Project 3 Help Documentation

Last Updated: 3/5/2025

Contents

Getting kali ready

To get kali in a good state to follow CTF4 and CTF5, you'll want to install a few packages.

Bring up a terminal and run the command

```
apt update
```

This command syncs the lists of apps you can install.

Next, run the following commands to download httprint and mariadb (mysql alternative):

```
Sudo apt install httprint mariadb-server
```

See the next section on installing nessus.

Installing nessus on kali:

Installing Nessus on Kali is not as straightforward as running “apt install nessus”. Instead, you need to find the community edition of nessus, install it using the dpkg system, and set it up. To help you through this, I’ve created a video.

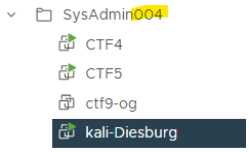
https://uni.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=b5d68c03-58d0-495d-80d3-b11f00ff24a7

I’m expecting at least one of the new CTF documents (either 4 or 5) to give enough details on the installation for a new computer science student to follow, including screenshots.

Both CTF documents should talk about nessus and run a nessus scan.

Finding the CTF machines:

Each group belongs to a specific subnet on vSphere. In particular, you belong to subnet 10.161.<folder_number>.0/24, where folder number is your vSphere folder number:



(In the picture above, my folder number is 4, so my subnet is 10.161.4.0/24.)

To figure out your ip address, you can use the command `ip a`

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN grou
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
    link/ether 00:50:56:82:90:fb brd ff:ff:ff:ff:ff:ff
    inet 10.161.4.31/24 brd 10.161.4.255 scope global dynamic noprefixro
       valid_lft 358sec preferred_lft 358sec
    inet6 fe80::590c:1f13:75f6:eb39/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

In this case, my ip address is 10.161.4.31.

To figure out the ip addresses of the CTF4 and CTF5 machines, you'll have to run a wider nessus scan.

```
┌──(kali㉿kali)-[~]
└─$ nmap -F 10.161.4.1-254
```

(Remember to replace the highlighted folder number with your actual folder number in the command above.)

The .1 host may currently have ssh open and is your upstream gateway. Do not attack it. The other hosts that have no ports open represent your kali machine and other group members' kali machines. Match the other hosts that remain with the CTF4/CTF5 documentation to determine which is which. For example, CTF 4 has only ports 22, 25, 80, and 631 open, whereas CTF 5 has more open ports.

Running Commands:

The documentation may have you cd into directories that are no longer necessary. For example, the following highlighted directory for httprint does not exist on modern installations:

```
$ cd ~/bin/httprint_301
```

You can then run the program using:

```
$ ./httprint -h 192.168.0.6 -P0 -s signatures.txt
```

Instead, you can just run the command without changing directories or using the "./", like this:

```
httprint -h 192.168.0.6 -P0 -s signatures.txt
```

However, this still might not work, because you don't have that signatures.txt file in your home directory of /home/kali. See the next section on how to find files via the command line.

Finding files:

You may often need to find the location of a file, like signatures.txt for the httprint command, or directory-list-2.3-medium.txt for dirbuster. I recommend using the 'locate' command.

To use the locate command, you have to run this command only one time:

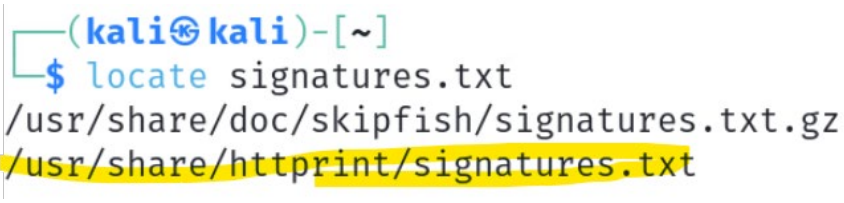
```
sudo updatedb
```

This command updates a system-wide index of where every file is stored.

