CLOUD SECURITY MISCONFIGURATIONS

Intro to Pentesting in the Cloud
("Oh look, something fluffy - poke, poke, poke")

Kat Fitzgerald

evilkat@rnbwmail.com

@rnbwkat

1

$WHOIAM

- evilkat@ - Kat Fitzgerald
- *CEO @BSidesChicago,*
  2019 COO @dianainitiative,
  CFP Chair @BSidesPGH, DefCon 3!
- *Based in Kirkland, WA and a natural creature of winter, you can typically find me sipping Casa Noblé Añejo whilst simultaneously defending my systems using OSS, magic spells and Dancing Flamingos*
- *Honeypots, Refrigerators and IoT (Internet of Threats) are a few of my favorite things*

2

DISCLAIMER

- The views and opinions expressed in this presentation are my own and do not necessarily reflect the official policy or position of any current or previous employer.
- Examples of exploitations, coding and vulnerabilities discussed within this presentation are only examples and they should not be utilized in the real-world.

3

WHY WE AREN'T HERE

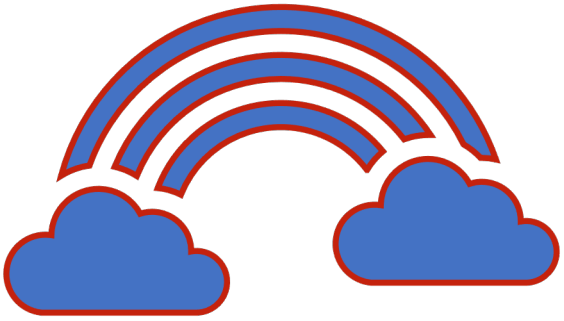
- I can't solve all your Security woes
- I won't teach you how to break-in to the cloud – only "concepts"
- Common Sense went out the window decades ago

- Cloud(s) are evolving and as things change, so do attack vectors
  - Being "Red" means adopting the change
  - Being "Blue" means adapting to that change

4

WHY WE ARE HERE

- The Cloud!
- Security
- Humans
- How?
  - *Magic!*

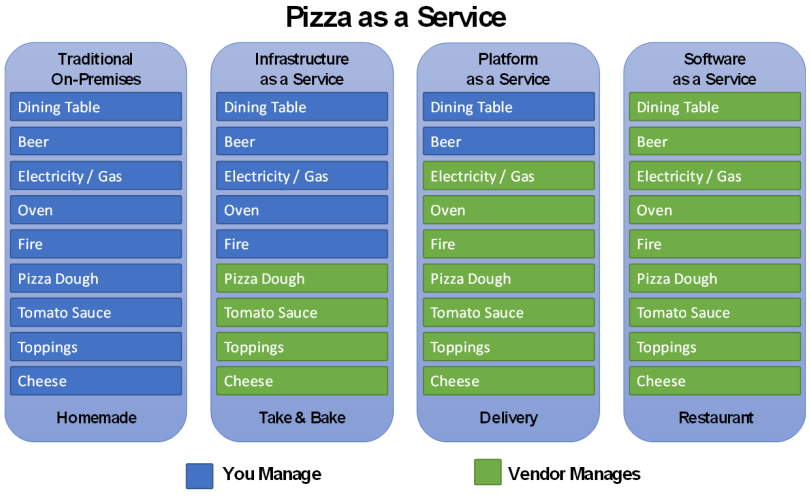


Commonsense is required – disregard previous slide ☺

5

CLOUD(S)

- IAM Policies
- ORG Policies
- Network too
- Creds ← FTW!
- Detection!!!



6

AN INCIDENT

- Most incidents are NOT 0-day
- Most incidents are NOT "fancy"
- Most incidents don't come from "vulnerability scanners"

1. Most breaches come from "Config Issues"
2. A close 2nd - compromised credentials
3. Trailing in 3rd - Over-Priv Users

7

CLOUD INCIDENTS

- Misconfigurations #1
  - Training non-existent
- Misplaced (forgotten?) keys/tokens
  - Once upon a time
- Lack of training cloud secrets usage and application
- Encryption @rest
  - transit too

8

OWASP A05:2021 SECURITY MISCONFIGURATION

"Nearly all successful attacks on cloud services are a result of customer misconfiguration, mismanagement and mistakes." –Neil MacDonald, Gartner

Pentesting BTC (before the cloud)

- Identify target
- Find vulns
- Exploit

- After
  - Find Misconfigurations (= vulns)
  - Line up targets

9

FIDDLER!

