Cybersecurity Risk Management Report

1. Introduction

This report demonstrates the application of risk management strategies in a cybersecurity context, focusing on the identification, assessment, treatment, and monitoring of risks derived from vulnerability scan results. The report leverages mock data inspired by the provided vulnerability scan findings from the "Apply Vulnerability Assessment Techniques.pdf" document. It includes the identification of two critical risks, their explanations, treatment recommendations, and mitigation steps. Additionally, a risk monitoring procedure is outlined to track identified risks effectively. All decisions are justified to ensure clarity and alignment with cybersecurity best practices.

The objective is to provide a structured approach to managing cyber risks, ensuring organizational assets are protected against potential threats while maintaining operational integrity.

2. Risk Identification

Using mock data based on the vulnerability scan results from a network (192.168.1.0/24), the following risks were identified. The scan was conducted using **Nmap 7.94SVN** with options -sV (service version detection) and --script vuln(vulnerability scripts). The results revealed open ports, unknown services, and non-responsive hosts, which form the basis for risk identification.

Identified Risks

1. **Unknown Service on Open Port 6783/tcp (192.168.1.93)**:
    - **Description**: An open port (6783/tcp) was detected on host 192.168.1.93, labeled as an "unknown" service. The lack of service identification prevents assessment of specific vulnerabilities.
    - **Threat**: Attackers could exploit this port to gain unauthorized access, deploy malware, or exfiltrate data if the service is vulnerable.
    - **Impact**: Potential system compromise, data breach, or network propagation.
    - **Likelihood**: High, as open ports are common attack vectors, especially with unknown services.
    - **Risk Level**: Critical, due to the uncertainty and potential for exploitation.
2. **Non-Responsive Host (192.168.1.253)**:

- **Description**: The host at 192.168.1.253 was reported as down during multiple scans, potentially indicating network issues, downtime, or active blocking.
- **Threat**: If the host is blocking scans, it may hide vulnerabilities or misconfigurations. If offline, it could indicate a compromised or misconfigured critical asset.
- **Impact**: Hidden vulnerabilities could lead to undetected compromises, while downtime of a critical asset (e.g., a server) could disrupt operations.
- **Likelihood**: Moderate, as the cause (blocking, downtime, or compromise) is unclear but plausible.
- **Risk Level**: Critical, due to the potential for undetected threats or operational disruption.

3. **Unknown Devices on Network (192.168.1.125, 192.168.1.131)**:
   - **Description**: Devices at 192.168.1.125 (DAEDMAC43) and 192.168.1.131 were discovered without identified roles or ownership.
   - **Threat**: Rogue or unauthorized devices could be malicious, hosting backdoors or conducting reconnaissance.
   - **Impact**: Network compromise, data theft, or unauthorized access.
   - **Likelihood**: Moderate, as unauthorized devices are a known risk in unmanaged networks.
   - **Risk Level**: High, but not critical, as their impact depends on their purpose.
4. **Outdated Service Versions (Hypothetical)**:
   - **Description**: Assume the scan identified an outdated Apache server (version 2.4.29) on 192.168.1.15, vulnerable to known CVEs (e.g., CVE-2019-0211).
   - **Threat**: Attackers could exploit known vulnerabilities to gain privileged access or execute arbitrary code.
   - **Impact**: System compromise, data loss, or service disruption.
   - **Likelihood**: High, as outdated software is frequently targeted.
   - **Risk Level**: High, but not critical, as mitigation is straightforward with patching.

Focus on Critical Risks

The two critical risks selected for detailed analysis are:

- **Risk 1**: Unknown Service on Open Port 6783/tcp (192.168.1.93).
- **Risk 2**: Non-Responsive Host (192.168.1.253).

These risks are prioritized due to their high likelihood and severe potential impact, including system compromise, data breaches, or operational disruptions. The uncertainty surrounding both risks (unknown service and host status) increases their criticality, as unaddressed vulnerabilities could remain undetected.

3. Risk Assessment and Explanation

Risk 1: Unknown Service on Open Port 6783/tcp (192.168.1.93)

- **Explanation**:
    - Open ports are prime targets for attackers, who use tools like Nmap to identify exploitable services. The "unknown" label for port 6783/tcp indicates that the service could not be identified by Nmap's service detection, possibly due to a non-standard or custom application.
    - Without knowing the service, it's impossible to assess specific vulnerabilities (e.g., CVEs) or apply targeted patches. This uncertainty increases the risk, as the service could be misconfigured, unpatched, or inherently insecure.
    - Potential attack scenarios include:
        - **Exploitation**: If the service is vulnerable, attackers could gain unauthorized access, escalating privileges or deploying malware.
        - **Data Exfiltration**: The service might allow data leakage if it handles sensitive information.
        - **Denial of Service**: Attackers could target the service to disrupt its functionality.
    - The host (192.168.1.93, identified as an Apple device) may be a workstation or server, amplifying the impact if compromised.
- **Risk Assessment**:
    - **Likelihood**: High (4/5). Open ports are easily discovered by attackers, and unknown services are often poorly monitored or secured.
    - **Impact**: High (4/5). Compromise could lead to data breaches, malware propagation, or network-wide attacks.

