Post-Incident Procedures Report

1. Introduction

Post-incident procedures are critical for restoring affected systems, analyzing the root cause, validating recovery, and improving incident response processes. This report details the steps taken to restore a **VirtualBox environment**, recover a **Parrot OS system**, and reconfigure **network settings** after an incident. Additionally, a **root cause analysis (RCA)** is conducted, a **recovery validation checklist** is implemented, and **recommendations for improving the IR process** are provided.

---

2. System Recovery Procedures

2.1 VirtualBox Environment Restoration

Purpose:

To ensure the integrity of the VirtualBox virtual environment by restoring it to a stable state after a security incident.

Steps for Recovery:

1️⃣ Restore from a VirtualBox Snapshot (Preferred Method)

1. **Open VirtualBox** and select the affected **Parrot OS VM**.
2. Click on the **Snapshots** tab.
3. Choose the latest stable snapshot and click **Restore**.
4. Confirm the restoration and start the VM to verify functionality.

2️⃣ Reinstall the VM (If No Snapshot is Available)

1. Download the latest **Parrot OS ISO** from the official website.
2. Create a **new VM** in VirtualBox with the recommended configuration.
3. Attach the **ISO file** and proceed with the installation.
4. Restore important files from backup (if available).

✅ **This ensures a clean and fully functional VirtualBox environment.**

2.2 Parrot OS System Recovery

Purpose:

To restore Parrot OS functionality and remove any malware or misconfigurations affecting system stability.

Steps for Recovery:

1️⃣ Check for System Integrity Issues

- Verify system file integrity:
  sudo debsums -c
- List system users to detect unauthorized accounts:
  cat /etc/passwd | grep "/bin/bash"

2️⃣ Use Parrot OS Recovery Mode

1. **Reboot the VM** and select **Advanced Options > Recovery Mode**.
2. Choose **"fsck - File System Check"** to repair disk corruption.
3. Select **"dpkg - Repair broken packages"** to reinstall essential system packages.
4. Restart the system:
   sudo reboot

3️⃣ Secure and Optimize the System

- **Update all packages:**
  sudo apt update && sudo apt upgrade -y
- **Reinstall security tools:**
  sudo apt install --reinstall ufw fail2ban clamav
- **Run a full malware scan:**
  sudo clamscan -r / --bell --remove

✅ **Parrot OS is now restored and secured.**

2.3 Network Configuration Recovery

Purpose:

To re-establish secure network connectivity and correct any misconfigurations.

Steps for Recovery:

1️⃣ Reset Firewall Rules

sudo ufw reset
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw enable

2️⃣ Restore Network Interfaces

- Check network interfaces:
  ip a
- Restart the network service:
  sudo systemctl restart networking

If network is broken, manually configure it:
sudo nano /etc/network/interfaces
Example configuration:
auto eth0

- iface eth0 inet dhcp
- Restart the network:
  sudo systemctl restart networking

✅ **Network connectivity is now restored.**

---

3. Root Cause Analysis (RCA)

Purpose:

To determine how the incident occurred and identify contributing factors.

3.1 Event Timeline

- **Check logs for unusual activity:**
  journalctl --since "1 hour ago"
- **Review authentication logs:**
  cat /var/log/auth.log | grep "Failed password"
- **Analyze system errors:**
  cat /var/log/syslog | grep "error"

3.2 Contributing Factors

- **Misconfigurations** (e.g., weak firewall rules)

- **Unpatched vulnerabilities** (e.g., outdated software)
- **User errors** (e.g., weak passwords, untrusted downloads)

3.3 Technical Findings

- **List suspicious IP connections:**
  sudo netstat -antp | grep ESTABLISHED
- **Identify active malicious processes:**
  ps aux | grep -E "nc|ssh|python|netcat"
- **Detect recently modified files:**
  sudo find / -mtime -1

✅ **RCA helps document the root cause and security gaps.**

---

4. Recovery Validation Checklist

Purpose:

To confirm that system recovery was successful.

4.1 System Integrity Tests

- Check disk health:
  sudo fsck -y /dev/sda
- Verify installed packages:
  sudo apt list --installed

4.2 Network Functionality Tests

- Test internet connectivity:
  ping -c 4 8.8.8.8
- Ensure firewall is working:
  sudo ufw status verbose

4.3 Security Checks

- Scan for rootkits:
  sudo rkhunter --check
- Monitor logs for new anomalies:
  journalctl --since "30 minutes ago"

✅ **System passes all recovery validation tests.**

---

5. IR Process Improvement Recommendations

Purpose:

To strengthen the IR process and prevent future incidents.

5.1 Lessons Learned

- Identify security **weaknesses** exploited.
- Evaluate response **efficiency and gaps**.
- Improve **log monitoring and alerting**.

5.2 Security Enhancements

- **Harden authentication:**
  sudo nano /etc/ssh/sshd_config
    - Disable root login: `PermitRootLogin no`
    - Enforce key-based authentication: `PasswordAuthentication no`
- sudo systemctl restart ssh

Improve logging and monitoring:
sudo apt install logwatch

- sudo logwatch --output file --format text --range today --filename /var/log/logwatch.log

Enable automatic security updates:
sudo apt install unattended-upgrades

- sudo dpkg-reconfigure unattended-upgrades

✅ **Future security incidents will be handled more efficiently.**

---

6. Conclusion

This report successfully documented the **post-incident procedures**, including **system recovery, network restoration, root cause analysis, recovery validation, and process improvement recommendations**. By implementing these steps, security posture is strengthened, ensuring a resilient response to future incidents.