|  |  |
| --- | --- |
| Penetration Test Report Prepared for Hotel Dorsey | Corporate Logo Haverbrook security lab corporate logo  Name:  Team Number:  Student Number: |

**Introduction**

In this section, provide an overview and discuss the scope of the penetration test. Note the name of the operating system of the attack machine and discuss the tools that you will use (e.g., Zenmap, Metasploit). Keep in mind that this report will be reviewed by nontechnical people who may not know about the tools.

**Target**

In this section, 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, placing this information into a table. 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. Provide a screenshot of the Zenmap scan. All screenshots and tables should be labeled for your report.

**Vulnerability**

In this section, discuss the specific vulnerability you are using to exploit the remote system. Provide a description of the vulnerability and how you used the vulnerability to exploit the victim machine. Include the time of intrusion as well as a screenshot of your connection to the victim system. Finally, discuss the level of access you achieved on the box (Apache, root, etc.). Show screenshots using the *getuid* or *whoami* command to verify your level of access for your client (two screenshots). All screenshots and tables should be labeled for your report.

**Data Exfiltration**

In this section, explain how you were able to take the company’s sensitive data out of the network. Provide a screenshot of the method by which the data was extracted. Talk about the implications to the company and possible costs of losing proprietary data.

**Recommendations**

In this section, you will explain what security controls should be implemented to remediate the vulnerability that you have exploited on the remote system. Talk about the steps the client should take to ensure that the vulnerability is no longer present as well as any other suggestions you may have to help improve the overall security posture.

## **References**