Question 1

ShieldsUP!

Starting with the ShieldsUP Scans, I ran the common service port scan first. This scan took only 5 seconds and showed that my system passed with a perfect "TruStealth" rating of the selected ports from 0 to 5000. I opened another tab and ran the other scan for all service ports. This one took 69 seconds and just like the other scan, it passed with a perfect "TruStealth" rating for the first 1056 TCP ports.

Tenable Nessus

Like my first report, I went to [REDACTED] to do the Nessus vulnerability scan. I first downloaded it onto [REDACTED] mac and waited a bit for the plugin compilers to finish. After that finished, all I did was type in [REDACTED] to capture all the devices on the network, and from there I ran the scan. The first scan simply detects all hosts on the network. After that one was completed, I removed my phone from the list of devices as it does not pertain to the business. For the actual network scan, this did take 13 minutes to complete, most of the devices showed that they completed very quickly, but the router was taking the longest. Either way, after the scan finished, I exported the results as a .nessus file, went home, and loaded them up on my PC to view.

How it Works (ShieldsUP!)

ShieldsUP is an online service provided by Gibson Research Corporation that checks the security of a computer's Internet connection. It focuses primarily on testing the exposure of the system to the internet by scanning ports and checking for vulnerabilities related to those ports.

How It Works:

1. **Common Service Port Scan:**
   - **Purpose:** To check the status (open, closed, stealth) of common service ports, which are frequently targeted by attackers.
   - **Process:** The scan involves sending packets to a list of well-known ports (such as 80 for HTTP, 443 for HTTPS, etc.) and observing how the system responds.
   - **Output:**
     - **Open:** The port is accessible and there is a service listening on it.
     - **Closed:** The port is reachable but not open; no service is listening.
     - **Stealth:** The port does not respond to the scan attempt, making it invisible (or "stealth") to the scanner.
2. **All Service Ports Scan:**

  - **Purpose:** Like the common service port scan but includes a broader range of ports, typically from 0 to 1055. This includes both well-known ports and registered ports.
  - **Process:** The scan sends packets to a wider range of ports and observes the system's response, like the common ports scan.
  - **Output:** As with the common service port scan, it reports ports as open, closed, or stealth.

Key Feature:

- **TruStealth Rating:** This indicates that all tested ports did not respond to the scan, making the system appear invisible to potential attackers. Achieving a "TruStealth" rating means that the system does not reply to unsolicited packets, including ping requests.

How it Works (Tenable Nessus)

Nessus is a vulnerability scanner that provides detailed insights into the security status of devices on a network. It performs comprehensive checks for vulnerabilities, configuration issues, and other security flaws.

How It Works:

1. **Installation and Setup:**
   - Nessus is installed on a machine (in my case, a Mac then my Windows PC). It requires an initial setup that includes downloading and compiling plugins, which are scripts that check for specific vulnerabilities.
2. **Host Detection:**
   - **Purpose:** To identify all active devices on the network.
   - **Process:** By scanning the specified IP range (e.g., 192.168.1.0/24), Nessus sends probes to discover devices. It identifies devices based on their responses and the services running on them.
3. **Vulnerability Scanning:**
   - **Purpose:** To find vulnerabilities, misconfigurations, and security issues on the detected devices.
   - **Process:**
     - **Plugins Execution:** Nessus uses a vast library of plugins that check for specific vulnerabilities, outdated software versions, open ports, and other security issues.
     - **Network and Host Assessment:** It can perform both network-based and host-based scans, depending on the configuration.

- **Results Compilation:** After the scan, Nessus compiles a detailed report, highlighting vulnerabilities with severity levels and providing remediation recommendations.

4. **Exporting Results:**

   - The results can be exported in various formats, including .nessus files, which contain detailed information about the scan results.

Key Feature:

- **Comprehensive Security Assessment:** Nessus provides detailed reports on vulnerabilities and security issues, helping administrators identify and mitigate risks.

Question 2

Results (ShieldsUP!)

