Anatomy of a Cloud Hack

Manish Rohilla: Principal Security Consultant

claranet cyber security

Claranet Cyber Security brings you
NotSoSecure
Training

Who’s this guy?

Manish Rohilla

- Principal Security Consultant @ NotSoSecure
- Specialize in Web, Infra and Cloud pen testing
- Blackhat and Corporate Trainer
- Certifications: OSCP and AWS-SSC
- @manishrhll

Claranet Cyber Security brings you
NotSoSecure
Training

Why am I here?

- Data breaches involving cloud-based infrastructure have become increasingly common
- We will provide a brief overview of several recent breaches
- Following that, we'll analyze the different attacks, scenarios, and vulnerabilities that contributed to these breaches
- This analysis is not exhaustive but highlights some noteworthy issues

case studies

Claranet Cyber Security brings you

NotSoSecure Training

Claranet Cyber Security brings you

NotSoSecure Training

Leaking Secrets!!

- 4x increase in hardcoded secret in last 4 years.
- In 2023, 12.8M secrets were detected → 28% increase from 2022.
- 18% of the keys belong to the Cloud service providers.
- 90% of exposed valid secrets remain active for at least five day.
- New Attack Vector: Open AI API keys → 1212x increase in 2023

Reference: https://www.gitguardian.com/files/the-state-of-secrets-sprawl-report-2024

Microsoft AI Researchers Data Leaked

- 38TB of sensitive data leaked.
- Due to Misconfigured Shared Access Signature (SAS) token.
- Allowed unrestricted public access to an Azure Storage account.
- Type of data: Private Keys, Secrets and MS Teams messages.
- Permissions Available on SAS Token: Read, Delete and Modify

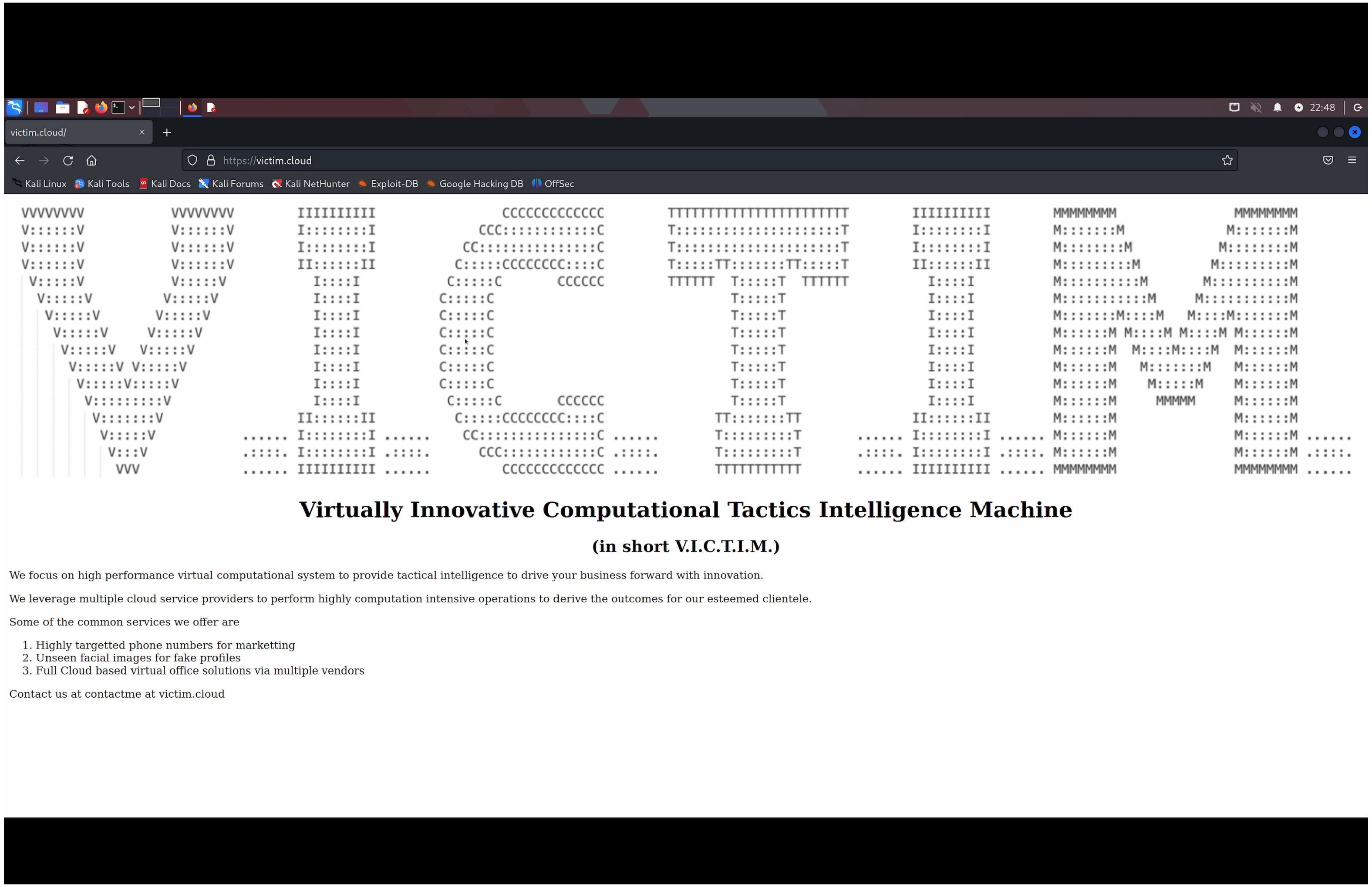
Reference: https://www.wiz.io/blog/38-terabytes-of-private-data-accidentally-exposed-by-microsoft-ai-researchers

