DEPI Final Project Documentation || *ACTIVE DIRCTORY* Prototype

1- Introduction

This project simulates a small network environment designed for incident response and security monitoring, utilizing an **Active Directory** server and a **Windows 10 client**. Both systems are equipped with **Splunk Universal Forwarder** and **Sysmon** for detailed log collection, enabling comprehensive monitoring of system and network activities. All collected logs are centralized on a **Splunk Server** for real-time analysis and threat detection.

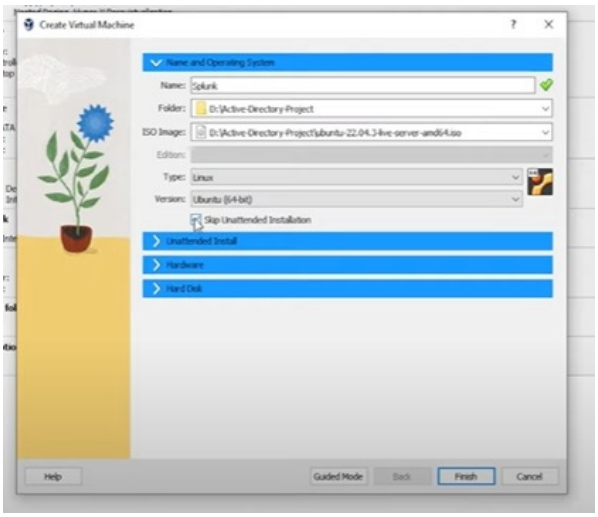
To simulate potential security threats, a **Kali Linux** machine is used as the attacker, mimicking various attack vectors against the network. This environment focuses on detecting and responding to security incidents, leveraging Splunk's powerful capabilities for monitoring, alerting, and forensic investigation.

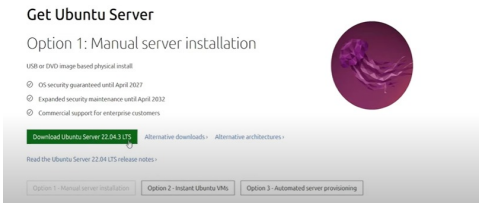
The setup provides a practical approach to enhancing security through active monitoring and the ability to swiftly identify and respond to any suspicious activity within the network.

2- Environment Setup

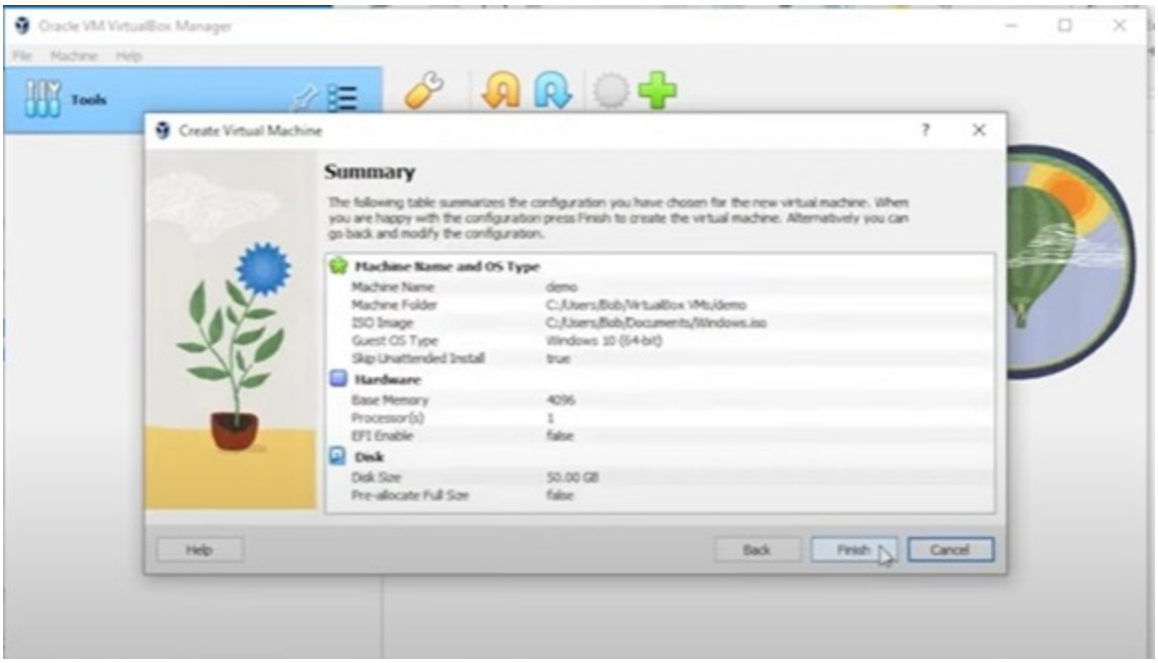
For the ***ACTIVE DIRCTORY*** project, multiple systems were configured to simulate attacks and monitor them using Splunk. The environment consists of:

1. **Ubuntu Server with Splunk Installed**:
    - The Ubuntu Server acts as the central logging hub, where Splunk is installed to aggregate logs from the connected systems. This server is responsible for collecting and analyzing logs in real-time, allowing security teams to monitor and investigate login attempts across the network.

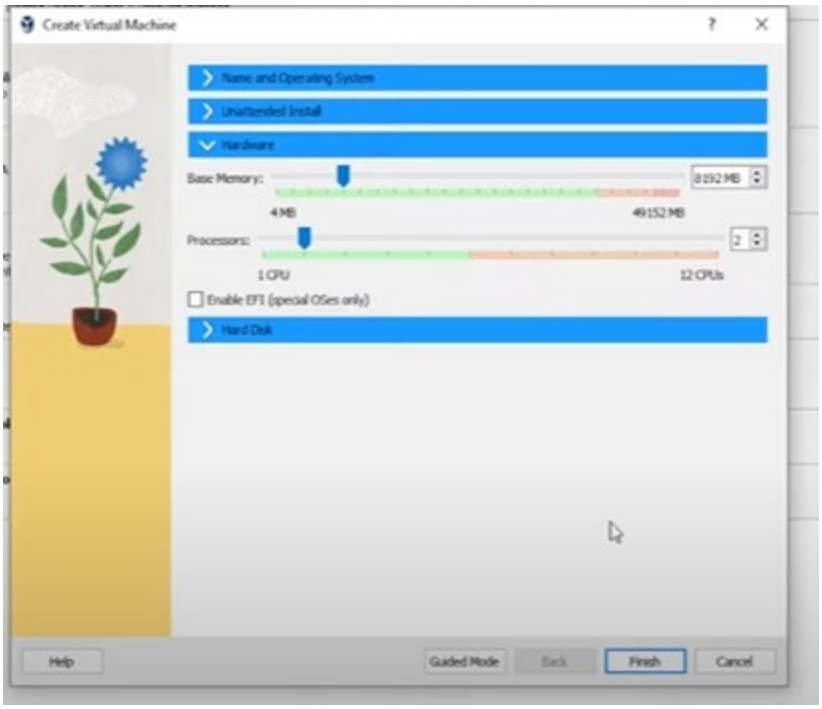




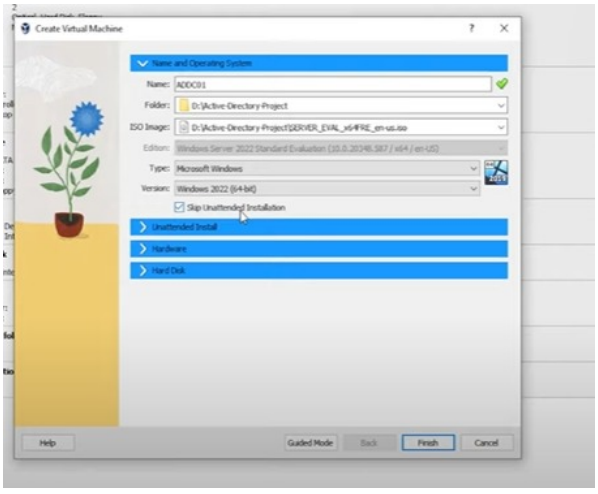
1. **Target PC (Windows 10) with Splunk Installed**:
    - The Windows 10 machine serves as the primary target for the brute force attack simulation. By installing Splunk, this PC captures essential security logs such as failed login attempts and user authentication errors, which are sent to the central server for analysis.

