Cloud Computing

Cloud computing delivers various types of services and applications over the Internet. These services enable users to use software and hardware managed by third parties at remote locations. Some well-known cloud service providers are Google, Amazon, and Microsoft.

Lab Scenario

Cloud computing is an emerging technology that delivers computing services such as online business applications, online data storage, and webmail over the Internet. Cloud implementation enables a distributed workforce, reduces organization expenses, provides data security, etc. As enterprises are increasingly adopting cloud services, cloud systems have emerged as targets for attackers to gain unauthorized access to the valuable data stored in them. Therefore, it is essential to regularly perform pen testing on cloud systems to monitor their security posture. Security administrators claim that cloud systems are more vulnerable to DoS assaults, because they involves numerous individuals or clients, making DoS assaults potentially very harmful. Because of the high workload on a flooded service, these systems attempt to provide additional computational power (more virtual machines, more service instances) to cope with the workload, and they will eventually fail. Although cloud systems try to thwart attackers by providing additional computational power, they inadvertently aid attackers by allowing the most significant possible damage to the availability of a service—a process that starts from a single flooding-attack entry point. Thus, attackers need not flood all servers that provide a particular service but merely flood a single, cloud-based address to a service that is unavailable. Thus, adequate security is vital in this context, because cloud-computing services are based on sharing. As an ethical hacker and penetration tester, you must have sound knowledge of hacking cloud platforms using various tools and techniques. The labs in this module will provide you with real-time experience in exploiting the underlying vulnerabilities in a target cloud platform using various hacking methods and tools. However, hacking the cloud platform may be illegal depending on the organization's policies and any laws that are in effect. As an ethical or pen tester, you should always acquire proper authorization before performing system hacking.

Cloud computing refers to on-demand delivery of IT capabilities, in which IT infrastructure and applications are provided to subscribers as metered services over a network. Cloud services are classified into three categories, namely infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS), which offer different techniques for developing cloud.

Perform S3 Bucket Enumeration using Various S3 Bucket Enumeration Tools

Ethical hackers and penetration testers are aided in enumeration by various tools that make information gathering an easy task.

Lab Scenario

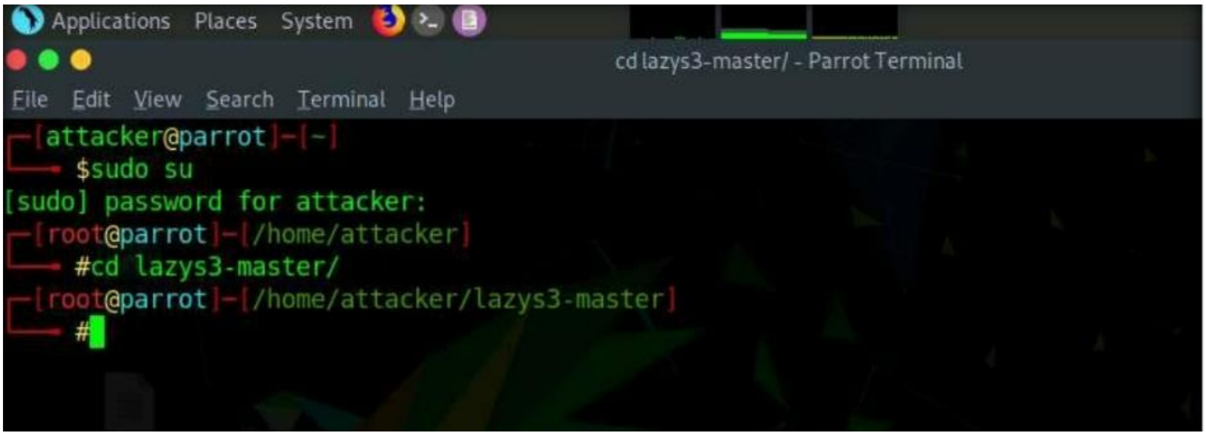
As an ethical hacker, you must try to obtain as much information as possible about the target cloud environment using various enumeration tools. This lab will demonstrate various S3 bucket enumeration tools that can help you in extracting the list of publicly available S3 buckets.

