CIS 76 – Ethical Hacking

Building an open source Pentest Sandbox, carrying out a Remote Code Execution exploit, and Remediating the RCE vulnerability.

Ryan Borden
December 3, 2017

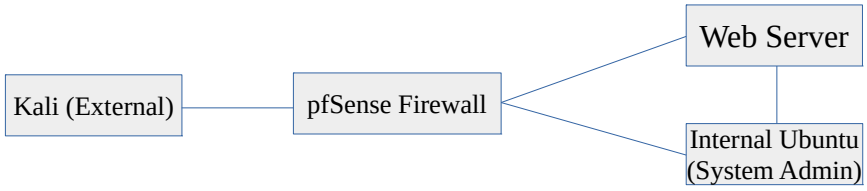
Contact: ryanborden81@gmail.com

Warning and Permission:

Unauthorized hacking can result in prison terms, large fines, lawsuits, and being dropped from the course!

Scenario & Diagram:

Many web applications contain file upload functionality intended to allow users to upload pictures, documents, videos, etc. While the intent of this functionality is to allow users to create and share content, it is often exploited by malicious users to attack others or to attack the underlying server and machines on the network. In this lab we will exploit a poorly coded file upload webpage to gain root access to the underlying server. Once we have root access we will use SSH to migrate from the server to an adjacent Ubuntu Machine used by an internal System Administrator and exfiltrate a sensitive file.



Requirements:

Oracle Virtualbox - https://www.virtualbox.org/wiki/Downloads

Kali Linux - http://cdimage.kali.org/kali-2017.3/kali-linux-2017.3-amd64.iso

PFSense Firewall - https://www.pfsense.org/download/

Ubuntu 16.04 LTS Server - https://www.ubuntu.com/download/server/thank-you?country=US&version=16.04.3&architecture=amd64

Ubuntu 16.04 LTS Desktop - https://www.ubuntu.com/download/desktop/thank-you?country=US&version=16.04.3&architecture=amd64

KeePassX (Optional) - https://www.keepassx.org/downloads

Vulnerability:

Unrestricted file upload occurs when a server is poorly coded and improperly configured. The result of this issue is that remote attackers are able to upload arbitrary, malicious files to the server which, when accessed, execute the code contained within[1]. In the most vulnerable application, this issue leads Remote Code Execution (RCE)[2].

Exploit:

RCE can grant the remote attacker full control over the web directory, and in some cases the attacker will be able to escalate their permission or attack peripheral machines on the same network. To date, the Exploit Database contains records for 6,629 individual RCE vulnerabilities on various services and applications[3].

Instructions:

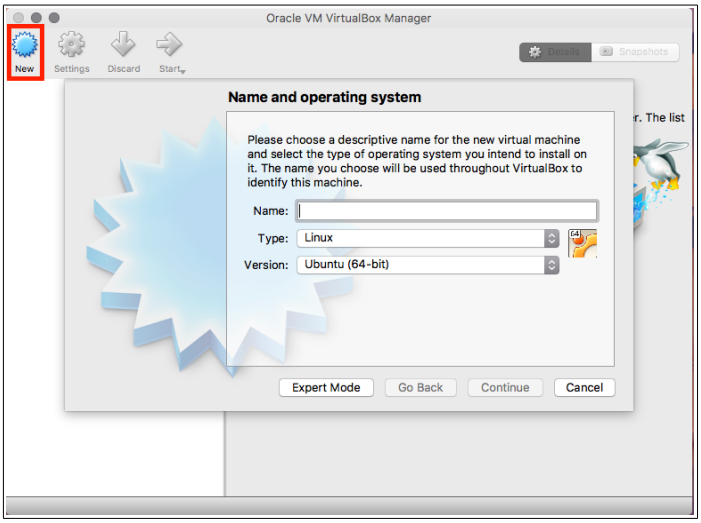
Before we begin the process of building the lab, it is important to note that things don't always go as planned. While initially building this lab I ran issues which required me to delete an entire VM and start from scratch a few times. If an install is not working correctly don't be afraid to scrap the install and start again. Sometimes while running updates, installing dependancies, etc. things can get corrupted and brick the install (especially with Kali). It is better and faster to start fresh than to waste time trying to fix a broken install.

1. Install VirtualBox on your host machine. This is a standard installation using the default settings for your OS.

Ubuntu Sysadmin setup

2. Open VirtualBox and install Ubuntu 16.04 Desktop.

    a. Click on "New", use the "Type" drop-down menu to select Linux, and use the "Version" drop-down menu to select Ubuntu (64-bit)



b. This VM will be the internal System Admin user, so name it accordingly. Click Continue.

c. You will be prompted to allocate the RAM for this VM. The default value of 1024 MB should be sufficient. Click Continue.

d. You will be prompted to create the new virtual hard disk. The default should be 10.00 GB with the "Create a virtual hard disk now" radial button selected. Confirm these settings and click Create.

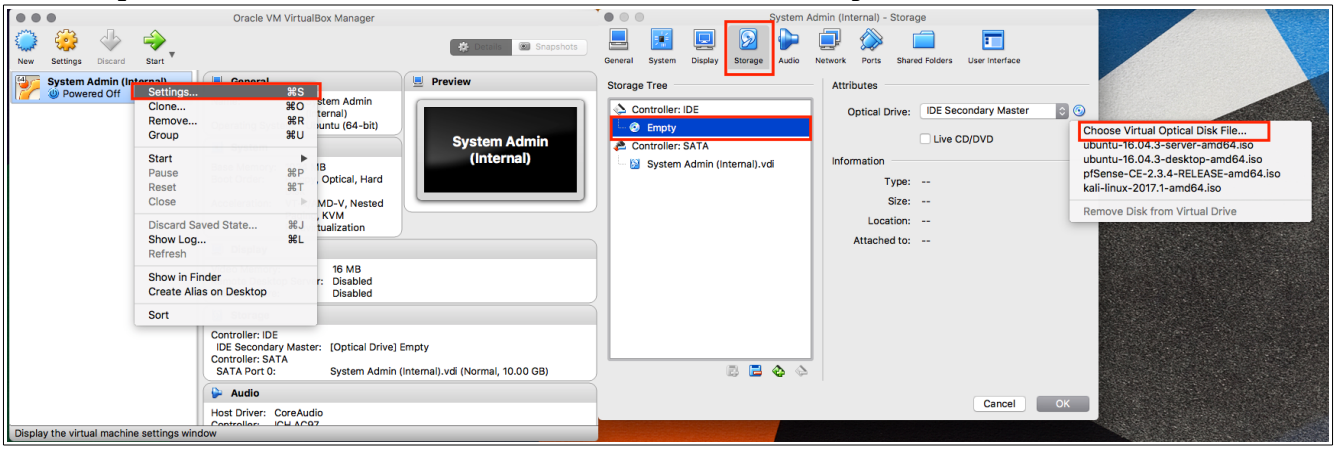
e. You will be prompted to select the hard disk file type. For this, the default VDI format is acceptable. Click Continue.

