# rPentest Technical Report for Lab # \_\_

|  |  |
| --- | --- |
| **System Summary** | |
| **IP Address(es)** | 172.16.202.10 |
| **Hostname** | Marlinspike/vtcsec |
| **Operating System** | Linux Ubuntu 2.4 |

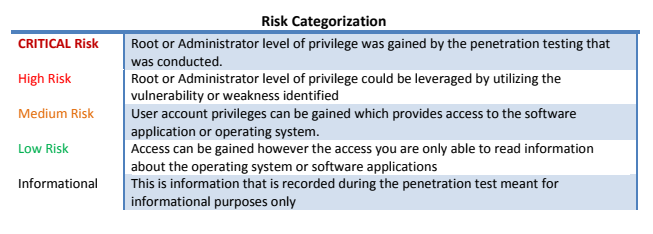
\*To find the operating system information from a shell, command prompt, terminal or through code injection run “uname -a”. To find the hostname run the command “hostname”.

|  |  |  |
| --- | --- | --- |
| **System Information** | | |
| **Services Running** | **Description of Services** | **Latest Version** |
| 21-22/ssh | remote access | 8.2 |
| 80/http | Apache web server | 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 | Server account | Password has compromised |
| marlinspike | User account | marlinspike |
| admin | wordpress | admin |
|  |  |  |
|  |  |  |

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



|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerability Summary** | | | |
| **Severity** | **Vulnerability** | **Description of Vulnerability** | **Exploited** |
| High Risk | password | Easy password | yes |
| High Risk | backdoor | To remote access and gain access | yes |
| Information | system | Out-of-dated service |  |
|  |  |  |  |

**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:**

Password

Backdoor

SSH

**Description of the Vulnerability:**

Password – same password as username

Backdoor – build-in backdoor can be found by metasploit

SSH – ssh password compromised by ssh attack

**How to Exploit the Vulnerability:**

Use the nmap to find the addresss and service available then use nitko to find the the vulnerability

Text

Description automatically generated

In order to access the website, modify the hosts find and add the host address

Text

Description automatically generated

Use WPSscan to find more about the web info



Text

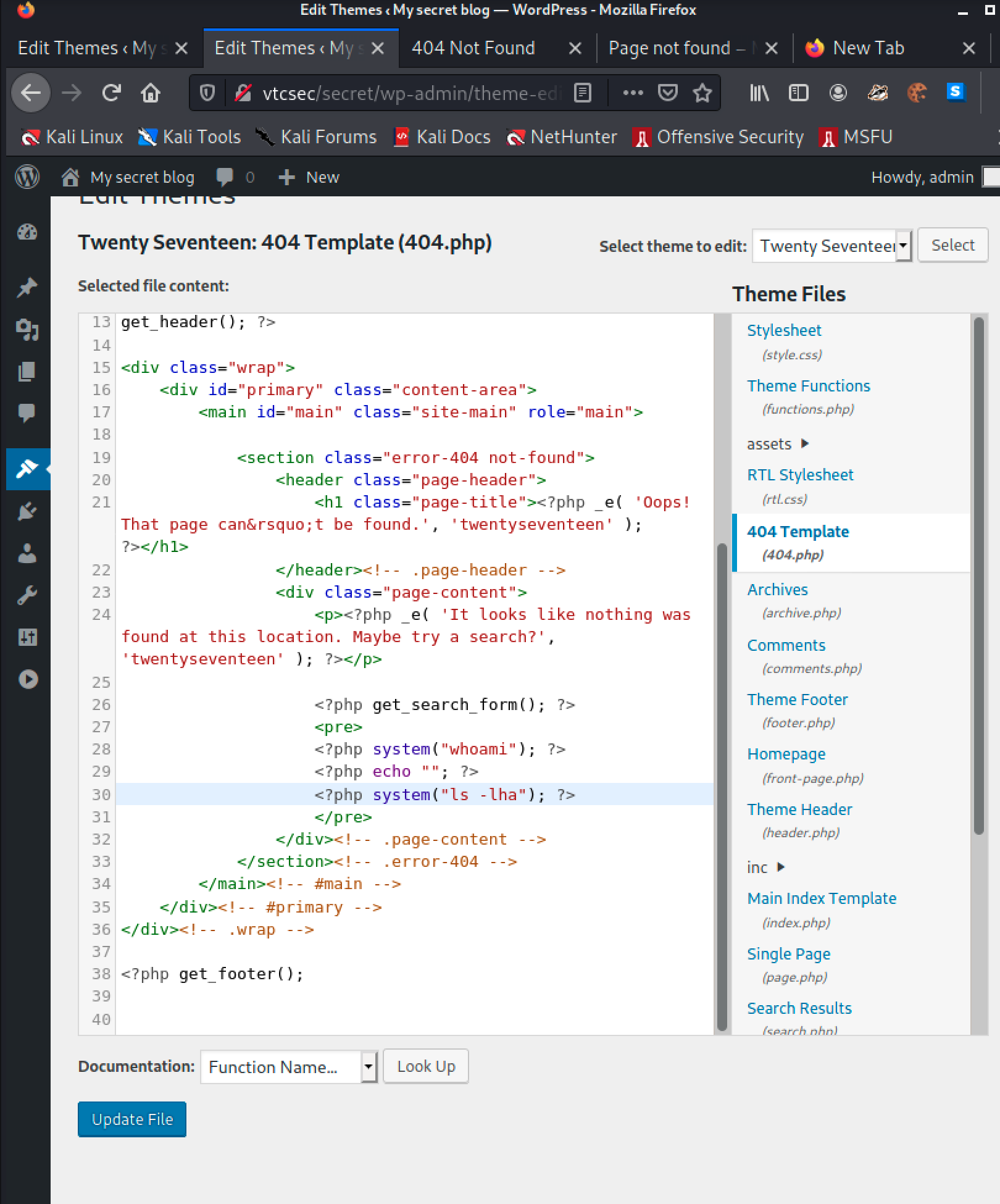
Description automatically generated

And you get into the web and web password is admin admin which is not configure

Graphical user interface, text, application

Description automatically generated

After modifying the web script, you can find the passwd file of the server



Graphical user interface, website

Description automatically generated

Use Metasploit to find build-in backdoor of the website

Text

Description automatically generated

Use the reverse payload to try to access the box

Text

Description automatically generated

After setting the LHOST, RHOST and payload. I could exploit the box successfully.

Graphical user interface, text

Description automatically generated

Use the leaked database password and add to rockyou filfe and Using hydra to access ssh attack

The password is marlinspike as indicate in the leaded database

Text

Description automatically generated

Text

Description automatically generated