

STEALING THE SILVER LINING FROM YOUR CLOUD

Anant Shrivastava : Technical Director



NotSoSecure part of

claranet cyber security

We hack



We teach

Web Application Security Assessment

Infrastructure Security Assessment

Mobile Application Security Assessment

Source Code Review

IoT Security Assessment

Red Team Exercises

Beginner Friendly

Hacking 101

Basic Infrastructure Hacking

Basic Web Hacking

Advanced/Specialist Offensive Courses

Advanced Infrastructure Hacking

Advanced Web Hacking

Hacking and Securing Cloud

Specialist Defensive Courses

Application Security for Developers

DevSecOps

For **private/corporate training** please contact us at:
training@notsosecure.com

About Myself

- Director NotSoSecure Global Services
- Sysadmin / Development / Security : all shades of IT
- Project Owner: HackingArchivesofIndia, AndroidTamer, CodeVigilant
- Contributor : null, G4H and many more
- @anantshri on social platforms



NotSoSecure part of



© 2021 NotSoSecure Global Services Ltd, all rights reserved

Agenda

- Setting the Stage
 - Everyone wants cloud
 - Organizations in cloud
 - Cloud Migration
- Understanding the environment
 - Cloud Responsibility matrix
 - Cloud Security Tooling
- Stealing the silver lining
 - ATT&CK Framework
 - Example Scenarios



NotSoSecure part of



© 2021 NotSoSecure Global
Services Ltd, all rights reserved

Everyone Wants Cloud

- Cloud Computing is the “In” thing.
- Besides the usuals of why cloud makes sense.
- 2020 has made it pretty clear remote working is here to stay.
- Data Centers & concepts of physical network boundaries are aging



NotSoSecure part of



© 2021 NotSoSecure Global
Services Ltd, all rights reserved

Orgs In the Cloud

- Born in Cloud Now (Fully cloud Native : no self datacenter footprint)
 - Mostly Startups
 - SaaS Service providers
 - Cloud service aggregator or consumers
- Migrating from existing
 - **Rehost** (Lift and Shift)
 - **Refactor** (modernize application for cloud but still stick largely to IaaS)
 - **Rearchitect** (monolith to microservices, containers / orchestration)
 - **Rebuild** (rewrite app as cloud native apps)
 - **Replace** (leveraging other SaaS options)



NotSoSecure part of



© 2021 NotSoSecure Global
Services Ltd, all rights reserved

Cloud Migration : Security Concerns

- Cloud is a paradigm shift from conventional environments
- Conventional wisdom and controls just won't work
- Cloud Security concerns
 - Misconfigurations are the biggest concerns
 - Access control failures (Insecure API's / Interfaces)
 - Unauthorized access due to credential leakage
 - Unintended Data Exposure to public
 - Data Loss and data sovereignty is next in line (GDPR and similar)

Ref: <https://notsosecure.com/security-architecture-review-of-a-cloud-native-environment/>



NotSoSecure part of



© 2021 NotSoSecure Global
Services Ltd, all rights reserved

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

NotSoSecure part of



© 2021 NotSoSecure Global Services Ltd, all rights reserved

Security Tooling in Cloud

- Most vendors provide basic set of tools
- 3rd parties are still needed for some tools
- Native tool offerings
 - Tightly coupled with Cloud providers and hence larger visibility
 - Mostly internals are hidden, and only limited stuff is exposed
 - Limitation in terms of flexibility on modifying the outputs
- 3rd Party offering
 - Especially useful if you are in multi cloud / hybrid environment
 - Limited to the stuff exposed to 3rd party
 - Allows more flexibility in terms of output modification