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

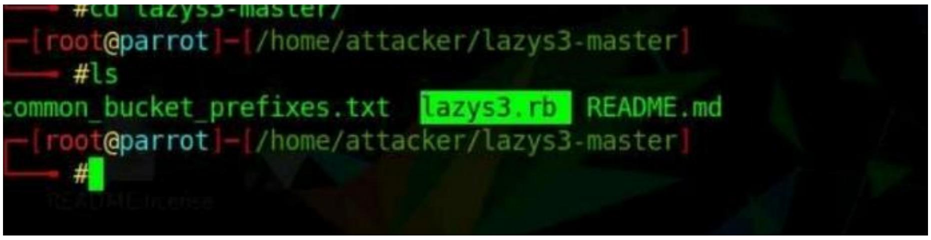
lazys3 is a Ruby script tool that is used to brute-force AWS S3 buckets using different permutations. This tool obtains the publicly accessible S3 buckets and also allows you to search the S3 buckets of a specific company by entering the company name.

In the terminal window, type cd lazys3-master/ and press Enter to navigate to the cloned repository. If not there install it.
https://github.com/nahamsec/lazys3.git


Applications Places System
cd lazys3-master/ - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd lazys3-master/
┌─[root@parrot]─[/home/attacker/lazys3-master]
└──╼ #
```

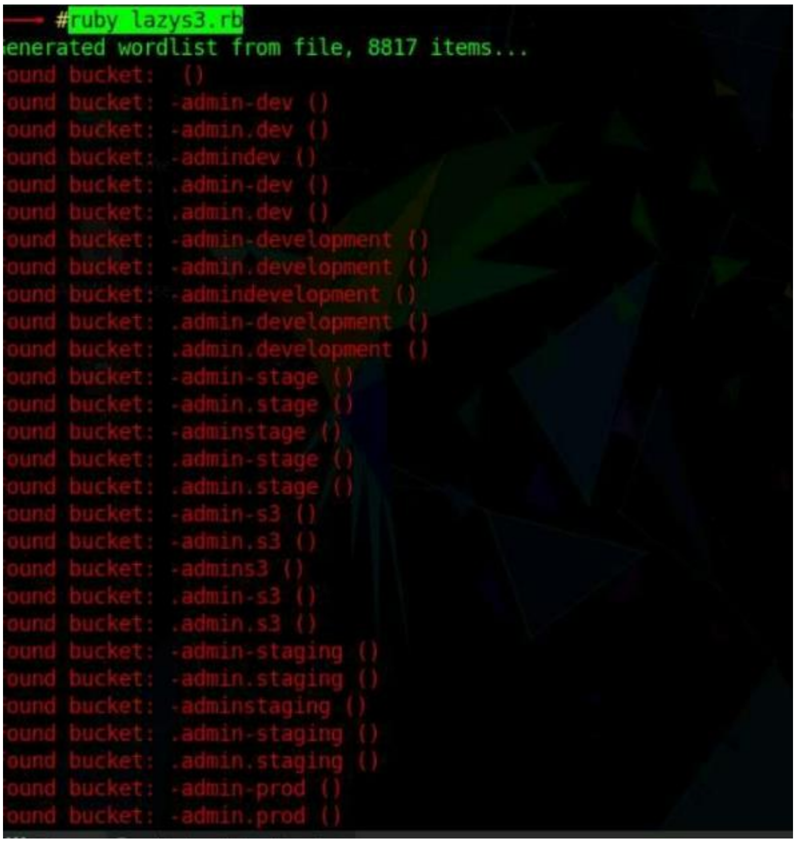
In the lazys3 folder, type ls and press Enter to list the folder content.
The folder content is displayed; here, we will run the lazys3.rb script to find the public S3 buckets.



