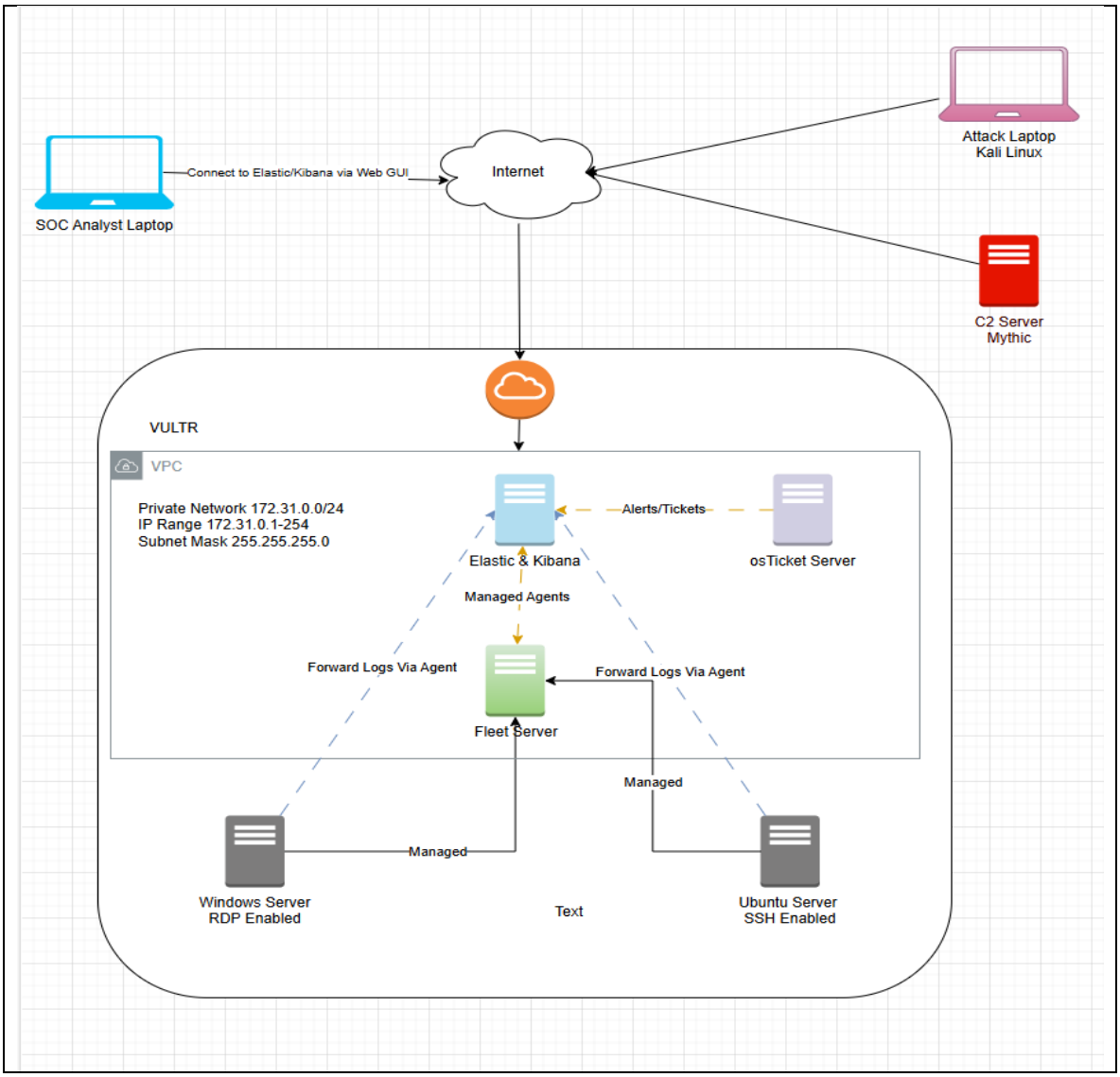
Executive Summary:

The "30-Day SOC Analyst Challenge" is a transformative initiative designed to address the critical gap in practical experience faced by aspiring Security Operations Center (SOC) analysts. Created by cybersecurity expert Steven, with over eight years of experience in the field, this challenge provides a structured, hands-on learning journey that empowers participants to acquire real-world skills necessary for SOC analyst roles—all within 30 days and at no cost.

