

Module 19: Cloud Computing

Lab 1: Perform S3 Bucket Enumeration using Various S3 Bucket Enumeration Tools

Lab Scenario

As an ethical hacker, you must try to obtain as much information as possible about the target cloud environment using various enumeration tools. This lab will demonstrate various S3 bucket enumeration tools that can help you in extracting the list of publicly available S3 buckets.

Lab Objectives

- Enumerate S3 buckets using lazys3
- Enumerate S3 buckets using S3Scanner

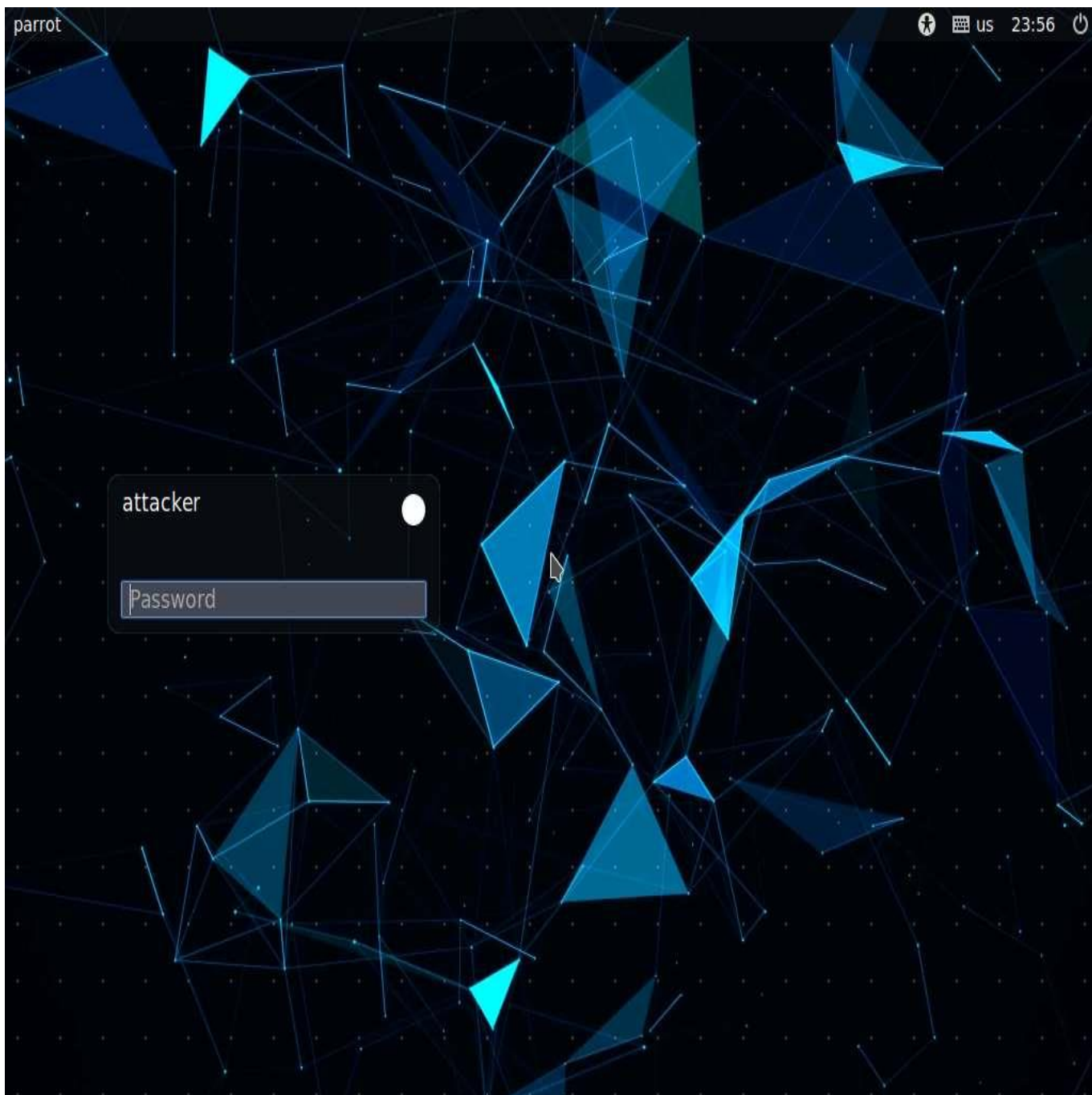
Overview of Enumeration Tools

Enumeration tools are used to collect detailed information about target systems to exploit them. Information collected by S3 enumeration tools consists of a list of misconfigured S3 buckets that are available publicly. Attackers can exploit these buckets to gain unauthorized access to them. Moreover, they can modify, delete, and exfiltrate the bucket content.

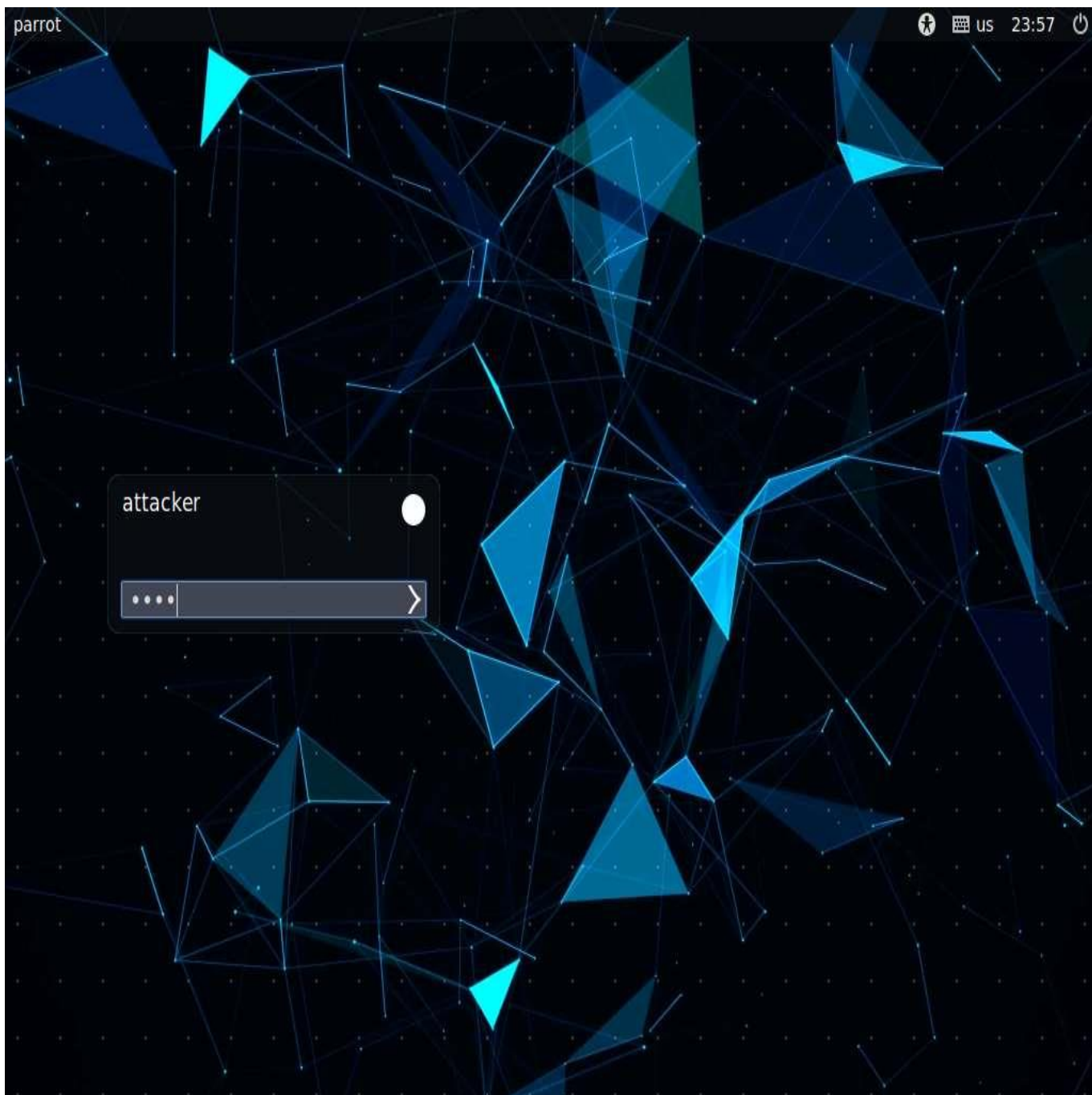
Task 1: Enumerate S3 Buckets using lazys3

