📋 Risk Management Strategy Report

Project Title: Vulnerability Risk Management for Parrot OS Security Environment
Date: April 24, 2025
Prepared by: [Your Name/Team]

🔍 1. Risk Identification

The vulnerability assessment revealed the following risks on host `192.168.1.100` running Parrot Security OS.

✅ Critical Risk 1: Outdated Apache HTTP Server (v2.4.52)

- **Service:** HTTP (Port 80)
- **CVE Reference:** CVE-2022-22720
- **Severity:** High
- **Impact:** This version is vulnerable to remote code execution and denial-of-service attacks.
- **Justification:** Apache HTTP server is directly exposed over the network. An unpatched version allows attackers to execute arbitrary code, compromise server integrity, or disrupt availability.

✅ Critical Risk 2: SMB Signing Disabled

- **Service:** SMB (Port 445)
- **Severity:** Medium (elevated to critical due to attack chaining potential)
- **Impact:** Allows Man-in-the-Middle (MitM) attacks on file shares.
- **Justification:** While SMB signing is optional in many configurations, its absence exposes sensitive file transactions to tampering or theft, especially on a high-value system like a Parrot OS used for security analysis.

🛠️ 2. Risk Treatment & Mitigation

Risk	Treatment	Mitigation Steps
Outdated Apache HTTP Server	Risk Reduction (Patching)	1. Backup server files. 2. Download and install latest Apache (v2.4.59 or higher).
SMB Signing Disabled	Risk Reduction (Hardening)	1. Edit `/etc/samba/smb.conf`. 2. Under `[global]`, add `server signing = mandatory`. 3. Restart Samba service. 4. Verify via `smbclient`.

Rationale: Both treatment strategies focus on **risk reduction**, which is ideal for critical services that must remain operational. Complete risk elimination (e.g., disabling HTTP or SMB) would hinder functionality.

🔄 3. Additional Mitigations for Supporting Risks

Risk	Severity	Recommended Actions
Weak SSH Key Exchange Algorithms	Low	Disable deprecated algorithms (`/etc/ssh/sshd_config`). Only allow secure modern ciphers.
RDP Exposure on 192.168.1.101	Medium	Restrict access using firewall rules. Enable Network Level Authentication (NLA).
Network Segmentation Gaps	Medium	Segment 192.168.1.100 from general access network using VLAN or host-based firewall.

📈 4. Risk Monitoring Procedure

🎯 Objective:

Continuously monitor the Parrot OS environment for the recurrence of identified vulnerabilities and potential exploitation attempts.

🧭 Procedure: Vulnerability Tracking and Alerting (Monthly)

Step	Description
1. Scheduled Vulnerability Scans	Automate monthly Nmap + NSE scans on 192.168.1.100 and 192.168.1.101.
2. Log Centralization	Collect Apache, SSH, SMB, and system logs using `rsyslog` or

3. Threat Intelligence Matching	Use OpenCTI to cross-reference findings with known IoCs or threat actor TTPs.
4. Alerting	Integrate Snort/Suricata with email/SMS alerting for known CVE
5. Review and	Monthly review of vulnerability reports and update of risk register.

Tools Used:

- **Nmap** – for monthly vulnerability scans.
- **OpenCTI** – for threat intelligence correlation.
- **Snort** – for real-time intrusion detection.
- **Syslog** – for centralized log collection.

Justification: Proactive monitoring ensures visibility over emerging threats and validates that mitigations remain in place. Automation improves efficiency and reduces human error.

📊 5. Risk Register Summary

Risk	Severity	Treatment	Status	Next Review
Outdated Apache HTTP Server	High	Patched	Mitigated (pending verification)	May 2025
SMB Signing Disabled	Medium (↑)	Hardened	Mitigated (verified)	May 2025
Weak SSH Algorithms	Low	Configuration	Pending	May 2025
RDP Exposure	Medium	Restricted	Mitigated	May 2025

✅ Conclusion

This risk management strategy effectively addresses both critical and supporting risks identified through vulnerability assessment. By prioritizing patching and service hardening, and implementing a detailed monitoring procedure, we can significantly reduce the attack surface of the Parrot OS environment.

Next Steps:

- Finalize Apache patch deployment and confirm resolution.
- Execute May 2025 monthly scan.

- Review and expand threat intelligence feeds in OpenCTI.