The challenge is divided into four progressive weeks, covering essential SOC skills such as setting up and configuring the ELK stack, detecting and investigating brute force attacks, analyzing command-and-control (C2) operations, and integrating ticketing systems for incident management. Through these tasks, we gain valuable exposure to practical cybersecurity operations using industry-standard tools and methods.

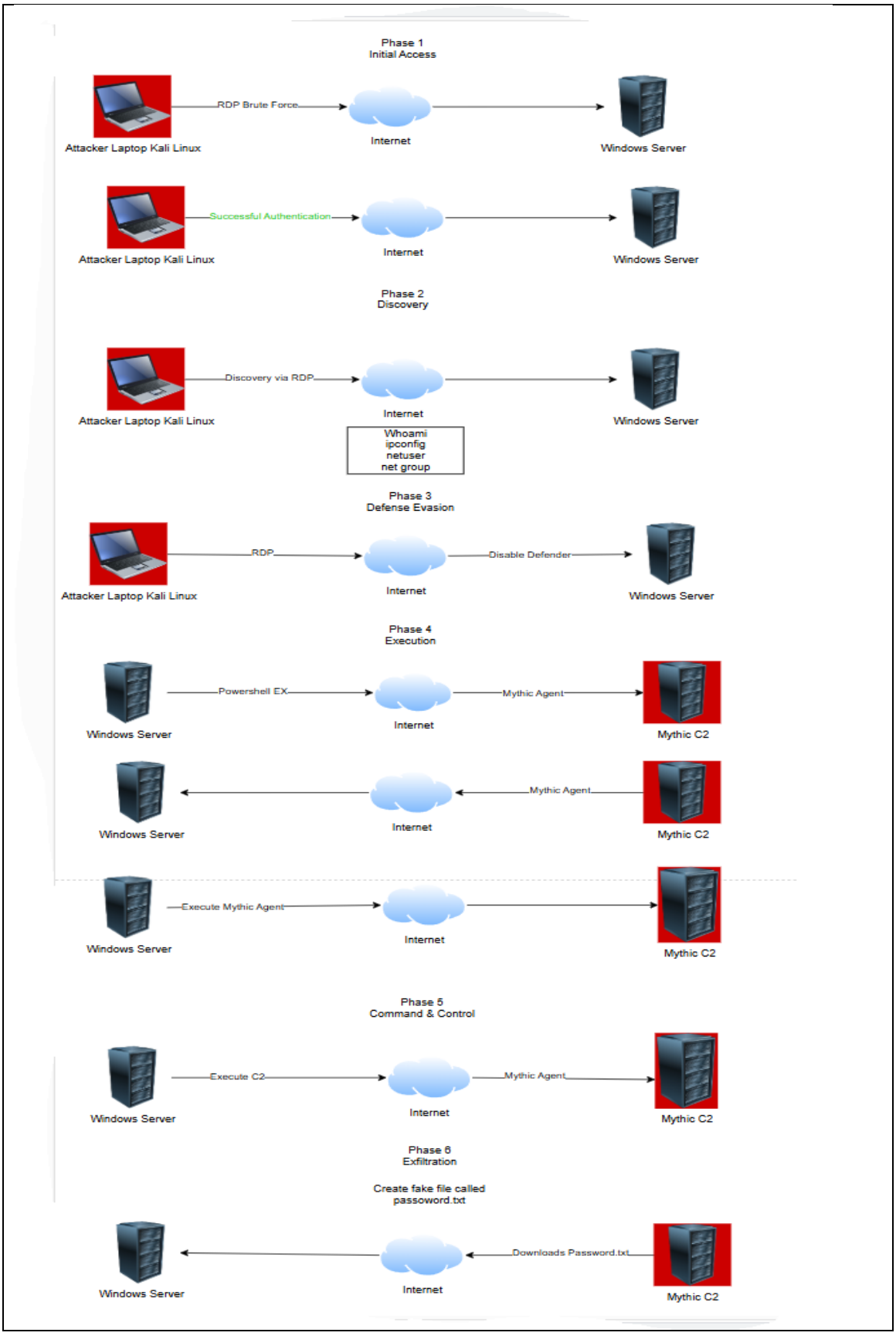
The "30-Day SOC Analyst Challenge" is more than just a learning opportunity - it is a step toward bridging the gap between theoretical knowledge and the demands of the cybersecurity industry. It equips aspiring SOC analysts with the tools, experience, and confidence needed to excel in their careers, fostering a new generation of skilled professionals ready to tackle the ever-evolving challenges of cybersecurity.