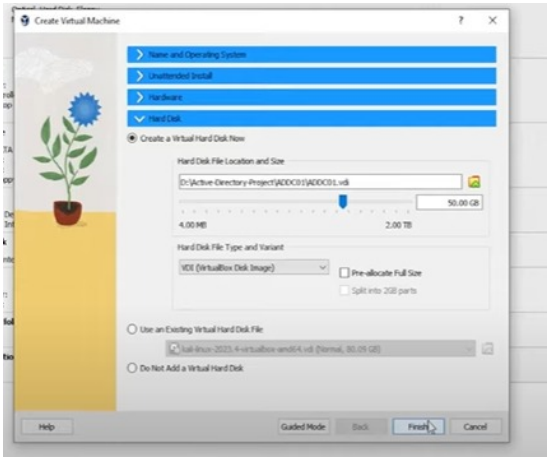


2. **Attacker PC (Kali Linux)**:
    - The attacker machine runs **Kali Linux**, a penetration testing distribution. This machine is used to simulate brute force attacks on the Windows 10 target and the Ubuntu server. Tools like **Crowbar** are utilized to perform automated credential-guessing attacks, allowing for a realistic simulation of attack scenarios.



3. **Windows Server with Splunk Installed**:
    - The Windows Server is used to monitor login attempts and collect logs related to administrative access and system events. These logs are crucial for identifying potential brute force attack vectors and unauthorized access attempts within the network.





- Data Collection:

- **Authentication Logs**:
  - From both the Windows 10 target machine and the Windows Server, logs of successful and failed login attempts are collected.
- **System Security Events**:
  - This includes logs related to unauthorized access attempts, login failures, and abnormal login behaviors.

- Data Flow:

- Logs from the Windows 10 target and the Windows Server are continuously forwarded to the Ubuntu server where Splunk is installed. The data is processed in real-time, allowing the detection of brute force attack attempts as they occur.
- This multi-system setup creates an effective environment for detecting and analyzing brute force attack scenarios, providing valuable insights into the attack methods and security responses.

- Used Software:

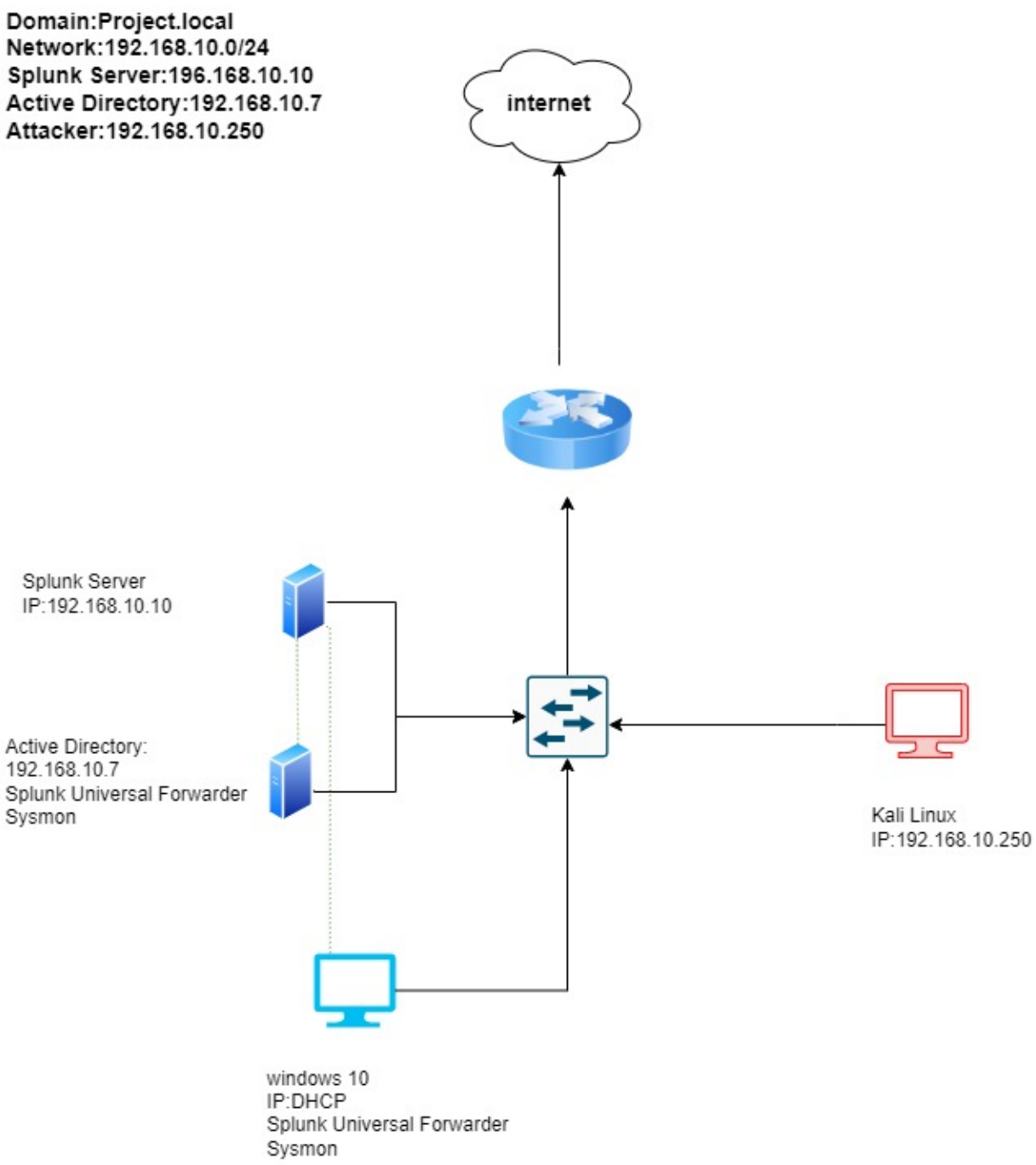
- Virtual Box
- Splunk
- Crowbar
- NMap
- Windows Server 2022
- Ubuntu Server
- Windows 10
- Kali Linux
- Draw. io

3-Installation Steps and Guide

Network Configuration

The network used for this project is **192.168.10.0/24**, with the following machines and their IP addresses:

- **Splunk Server (Ubuntu)**: `192.168.10.10`
- **Active Directory (Windows Server)**: `192.168.10.7`
- **Target PC (Windows 10)**: `192.168.10.100`
- **Attacker Machine (Kali Linux)**: `192.168.10.250`



