Action Plan

Summary of Audit Report

The recent audit of OpenPharma's information systems revealed several vulnerabilities that could significantly impact the security of proprietary research, patient health information, and regulatory compliance. These vulnerabilities range from network poisoning attacks to outdated operating systems, all of which pose risks to the company's data integrity and operational security. Given resource constraints, eight critical vulnerabilities have been selected for remediation based on their potential impact, feasibility of resolution, and alignment with business risks and compliance needs.

Eight Prioritized Vulnerabilities

Vulnerability #1

- Title: Outdated Operating Systems (High)
- Description: Older systems no longer receive security updates, leaving them open to exploitation.
- Priority: 1
- Remediation action: Upgrade all outdated operating systems to supported versions with security patches applied.
- Justification and explanation: End-of-life operating systems no longer receive security updates, making them prime targets for attackers. Immediate remediation aligns with CIS Control 7 (Continuous Vulnerability Management)**.**
- Additional notes and observations: Develop a long-term OS lifecycle policy to prevent future instances of outdated systems.

Vulnerability #2

- Title: IPv6 Network Poisoning (Critical)
- Description: This vulnerability enables attackers to use rogue IPv6 router advertisements to redirect or intercept traffic.
- Priority: 2
- Remediation action: Disable unused IPv6 protocols or implement RA Guard and DHCPv6 Guard to protect against rogue router advertisements.
- Justification and explanation: Attackers can exploit IPv6 to intercept and manipulate traffic. Aligns with CIS Control 12 (Network Infrastructure Management).
- Additional notes and observations: Conduct periodic assessments of IPv6 configurations and monitor for unauthorized IPv6 traffic.

Vulnerability #3

- Title: LLMNR/NBT-NS Poisoning (Critical)
- Description: Local Link Multicast Name Resolution (LLMNR) can be exploited by attackers to impersonate systems and capture user credentials.
- Priority: 3
- Remediation action: Disable LLMNR and configure DNS settings to resolve names securely through authoritative sources.
- Justification and explanation: LLMNR poisoning is commonly used in internal attacks to capture user credentials. Aligns with CIS Control 12 (Network Infrastructure Management).
- Additional notes and observations: Use monitoring tools like Responder detection to identify LLMNR misuse.

Vulnerability #4

- Title: MDNS Network Poisoning (Critical)
- Description: Multicast DNS (mDNS) can be exploited to spoof responses and redirect traffic, especially in poorly segmented networks.
- Priority: 4
- Remediation action: Disable mDNS on systems where it is not required and restrict its use to specific network segments.
- Justification and explanation: Like LLMNR, mDNS can be exploited to redirect traffic and gather sensitive data. Aligns with CIS Control 12 (Network Infrastructure management).
- Additional notes and observations: Audit mDNS use across departments and apply control lists.

Vulnerability #5

- Title: NBT-NS Poisoning (Critical)
- Description: NetBIOS Name Service (NBT-NS) spoofing allows attackers to respond to name resolution requests and capture user credentials.
- Priority: 5
- Remediation action: Disable NetBIOS over TCP/IP and ensure name resolution is handled by secure DNS servers.
- Justification and explanation: NBT-NS attacks allow attackers to impersonate systems and intercept credentials. Aligns with CIS Control 12 (Network Infrastructure Management).
- Additional notes and observations: Regularly validate network name resolution policies to minimize attack surfaces.

Vulnerability #6

- Title: ASREP-Roastable Users (Med)
- Description: This vulnerability involves accounts without Kerberos pre-authentication, making them susceptible to offline password cracking.
- Priority: 6
- Remediation action: Enforce strong password policies and ensure pre-authentication is enabled for all applicable accounts.
- Justification and explanation: ASREP-roasting allows attackers to retrieve hashes of accounts with pre-auth disabled. Aligns with CIS Control 5 (Account Management).
- Additional notes and observations: Regularly audit Active Directory for ASREP-enabled users and apply monitoring alerts.

Vulnerability #7

- Title: Kerberoastable Users (Med)
- Description: Service accounts with weak passwords can be targeted via Kerberoasting attacks to obtain credentials from service tickets.
- Priority: 7
- Remediation action: Require complex passwords for service accounts and monitor for abnormal ticket requests.
- Justification and explanation: Attackers can exploit service tickets to crack passwords offline. Aligns with CIS Control 5 (Account Management).
- Additional notes and observations: Implement Managed Service Accounts (MSAs) to automate password complexity and rotation.

Vulnerability #8

- Title: Machines without required SMB signing (Med)
- Description: Systems that do not enforce SMB signing are vulnerable to man-in-the-middle (MITM) attacks during file sharing operations.
- Priority: 8
- Remediation action: Enforce SMB signing via Group Policy to protect the integrity of SMB communications.
- Justification and explanation: Unsigned SMB traffic can be intercepted and altered, allowing for MITM attacks. Aligns with CIS Control 12 (Network Infrastructure Management).
- Additional notes and observations: Confirm SMBv1 is disabled and use security event logging to verify SMB signature usage.

Future Considerations

The following vulnerabilities were not selected for immediate remediation but remain important for future planning:

- Group Policy Preferences (GPP) Passwords (8.8 High): Highly exploitable; remove stored credentials from GPP files.
- Sensitive Information in Network Shares: Consider deploying DLP solutions and auditing access rights.
- Inactive Enabled User Accounts: Enforce account lifecycle policies and regular audits to prevent account misuse.

Incident Response & Employee Readiness

- Employee Awareness: Conduct phishing simulations and training on secure practices for credential and network use.
- Response Drills: Run tabletop and live exercises to evaluate OpenPharma's ability to respond to attacks.
- Monitoring: Implement centralized logging and alerting for key events like privilege escalation and protocol misuse.

Conclusion

This action plan prioritizes vulnerabilities based on critical severity, real-world exploitability, and business impact. It aligns OpenPharma with essential CIS Controls, and supports a strategic path toward improved security, regulatory compliance, and operational resilience.