- Traditional – Sort Of
- Unpatched = Misconfiguration
  - Unpatched still exists!
- Just a tenant
- Only one root vs IAM roles
- Apps still equal Apps
  - Attack Vector

10

GENERAL ATTACK VECTORS
MISCONFIGURATIONS

- Unrestricted Ingress/Egress ports
- Secrets Mgmt (what else?!)
- Missing Logging/Monitoring
  - https://www.cloudquery.io/ *(osquery on steroids)*
  - Extracts cloud assets into normalized PostgreSQL tables
- Insecure Backups
- Buckets/Storage Access
- Lack of TLS/SSL
- Permissive Access to VMs/Containers

11

GENERAL ATTACK EXAMPLES

- IaaS
  - Weak creds
  - Anything belonging to tenant = attack surface
  - Application bugs = RCE (reading files?)
  - Misconfigured "fw"
  - Metadata API
    - AC = After Credentials
- PaaS
  - <IaaS >SaaS
  - Application vulns
  - Storage
  - Data in Transit

12

METADATA API

- All clouds have them
- A good AWS Blog
- A good GCP starting point
- An Azure good place to start
- Provides access to lots (all?) of info about services
  - *Caution: Any process that can query the metadata URL, has access to all values in the metadata server. This includes any custom metadata values that you write to the server. Google recommends that you exercise caution when writing sensitive values to the metadata server or when running third-party processes.*

13

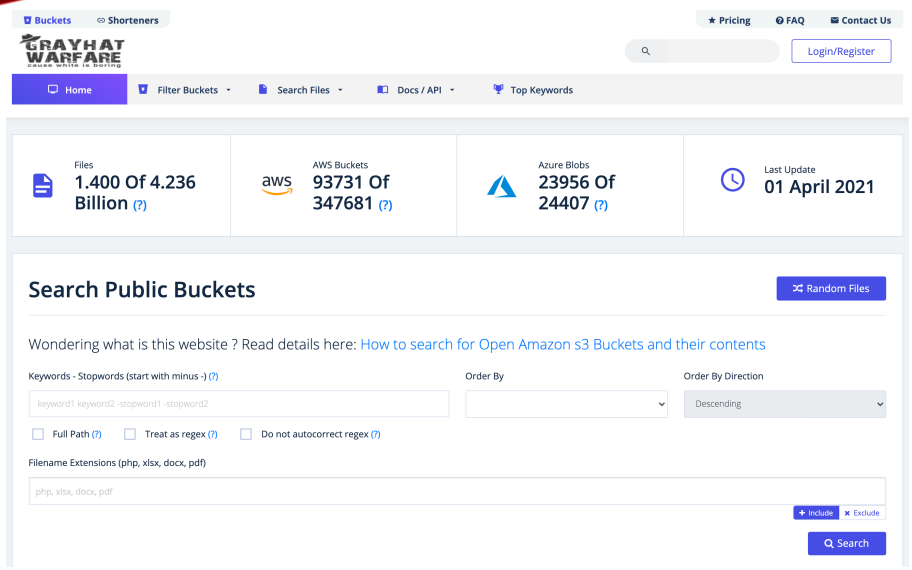
MORE ON STORAGE

- All do it
  - Remember NFS?
  - Cloud Snapshots!
  - "Volumes"
- Perms
  - Public
  - Writeable
  - Guessable names/passwords
- Github tools
  - *https://buckets.grayhatwarfare.com/*

- Cloud Snapshots are very much IaaS attack surface
- A disk image copy of the cloud instance
- Snapshots (and volumes) can be retrieved
- Once attached they bypass perms

14

Shodan(?)



