S3 Bucket Enumeration Report

# 1. Introduction

This report details an enumeration task on publicly accessible Amazon S3 buckets using the LazyS3 tool. The goal of this process is to discover exposed or misconfigured storage buckets associated with a specific domain. This is a common part of cloud security assessments.

# 2. Tool Used: LazyS3

LazyS3 is a Ruby-based tool that attempts to brute-force Amazon S3 bucket names using common naming conventions and wordlists. The tool checks for the existence of buckets related to the target domain.

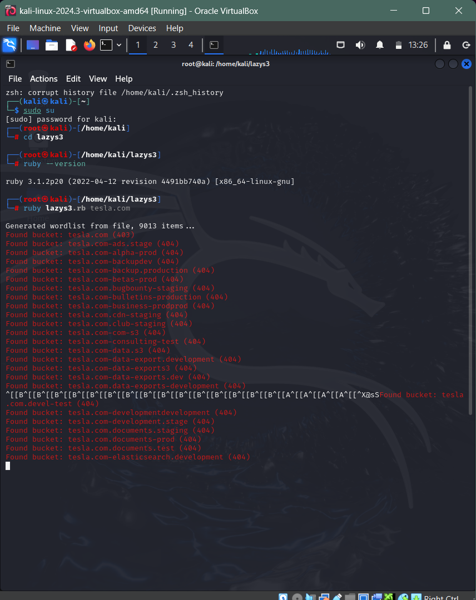
Installation and Usage:

* 1. Clone the repository: `git clone https://github.com/nahamsec/lazys3.git`
* 2. Navigate to the directory: `cd lazys3`
* 3. Run the tool: `ruby lazys3.rb <target-domain>`

# 3. Enumeration Results

The target domain for this test was `tesla.com`. The LazyS3 tool was executed and identified several potential buckets. Most returned 403 (Forbidden) or 404 (Not Found) errors, indicating that they exist or are inaccessible, but do not allow anonymous access.

# 4. Evidence (Screenshots)

**

# 5. Recommendations

To avoid unintentional exposure of S3 buckets, it is recommended that organizations:

* 1. Disable public access unless absolutely necessary.
* 2. Use bucket policies and IAM roles to tightly control access.
* 3. Regularly audit bucket permissions and configurations.
* 4. Use tools like AWS Config to monitor changes to S3 access settings.