|  |  |
| --- | --- |
| System Scan Report  Prepared for Hotel Dorsey | Haverbrook security lab corporate logo  Name: XXXXXXXXXXXXX  Team Number: XXX  Student Number: XXX |

Introduction

This report has been prepared for **Hotel Dorsey** as part of a network security assessment designed to identify potential weaknesses and evaluate the overall security posture of the organization’s systems. The purpose of this engagement is to provide Hotel Dorsey with actionable insights into its network vulnerabilities and to recommend measures that will strengthen its defenses against malicious cyber threats.

During this assessment, a combination of automated scanning tools and manual testing methods were employed. Specifically, Zenmap (a graphical interface for Nmap) was used to map the network and identify open ports and services, while OpenVAS was utilized to perform a more comprehensive vulnerability analysis. Manual verification techniques, such as socket testing and banner grabbing, were also applied to validate findings and uncover potential weaknesses that automated tools may not fully reveal.

It is important to note that this report is written for a broad audience, including stakeholders who may not have technical expertise. Therefore, findings are explained in clear, nontechnical language with an emphasis on the business risks posed by identified vulnerabilities. By presenting both the technical evidence and its practical implications, this report aims to equip Hotel Dorsey with the knowledge needed to make informed decisions about improving its cybersecurity posture.

As part of this engagement, I conducted a network security assessment against the client’s designated target system. The purpose of this assessment was to identify which services are visible on the network, determine whether any vulnerabilities exist, and evaluate potential risks to the organization.

The scans were performed from a Kali Linux virtual machine, which is a security-focused operating system commonly used by cybersecurity professionals for penetration testing and vulnerability assessment.

Two primary tools were used during this assessment:

* **Zenmap (Nmap with a graphical interface):**  
  Zenmap is a tool used to map out the network. It identifies which ports are open and which services (such as websites, databases, or remote login services) are available. This gives us a “map” of what is exposed to potential attackers.
* **OpenVAS (Open Vulnerability Assessment System):**  
  OpenVAS goes a step further by comparing the services it finds against a large database of known security flaws. It highlights which versions of software may be outdated or misconfigured and provides a risk rating (from low to critical). This helps prioritize which issues are most urgent to fix.

**Target**

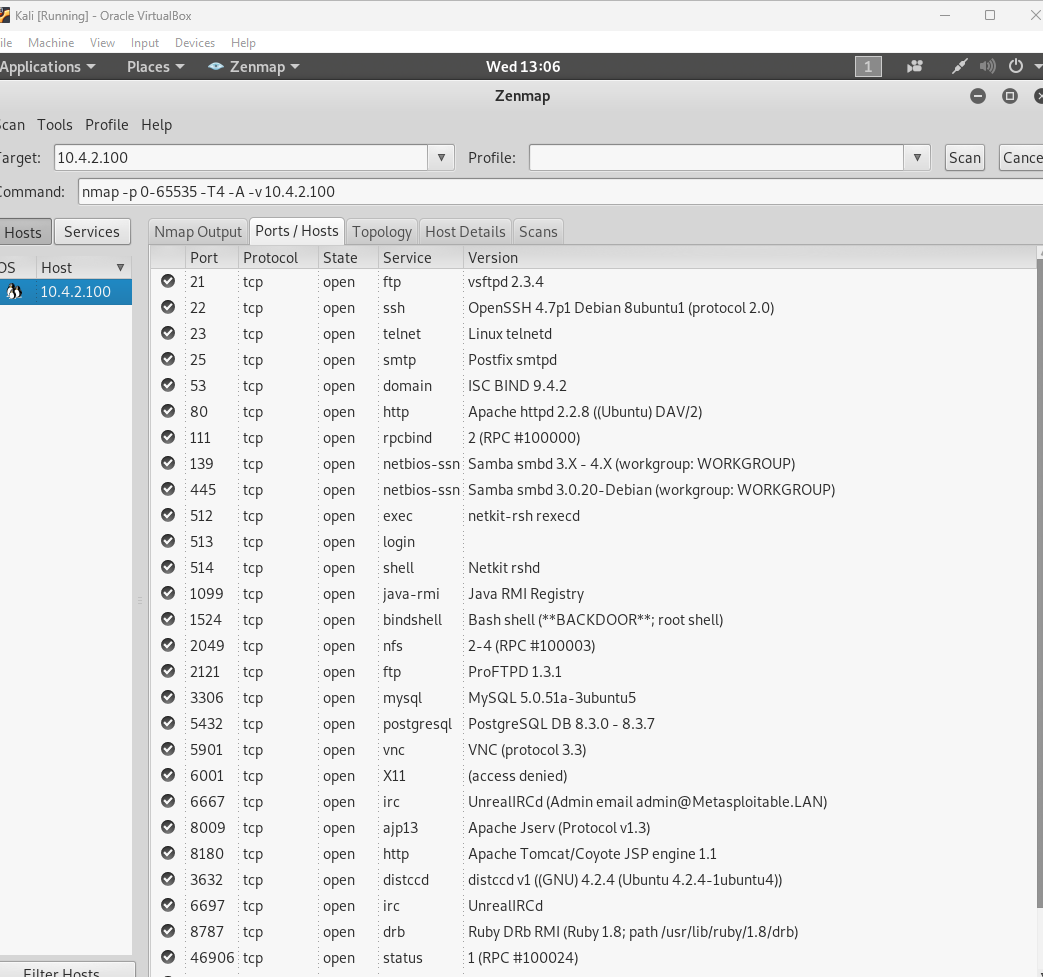
* The assessment was limited to scanning the client’s assigned system at IP address 10.4.2.100.
* The testing was performed remotely from my Kali Linux attack machine at IP address 10.4.2.50

