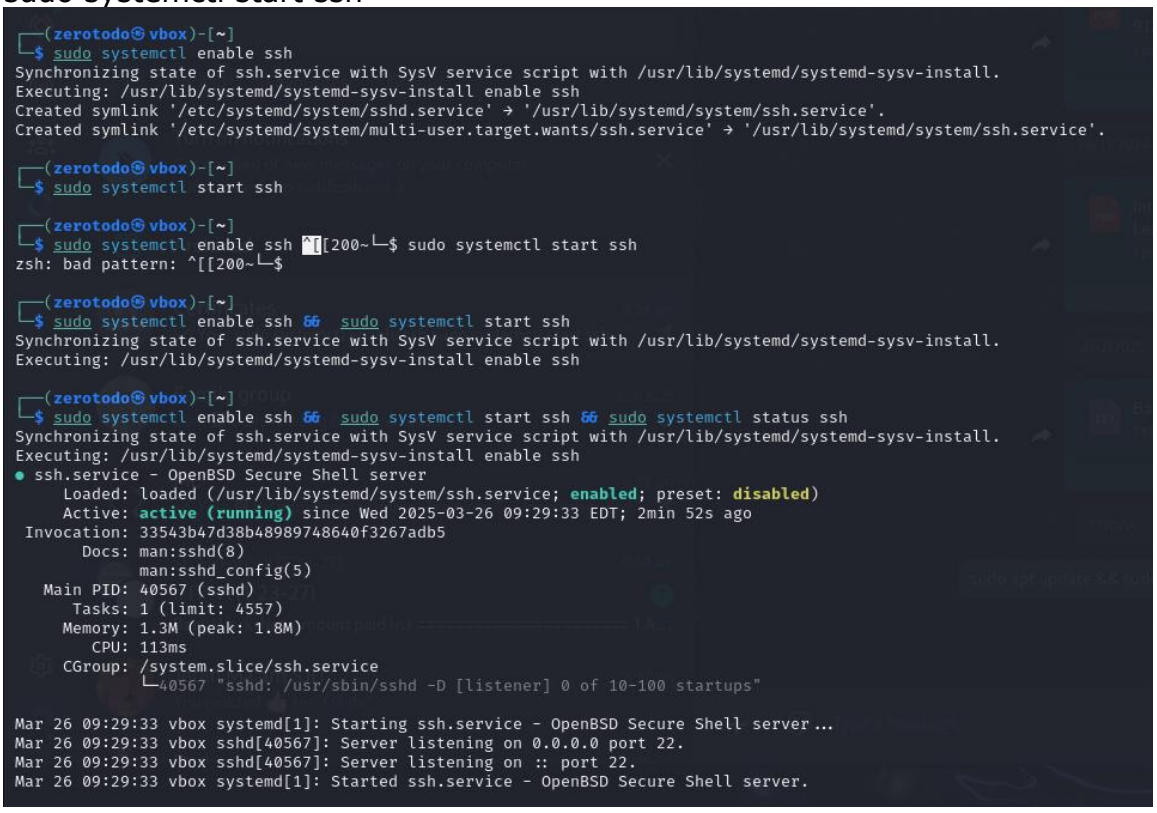
Create the Markdown content for Task 2: Remote Access & SSH Hardening
Linux Security - Remote Access & SSH Hardening (PoC)

This Proof of Concept (PoC) demonstrates SSH misconfigurations, how they can be exploited using brute-force attacks, and the necessary security hardening techniques.

Task 2: Remote Access & SSH Hardening

<u>Setup: Enabling SSH & Weak Security Configurations</u>

Ensure SSH is installed and running:
sudo apt update && sudo apt install -y openssh-server
sudo systemctl enable ssh
sudo systemctl start ssh