1. Installation and Configuration of Ubuntu Server with Splunk

1.1 Ubuntu Server Installation

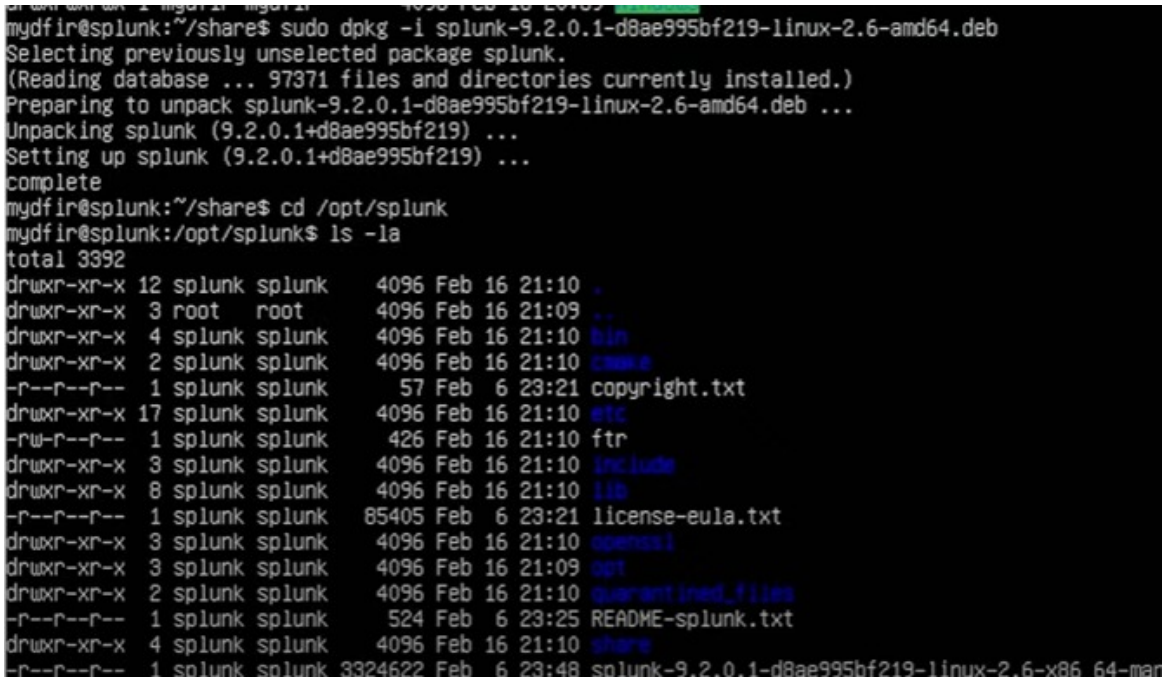
1. **Virtual Machine Setup**:

- A new virtual machine was created using **VirtualBox**. The VM was configured with **8 GB of RAM**, **2 CPU cores**, and **100 GB** of dynamically allocated storage. The operating system was set to **Ubuntu (64-bit)**.
- The **Ubuntu Server ISO** was attached, and the installation began.

2. **Ubuntu Installation**:
   - Selected language, keyboard layout, and region during installation.
   - Configured the network manually:
     - **IP Address**: `192.168.10.10`
     - **Subnet Mask**: `255.255.255.0`
     - **Gateway**: `192.168.10.1`
   - Created a user account and opted to install the OpenSSH server for remote access.
   - Completed installation and rebooted the server.

1.2 Splunk Installation on Ubuntu Server

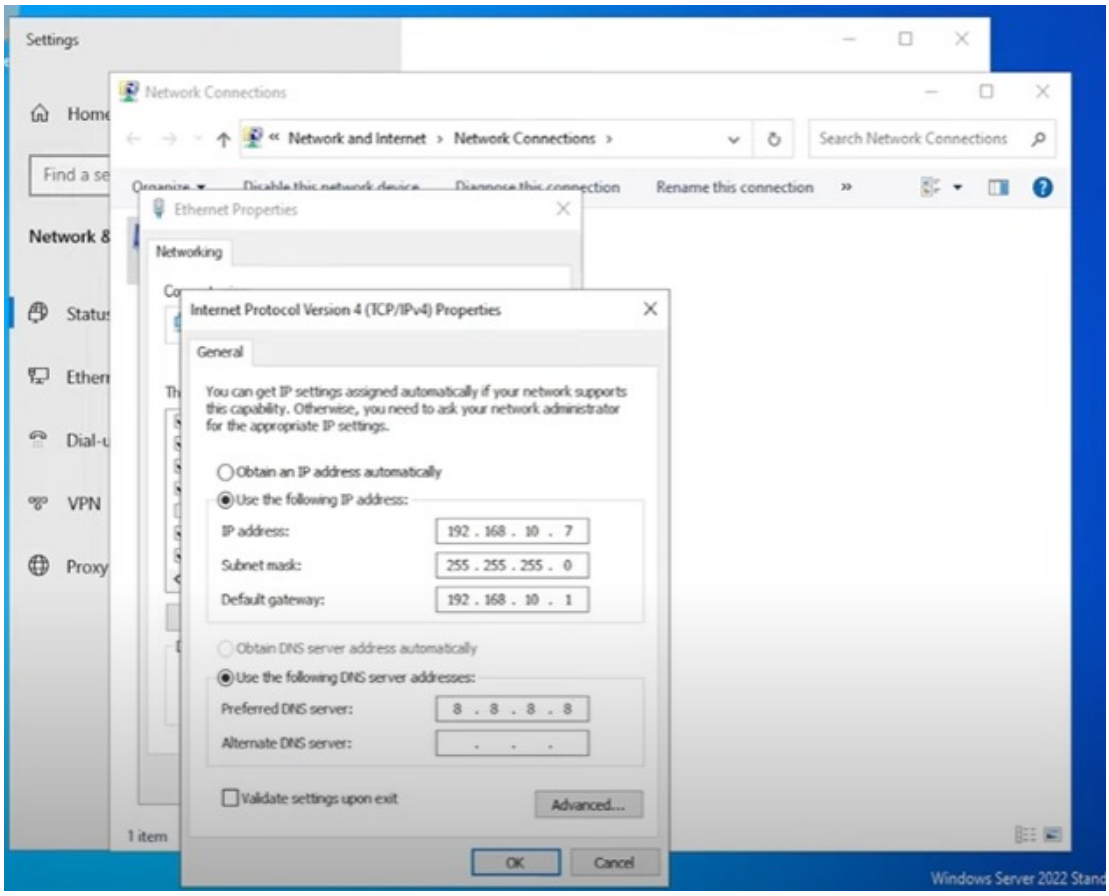
1. **Download Splunk**:
   - Splunk was downloaded using `wget` directly to the Ubuntu machine.
2. **Install Splunk**:
   - The downloaded Splunk package was installed using the `dpkg` command.
3. **Start Splunk**:
   - Splunk was started with the `sudo /opt/splunk/bin/splunk start` command, and the license agreement was accepted.
4. **Access Splunk Web Interface**:
   - The Splunk web interface was accessed from `http://192.168.10.10:8000` using the `admin` credentials.



2. Installation and Configuration of Windows Server with Splunk

2.1 Windows Server Installation

1. **Virtual Machine Setup**:
   - A new VM was created in **VirtualBox** with **4 GB of RAM**, **1 CPU core**, and **50 GB** of dynamically allocated storage. The **Windows Server 2022 ISO** was attached to the VM.
2. **Windows Server Installation**:
   - Installed **Windows Server 2022**, selecting language, region, and creating a new administrator account.
3. **Network Configuration**:
   - Configured the network settings manually:
     - **IP Address**: `192.168.10.7`
     - **Subnet Mask**: `255.255.255.0`
     - **Gateway**: `192.168.10.1`
     - **DNS**: Configured to point to the local domain or `8.8.8.8`



2.2 Splunk Installation on Windows Server

1. **Download Splunk**:
   - Downloaded the **Splunk Windows Installer** from the official website.
2. **Install Splunk**:
   - Ran the installer and completed the setup by following the on-screen instructions.
3. **Start Splunk**:
   - After installation, Splunk was started, and the web interface was accessed through `http://192.168.10.7:8000`.
4. **Active Directory Configuration**:
   - Active Directory Domain Services (AD DS) were installed and configured, and the server was promoted to a domain controller.