Common Ports Scan

- **Date & Time of Scan:** 2024-08-04 at 03:17:22 (UTC)
- **Ports Scanned:** 0, 21-23, 25, 79, 80, 110, 113, 119, 135, 139, 143, 389, 443, 445, 1002, 1024-1030, 1720, 5000
- **Results:**
  - **0 Ports Open:** No open ports were found. This means no services were actively listening on these ports.
  - **0 Ports Closed:** No ports were explicitly reported as closed.
  - **26 Ports Stealth:** All the scanned ports were in stealth mode. This means the system did not respond to the port scan probes, making the ports invisible or unresponsive to external scanning attempts.
- **TruStealth Analysis:**
  - **ALL tested ports were STEALTH:** Indicates that the system did not respond to any probes on the tested ports, making it highly secure against external attacks or scans.
  - **NO unsolicited packets were received:** No unexpected or unsolicited traffic was detected, implying that the system is not leaking information or responding to unwanted requests.
  - **NO Ping reply (ICMP Echo) was received:** The system did not respond to ICMP Echo (ping) requests, further increasing its stealthiness.

All Service Ports Scan

- **Date & Time of Scan:** 2024-08-04 at 03:12:06 (UTC)

- **Ports Scanned:** 0-1055 (commonly well-known ports)
- **Results:**
  - **0 Ports Open:** No open ports were found within the scanned range.
  - **0 Ports Closed:** No ports were explicitly reported as closed.
  - **1056 Ports Stealth:** All the scanned ports were in stealth mode.
- **TruStealth Analysis:**
  - **ALL tested ports were STEALTH:** The system did not respond to any probes on the ports, indicating a high level of security.
  - **NO unsolicited packets were received:** No unexpected or unsolicited traffic was detected.
  - **NO Ping reply (ICMP Echo) was received:** The system did not respond to ICMP Echo requests.

Interpretation

Both scans on my network indicate that it is well-protected and secure. All ports are in "stealth" mode, which means they do not respond to external scanning attempts. This setup is ideal for security, as it prevents potential attackers from gathering information about the services running on the system. Stealth mode effectively hides the system's presence on the network, reducing the likelihood of becoming a target for attacks. Additionally, not responding to ping requests further increases security by preventing network mapping and discovery.

Results (Nessus)

Hosts Scan

- **Command Used:** [REDACTED]
- **Hosts Detected:** 7 (6 used)
  - [REDACTED]**:** imac-3.home (macOS 14.5)
  - [REDACTED]**:** router.home
  - [REDACTED]**:** imac.home (Darwin)
  - [REDACTED]**:** imac-2.home (Mac OS X 10.4)
  - [REDACTED]**:** [REDACTED]-imac.home (Mac OS X 10.4)
  - [REDACTED]**:** Xerox Printer

Vulnerability Scan

- **Date & Time of Scan:**
  - **Start:** August 3rd at 8:31 PM
  - **End:** August 3rd at 8:44 PM
- **Severity Base:** CVSS v3.0

- **Results:**
    - **Vulnerabilities:** 66 total vulnerabilities
    - [REDACTED]**:** 1 high severity, 2 medium severity, 83 info
    - [REDACTED]: 4 medium severity, 3 low severity, 44 info
    - [REDACTED]**:** 29 info
    - [REDACTED]**:** 18 info
    - [REDACTED]**:** 18 info
    - [REDACTED]**:** 13 info
- **Severity Analysis:**
    - **High:** macOS 14.x < 14.6 Multiple Vulnerabilities (HT214119)
        - **Severity:** High
        - **ID:** 204837
        - **Version:** 1.2
        - **Type:** local
        - **Family:** MacOS X Local Security Checks
        - **Published:** July 29, 2024
        - **Modified:** August 2, 2024
        - **Threat Recency:** 0 to 7 days
        - **Threat Intensity:** Very High
        - **Exploit Code Maturity:** PoC
        - **Age of Vuln:** 30 - 60 days
        - **Product Coverage:** Very HighCVSSV3
        - **Impact Score:** 5.9
        - **Threat Sources:** Social Media
        - **Vulnerability Priority Rating (VPR):** 9.4
        - **Exploit Prediction Scoring System (EPSS):** 0.7147
        - **Risk Factor:** High
        - **CVSS v3.0 Base Score:** 8.1
        - **Solution:** Upgrade to macOS 14.6 or later
    - **Medium:** Ruby < 3.0.7 / 3.1.x < 3.1.5 / 3.2.x < 3.2.4 / 3.3.x < 3.3.1 RCE
        - **Severity:** Medium
        - **ID:** 200138
        - **Version:** 1.2
        - **Type:** local
        - **Family:** Misc.
        - **Published:** June 6, 2024
        - **Modified:** June 7, 2024
        - **Threat Recency:** No recorded events

