Cloud Open Source Intelligence Gathering

Introduction

This section covers the different OSINT techniques that can be employed to find information about particular AWS services and the tools that can use the information obtained to chain other attacks.

This chapter will primarily cover

- Tools and techniques for Open Source Intelligence Gathering to find information

Techniques for OSINT

Introduction

With the varied number of services that Amazon AWS provides, there is bound to be information floating around the Internet that can leak company asset information in the form of IP addresses, hostnames, S3 bucket names, open ports and services, leaked keys and secrets, and accidentally exposed snapshots/backup.

There are several techniques that can be used to find and isolate information to plan for attacks. Open Source Intelligence Gathering (OSINT) is the art of collecting information using various open-source sources that can be used to weaponize and plan for attacks.

What are we going to cover?

This chapter covers various open-source techniques that can be used to perform OSINT on cloud targets.

OSINT Techniques

AWS IP Address Ranges

Amazon Web Services (AWS) publishes its current IP address ranges in JSON format. To view the current ranges, download the .json file. Multiple revisions of this file can be downloaded and maintained for version control.

Download the JSON file from the Amazon website

- wget https://ip-ranges.amazonaws.com/ip-ranges.json

The jq tool can be used to query the JSON

- sudo apt-get install jq

You can get the file creation date for example using

- jq .createDate < ip-ranges.json

Getting information for a specific region

- jq '.prefixes[] | select(.region=="us-east-1")' < ip-ranges.json

Get all IP addresses from the file

- jq -r '.prefixes | .[].ip_prefix' < ip-ranges.json

Obtaining IP information

Online services that can provide IP and host information and historical DNS data.

- https://viewdns.info/
- https://securitytrails.com/

Shodan

Shodan is a search engine for Internet-connected devices. Advanced search queries may need a (free) account.

Note of caution: Do not browse to the targets that the search engine throws up.

We can use Shodan to search for various assets that belong to the AWS IP ranges for example

- https://www.shodan.io/
- https://www.shodan.io/search?query=net%3A%2234.227.211.0%2F24%22

Censys

Censys is another search engine that is used to search through the Internet's public-facing data.

- https://censys.io/
- https://censys.io/ipv4?q=s3

Google dorks

Google advanced search queries can be used to find information about AWS assets and other resources.

The entire list of advanced search operators can be found at

- https://www.google.com/advanced_search

For finding specific AWS EC2 and RDS instance names that leak on the Internet, we can use the following operators (this is a subset of the many available)

Note of caution: Do not click on any of the following search results.

- site:*.amazonaws.com -www "compute"
- site:*.amazonaws.com -www "compute" "ap-south-1"

The following search phrase can be used to find people leaking their RDS endpoint names on the Internet. You can follow search results from the following search:

- site:pastebin.com "rds.amazonaws.com" "u " pass OR password

Sites like HackerOne which run bug bounty programs have some AWS related reports made public. These reports often contain information about AWS assets and resources

Try this as an example

- site:hackerone.com inurl:reports -support.hackerone.com "AWS" "s3"

Additional references

- AWS IP Ranges documentation
- Shodan Help
- Shodan for Penetration Testers

Tools for finding public buckets

Introduction

Due to the common mistakes that administrators and AWS users do, a lot of buckets get exposed to the Internet. In recent years, a lot of data has been revealed through open S3 buckets ranging from employee contracts, software code base, sensitive information like network diagram to usernames and passwords etc.

There are several tools to find and dump the contents of public buckets.

What are we going to cover?

This chapter covers some popular tools that can be used find public buckets and dump data from within if required.