Next, run the following command to show you where a file is stored.

```
locate <file-you-want-to-find>
```

For example, I'll run locate to find signatures.txt for the httprint command:

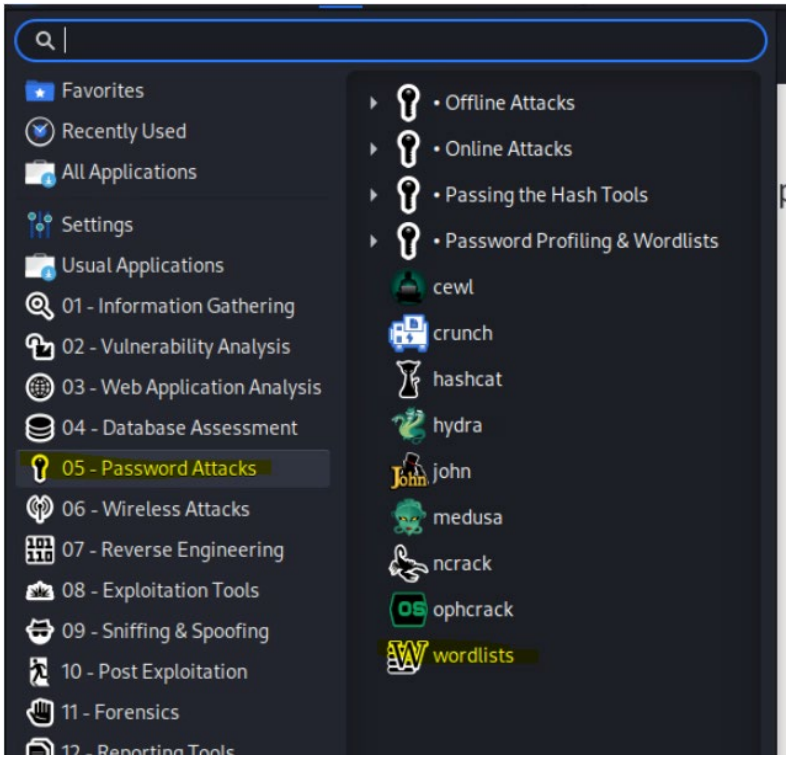


The second result (highlighted) is the one I want. I can then use the cp (copy) command to copy it to my home directory, like this:

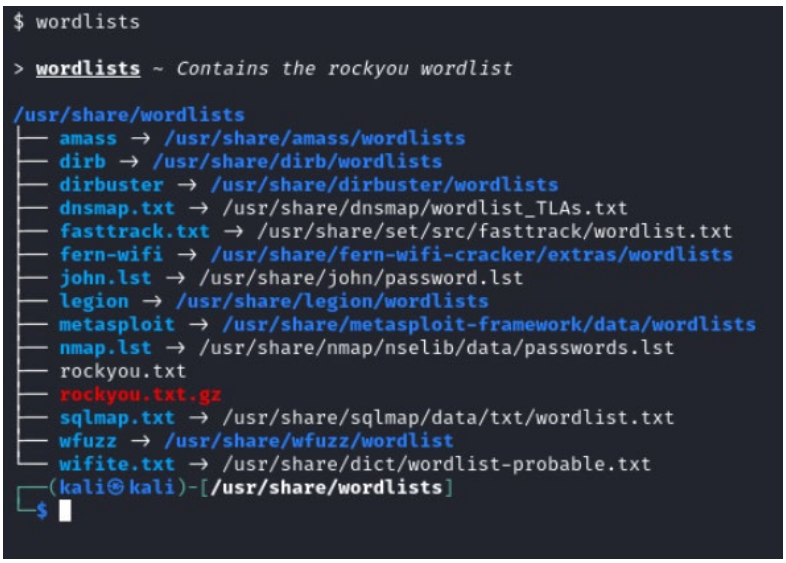
Now signatures.txt should be available in my home directory to use in the httprint command.

Finding good password cracking files:

Sometimes you just need a good file full of passwords. For reasons. Luckily kali comes pre-populated with some good ones. You can find them by going to the start menu, selecting 05-Password Attacks, and clicking on Wordlists:



This will bring up a terminal window showing you the location of some nice files. If this is the first time you run this program, it will also ask you if you want to unzip the rockyou file. Do it!



