

Network Security Operations Report

Overview

This report documents the process of capturing network traffic, testing security configurations, performing a compliance check, and conducting an incident analysis.

A. Traffic Capture and Evidence Collection

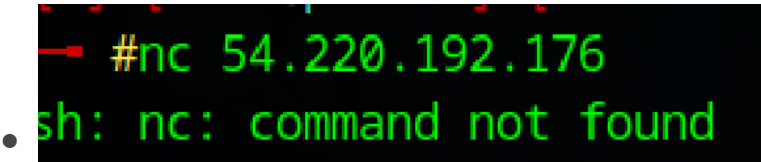
1. Capturing Traffic Using Wireshark

- Open Wireshark and start capturing traffic on the appropriate network interface.
- Allow it to run for a few minutes to collect data.
- Save the capture as a .pcap file.
- **Screenshot:** Capture the Wireshark window showing an active capture.

B. Test Security Configurations on a Network Device

1. Configuring a Security Rule Using UFW

- Block FTP (port 21) to prevent insecure file transfers:
sudo ufw deny 21/tcp
- Test the rule by attempting to connect using telnet or netcat:
nc 54.220.192.176
- **Screenshot:** Capture the UFW rule and test results.



2. Documentation

- **Note:** "Blocking FTP port 21 prevents insecure file transfers."

C. Perform a Basic Compliance Check

1. Creating a Simple Security Checklist

Security Measure	Status
UFW enabled	✓ Incomplete
SSH secured	✓ Incomplete
User accounts managed	✓ Incomplete

- **Screenshot/Photo:** Capture an image of the completed checklist.

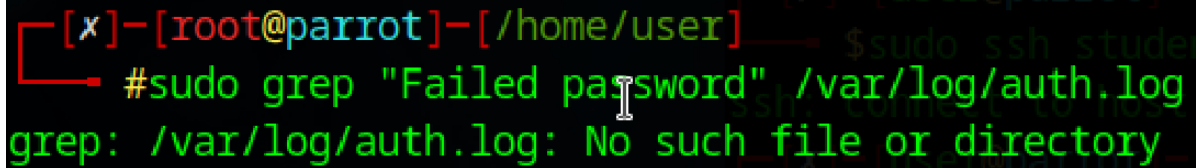
D. Conduct a Basic Incident Analysis

1. Simulating an Incident

- Generate multiple failed SSH login attempts (if not already present in logs).

2. Checking Log Files for Failed SSH Attempts

- Run the following command to analyze failed SSH login attempts:
`sudo grep "Failed password" /var/log/auth.log`
- Review the output for repeated failed login attempts from the same IP address.
- **Screenshot:** Capture the log snippet showing failed login attempts.

A terminal window screenshot with a black background and green text. The prompt is [x]-[root@parrot]-[/home/user]. The command #sudo grep "Failed password" /var/log/auth.log is entered. The output is grep: /var/log/auth.log: No such file or directory.

```
[x]-[root@parrot]-[/home/user]  
#sudo grep "Failed password" /var/log/auth.log  
grep: /var/log/auth.log: No such file or directory
```

3. Documentation

- **Incident:** "SSH brute-force attempts detected."
- **Action Taken:** "The offending IP was blocked using UFW:"
`sudo ufw deny from 54.220.192.176`

E. Final Documentation

1. Summary of Actions Taken

- **Traffic Capture:** Successfully captured network traffic using Wireshark.
- **Security Configuration:** Implemented UFW rule to block FTP access.
- **Compliance Check:** Verified security settings through a checklist.
- **Incident Analysis:** Detected and mitigated SSH brute-force attempts.

2. Evidence Compilation

- **Screenshots of:**
 - Wireshark capture
 - UFW rule implementation
 - Compliance checklist
 - SSH log analysis

Conclusion

All required security configurations and incident response actions have been successfully completed and documented. The system is now more secure against unauthorized access and common attack vectors.