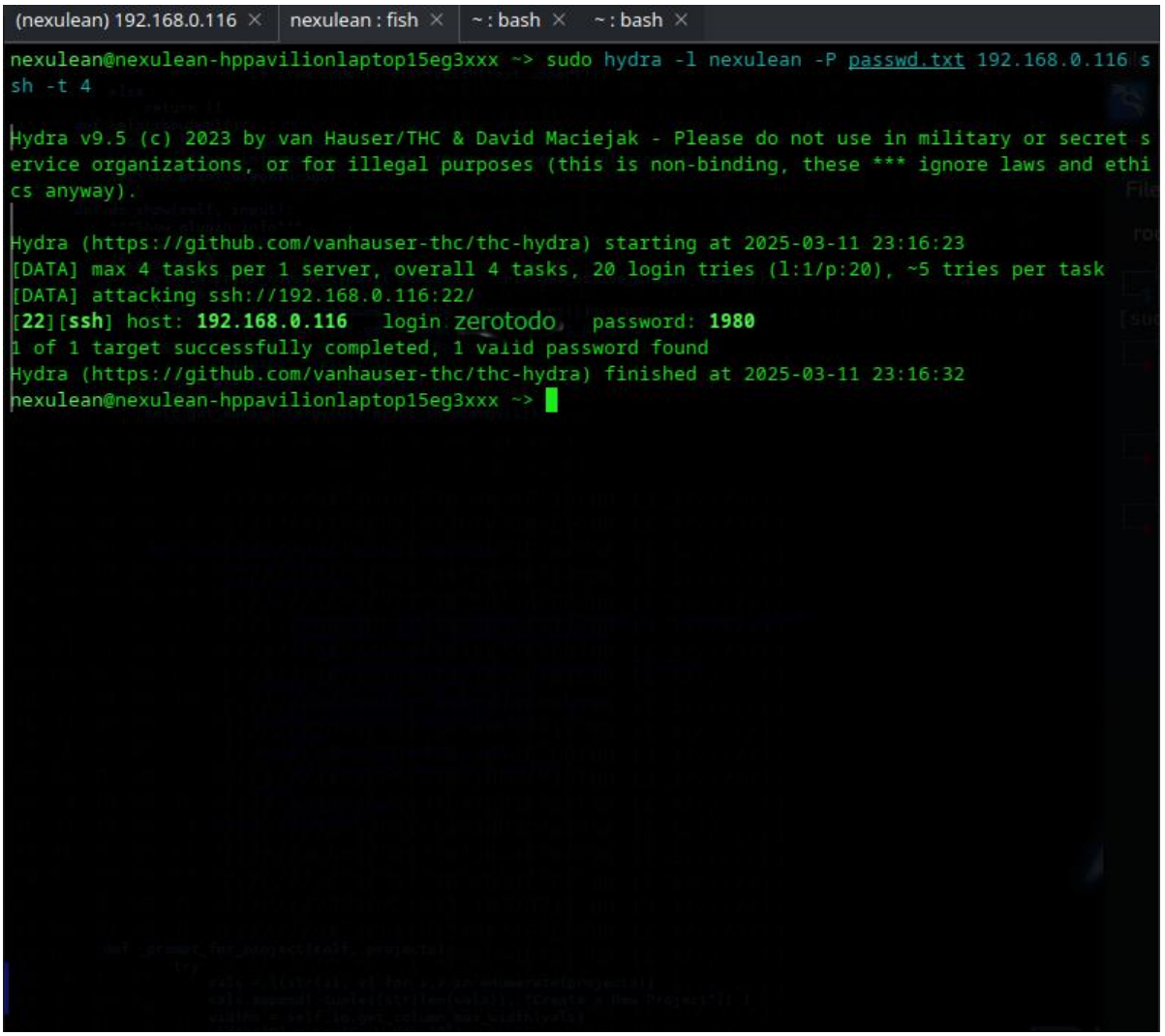
- Allow root login and password authentication: Open the SSH configuration file:
  sudo nano /etc/ssh/sshd_config