```
└──╼ #cd lazys3-master/
┌─[root@parrot]─[/home/attacker/lazys3-master]
└──╼ #ls
common_bucket_prefixes.txt  lazys3.rb  README.md
┌─[root@parrot]─[/home/attacker/lazys3-master]
└──╼ #
```

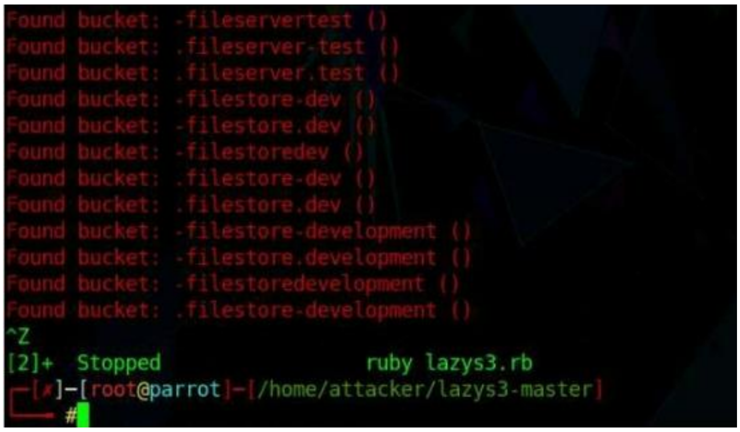
Now, type ruby lazys3.rb and press Enter.

A list of public S3 buckets is displayed, as shown in the screenshot.



```
──╼ #ruby lazys3.rb
enerated wordlist from file, 8817 items...
ound bucket:  ()
ound bucket: -admin-dev ()
ound bucket: -admin.dev ()
ound bucket: -admindev ()
ound bucket: .admin-dev ()
ound bucket: .admin.dev ()
ound bucket: -admin-development ()
ound bucket: -admin.development ()
ound bucket: -admindevelopment ()
ound bucket: .admin-development ()
ound bucket: .admin.development ()
ound bucket: -admin-stage ()
ound bucket: -admin.stage ()
ound bucket: -adminstage ()
ound bucket: .admin-stage ()
ound bucket: .admin.stage ()
ound bucket: -admin-s3 ()
ound bucket: -admin.s3 ()
ound bucket: -admins3 ()
ound bucket: .admin-s3 ()
ound bucket: .admin.s3 ()
ound bucket: -admin-staging ()
ound bucket: -admin.staging ()
ound bucket: -adminstaging ()
ound bucket: .admin-staging ()
ound bucket: .admin.staging ()
ound bucket: -admin-prod ()
ound bucket: -admin.prod ()
```

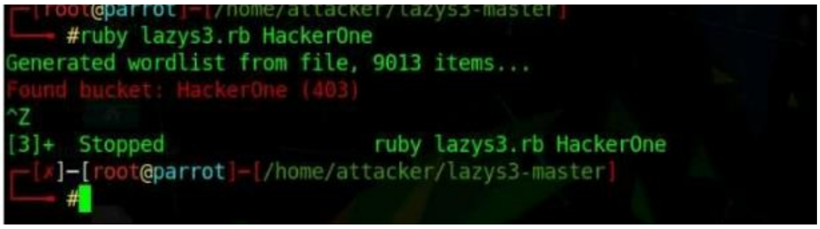
Press Ctrl+Z to stop the script.



```
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]
└──╼ #
```

You can search the S3 buckets of specific company. To do so, type ruby lazys3.rb [Company] and press Enter. Note: Here, the target company name is HackerOne; you can enter the company name of your choice.

The result appears, showing the obtained list of S3 buckets of the specified company. Note: It will take some time to obtain a complete list of the available S3 buckets.



