|  |  |
| --- | --- |
| System Scan Report Prepared for Hotel Dorsey | Haverbrook security lab corporate logo  Name: Mark Go  Team Number: RedTeam2  Student Number: 2 |

**Introduction**

This report presents the outcomes of our network scanning initiative carried out on behalf of the client, Hotel Dorsey. The primary objective of this scan was to evaluate the Linux system that hosts the company's network services and database applications, with a specific focus on identifying vulnerabilities and potential security risks. It is crucial to note that, in adherence to the predefined scope of work, no attempts were made to exploit the remote systems during this assessment. Our aim was to furnish Hotel Dorsey with valuable insights into crucial vulnerabilities, application versions, and banner messages, thereby elevating their awareness of cybersecurity threats and augmenting their overall state of preparedness.

|  |  |
| --- | --- |
| **Target System** | **Penetration Testing System** |
| - IP Address: 10.2.2.100 - Operating System: Linux Metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:59:00 UTC 2008 i686 GNU/Linux | - IP Address: 10.2.2.50  - Operating System: Linux kali 4.19.0-kali5-amd64 #1 SMP Debian 4.19.37-2kali1 (2019-05-15) x86\_64 GNU/Linux |

**Systems, Tools, and Testing Software**

In our comprehensive penetration testing engagement, our experienced team leveraged the power of Kali Linux, a specialized and trusted Linux distribution specifically designed for penetration testing and ethical hacking. Kali Linux offers a wide array of pre-installed tools, making it an ideal choice for security professionals to assess and secure systems. Among the tools we skillfully employed were Zenmap and OpenVAS, which played pivotal roles in our assessment of the client's Linux system's security posture.

Zenmap is a valuable graphical user interface (GUI) built on top of the renowned Nmap network scanning utility. Nmap, or Network Mapper, is a robust and versatile tool that is fundamental for network discovery and vulnerability scanning [2]. With Zenmap, our team could efficiently perform both simple and complex network scans, gather essential information about open ports, services, and vulnerabilities, and visualize the results in an intuitive interface. This enabled us to identify potential weaknesses and areas of concern within the client's network infrastructure.

OpenVAS is a powerful open-source vulnerability assessment scanner designed to identify and assess security vulnerabilities in networks and systems [3]. Our penetration testing team utilized OpenVAS to conduct thorough and systematic vulnerability assessments of the client's Linux environment. By running comprehensive scans and analyzing the results, we could pinpoint potential vulnerabilities, misconfigurations, or weaknesses that might expose the client's system to security risks.

The Metasploit Framework is an advanced and widely-used penetration testing tool that provides security professionals with a powerful set of exploits, payloads, and auxiliary modules. It facilitates the identification of vulnerabilities, the exploitation of security weaknesses, and the assessment of network and system defenses. Metasploit's modular design, extensive database of known vulnerabilities, and user-friendly interface make it a versatile and essential tool for ethical hackers and security experts, enabling them to test, secure, and enhance the resilience of computer systems and networks. [5]

Incorporating the Metasploit Framework into our comprehensive approach, we not only relied on automated tools but also integrated manual methods for open socket analysis. Our team conducted in-depth manual port scanning and analysis to augment the automated assessments. This meticulous manual inspection empowered us to closely examine ports, services, and configurations that automated tools might inadvertently neglect. By doing so, we added an extra layer of scrutiny to our testing methodology, ensuring that we could identify subtle or less prevalent vulnerabilities that could potentially evade detection through automated scans.

Collectively, these sophisticated tools, combined with our expertise and manual analysis, allowed us to conduct an in-depth and holistic evaluation of the client's Linux system. We identified vulnerabilities, assessed potential risks, and provided valuable insights and recommendations to enhance the security posture of their infrastructure. Our commitment to utilizing cutting-edge tools, along with the precision of manual analysis, ensures that our clients receive the highest level of security assessment and protection for their valuable assets.

**Zenmap Scan**

A screenshot of a computer

Description automatically generated

*Figure 1. Zenmap Scan Result.*

The Nmap scan report reveals the following information about the target (10.2.2.100):

1. Host Information:

- The host is up with a latency of 0.00084 seconds.

- The host is running a Linux operating system with an estimated uptime of approximately 497.102 days (since April 17, 2022).

- The target is running Linux 2.6.X, with an OS kernel version between 2.6.9 and 2.6.33.