**Scope of Engagement:**

* Only nonintrusive scans were performed (identifying vulnerabilities without exploiting them).
* No changes were made to the target system; this was strictly an observation and reporting exercise. Only the identified target system was scanned.
* No brute force, privilege escalation, or data exfiltration attempts were performed.
* The engagement was limited to reconnaissance and vulnerability scanning.

**Zenmap Scan**

As part of the security assessment, I used Zenmap to scan the target system at 10.4.2.100. Zenmap is a tool that maps out which “doors” (ports) are open on a computer and identifies the services running behind them. This is important because every open service is a possible way for attackers to gain access.

**Screenshot of Scan:**  


**Findings:**  
The Zenmap scan revealed a large number of open ports and active services, including:

* Port 21 – FTP (vsftpd 2.3.4): This version of FTP has a known vulnerability that can allow attackers to gain unauthorized access.
* Port 22 – SSH (OpenSSH 4.7p1): Used for secure remote access. If weak passwords are used, attackers may brute force their way in.
* Port 23 – Telnet: Telnet transmits usernames and passwords in plaintext, making it insecure and obsolete.
* Port 80 – HTTP (Apache 2.2.8): Hosts a website. Outdated Apache versions are prone to security flaws like remote code execution.
* Port 3306 – MySQL Database: If default or weak credentials are in use, attackers can directly access sensitive data.
* Port 5432 – PostgreSQL Database: Same risk as MySQL — database compromise could lead to data theft.
* Port 5901 – VNC (Virtual Network Computing): Allows remote desktop access. If not properly secured, attackers could take control of the system’s desktop environment.
* Port 1524 – Backdoor (Bash shell): This was especially concerning, as it indicates a known backdoor vulnerability that could give attackers direct root-level access.

Impact on the Client:

* These results show that the system is running many outdated and insecure services, which significantly increases the attack surface.
* Attackers could exploit these services to:
  + Steal usernames, passwords, or customer data.
  + Install ransomware or other malicious software.
  + Gain full control of the server (particularly through the backdoor or weak login services like Telnet and rexec).
* If left unaddressed, these vulnerabilities could result in a full system compromise, operational downtime, or data breaches.

OpenVAS Scan.

After the initial Zenmap scan, I performed a deeper vulnerability assessment using **OpenVAS (Open Vulnerability Assessment System)**. OpenVAS is a security tool that compares the detected services and software versions against a database of known security issues. Unlike Zenmap, which only shows what doors are open, OpenVAS identifies **how dangerous those open doors are** by listing specific weaknesses and their severity.

**Screenshot of Scan:**  
A screenshot of a computer

AI-generated content may be incorrect.

**Findings:**  
The OpenVAS scan of the target system (**10.4.2.100**) detected **multiple high-risk vulnerabilities** across several services:

* **Unencrypted Login Services (rexec, rlogin, rsh):** These services transmit usernames and passwords in plaintext. Attackers monitoring the network could capture credentials and log in as an administrator.
* **Weak Database Security (MySQL, PostgreSQL):** Databases were flagged for weak or default passwords. This could allow attackers to access or steal sensitive information stored in the databases.
* **Backdoors and Outdated Software:** The scan found signs of a **possible backdoor (Ingreslock, port 1524)** and outdated services such as **vsftpd** and **Apache** that are vulnerable to remote code execution. These vulnerabilities could give attackers full control of the system.
* **VNC (Virtual Network Computing) Brute Force Risk:** The VNC service on port 5901 could allow attackers to attempt brute force logins and gain remote desktop access to the machine.
* **Cross-Site Scripting (XSS) and Command Execution (TWiki):** Outdated web applications were identified that could allow attackers to execute malicious code or steal user data from the website.

