|  |  |
| --- | --- |
| System Scan Report Prepared for Hotel Dorsey | Haverbrook security lab corporate logo  Name: Michael R. Lee  Team Number: 0  Student Number: 3 |

**Introduction**

The scope of the network scan provided to my team by Hotel Dorsey are to do a network scan using the following tools: Zenmap & NMAP, two open-source scanners used for network discovery and security auditing [2]. OpenVAS is the next tool that will be used, which is a large-scale scanner that boasts a powerful internal programming language to be used in any vulnerability test [3]. My team is aware that exploiting any found vulnerabilities is out of scope and our purpose is to simply identify any vulnerabilities that will require further attention from Hotel Dorsey and their staff.

**Target**

The hostname for the target machine is Metasploitable with the IP address of 10.0.3.100. The hostname and IP address of the attack machine is Kali Linux with the IP address of 10.0.3.50. The following explains the results of scanning the target machine with Nmap:

|  |  |  |
| --- | --- | --- |
| Port | Service | Explanation |
| 21 | FTP | File Transfer Protocol [4] |
| 22 | SSH | Secure Shell, Secure Logins, Port Forwarding [4] |
| 23 | TELNET | Telnet Protocol-unencrypted text communications [4] |
| 25 | SMTP | Simple Mail Transfer Protocol-email routing between mail servers [4] |
| 53 | DOMAIN | Domain Name System name resolver [4] |
| 80 | HTTP | Hypertext Transfer Protocol, connection to the internet [4] |
| 111 | RCPBIND |  |
| 139 | NETBIOS-SSN | NetBIOS Session Service [4] |
| 445 | MICROSOFT-DS | Samba (Zenmap version info) |
| 512 | EXEC | Netkit-rsh (Zenmap version info) |
| 513 | LOGIN | OpenBSD or Solaris rlogind (Zenmap version info) |
| 514 | SHELL | Netkit rshd (Zenmap version info) |
| 1099 | RMIREGISTRY | Java RMI Registery (Zenmap version info) |
| 1524 | INGRESLOCK | Metasploitable root shell (Zenmap version info) |
| 2049 | NFS | Network file system 2-4 (Zenmap version info) |
| 3306 | MYSQL | MySQL database system [4] |
| 5432 | POSTGRESQL | PostgreSQL database system [4] |
| 6667 | IRC | Internet Relay Chat [4] |
| 8009 | AJP13 | Apache Jserv (Zenmap version info) |
| 8180 | UNKNOWN | Regular Nmap scan pulled no results for this port |

**Zenmap Scan**

I proceeded to accomplish a Zenmap scan, and the following are screenshot results of that scan:

Graphical user interface, text, application, email

Description automatically generated

Screenshot 1: Ports 21, 22, 23, 25, 53, and 80 open.

