# OSCP Exam Report

**Offensive Security Certified Professional**
**Candidate Name:** John Doe
**OS-ID:** OS-123456
**Exam Date:** May 15, 2025
**Institute:** Ethical Hacking Training Institute
**Instructor:** Mr. Aakash Sharma

**Table of Contents**

## 1. Introduction

This report provides a detailed account of the exploitation process performed during the OSCP 24-hour certification exam. Each target machine was attacked using manual methods, scripts, and tools, with privilege escalation achieved where required. Screenshots, flags, and supporting evidence are included in each section.

## 2. Exam Environment and Setup

- **Operating System:** Kali Linux 2024.4
- **Tools Used:** nmap, gobuster, metasploit (minimal), netcat, python, linpeas, smbclient
- **VPN Connection:** Established via .ovpn file provided by Offensive Security
- **Notes Tool:** CherryTree
- **Report Tool:** LibreOffice / Word (for export to PDF)

## 3. Exploitation Summary

| Machine Name | IP Address | Initial Access | Privilege Escalation | Root Flag Found |
|---|---|---|---|---|
| Alpha | 10.10.10.5 | RFI | Sudo Misconfig | Yes |
| Bravo | 10.10.10.6 | SMB Null Share | Kernel Exploit | Yes |
| Charlie | 10.10.10.7 | WebShell | Cron Job Abuse | Yes |
| Delta | 10.10.10.8 | FTP Login | PATH Hijacking | Yes |
| BufferOverflow | 10.10.10.9 | BOF Exploit | Local System Access | Yes |

## 4. Target Machines

### 4.1 Machine 1 – Alpha

- **IP:** 10.10.10.5
- **Initial Exploit:** RFI via vulnerable.php?page=../../etc/passwd
- **Privilege Escalation:** User had sudo access to /usr/bin/vim
- **Exploit:** Used sudo vim -c '!sh' to escalate to root
- **Root Flag:** 6d9ab3c3b23f1239...

**Screenshot:**

### 4.2 Machine 2 – Bravo

- **IP:** 10.10.10.6
- **Initial Exploit:** Anonymous SMB login; download of backup files
- **Exploit:** Discovered hardcoded credentials, SSH login
- **Privilege Escalation:** Kernel exploit using dirtycow.c
- **Root Flag:** 91d29fd1212bdabc...

### 4.3 Machine 3 – Charlie

- **IP:** 10.10.10.7
- **Initial Exploit:** LFI and reverse shell via vulnerable webapp
- **Privilege Escalation:** Found cronjob running script in /tmp
- **Exploit:** Replaced script with reverse shell
- **Root Flag:** f21cdac23183abc4...

### 4.4 Machine 4 – Delta

- **IP:** 10.10.10.8
- **Initial Exploit:** FTP login with default creds
- **Exploit:** Found .sh file executed by root via PATH hijacking
- **Root Flag:** 9a321cdef90123dd...

## 5. Buffer Overflow Walkthrough

**Target: 10.10.10.9 (Buffer Overflow Machine)**

- **Vulnerable Service:** Custom binary running on port 31337
- **Tool Used:** Immunity Debugger, mona.py
- **Steps:**
    1. Sent fuzzed payload to find crash offset
    2. Identified EIP offset (524)
    3. Controlled EIP with exact pattern

4. Verified bad characters
5. Generated shellcode using msfvenom
6. Final Payload:

junk = "A"*524 eip = "\xF3\x12\x17\x31" nop = "\x90"*16
shellcode = [reverse shell payload]

- **Exploit Result:** Reverse shell as SYSTEM
- **Root Flag:** 7cd3bbd8fabc3213...

**Screenshot:**

**6. Privilege Escalation Techniques Used**

| Technique | Used On |
|---|---|
| Sudo Misconfiguration | Alpha |
| Kernel Exploit | Bravo |
| Cron Job Abuse | Charlie |
| PATH Variable Hijack | Delta |
| BOF to SYSTEM Shell | BOF Target |

**7. Final Root Flag Summary**

| Machine | Root Flag |
|---|---|
| Alpha | 6d9ab3c3b23f1239... |
| Bravo | 91d29fd1212bdabc... |
| Charlie | f21cdac23183abc4... |
| Delta | 9a321cdef90123dd... |
| BOF | 7cd3bbd8fabc3213... |

**8. Lessons Learned**

- Automation helps, but manual enumeration is key
- Time management is crucial, especially during the last 8 hours

- Taking notes using CherryTree greatly aided report writing
- Practice buffer overflows thoroughly to avoid errors during exam

**9. Tools Used**

- nmap
- gobuster
- enum4linux
- metasploit (minimal use)
- linpeas
- msfvenom
- mona.py
- gdb
- netcat
- python3
- vim, nano

**10. Screenshots**

(Screenshots of each root flag, privilege escalation step, buffer overflow shell, and initial foothold)

**11. Conclusion**

All five machines were successfully exploited with root-level access, and all required flags were collected and documented as per Offensive Security guidelines. The Ethical Hacking Training Institute provided excellent preparation for the OSCP exam with hands-on lab simulations, expert mentorship, and structured reporting practice.