# Pentest Technical Report for Lab # \_\_

|  |  |
| --- | --- |
| **System Summary** | |
| **IP Address(es)** | 172.16.202.9 |
| **Hostname** |  |
| **Operating System** | Linux Debian Ubuntu 2.6 |

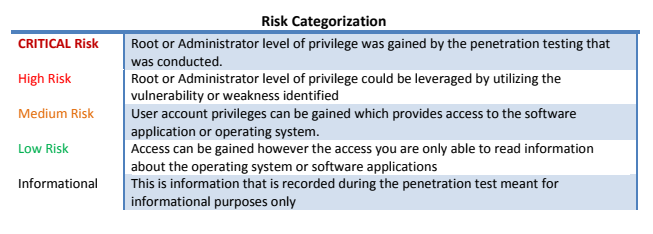
\*To find the operating system information from a shell, command prompt, terminal or through code injection run “uname -a”. To find the hostname run the command “hostname”.

|  |  |  |
| --- | --- | --- |
| **System Information** | | |
| **Services Running** | **Description of Services** | **Latest Version** |
| 22/SSH | OpenSSH Use for shell remote access | 8.8 |
| 80/HTTP | For apache httpd web service. | 2.2.34 |

\*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 | Linux root admin account. | Not compramised |
| admin | Php web account | Password is compromised “admin” |
| zico | Account admin | Not compramised |
|  |  |  |
|  |  |  |

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



|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerability Summary** | | | |
| **Severity** | **Vulnerability** | **Description of Vulnerability** | **Exploited** |
| low risk | httpd | Out-dated-version software |  |
| High Risk | directory | Web admin page is available | yes |
| High Risk | password | Admin password too simple | yes |
| Informational | OpenSSH | Out-dated-version software |  |

**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

Website directory

Admin password

OpenSSH

**Description of the Vulnerability:**

http is not secure, https is not implemented – this can be perform man-in-the-middle attack to find the password hash

Website directory – can be find by brute forcing or rainbow attack to find the admin login directory

Admin password – admin password too s

OpenSSH - out of date software

**How to Exploit the Vulnerability:**

As both OS are in the same network, use ifcoonfig and nmap to find the target. So it is 172.16.202.9 with http and ssh open. Ubuntu System.

Text

Description automatically generated

Use nmap with in depth scan and nikto to see the open port, system info, and system’s vulnerability. As you can see some directory are open for more info.

Text

Description automatically generated

Use OWASP dirbuster and select wfuzz wordlists to find some useful directories. And find the dbamin directory to access the test\_db.php

Table

Description automatically generated

And access the website

A screenshot of a computer

Description automatically generated with medium confidence

We can perform the man-in-the-middle using durp suites to try the find the hash. And we find the PHPSSID hash

Graphical user interface, text, application

Description automatically generated

And we can find the hash and decrypt it and find the “admin” password.

And we can find the hash password for the server. But could not decrypt through hash.

Graphical user interface, text, application

Description automatically generated