Name: Sithulisiwe

Surname: Peko

Task 1: Cybersecurity Risk Assessment

1. Threat Identification

Sample Network/System Setup:

Assume the network setup consists of the following key components:

Web server: Makes a website accessible to the public.

Database Server: Holds private user information, such as payment information and login passwords.

Workstations: used by staff members for daily tasks and linked to the internal network of the business.

The perimeter devices that guard access to the internal network are the firewall and router.

Secure remote network access is made possible via a VPN gateway.

Backup Storage: Important data stored offline.

Potential Threats:

External Attacks:

SQL Injection: SQL injection attacks provide hackers access to or control over the database on the web server that hosts a website that is visible to the public.

Web applications that are susceptible to cross-site scripting (XSS) could let hackers insert malicious code onto other users' web sites.

Distributed Denial of Service (DDoS): To overwhelm the web server or VPN gateway and result in service interruptions, an attacker may initiate a DDoS attack.

- Internal Threats:

Insider Threats: Workers who have too many privileges may abuse them or unintentionally reveal private information.

Malware: Workstations may get infected with malware, which might then propagate throughout the network and jeopardies private information.

Network Vulnerabilities:

Weak Firewall Rules: Inadequately set firewalls may allow unapproved access to the network by leaving open ports.

Unpatched Software: Older software on workstations, servers, or network equipment may have known security flaws that hackers could take advantage of.

2. Vulnerability Scanning

Tools Used:

Nmap: A tool for network mapping that finds open ports and server services.

Wireshark: Recorded and examined network traffic to find suspicious activities or sensitive information that wasn't encrypted.

Findings:

Web Server:

Open ports that could be subject to brute force attacks or illegal access include HTTP (80), HTTPS (443), and SSH (22).

Vulnerabilities include an old PHP version that is vulnerable to known exploits (Severity: High) and SQL Injection discovered in the login form (Severity: Critical).

Database Server:

Open ports: MySQL (3306); if firewall restrictions are lax, this port could be accessible remotely.

Vulnerabilities: No encryption for stored passwords (Severity: High), weak password policy for database access (Severity: High).

Workstations:

Older Microsoft Office versions that are susceptible to remote code execution were found to have unpatched software (Severity: Medium).

Trojan horses on two computers with the ability to spread laterally were identified as the malware signature (Severity: High).

Router and firewall:

Internet-accessible open ports include FTP (21), RDP (3389) (Severity: Critical).

Vulnerabilities: Some routers have default credentials that give attackers control over network traffic (Severity: Critical).

3. Risk Analysis

Risk Assessment:

High Risk:

Web server SQL injection could result in data breaches by giving hackers the ability to retrieve or alter private data.

Weak firewall configuration—allowing attackers to obtain unauthorized access by exposing vital services like FTP or RDP to the internet.

An entry point for attackers to take advantage of known flaws in outdated software.

Medium Risk

Workstation malware is now confined but has the potential to propagate.

Weak password rules can be countered by stricter authentication, although they may still permit brute-force or password guessing attacks.

Low Risk:

Misconfigured SSL/TLS on the web server—while still a vulnerability, it is lower priority compared to others and can be fixed easily by enforcing stronger encryption protocols.

4. Mitigation Strategies

High-Risk Mitigation:

SQL Injection:

Implement input validation and use prepared statements to prevent injection attacks. Regularly update and patch web application frameworks.

Weak Firewall Rules:

Reconfig the firewall to restrict access to trusted IPs and disable unused ports (such as FTP and RDP).

To guarantee security, perform penetration tests on a regular basis.

Outdated Software:

Patch or upgrade susceptible systems right away.

Plan security checks and software updates on a regular basis.

Medium-Risk Mitigation:

Malware on Workstations:

Conduct a full malware sweep and isolate infected machines.

Implement endpoint protection software (antivirus, EDR solutions) and conduct regular scans.

Weak Password Policies:

Implement multi-factor authentication (MFA) across the network.

Enforce strong password policies (e.g., minimum length, complexity requirements).

Low-Risk Mitigation:

SSL/TLS Misconfiguration:

Enforce the use of strong SSL/TLS configurations (e.g., TLS 1.2/1.3, disable weak ciphers).

Conduct regular security scans of the server configuration.

5. Report and Presentation

Report: Title: Cybersecurity Risk Assessment Report

Scope: Identifying and assessing vulnerabilities within a sample network including web server, database server, workstations, and network devices.

Findings: Several critical and high-severity vulnerabilities were identified, including SQL injection, weak firewall rules, outdated software, and malware on workstations.

Mitigation Recommendations: Immediate patching of outdated software, reconfiguration of firewall settings, implementation of stronger password policies, and improving endpoint security.

Next Steps: Regularly monitor the network for new vulnerabilities, conduct quarterly penetration testing, and train employees on recognizing phishing and malware.

Presentation Summary:

Overview: Presented key vulnerabilities found in the network setup.

High-Risk Areas: Focused on critical issues like SQL injection and weak firewall rules.

Mitigation Strategies: Discussed immediate actions to reduce risks, including patch management, firewall reconfiguration, and improving employee security awareness.

Incident Response Simulation Report

1. Scenario Creation:

Scenario:

An executive employee was the target of a pear-phishing assault, which led to the installation of a remote access trojan on their computer. The attacker has now turned to try lateral movement across the network to get to the database server after the RAT successfully exfiltrated sensitive data.

Objectives:

Detect the malicious activity in the network.

Implement containment measures to limit the attacker’s movement.

Conduct forensic analysis to understand the attack vector and identify compromised systems

2. Incident Detection

Tools Used:

Splunk/ELK Stack: Used to monitor logs in real time and identify irregularities.

Wireshark: To find odd outgoing connections to dubious IP addresses, it captured traffic.

Detection Process

Log Analysis: Unusual login timings and the emergence of an unknown process (RAT) are among the anomalies found in the system logs.

Traffic Analysis: Wireshark was used to identify suspicious outgoing traffic to recognize Command and Control (C2) servers.

3. Response Plan Execution

Actions Taken:

Containment: To stop more lateral movement, the infected workstation was disconnected from the network.

Eradication: A complete system restore from a clean backup was started when the RAT was eliminated from the compromised system.

Communication: TheHive was used by the incident response team to coordinate, making sure that every step was recorded.

4. Forensic Analysis

Tools Used:

GRR Rapid Response: Used to perform live remote forensics and capture memory dumps.

The Hive: Centralized incident response platform for managing forensic evidence and coordinating team efforts.

Findings:

The RAT was delivered via a spear-phishing email with a malicious attachment.

Forensic evidence indicates the attacker attempted to escalate privileges on the compromised system.

5. Post-Incident Assessment

Review:

Effectiveness of Response: The containment procedures were effective, limiting lateral movement.

Areas for Improvement: More robust email filtering to prevent phishing emails from reaching users.

Lessons Learned: Enhanced user training to spot phishing attempts is necessary. Further implementation of behavior-based detection systems could have identified the RAT earlier.

6. Documentation and Presentation

Incident Report:

Title: Spear-Phishing Incident Response and Forensics Report

Summary: Detailed steps of the incident detection, containment, and eradication efforts, along with forensic findings.

Presentation:

Incident Overview: Presented the timeline and actions taken during the incident.

Key Findings: Focused on how the RAT was identified, contained, and removed.

Recommendations: Suggested improvements in email security, endpoint monitoring, and user awareness training.