|  |  |
| --- | --- |
| the5 System Scan Report Prepared for Hotel Dorsey | Haverbrook security lab corporate logo  Name: Jordan Lee  Team Number: 2  Student Number: 3 |

**Introduction:**

This report was created to perform systems scans on Hotel Dorsey's network to find exploitable vulnerabilities and other critical threats. Penetration testers and security analysts utilized Kali, a Linux distribution, as an attack machine against the Hotel's internal network. Kali Linux allowed us to use Zenmap and OpenVAS, which are good scanning tools. Zenmap utilizes a GUI (graphical user interface) and provides all the activated and open ports within a network. Each scan guarantees that the Hotel's system and network are protected against every known vulnerability. OpenVAS is a tool developed by Greenbone Networks that tests and scans the system against all known vulnerabilities. This tool is essential because every vulnerability can be exploited, and every exploitable vulnerability that the system has given hackers one more way into the system.

**Target:**

|  |  |  |
| --- | --- | --- |
| **IP Address** | **Hostname** | **Open Ports** |
| **10.2.3.50** | Kali Linux (Attacker Machine) | Scan showed no open ports |
| **10.23.100** | Metasploit (Victim Machine) | **Port 22**- (SSH) Secure Shell, used for secure loin, file transfers, and port forwarding.  **Port 53-** (DNS) Domain name service is used for domain name resolution. The hotel should not open this port if it uses a DNS server due to potential attacks.  **Port 111**- (RPC) used by the portmapper service to map Remote Procedure Call programs and versions to specific transport port numbers.  **Port 139**- This port is used for NetBIOS. A protocol used for File and Print Sharing under all current versions of Windows.  **Port 445**- Is used for direct TCP/IP Microsoft Networking access without the need for a NetBIOS layer. Leaving port 445 open leaves Windows machines vulnerable to trojans and worm attacks.  **Port 3306**- This port is used by MySQL database server connections  **Port 25**- This port is used for (STMP) Simple Mail Transfer Protocol. The port is used for email servers, so if the company doesn't host one, it should not be used.  **Port 23**- This port is designated for Telnet, one of the oldest Internet protocols. It is used to  **Port 21**- (FTP) Port 21 is primarily utilized for File Transfer Protocol (FTP) file transfers and can be utilized by various network devices to monitor network traffic.  **Port 80**- (HTTP) Hyper Text Transfer Protocol. This port should be disabled unless the hotel is running any web services.  **Port 514**- Interactive shell utilizes this port.  **Port 2049**- (NFS) Network File System. This is used for remote filesystem access.  **Port 512**- Automatic authentication using privileged port numbers takes place on this port.  **Port 8009**- Tomcat is a Java HTTP web server environment that enables Java code to execute, and the Apache Tomcat service uses this port.  **Port 8180**- This is an unassigned port.  **Port 5432**- PostgreSQL Database Server, an object-relational database management system.  **Port 1524**- The Ingres database, a SQL database, uses this port; however, hackers primarily use it for Distributed Denial of Service (DDoS) trojans and backdoor viruses.  **Port 6667**-  **Port 1099**- RMIRegistry, a service that establishes and launches a remote object registry, uses this port.  **Port 513**- Automatic authentication using privileged port numbers takes place on this port. |

**Zenmap Scan:**

The four images below show some of the Zenmap scan results on the victim machine. From the scan results, penetration testers and security analysts can see what ports are open and closed. The results also show basic networking settings from the target machine. An intense scan was utilized on the victim machine (IP address 10.2.3.100), showing that 20 ports were open, and 980 ports were closed. The report reveals open ports, which can be determined based on the company's needs, allowing for some reductions. If Hotel Dorsey uses a DNS server and that port is open, that will create a critical exploit in their system. An open Port 53 can be exploited in DNS-based attacks, such as DNS amplification or reflection attacks. Attackers can abuse open DNS servers to launch distributed denial-of-service (DDoS) attacks against targets by amplifying traffic through Port 53. Closing Port 53 helps prevent the organization's DNS infrastructure from being used maliciously.

Port 22 SSH was discovered to be open during the scan, and whether this port should be open or closed depends on Hotel Dorsey's specific network needs. They can close the port when it is not needed to reduce the attack surface, or they can restrict access and limit the traffic using firewall configurations, allowing for only specific and trusted IP addresses. Hotel Dorsey should only open port 22 when SSH access is essential and, even then, apply restrictions. Port 23 should be closed unless there is a specific, controlled reason to keep it open. This is because Port 23 is associated with Telnet, which is highly insecure due to its lack of encryption. Telnet transmits data, including usernames and passwords, in plain text, making it easy for attackers to intercept sensitive information. Keeping Port 23 closed helps protect against unauthorized access and reduces exposure to man-in-the-middle attacks and credential theft. For remote access, it is best to use SSH (Secure Shell) on Port 22, which provides encrypted communication and is a much safer alternative to Telnet.