AWS Buckets

The following is a list of valid S3 bucketnames on EC2

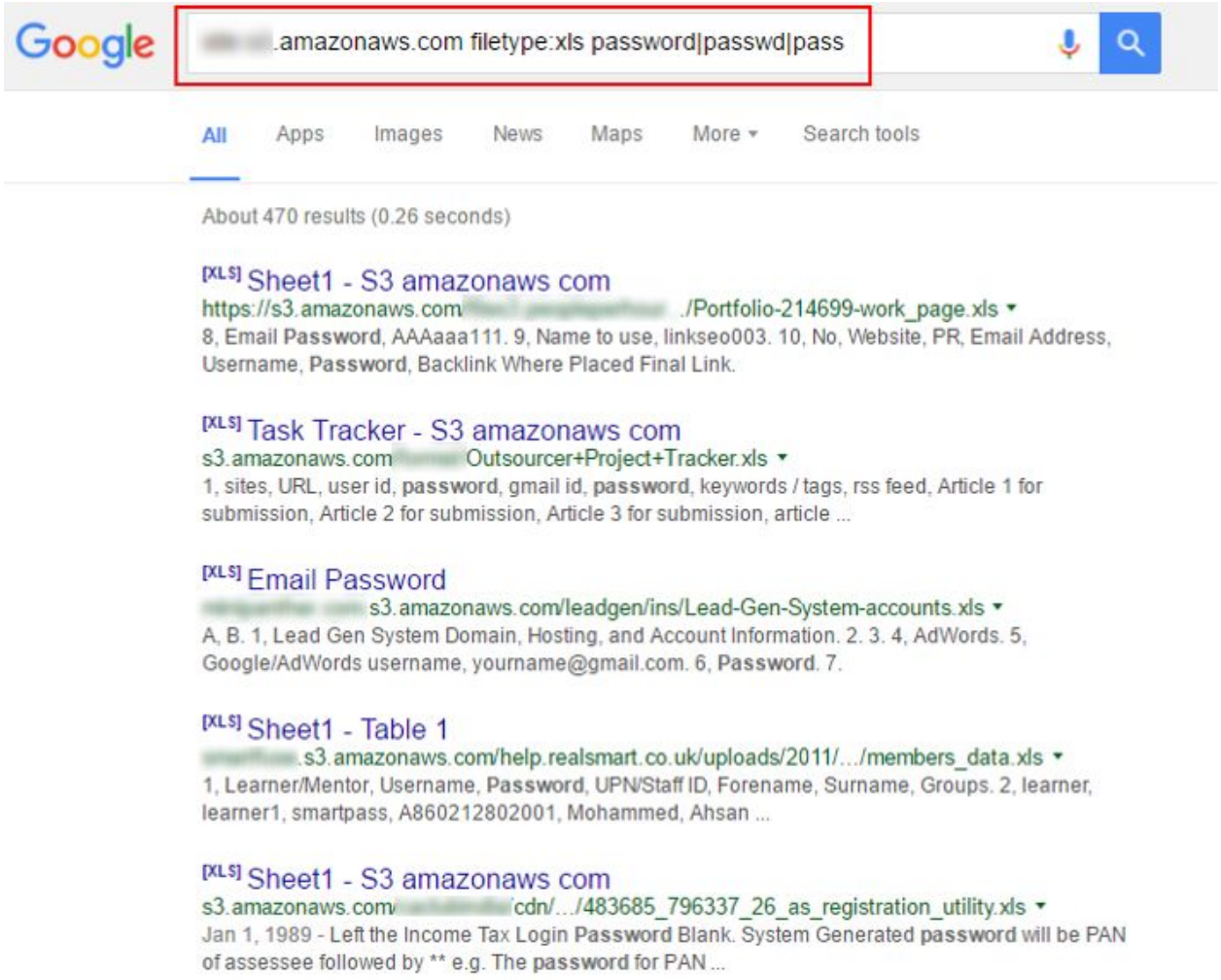
1. https://bucketname.s3.eu-west-1.amazonaws.com/file.txt
2. https://s3-eu-west-1.amazonaws.com/bucketname/file.txt
3. https://bucketname.s3.amazonaws.com/file.txt
4. https://s3.amazonaws.com/bucketname/file.txt

Google dorking

Google is an extremely powerful search engine that can be used to find specific resources on the Internet

For example, the following dork can be used to find S3 buckets containing excel sheets which in turn contain potential passwords

site:*.s3.amazonaws.com ext:xls | ext:xlsx | ext:csv password|passwd|pass user|username|uid|email



Other keywords can also be used to find other information

Practice Exercise: DigiNinja Bucket Finder

Bucket finder is a ruby script that was written to work with discovering buckets with a provided dictionary.

bucket_finder ~/tools/AWSBucketDump/BucketNames.txt -l results.txt

If you want to download the contents of the discovered buckets then specify -d to enable file downloads

bucket_finder -d ~/tools/AWSBucketDump/BucketNames.txt -l results-download.txt

Additional references

- Bucket finder - DigiNinja
- Enumerate S3 buckets via certstream
- Bucket Stream
- Misconfigured bucket to system calls