Task:

***“Developing Incident Response Plans”.***

Provided by:

***“Digital Empowerment Networks”.***

Done by:

**“Khawar Amin”.**

## Scenario:

For this incident response task, I will Develop and implement an incident response plan for this scenario where the Windows machine is detected performing unauthorized access attempts to the Kali Linux machine via SSH.

Let's Develop Incident Response Plan Step-By-Step.

Remember I did it with my own devices.

### Step_1. Identifying Potential Security Incidents and Scenarios

- **Incident Type**: Unauthorized Access Attempt
- **Scenario Description**: Unauthorized access attempts are being made from the Windows machine to the Kali Linux machine over SSH ON PORT 22. This could be due to malicious intent or compromised credentials.

### Step_2. Defining Roles and Responsibilities

- **Incident Commander**: Oversees the incident response process. I noticed it.
- **Forensic Analyst**: Analyzes logs and data to understand the scope and impact. (I with my Forensics team)
- **Communications Lead**: Manages communications within the team and any external parties if needed. (another team member)
- **IT Support**: Handles technical tasks such as isolating the threat and securing systems. (I)

### Step_3. Developing Step-by-Step Response Procedures

#### *1.Preparation:*

**1.1. Install Monitoring and Security Tools on Kali Linux**:

- **Wireshark**: For network traffic analysis.
- **Fail2ban**: To block IP addresses after repeated failed login attempts
- Nmap: To scan whole network and list all devices connected to it.

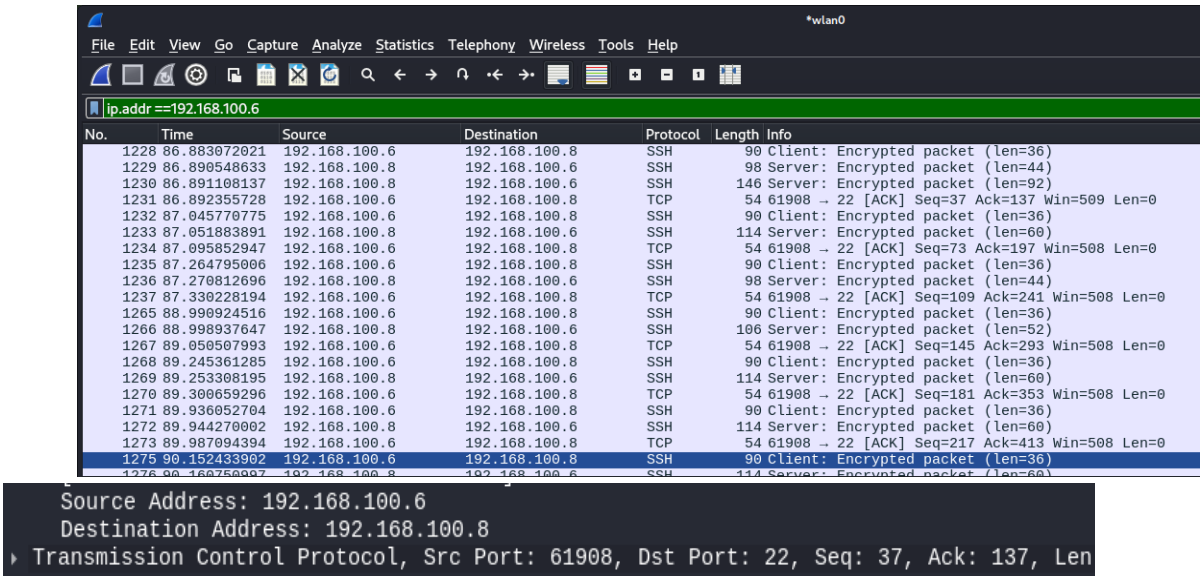
**1.2. Configure SSH Logging**:

- Ensure SSH logging is enabled on Kali Linux to capture login attempts.
- Modify /etc/ssh/sshd_config to set LogLevel VERBOSE for detailed logging. Using following command.
- ┌──(root㉿Lt-GH0ST)-[~]
- └─# leafpad /etc/ssh/sshd_config
-

```
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel Verbose
```

## 2. Detection:

1. Check SSH logs on Kali Linux, typically located in /var/log/auth.log or /var/log/secure.
2. Check Network Traffic using Wireshark.




