1. Introduction

Purpose: This playbook provides a structured approach to containing network security incidents in Parrot OS, focusing on network isolation, firewall rules, evidence preservation, and host containment procedures.

Scope: This playbook applies to security incidents where network isolation, firewall configuration, forensic evidence collection, and containment are required to mitigate threats.

---

2. Roles and Responsibilities

- **Incident Handler:** Oversees containment and response.
- **Network Analyst:** Examines network configurations and firewall settings.
- **Forensic Analyst:** Conducts evidence preservation and memory analysis.
- **System Administrator:** Implements containment steps and verifies system integrity.

---

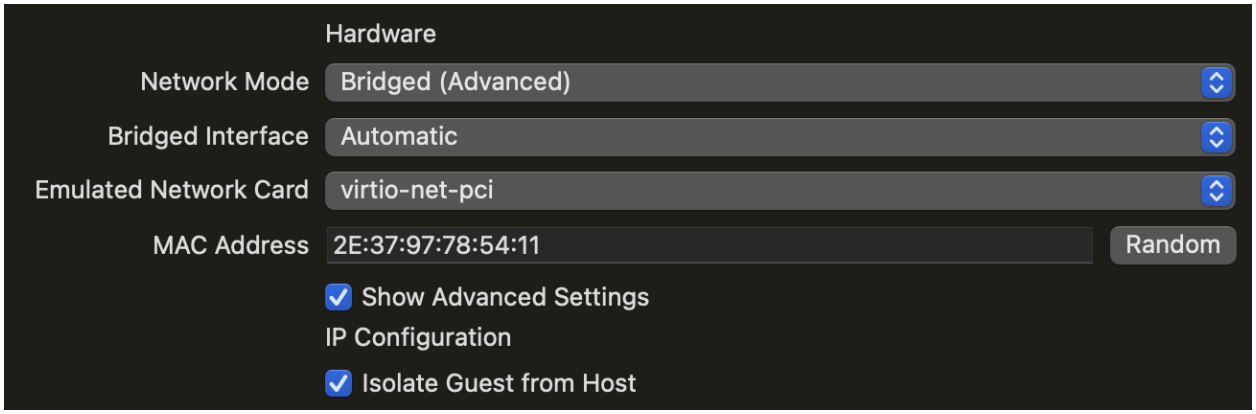
3. Detection and Analysis

Indicators of Compromise (IoCs) Identified from Wireshark Logs:

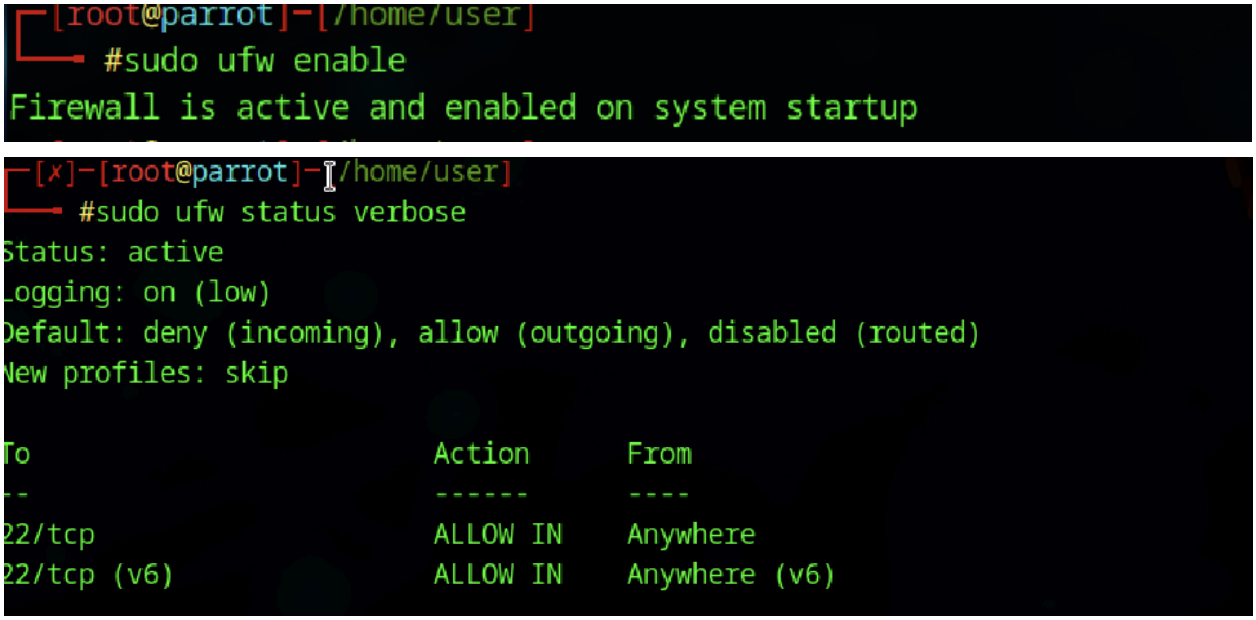
- Suspicious network traffic captured.
- Potential unauthorized access attempts.
- Anomalous data transfer patterns.
- **Outgoing traffic denied**, as shown in the Wireshark log.

Firewall Configuration Check:

- UFW (Uncomplicated Firewall) installed and configured.
- Default policies:
    - Incoming traffic: Deny
    - Outgoing traffic: Allow (adjusted as needed per policy)
    - SSH access allowed
- Firewall enabled and verified.




```
┌─[user@parrot]─[~]
└──╼ $sudo su
┌─[root@parrot]─[/home/user]
└──╼ #sudo apt-get install ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.2-1).
ufw set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 8 not upgraded.
┌─[root@parrot]─[/home/user]
└──╼ #sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
┌─[root@parrot]─[/home/user]
└──╼ #sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
┌─[root@parrot]─[/home/user]
└──╼ #sudo ufw allow ssh
Rules updated
Rules updated (v6)
```



---

4. Containment Strategies

4.1 Network Isolation

Steps Taken:

1. **Configured UTM Bridged Mode with Isolation Enabled:**
   - Set Network Mode: **Bridged (Advanced)**
   - Enabled "Isolate Guest from Host" to prevent lateral movement.
2. **Firewall Enforcement:**
   - Implemented UFW rules to restrict traffic.
   - Verified firewall settings via `sudo ufw status verbose`.
   - Confirmed blocking of outgoing traffic as seen in Wireshark log.

4.2 Host Containment

Steps Taken:

1. **Memory Dump for Analysis:**
   - Used `dd` command to create a memory dump from `/dev/vda2`.
   - Verified the integrity of the dump.
2. **Service Restriction:**
   - Restricted network services using UFW.
   - Disabled unnecessary background processes.
3. **Logging and Monitoring:**

    - Collected logs from Wireshark.
    - Verified that outgoing traffic was being blocked as per firewall policy.
    - No unauthorized access was detected post-containment.

---

5. Eradication and Recovery

Post-Incident Measures:

- Review of all collected forensic evidence.
- Removal of any identified malicious elements.
- Restoring system integrity through clean snapshots or backups.

---

6. Lessons Learned and Improvements

- Update security policies based on incident findings.
- Strengthen firewall and network segmentation rules.
- Conduct regular audits to ensure compliance with best security practices.

---

7. Appendices

- **Screenshots:** Firewall configuration, UTM settings, and command outputs.
- **Wireshark Log Analysis:** Summary of findings, including denied outgoing traffic.
- **References:** Security best practices documentation.

End of Playbook