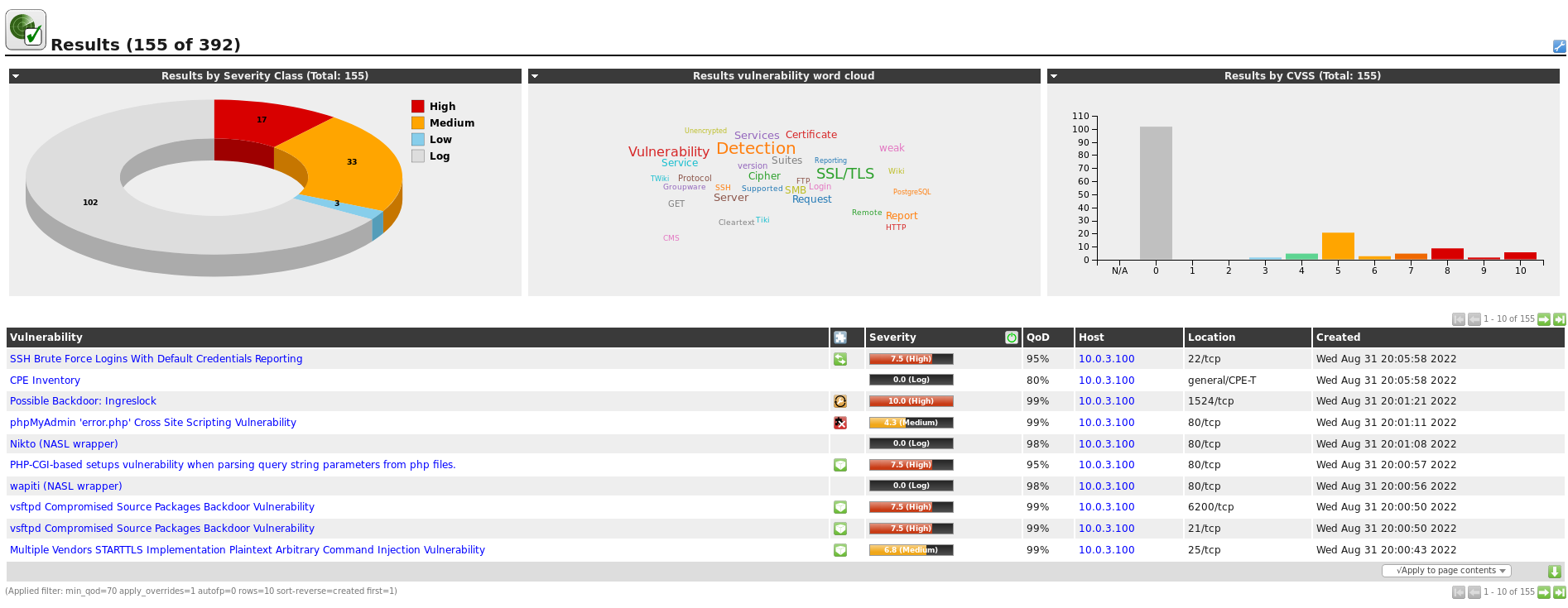
Graphical user interface, text, application

Description automatically generated

Screenshot 2: Ports 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 3306, 5432, 6667, 8009, 8180.