---

3. Installation and Configuration of Target Machine (Windows 10) with Splunk

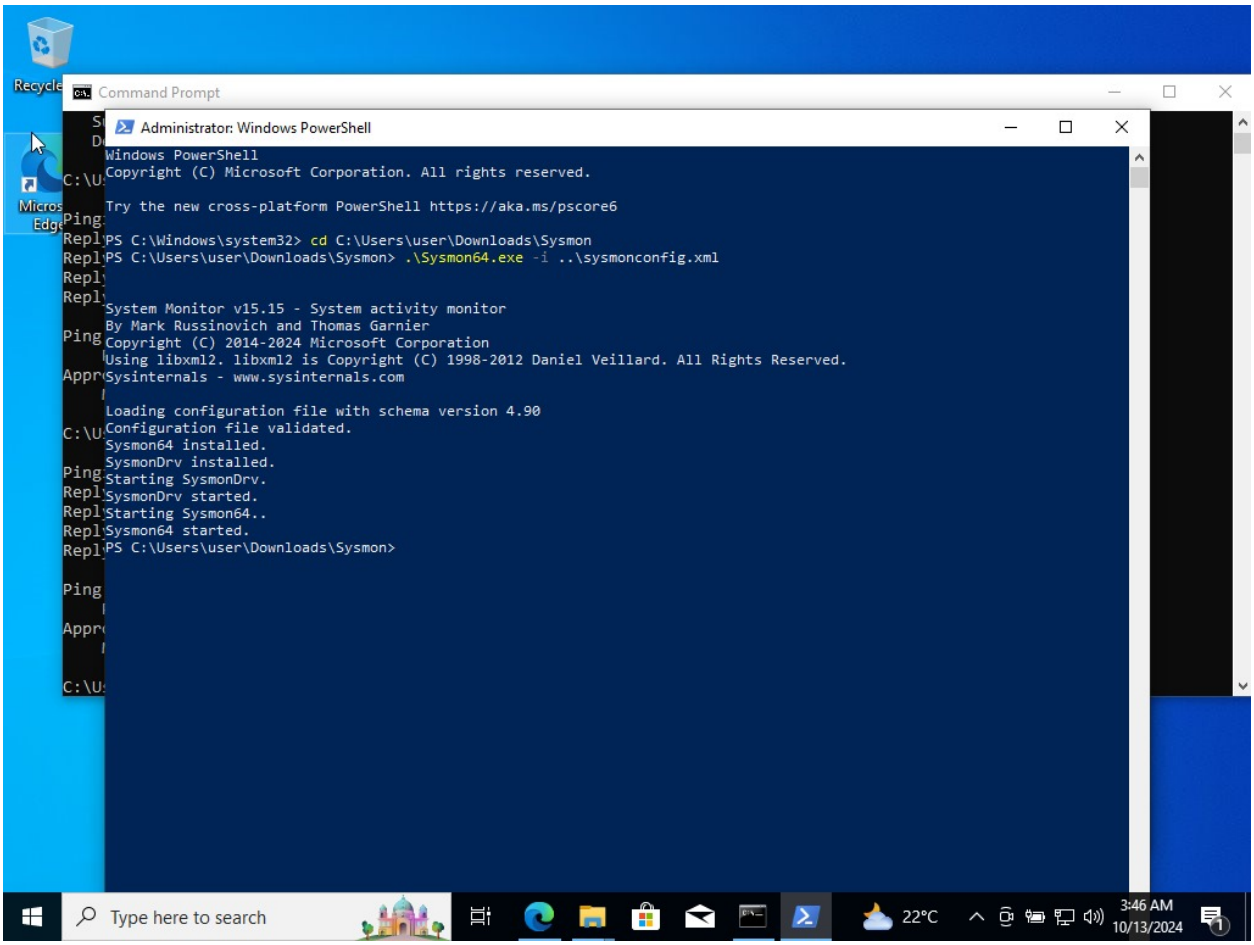
3.1 Windows 10 Installation

1. **Virtual Machine Setup**:
   - A new virtual machine was created with **Windows 10** ISO, allocating **4 GB of RAM**, **1 CPU core**, and **50 GB** of storage.
2. **Windows 10 Installation**:
   - Installed **Windows 10**, configured regional settings, and created a local administrator account.
3. **Network Configuration**:
   - Configured the network settings manually:
     - **IP Address**: `192.168.10.100`
     - **Subnet Mask**: `255.255.255.0`
     - **Gateway**: `192.168.10.1`
     - **DNS**: Used `192.168.10.7` (Active Directory Server) for domain-related activities.

3.2 Splunk Installation on Windows 10 (Target Machine)

1. **Download Splunk**:
   - Downloaded the **Splunk Windows Installer** from the official website.
2. **Install Splunk**:
   - Installed Splunk by following the installation wizard.
3. **Start Splunk**:
   - After installation, Splunk was started and accessed via `http://192.168.10.20:8000`.

3.3 Sysmon and Splunk Integration Installation on Both Windows Server and target:



The integration of **Sysmon** and **Splunk** provides comprehensive monitoring and detection of security events within the network. This setup helps in identifying potential threats and assists in incident response.

1. Sysmon (System Monitor)

Function:

Sysmon is a Windows system service and driver that logs critical system activity, including:

- **Process creation and termination**
- **Network connections**
- **File creation and modification**

- **Registry changes**

Why Use Sysmon:

- Provides **detailed logs** on endpoint behavior (e.g., on the Active Directory server and Windows 10 client).
- Detects suspicious activities like **malware execution**, **privilege escalation**, and **lateral movement** across the network.

2. Splunk

Function:

Splunk is a Security Information and Event Management (SIEM) platform that:

- Collects, indexes, and analyzes logs from multiple sources.
- Provides **real-time monitoring** and alerts based on the collected log data.

Why Use Splunk:

- **Centralizes log collection** from all endpoints, simplifying network monitoring.
- Correlates log data to detect security incidents such as **brute force attacks**, **malware infections**, and abnormal activities.
- Assists in **forensic analysis** and **incident response** by providing insights into the logs.

3. Sysmon and Splunk Integration

- **Log Forwarding:** The **Splunk Universal Forwarder** is installed on the Active Directory and Windows 10 machines to send Sysmon logs to the central Splunk server.

Benefits of Integration:

- **Real-time Monitoring:** Logs from Sysmon are continuously sent to Splunk for real-time analysis.
- **Threat Detection:** Splunk’s powerful search and alerting capabilities help detect security incidents from Sysmon’s detailed logs.

- **Incident Response:** Sysmon logs provide in-depth details about the system activities, crucial for investigating and responding to incidents. Splunk's interface allows for efficient querying and visualization of this data.

