Cloud Resources

The use of cloud, such as AWS, GCP, Azure, and others, is now one of the essential components for many companies nowadays. After all, all companies want to be able to do their work from anywhere, so they need a central point for all management. This is why services from `Amazon (AWS)`, `Google (GCP)`, and `Microsoft (Azure)` are ideal for this purpose.

Even though cloud providers secure their infrastructure centrally, this does not mean that companies are free from vulnerabilities. The configurations made by the administrators may nevertheless make the company's cloud resources vulnerable. This often starts with the `S3 buckets` (AWS), `blobs` (Azure), `cloud storage` (GCP), which can be accessed without authentication if configured incorrectly.

Company Hosted Servers

Company Hosted Servers

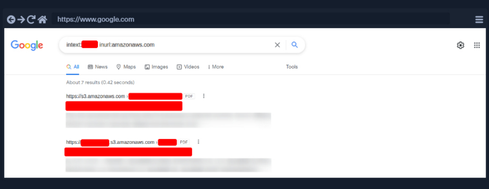
```
Govardhan Gujji22@htb[/htb]$ for i in $(cat subdomainlist);do host $i | grep "has address" | grep inlanef

blog.inlanefreight.com 10.129.24.93
inlanefreight.com 10.129.27.33
matomo.inlanefreight.com 10.129.127.22
www.inlanefreight.com 10.129.127.33
s3-website-us-west-2.amazonaws.com 10.129.95.250
```

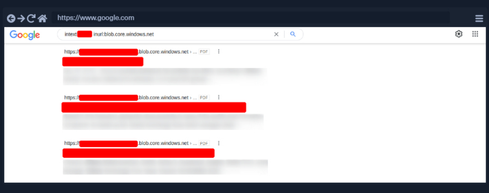
Often cloud storage is added to the DNS list when used for administrative purposes by other employees. This step makes it much easier for the employees to reach and manage them. Let us stay with the case that a company has contracted us, and during the IP lookup, we have already seen that one IP address belongs to the `s3-website-us-west-2.amazonaws.com` server.

However, there are many different ways to find such cloud storage. One of the easiest and most used is Google search combined with Google Dorks. For example, we can use the Google Dorks `inurl:` and `intext:` to narrow our search to specific terms. In the following example, we see red censored areas containing the company name.

Google Search for AWS



Google Search for Azure



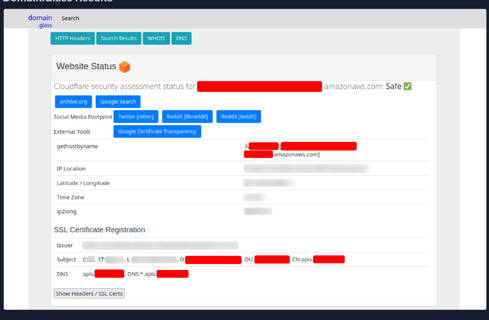
Here we can already see that the links presented by Google contain PDFs. When we search for a company that we may already know or want to know, we will also come across other files such as text documents, presentations, codes, and many others.

Such content is also often included in the source code of the web pages, from where the images, JavaScript codes, or CSS are loaded. This procedure often relieves the web server and does not store unnecessary content.

Target Website - Source Code

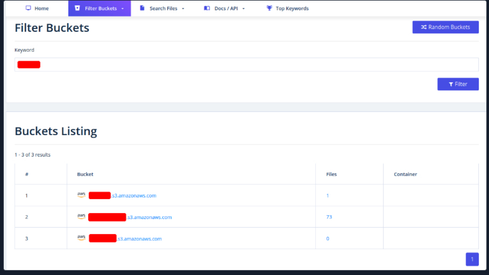
Third-party providers such as domain.glass can also tell us a lot about the company's infrastructure. As a positive side effect, we can also see that Cloudflare's security assessment status has been classified as "Safe". This means we have already found a security measure that can be noted for the second layer (gateway).

Domain.Glass Results



Another very useful provider is GrayHatWarfare. We can do many different searches, discover AWS, Azure, and GCP cloud storage, and even sort and filter by file format. Therefore, once we have found them through Google, we can also search for them on GrayHatWarefare and passively discover what files are stored on the given cloud storage.

GrayHatWarfare Results

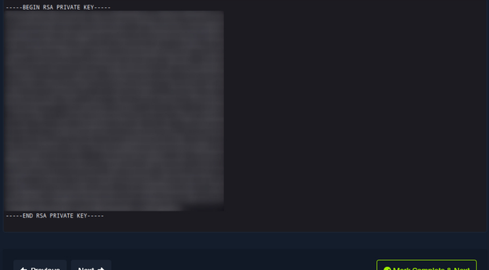


Many companies also use abbreviations of the company name, which are then used accordingly within the IT infrastructure. Such terms are also part of an excellent approach to discovering new cloud storage from the company. We can also search for files simultaneously to see the files that can be accessed at the same time.

Private and Public SSH Keys Leaked

Sometimes when employees are overworked or under high pressure, mistakes can be fatal for the entire company. These errors can even lead to SSH private keys being leaked, which anyone can download and log onto one or even more machines in the company without using a password.

SSH Private Key



Cheat Sheet
Resources

Table of Contents

Introduction
Enumeration Principles
Enumeration Methodology

Infrastructure Based Enumeration
Domain Information
Cloud Resources
Staff

Host Based Enumeration
FTP
SMB
NFS
DNS
SMTP
IMAP / POP3
SNMP
MySQL
MSSQL
IPMI

Remote Management Protocols
Linux Remote Management Protocols
Windows Remote Management Protocols

Skills Assessment
Footprinting Lab - Easy
Footprinting Lab - Medium
Footprinting Lab - Hard

My Workstation
OFFLINE
Start Instance
0/1 / 1 spawns left

Previous
Next
Mark Complete & Next