NotSoSecure part of



© 2021 NotSoSecure Global Services Ltd, all rights reserved

ON-PREMISES	AWS	AZURE	GOOGLE	ORACLE	IBM	ALIBABA
Firewall & ACLs	Security Groups AWS Network ACLs	Network Security Groups Azure Firewall	Cloud Armor VPC Firewall	VCN Security Lists	Cloud Security Groups	NAT Gateway
IPS/IDS	3 rd Party Only	3 rd Party Only	3 rd Party Only	3 rd Party Only	3 rd Party Only	Anti-Bot Service Website Threat Inspector
Web Application Firewall (WAF)	AWS WAF AWS Firewall Manager	Application Gateway	Cloud Armor	Oracle Dyn WAF	Cloud Internet Services	Web Application Firewall
SIEM & Log Analytics	AWS Security Hub Amazon GuardDuty	Azure Sentinel Azure Monitor	Stackdriver Monitoring Stackdriver Logging	Oracle Security Monitoring and Analytics	IBM Log Analysis Cloud Activity Tracker	ActionTrail
Antimalware	3 rd Party Only	Microsoft Antimalware / Azure Security Center	3 rd Party Only	3 rd Party Only	3 rd Party Only	Server Guard
Data Loss Prevention (DLP)	Amazon Macie	Information Protection (AIP)	Cloud Data Loss Prevention API	3 rd Party Only	3 rd Party Only	Web Application Firewall
Key Management	Key Management Service (KMS)	Key Vault	Cloud Key Management Service	Cloud Infrastructure Key Management	Key Protect Cloud Security	Key Management Service
Encryption At Rest	EBS/EFS Volume Encryption, S3 SSE	Storage Encryption for Data at Rest	Part of Google Cloud Platform	Cloud Infrastructure Block Volume	Hyper Protect Crypto Services	Object Storage Service
DDoS Protection	AWS Shield	Built-in DDoS defense	Cloud Armor	Built-in DDoS defense	Cloud Internet Services	Anti-DDoS
Email Protection	3 rd Party Only	Office Advanced Threat Protection	Various controls embedded in G-Suite	3 rd Party Only	3 rd Party Only	3 rd Party Only
SSL Decryption Reverse Proxy	Application Load Balancer	Application Gateway	HTTPS Load Balancing	3 rd Party Only	Cloud Load Balancer	Server Load Balancer (SLB)
Endpoint Protection	3 rd Party Only	Microsoft Defender ATP	3 rd Party Only	3 rd Party Only	3 rd Party Only	Server Guard
Certificate Management	AWS Certificate Manager	Key Vault	3 rd Party Only	3 rd Party Only	Certificate Manager	Cloud SSL Certificates Service
Container Security	Amazon EC2 Container Service (ECS)	Azure Container Service (ACS)	Kubernetes Engine	Oracle Container Services	Containers - Trusted Compute	Container Registry
Identity and Access Management	Identity and Access Management (IAM)	Azure Active Directory	Cloud Identity Cloud IAM	Oracle Cloud Infrastructure IAM	Cloud IAM App ID	Resource Access Management
Privileged Access Management (PAM)	3 rd Party Only	Azure AD Privileged Identity Management	3 rd Party Only	3 rd Party Only	3 rd Party Only	3 rd Party Only
Multi-Factor Authentication (MFA)	AWS MFA (part of AWS IAM)	Azure Active Directory	Security Key Enforcement	Oracle Cloud Infrastructure IAM	App ID	Resource Access Management
Centralized Logging / Auditing	CloudWatch / S3 bucket	Azure Audit Logs	VPC Flow Logs Access Transparency	Oracle Cloud Infrastructure Audit	Log Analysis with LogDNA	Log Service
Load Balancer	Application Load Balancer Classic Load Balancer	Azure Load Balancer	Cloud Load Balancing HTTPS Load Balancing	Cloud Infrastructure Load Balancing	Cloud Load Balancer	Server Load Balancer
LAN	Virtual Private Cloud (VPC)	Virtual Network	Virtual Private Cloud Network (VPC)	Virtual Cloud Network (VCN)	VLANs	Virtual Private Cloud (VPC)
WAN	Direct Connect	ExpressRoute	Dedicated Interconnect	FastConnect	Direct Link	VPN Gateway Express Connect
VPN	VPC Customer Gateway AWS Transit Gateway	Virtual Network SSTP	Google VPN	Dynamic Routing Gateway (DRG)	IPSec VPN Secure Gateway	VPN Gateway
Governance Risk and Compliance Monitoring	AWS CloudTrail AWS Compliance Center	Azure Policy	Cloud Security Command Center	3 rd Party Only	3 rd Party Only	ActionTrail
Backup and Recovery	AWS Backup Amazon S3 Glacier	Azure Backup Azure Site Recovery	Object Versioning Cloud Storage Nearline	Archive Storage	IBM Cloud Backup	Hybrid Backup Recovery
Vulnerability Assessment	Amazon Inspector AWS Trusted Advisor	Azure Security Center	Cloud Security Scanner	Security Vulnerability Assessment Service	Cloud Security Advisor Vulnerability Advisor	Server Guard Website Threat Inspector
Patch Management	AWS Systems Manager	Update Management	3 rd Party Only	3 rd Party Only	IBM Cloud Orchestrator	3 rd Party Only
Change Management	AWS Config	Azure Automation (Change Tracking)	3 rd Party Only	3 rd Party Only	3 rd Party Only	Application Configuration Management (ACM)