Microsoft Blob Storage Misconfiguration

- SOC Radar scans for misconfigured buckets, storage, apps, etc.
- Found an Azure Blob Storage which was accidentally left public.
- Misconfigured storage belongs to the Microsoft cloud service provider
- Storage containing Microsoft's client data
- 2.4TB data with 65k entities, 133k project files and 548k users and many more.
- Data Includes: SOW Documents, Invoices, Signed Customer Documents, etc.

Reference: https://socradar.io/details-on-the-largest-b2b-leak-bluebleed/

Demo: Misconfigured SAS URL



```
VVVVVVVV           VVVVVVVV        IIIIIIIIII                CCCCCCCCCCCCC        TTTTTTTTTTTTTTTTTTTTTTT        IIIIIIIIII        MMMMMMMM               MMMMMMMM
V::::::V           V::::::V        I::::::::I             CCC::::::::::::C        T:::::::::::::::::::::T        I::::::::I        M:::::::M             M:::::::M
V::::::V           V::::::V        I::::::::I           CC:::::::::::::::C        T:::::::::::::::::::::T        I::::::::I        M::::::::M           M::::::::M
V::::::V           V::::::V        II::::::II          C:::::CCCCCCCC::::C        T:::::TT:::::::TT:::::T        II::::::II        M:::::::::M         M:::::::::M
 V:::::V           V:::::V           I::::I           C:::::C       CCCCCC        TTTTTT  T:::::T  TTTTTT          I::::I          M::::::::::M       M::::::::::M
  V:::::V         V:::::V            I::::I          C:::::C                              T:::::T                  I::::I          M:::::::::::M     M:::::::::::M
   V:::::V       V:::::V             I::::I          C:::::C                              T:::::T                  I::::I          M:::::::M::::M   M::::M:::::::M
    V:::::V     V:::::V              I::::I          C:::::C                              T:::::T                  I::::I          M::::::M M::::M M::::M M::::::M
     V:::::V   V:::::V               I::::I          C:::::C                              T:::::T                  I::::I          M::::::M  M::::M::::M  M::::::M
      V:::::V V:::::V                I::::I          C:::::C                              T:::::T                  I::::I          M::::::M   M:::::::M   M::::::M
       V:::::V:::::V                 I::::I          C:::::C                              T:::::T                  I::::I          M::::::M    M:::::M    M::::::M
        V:::::::::V                  I::::I           C:::::C       CCCCCC                T:::::T                  I::::I          M::::::M     MMMMM     M::::::M
         V:::::::V                 II::::::II          C:::::CCCCCCCC::::C              TT:::::::TT              II::::::II        M::::::M               M::::::M
          V:::::V           ...... I::::::::I ......    CC:::::::::::::::C ......       T:::::::::T       ...... I::::::::I ...... M::::::M               M::::::M ......
           V:::V            .::::. I::::::::I .::::.      CCC::::::::::::C .::::.       T:::::::::T       .::::. I::::::::I .::::. M::::::M               M::::::M .::::.
            VVV             ...... IIIIIIIIII ......         CCCCCCCCCCCCC ......       TTTTTTTTTTT       ...... IIIIIIIIII ...... MMMMMMMM               MMMMMMMM ......
```

Virtually Innovative Computational Tactics Intelligence Machine

(in short V.I.C.T.I.M.)

