# Pentest Technical Report for Lab # \_\_

|  |  |
| --- | --- |
| **System Summary** | |
| **IP Address(es)** | 172.16.202.4 |
| **Hostname** | indisshell |
| **Operating System** | Ubuntu precise (12.04.5 LTS) |

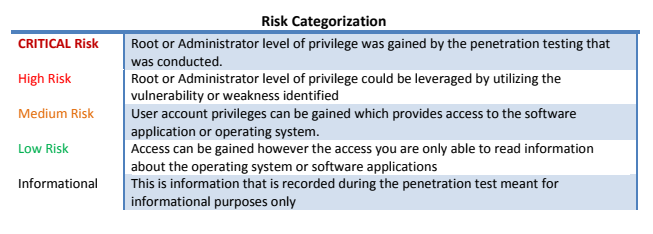
\*To find the operating system information from a shell, command prompt, terminal or through code injection run “uname -a”. To find the hostname run the command “hostname”.

|  |  |  |
| --- | --- | --- |
| **System Information** | | |
| **Services Running** | **Description of Services** | **Latest Version** |
| 22/tc | OpenSSH 5.9p1 Debian | OpenSSH 8.2 |
| 80/tcp | Apache httpd 2.2.22 ((Ubuntu)) | **Apache httpd** 2.4.49 |

\*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** |
| root | Root admin | roottoor |
| billu | MySQL acc | b0x\_billu |
| ica | Linux User acc | Password compprimised |
| biLLu | Web Admin | hEx\_it |
| root | MySQL acc Admin | roottoor |

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



|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerability Summary** | | | |
| **Severity** | **Vulnerability** | **Description of Vulnerability** | **Exploited** |
| Informational | Out-of-Date Services | Apache and OpenSSH servers need to be updated | no |
| Informational | Out-of-Date  OS | OS need to be updated to the lates version | no |
| High Risk | Password | Root password need to be changed for SSH and MySQL | yes |
| High Risk | Local File | The file test.php display the web users and it allows access to the Linux databass, passwd or shadow/ | 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:**

**Weakness in an information system**: simple password, http not secure.

**Description of the Vulnerability:**

**Simple password: the password can easily be brutforce, need to be complex.**

**http can be easily be intercept by the burpsuite, and can fine the password**

**PHP version outdated, can easily be request and POST to deceit the website**

**How to Exploit the Vulnerability:**

**Scan the local network, and find the box**

Graphical user interface, application

Description automatically generated

Find the open port and weaknesses

Graphical user interface, application

Description automatically generated

Then bruteforce the box by using the big.txt list

Graphical user interface, text, application

Description automatically generated

Then find out the website readme to know more about the system weaknesses

A screenshot of a computer

Description automatically generated with medium confidence

Then use the burp suite to intercept the request and re-send the request to trick the server to give more info

Graphical user interface, text, website

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Using the file /etc/passwd to find the users and password

Graphical user interface, text, application, email

Description automatically generated

Then login to your box using the username and pw you found

Graphical user interface, text, application

Description automatically generated

And you can see the Web admin user and pw

Graphical user interface, text, application, chat or text message

Description automatically generated

Login to see more info for the website.

A screenshot of a computer

Description automatically generated with medium confidence