# Pentest Technical Report for Lab # \_\_

|  |  |
| --- | --- |
| **System Summary** | |
| **IP Address(es)** | 172.168.202.8 |
| **Hostname** |  |
| **Operating System** | Linux x86\_64 Fedora |

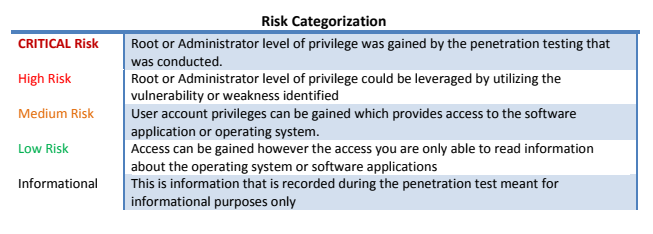
\*To find the operating system information from a shell, command prompt, terminal or through code injection run “uname -a”. To find the hostname run the command “hostname”.

|  |  |  |
| --- | --- | --- |
| **System Information** | | |
| **Services Running** | **Description of Services** | **Latest Version** |
| 80 http | Apache httpd 2.4.16 | 2.4.37 |
| PHP | Web code 5.6.14 | 5.6.33 |

\*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** |
| admin | Website account | Pw is compromised |
| admin@seattlesounds.net | Website email account | Pw is compromised |
|  |  |  |
|  |  |  |
|  |  |  |

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



|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerability Summary** | | | |
| **Severity** | **Vulnerability** | **Description of Vulnerability** | **Exploited** |
| Informational | Out-of-Date | Apache and OpenSSH servers need to be  updated | no |
| Informational | Out-of-Date | OS need to be updated to the lattest version | no |
| High Risk | Password | Password can be rainbow attack exploited. | yes |
| High Risk | SQL | The sql database is vulnerable, is has public exploit to compromised | yes |

**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:**

**Http not secure**

**Password too simple**

**Out-dated software**

**Description of the Vulnerability:**

**HTTP port is open can easily perform man-in-middle attack to extract info.**

**Out-dated software has public exploit method online.**

**Password too simple can be easily crack through rainbow attack.**

**How to Exploit the Vulnerability:**

**Use scan to find the port and services and vulnerabilities**

**Such as nmap -sn -sv and Owasp**

Text

Description automatically generated

Then use nc to find the web info

Text

Description automatically generated

Use owasp to find more directory of the website available that you can access the info.

Table

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text

Description automatically generated

This perform man-in-the-middle to hash the password.

Graphical user interface, text, application

Description automatically generated

Then you use the rainbow attack to find the password “Assassin1”

Graphical user interface, text, application, email

Description automatically generated

You can find the system file in the download directory to see the user accounts

Text

Description automatically generated

Explore more in the website directory to see more content

Text

Description automatically generated

Explore more in the website you will find the admin email so you can access the box via the email provided

Graphical user interface, website

Description automatically generated

Use burp suite you find the email and see sql injection vulnerbility

Graphical user interface, application

Description automatically generated

Too see the website has sql vulnerabilities and look up online the possible password injectionGraphical user interface, table

Description automatically generated

Graphical user interface, application

Description automatically generated

Then you enter the website through the SQL vulnerabilities passwords ‘ or ‘1’=’1

Graphical user interface, website

Description automatically generatedGraphical user interface, website

Description automatically generated