f. You will be prompted to set the disk allocation to dynamic or fixed. Select dynamic and click Continue.

g. You will now be on the final check for the disk creation. Confirm all of the information is correct and click Create.

h. You will now see the main VirtualBox screen with your new VM. Right click the VM and selected Settings.

i. You will now see the newly created VM in the VirtualBox menu. Right click this VM, and select Settings. Then click on the Storage tab. Select the CD icon from the storage tree, and then click the CD icon next to the Optical Drive drop-down menu. Select "Choose Virtual Optical Disk File..."; this will open a file browser. Navigate to the Ubuntu 16.04 Desktop ISO and click Open. Then click OK to close the Settings window.

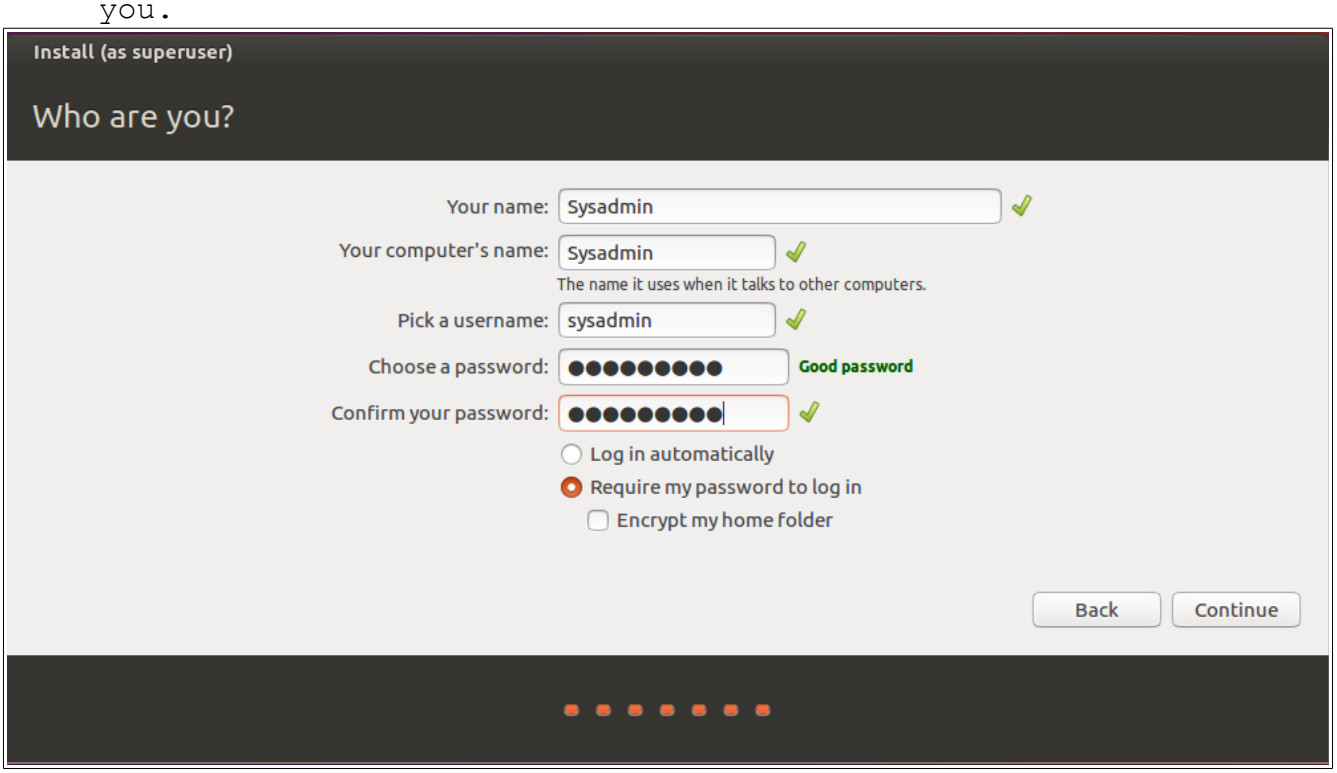


j. Start the VM. The installer will launch. Select your language, and click the Install Ubuntu button. Check both the Download Updates & Install 3rd part software boxes and click Continue. Select the Erase disk and install Ubuntu radial button

then click Install Now. You will be prompted with a dialog box; Click Continue. Select your timezone and click Continue. Select your keyboard layout and click Continue.