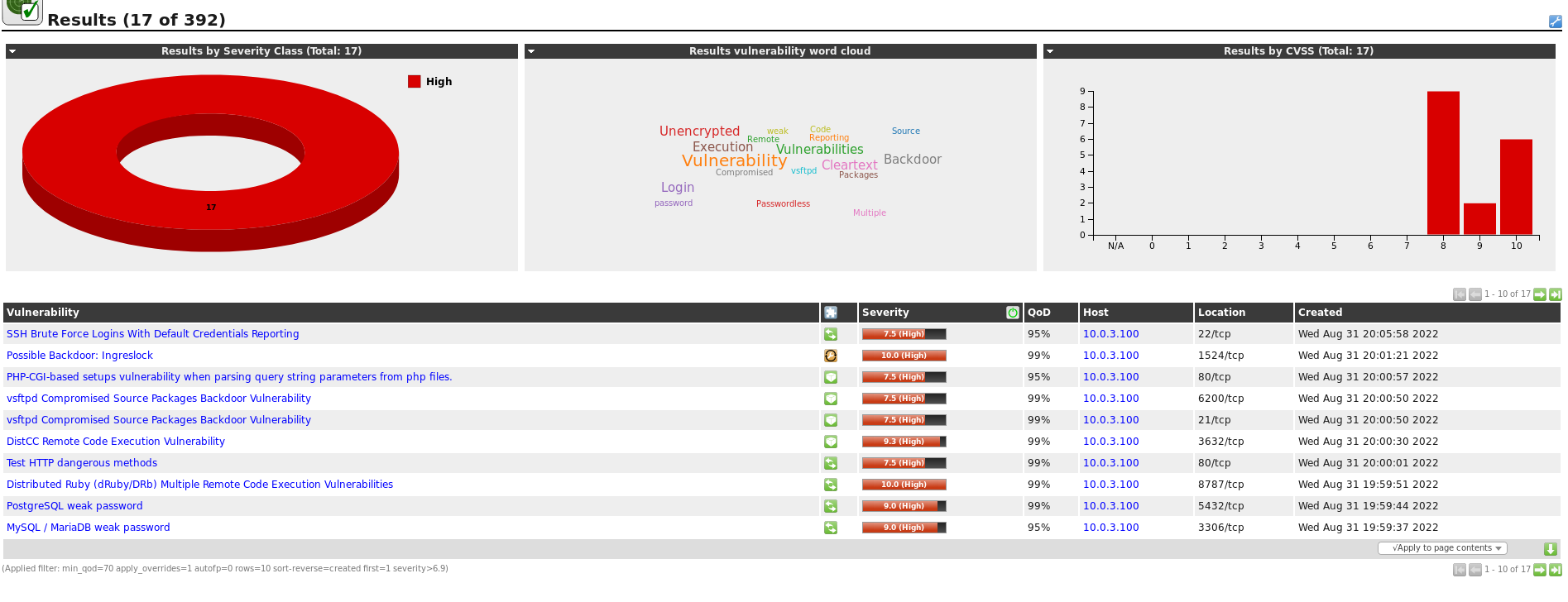
**OpenVAS Scan**

The OpenVAS scan revealed many vulnerabilities. The results are in the screenshots below:



Screenshot 3: OpenVAS scan results.

As you can see in the scan above there are 102 log files, 17 High severity items, 33 Medium severity items, and 3 Low severity items. With these results, there is a very high chance this machine’s vulnerabilities can be exploited.