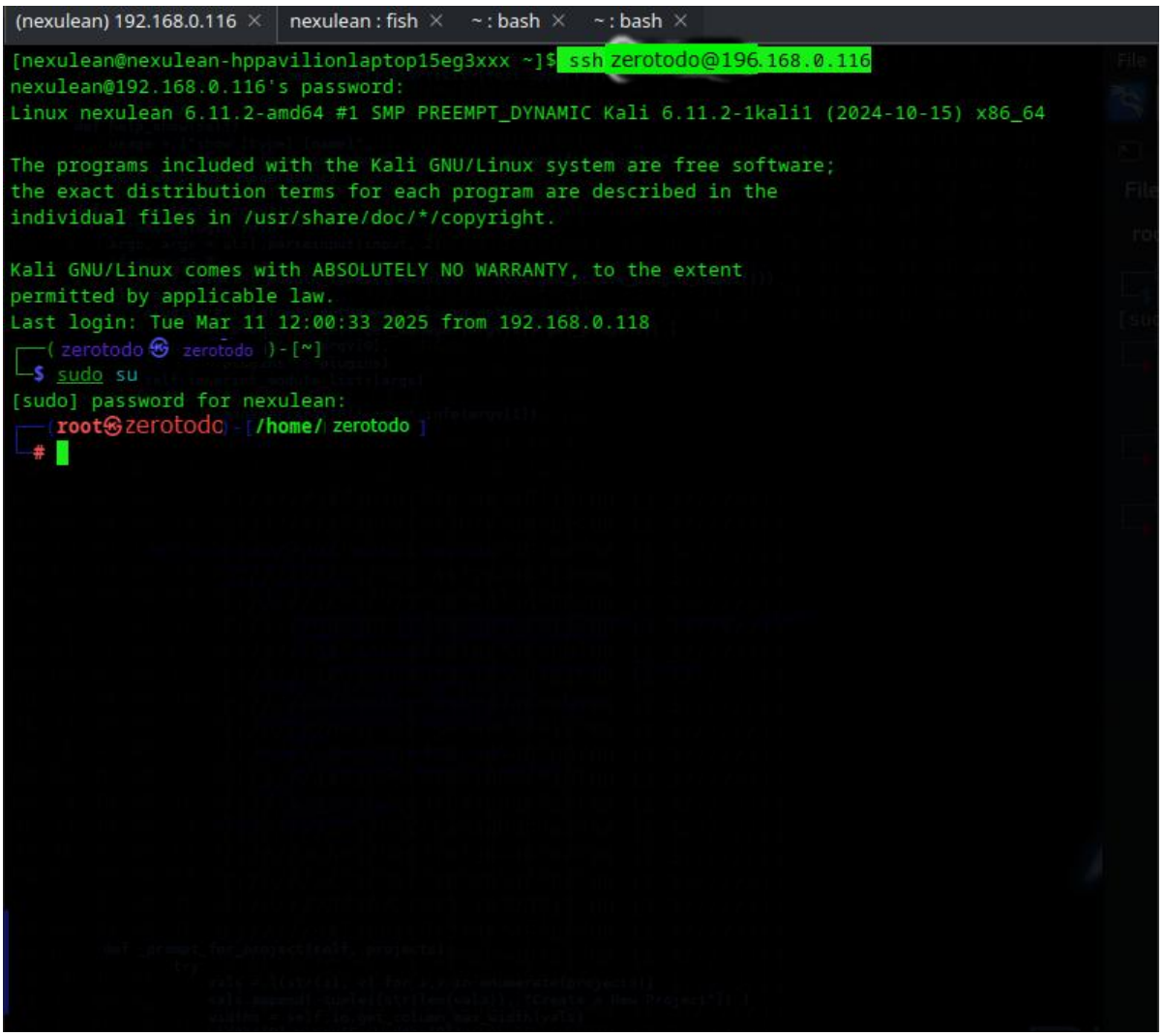
- Modify or add the following lines:
  PermitRootLogin yes
  PasswordAuthentication yes
- Save and exit, then restart SSH:
  sudo systemctl restart ssh
- Verify SSH access:
  Use a second machine or terminal to connect via SSH:
  ssh root@<server-ip>

Exploit: Brute-Force Attack on SSH

Using Hydra to brute-force SSH credentials:

hydra -l root -P passwords.txt <server-ip> ssh





-l root: Specifies the username.

-P passwords.txt: List of common passwords for brute-force attack.

server-ip : Replace with the target machine's IP.