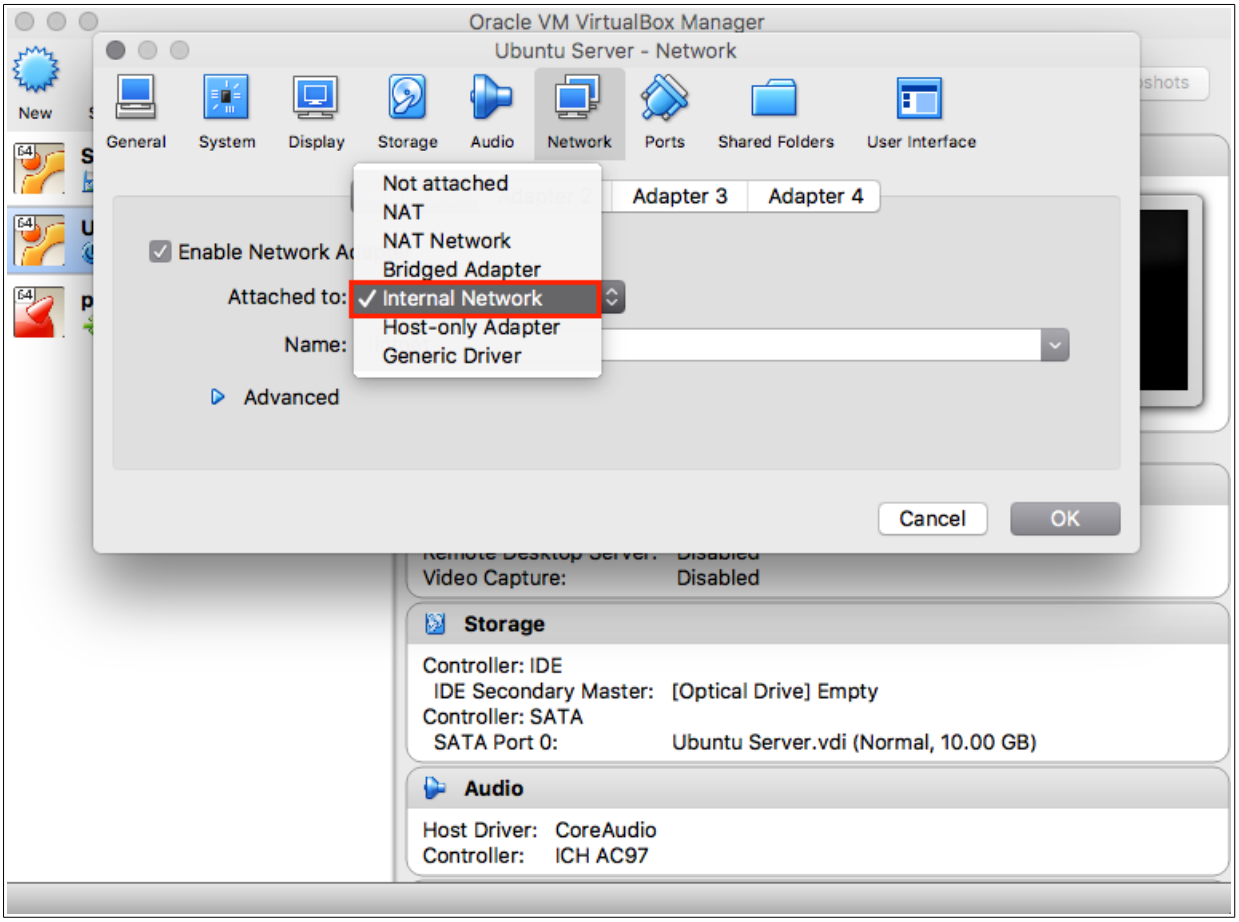
k. You will now be prompted to create the user. Enter the following values and set your password (mine is P@ssw0rd! Because it's super secure). Click Continue.

Optional: Save the account information in KeePassX. The benefit of KeePassX is that it can auto-generate secure passwords for you.



l. Once the install has completed you will be prompted to Restart. The install ISO should auto-detach. If not, return to the Storage settings of the VM and remove it.

m. After you have completed the install of the VM return to the VirtualBox menu. Right click on the VM, select Settings, click on the Network tab, and change the "Attach to:" drop-down to Internal Network for Adapter 1



n. At this point you may want to take a snapshot of this VM, because later you will be making it extremely vulnerable. In order to take a snapshot start the VM. Once it has booted up click on Machine tab in the menu and select "Take a Snapshot" and name it.

Ubuntu Server setup

3. Repeat this process but this time install the Ubuntu 16.04 Server ISO. The following details the installation variations:

a. After selecting your language there will be a list of available options. Select the "Install Ubuntu Server" option.

b. During the install process you will be prompted to set a hostname. Set this to "ubuntu-server". After this you will be prompted to enter a full name and username; set these to "server". You will be asked to set the password. (Optional: Save the account information in KeePassX) Next you will be asked if you want to encrypt the home directory; select No. The installer should auto detect your time zone. Finally, you will be prompted to select the disk partition; select Guided – use entire disk.

c. During the installation you will be prompted for software selection. From this list select LAMP server and OpenSSH server (arrow up and down to the option and press Space to select).

d. You will be prompted to setup the password for MySQL. Set this to P@ssw0rd! (Optional: Save the account information in KeePassX)

e. Next, you will be asked to install the GRUB boot loader, select Yes.

Kali Setup

4. The setup on Kali is similar to Ubuntu. Go through the same Vbox initial setup (Version will be Other Linux) and put the ISO in the drive. One key difference is that you will **NOT** be changing the network adapter. It will remain on NAT. Once it boots up select Graphical Install. The install process is pretty straight forward; for the most part leave everything at default.

a. When it comes to the disk partition prompt use the entire disk, select Guided partitioning, and have all files in one partition.

b. At this point you will want to install the VirtualBox Guest Additions. Follow this guide: https://www.blackmoreops.com/2014/06/10/correct-way-install-virtualbox-guest-additions-packages-kali-linux/[4]

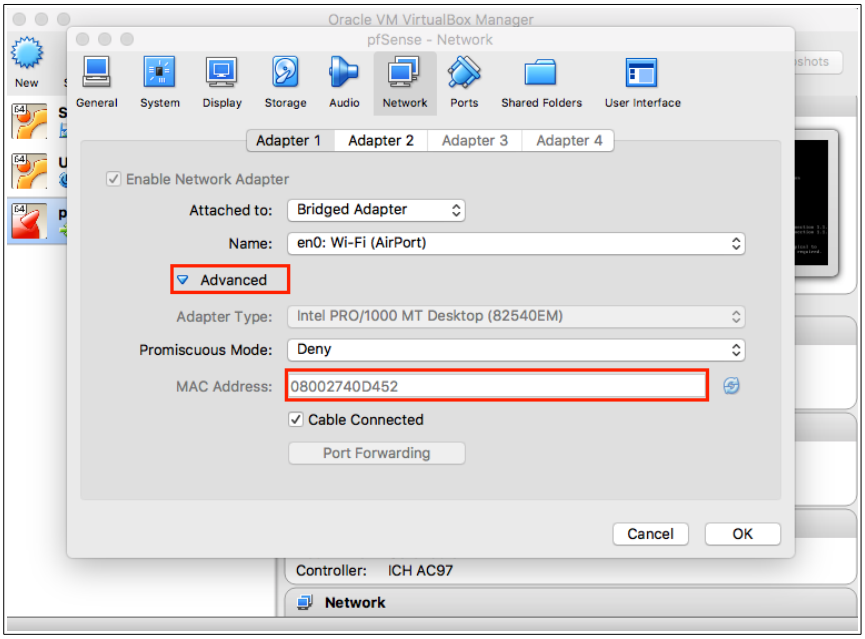
c. Once you have your Kali VM operation change the network sudo adapter to Bridged.

