


```
INFO[0000] Building permutations....
INFO[0000] Processing permutations....
INFO[0002] FORBIDDEN http://[REDACTED]-aaa.s3.amazonaws.com ([REDACTED])
INFO[0002] FORBIDDEN http://[REDACTED]-accounts.s3.amazonaws.com ([REDACTED])
INFO[0003] FORBIDDEN http://[REDACTED]-activity.s3-ap-northeast-1.amazonaws.com/ ([REDACTED])
INFO[0003] FORBIDDEN http://[REDACTED]-ads.s3.amazonaws.com ([REDACTED])
INFO[0004] FORBIDDEN http://[REDACTED]-alerts.s3.amazonaws.com ([REDACTED])
INFO[0004] FORBIDDEN http://[REDACTED]-analytics.s3.amazonaws.com ([REDACTED])
INFO[0005] FORBIDDEN http://[REDACTED]-amp.s3-ap-south-1.amazonaws.com/ ([REDACTED])
INFO[0005] FORBIDDEN http://[REDACTED]-api.s3.amazonaws.com ([REDACTED])
INFO[0006] FORBIDDEN http://[REDACTED]-api-test.s3-ap-northeast-1.amazonaws.com/ ([REDACTED])
INFO[0006] FORBIDDEN http://[REDACTED]-article.s3.amazonaws.com ([REDACTED])
INFO[0006] FORBIDDEN http://[REDACTED]-apps.s3-ap-southeast-2.amazonaws.com/ ([REDACTED])
```

Amazon AWS, amazon s3, Hacking, Hacking Tools, Top News, Vulnerability

# Slurp – Amazon AWS S3 Bucket Enumerator

July 1, 2019, 2:50 PM  349

```
~/Desktop/slurp $ ./slurp keyword -p permutations.json -t [REDACTED] -c 25
INFO[0000] Building permutations....
INFO[0000] Processing permutations....
INFO[0002] FORBIDDEN http://[REDACTED]-aaa.s3.amazonaws.com ([REDACTED])
INFO[0002] FORBIDDEN http://[REDACTED]-accounts.s3.amazonaws.com ([REDACTED])
INFO[0003] FORBIDDEN http://[REDACTED]-activity.s3-ap-northeast-1.amazonaws.com/ ([REDACTED])
INFO[0003] FORBIDDEN http://[REDACTED]-ads.s3.amazonaws.com ([REDACTED])
INFO[0004] FORBIDDEN http://[REDACTED]-alerts.s3.amazonaws.com ([REDACTED])
INFO[0004] FORBIDDEN http://[REDACTED]-analytics.s3.amazonaws.com ([REDACTED])
INFO[0005] FORBIDDEN http://[REDACTED]-amp.s3-ap-south-1.amazonaws.com/ ([REDACTED])
INFO[0005] FORBIDDEN http://[REDACTED]-api.s3.amazonaws.com ([REDACTED])
INFO[0006] FORBIDDEN http://[REDACTED]-api-test.s3-ap-northeast-1.amazonaws.com/ ([REDACTED])
INFO[0006] FORBIDDEN http://[REDACTED]-article.s3.amazonaws.com ([REDACTED])
INFO[0006] FORBIDDEN http://[REDACTED]-apps.s3-ap-southeast-2.amazonaws.com/ ([REDACTED])
INFO[0007] FORBIDDEN http://[REDACTED]-archive.s3-eu-west-1.amazonaws.com/ ([REDACTED])
INFO[0009] PUBLIC http://[REDACTED]-auth.s3-eu-west-1.amazonaws.com/ ([REDACTED])
INFO[0009] FORBIDDEN http://[REDACTED]-authorization.s3-ap-northeast-2.amazonaws.com/ ([REDACTED])
INFO[0009] FORBIDDEN http://[REDACTED]-authorize.s3-ap-northeast-2.amazonaws.com/ ([REDACTED])
INFO[0009] FORBIDDEN http://[REDACTED]-authentication.s3-ap-southeast-2.amazonaws.com/ ([REDACTED])
```

Slurp is a blackbox/whitebox S3 bucket enumerator written in Go that can use a permutations list to scan from an external perspective or an AWS API to scan internally.