We focus on high performance virtual computational system to provide tactical intelligence to drive your business forward with innovation.

We leverage multiple cloud service providers to perform highly computation intensive operations to derive the outcomes for our esteemed clientele.

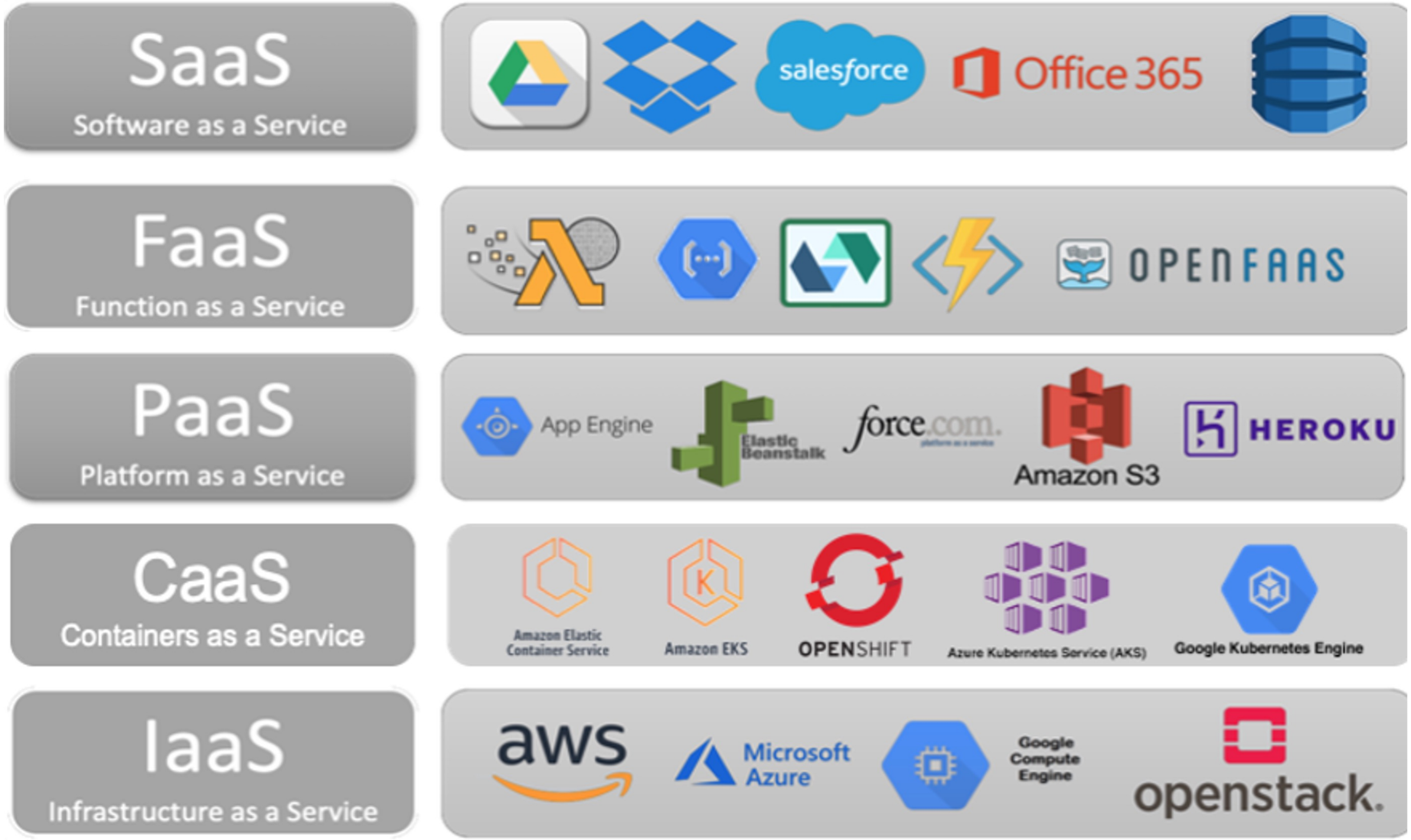
Some of the common services we offer are