pfSense Firewall Setup

5. Now it is time to install pfSense. This is a little more complex, and therefore I am going to default to this great video tutorial on installing pfSense https://youtu.be/7nr9HNZ7OmY[5] Follow his VirtualBox setup ensuring that you allocate sufficient RAM, and that you set up 2 NIC's (one Bridged and one Internal). The install for 2.4.x is a little different. Just choose the Install option, and the Auto option.

a. After the install has completed you will need to unmount the ISO. Click the Devices menu, scroll over Optical Drives, and choose "Remove disk from virtual drive"

b. If you need to manually set the interfaces you will be able to check the MAC addresses by right clicking the VM in VirtualBox, selecting settings, clicking the Network tab, and clicking the Advanced item to expand the list. Compare the MAC addresses listed for each adapter to em0 and em1 in pfSense.



c. After you have completed the initial setup it is time to configure the firewall. Follow this video https://youtu.be/rgupXMlz3is[6]

tl;dr: It's a long video so I'll give a quick guide to setting up the firewall if you don't want to watch it (though I would encourage you to watch it as there is a lot of good information).

1) Navigate to Firewall > NAT
2) Click Add (either one)
3) Set the Destination Port Range from HTTP to HTTPS
4) Start up the Ubuntu server VM, and once it has loaded type ifconfig to get the IP
5) Enter the Ubuntu server IP in Redirect Target IP
6) Set Redirect Target Port to HTTP
7) Set the Description to something meaningful
8) Leave everything else at default
9) Click Save
10) Click Apply Changes
11) Click on Interfaces > WAN
12) Scroll down and Uncheck "Block private networks and loopback addresses"
13) Click Save
14) Click Apply Changes
15) From your host machine browse to the WAN IP of pfSense and confirm that you see the Apache "It Works" page.

Building the Vulnerable Web Site

6. It is now time to build the vulnerable file upload page. To do this you will need to enter the web directory on the Ubuntu Server machine.

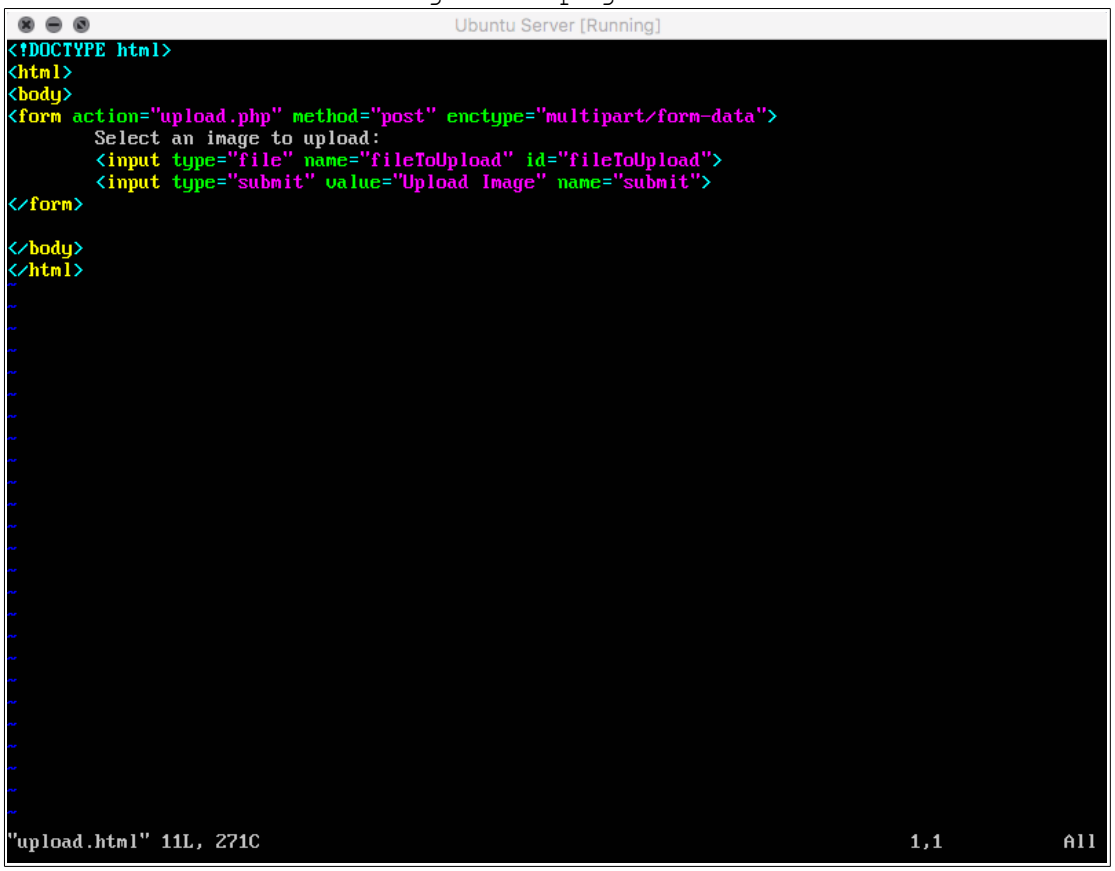
a. Enter the following command:

:$cd /var/www/html

b. Now open a text editor with root permissions and create the file upload HTML page. For this I used vim:

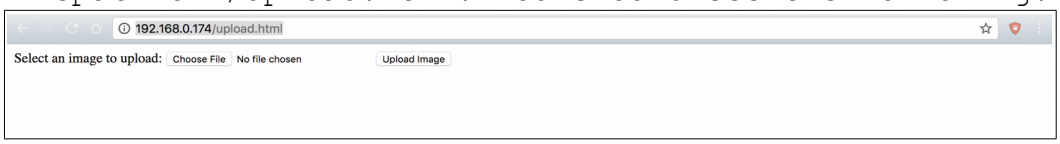
:$sudo vim upload.html

c. Create the following HTML page[7]:



Notes: If you use vim you will need to first type "I" for insert. After you have entered your code press the esc key to exit insert mode, and then enter ":wq" for write & quit. Other vim commands include ":q" for quit, and ":q!" for quit without saving.

