# Pentest Technical Report for Lab # \_\_

|  |  |
| --- | --- |
| **System Summary** | |
| **IP Address(es)** |  |
| **Hostname** |  |
| **Operating System** |  |

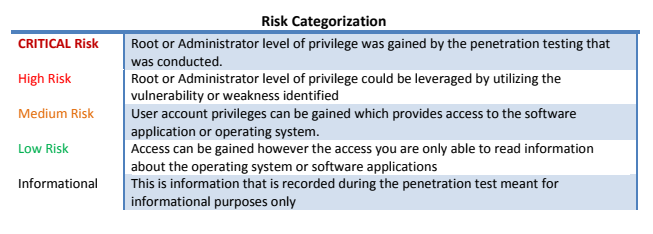
\*To find the operating system information from a shell, command prompt, terminal or through code injection run “uname -a”. To find the hostname run the command “hostname”.

|  |  |  |
| --- | --- | --- |
| **System Information** | | |
| **Services Running** | **Description of Services** | **Latest Version** |
|  |  |  |
|  |  |  |

\*To find the information about the services and description of the services run “nmap -sV <IP Address>”. The output of this command will allow you to fill in the first 2 columns above. Then to find the latest version google the parent softwares name from the description and place latest version in it.

|  |  |  |
| --- | --- | --- |
| **User Information** | | |
| **User Accounts** | **Description of Account (Admin?)** | **Password if Compromised or Indicate if Compromised** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

\*The user information above is gathered throughout the lab.



|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerability Summary** | | | |
| **Severity** | **Vulnerability** | **Description of Vulnerability** | **Exploited** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Detail of the Vulnerabilities Discovered**

Below is the information necessary for you to recreate the vulnerabilities that were used to exploit the system. Not all vulnerabilities listed above in the summary will appear in this section.

**Vulnerability:**

**Description of the Vulnerability:**

**How to Exploit the Vulnerability:**