Attacking the Cloud



- MITRE does a good job

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
5 techniques	1 techniques	5 techniques	2 techniques	6 techniques	5 techniques	10 techniques	2 techniques	4 techniques	1 techniques	6 techniques
Drive-by Compromise	User Execution (1)	Account Manipulation (3)	Domain Policy Modification (1)	Domain Policy Modification (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Data from Cloud Storage Object	Transfer Data to Cloud Account	Data Destruction
Exploit Public-Facing Application		Create Account (1)	Valid Accounts (2)	Impair Defenses (3)	Forge Web Credentials (2)	Cloud Infrastructure Discovery		Data from Information Repositories (2)		Data Encrypted for Impact
Phishing (1)		Implant Internal Image		Modify Cloud Compute Infrastructure (4)	Steal Application Access Token	Cloud Service Dashboard		Data Staged (1)		Defacement (1)
Trusted Relationship		Office Application Startup (6)		Unused/Unsupported Cloud Regions	Steal Web Session Cookie	Cloud Service Discovery		Email Collection (2)		Endpoint Denial of Service (3)
Valid Accounts (2)		Valid Accounts (2)		Use Alternate Authentication Material (2)	Unsecured Credentials (2)	Network Service Scanning				Network Denial of Service (2)
				Valid Accounts (2)		Permission Groups Discovery (1)				Resource Hijacking
						Software Discovery (1)				
						System Information Discovery				
						System Location Discovery				
						System Network Connections Discovery				

Last modified: 27 April 2021

Enumeration



```
→ cloud_enum git:(master) python3 cloud_enum.py -k [REDACTED]

#####
cloud_enum
github.com/initstring
#####

Keywords: [REDACTED]

+++++
azure checks
+++++

[+] Checking for Azure Storage Accounts
[*] Brute-forcing a list of 455 possible DNS names
HTTP-OK Storage Account: http://[REDACTED].blob.core.windows.net/
HTTP-OK Storage Account: http://[REDACTED].blob.core.windows.net/
HTTPS-Only Storage Account: http://[REDACTED].blob.core.windows.net/

Elapsed time: 00:00:19

Protected S3 Bucket: http://[REDACTED].s3.amazonaws.com/
[!] Connection error on [REDACTED] Investigate
OPEN S3 BUCKET: http://[REDACTED].s3.amazonaws.com/
FILES:
->http://[REDACTED].s3.amazonaws.com/[REDACTED]
->http://[REDACTED].s3.amazonaws.com/[REDACTED]
->http://[REDACTED].s3.amazonaws.com/[REDACTED]

+++++
google checks
+++++

[+] Checking for Google buckets
Protected Google Bucket: http://storage.googleapis.com/[REDACTED]
OPEN GOOGLE BUCKET: http://storage.googleapis.com/[REDACTED]
FILES:
->http://storage.googleapis.com/[REDACTED]
->http://storage.googleapis.com/[REDACTED]
->http://storage.googleapis.com/[REDACTED]
```

NotSoSecure part of



© 2021 NotSoSecure Global
Services Ltd, all rights reserved

Storage Accounts

- Lynchpin of cloud existence
- Storage attacks
 - Enumeration
 - Attack
 - Exploit and post exploit