d. Confirm that the upload HTML page has been created and is working correctly by browsing to the pfSense WAN IP with the filepath of /upload.html. You should see the following:



e. Next you will need to create the PHP file upload script. Open the text editor again (make sure to name the file "upload.php"), and enter the following code[7]:

```php
<?php
$target_dir = "uploads/";
$target_file = $target_dir . basename($_FILES["fileToUpload"]["name"]);
$uploadOk = 1;
$imageFileType = pathinfo($target_file,PATHINFO_EXTENSION);
// Accept the file maybe?
if(isset($_POST["submit"])) {
        $check = filesize($_FILES["fileToUpload"]["tmp_name"]);
        if($check !== false) {
                echo "File is a file - " . $check["mime"] . ".";
                $uploadOk =1;
        } else {
                echo "File is not a file";
                $uploadOk = 0;
        }
}
//Check if $uploadOK is set to 0
if ($uploadOk == 0) {
        echo "The file was not uploaded";
} else {
        if (move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file)) {
                echo "The file". basename($_FILES["fileToUpload"]["name"]). "has been uploaded.";
        } else {
                echo "Sorry, there was an error uploading your file.";
        }
}
echo "$target_file";
?>
```

f. Now create the uploads folder with the following command:

:$sudo mkdir uploads

g. In order for PHP to be able to write to this folder it needs permission. Since the intent is for this server to be vulnerable, we are going to make the whole www folder readable, writeable, and executable by anyone with the following commands:

:$cd /var/

:$sudo chmod -R 777 www

h. Now it is time to test out the uploader. Navigate to the upload page, and upload a test text file. Once the upload has completed navigate to /uploads in your browser and confirm that you see the file.

i. The ssh_config file will need to have StrictHostKeyChecking set to no. Enter the following command:

:$sudo vim /etc/ssh/ssh_config

j. Find the StrictHostKeyChecking line, uncomment it, and set the value to no.

Making The Sysadmin VM Vulnerable

7. We now need to make out sysadmin VM vulnerable. To do this we are going to open up SSH functionality, remove the password for the root user, and allow SSH to connect with no password.

a. First you will need to install OpenSSH on the sysadmin VM. To do this enter the following command:

:~$sudo apt-get install openssh-server

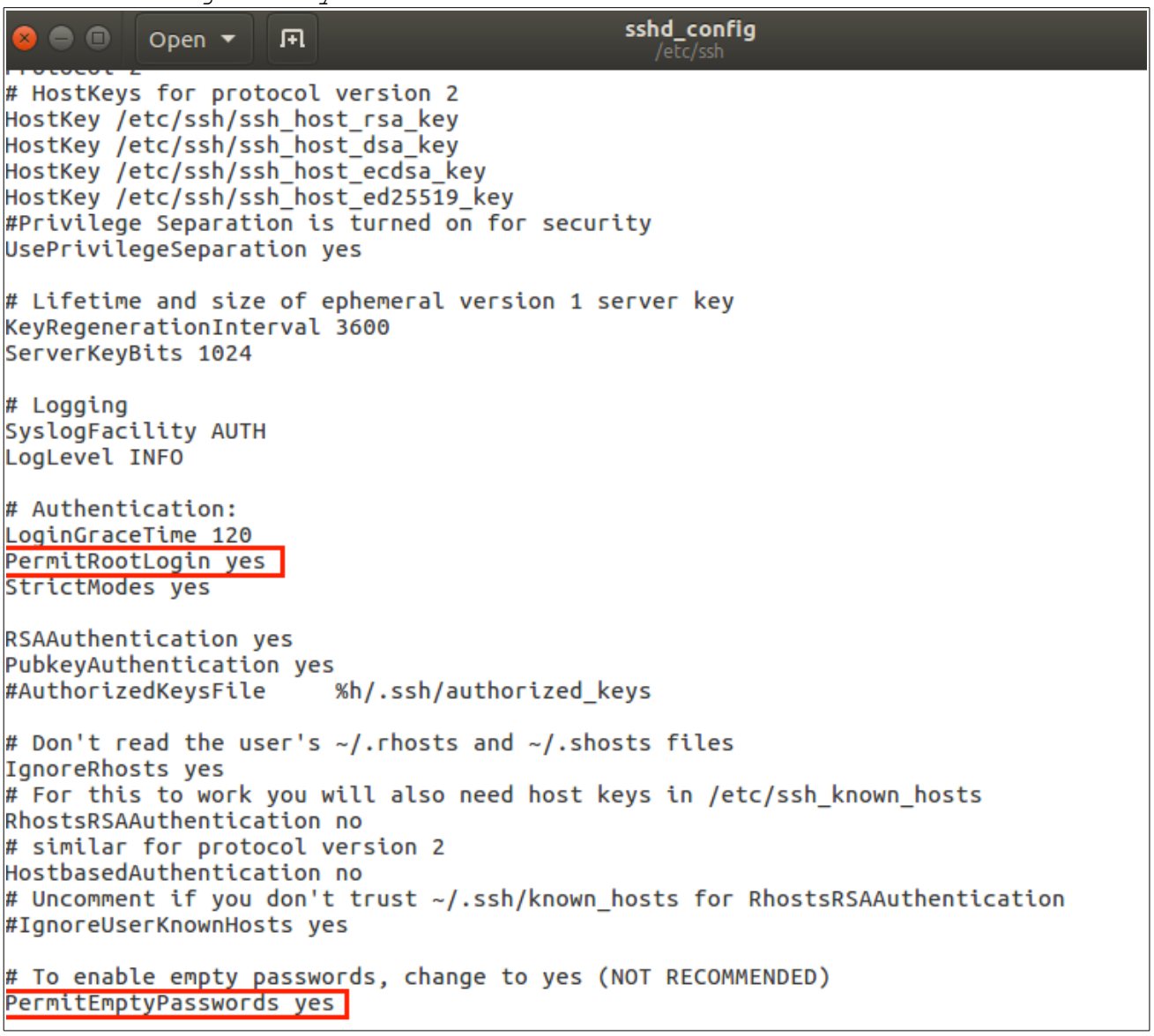
b. Now you need to set the root user to have no password. Enter the following command:

:$ sudo passwd -d root

c. Now you will configure OpenSSH to accept empty password. To edit this file enter the following command:

:$sudo gedit /etc/ssh/sshd_config

d. Edit the PermitEmptyPasswords entry to yes. Also change PermitRootLogin to yes.