- The host's MAC address is 00:0C:29:30:E1:15, indicating that it's a VMware virtual machine.

2. Open Ports and Services: Nmap discovered a total of 20 open ports on the target:

* 21/tcp: FTP service (vsftpd 2.3.4) with anonymous FTP login allowed.
* 22/tcp: SSH service (OpenSSH 4.7p1 Debian 8ubuntu1).
* 23/tcp: Telnet service (Linux telnetd).
* 25/tcp: SMTP service (Postfix smtpd).
* 53/tcp: DNS service (ISC BIND 9.4.2).
* 80/tcp: HTTP service (Apache httpd 2.2.8 on Ubuntu).
* 111/tcp: RPC service (RPC #100000).
* 139/tcp: NetBIOS-SSN service (Samba smbd 3.X - 4.X).
* 445/tcp: NetBIOS-SSN service (Samba smbd 3.0.20-Debian).
* 512/tcp: Exec service (netkit-rsh rexecd).
* 513/tcp: Login service (OpenBSD or Solaris rlogind).
* 514/tcp: Shell service (Netkit rshd).
* 1099/tcp: Java RMI Registry service.
* 1524/tcp: Bindshell service (Metasploitable root shell).
* 2049/tcp: NFS service (RPC #100003).
* 3306/tcp: MySQL service (MySQL 5.0.51a-3ubuntu5).
* 5432/tcp: PostgreSQL service (PostgreSQL DB 8.3.0 - 8.3.7).
* 6667/tcp: IRC service (UnrealIRCd).
* 8009/tcp: AJP13 service (Apache Jserv Protocol v1.3).
* 8180/tcp: HTTP service (Apache Tomcat/Coyote JSP engine 1.1)

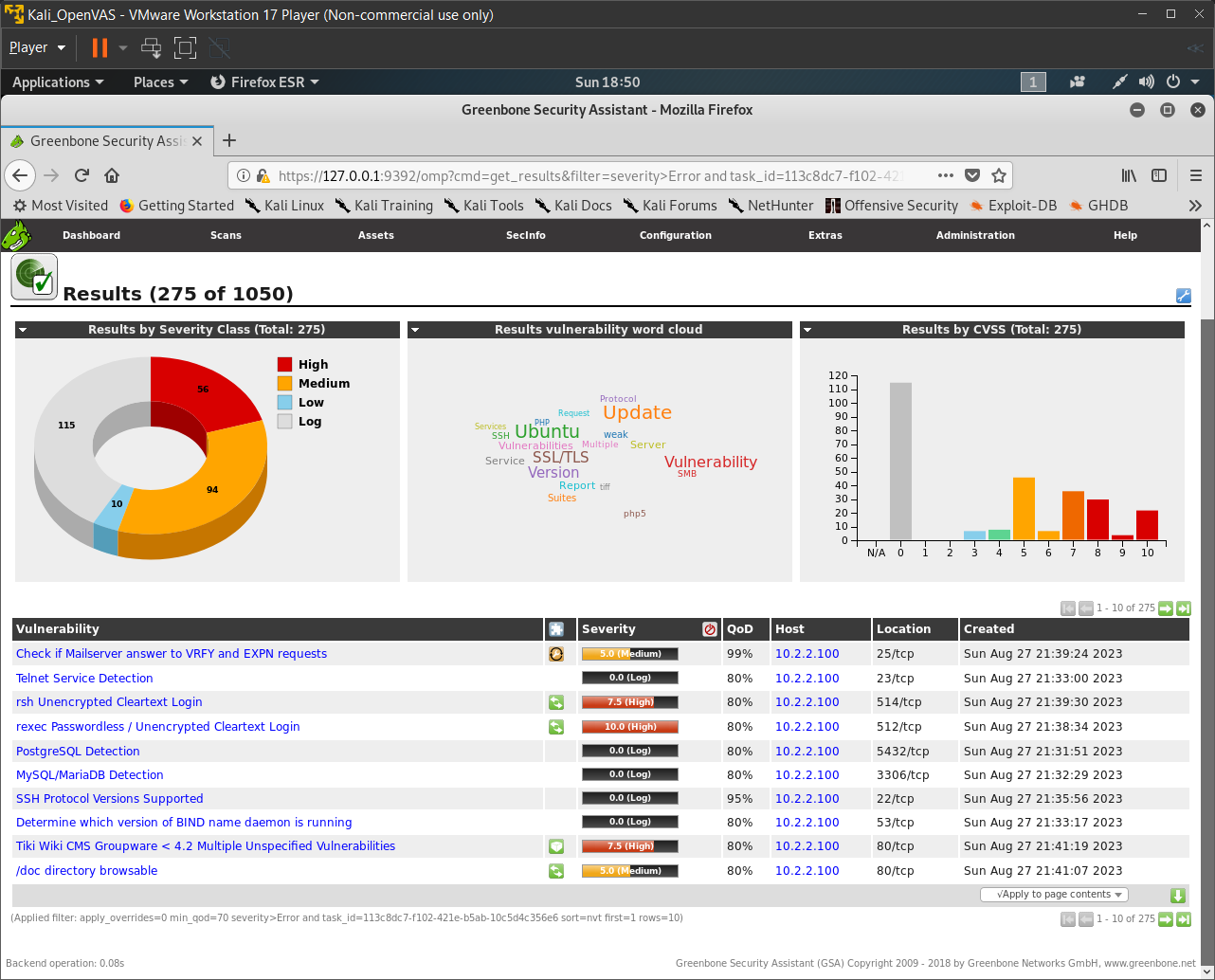
3. Service Versions: Detailed service information is provided, including version numbers for FTP, SSH, SMTP, DNS, HTTP, and more.