lazys3 is a Ruby script tool that is used to brute-force AWS S3 buckets using different permutations. This tool obtains the publicly accessible S3 buckets and also allows you to search the S3 buckets of a specific company by entering the company name.

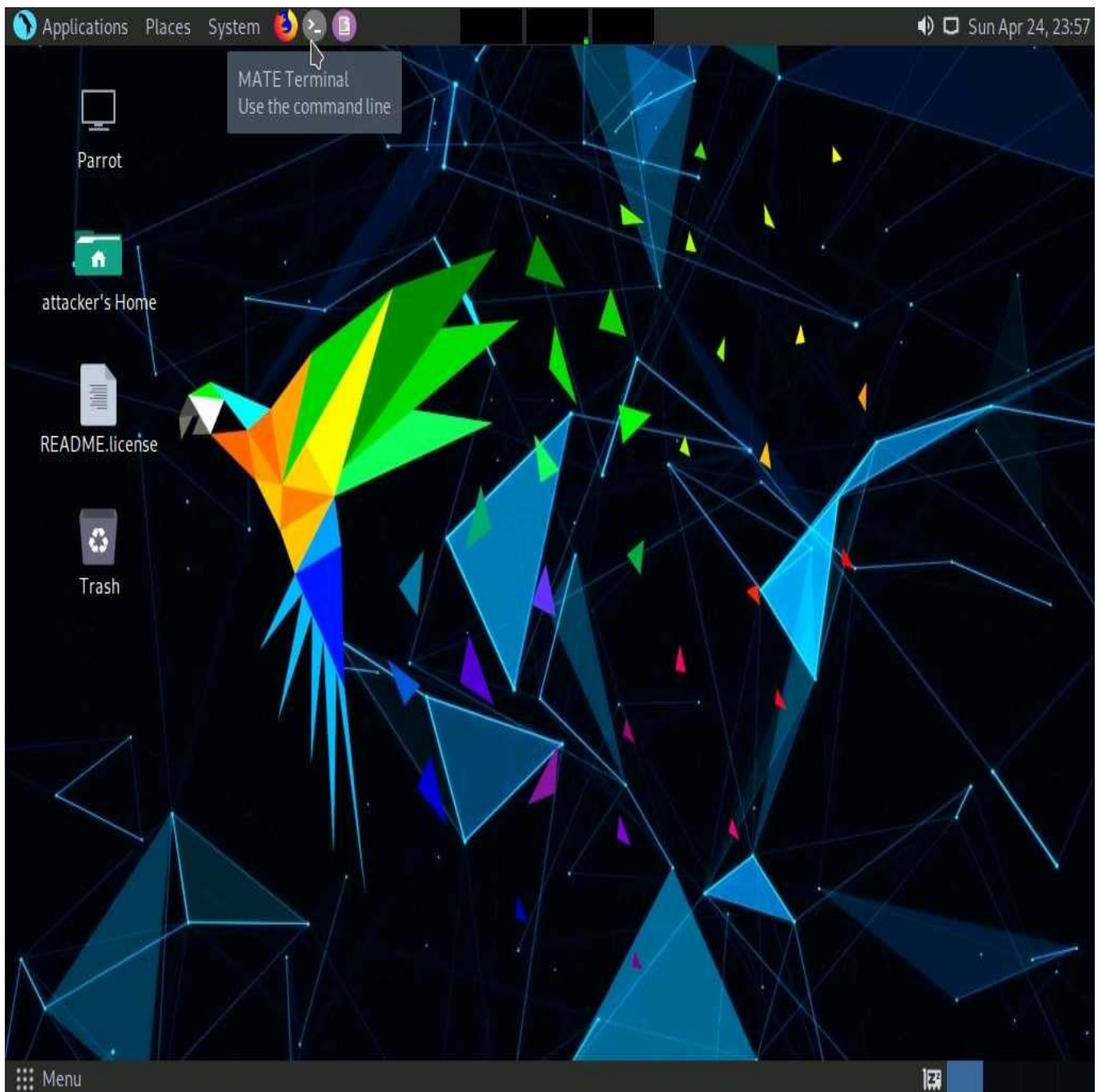
1. ☐ Click [Parrot Security](#) to switch to the **Parrot Security** machine.