```
┌─[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]
└──╼ #
```

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

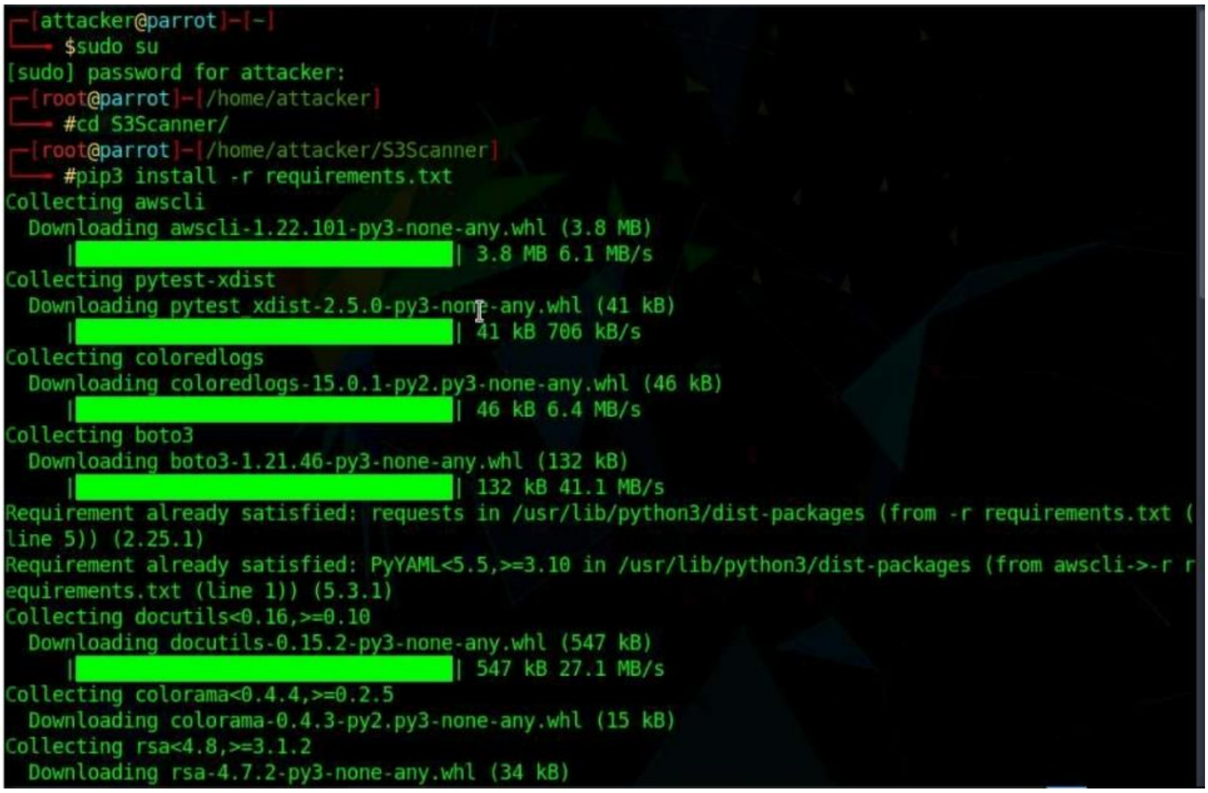
Task 2 : Enumerate S3 Buckets using S3Scanner

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.

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

Note: By default, the tool is cloned to the root directory.
https://github.com/sa7mon/S3Scanner.git

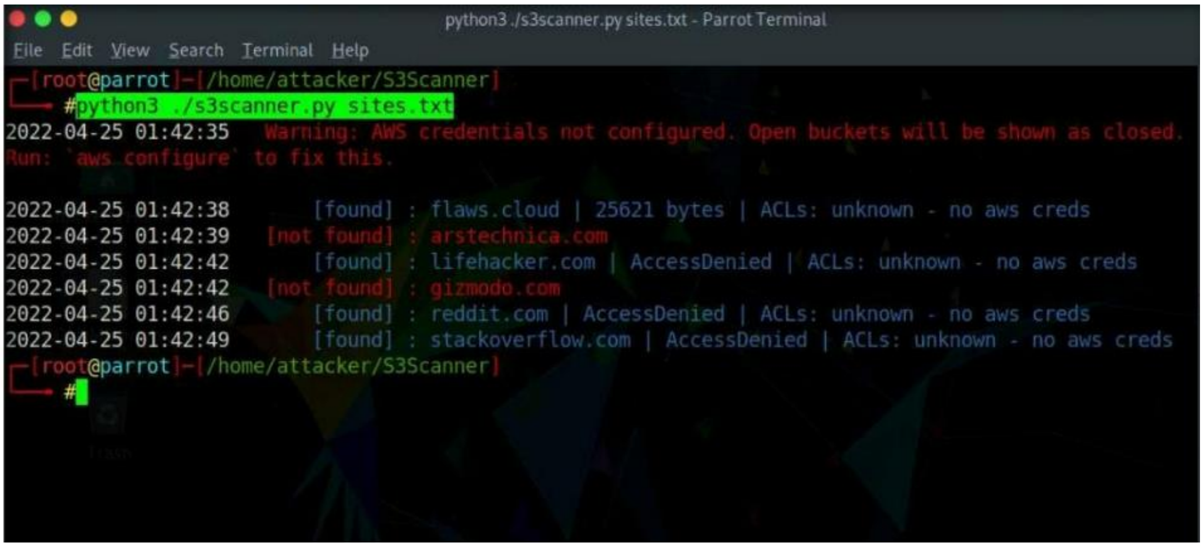
In the S3Scanner folder, type pip3 install -r requirements.txt and press Enter to install the required dependencies.



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd S3Scanner/
┌─[root@parrot]─[/home/attacker/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 r
equirements.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)
```