e. Now the sshd service needs to be restarted. Enter the following command:

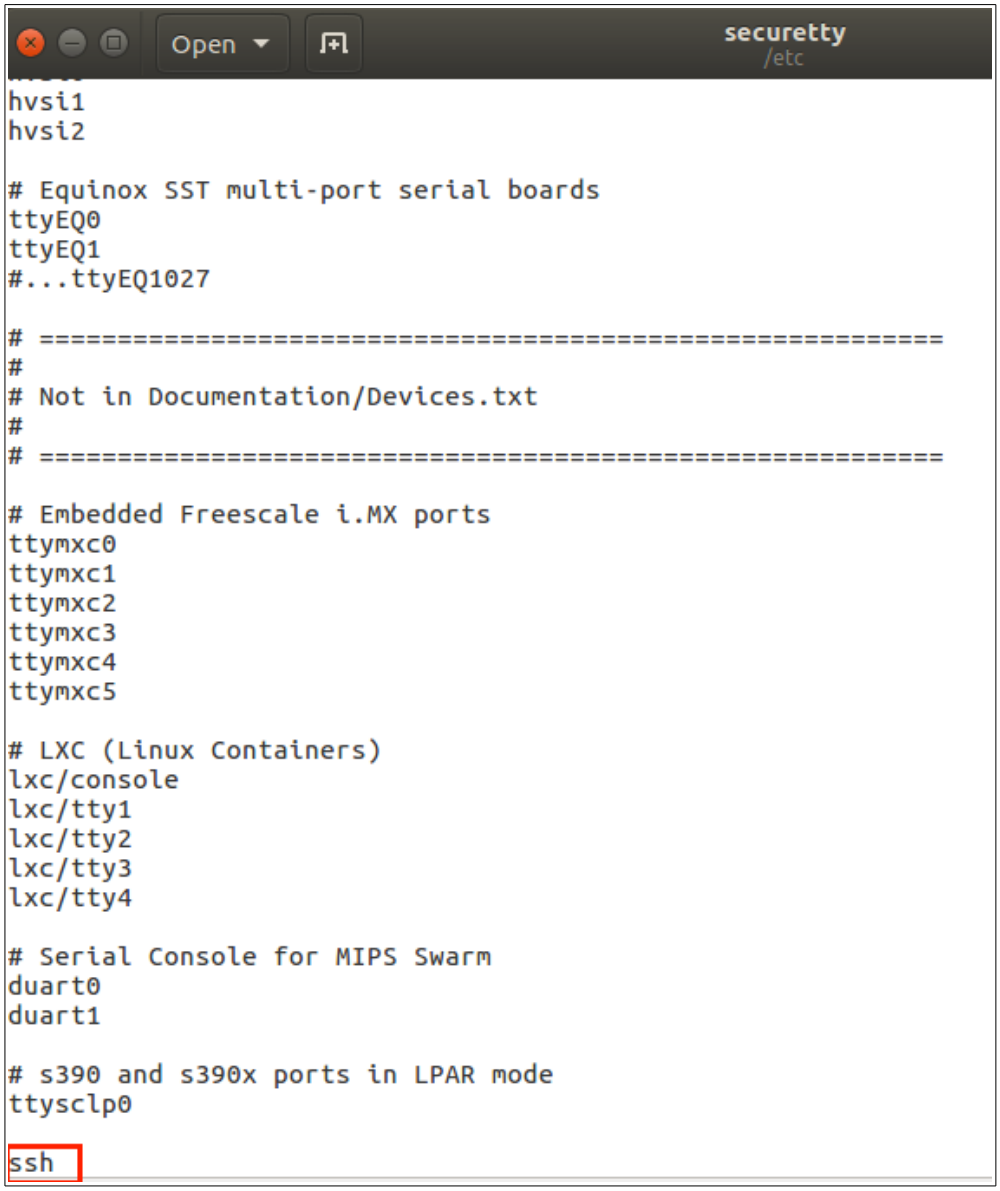
:$sudo service sshd restart

f. Finally, the securetty file needs to be modified to allow root to login to a terminal over ssh. Enter the following command:

:$ sudo gedit /etc/securetty

g. Scroll to the end of the file and enter the following:

ssh



h. Save and exit the file.

I. Finally, you need to create a file to exfiltrate. Using a text editor create a file with “My password is [enter the password]” in it. Save the file as “Password”.

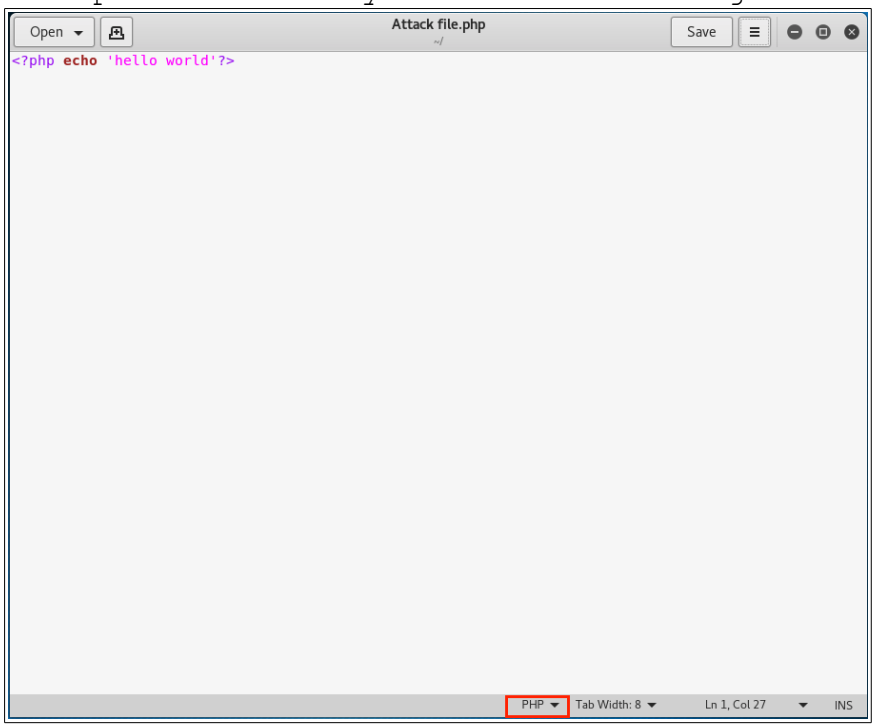
Hacking the Server

8. We now have a working, vulnerable web server; it is time to begin attacking it!

a. Start out by opening your Kali VM, as this will be the attacking machine. Browse to the pfSense WAN IP with the filepath of /upload.html