2. ☐ In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



3. ☐ Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

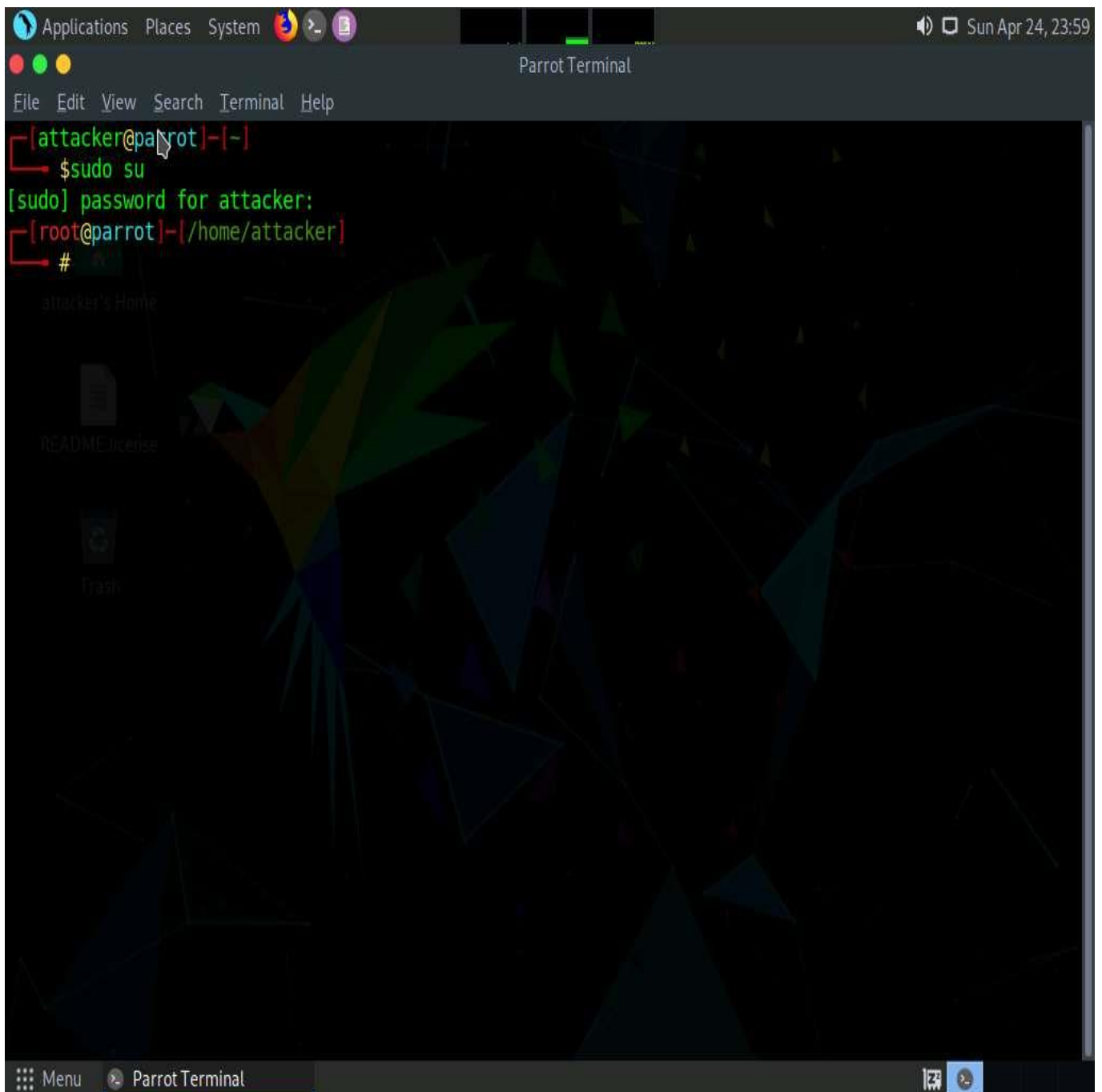


4. ☐ A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

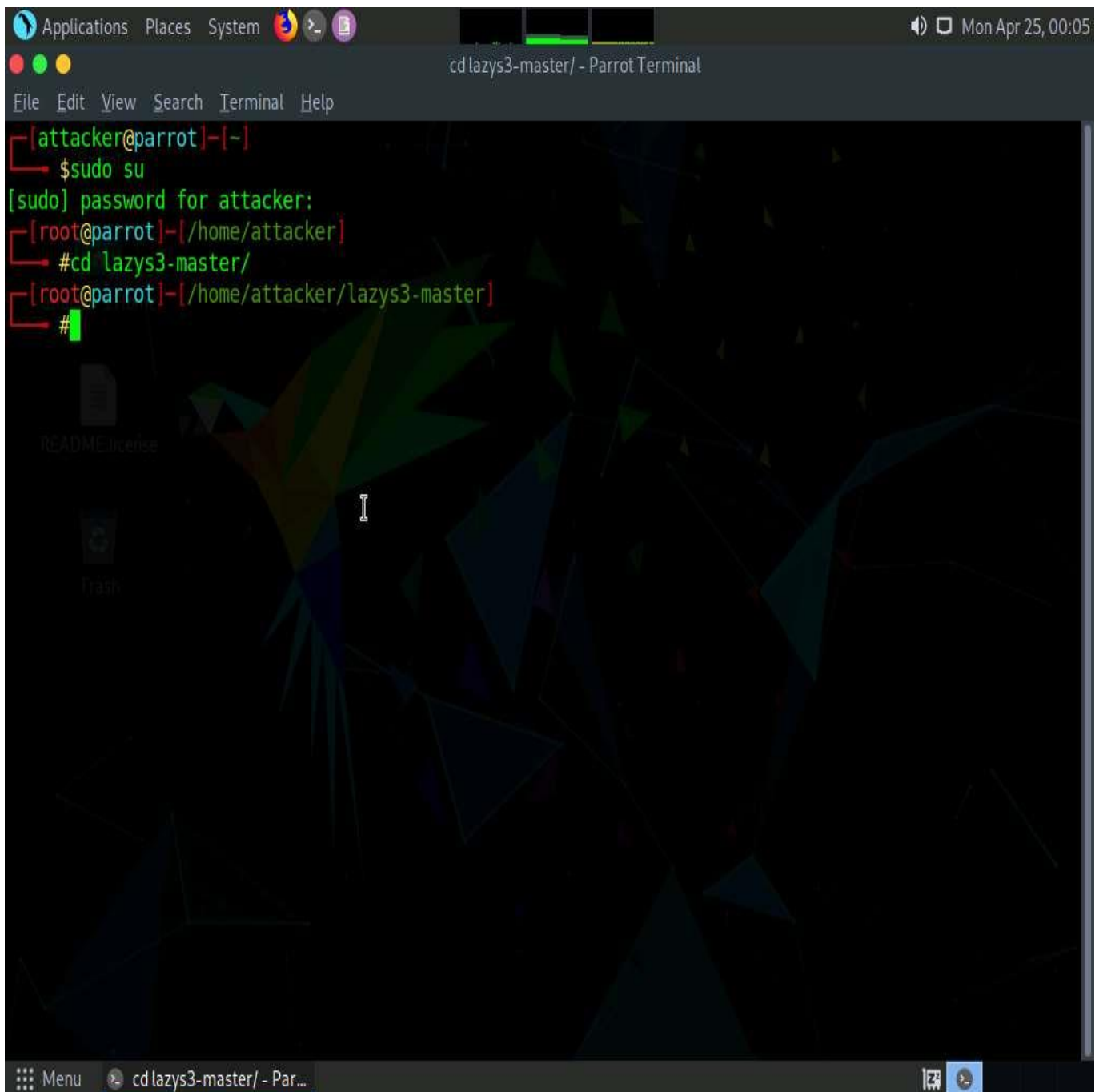
5. ☐ In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