- **Risk Score**: Likelihood (4) × Impact (4) = 16/25 (Critical).

Risk 2: Non-Responsive Host (192.168.1.253)

- **Explanation**:
  - The host's non-responsiveness during scans could result from:
    - **Network Issues**: Misconfigured firewall or routing preventing scan responses.
    - **Active Blocking**: Security measures (e.g., IPS/IDS) blocking Nmap probes, potentially hiding vulnerabilities.
    - **Downtime/Compromise**: The host may be offline due to failure or compromise, especially if it's a critical asset like a server.
  - As an Apple device (per scan results), it could be a workstation or server critical to operations. If blocking scans, it may conceal vulnerabilities, delaying detection and remediation. If offline, it could disrupt services or indicate a prior compromise.
  - Potential attack scenarios include:
    - **Hidden Exploits**: Unscanned vulnerabilities could be exploited by attackers who bypass blocking mechanisms.
    - **Operational Disruption**: Downtime of a critical asset affects productivity or service availability.
    - **Compromise Detection Failure**: A compromised host might remain undetected if not scanned.
- **Risk Assessment**:
  - **Likelihood**: Moderate (3/5). The cause is unclear, but active blocking or compromise is plausible in a network with identified vulnerabilities.
  - **Impact**: High (4/5). Hidden vulnerabilities or downtime could lead to significant operational or security impacts.
  - **Risk Score**: Likelihood (3) × Impact (4) = 12/25 (Critical).

4. Risk Treatment Recommendations

Risk 1: Unknown Service on Open Port 6783/tcp

- **Treatment Strategy**: Mitigate and Reduce.
    - **Rationale**: Closing the port or securing the service reduces the attack surface while maintaining functionality if the service is legitimate. Complete avoidance (e.g., shutting down the host) is impractical without understanding the service's role.
- **Mitigation Steps**:
    - **Service Identification**:
        - Use advanced scanning tools (e.g., nmap -sV -p 6783 --script http-title,ssl-cert) to identify the service.
        - Analyze host logs or network traffic (e.g., using Wireshark) to determine the service's purpose.
    - **Port Closure (if unnecessary)**:
        - If the service is not required, disable it via host configuration (e.g., stop the service, update firewall rules to block port 6783).
    - **Service Hardening (if necessary)**:
        - Apply patches or configuration changes if the service is identified and vulnerable.
        - Restrict access to the port using firewall rules (e.g., allow only specific IPs).
    - **Monitoring**:
        - Deploy an IDS/IPS to monitor traffic to port 6783 for suspicious activity.
        - Set up alerts for unauthorized access attempts.
- **Justification**:
    - Identifying the service is critical to assess its necessity and vulnerabilities. Closing unnecessary ports eliminates the risk, while hardening essential services balances security and functionality. Monitoring ensures ongoing protection against exploitation attempts.

Risk 2: Non-Responsive Host

- **Treatment Strategy**: Mitigate and Investigate.

    - **Rationale**: Investigating the host's status and security posture reduces the risk of hidden vulnerabilities or downtime. Transferring or avoiding the risk is not feasible, as the host may be critical.

- **Mitigation Steps**:
    - **Host Status Verification**:
        - Physically or remotely check if the host is online (e.g., ping, SSH, or console access).
        - Review network configurations (e.g., firewall rules, routing tables) to identify scan blocking.
    - **Comprehensive Scanning**:
        - If online, perform targeted scans (e.g., nmap -Pn -sV --script vuln) to bypass host discovery and identify vulnerabilities.
        - Use alternative tools (e.g., Nessus) for deeper vulnerability assessment.
    - **Security Hardening**:
        - If vulnerabilities are found, apply patches, update configurations, or isolate the host.
        - If blocking scans, ensure legitimate security measures (e.g., IPS) are configured correctly without hiding issues.
    - **Redundancy (if critical)**:
        - If the host is critical and offline, implement failover mechanisms (e.g., backup servers) to maintain operations.
- **Justification**:
    - Verifying the host's status clarifies whether the risk stems from downtime, blocking, or compromise. Comprehensive scanning ensures vulnerabilities are not missed, while hardening or redundancy mitigates impacts. This approach balances thorough investigation with operational continuity.