4. Installation and Configuration of Kali Linux for Brute Force Attack Testing

4.1 Kali Linux Installation

1. **Virtual Machine Setup**:
   - A virtual machine was created using **VirtualBox** with **4 GB of RAM**, **1 CPU core**, and **50 GB** of dynamically allocated storage. The **Kali Linux ISO** was attached to the virtual machine.
2. **Kali Linux Installation**:
   - Configured the following settings during installation:
     - **Language**: English.
   - The network was manually configured:
     - **IP Address**: `192.168.10.250`
     - **Subnet Mask**: `255.255.255.0`
     - **Gateway**: `192.168.10.1`
     - **DNS**: `8.8.8.8`.
3. **Post-Installation**:
   - After installation, the system was updated by running:

     ```
     sudo apt update && sudo apt upgrade
     ```

   - Verified the network configuration by using:

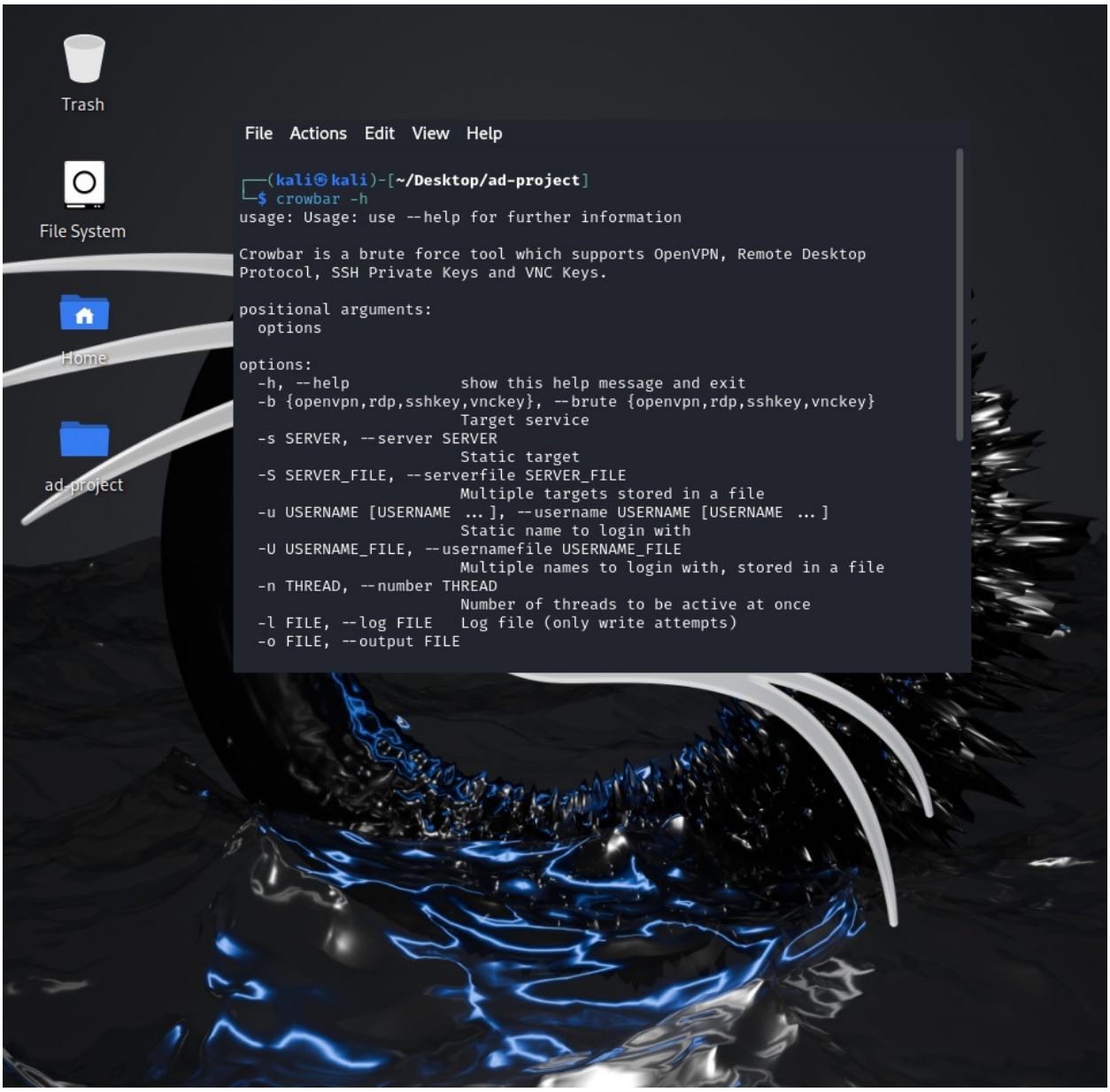
     ```
     ifconfig
     ```

- Confirmed connectivity with other devices by pinging the **Splunk Server (192.168.10.10)** and the **Target Machine (192.168.10.100)**.

4.2 Brute Force Attack Simulation Using Kali Linux (Crowbar)

1. **Install Crowbar**:
   - **Crowbar** is a tool used for brute-forcing services like **RDP** or **SSH**. It comes pre-installed with **Kali Linux**, but if necessary, it can be installed using:

     ```
     sudo apt install crowbar
     ```



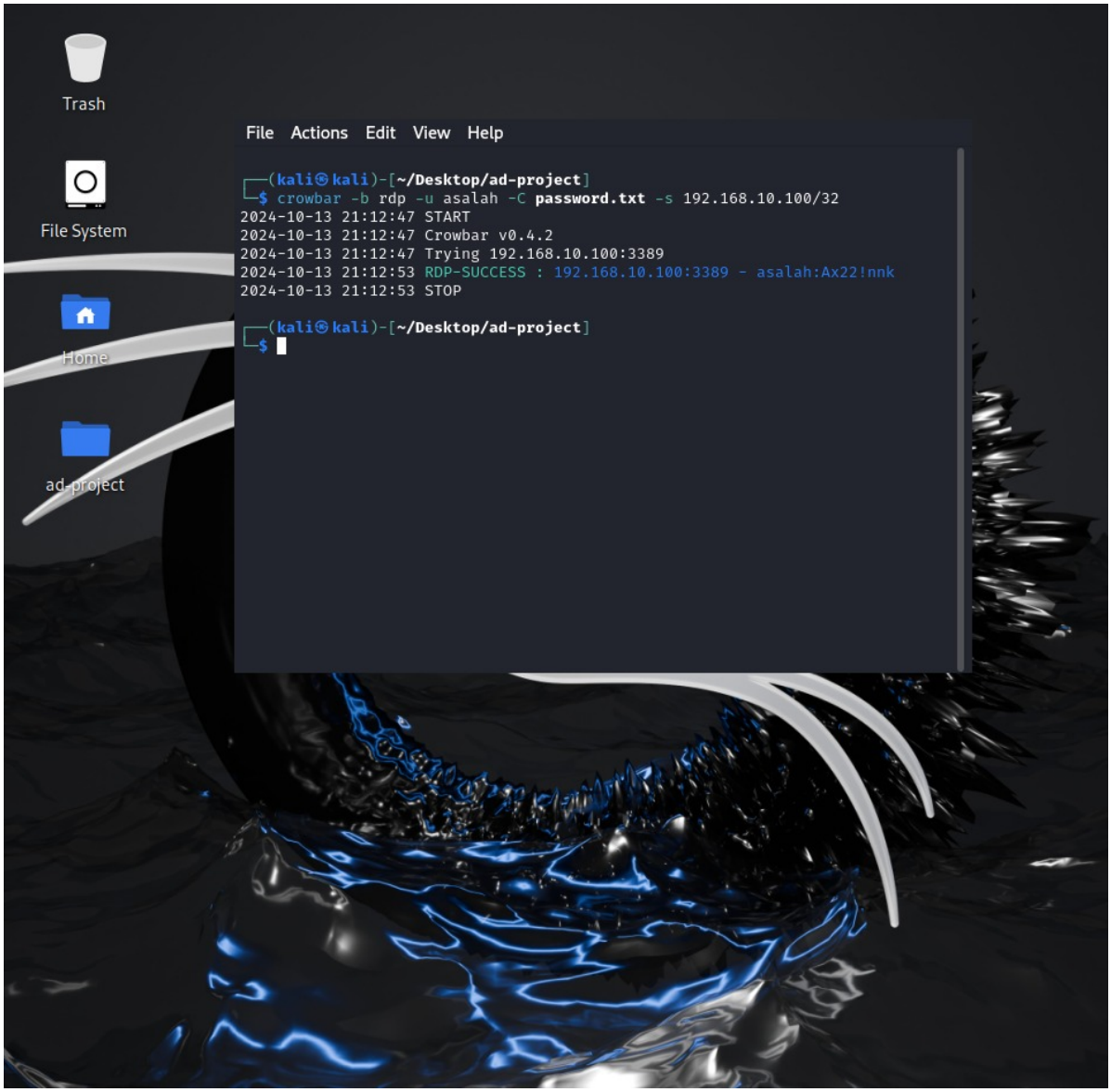
1. **Identify Target Machines**:
    - Used **nmap** to scan the network and identify the active machines and open services:

      ```
      nmap -sS 192.168.10.0/24
      ```

    - This scan helped identify the **Target PC (192.168.10.100)** and **Windows Server (192.168.10.7)** with open RDP ports.

2. **Launch Brute Force Attack Using Crowbar**:
    - **Crowbar** was used to attempt brute force attacks on the **RDP** service of the **Windows Target (192.168.10.100)**. The attack was launched with a dictionary of passwords:

```
crowbar -b rdp -s 192.168.10.100/32 -u admin -C passwor
ds.txt
```



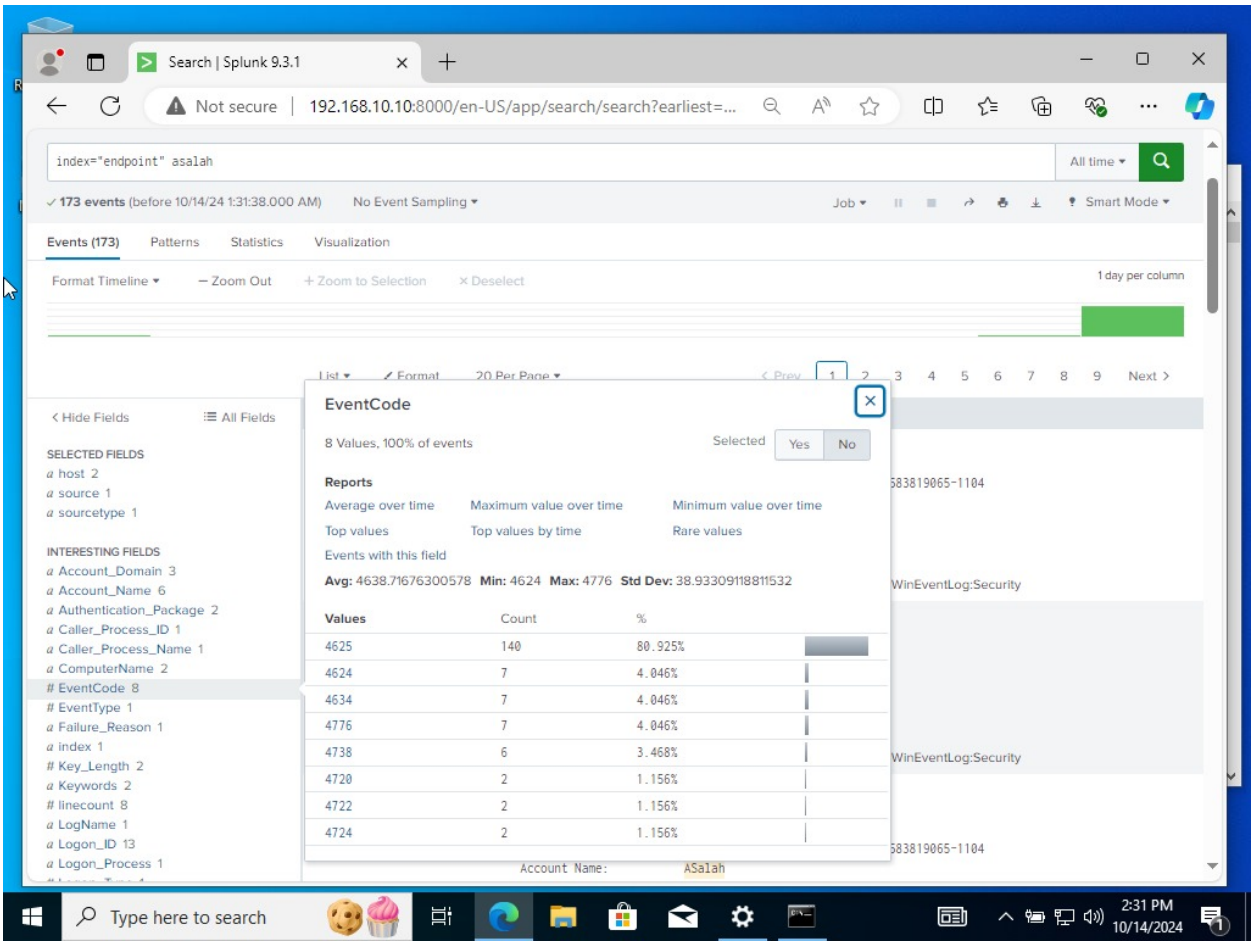
- In this example:

- `b rdp`: Specifies the RDP protocol.
- `s 192.168.10.100/32`: Defines the target IP address.
- `u admin`: Specifies the username to attack.
- `C passwords.txt`: Defines the path to the password list.

3. **Monitor Brute Force Attempts via Splunk**:
   - As the attack proceeded, **Splunk** monitored real-time logs generated by failed login attempts from the **Kali Linux (192.168.10.250)** machine.
   - Splunk was configured to alert the administrator when repeated failed logins occurred, indicating potential brute force attacks.

5- Monitoring and Analyzing Brute Force Activity with Splunk

5.1 Configuring Splunk for Monitoring



1. **Log in to Splunk**:
   - Open a browser and go to `http://192.168.10.10:8000`.
   - Enter your **Splunk admin** credentials to access the dashboard.
2. **Data Input Setup**:
   - Navigate to **Settings** > **Data** > **Data Inputs**.
   - Add new data sources to capture logs from:
     - **Windows 10 Target PC**: Monitor the **Security Event Log** to capture login activities.
     - **Windows Server**: Collect logs for monitoring administrative access and login events.
     - **Ubuntu Server**: Monitor `/var/log/auth.log` for failed SSH login attempts.

3. **Creating an Alert for Failed Login Attempts**:
    - Go to **Settings** > **Searches, Reports, and Alerts** > **Create Alert**.
    - Define a **search query** to capture failed login attempts:

```
index=your_index sourcetype=your_sourcetype "failed log
in" OR "authentication failure"
```

    - Set conditions for triggering the alert, such as the **threshold** for failed attempts (e.g., more than five failed attempts in five minutes).
    - Configure the alert to send an email or trigger other actions like logging the event or blocking IP addresses.