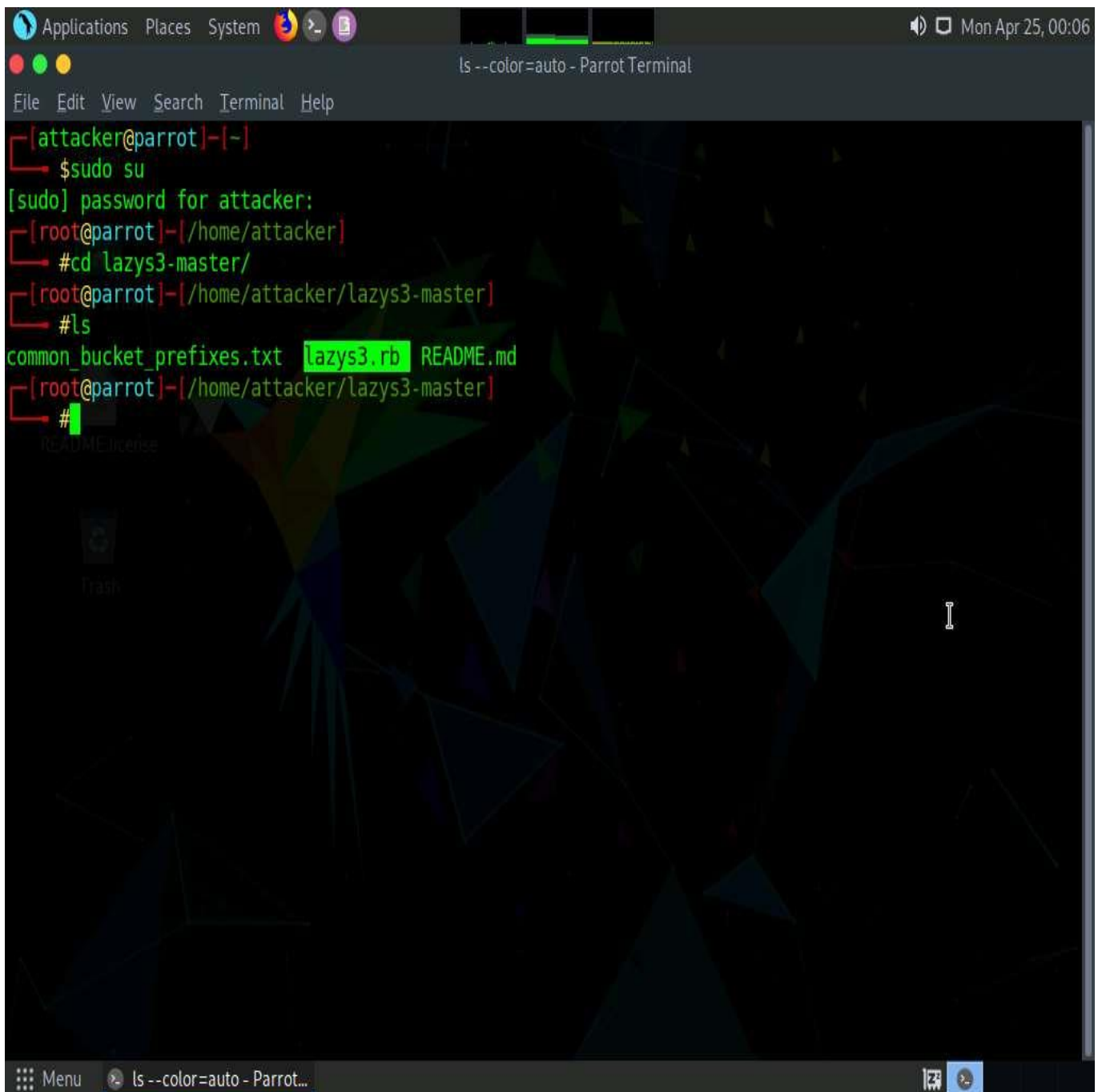


6. ☐ In the terminal window, type **cd lazys3-master/** and press **Enter** to navigate to the cloned repository.

We have already downloaded lazys3 tool in the Lab setup.

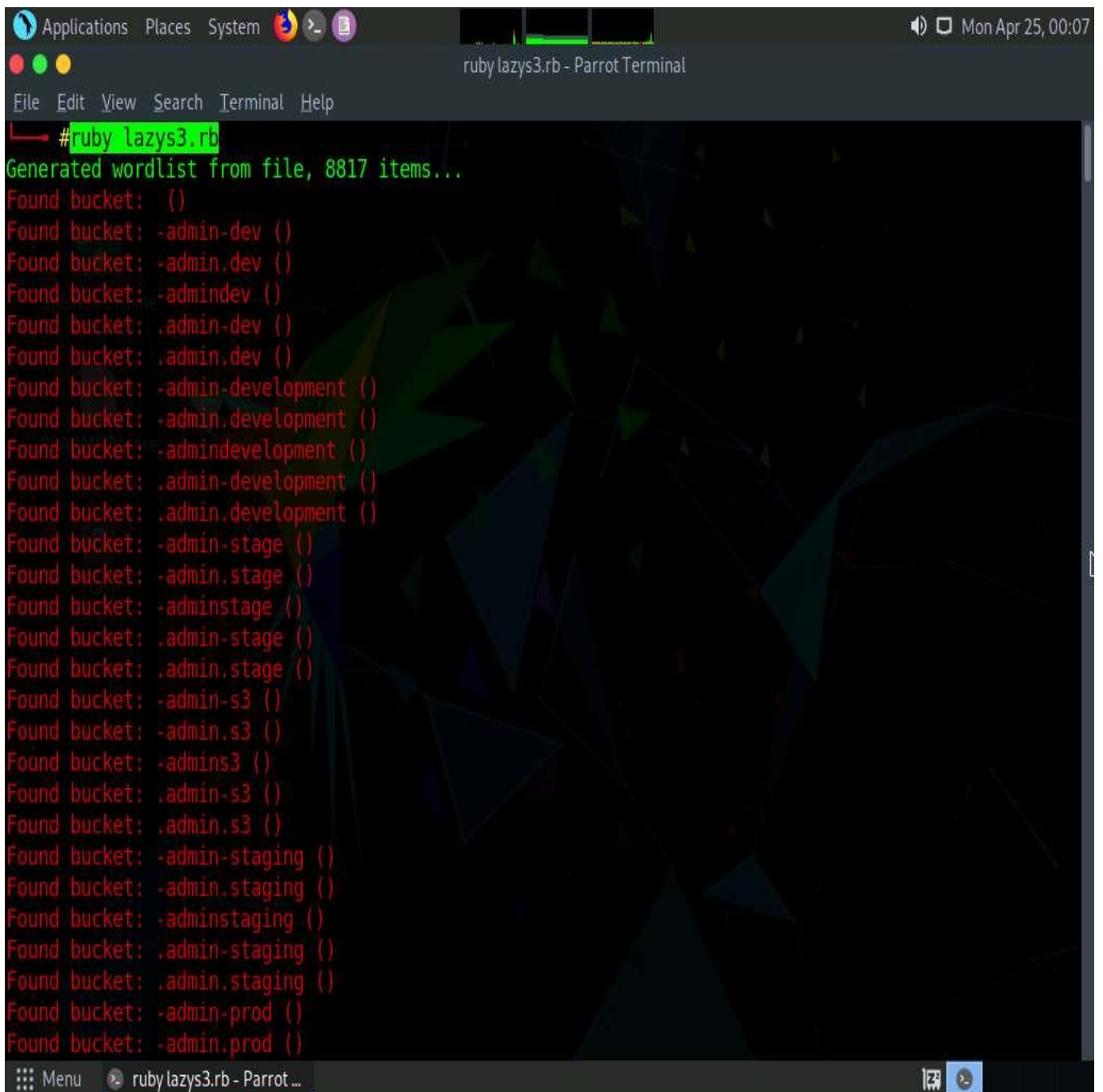


7. ☐ In the lazys3 folder, type **ls** and press **Enter** to list the folder content.
8. ☐ The folder content is displayed; here, we will run the **lazys3.rb** script to find the public S3 buckets.