As part of the "30-Day SOC Analyst Challenge," we developed a comprehensive logical diagram to serve as the foundation for our SOC environment. This diagram illustrates a carefully designed architecture hosted on a virtual private cloud (VPC) through Vultr, integrating critical components such as Elastic and Kibana for centralized monitoring and log analysis, a Fleet Server for managing and forwarding logs, and managed endpoints including a Windows Server (RDP enabled) and an Ubuntu Server (SSH enabled). Additionally, the setup includes an osTicket server for ticketing and incident management, along with SOC Analyst and Attack laptops to simulate real-world monitoring and adversarial activities. This logical design provided the framework for executing hands-on tasks throughout the challenge, ensuring a realistic and scalable environment for learning SOC analyst skills.



Components of the 30-Day SOC Analyst Challenge:

1. **The ELK Stack**
    a. Overview of the ELK stack (Elasticsearch, Logstash, Kibana).
    b. Setting up the ELK stack in a cloud environment.
    c. Ingesting logs from endpoints, including configuring Sysmon for detailed system monitoring.
2. **Brute Force Attack Detection**
    a. Simulating brute force attacks using SSH and RDP on a public server.
    b. Setting up alerts to detect these attacks in real-time.
    c. Creating dashboards in Kibana for visualizing and monitoring attack patterns.
3. **Command-and-Control (C2) Operations**


Phase 1
Initial Access
RDP Brute Force
Attacker Laptop Kali Linux
Internet
Windows Server
Successful Authentication
Attacker Laptop Kali Linux
Internet
Windows Server
Phase 2
Discovery
Discovery via RDP
Attacker Laptop Kali Linux
Internet
Windows Server
Whoami
ipconfig
netuser
net group
Phase 3
Defense Evasion
RDP
Disable Defender
Attacker Laptop Kali Linux
Internet
Windows Server
Phase 4
Execution
Powershell EX
Mythic Agent
Windows Server
Internet
Mythic C2
Mythic Agent
Windows Server
Internet
Mythic C2
Execute Mythic Agent
Windows Server
Internet
Mythic C2
Phase 5
Command & Control
Execute C2
Mythic Agent
Windows Server
Internet
Mythic C2
Phase 6
Exfiltration
Create fake file called
passoword.txt
Downloads Password.txt
Windows Server
Internet
Mythic C2

a. Understanding command-and-control (C2) server operations.
b. Setting up a C2 server using Mythic to simulate advanced cyber threats.
c. Analyzing attacks against public servers and developing detection strategies.

4. **Incident Management and Investigation**
    a. Integrating a ticketing system for handling and tracking security incidents.
    b. Conducting real-world investigations based on log data, alerts, and attack scenarios.
    c. Applying analytical techniques to understand the nature and impact of incidents.
5. **Cloud-Based Implementation**
    a. Leveraging cloud platforms like Vultr.com for hosting virtual machines and running simulations.
    b. Exploring alternative cloud providers for flexibility and scalability.
    c. Ensuring resource efficiency for running resource-intensive tasks.
6. **Practical Skill Development**
    a. Building and managing a SOC environment using real-world scenarios.
    b. Configuring alerts, dashboards, and workflows to respond effectively to security events.
    c. Developing the expertise required to handle diverse cybersecurity incidents.