5.2 Analyzing Brute Force Attempts

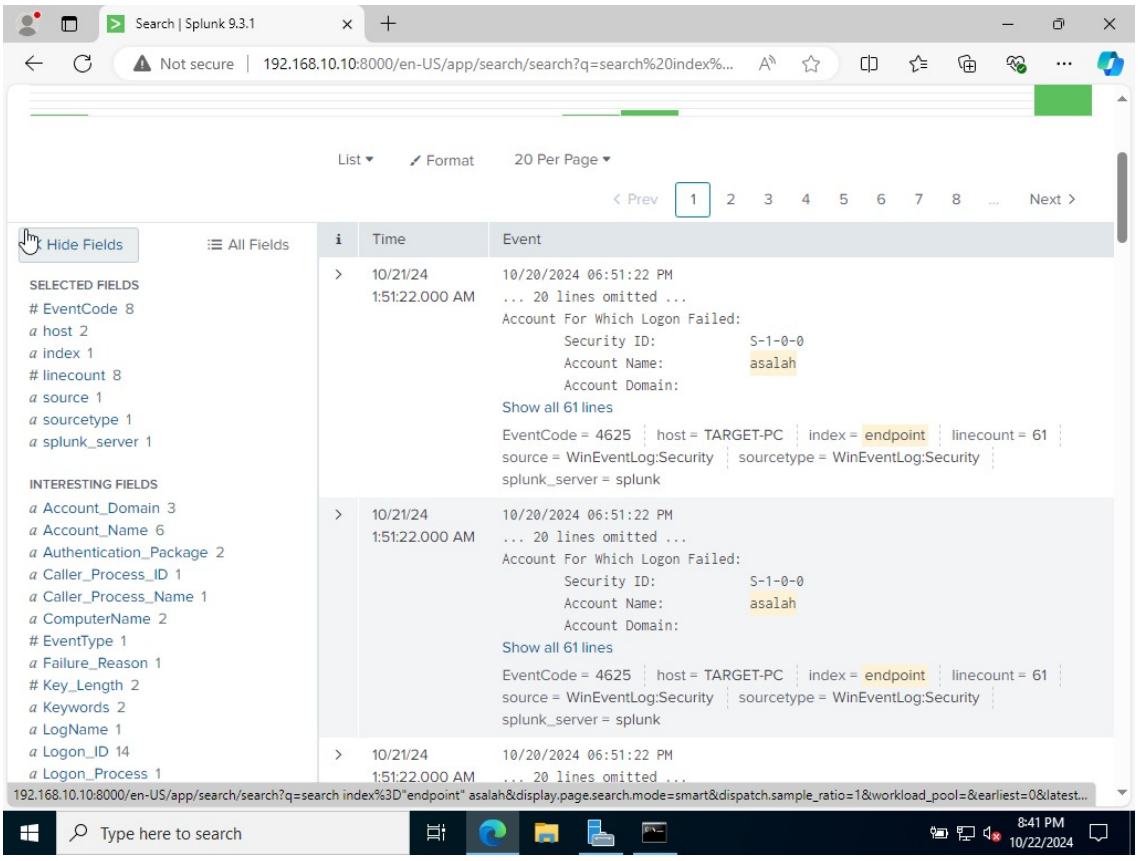
1. **Searching for Attack Patterns**:
    - Use Splunk's search bar to analyze failed login events:

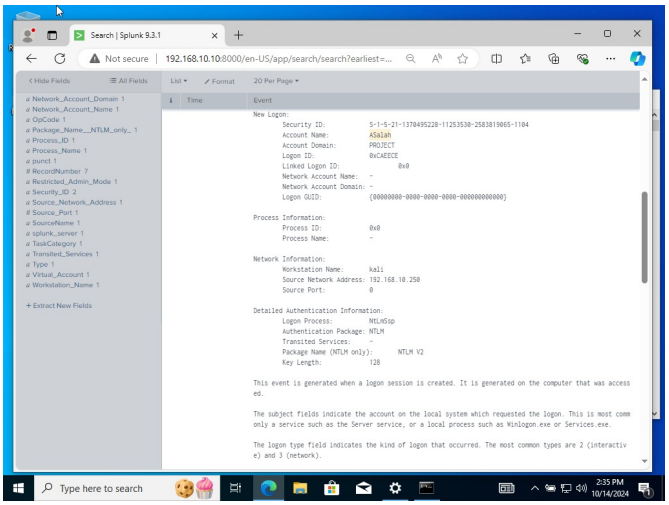
```
index=your_index sourcetype=your_sourcetype "failed log
in" OR "authentication failure"
```

    - This helps identify:
        - IP addresses of the attacker.
        - Targeted usernames.
        - Frequency and timing of the attempts.
2. **Create Dashboards for Visualization**:
    - Create a Splunk dashboard to visually track failed login attempts.
    - Add panels for:
        - **Top attacking IP addresses**.
        - **Top targeted usernames**.
        - **Total failed login attempts**.

- This provides a clear visual representation of brute force activity over time, helping to quickly detect active attacks.

3. **Investigating Alerts**:
   - When an alert is triggered, review the logs for further investigation.
   - Focus on:
     - The **IP addresses** attempting the attack.
     - The specific **usernames** targeted.
     - The **timeline** and frequency of attempts.
4. **Generate Reports**:
   - Use Splunk to generate periodic reports summarizing brute force activity.
   - Include:
     - Total number of attempts.
     - Targeted accounts.
     - Identified IP addresses and their geographic location (if applicable).





6- Incident Response and Remediation

6.1 Responding to Brute Force Attempts

1. **Immediate Response**:

- Upon receiving a brute force attack alert, perform these actions:
    - Review the **alert logs** for specific details (failed attempts, IP addresses, targeted users).
    - Check if any successful logins occurred after the failed attempts.

2. **Identify the Attack Source**:
    - Use tools like `traceroute` or `whois` to trace the attack's origin.
    - Determine if the IP is known to be malicious or if it's internal traffic.
3. **Isolate Affected Systems**:
    - If an attack is ongoing or a system is compromised, isolate it by:
        - **Disabling the network interface** on the affected machine.
        - Restricting access to sensitive services or files.

6.2 Mitigation Actions

1. **Account Lockout Policies**:
    - Implement policies to lock user accounts after repeated failed login attempts. This can reduce the success of brute force attacks.
2. **Enhance Password Security**:
    - Enforce strong password policies requiring complexity and periodic changes.
    - Introduce **two-factor authentication (2FA)** for all users to add an extra layer of security.
3. **Strengthen Network Defenses**:
    - Ensure firewalls are configured to restrict access to sensitive services (like SSH or RDP).
    - Deploy **intrusion detection systems (IDS)** and **intrusion prevention systems (IPS)** to monitor and block unusual traffic patterns.
4. **Regular Security Protocol Reviews**:
    - Conduct regular reviews of security protocols and update them as needed.

- Perform routine vulnerability assessments and penetration testing to identify and fix weaknesses.

6.3 Post-Incident Review and Documentation

1. **Root Cause Analysis**:
   - After the immediate threat is neutralized, conduct an in-depth analysis to determine how the attack occurred.
   - Review logs to track patterns, methods used, and any vulnerabilities exploited.
2. **Incident Documentation**:
   - Document the entire incident, including:
     - Timeline of events.
     - Response actions taken.
     - Lessons learned.
   - This documentation helps improve future responses and security strategies.
3. **Training and Awareness**:
   - Educate staff on identifying security threats like phishing attempts.
   - Raise awareness of the importance of password security and following best practices for system access.

7- Development Plans

In the next phase of the **Brute Force Attack** project, the primary goal is to expand and refine the detection capabilities by adding new, more advanced alerting mechanisms. These improvements will help strengthen the network's defenses against brute force attacks and other potential threats.

7.1 Implementing Advanced Brute Force Attack Alerts

One of the main future objectives is to design and configure specialized alerts to detect brute force attacks with greater accuracy and efficiency. While the current system monitors basic failed login attempts, the next stage will involve creating a dedicated **Brute Force Attack Alert** that uses more advanced techniques to identify potential threats.