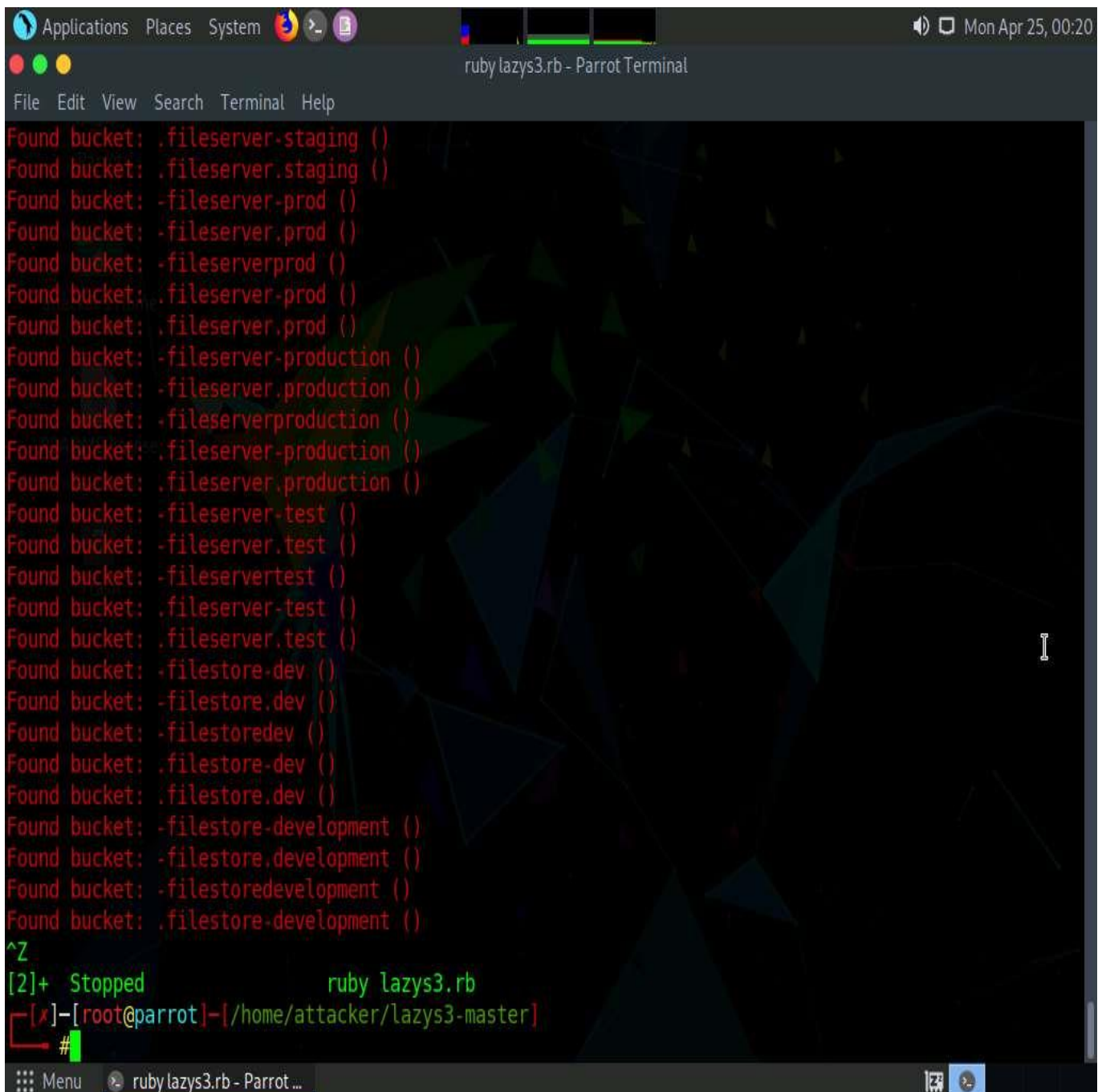
```
[attacker@parrot]~  
$sudo su  
[sudo] password for attacker:  
[root@parrot]~/home/attacker  
#cd lazys3-master/  
[root@parrot]~/home/attacker/lazys3-master  
#ls  
common_bucket_prefixes.txt lazys3.rb README.md  
[root@parrot]~/home/attacker/lazys3-master  
#
```

9. ☐ Now, type **ruby lazys3.rb** and press **Enter**.
10. ☐ A list of public S3 buckets is displayed, as shown in the screenshot.



```
Applications Places System ruby lazys3.rb - Parrot Terminal
File Edit View Search Terminal Help
#ruby lazys3.rb
Generated wordlist from file, 8817 items...
Found bucket: ()
Found bucket: -admin-dev ()
Found bucket: -admin.dev ()
Found bucket: -admindev ()
Found bucket: .admin-dev ()
Found bucket: .admin.dev ()
Found bucket: -admin-development ()
Found bucket: -admin.development ()
Found bucket: -admindevelopment ()
Found bucket: .admin-development ()
Found bucket: .admin.development ()
Found bucket: -admin-stage ()
Found bucket: -admin.stage ()
Found bucket: -adminstage ()
Found bucket: .admin-stage ()
Found bucket: .admin.stage ()
Found bucket: -admin-s3 ()
Found bucket: -admin.s3 ()
Found bucket: -admins3 ()
Found bucket: .admin-s3 ()
Found bucket: .admin.s3 ()
Found bucket: -admin-staging ()
Found bucket: -admin.staging ()
Found bucket: -adminstaging ()
Found bucket: .admin-staging ()
Found bucket: .admin.staging ()
Found bucket: -admin-prod ()
Found bucket: -admin.prod ()
```

11. ☐ Press **Ctrl+Z** to stop the script.