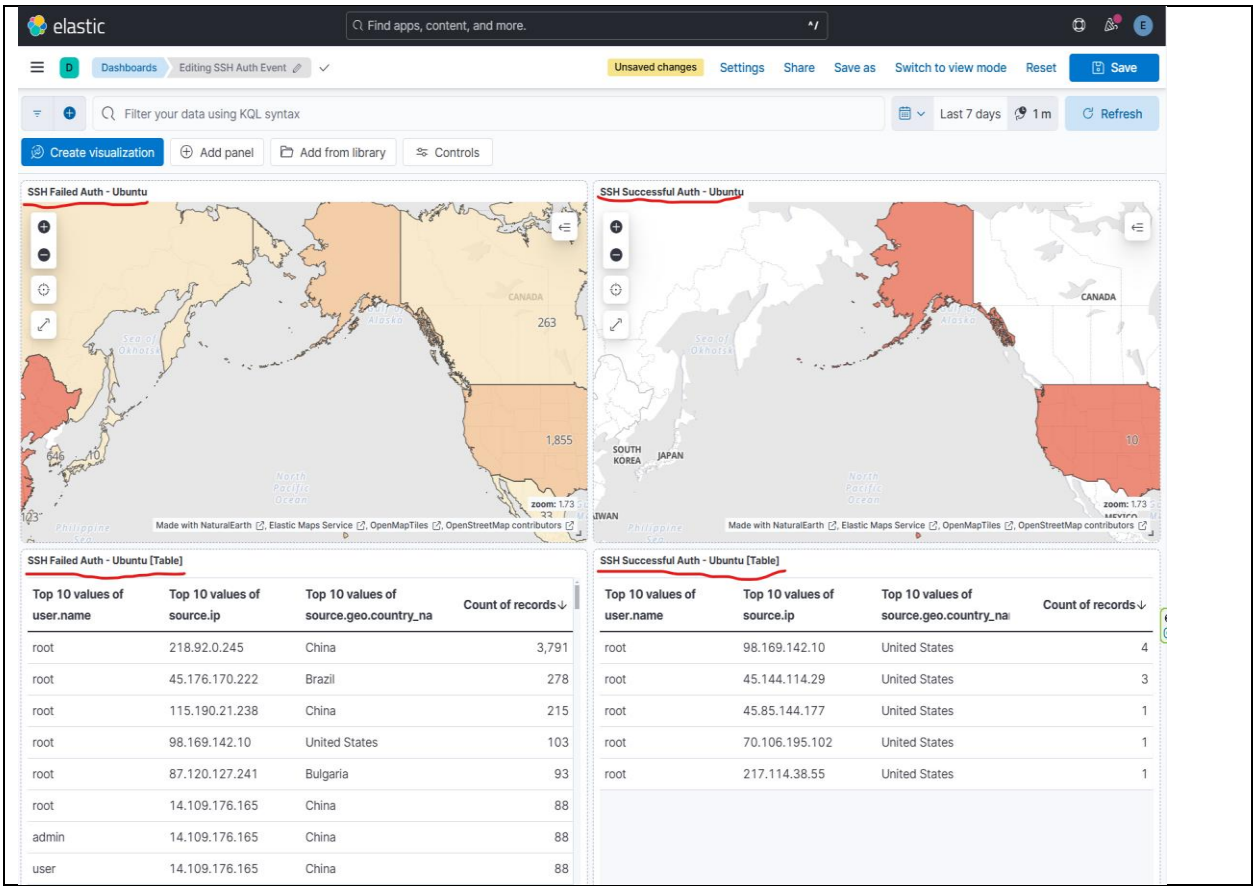
Methodologies, Tools, and Implementation Process:

1. Elasticsearch and Kibana formed the core components of our SOC environment, enabling log ingestion, storage, and analysis.
    - **Elasticsearch** was configured to store large volumes of log data from various sources, providing the ability to query and retrieve information quickly.
    - **Kibana** acted as the visualization layer, offering dashboards, charts, and filtering tools for real-time data monitoring. These tools allowed us to effectively identify security anomalies and generate actionable insights.
2. The Fleet Server served as the centralized management tool for Elastic Agents, streamlining log collection and forwarding to Elasticsearch.
    - By configuring Fleet Server, we enabled endpoint visibility and efficient log ingestion.
    - It also facilitated seamless agent deployment across Windows and Linux environments, reducing manual configuration efforts.
3. Elastic Agents on Windows and Linux
    - **Windows**: Elastic Agents were deployed on a Windows endpoint alongside Sysmon to collect detailed system activity logs.
    - Sysmon provided granular details such as process creation, network connections, and file modifications, which were invaluable for threat detection. Sysmon provided granular details such as process creation, network connections, and file modifications, which were invaluable for threat detection.