The rockyou word list is a real cracked list of passwords from an attack a few years ago. The longest password in this file is 255 characters long, and it has **a lot** of passwords. The file is currently located in /usr/share/wordlists/rockyou.txt

You'll find other nice wordlists here, like a wordlist for the password cracking program john and a few dirbuster wordlists.

Other Hints for CTF 4

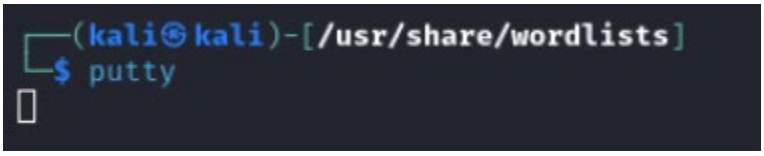
The ssh protocol is very old on CTF4, and you won't be able to connect to it using normal methods from your kali machine. To ssh, use the flags -oKexAlgorithms and -oHostKeyAlgorithms. To figure out how to use these, explore the following page:

https://askubuntu.com/questions/836048/ssh-returns-no-matching-host-key-type-found-their-offer-ssh-dss

When it asks you to install wine to emulate putty, do not do that. Instead, just install putty the normal "ubuntu" way with apt, like this:

apt install putty

You can the run the putty GUI by starting it up on the command line, like this:



Use the putty GUI menu system to upload the key you steal, then connect to the CTF 4 machine using putty instead of command line.

Other hints for CTF 5:

Near the beginning of the walkthrough, you are making a database to hold a rainbow table of hashes to passwords. A fantastic file to use for this is the rockyou.txt file (see password cracking files section). However, when you make a table, the directions ask you to make a table that has a field for passwords that is only 100 characters wide:

```
mysql> create table hash (hash_word varchar(100), hash_hash
```

To later use the rockyou.txt file correctly, change the highlighted value to 300 when you type this command.

On a later page, it asks you to find a password file that no longer exists. For example, you don't have a bin/Brutus directory (see below):

```
[sasattack@localhost ~]$ cd
[sasattack@localhost ~]$ cp bin/Brutus/words.txt .
```

Instead, copy the rockyou.txt password file to your home directory by issuing the following command:

```
cp /usr/share/wordlists/rockyou.txt /home/kali/.
```

Now, when you type the following perl script, replace the highlighted words.txt with rockyou.txt:

```
use Digest::MD5  qw(md5 md5_hex md5_base64);
use DBI;

my $dbh = DBI->connect('DBI:mysql:rainbow', 'root', '') || die "Could
not connect $DBI::errstr";

open (FILE, 'words.txt') || die('Could not open file');
while (<FILE>) {
        my $data;
        chomp($data = $_);
        $data =~ s/\r\n?//g;
        $hash = md5_hex $data;
        $data =~ s/'/''/g;
        my @vals = ($data, $hash);
        my $sth = $dbh->prepare("insert into hash
(hash_word,hash_hash) values (?,?)");
        $sth->execute(@vals) || die "Query failed! $DBI::errstr";
}
close(FILE);
$dbh->disconnect();
```

This will create a nice rainbow table for you.

What do I do?

I can't find mysql

The mariadb-server package installs an open source branch of mysql on your kali machine. Once the package is installed, you do not have to "start" the mysql server. All the following mysql commands will work as they are given in the CTF5 documentation.

The program is too old

If you are working through the CTF4 and CTF5 documentation, you might find some use of applications that are no longer supported. If this happens, I give you permission to use a modern application to do something similar.

How do I split this project 3 ways?

Don't just have one group member do CTF4, another do CTF5, and a third do unscripted vectors. You need to do the walkthrough for at least one machine to understand unscripted vectors. I recommend splitting up the work of CTF4 and CTF 5 into 3, and only then once the walkthroughs are done doing the unscripted vectors.