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

The result appears, displaying a list of public S3 buckets, as shown in the screenshot. Note: 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]
└──╼ #
```

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

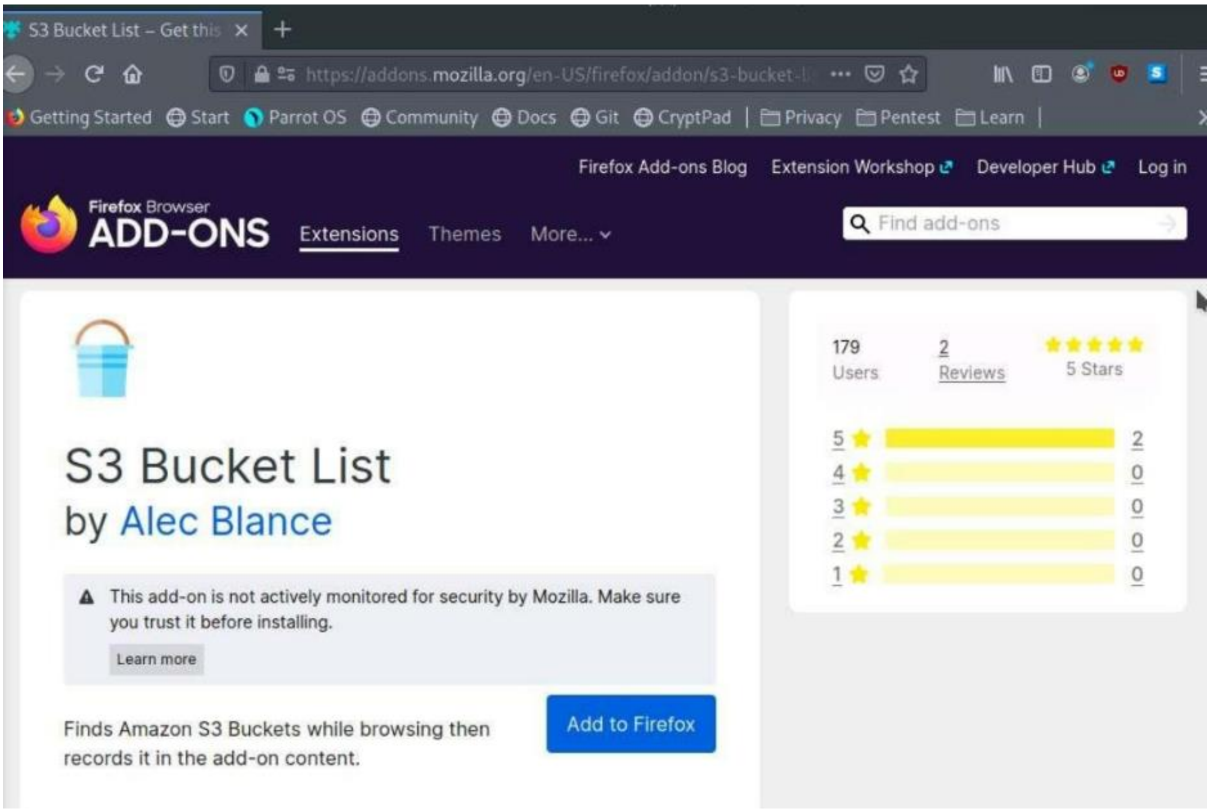
This concludes the demonstration of enumerating S3 buckets using the S3Scanner tool.

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.

Task 3: Enumerate S3 Buckets using Firefox Extension

S3BucketList is a Firefox extension that records S3 buckets found in requests and lists them along with their permissions. Using this tool, we can determine whether an S3 bucket is public or private.