Impact Analysis:
If the root account uses a weak password, an attacker can gain full control over the system.
Automated brute-force tools make SSH a common attack vector.

Mitigation: Hardening SSH Security

1. Disable root login and password authentication:
   sudo nano /etc/ssh/sshd_config

Update the following:
   PermitRootLogin no
   PasswordAuthentication no

```
  GNU nano 8.2                                        /etc/ssh/sshd_config *
PermitRootLogin no
PasswordAuthentication no

# 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 INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

^G Help      ^O Write Out   ^F Where Is    ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File   ^\ Replace     ^U Paste     ^J Justify   ^/ Go To Line
```

Restart SSH:

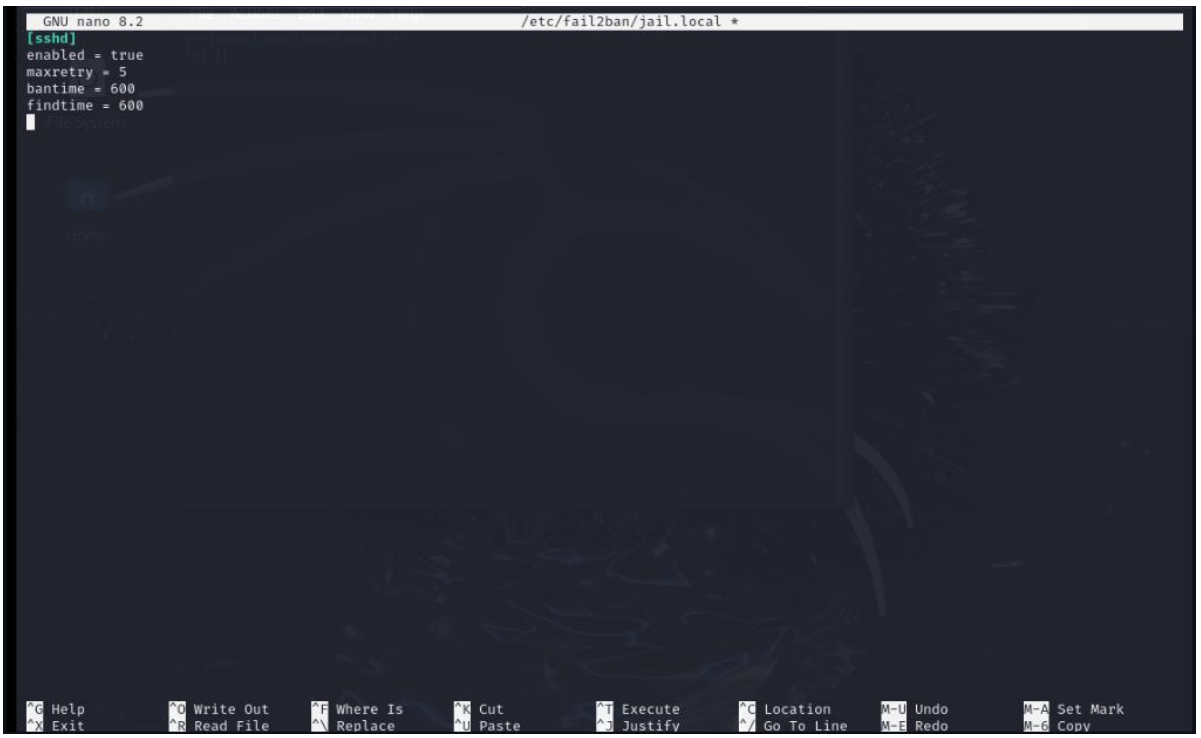
```
sudo systemctl restart ssh
```

2. Install and configure Fail2Ban to prevent brute-force attempts:

```
sudo apt install fail2ban -y
sudo nano /etc/fail2ban/jail.local
```

Add the following:

```
[sshd]
enabled = true
maxretry = 5
bantime = 600
findtime = 600
```



Restart Fail2Ban:

```
sudo systemctl restart fail2ban
```

Conclusion

This PoC highlights the importance of disabling root login, enforcing key-based authentication, and using Fail2Ban to prevent unauthorized access.