5. Risk Monitoring Procedure

Procedure: Continuous Network Risk Monitoring

Objective: Track identified risks (e.g., unknown service on port 6783/tcp, non-responsive host) to detect changes, new threats, or mitigation effectiveness.

Steps:

1. **Establish Monitoring Tools**:
    - Deploy a **SIEM system** (e.g., Splunk, ELK Stack) to aggregate logs from hosts, firewalls, and IDS/IPS.
    - Use **network monitoring tools** (e.g., Nagios, Zabbix) to track host availability and port status.
    - Integrate **EDR solutions** (e.g., CrowdStrike, Microsoft Defender) for endpoint monitoring.
    - **Justification**: Centralized tools provide real-time visibility into network and host activities, enabling rapid detection of anomalies.
2. **Define Monitoring Parameters**:
    - **For Risk 1 (Port 6783/tcp)**:
        - Monitor traffic to/from port 6783 on 192.168.1.93 for unauthorized access or unusual patterns.
        - Track service status (e.g., running, stopped) and any new vulnerabilities via CVE databases.
    - **For Risk 2 (Non-Responsive Host)**:
        - Monitor host availability (192.168.1.253) via ping or service checks.
        - Track scan results for changes in responsiveness or detected vulnerabilities.
    - **Justification**: Specific parameters ensure focused monitoring of high-risk areas, reducing noise and improving detection accuracy.
3. **Set Up Alerts**:
    - Configure alerts for:
        - Unauthorized access attempts to port 6783 (e.g., multiple failed connections).
        - Changes in host 192.168.1.253 status (e.g., suddenly responsive or offline).

        - New vulnerabilities associated with identified services.
    - Route alerts to the security team via email or a ticketing system (e.g., ServiceNow).
    - **Justification**: Automated alerts enable timely response to potential incidents, minimizing damage.

4. **Periodic Review and Scanning**:
    - Conduct weekly Nmap scans (nmap -sV --script vuln 192.168.1.0/24) to detect changes in open ports or services.
    - Review SIEM and EDR logs bi-weekly to identify trends or anomalies.
    - Update risk assessments quarterly or after significant network changes.
    - **Justification**: Regular reviews and scans ensure risks remain mitigated and new threats are identified promptly.

5. **Document and Report**:
    - Log all monitoring activities, alerts, and scan results in a centralized repository (e.g., Confluence, SharePoint).
    - Generate monthly risk reports summarizing findings, mitigation status, and recommendations.
    - **Justification**: Documentation ensures accountability, supports audits, and informs future risk management decisions.

Frequency:

- Real-time monitoring via SIEM/EDR.
- Weekly scans and bi-weekly log reviews.
- Monthly reporting and quarterly risk reassessments.

Responsible Parties:

- **Security Analyst**: Configures and monitors SIEM/EDR, reviews logs, and responds to alerts.
- **Network Administrator**: Conducts scans, verifies host status, and implements mitigations.
- **Security Manager**: Reviews reports, approves mitigation plans, and ensures compliance.

Justification for Procedure:

- The procedure combines automated monitoring (SIEM, EDR) with periodic manual checks (scans, reviews) to balance proactive detection and resource efficiency. It focuses on critical risks while maintaining network-wide visibility, ensuring timely identification of new threats or mitigation failures. Assigning clear roles enhances accountability and response effectiveness.

6. Conclusion

This report demonstrates a comprehensive approach to cybersecurity risk management by identifying, assessing, treating, and monitoring risks derived from vulnerability scan results. The two critical risks—unknown service on port 6783/tcp and non-responsive host at 192.168.1.253—were prioritized due to their high likelihood and severe potential impacts, including system compromise and operational disruption. Mitigation steps, such as service identification, port closure, host verification, and comprehensive scanning, address these risks effectively while maintaining functionality. The continuous network risk monitoring procedure ensures ongoing vigilance through automated tools, periodic reviews, and clear documentation.

By implementing these strategies, organizations can reduce their attack surface, detect threats promptly, and maintain a robust security posture. The justified decisions—prioritizing critical risks, balancing mitigation with functionality, and establishing structured monitoring—align with industry best practices and enhance resilience against cyber threats.

7. References

- NIST SP 800-30: Guide for Conducting Risk Assessments.
- MITRE ATT&CK Framework: https://attack.mitre.org/.
- Nmap Documentation: https://nmap.org/book/man.html.
- OWASP Risk Assessment Framework: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology.