Penetration Test Report — Stages & Tools

Test Date: September 24, 2025 - September 26,2025

Tested By: Chinonso Uche Unogu

Target: IP 10.10.77.53

Why this test was done:

To identify vulnerabilities and retrieve training flags to validate detection and response controls in a safe, authorized lab environment.

Stages / Tasks (with short process and tools)

1. Reconnaissance

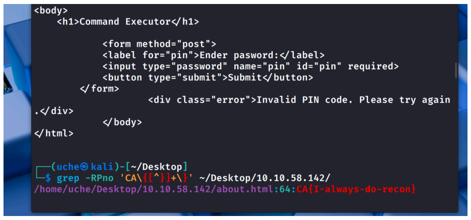
Performed passive and active reconnaissance to discover live hosts, open ports, and service banners.

Tools: Using nmap ports and service discovery, Gobuster for directory/virtual-host brute forcing, Curl for Probe endpoint and grep for searching output/logs.

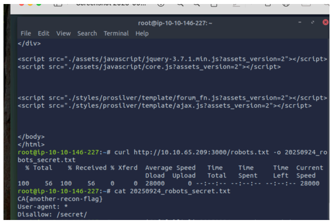
Ports Discovered: 80/Tcp open http Apache https 2.4.62 ((debian)) http tittle: dev.bittu | portfolio. 3000/Tcp open http Apache httpd 2.4.62 ((Debian)) http tittle: http-robots.txt

11010/Tcp open http Apache httpd 2.4.62((Debian) http tittle: Command Executor

Flag #1 & 2



```
<body>
    <h1>Command Executor</h1>

            <form method="post">
            <label for="pin">Ender pasword:</label>
            <input type="password" name="pin" id="pin" required>
            <button type="submit">Submit</button>
        </form>
                <div class="error">Invalid PIN code. Please try again
.</div>
            </body>
</html>


┌──(uche㉿kali)-[~/Desktop]
└─$ grep -RPno 'CA\{[^}]+\}' ~/Desktop/10.10.58.142/
/home/uche/Desktop/10.10.58.142/about.html:64:CA{I-always-do-recon}
```

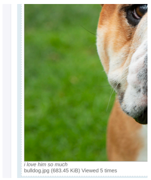


```
</div>

<script src="./assets/javascript/jquery-3.7.1.min.js?assets_version=2"></script>
<script src="./assets/javascript/core.js?assets_version=2"></script>



<script src="./styles/prosilver/template/forum_fn.js?assets_version=2"></script>
<script src="./styles/prosilver/template/ajax.js?assets_version=2"></script>



</body>
</html>
root@ip-10-10-146-227:~# curl http://10.10.65.209:3000/robots.txt -o 20250924_ro
bots_secret.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    56  100    56    0     0  28000      0 --:--:-- --:--:-- --:--:-- 28000
root@ip-10-10-146-227:~# cat 20250924_robots_secret.txt
CA{another-recon-flag}
User-agent: *
Disallow: /secret/
```

2. Administrator password

Searched for exposed configuration files, backups, or dumps that may contain credentials and checked for default accounts. And also found the Administrator password(bulldog) on a publicly accessible webpage.

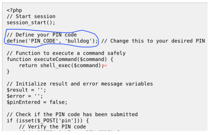
Tools: gobuster (to find files), curl and grep/strings (to search content).



i love him so much

bulldog.jpg (683.45 KiB) Viewed 5 times

Flag #3

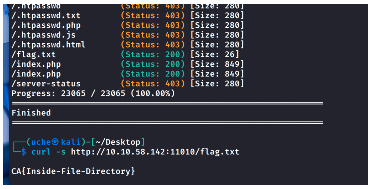


```
<?php
// Start session
session_start();

// Define your PIN code
define('PIN_CODE', 'bulldog'); // Change this to your desired PIN

// Function to execute a command safely
function executeCommand($command) {
    return shell_exec($command);
}

// Initialize result and error message variables
$result = '';
$error = '';
$pinEntered = false;

// Check if the PIN code has been submitted
if (isset($_POST['pin'])) {
    // Verify the PIN code
```

3. Web directory flag

Enumerated web directories and endpoints to locate hidden files such as flag.txt and retrieved contents via HTTP. curl for direct HTTP requests.

Flag #4

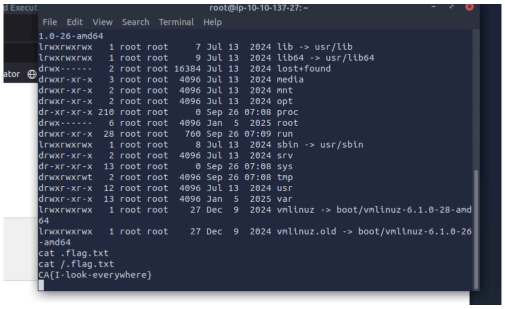


```
/.htpasswd            (Status: 403) [Size: 280]
/.htpasswd.txt        (Status: 403) [Size: 280]
/.htpasswd.php        (Status: 403) [Size: 280]
/.htpasswd.js         (Status: 403) [Size: 280]
/.htpasswd.html       (Status: 403) [Size: 280]
/flag.txt             (Status: 200) [Size: 26]
/index.php            (Status: 200) [Size: 849]
/index.php            (Status: 200) [Size: 849]
/server-status        (Status: 403) [Size: 280]
Progress: 23065 / 23065 (100.00%)
===============================================================
Finished
===============================================================

┌──(uche㉿kali)-[~/Desktop]
└─$ curl -s http://10.10.58.142:11010/flag.txt

CA{Inside-File-Directory}
```

4. File system flag

Explored accessible file system areas using available access (LFI, shell, or misconfig) to find hidden files like dot files. Tools: nc/ncat or SSH (for shells), find/ls/grep/cat (to locate and read files).

Flag #5



```
1.0-26-amd64
lrwxrwxrwx   1 root root     7 Jul 13  2024 lib -> usr/lib
lrwxrwxrwx   1 root root     9 Jul 13  2024 lib64 -> usr/lib64
drwx------   2 root root 16384 Jul 13  2024 lost+found
drwxr-xr-x   3 root root  4096 Jul 13  2024 media
drwxr-xr-x   2 root root  4096 Jul 13  2024 mnt
drwxr-xr-x   2 root root  4096 Jul 13  2024 opt
dr-xr-xr-x 210 root root     0 Sep 26 07:08 proc
drwx------   6 root root  4096 Jan  5  2025 root
drwxr-xr-x  28 root root   760 Sep 26 07:09 run
lrwxrwxrwx   1 root root     8 Jul 13  2024 sbin -> usr/sbin
drwxr-xr-x   2 root root  4096 Jul 13  2024 srv
dr-xr-xr-x  13 root root     0 Sep 26 07:08 sys
drwxrwxrwt   2 root root  4096 Sep 26 07:08 tmp
drwxr-xr-x  12 root root  4096 Jul 13  2024 usr
drwxr-xr-x  13 root root  4096 Jan  5  2025 var
lrwxrwxrwx   1 root root    27 Dec  9  2024 vmlinuz -> boot/vmlinuz-6.1.0-28-amd
64
lrwxrwxrwx   1 root root    27 Dec  9  2024 vmlinuz.old -> boot/vmlinuz-6.1.0-26
-amd64
cat .flag.txt
cat /.flag.txt
CA{I-look-everywhere}
```

5. Root folder flag

Performed local enumeration and safe privilege-escalation checks to identify misconfigurations or exploitable vectors to access /root for the root flag.

Key Recommendations:

Keep systems and software patched regularly.

Use strong authentication and enable multi-factor authentication for admin accounts.

Harden web applications by validating inputs and removing debug endpoints from production.

Restrict file permissions and apply the principle of least privilege.

Enable centralized logging and monitoring with alerts for suspicious activity.

Conclusion

The exercise showed how exposed information and misconfigurations can be leveraged; implement the recommendations to reduce risk.