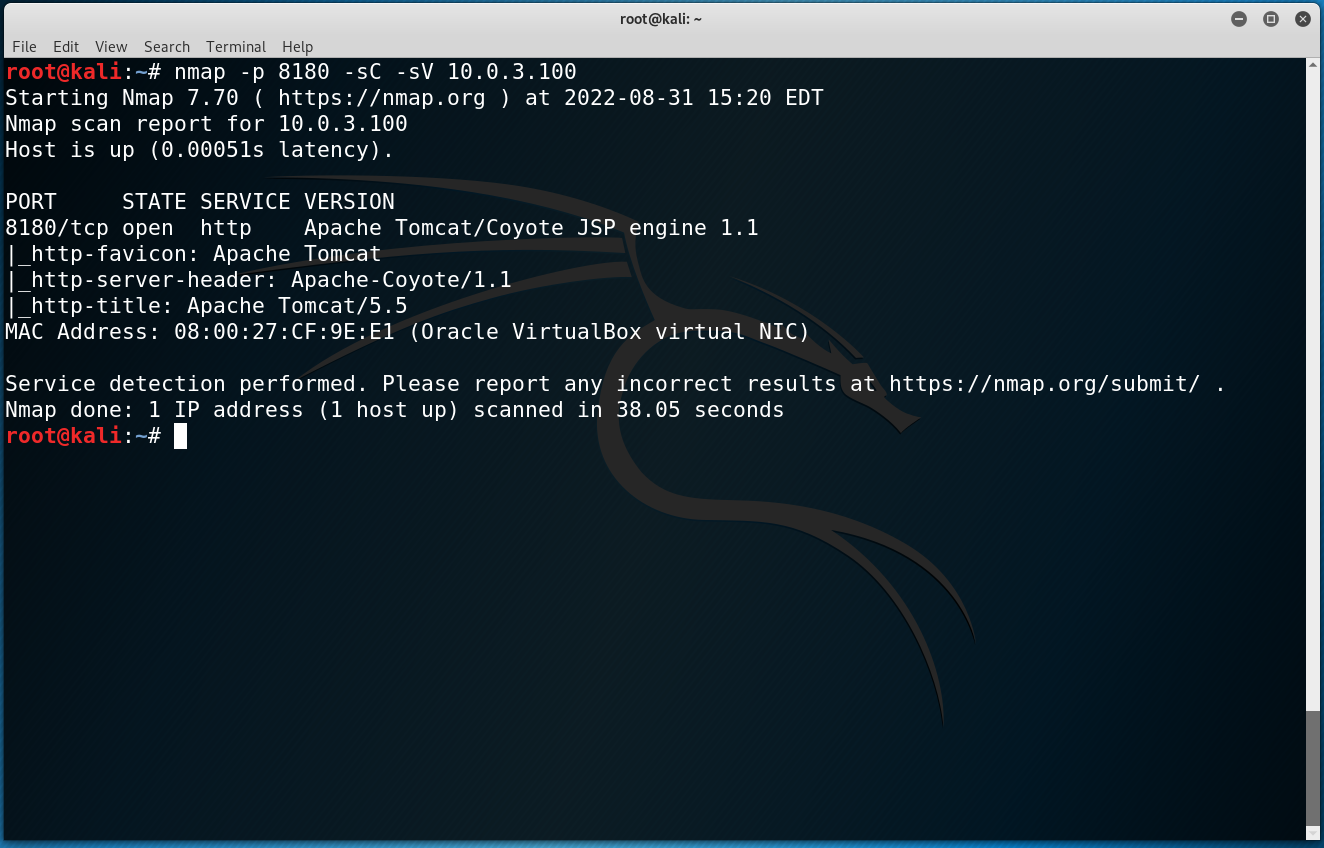


Screenshot 4: High Severity vulnerabilities.

In the screenshot above, I have filtered the results to only the high severity items. The interesting part about all results is that they correlate with the Zenmap scan I accomplished in the steps beforehand. In the location column of the results, OpenVAS lists the affected port of the vulnerability. Some of the most troubling vulnerabilities on this list are a possible backdoor (port 1524/tcp), a PostgreSQL weak password (5432/tcp), and MySQL/ MariaDB weak password (3306/tcp). At a minimum, attackers could use enumeration tools to brute force weak passwords and gain unauthorized access to the system. Unless something is done to start repairing these vulnerabilities, the network at Hotel Dorsey can be taken over by threats outside the network.

**Open Socket**

While performing a regular Nmap scan with no switches (options), port 8180 showed unknown. To remedy this unknown I scanned port 8180 directly with switches that shows specific port service information. The screenshot of this scan is below:



Verbose version scan of port 8180

The above scan does reveal what service is operating on that port, and it is Apache Tomcat version 5.5. The main concern for this version of Apache Tomcat is that Apache 5.0.x is no longer supported. As a server version that is no longer supported, there are no security fixes or patches for known vulnerabilities [1]. This leaves the server open to publicly known vulnerabilities that can be easily exploited.

**Recommendations**

My recommendations moving forward is that the contract for my team to test Hotel Dorsey’s network be amended to include a full penetration test. A full penetration test will allow me and my team to look deeper into the vulnerabilities we have discovered and provide full transparency as to how your network can be exploited, instead of using hypothetical scenarios for what could occur. Should you elect not to get a full penetration test, my suggestion is that you update all servers in your company to a version that is supported and receives regular updates. My next suggestion is that you work with your IT department to create a password policy that will ensure strong passwords from users of your network. This will strengthen your network presence alleviate your company becoming an easy target for threats. I hope you find this report informative, and it meets the expectation of your company. Thank you for your time and attention!

## **References**

[1] Apache Foundation, “Apache Tomcat®,” *Apache Tomcat® - Apache Tomcat 5 vulnerabilities*, 2022. [Online]. Available: https://tomcat.apache.org/security-5.html. [Accessed: 04-Sep-2022].

[2] G. Lyon, “Zenmap,” *FileHorse*, 02-Sep-2022. [Online]. Available: https://www.filehorse.com/download-zenmap/. [Accessed: 04-Sep-2022].

[3] Open Source, “Greenbone openvas,” *OpenVAS*, 2022. [Online]. Available: https://www.openvas.org/. [Accessed: 04-Sep-2022].

[4] rishavkumarj7, “50 common ports you should know,” *GeeksforGeeks*, 28-Feb-2022. [Online]. Available: https://www.geeksforgeeks.org/50-common-ports-you-should-know/. [Accessed: 04-Sep-2022].