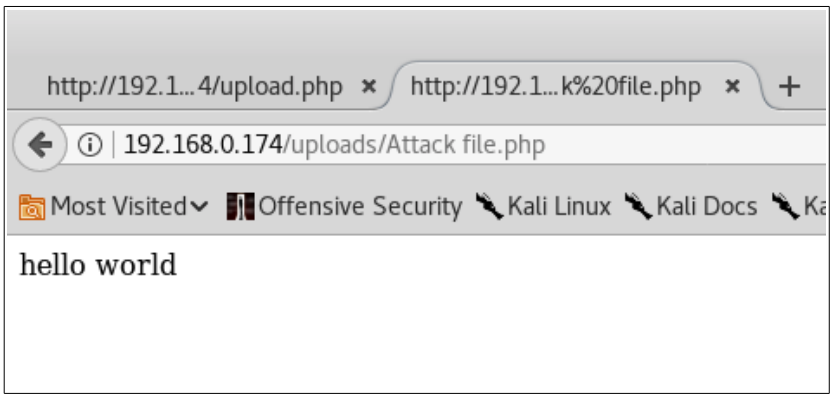
b. Open the Text Editor application in Kali. This is located in the Applications > Usual Applications > Accessories menu of click the grid of dots on the quick launch bar and search for it.

c. Since this is a file upload page and we'll imagine that the attacker has already gone through recon to fingerprint the server as a LAMP server, we are going to test is this server is vulnerable to Remote Code Execution. Create the following PHP file (note: on the bottom bar of the editor window you will see a drop-down that says Plain Text. Change this to PHP):

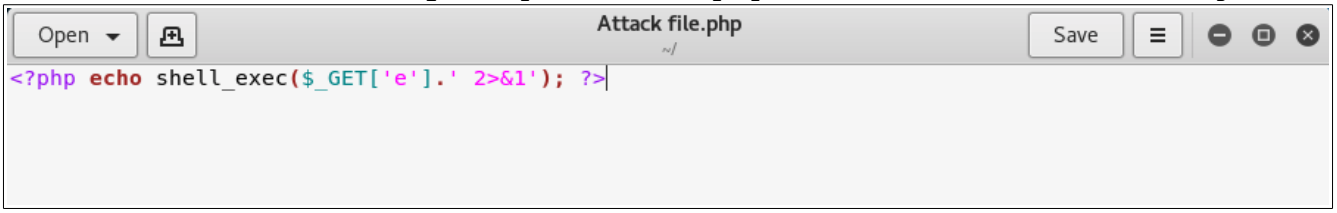


d. Save this file with a .php extension, and return to the file upload page in your browser. Upload the PHP test file.

e. Browse to the /uploads directory and open the PHP test file. You should see the following which means the PHP code was run:



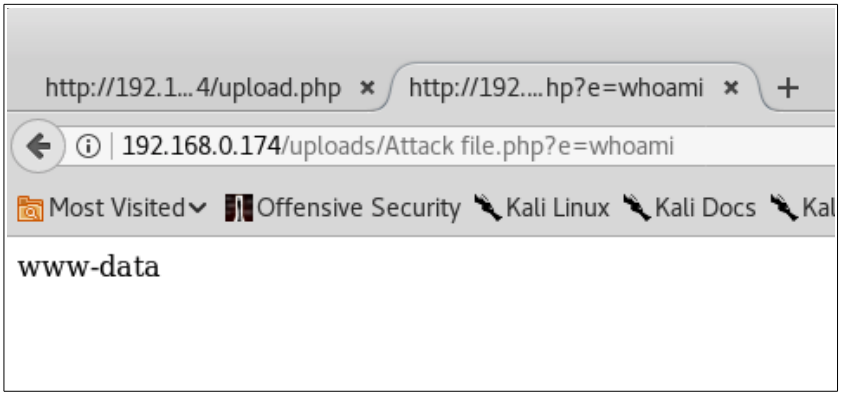
f. At this point we know our code is going to run, lets start probing for information. To do this we are going to write a shell in one line (yes, shell control with just one line of code). Overwrite your previous .php file with the following[8]:



g. Upload this file to the server and browse to it. You should see a blank page. Now add the following to the URL:

?e=whoami

You should now see the current role you have control over:



h. Now that we have control over the server it is time to begin probing the network. The first step is to determine which subnet this server is running on so that we can probe for other systems. Enter the following command:

?e=ifconfig

This should return an IP in the 192.168.x.x subnet.

i. Next we want to probe for active IP addresses on the LAN network. In this case, we know that there is only going to be one so enter the following replacing the "x" with the IP for your sysadmin VM:

?e=ping%20-c1%20192.168.x.x

j. Next we will get a reserve shell which we will place on the vulnerable server. Browse to the following URL, download the reverse shell tarball, and extract it into the Documents folder: http://pentestmonkey.net/tools/web-shells/php-reverse-shell[9]

k. Navigate to your Documents folder and open the php-reverse-shell.php file in a text editor.

l. Scroll down to the ip and port variables. Change the ip variable to the ip of the Kali VM. Change the port variable to 80. Save and close.

m. Return to the file upload page in your browser and upload the reverse shell to the server.

n. Open a terminal in Kali and enter the following command:

:$nc -v -n -l -p 80

o. Navigate to the uploads directory in your browser, and open the reverse shell file.

p. Return to the terminal window and you will now have a reverse shell into the server. Now you can establish an ssh session to the Sysadmin machine.