    - **Threat Intensity:** Very Low
    - **Exploit Code Maturity:** Unproven
    - **Age of Vuln:** 60 - 180 days
    - **Product Coverage:** LowCVSSV3
    - **Impact Score:** 3.4
    - **Threat Sources:** No recorded events
    - **Vulnerability Priority Rating (VPR):** 3.4
    - **Risk Factor:** Low
    - **CVSS v3.0 Base Score:** 4.5
    - **Solution:** Upgrade to Ruby version 3.0.7 / 3.1.5 / 3.2.4 / 3.3.1 or later.
  - **Medium:** SSL Certificate Cannot Be Trusted
    - **Severity:** Medium
    - **ID:** 51192
    - **Version:** 1.19
    - **Type:** remote
    - **Family:** General
    - **Published:** December 15, 2010
    - **Modified:** April 27, 2020
    - **Risk Factor:** Medium
    - **CVSS v3.0 Base Score:** 6.5
    - **Solution:** Purchase or generate a proper SSL certificate for this service.
  - **Medium**: IP Forwarding Enabled
    - **Severity:** Medium
    - **ID:** 50686
    - **Version:** 1.16
    - **Type:** remote
    - **Family:** Firewalls
    - **Published:** November 23, 2010
    - **Modified:** October 17, 2023
    - **Threat Recency:** No recorded events
    - **Threat Intensity:** Very Low
    - **Exploit Code Maturity:** Unproven
    - **Age of Vuln:** 730 days +
    - **Product Coverage:** Low
    - **CVSSV3 Impact Score:** 3.7
    - **Threat Sources:** No recorded events
    - **Vulnerability Priority Rating (VPR):** 4.0
    - **Exploit Prediction Scoring System (EPSS):** 0.0035

    - **Risk Factor:** Medium
    - **CVSS v3.0 Base Score:** 6.5
    - **Solution:** On Mac OS X, you can disable IP forwarding by executing the command: sysctl -w net.inet.ip.forwarding=0
  - **Medium:** SSL Certificate Cannot Be Trusted
    - **Severity:** Medium
    - **ID:** 51192
    - **Version:** 1.19
    - **Type:** remote
    - **Family:** General
    - **Published:** December 15, 2010
    - **Modified:** April 27, 2020
    - **Risk Factor:** Medium
    - **CVSS v3.0 Base Score:** 6.5
    - **Solution:** Purchase or generate a proper SSL certificate for this service.
  - **Medium: SSL Self-Signed Certificate**
    - **Severity:** Medium
    - **ID:** 57582
    - **Version:** 1.6
    - **Type:** remote
    - **Family:** General
    - **Published:** January 17, 2012
    - **Modified:** June 14, 2022
    - **Risk Factor:** Medium
    - **CVSS v3.0 Base Score:** 6.5
    - **Solution:** Purchase or generate a proper SSL certificate for this service.
  - **Medium:** TLS Version 1.1 Deprecated Protocol
    - **Severity:** Medium
    - **ID:** 157288
    - **Version:** 1.4
    - **Type:** remote
    - **Family:** Service detection
    - **Published:** April 4, 2022
    - **Modified:** May 14, 2024
    - **Risk Factor:** Medium
    - **CVSS v3.0 Base Score:** 6.5
    - **Solution:** Enable support for TLS 1.2 and/or 1.3 and disable support for TLS 1.1.