**Recommendations for Mitigation**

To reduce the risk posed by the vulnerabilities identified in the scan, I recommend the following concrete actions for Hotel Dorsey:

1. **Patch and Update Systems Regularly**
   * Ensure all operating systems and applications are up to date with the latest security patches.
   * Implement a patch management policy that includes scheduled updates and emergency patching for critical vulnerabilities.
2. **Close or Restrict Unnecessary Open Ports**
   * Disable any services that are not essential to business operations.
   * For services that must remain open, configure firewalls to restrict access to only trusted IP addresses.
3. **Strengthen Authentication Mechanisms**
   * Require strong, complex passwords and enforce regular password changes.
   * Where possible, implement **multi-factor authentication (MFA)** to protect remote access points.
4. **Conduct a Full Penetration Test**
   * Go beyond vulnerability scanning to validate whether attackers could exploit these weaknesses in practice.
   * Use the results to prioritize remediation based on business impact.
5. **Enhance Security Monitoring and Staffing**
   * Hire or contract IT security staff to monitor systems, review logs, and respond to incidents.
   * Consider a managed security service provider (MSSP) if internal resources are limited.

By implementing these measures, the client can significantly reduce exposure to threats such as ransomware, credential theft, or data exfiltration, and build a stronger long-term security posture.

**Open Socket Connection**

During the vulnerability assessment, a manual socket connection test was performed to validate scan results. Using nc (netcat) against TCP port 1524 on the target system revealed that the service was improperly configured. The banner response suggested that the port was tied to a root-level shell service.

It is important to clarify that the scope of this engagement was limited to scanning and verification only. No attempts were made to execute commands or take control of the system. However, the presence of an open root-level shell represents a **critical vulnerability**. If a malicious actor were to connect to this service, they would gain full administrative access to the system, bypassing all authentication and security mechanisms.

This finding demonstrates the importance of manual validation in addition to automated scans, as such a vulnerability may not always be fully flagged by tools like Zenmap or OpenVAS [3], [5].

**nc 10.4.2.100 1524**

**Findings:**

 This finding confirms that the system contains a **backdoor** that gives attackers full administrative privileges.

 Unlike the weaker services (such as FTP or Telnet), this backdoor bypasses all normal login procedures.

 An attacker exploiting this could:

* **Take full control** of the system.
* Install malicious software (keyloggers, ransomware, etc.).
* Use the compromised machine to attack other systems on the network.

Screenshot:  
A black background with white text

AI-generated content may be incorrect.

Recommendations

Based on the results of our Zenmap and OpenVAS scans, as well as manual verification of open services, the target system is highly vulnerable. Several services, including FTP, Telnet, Samba, and especially a root-level backdoor accessible through TCP port 1524, provide direct pathways for attackers to compromise the environment.

While the current contract only covers vulnerability scanning and basic reporting, these findings demonstrate that a full penetration test is necessary. Vulnerability scanning identifies weaknesses, but a penetration test goes further by simulating real-world exploitation attempts to determine the actual business impact.

Why the Scope Should Be Amended

* **Proven Exploitability**: During manual testing, I confirmed that certain ports can be accessed in ways that bypass authentication. This suggests that I would be able to gain unauthorized access to proprietary information stored on the network.
* **Business Risk**: If a malicious actor exploited these same vulnerabilities, they could exfiltrate sensitive client data, disrupt operations, or use the compromised system to attack other parts of the network.
* **Due Diligence**: Without a penetration test, the organization will not know the full extent of its exposure or whether proprietary or regulated data could realistically be stolen.

I strongly recommend that the client amend the existing contract to authorize a full penetration test. This would allow me to demonstrate, under controlled and ethical conditions, whether the vulnerabilities can lead to the compromise of confidential business data. The results will give leadership a clear picture of the true risks to confidentiality, integrity, and availability of organizational assets, and provide a basis for prioritizing remediation.

References

[1] M. Chapple, J. M. Stewart, and D. Gibson, CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide, 9th ed. Hoboken, NJ: Wiley, 2022.

[2] R. A. Grimes, Hacking the Hacker: Learn from the Experts Who Take Down Hackers. Hoboken, NJ: Wiley, 2017.

[3] R. Kaur and H. Kaur, “Vulnerability assessment and penetration testing,” Materials Today: Proceedings, vol. 37, pp. 2626–2630, 2021, doi: 10.1016/j.matpr.2020.08.735.

[4] OWASP Foundation, OWASP Testing Guide v4, 2021. [Online]. Available: <https://owasp.org/www-project-web-security-testing-guide/>

[5] K. Scarfone and P. Mell, Guide to Vulnerability Scanning and Penetration Testing (NIST Special Publication 800-115), Gaithersburg, MD: NIST, 2008. doi: 10.6028/NIST.SP.800-115

[6] J. Srinivas, A. K. Das, and N. Kumar, “State-of-the-art lightweight authentication protocols for IoT: A survey,” Journal of Network and Computer Applications, vol. 149, p. 102459, 2019, doi: 10.1016/j.jnca.2019.102459.