- **Linux**: On Linux systems, Elastic Agents ingested logs from the auth.log file, capturing authentication events and other critical security data.
- The integration of Beats modules with Elastic Agents further enhanced our ability to parse and visualize collected data.

1. **Filebeat**
    a. **Purpose**: Collects and forwards log files from various sources, such as system logs or application logs.
    b. **Use Case**: Gathered auth.log from Linux systems to monitor authentication events and detect brute force or unauthorized access attempts.
2. **Metricbeat**
    a. **Purpose**: Collects system and application metrics such as CPU usage, memory, disk I/O, and network traffic.
    b. **Use Case**: Monitored endpoint health and performance for signs of resource exhaustion or anomalies.
3. **Packetbeat**
    a. **Purpose**: Captures network packets and provides insights into protocol-level activity.
    b. **Use Case**: Monitored network traffic to detect unusual patterns, such as suspicious outbound connections.
4. **Winlogbeat**
    a. **Purpose**: Collects Windows event logs.
    b. **Use Case**: Gathered event logs from Windows systems, such as logon events and Sysmon logs, for detailed endpoint activity monitoring.

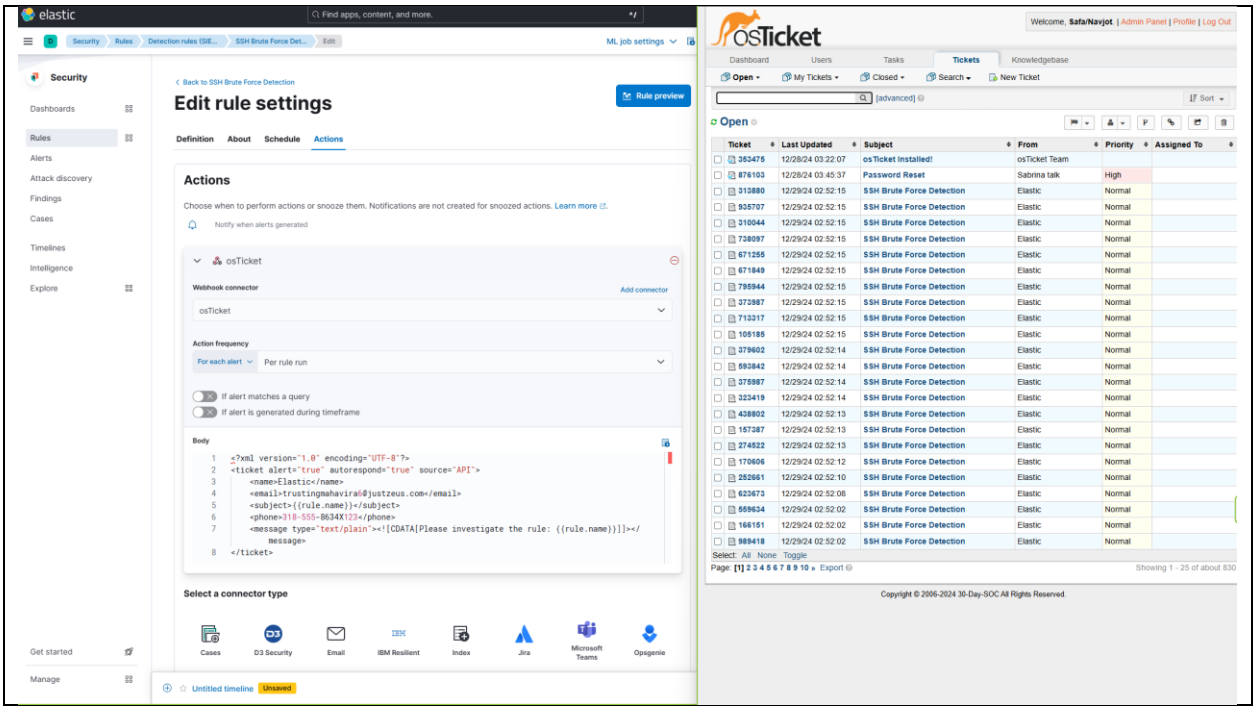
4. Alert and Dashboard Creation



- Alerts were set up to detect specific security events such as SSH brute force attempts and anomalous RDP activity.
- Custom dashboards were created in Kibana using tools like **maps, tables, and filters** for interactive and comprehensive visualization of attack patterns.
- These dashboards provided actionable insights, enabling faster response times during incident investigations.