15

ONCE UPON A TIME..

```
7.18 [extra718] Check if S3 buckets have server access logging enabled [redacted]
      FAIL! Bucket 00247[redacted]660497866f has server access logging disabled!
      FAIL! Bucket 1334e[redacted]c44246fedc has server access logging disabled!
      FAIL! Bucket 1da42[redacted]3a7c557bdf has server access logging disabled!
      FAIL! Bucket 26f44[redacted]08776a7a6e has server access logging disabled!
      FAIL! Bucket 28c4d[redacted]92f8df19ec has server access logging disabled!
      FAIL! Bucket 32f4f[redacted]dfd4fecb7c has server access logging disabled!

7.29 [extra729] Ensure there are no EBS Volumes unencrypted [redacted]
      INFO! Looking for EBS Volumes in all regions...
      FAIL! us-west-1: vol-0e[redacted]d2aba is not encrypted!
      FAIL! us-west-1: vol-0e[redacted]678be is not encrypted!
      FAIL! us-west-1: vol-0f[redacted]f9297 is not encrypted!
      FAIL! us-west-1: vol-09[redacted]0a69b is not encrypted!
      FAIL! us-west-1: vol-07[redacted]3c68a is not encrypted!
      FAIL! us-west-1: vol-0c[redacted]e761b is not encrypted!
      FAIL! us-west-1: vol-0f[redacted]76e46 is not encrypted!
      FAIL! us-west-1: vol-08[redacted]4c38b is not encrypted!
      FAIL! us-west-1: vol-0c[redacted]a5318 is not encrypted!
```

16

ONCE UPON A TIME..

```
FAIL! us-east-1: Potential secret found in i-00[redacted]cc127 User Data
FAIL! us-east-1: Potential secret found in i-00[redacted]fb0b7 User Data
PASS! us-east-1: No secrets found in i-0c5[redacted]61abb User Data
PASS! us-east-1: No secrets found in i-0183[redacted]f366 User Data or it is empty
FAIL! us-east-1: Potential secret found in i-027[redacted]0913 User Data

   FAIL! us-east-1: Potential secret found in i-0b4[redacted]9f956 User Data
   FAIL! us-east-1: Potential secret found in i-0f4[redacted]f0465 User Data
   FAIL! us-east-1: Potential secret found in i-083[redacted]36651 User Data
   FAIL! us-east-1: Potential secret found in i-077[redacted]0521e User Data
   FAIL! us-east-1: Potential secret found in i-09e[redacted]77d78 User Data
   FAIL! us-east-1: Potential secret found in i-0ac[redacted]ed82 User Data
   FAIL! us-east-1: Potential secret found in i-052[redacted]38d68 User Data
   FAIL! us-east-1: Potential secret found in i-0a79[redacted]ac80e User Data
   FAIL! us-east-1: Potential secret found in i-004[redacted]1b8c7 User Data
   FAIL! us-east-1: Potential secret found in i-058f[redacted]f0452 User Data
```

17

(SOME) MORE TOOLS

- AWS
  - https://github.com/RhinoSecurityLabs/pacu
  - https://github.com/duo-labs/cloudmapper
  - https://github.com/toniblyx/prowler
- GCP
  - https://github.com/RhinoSecurityLabs/GCPBucketBrute
  - https://forsetisecurity.org/
  - https://cloud.google.com/asset-inventory/docs/samples/asset-quickstart-analyze-iam-policy

18

HARDENING

- https://www.cisecurity.org/benchmark/google_cloud_computing_platform/
- https://www.cisecurity.org/benchmark/azure/
- https://www.cisecurity.org/benchmark/amazon_web_services/
- https://docs.github.com/en/code-security/secret-security/configuring-secret-scanning-for-your-repositories
- https://github.com/RhinoSecurityLabs/cloudgoat

19

LET'S DO BETTER

1. Training with security controls in the cloud
2. Training with secrets management in the cloud

20

KEY TAKEAWAYS

- Common Sense – *FTW!*
  - *Stop overthinking*
- The Basics ← *Ding ding ding*!
  - *Stop the Fancy*
  - *Audit!*
- Secure the Environment – Security Awareness!!
  - Monitor everything – look for anomalies
  - Apply Security at "All" Layers
  - Automate CIS!
  - Encrypt Data in Transit and at Rest
  - Prepare for incidents
- *Practice what the bad actors do!*

21

- Thank You!!

Kat Fitzgerald

evilkat@rnbwmail.com

@rnbwkat

https://tinyurl.com/rnbwkat

22