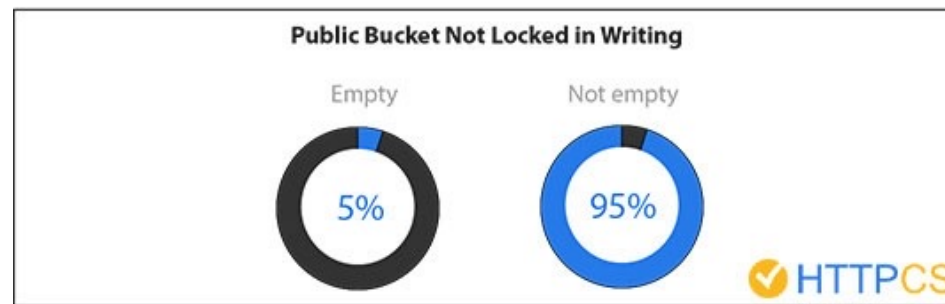
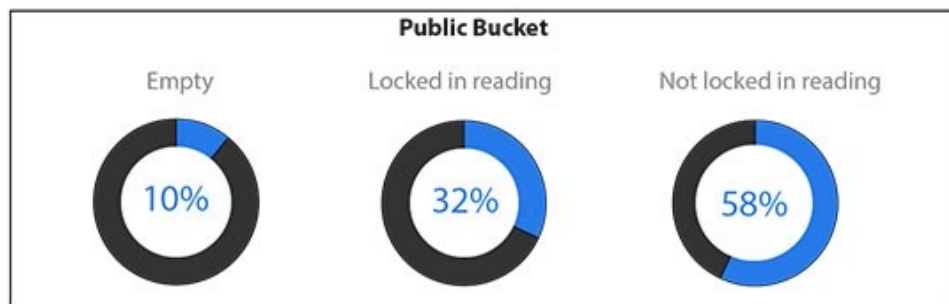
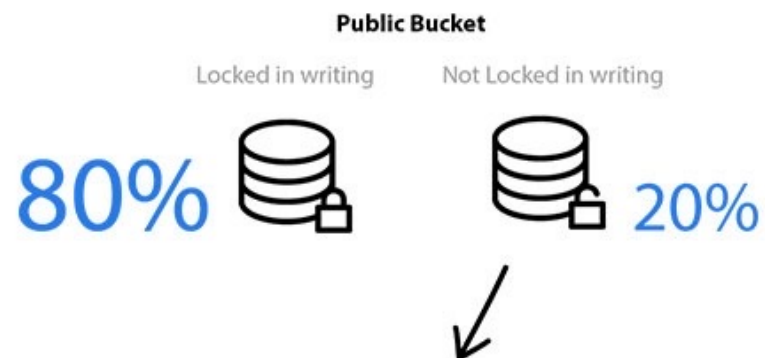
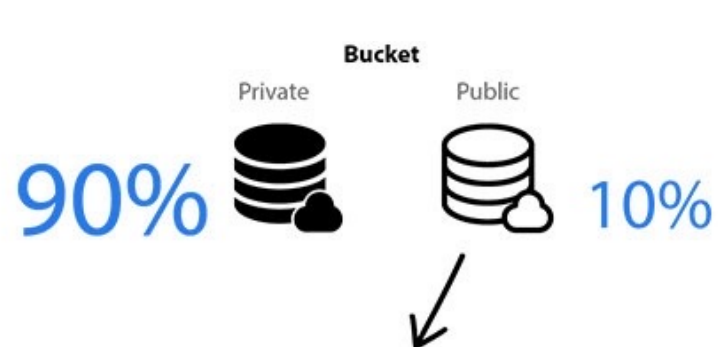


NotSoSecure part of



© 2021 NotSoSecure Global
Services Ltd, all rights reserved

AWS S3



Azure blob



GitHub, Inc. [US] | <https://github.com/search?q=DefaultEndpointsProtocol&type=Code>