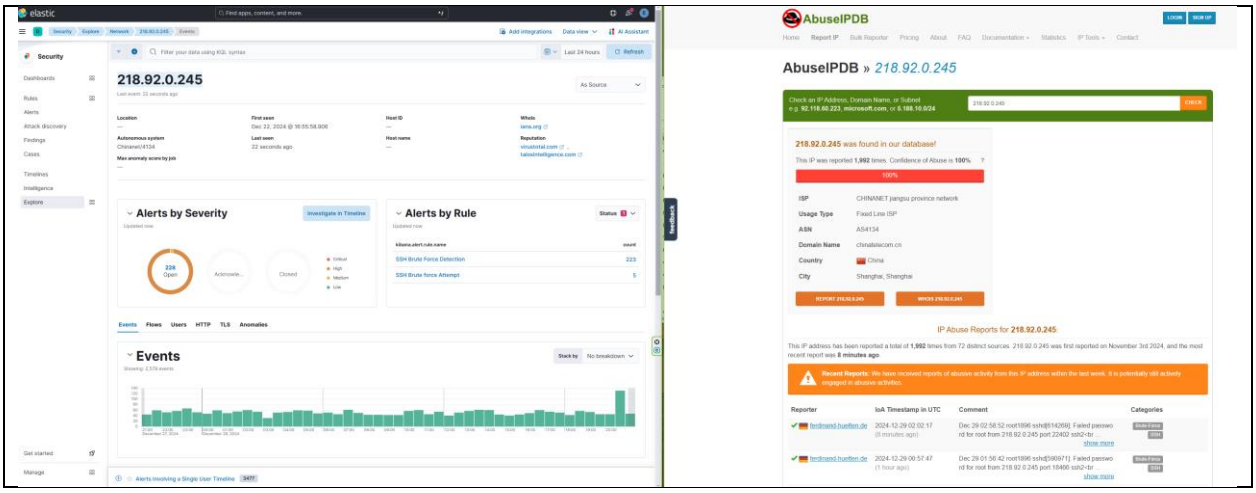
5. **Mythic C2 Framework**: A modular, open-source platform for managing agents (payloads) and communications in red team operations.
   - **Key Functionality**: The Mythic server uses C2 profiles (e.g., HTTP, DNS) to communicate with deployed agents, which execute tasks and send results back securely.

5. **osTicket** is an open-source ticketing system where clients submit tickets via a web portal or email to report issues or requests and track their status with a unique ID. Admins manage tickets by assigning them to agents, configuring workflows, customizing forms, and generating reports to ensure efficient issue resolution and seamless communication.