4. Vulnerabilities and Security Implications: Several of the services are running older or potentially vulnerable versions, which could pose security risks if not properly configured and maintained.

5. Additional Information: The report includes information about network distance, TCP sequence prediction, IP ID sequence generation, and more.

This Nmap scan provides a comprehensive overview of the target system's open ports, services, and potential security vulnerabilities. It serves as a valuable starting point for further security assessment and hardening efforts to ensure the system's integrity and protect against potential threats.

**OpenVAS Scan**



*Figure 2. OpenVAS Scan Result.*

Following an OpenVAS scan, several ports and vulnerability findings were identified on the target system.

* In Port 21, vulnerabilities were found related to FTP, including an Anonymous FTP Login vulnerability, FTP Unencrypted Cleartext Login, and the presence of vsftpd Compromised Source Packages Backdoor Vulnerability.
* Moving to Port 22, the scan detected SSH-related issues, including SSH Brute Force Logins with Default Credentials Reporting, SSH Weak Encryption Algorithms Supported, and SSH Weak MAC Algorithms Supported.
* Port 23 revealed vulnerabilities related to Telnet, specifically an Unencrypted Cleartext Login. Port 25 highlighted concerns related to the Mailserver, with checks for VRFY and EXPN requests, Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability, and SSL/TLS certificate-related issues such as expiration and weak signatures.
* Port 80 raised significant concerns, with multiple findings related to the Apache HTTP Server. These findings included a browsable /doc directory, httpOnly Cookie Information Disclosure Vulnerability, several instances of local file inclusion vulnerabilities, cleartext transmission of sensitive information via HTTP, and the presence of debugging methods like TRACE/TRACK. Additionally, PHP-CGI-based setups were found vulnerable when parsing query string parameters from PHP files, and various Cross-Site Scripting (XSS) vulnerabilities were identified in applications such as phpMyAdmin, Tiki Wiki CMS Groupware, and TWiki.
* Port 445 indicated a critical vulnerability: the Samba MS-RPC Remote Shell Command Execution Vulnerability. Port 512 and Port 513 both showed issues with unencrypted cleartext login methods (rexec and rlogin, respectively). Port 514 similarly revealed an unencrypted cleartext login vulnerability related to rsh.
* Port 1524 suggested a possible backdoor presence. Port 3306 raised concerns about weak passwords in MySQL/MariaDB.
* Port 3632 identified a vulnerability related to DistCC Remote Code Execution. Port 5432 exhibited vulnerabilities such as weak PostgreSQL passwords and SSL/TLS certificate issues. Port 6200 highlighted a similar vsftpd vulnerability to Port 21.
* Port 8787 uncovered vulnerabilities related to Distributed Ruby (dRuby/DRb), including multiple remote code execution vulnerabilities.
* The scan also identified various Linux-related vulnerabilities, such as those associated with GNU Bash, insecure file saving in Mozilla Firefox, end-of-life detection, and Pidgin vulnerabilities. Additionally, issues with TCP timestamps, TightVNC, and Ubuntu updates for various software packages were flagged.