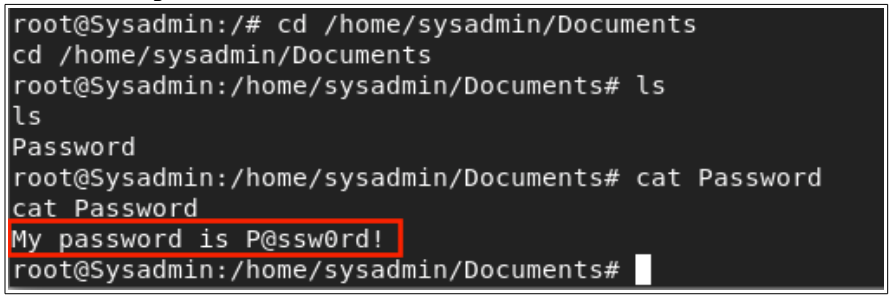
p. Enter the following command in your reverse shell:

$ssh -tt root@192.168.x.x

q. You are now in control of the Sysadmin machine. Let's see what the Sysadmin user has in his Documents folder. Enter the following commands in your reverse shell:

#cd /home/sysadmin/Documents
#ls

r. There is a file called Password; I wonder what is in there. Cat this file out and retrieve the contents. You should see the following:



Remediating the Vulnerability

9. Now that we have exploited the vulnerable web server, it is time to remediated the file upload vulnerability.

a. Return to the web directory of the server

:$cd /var/www/html

b. Open the upload.php file in your text editor

:$sudo vim upload.php

c. Enter the following code to your upload.php file[7]:

```
<?php
$target_dir = "uploads/";
$target_file = $target_dir . basename($_FILES["fileToUpload"]["name"]);
$uploadOk = 1;
$imageFileType = pathinfo($target_file,PATHINFO_EXTENSION);
//Accept the file
if(isset($_POST["submit"])) {
        $check = filesize($_FILES["fileToUpload"]["tmp_name"]);
        if($check !== false) {
                echo "File is valid - " . $check["mime"] . ". ";
        } else {
                echo "File is not a file.";
                $uploadOk = 0;
        }
}
//Allow certain file formats
if($imageFileType != "jpg" && $imageFileType != "png" && $imageFileType != "jpeg" && $imageFileType
!= "gif") {
        echo "Sorry, only JPG, JPEG, PNG, and GIF files are allowed. ";
        $uploadOk = 0;
}
//Check if $uploadOk is set to 0
if ($uploadOk == 0) {
        echo "The file was not uploaded";
} else {
        if (move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file)) {
                echo "The file ". basename($_FILES["fileToUpload"]["name"]). " has been uploaded.";
        } else {
                echo "Sorry, there was an error uploading your file.";
        }
}
echo "$target_file";
?>
~
~
~
-- INSERT --                                                    20,2          All
```

d. Now take one additional step, and make sure that PHP will not run in the uploads directory. To do this enter the following command:

:$sudo vim /etc/apache2/sites-available/000-default.conf

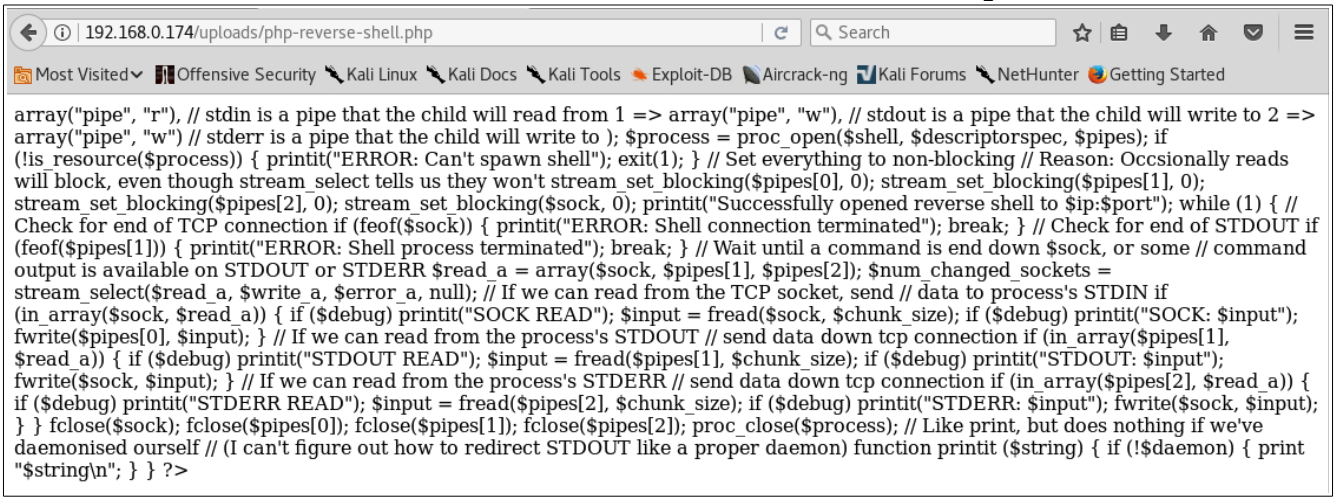
e. Enter the following line to this file:

```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
        <Directory /var/www/html/uploads>
                php_admin_value engine off
        </Directory>
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
~
~
-- INSERT --                                                    31,1          All
```

f. Now restart the Apache service with the following command:

:$sudo apachectl restart

g. Return to Kali, navigate to the Uploads directory, and open the reverse shell file. You should now see only text:



h. At this point, if you plan on reusing this pentest lab in the future, you will need to restore the sysadmin machine to a non-vulnerable state. This can be accomplished by deleting and reinstalling it, or by rolling back to a snapshot. If you took a snapshot following the VM's creation simply click the close button on the VM's window, check the "Restore current snapshot '{NAME}' box, and power the machine down.

Appendix A:

[1]: OWASP Unrestricted File Upload - https://www.owasp.org/index.php/Unrestricted_File_Upload

[2]: OWASP Code Injection - https://www.owasp.org/index.php/Code_Injection

[3]: Exploit Database RCE Vulnerabilities - https://www.exploit-db.com/remote/?order_by=date_published&order=desc&pg=1

[4]: Installing Vbox Guess Additions Guide - https://www.blackmoreops.com/2014/06/10/correct-way-install-virtualbox-guest-additions-packages-kali-linux/

[5]: Mark Funeaux Youtube pfSense Installation Tutorial - https://youtu.be/7nr9HNZ7OmY

[6]: Mark Funeaux Youtube pfSense Configuration Tutorial - https://youtu.be/rgupXMlz3is

[7]: W3Schools Guide to building a PHP File Upload - https://www.w3schools.com/php/php_file_upload.asp

[8]: One line PHP Shell - http://www.grobinson.me/single-line-php-script-to-gain-shell/

[9]: Pentest Monkey Reverse Shell - http://pentestmonkey.net/tools/web-shells/php-reverse-shell