Here, we will use S3BucketList Firefox extension to find S3 buckets from a target website.

In the address bar type https://addons.mozilla.org/en-US/firefox/addon/s3-bucket-list/ and press Enter.



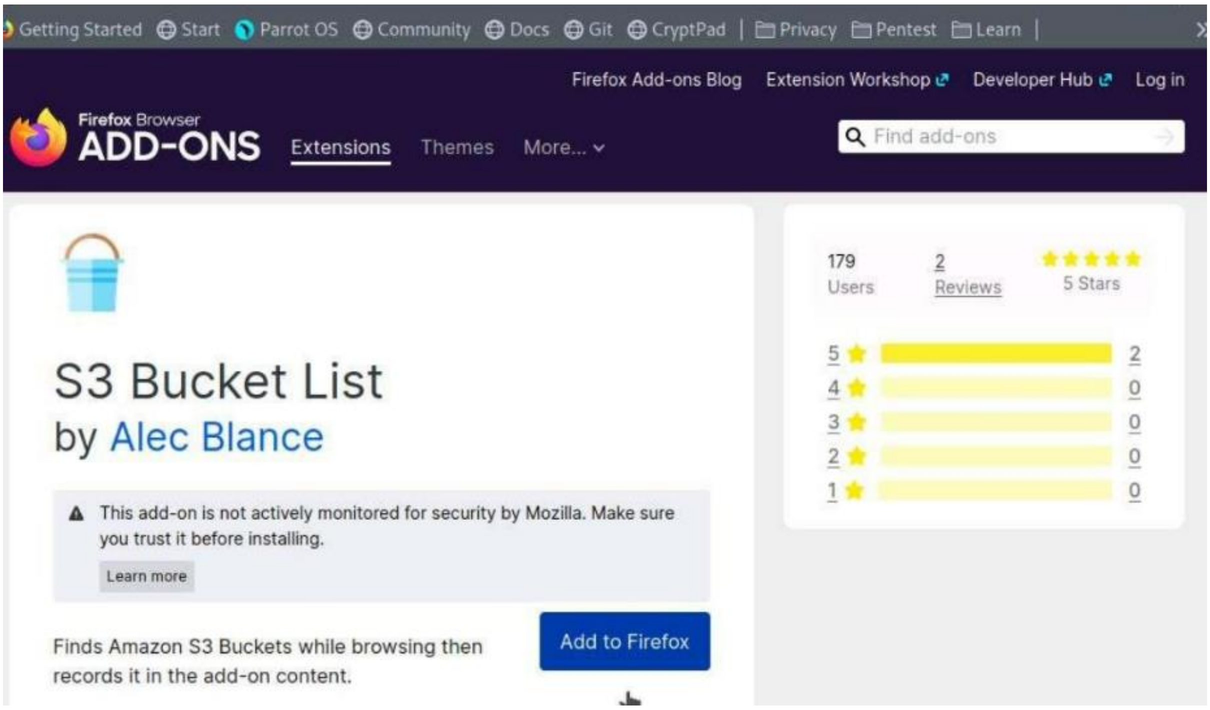
S3 Bucket List

by Alec Blance

This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

Finds Amazon S3 Buckets while browsing then records it in the add-on content.

In the Firefox Browser ADD-ONS page, click on Add to Firefox button.



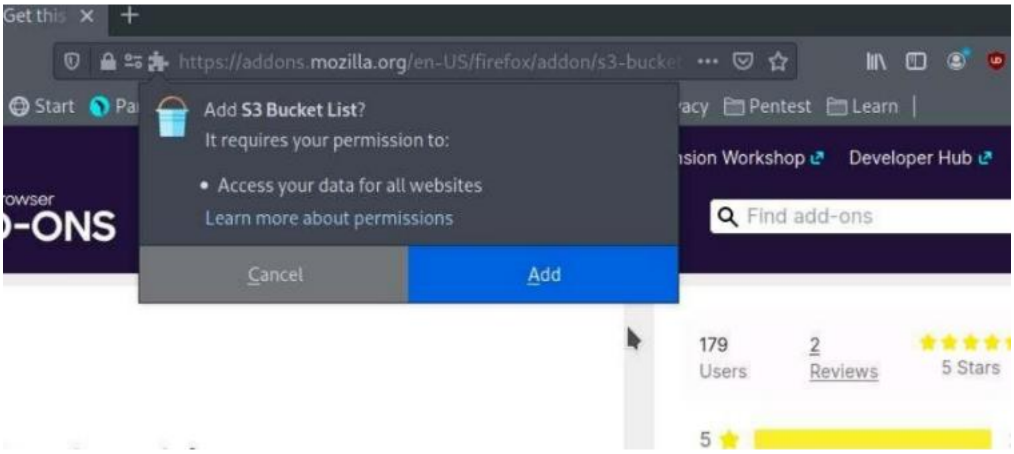
S3 Bucket List

by Alec Blance