DefaultEndpointsProtocol / Pull requests Issues Marketplace Explore

Repositories 0

Code 64K

Commits 14

Issues 391

Packages 0

Marketplace 0

Topics 0

Wikis 49

Users 0

Languages

Markdown 18,380

XML 14,608

64,479 code results Sort: Best match

DX

MicrosoftDX/Dash – TestConfigurations.json

Showing the top two matches Last indexed on Jun 30, 2018

```
3      "Description": "Single data account",
4      "NamespaceConnectionString": "DefaultEndpointsProtocol=https;AccountName=;AccountKey=",
5      "DataConnectionStrings": [
6          "DefaultEndpointsProtocol=https;AccountName=;AccountKey=",
```

asano-fixer/Realize.BackendServices – CloudQueueClusterSettings.pr.json

Showing the top two matches Last indexed on Jul 11, 2018

```
6      "CloudStorageAccount":
      "DefaultEndpointsProtocol=https;AccountName=przequeue0101;AccountKey=WkJ3dVBb+/Cw2a15whU87kCJID
...
9      "DeleteClusterName": ""
10     },
11     {
12         "CloudStorageAccount":
            "DefaultEndpointsProtocol=https;AccountName=przequeue0102;AccountKey=1FZT3CUjGP1e1UgZuhPs+H5ZbH
```




Case Study

Azure Attacks: Azure Storage

Starting point: Overly Privileged Azure Storage SAS URL is exposed

Exploitation Process:

- Obtain an Azure Storage SAS URL
- Load the URL in Azure Storage explorer or similar
- Identify various assets available in the storage
- Access the source code of the Azure function
- Plant a backdoor, next invocation gets the backdoor running
- Hide the backdoor

Reference:
<https://www.notsossecure.com/identifying-exploiting-leaked-azure-storage-keys/>



Case Study

PaaS: Elastic Beanstalk: Attack Case Study

- Starting point: SSRF on an application hosted in AWS Elastic Beanstalk

Exploitation Process:

1. Obtained Metadata details (account id, region, security-credentials)
2. No direct access to read S3 bucket list
3. Enumerated bucket name using the account id and region
4. Access source code of the application via AWS S3 CLI
5. CI/CD in place hence a backdoor pushed to S3 bucket will result in shell deployed on the official website
6. Summitroute did extra research & identified more such naming patterns

Reference:

<https://www.notsossecure.com/exploiting-ssrf-in-aws-elastic-beanstalk/>
https://summitroute.com/blog/2019/02/10/aws_resource_naming_patterns/
<https://gist.github.com/0xdabbad00/645837c1fcd043876d13a56819188227>

Authentication Services: AWS IAM

- Cloud shadow admins are the accounts which have permissions that attackers could abuse to escalate privileges and take hold of the entire environment
- These accounts are typically overlooked as they are not a member of privileged group (Ex. Domain Admin)



NotSoSecure part of



© 2021 NotSoSecure Global Services Ltd, all rights reserved



Case Study

AWS Policies

- AWS has multiple policies which are basically mapped to user roles to grant/restrict the access
- “AmazonElasticTranscoderFullAccess” policy has “iam:PutRolePolicy” permissions.
- “iam:PutRolePolicy” permission allows us to attach an inline policy to role.
- AWS has fixed this by rolling out new policy “AmazonElasticTranscoder_FullAccess”



Case Study

AWS Cognito

- Cognito supports two types of credentials
Unauthenticated and Authenticated
- Unauthenticated credentials related research was performed by Andres Riancho (BlackHat 2019)
- We extended the research around authenticated Credentials and found ways to leverage hidden signup features

Reference:

<https://andresriancho.com/internet-scale-analysis-of-aws-cognito-security/>
<https://www.notsosecure.com/hacking-aws-cognito-misconfigurations/>

Thank You

Contact / Feedback : anant@notsosecure.com

We are running multiple training programs @ BlackHat USA 2021



Hacking & Securing
Cloud Infrastructure
2/4 days



Web Hacking Black Belt Edition
2/4 days



Advanced Infrastructure
Hacking
2/4 days

<https://notsosecure.com/blackhat-2021/>



NotSoSecure part of



© 2021 NotSoSecure Global
Services Ltd, all rights reserved

