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

**Introduction**

Describe an overview and discuss the scope of your network scan. Note the name of the operating system of your attack machine and discuss and describe the tools you will use (Zenmap, OpenVAS). Keep in mind that this report will be reviewed by nontechnical people who may not know about Zenmap or OpenVAS.

**Target**

List the IP address and hostname of the target system as well as the IP address assigned to the attack machine. Focus on the open ports and describe the corresponding services associated with the open ports. Keep in mind that this report will be reviewed by nontechnical people who will not know about FTP or SSH or may not know what functions the services provide on a network. Put the information about the ports and corresponding services into a table and label it.

**Zenmap Scan**

Use Zenmap to scan the victim machine and include a screenshot of your connection to the victim system. Show a labeled screenshot of your Zenmap scan. Explain the results and how the client could be affected by any vulnerabilities that emerge.

**OpenVAS Scan**

Use OpenVAS to scan the victim machine and include a screenshot of your connection to the victim system. Show a labeled screenshot of your OpenVAS scan. Explain the results and how the client could be affected by any vulnerabilities that emerge.

**Open Socket**

You have already scanned the system with Zenmap and OpenVAS. Go back to either of the reports and look for a port that provided little information about the banner or provided you with an *unknown*. By manually connecting to the IP and port (socket), you can sometimes discover a vulnerability not listed by the tool. This shows the importance of not just relying on a tool. Show a labeled screenshot of your connection to a socket that provided interesting results using a browser or netcat, etc. If you find something concerning, explain that to the client.

**Recommendations**

Suggest that the client amend the contract to add a full penetration test. Explain that you are confident that you will be able to exploit the system and take proprietary data from the network.

## **References**

Include at least two to three references in IEEE format.