This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

Finds Amazon S3 Buckets while browsing then records it in the add-on content.

If Add S3 Bucket List? pop-up appears, click Add button.



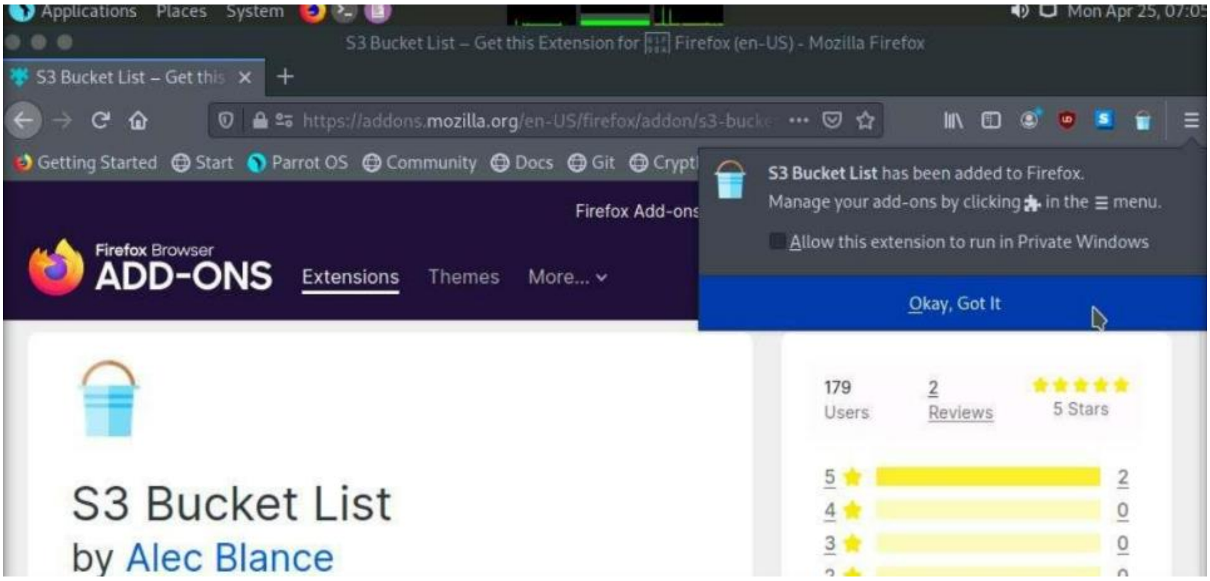
Add S3 Bucket List?

It requires your permission to:

- Access your data for all websites

Learn more about permissions

A S3 Bucket List has been added to Firefox, pop-up appears click Okay, Got It

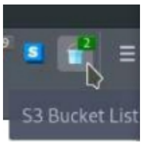


S3 Bucket List has been added to Firefox.
Manage your add-ons by clicking in the ≡ menu.

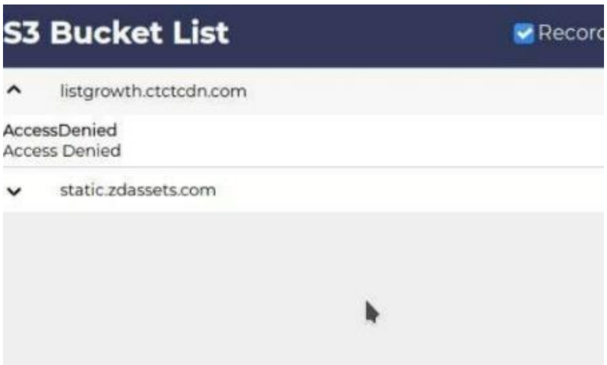