There are two modes that this tool operates at; blackbox and whitebox mode. Whitebox mode (or internal) is significantly faster than blackbox (external) mode.

### Blackbox (external)

In this mode, you are using the permutations list to conduct scans. It will return false positives and there is **NO WAY** to link the buckets to an actual AWS account.

### Whitebox (internal)

In this mode, you are using the AWS API with credentials on a specific account that you own to see what is open. This method pulls all S3 buckets and checks Policy/ACL permissions. Your credentials should be in `~/ .aws/credentials`.

## Slurp – Amazon AWS S3 Bucket Enumerator Features

The main features of Slurp are:

- Scan via domain(s); you can target a single domain or a list of domains
- Scan via keyword(s); you can target a single keyword or a list of keywords
- Scan via AWS credentials; you can target your own AWS account to see which buckets have been exposed
- Colorized output for visual grep
- Currently generates over 28,000 permutations per domain and keyword
- Punycode support for internationalized domains

## Usage of Slurp S3 Bucket Enumerator

Will enumerate the S3 domains for a specific target:

```
<br />
slurp domain <-t|-
target> example.com
```

\_\_\_\_\_

slurp domain <-t -target> example.com
---------------------------------------

Will enumerate S3 buckets based on those 3 key words (linux, golang & python):

```
<br />
slurp keyword <-t|-
target>
linux,golang,python
```

\_\_\_\_\_

slurp keyword <-t --target> linux,golang,python
---

Will perform an internal scan using the AWS API:

<br />  
slurp internal



slurp internal
----------------

You can download Slurp here:

[slurp.tar.gz](https://github.com/0x00sec/slurp/releases/download/v1.0.0/slurp.tar.gz)

Or you can read more [here](#).

Source : [DarkNet](#)



[#Amazon AWS](#) [#amazon s3](#) [#dark net](#) [#Hacking Tools](#) [#Top Story](#)

PREVIOUS ARTICLE

## US GOVERNMENT CYBER SECURITY STILL INADEQUATE

NEXT ARTICLE

## MOSCA – MANUAL STATIC ANALYSIS TOOL TO FIND BUGS

Type and hit enter to search ...

---

### Recent Posts

[The Computer Hut Acquires iTechs of Jonesboro](#)

October 16, 2019

[DeTTecT – Detect Tactics, Techniques & Combat Threats](#)

October 15, 2019

## [What is the Future of Cybersecurity?](#)

October 15, 2019

---

## [Why Use a Content Delivery Network \(CDN\)?](#)

October 15, 2019

---

## [TheTick – A simple embedded Linux backdoor](#)

October 14, 2019

---

## [CATPHISH – Phishing and Corporate Espionage](#)

October 14, 2019

---

## [Wireless LAN Market Foresight By 2025 | Key Companies- Huawei, TP-Link, Cisco](#)

October 14, 2019

---

## [eConnect to Showcase Its Facial Recognition Engine at G2E 2019](#)

October 14, 2019

---

## [Singaporean Unlawful Mining Indicted in the United States](#)

October 12, 2019

---

## [Patches for Internet Explorer Zero-Day Causing Problems for Many Users](#)

October 12, 2019





## Subscribe to PHI via Email

Enter your email address to subscribe to PHI and receive notifications of new posts by email.

Join 3,550 other subscribers

Email Address

---

SUBSCRIBE >

### PROFESSIONAL HACKERS INDIA

We are proud to offer premier information security updates, IT updates, Core Tools And Techniques across the globe. Our mission is to make the internet more secure, more trendy, more aware and more reliable.

### POPULAR TOPICS

[About Us](#)

[Submit Article/News](#)

[Advertise With Us](#)

[Privacy Policy](#)

[Contact Us](#)

### REGISTERED AND PROTECTED

All Rights Reserved.



All latest updates on our

[Disclaimer](#)

RSS Feed:

