Post-Incident Procedures Documentation

1. System Recovery Procedures

1.1 VirtualBox Environment Restoration

- **Snapshot Recovery:**
  - Restore VM snapshot taken prior to incident
  - Use VirtualBox GUI > Select VM > Snapshots > Restore
- **VM Cloning:**
  - Use clone feature to preserve recovered state as backup

1.2 Parrot OS System Recovery

- **Backup Restore:**
  - Revert from system backup (e.g., Timeshift or rsync backup)
- **Package Check:**
  - Reinstall critical packages using `sudo apt reinstall <package>`
- **Log Clean-Up:**
  - Archive or clear logs post-analysis: `sudo journalctl --rotate && sudo journalctl --vacuum-time=1s`

1.3 Network Configuration Recovery

- **Reset Interfaces:**
  - Restart NetworkManager: `sudo systemctl restart NetworkManager`
- **Reapply Firewall Rules:**
  - Reload `iptables` or `ufw` configurations from backup

---

2. Root Cause Analysis

2.1 Event Timeline Recap:

- 03:14:55 – SSH login attempt from macOS
- 03:14:57 – Failed login logged on Parrot OS
- 03:15:00 – Wazuh alert triggered
- 03:15:30 – Evidence collection started

2.2 Contributing Factors:

- Weak or default SSH credentials
- Lack of IP filtering for SSH access
- Inadequate alert thresholds

2.3 Technical Findings:

- Parrot logs confirmed brute-force source
- Wireshark confirmed packet trace from macOS
- No firewall rule preventing unauthorized SSH traffic

---

3. Recovery Validation Checklist

Test Item	Procedure	Status
Wazuh Services	`systemctl status wazuh-*`	✅
Network Access	`ping`, `curl` to internal/external services	✅
SSH Hardening	Attempt unauthorized login (expect fail)	✅
Firewall Rules	Verify with `sudo iptables -L`	✅
Volatility Readiness	Test `vol.py` on sample dump	✅

---

4. IR Process Improvement Recommendations

- **Enforce SSH Key Authentication:** Disable password logins
- **Automate Snapshot Creation:** Use cron job with `VBoxManage snapshot`
- **USB Monitoring Scripts:** Auto-alert on new USB insertion
- **Regular Log Review:** Set schedule for log inspections using `logwatch`
- **Documented SOPs:** For evidence collection, agent deployment, and rollback procedures
- **2FA Integration:** Add multi-factor for all critical access points

End of Document