1. Highly targetted phone numbers for marketting
2. Unseen facial images for fake profiles
3. Full Cloud based virtual office solutions via multiple vendors

Contact us at contactme at victim.cloud

Enumeration

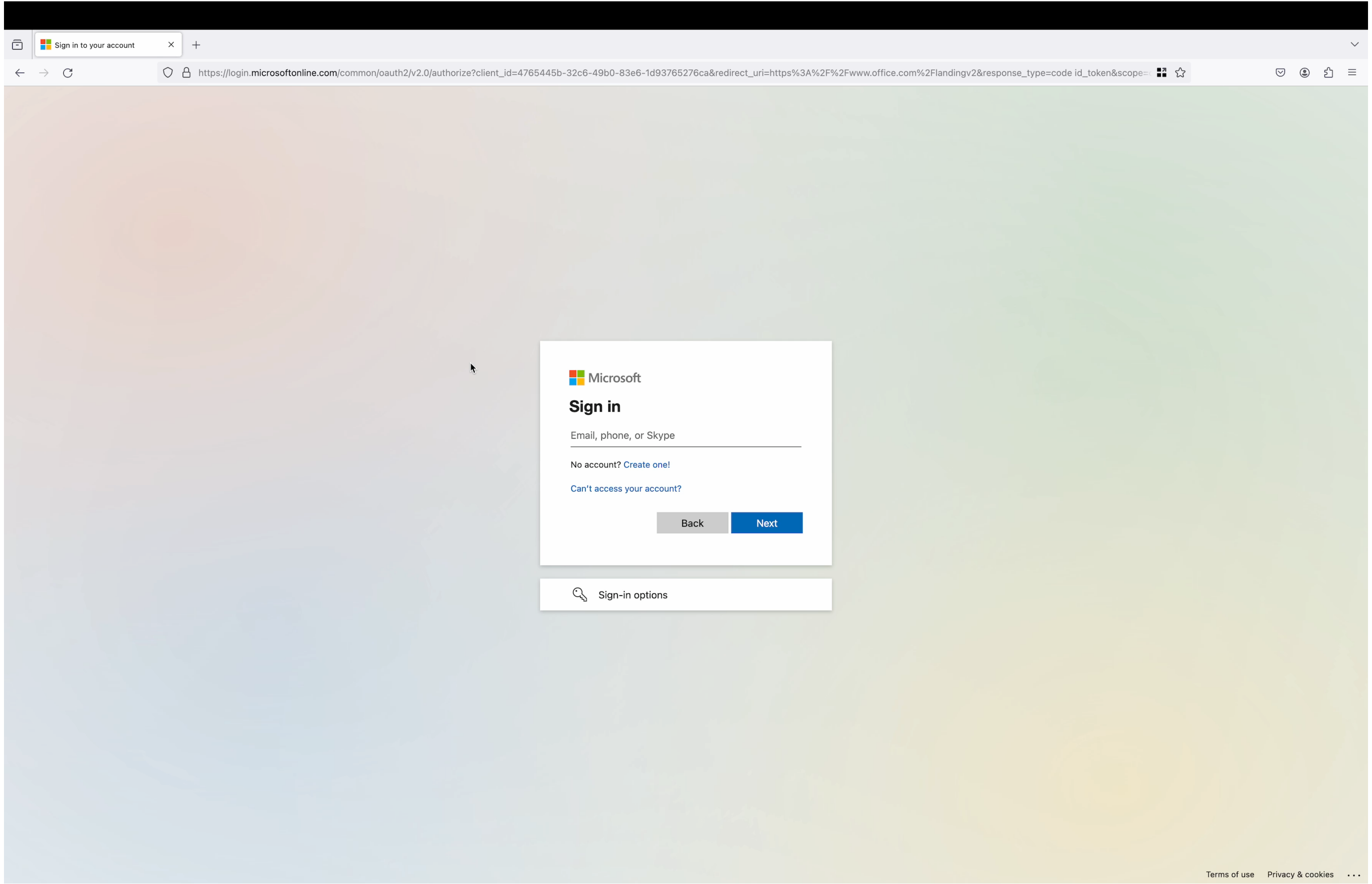
Types of Cloud Services



Enumeration

- DNS Enumeration
- Secret Hunt
- Subdomain Enumeration
- Misconfigured Storage
- Username Enumeration