Steps for Implementation:

1. **Threshold-Based Alerting**:
   - Set up a custom **Brute Force Attack Alert** to monitor multiple failed login attempts within a specific time window (e.g., more than 5 failed login attempts in 1 minute from a single IP address).

   Example search query for the alert:

   ```
   index="endpoint" sourcetype="WinEventLog: Security" EventCode
   ```

   ```
   index=your_index sourcetype=your_sourcetype "failed login"
   | stats count by src_ip, user
   | where count > 5
   ```

2. **Machine Learning and Predictive Analysis**:
   - Explore the possibility of using **machine learning** models within Splunk to predict potential brute force attacks based on patterns in the logs. This would involve analyzing historical data to identify unusual login behavior.
3. **Geo-IP Alerting**:
   - Add **geolocation-based alerts** to detect login attempts from unexpected or suspicious regions. For example, if login attempts come from a region outside the typical operational areas of the network, an alert can be triggered.
4. **Integration with Other Security Tools**:
   - Integrate Splunk with additional **security tools** such as **firewalls** or **intrusion prevention systems (IPS)** to automatically block IP addresses after a certain threshold of failed login attempts is reached.

7.2 Expanding Coverage for Different Attack Vectors

To further strengthen the system, future plans will include monitoring for additional attack vectors:

- **SSH Brute Force Attacks**: Enhancing the existing alert system to detect brute force attacks against **SSH** services on the **Ubuntu Server**.
- **RDP Brute Force Detection**: Adding alerting capabilities to identify brute force attempts on **RDP** connections to the **Windows Server**.

7.3 Continuous Improvement and Updates

As part of the ongoing development, the team will regularly review and update the detection rules and alerting mechanisms to ensure they remain effective against evolving threats. Additionally, new Splunk apps and add-ons may be integrated to enhance performance and security.

By implementing these future plans, the system will be better equipped to detect and respond to brute force attacks, providing a more secure environment for all connected systems.

8- Troubleshooting

During the development of the **Brute Force Attack Alert** project using Splunk, an issue was encountered related to the Splunk license when attempting to set up real-time alerts. Below is a detailed explanation of the problem and the steps taken to resolve it.

8.1 Problem Encountered

While configuring the real-time alerts for brute force detection, Splunk displayed an error indicating that the alerting feature was restricted due to license limitations. Specifically, Splunk's **free version** does not support certain alerting features, and to enable this functionality, an **enterprise license** or a **paid subscription** was required.

8.2 Root Cause

The issue stemmed from the use of Splunk's free license, which limits several key features, including the ability to set up **real-time alerts**. Since this project relied on the alerting system to notify security teams about potential brute force attacks, the limitation became a blocker.

Key restrictions in the **free Splunk version** include:

- **No real-time alerting**.
- Limited data indexing volume (500 MB/day).
- Lack of access to premium apps and add-ons, such as **Splunk Enterprise Security**.

8.3 Solution: Upgrading to Splunk Enterprise

To resolve this issue and enable real-time alerting, we upgraded to a **Splunk Enterprise trial license**, which provided the necessary features to complete the project without immediate costs.

Steps taken:

1. **Requesting a Trial License**:
    - We navigated to the Splunk website and requested a **Splunk Enterprise 60-day trial license**, which offered full functionality, including real-time alerting.
    - This allowed us to proceed with the setup and configuration of alerts without immediate payment.
2. **Installing the Enterprise License**:
    - After receiving the license file, we accessed the Splunk web interface and uploaded the trial license.
    - The license was applied successfully, unlocking the features needed to complete the project.

8.4 Lessons Learned

- **Splunk Free License Limitations**: The free version is great for learning and testing purposes, but for projects requiring **advanced alerting**, **reporting**, or **higher data indexing limits**, a paid license is essential.

- **Budget Planning**: In future implementations, especially for enterprise environments, it is crucial to plan for the cost of Splunk's licenses to avoid interruptions in the deployment process.

9- Security Recommendations

To strengthen the security posture of the network and minimize the risk of future attacks, it is essential to implement the following security best practices:

1. **Disable Remote Desktop Protocol (RDP)**:
    - RDP is a common target for brute force attacks. Disabling RDP on systems where it is not necessary can significantly reduce the attack surface. If remote access is required, consider using more secure alternatives such as a VPN or using **multi-factor authentication (MFA)** for RDP access.
2. **Enable Multi-Factor Authentication (MFA)**:
    - Enforcing MFA on all user accounts adds an extra layer of security, ensuring that even if passwords are compromised, unauthorized access is prevented.
3. **Implement Account Lockout Policies**:
    - Set up account lockout policies to automatically lock accounts after several failed login attempts. This limits the effectiveness of brute force attacks by preventing unlimited attempts to guess passwords.
4. **Regularly Patch and Update Systems**:
    - Ensure that all systems, including servers and endpoints, are regularly updated with the latest security patches to protect against vulnerabilities that can be exploited by attackers.
5. **Monitor Network Activity**:
    - Continuously monitor network logs for any unusual activity, such as repeated failed login attempts or unexpected connections. Real-time monitoring tools like Splunk can help in identifying threats early.
6. **Restrict Access to Critical Services**:

- Limit access to sensitive services such as SSH and RDP to trusted IP addresses only. Consider using firewalls or security groups to control access to these services.

7. **Conduct Regular Security Audits**:
    - Periodically perform security audits and penetration testing to identify and address potential vulnerabilities in the network before they can be exploited by attackers.

10- Conclusion

In conclusion, this project successfully establishes a robust network environment for incident response and security monitoring. By integrating Active Directory, a Windows 10 client, and various security tools such as Splunk Universal Forwarder and Sysmon, we can effectively collect and analyze logs to detect and respond to security incidents in real time.

The inclusion of a Kali Linux machine as an attacker allows for the simulation of potential threats, providing invaluable insights into the security posture of the network. This hands-on approach not only enhances our understanding of security monitoring and incident response but also emphasizes the importance of proactive measures in defending against cyber threats.

Through this project, we have demonstrated the critical role of centralized log management and analysis in identifying vulnerabilities, improving response times, and strengthening overall security strategies. Moving forward, the implementation of additional alerts and monitoring capabilities will further enhance the effectiveness of the security infrastructure, ensuring a more resilient network environment against evolving threats.

11- References

The following resources were used during the project for downloading software, setting up the environment, and referencing best practices:

1. **Ubuntu Server**:
   - Official Download Page: https://ubuntu.com/download/server
   - Installation Guide: https://ubuntu.com/tutorials/install-ubuntu-server
2. **Splunk**:
   - Splunk Enterprise Download: https://www.splunk.com/en_us/download/splunk-enterprise.html
   - Splunk Universal Forwarder: https://www.splunk.com/en_us/download/universal-forwarder.html
   - Official Splunk Documentation: https://docs.splunk.com
3. **Sysmon (System Monitor)**:
   - Sysmon Download and Documentation: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
4. **Kali Linux**:
   - Official Download Page: https://www.kali.org/get-kali/
   - Installation Guide: https://www.kali.org/docs/installation/
5. **Crowbar** (Brute Force Tool):
   - Crowbar GitHub Repository: https://github.com/galkan/crowbar
6. **VMware Workstation** (for Virtual Machine setup):
   - VMware Download Page: https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html
7. **Splunk Security Essentials**:
   - Best Practices for Splunk Security: https://splunkbase.splunk.com/app/3435/

These references provided guidance on installing, configuring, and utilizing the various tools required to complete this project.

Acknowledgments

- Reham Rafie El-said Seria
- AbdelRahman Mohamed Mosad
- Hager Saad Abdelkhabeer
- Ahmed Samir Mohamed