A screenshot of a computer

Description automatically generated

**Figure 1:**

**A screenshot of a computer

Description automatically generated**

**Figure 2:**

**A screenshot of a computer

Description automatically generated**

**Figure 3:**

**OpenVAS Scan:**

**A screenshot of a computer

Description automatically generated**

**Figure 4:**

OpenVAS Scan showed 369 results from the scan of the victim machine's IP address, 10.2.3.100. Of that total, 52 vulnerabilities were reported. The scan results are categorized by severity: 16 high-severity threats, 33 medium-severity threats, and three low-severity threats. Five vulnerabilities have a severity score of 10, meaning that these vulnerabilities have the potential to cause severe damage to an organization's network. The outlining vulnerability is the "OS End of Life Detection." This vulnerability is critical because the OS has reached the end of its service life, and the machine is not receiving critical security updates to keep up with evolving security threats.

To remediate these vulnerabilities, the client needs to work through them in order of importance. The "OS End of Life Detection" is the most critical, and it needs to be addressed first. The client can choose a different type of OS or continue service with the same OS by upgrading to a newer version of that OS. If the client does not address this vulnerability, they run the risk of becoming vulnerable to malware, cyber-attacks, and data breaches. Since attackers often target unpatched systems, continuing to use an end-of-life OS will put company data and the network at risk. Many industries have strict regulations about using up-to-date, secure software to protect customer data and other sensitive information; by continuing to use an end-of-life OS, the client would not be in compliance and risk fines or penalties.

**Open Socket:**

As mentioned, some ports will return an “unknown” service, as shown in Figure 6 below. The Nmap scan I ran indicates that port 8180 has an unknown service. I type the IP address and port number in the URL to find out what service is running on that port. I type 10.2.3.100:8081 in the URL bar and press enter. The Apache Tomcat service is running on port 8081. The Apache Tomcat service is running on port 8081. Organizations still use this service, but in the case of the client, Hotel Dorsey should consider closing this port whenever it is not in use since the port and service can exploited via Metasploit.

**A screenshot of a computer

Description automatically generated**

**Figure 5:**

A computer screen with a computer screen

Description automatically generated

**Figure 6:**

**Recommendations:**

We are confident that we will be able to exploit the system fully and take not only proprietary data but also personal and financial information. Because we have identified several easily exploitable vulnerabilities in the Hotel's system, we propose an amendment to the contract that includes a comprehensive penetration test of the system. The penetration test results will enable us to provide the Hotel with a complete and secure network environment. It is essential to remember that exploitation of a system does not simply mean that they can see various IP addresses on the network. In addition to replacing outdated operating systems, we strongly recommend performing a full penetration test on the Hotel's IT system and network. This proactive security measure will help identify existing vulnerabilities and weaknesses that could lead to unauthorized access, data theft, or disruption of operations.

Penetration testing simulates real-world attacks on the network, enabling security teams to understand the effectiveness of their defenses. By amending the contract to include this service, we can gain valuable insights into your network's security gaps and provide actionable recommendations for strengthening it, thereby enhancing your overall security posture and instilling confidence in your guests and stakeholders. A penetration test is more than just a technical exercise; it is a strategic step toward comprehensive risk management. In today's threat landscape, companies prioritizing security gain a competitive advantage by building trust with their customers and partners. Amending the contract to include a full penetration test will ensure that your organization's network is fortified against both internal and external threats. Through our thorough testing and analysis, we will help safeguard your company's assets and reputation, ensuring your IT systems remain resilient against cyber threats.

**References:**

[1] Chapple, M., & Seidl, D. (2023). Chapter 7 Analyzing Vulnerability Scans. In CompTIA CySA+ Study Guide Exam CS0-003 (3rd ed., pp. 245–284). essay, John Wiley & Sons, Inc.

[2] Chapple, M., & Seidl, D. (2023). Chapter 8 Responding to Vulnerabilities. In CompTIA CySA+ Study Guide Exam CS0-003 (3rd ed., pp. 293–333). essay, John Wiley & Sons, Inc.

[3] Chapple, M., & Seidl, D. (2023). Chapter 8 Responding to Vulnerabilities. In CompTIA CySA+ Study Guide Exam CS0-003 (3rd ed., pp. 293–333). essay, John Wiley & Sons, Inc.

[4] IT Convergence. (2023, March 9). 5 security issues from using an unsupported operating system. <https://www.itconvergence.com/blog/how-safe-are-your-unsupported-legacy-operating-systems-and-software/>

[5] "Chapter 5: Implementing an Information Security Vulnerability Management Process", Pearson CompTIA Cybersecurity Analyst (CySA+), 2020. [Online]. Available: <https://www.ucertify.com/>.

[6] Nmap. (n.d). Zenmap – Official cross-platform Nmap Security Scanner GUI. Nmap.Org

Retrieved November 1, 2024, from <https://nmap/org/zenmap/>