Username Enumeration



https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect_uri=https%3A%2F%2Fwww.office.com%2Flandingv2&response_type=code id_token&scope=

Microsoft

Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Entering Into Cloud

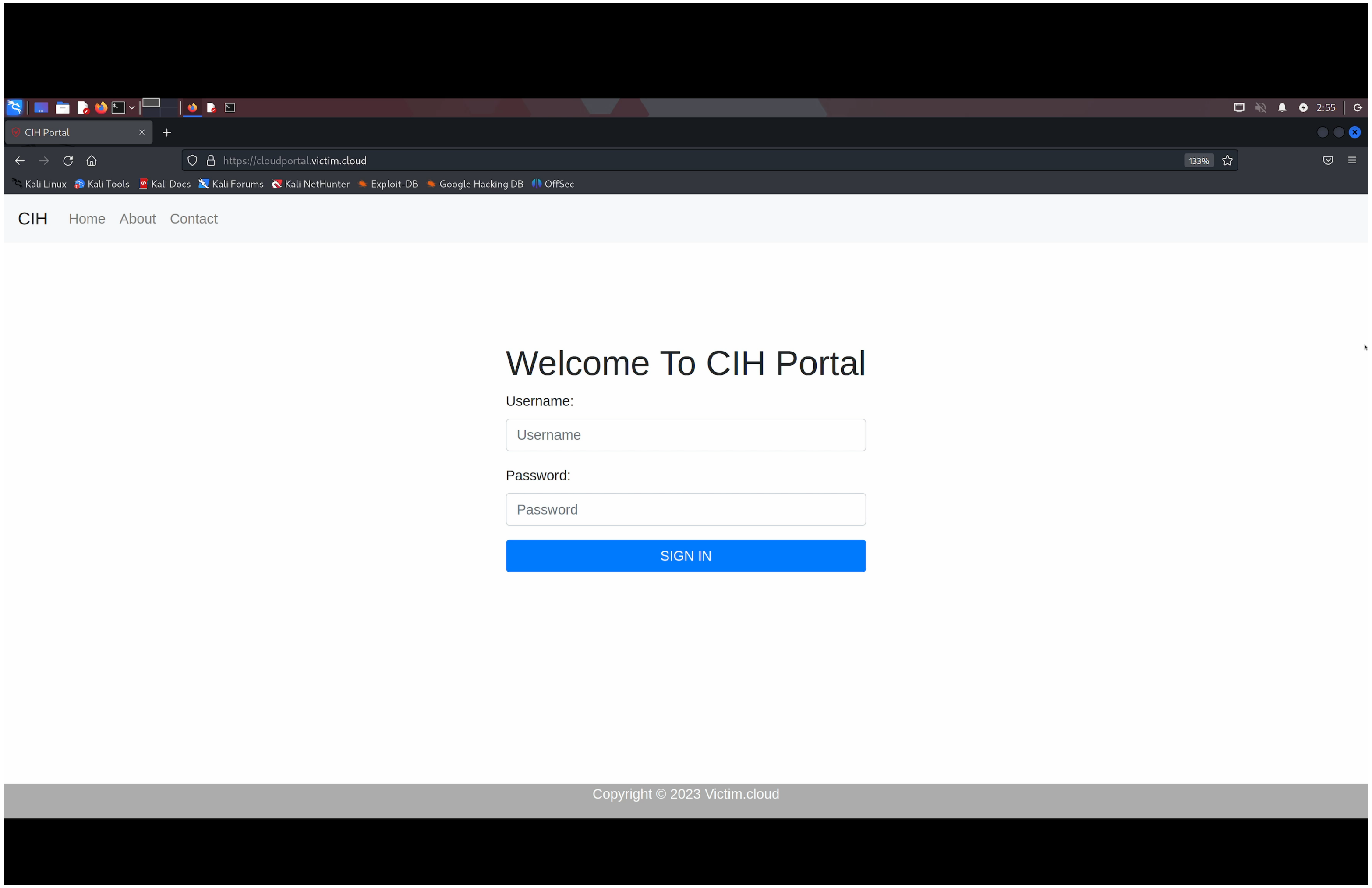
Shared Responsibility Matrix

Responsibilities	On Prem	IaaS	CaaS	PaaS	FaaS	SaaS
All Things Client Side	Tenant	Tenant	Tenant	Tenant	Tenant	Tenant
Data (Transit and Cloud)	Tenant	Tenant	Tenant	Tenant	Tenant	Tenant
Identity & Access Management	Tenant	Tenant	Tenant	Tenant	Tenant	Tenant
Functional Logic	Tenant	Tenant	Tenant	Tenant	Tenant	Provider
Applications	Tenant	Tenant	Tenant	Tenant	Provider	Provider
Runtime	Tenant	Tenant	Tenant	Provider	Provider	Provider
MiddleWare	Tenant	Tenant	Provider	Provider	Provider	Provider
OS	Tenant	Tenant	Provider	Provider	Provider	Provider
Virtualization	Tenant	Provider	Provider	Provider	Provider	Provider
Load Balancing	Tenant	Provider	Provider	Provider	Provider	Provider
Networking	Tenant	Provider	Provider	Provider	Provider	Provider
Servers	Tenant	Provider	Provider	Provider	Provider	Provider
Physical Security	Tenant	Provider	Provider	Provider	Provider	Provider

Ways Of Gaining Initial Foothold!!

- Leaked Tokens
- Remote Code Execution
- Server-Side Request Forgery (Less likely)
- Path/Directory Traversal
- Exposed Services

Azure Initial Foothold via App Service



Welcome To CIH Portal

Username:

Username

Password:

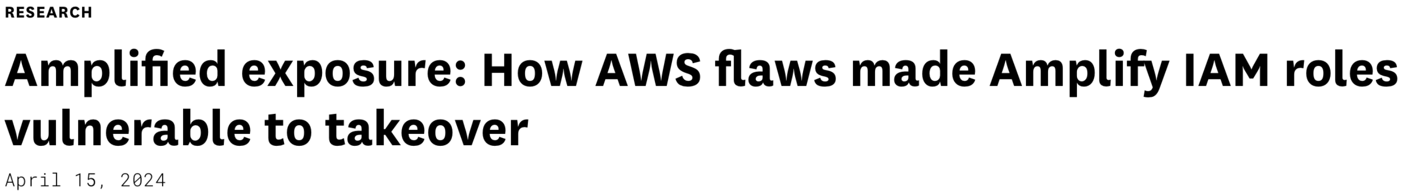
Password

SIGN IN

Copyright © 2023 Victim.cloud

Pitfall of Default Permissions

- Excessive access to the resources
- If compromised, gives elevated access



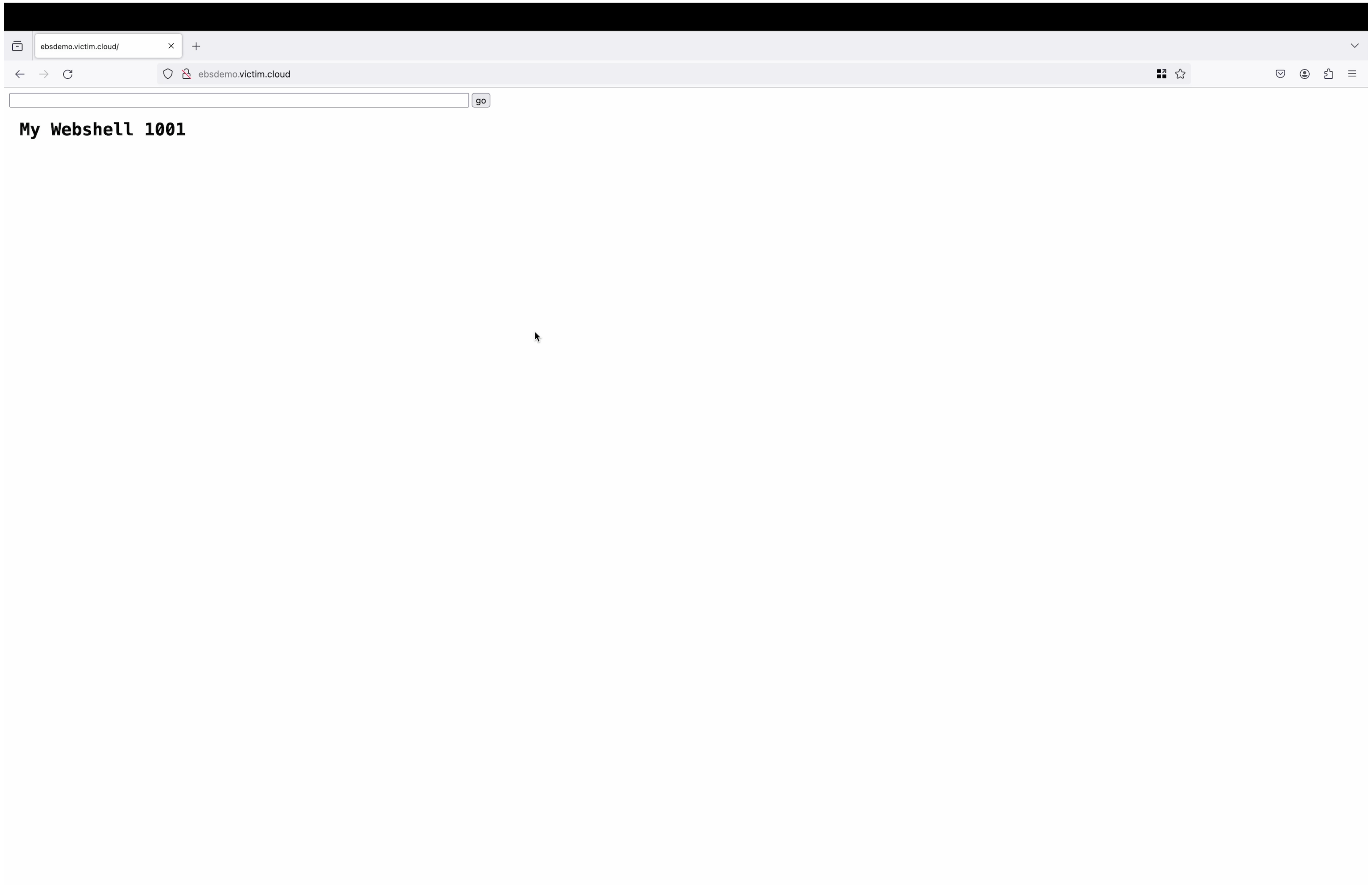
RESEARCH

Amplified exposure: How AWS flaws made Amplify IAM roles vulnerable to takeover

April 15, 2024

Reference: https://securitylabs.datadoghq.com/articles/amplified-exposure-how-aws-flaws-made-amplify-iam-roles-vulnerable-to-takeover/

RCE on AWS EBS Deployment



My Webshell 1001

Impact

Claranet Cyber Security brings you

NotSoSecure Training

Impact Of Cloud Compromise

- Financial Loss
- Data Loss
- Reputation Loss

Claranet Cyber Security brings you

NotSoSecure Training

Defence

Claranet Cyber Security brings you

NotSoSecure Training

Claranet Cyber Security brings you

NotSoSecure Training

But what could I have done?

- **Protect the Metadata API**
- **Monitor, Log, Alert!**
  - Vendor Native / 3rd Party / Open-source
  - Automatic Remediation
- **Host Security**
- **Audit & Benchmarking**
  - e.g. CIS
  - Environment auditing
  - Image auditing
- **Continuous process!**

What More You Can Expect?

Azure

- Service Principle
- Azure Dynamic Membership
- Keyvault
- App Service
- Abusing Overly Permissive Permission in Entra ID

AWS

- IAM Shadow Admin Permissions
- Misconfigured Resource Based Policy
- Cross-Account Misconfigured
- AWS ECR & ECS Misconfigurations
- AWS Lambda and API Gateway

Claranet Cyber Security brings you
NotSoSecure
Training

Thank you

Any questions / comments / feedback / requests: john@claranet.com or manish@claranet.com

Claranet Cyber Security brings you

NotSoSecure Training