Source IP: 192.168.100.6(Windows Device).

Destination IP: 192.168.100.8(Linux Device).

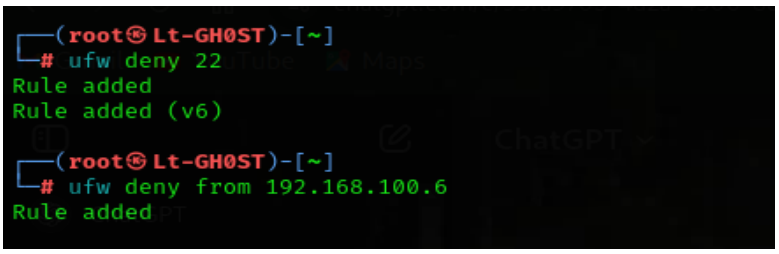
3. Review System alerts.

## *3. Containment:*

**Firewall Rules**: Create firewall rules on Kali Linux to block incoming connections from the Windows machine IP (192.168.100.6).

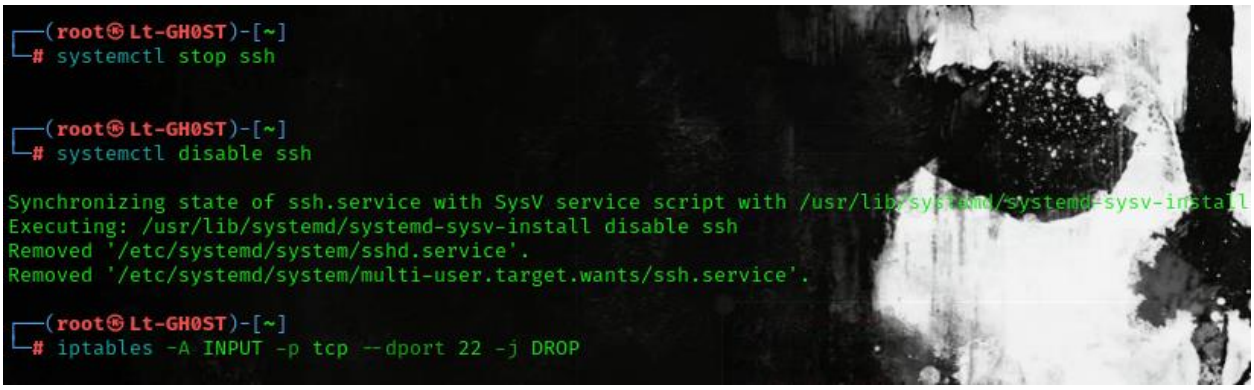
Run following commands as shown in the screenshot below

Disable port 22 and incoming traffic from 192.168.100.6 using ufw.