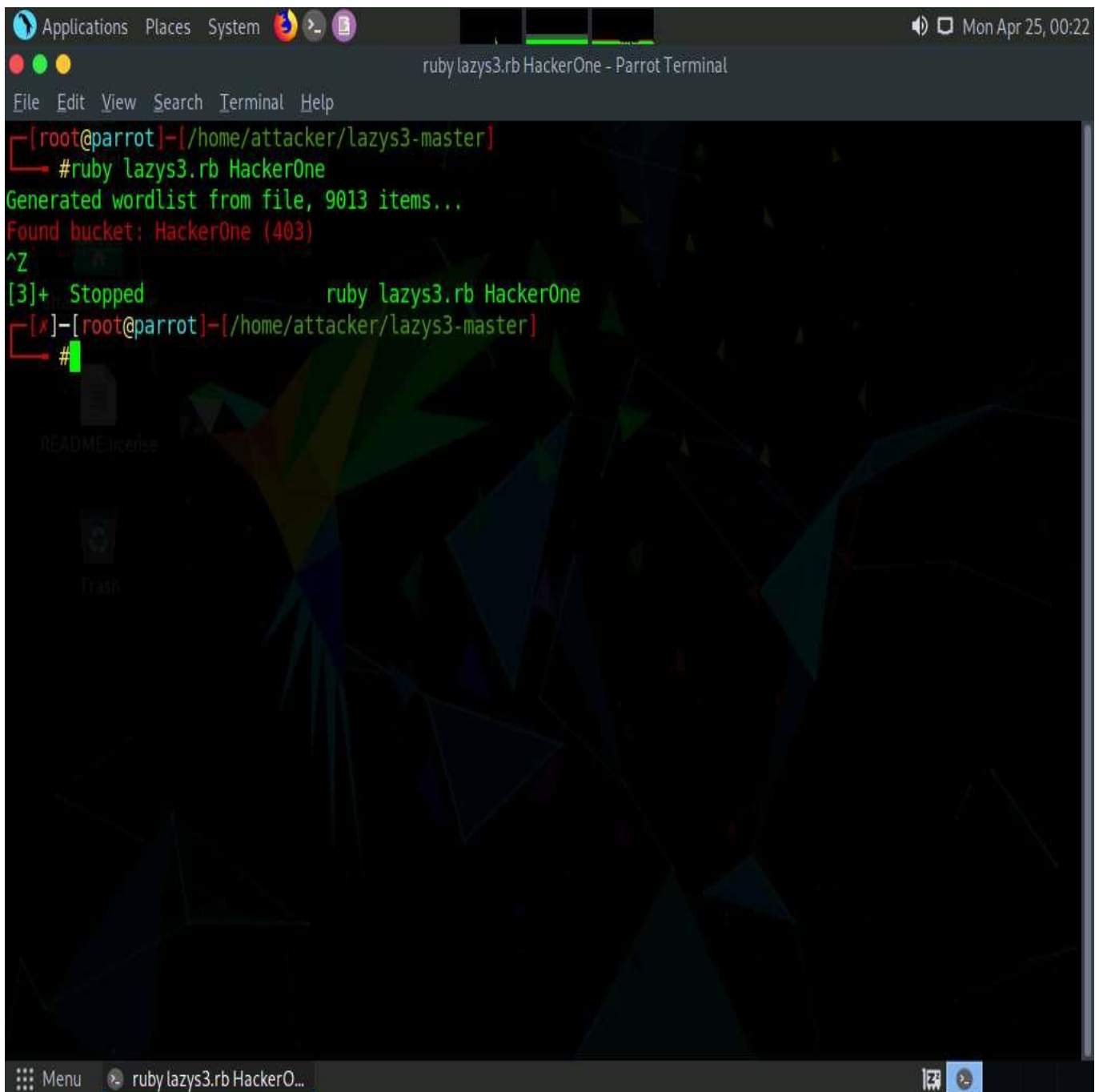
```
Applications Places System ruby lazys3.rb - Parrot Terminal
File Edit View Search Terminal Help
Found bucket: .fileserver-staging ()
Found bucket: .fileserver.staging ()
Found bucket: -fileserver-prod ()
Found bucket: -fileserver.prod ()
Found bucket: -fileserverprod ()
Found bucket: .fileserver-prod ()
Found bucket: .fileserver.prod ()
Found bucket: -fileserver-production ()
Found bucket: -fileserver.production ()
Found bucket: -fileserverproduction ()
Found bucket: .fileserver-production ()
Found bucket: .fileserver.production ()
Found bucket: -fileserver-test ()
Found bucket: -fileserver.test ()
Found bucket: -fileservertest ()
Found bucket: .fileserver-test ()
Found bucket: .fileserver.test ()
Found bucket: -filestore-dev ()
Found bucket: -filestore.dev ()
Found bucket: -filestoredev ()
Found bucket: .filestore-dev ()
Found bucket: .filestore.dev ()
Found bucket: -filestore-development ()
Found bucket: -filestore.development ()
Found bucket: -filestoredevelopment ()
Found bucket: .filestore-development ()
^Z
[2]+  Stopped                  ruby lazys3.rb
[~]-[root@parrot]-[/home/attacker/lazys3-master]
#
```

12. ☐ **You can search the S3 buckets of specific company.** To do so, type **ruby lazys3.rb [Company]** and press **Enter**.

Here, the target company name is **HackerOne**; you can enter the company name of your choice.

13. ☐ The result appears, showing the obtained list of S3 buckets of the specified company.

It will take some time to obtain a complete list of the available S3 buckets.



```
Applications Places System ruby lazys3.rb HackerOne - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker/lazys3-master]
#ruby lazys3.rb HackerOne
Generated wordlist from file, 9013 items...
Found bucket: HackerOne (403)
^Z
[3]+ Stopped ruby lazys3.rb HackerOne
[~]-[root@parrot]-[/home/attacker/lazys3-master]
#
```

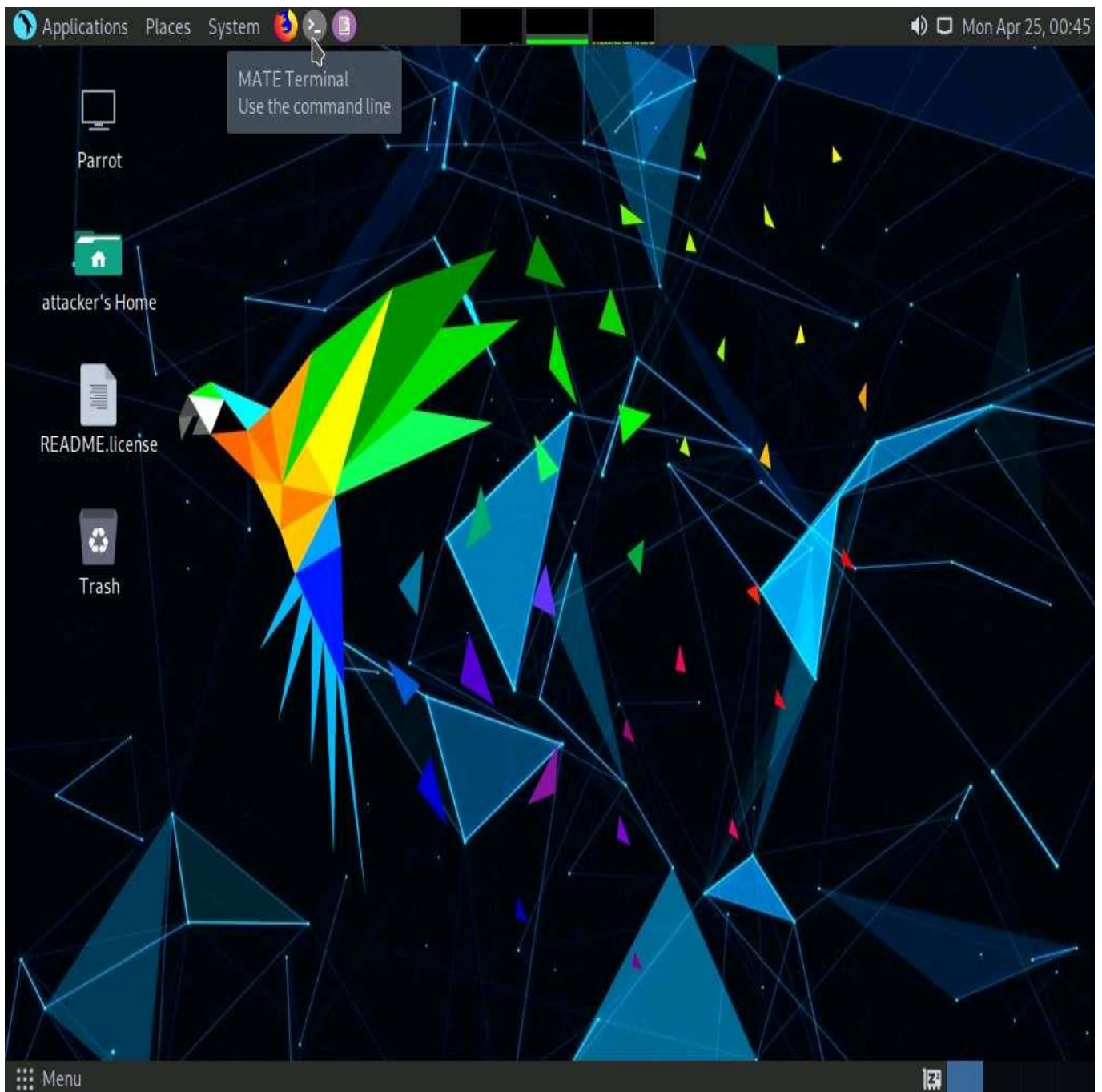
14. ☐ Press **Ctrl+Z** to stop running the script.
15. ☐ This concludes the demonstration of enumerating public S3 buckets.
16. ☐ Close all open windows and document all acquired information.