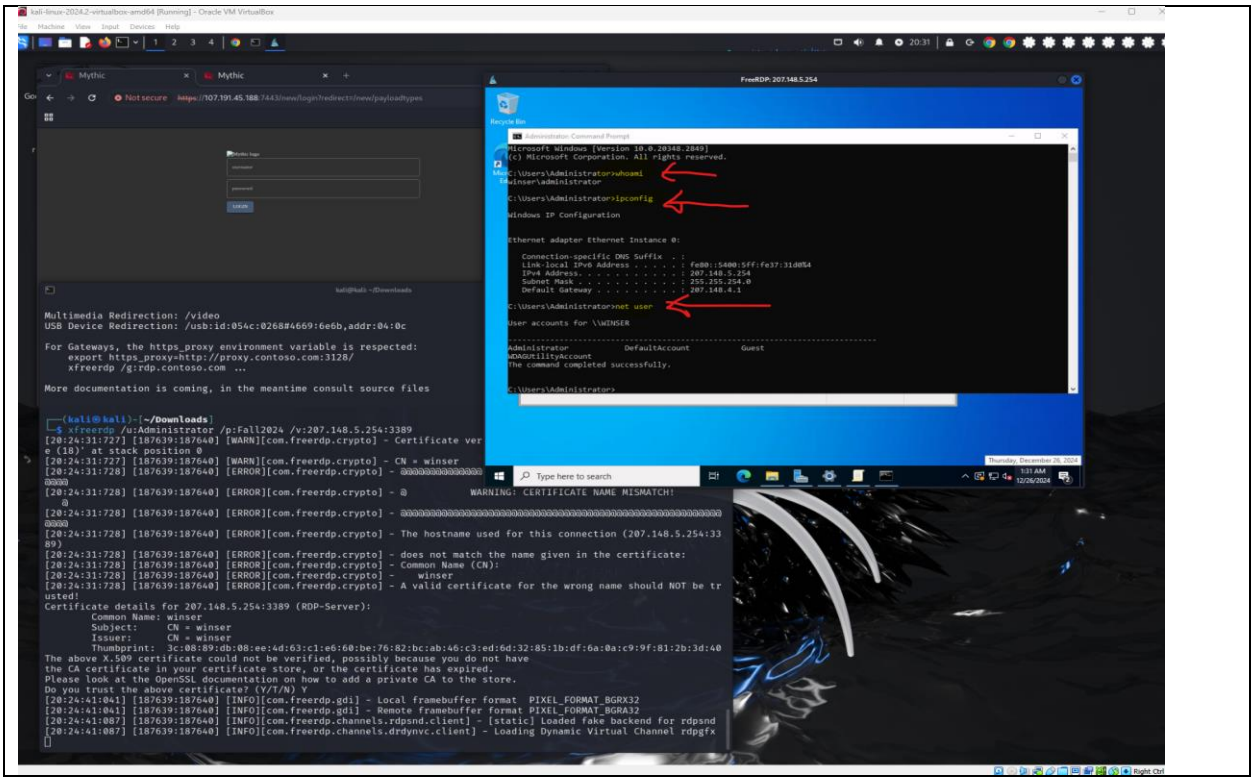


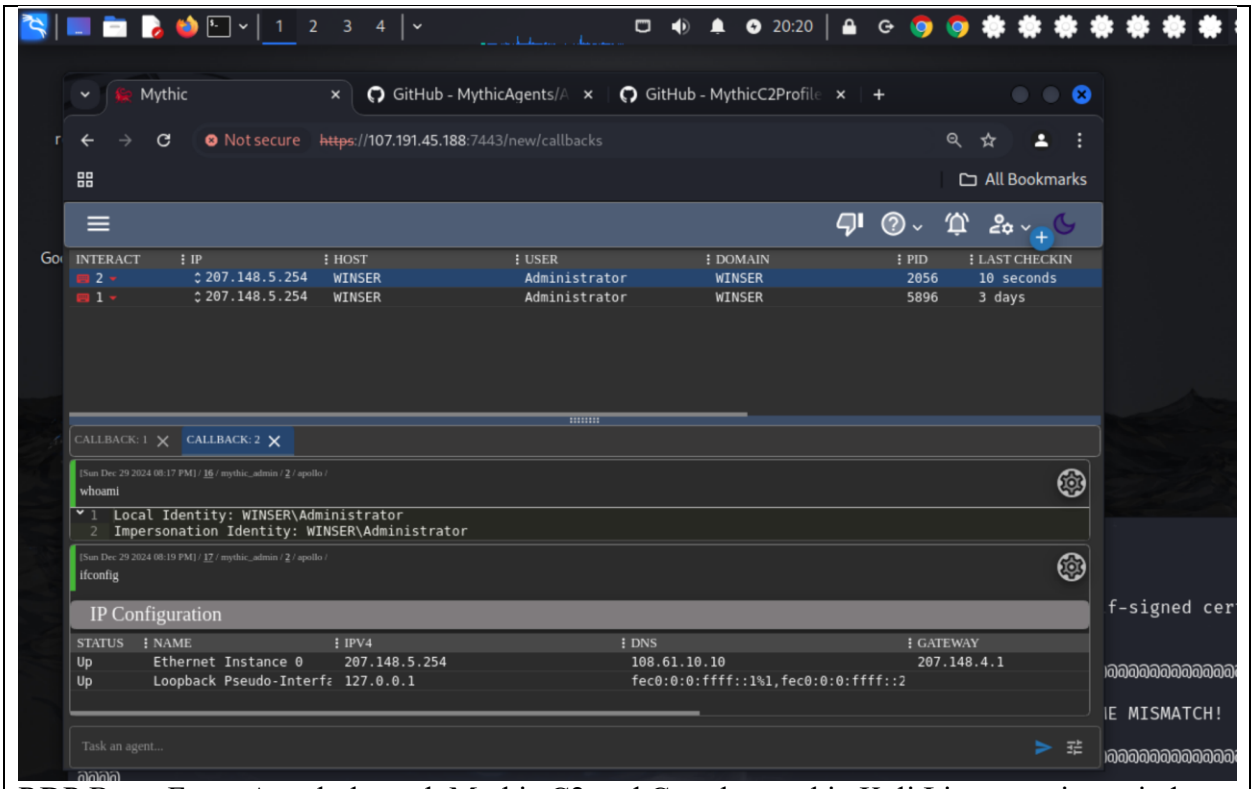
6. **Elastic Defend** is a powerful Endpoint Detection and Response (EDR) solution that provides real-time monitoring, threat detection, and incident response by leveraging the Elastic Stack for data analysis and scalability. It uses lightweight agents to collect telemetry data, enabling proactive threat hunting, automated remediation, and detailed forensics. While Elastic Defend is highly effective, other EDR solutions like CrowdStrike Falcon and Splunk Enterprise Security also offer robust capabilities, each with unique features tailored to different organizational needs, ensuring comprehensive endpoint security.