These findings underscore the importance of addressing these vulnerabilities promptly to enhance the security posture of the target system.

**Open Socket**

Following the Zenmap and OpenVAS scans, we conducted an in-depth analysis of port 6667. We utilized Nmap to gather detailed information about the port and the Metasploit Framework to identify known modules and exploits. Our objective was to uncover any vulnerabilities missed by the initial assessments.   
  
Port 6667 is associated with the Unreal Internet Relay Chat daemon, which has a known vulnerability, CVE-2010-2075. “UnrealIRCd 3.2.8.1, as distributed on certain mirror sites from November 2009 through June 2010, contains an externally introduced modification (Trojan Horse) in the DEBUG3\_DOLOG\_SYSTEM macro, which allows remote attackers to execute arbitrary commands. [4]”

With Nmap, we obtained precise insights into port 6667, including its services and potential weaknesses. Simultaneously, we employed the Metasploit Framework to identify relevant exploits. Through this meticulous analysis, we successfully identified an exploitable vulnerability, enabling us to gain root access to the system.

This comprehensive evaluation provided critical insights, allowing us to recommend targeted remediation measures to enhance the client's system security. Our commitment to thorough assessments and proactive security measures ensures the protection of our clients' valuable assets.  
  
A screenshot of a computer

Description automatically generated

*Figure 3. Port 6667 Internet Relay Chat daemon exploited to gain root shell access.*Gaining root access provides attackers with unrestricted control over a system, allowing them to install malware, alter configurations, view, modify, and delete files, escalate privileges, monitor users, disrupt services, cover their tracks, exploit resources, and exfiltrate data. It poses an immense security threat, and safeguarding against unauthorized root access is vital for system security.

**Summary/ Recommendations**

Conducting thorough and in-depth analysis of a network, system, and business infrastructure is essential for several reasons, particularly when considering applicable regulations. Firstly, it helps uncover hidden threats that may not be evident during initial assessments, a crucial step in complying with various cybersecurity regulations.

In the context of regulatory compliance, comprehensive analysis is frequently mandated. Industry-specific regulations, such as PCI DSS for payment card data [6], require organizations to conduct extensive security assessments and maintain continuous monitoring to protect sensitive information. Compliance with these standards is not only a legal obligation but also crucial for maintaining trust with customers and partners.

Comprehensive analysis allows organizations to understand how various components interact within their infrastructure, revealing potential attack vectors and weak points that adversaries might exploit. This level of insight is critical for meeting compliance requirements, as many regulations demand a deep understanding of network and system security.

Moreover, in-depth analysis plays a vital role in detecting stealthy, long-term cyberattacks, which are of increasing concern in the face of evolving threats. Meeting regulatory standards often involves continuous monitoring and advanced threat detection, which can only be achieved through thorough analysis of network traffic, system logs, and user behavior.

In-depth analysis helps organizations test their incident response capabilities; another aspect often covered by regulations. Simulations of security incidents allow businesses to evaluate the effectiveness of their response procedures and identify areas for improvement, ensuring they meet regulatory requirements for incident handling.

In summary, comprehensive analysis is critical for both enhancing overall security posture and meeting the stringent requirements set forth by cybersecurity regulations. It allows organizations to proactively strengthen their defenses, identify weaknesses, and implement necessary safeguards to prevent security breaches while staying compliant with the law.

## **References**

[1] "Nmap Reference Guide," Nmap Project, [Online]. Available: <https://nmap.org/book/man.html#man-description>

[2] G. Lyon, "Zenmap - Official User Guide," Nmap Project, [Online]. Available: <https://nmap.org/book/zenmap.html#zenmap-intro>.

[3] Greenbone Networks GmbH. (2021). OpenVAS - Open Vulnerability Assessment System. [Online]. Available: <https://www.openvas.org/>

[4] CVE Details. (2010). CVE-2010-2075. [Online]. Available: <https://www.cvedetails.com/cve/CVE-2010-2075/?q=cVE-2010-2075>

[5] Rapid7 LLC. (Year). Metasploit Framework. [Online]. Available: <https://www.metasploit.com/>

[6] Payment Card Industry Security Standards Council. (Year). Payment Card Industry Data Security Standard (PCI DSS), Version X.X. [Online]. Available: <https://www.pcisecuritystandards.org/documents/PCI-DSS-vX.X.pdf>