Task 2: Enumerate S3 Buckets using S3Scanner

S3Scanner is a tool that finds the open S3 buckets and dumps their contents. It takes a list of bucket names to check as its input. The S3 buckets that are found are output to a file. The tool also dumps or lists the contents of "open" buckets locally.

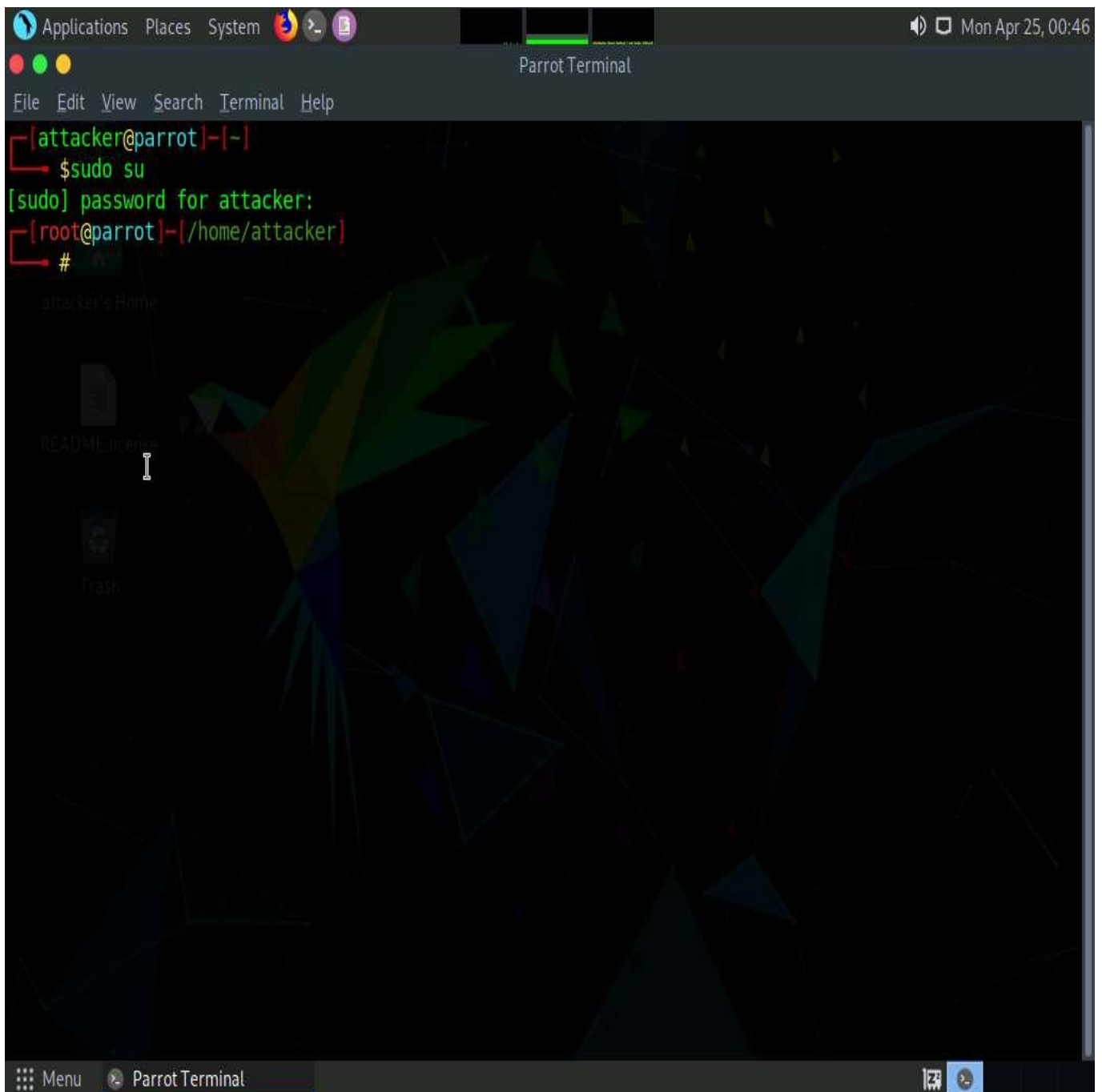
Here, we will use the S3Scanner tool to enumerate open S3 buckets.

1. ☐ Click the **MATE Terminal** icon in the menu to launch the terminal.



2. ☐ A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. ☐ In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