7. **Threat hunting** is a proactive security practice aimed at identifying hidden threats before they cause harm. It often involves using frameworks like **MITRE ATT&CK**, which classifies adversary tactics, techniques, and procedures (TTPs) to detect suspicious activities. By mapping real-world observations to the framework, threat hunters can recognize attack methods and identify gaps in defenses. Common attack vectors such as SSH (Secure Shell) and RDP (Remote Desktop Protocol) are frequently targeted for lateral movement, and hunters investigate logs for unusual login attempts, failed access attempts, or unauthorized connections, which could indicate a potential breach.



In addition to traditional logs, **MYTHIC C2 logs** provide key insights into potential malicious activities during red team operations or post-exploitation phases. By analyzing Mythic agent logs, security teams can identify anomalies such as unusual agent callbacks or unexpected command execution, which might signal a compromise. Combining this log data with information from MITRE ATT&CK and endpoint analysis enables a comprehensive threat-hunting approach to detect advanced threats, including data exfiltration or privilege escalation, and respond before they escalate into full-scale attacks.





RDP Brute Force Attack through Mythic C2 and Crowbar tool in Kali Linux, against windows OS.

Lessons Learned and Challenges Faced:

The "30-Day SOC Analyst Challenge" provided invaluable hands-on experience in building and managing a fully functional SOC environment. Key lessons included the importance of structured methodologies like the MITRE ATT&CK framework for threat detection, the power of centralized logging and visualization through the ELK stack, and the critical role of incident management tools like osTicket in streamlining operations. Practical exercises in simulating attacks, analyzing logs, and responding to incidents underscored the necessity of real-time monitoring and proactive defense strategies.

However, the challenge was not without its difficulties. One notable challenge was ensuring seamless log ingestion and processing from diverse endpoints while maintaining system performance. Configuring agents and troubleshooting connectivity issues, particularly in cross-platform environments, required persistence and a deep understanding of the tools. Another obstacle was the steep learning curve associated with advanced tools like Mythic C2, and Elastic Defend, which necessitated additional research and practice to master. This challenge reinforced the importance of continuous learning and adaptability in cybersecurity.

Future Enhancements and Scalability:

The SOC lab environment can be enhanced by incorporating advanced automation and machine learning for anomaly detection, enabling faster and more accurate threat identification. Integrating additional threat intelligence feeds can further improve detection capabilities by providing real-time updates on emerging threats. Expanding the lab to include more diverse operating systems, cloud environments, and IoT devices would offer a broader scope for testing and skill development.

Scalability is another critical focus. Leveraging containerized solutions like Docker for deploying SOC components can simplify scaling the environment to accommodate larger networks or additional users. Exploring alternative cloud platforms can enhance flexibility, ensuring the lab can adapt to varying resource requirements. These future improvements will not only strengthen the SOC lab's capabilities but also prepare SOC environments for the rapidly evolving landscape of cybersecurity challenges.