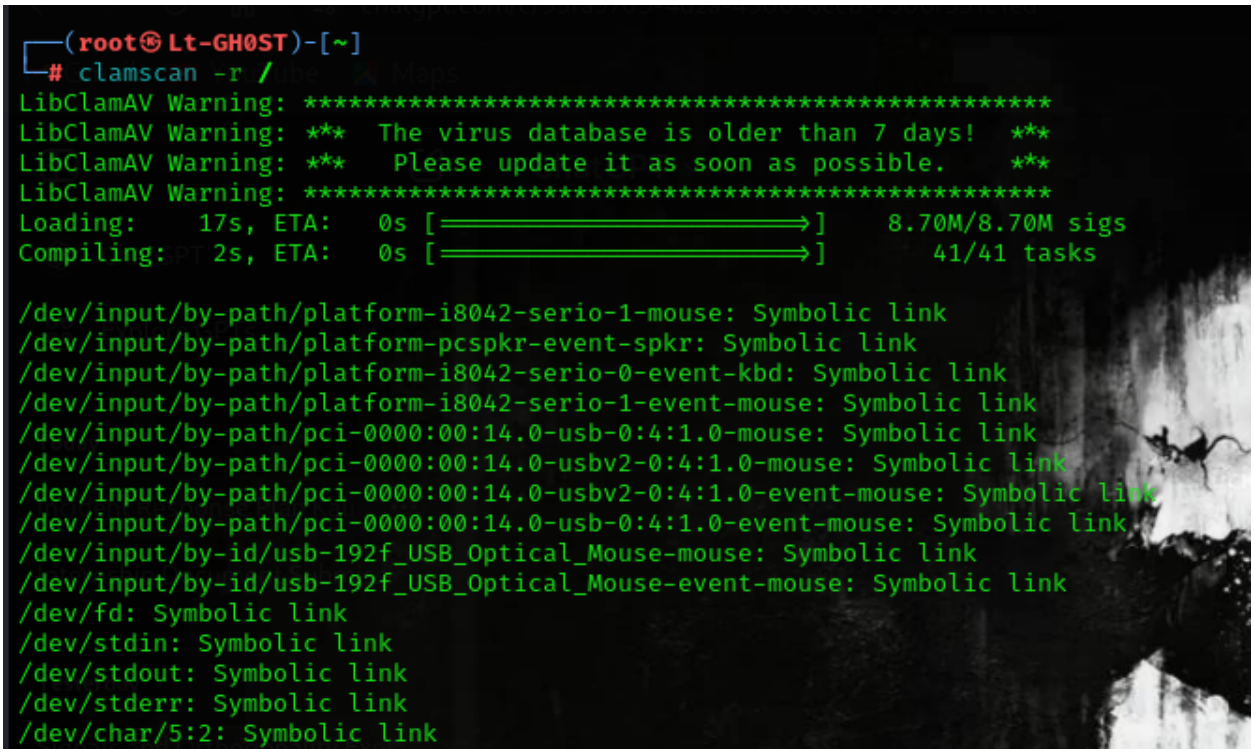

Stop and disable the service of SSH using systemctl .

So that attacker cannot access my Linux machine.




### *4.Eradication:*

- Check for user sessions in Linux using who and terminate unnecessary user sessions using command. sudo pkill -u <username>
- Checks for the Any malware, virus or any unauthorize script in your system use antivirus software. Like i used ClamAV which is free in Linux.




- Keep checking recent changes in files using different commands like.
  find / -type f -mtime -1
- Improve policies on remote login using SSH clients. Apply multiple security procedures for enhancing the security for logging on remote devices.
- Keep checking logs files like.
  sudo cat /var/log/auth.log

sudo cat /var/log/syslog
sudo cat /var/log/messages

- Remove unnecessary softwires and vulnerable software. You can use dpkg commands for this
- Update and modify the remote login sessions policies using ssh. Implement MFA of top vendors like google microsoft.
  sudo nano /etc/ssh/sshd_config
  sudo systemctl restart ssh
  sudo apt install libpam-google-authenticator
  google-authenticator

## *5.Recovery:*

**Restore Systems**:

- Re-enable SSH access after ensuring that the threat has been contained and eradicated.
- Restore any configurations or settings that were modified during the incident.

**Reconnect to Network**:

- Reconnect the Kali Linux machine to the network and monitor for any further suspicious activity.

## *6. Lessons Learned:*

**Incident Analysis**:

- Review the incident to understand how unauthorized access was attempted and what could have been done to prevent it.
- Analyze the effectiveness of your detection and response efforts.

**Update Procedures**:

- Update your incident response plan based on the lessons learned from the incident.
- Implement additional security measures if needed, such as enhanced logging or more stringent firewall rules.

### *7. Training and Simulation Exercises:*

**Run Simulations**:

- Conduct regular simulations of unauthorized access scenarios to practice and refine your response procedures.
- Test different response strategies to improve preparedness.

**Train Your Team**:

- Educate team members on recognizing signs of unauthorized access and following the incident response plan.

### *8. Review and Update the Plan Regularly:*

**Schedule Reviews**:

- Regularly review and update your incident response plan to ensure it remains effective and current.

**Incorporate Feedback**:

- Use feedback from simulations and actual incidents to continuously improve the plan.