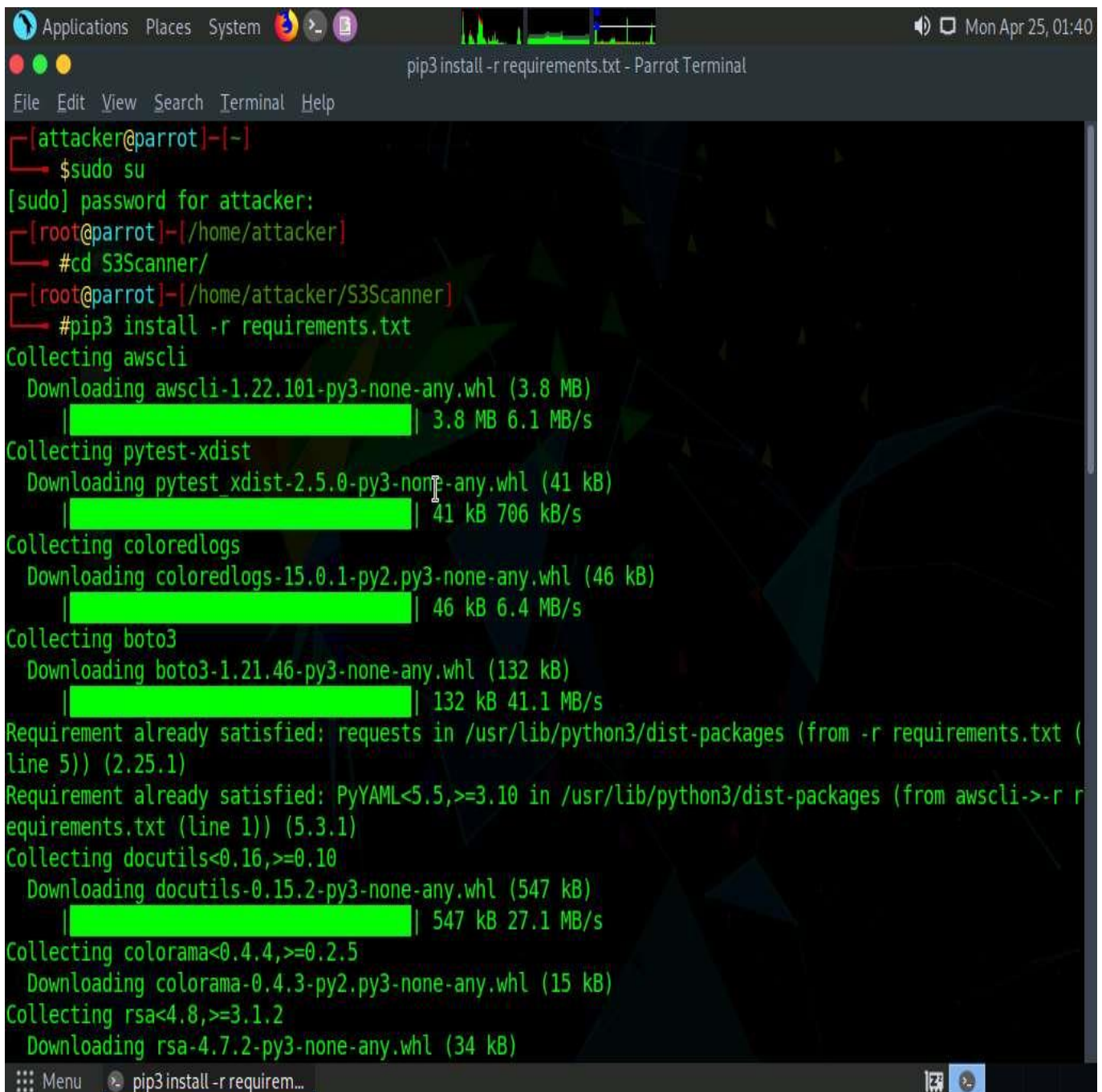
The password that you type will not be visible.



4. ☐ Type **cd S3Scanner/** and press **Enter** to navigate to the cloned repository.

By default, the tool is cloned to the root directory.

5. ☐ In the S3Scanner folder, type **pip3 install -r requirements.txt** and press **Enter** to install the required dependencies.



```
Applications Places System [Icons] [System Monitor] [Network] [Volume] [Mon Apr 25, 01:40]
pip3 install -r requirements.txt - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# cd S3Scanner/
[root@parrot]~/S3Scanner# pip3 install -r requirements.txt
Collecting awscli
  Downloading awscli-1.22.101-py3-none-any.whl (3.8 MB)
    |████████████████████████████████████████| 3.8 MB 6.1 MB/s
Collecting pytest-xdist
  Downloading pytest_xdist-2.5.0-py3-none-any.whl (41 kB)
    |████████████████████████████████████████| 41 kB 706 kB/s
Collecting coloredlogs
  Downloading coloredlogs-15.0.1-py2.py3-none-any.whl (46 kB)
    |████████████████████████████████████████| 46 kB 6.4 MB/s
Collecting boto3
  Downloading boto3-1.21.46-py3-none-any.whl (132 kB)
    |████████████████████████████████████████| 132 kB 41.1 MB/s
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 5)) (2.25.1)
Requirement already satisfied: PyYAML<5.5,>=3.10 in /usr/lib/python3/dist-packages (from awscli->-r requirements.txt (line 1)) (5.3.1)
Collecting docutils<0.16,>=0.10
  Downloading docutils-0.15.2-py3-none-any.whl (547 kB)
    |████████████████████████████████████████| 547 kB 27.1 MB/s
Collecting colorama<0.4.4,>=0.2.5
  Downloading colorama-0.4.3-py2.py3-none-any.whl (15 kB)
Collecting rsa<4.8,>=3.1.2
  Downloading rsa-4.7.2-py3-none-any.whl (34 kB)
```

6. ☐ After the successful installation of the dependencies, in the terminal window, type **python3 ./s3scanner.py sites.txt** and press **Enter** to run the tool.

Here, **sites.txt** is a text file containing the target website URL that is scanned for open S3 buckets. You can edit the **sites.txt** file to enter the target website URL of your choice.

7. ☐ The result appears, displaying a list of public S3 buckets, as shown in the screenshot.

You might encounter the following error: "AWS credentials not configured." Ignore the error, as we will install and configure the AWS CLI in the next lab.


```
python3 ./s3scanner.py sites.txt - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker/S3Scanner]
#python3 ./s3scanner.py sites.txt
2022-04-25 01:42:35 Warning: AWS credentials not configured. Open buckets will be shown as closed.
Run: `aws configure` to fix this.
2022-04-25 01:42:38 [found] : flaws.cloud | 25621 bytes | ACLs: unknown - no aws creds
2022-04-25 01:42:39 [not found] : arstechnica.com
2022-04-25 01:42:42 [found] : lifehacker.com | AccessDenied | ACLs: unknown - no aws creds
2022-04-25 01:42:42 [not found] : gizmodo.com
2022-04-25 01:42:46 [found] : reddit.com | AccessDenied | ACLs: unknown - no aws creds
2022-04-25 01:42:49 [found] : stackoverflow.com | AccessDenied | ACLs: unknown - no aws creds
[root@parrot]-[/home/attacker/S3Scanner]
#
```

8. ☐ Apart from the aforementioned command, you can use the S3Scanner tool to perform the following functions:
- Dump all open buckets and log both open and closed buckets in found.txt:
python3 ./s3scanner.py --include-closed --out-file found.txt --dump names.txt
 - Just log open buckets in the default output file (buckets.txt):
python3 ./s3scanner.py names.txt
 - Save the file listings of all open buckets to a file:
python ./s3scanner.py --list names.txt
9. ☐ This concludes the demonstration of enumerating S3 buckets using the S3Scanner tool.

10. ☐ You can also use other S3 bucket enumeration tools such as **S3Inspector** (<https://github.com>), **s3-buckets-bruteforcer** (<https://github.com>), **Mass3** (<https://github.com>), **Bucket Finder** (<https://digi.ninja>), and **s3recon** (<https://github.com>) to perform S3 bucket enumeration for a target website or company.
11. ☐ Close all open windows and document all acquired information.