- **Low:** SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
    - **Severity:** Low
    - **ID:** 69551
    - **Version:** 1.4
    - **Type:** remote
    - **Family:** General
    - **Published:** September 3, 2013
    - **Modified:** November 15, 2018
    - **Risk Factor:** Low
    - **Solution:** Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.
- **Low:** DHCP Server Detection
    - **Severity:** Low
    - **ID:** 10663
    - **Version:** 1.24
    - **Type:** remote
    - **Family:** Service detection
    - **Published:** May 5, 2001
    - **Modified:** March 6, 2019
    - **Risk Factor:** Low
    - **CVSS v2.0 Base Score:** 3.3
    - **Solution:** Apply filtering to keep this information off the network and remove any options that are not in use.
- **Low:** ICMP Timestamp Request Remote Date Disclosure
    - **Severity:** Low
    - **ID:** 10114
    - **Version:** 1.53
    - **Type:** remote
    - **Family:** General
    - **Published:** August 1, 1999
    - **Modified:** May 3, 2024
    - **Threat Recency:** No recorded events
    - **Threat Intensity:** Very Low
    - **Exploit Code Maturity:** Unproven
    - **Age of Vuln:** 730 days +
    - **Product Coverage:** Very High
    - **CVSSV3 Impact Score:** 3.4

- **Threat Sources:** No recorded events
- **Vulnerability Priority Rating (VPR):** 4.2
- **Exploit Prediction Scoring System (EPSS):** 0.8808
- **Risk Factor:** Low
- **CVSS v2.0 Base Score:** 2.1
- **Solution:** Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Interpretation

The Nessus scan results indicate several vulnerabilities across the network's devices, with a mix of high, medium, and low-severity issues. The high-severity vulnerability on the macOS device [REDACTED] is the most critical and should be addressed immediately by updating to the latest OS version.

The medium-severity issues are mostly related to outdated protocols, self-signed or untrusted SSL certificates, and potential configuration issues like IP forwarding. These issues, while not immediately critical, pose security risks that should be mitigated to prevent potential exploitation.

The low-severity issues generally relate to less critical security concerns but should still be considered, especially if they can be easily resolved.

Practical Uses of Analysis Results

1. **Improving Network Security Posture:**
    - **ShieldsUP! Findings:** The fact that all ports are in stealth mode suggests a strong initial security posture. This configuration makes the system resistant to external probing and attacks. However, ensuring that this stealth mode remains intact is crucial. Regular scans can help detect any accidental exposure to ports.
    - **Nessus Findings:** The detection of vulnerabilities, particularly the high-severity issue on macOS, underscores the importance of timely software updates. Addressing these vulnerabilities promptly can prevent potential exploitation by attackers.
2. **Implementing Mitigation Strategies:**
    - **High-Severity Vulnerability:** The macOS device should be updated to the latest version (14.6) to patch the critical vulnerabilities. This action reduces the risk of potential breaches and ensures the system is protected against known exploits.
    - **Medium-Severity Issues:** Issues like outdated SSL certificates, deprecated protocols, and IP forwarding can be mitigated by:

  - Acquiring trusted SSL certificates from reputable certificate authorities to replace self-signed ones.
  - Disabling outdated protocols like TLS 1.1 and enforcing the use of modern protocols such as TLS 1.2 or TLS 1.3.
  - Disabling IP forwarding unless explicitly required for network functionality, as it can inadvertently expose internal systems to external threats.

3. **Continuous Monitoring and Auditing:**
   - **Periodic Vulnerability Scans:** Regular vulnerability assessments using tools like Nessus should be scheduled to identify new vulnerabilities as they arise. This practice helps in maintaining a secure network environment and allows for quick response to potential threats.
   - **Log Analysis and Network Monitoring:** Implementing robust logging and monitoring can help detect unusual activities, such as unauthorized access attempts or data exfiltration. This proactive approach can provide early warning signs of security incidents.
4. **User Awareness and Training:**
   - Educating users about potential security risks, such as phishing attacks and the importance of strong, unique passwords, can complement technical defenses. Awareness programs can help prevent social engineering attacks that bypass technical safeguards.
5. **Network Segmentation and Access Control:**
   - Using the information about network devices and their vulnerabilities, administrators can implement network segmentation to isolate critical systems from less secure areas of the network. Access control measures, such as firewalls and intrusion detection/prevention systems, can further protect sensitive data and resources.
6. **Incident Response Planning:**
   - Having an incident response plan that includes steps for addressing detected vulnerabilities and potential breaches is essential. The analysis results can inform the prioritization of response actions based on the severity of identified vulnerabilities.