□ Allow this extension to run in Private Windows

Open a new tab in the browser, in the address bar, type any website and press Enter.

Now, click S3 Bucket List icon present on the top-right of the browser window to view the recorded S3 buckets.



You can observe the discovered S3 buckets under S3 Bucket List section, as shown in the screenshot.



S3 Bucket List

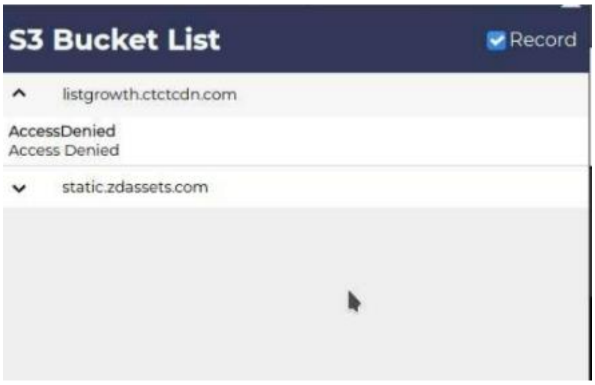
☑ Record

listgrowth.ctctcdn.com

AccessDenied
Access Denied

static.zdassets.com

By selecting an S3 bucket you can check its permissions.



S3 Bucket List

☑ Record

listgrowth.ctctcdn.com

AccessDenied
Access Denied

static.zdassets.com