Question 3

Key Takeaways from the Assignment

1. **Understanding of Network Security Posture**:
    - ShieldsUP provided a clear picture of the system's exposure to the internet, emphasizing the importance of keeping ports in stealth mode to minimize visibility to potential attackers.
    - Nessus offered a comprehensive view of the vulnerabilities present in the network's devices, highlighting the critical nature of keeping software and systems up to date.
2. **Importance of Regular Scanning**:
    - Regular vulnerability scanning is essential to identify and mitigate potential security weaknesses before they can be exploited. This practice helps maintain a proactive security posture, reducing the risk of data breaches and unauthorized access.
3. **Value of Detailed Vulnerability Reporting**:
    - The detailed reports generated by tools like Nessus provide valuable insights into the specific vulnerabilities present, including their severity, potential impact, and recommended remediation steps. This information is crucial for prioritizing security efforts and ensuring that the most critical issues are addressed first.
4. **Security Configuration Best Practices**:
    - The findings emphasized the importance of proper security configurations, such as disabling unnecessary services, using strong encryption, and ensuring that only necessary ports are open.
5. **The Role of User Awareness**:
    - Technical measures alone are not enough; user awareness and training play a crucial role in preventing social engineering attacks and ensuring that security policies are followed.

Future Uses

In the future, I can leverage the knowledge gained from this assignment in several ways:

1. **Routine Security Audits**:
    - Implementing regular vulnerability scans as part of the organization's security protocol will help identify and address vulnerabilities before they are exploited.

This proactive approach will ensure continuous improvement in the organization's security posture.

2. **Security Baseline Establishment**:
    - Using tools like Nessus, I can establish a security baseline for systems and networks. This baseline will serve as a reference point for assessing the impact of changes and updates on the security posture.
3. **Incident Response and Forensics**:
    - In case of a security incident, vulnerability scanning can help quickly identify compromised systems and the vulnerabilities exploited, aiding in incident response and forensic analysis.
4. **Security Awareness Training**:
    - The insights gained from vulnerability assessments can be used to develop targeted security awareness training for employees, focusing on the specific threats and vulnerabilities relevant to the organization.

Organizational Use

For [REDACTED], the implementation of vulnerability scanning offers specific benefits:

1. **Protection of Sensitive Client Data**:
    - As an insurance company, [REDACTED] handles sensitive client information, including personal and financial data. Regular vulnerability scans help ensure that this data is protected from unauthorized access and potential breaches.
2. **Compliance with Insurance Regulations**:
    - The insurance industry is subject to strict regulatory requirements regarding data protection and cybersecurity. Vulnerability scanning helps [REDACTED] comply with these regulations, such as those related to the protection of personally identifiable information (PII) and financial data. Compliance reduces the risk of legal repercussions and penalties.
3. **Business Continuity and Reliability**:
    - By identifying and mitigating vulnerabilities, [REDACTED] can prevent disruptions caused by cyber incidents. Ensuring the security and reliability of IT systems is crucial for maintaining continuous service to clients, especially during critical

times like natural disasters or market fluctuations when clients rely heavily on insurance support.

4. **Safeguarding Financial Assets**:
    - The company's financial assets, including operational funds and client reserves, can be targeted by cybercriminals. Vulnerability scanning helps protect these assets by identifying and addressing security weaknesses that could be exploited in financial fraud or theft.
5. **Client Trust and Competitive Advantage**:
    - Demonstrating a commitment to cybersecurity can enhance client trust in [REDACTED]. Clients are more likely to choose a company that prioritizes the security of their information. This dedication to cybersecurity can also serve as a competitive advantage in the market, distinguishing [REDACTED] from other providers.
6. **Internal Efficiency and Cost Management**:
    - Identifying vulnerabilities early allows for efficient allocation of resources to address issues before they escalate into costly incidents. By prioritizing remediation efforts, the company can manage its security budget effectively, ensuring funds are directed to the most critical areas.