SYNERCOMM
SECURE • INTELLIGENT • NETWORKS

# CLOUD DEFENSE:

## AWS Common Findings & Mitigating Controls

3265 GATEWAY ROAD, SUITE 650 BROOKFIELD, WI 53045 / P: 262.373.7100 / INFO@SYNERCOMM.COM / SYNERCOMM.COM

# Overview

- Discuss common pitfalls of the AWS cloud architecture
- Shed light on practical pentest findings
- Display remediation methods for findings
- Rinse and Repeat

SYNERCOMM

- Region – A separate geographic location
- Availability zones – Isolated locations within a region
- VPC – Virtual Private Cloud (Virtual Network)
- Security Groups – Instance level Security
- AMI – Amazon Machine Images
- S3 – Simple Storage Service
- IAM – Identity Access Management
- ENI – Elastic network interface

# AWS Terms

SYNERCOMM

- Think adaptive and elastic
- Treat servers as disposable resources
- Automate
- Implement loose coupling
- Focus of services, not servers
- Database is the base of it all
- Remove single points of failure
- Optimize for cost
- Cache
- Cloud Architecture Security

# AWS Cloud architecture

SYNERCOMM

- Utilize AWS features for Defense
- Shared security responsibility model
- Reduce privileged access
- Create AWS scripts
- Testing and Auditing

# AWS Cloud Security

SYNERCOMM

- Prioritizing a Security Strategy Ahead of Controls and Tools
- Overcoming the Lack of Security Visibility in the Cloud
- Improving Confidence in Cloud Provider Security
- Defining Who is Liable
- Understanding Why Attackers are Attracted to the Cloud
- Defending Against Curious Onlookers in Multi-Tenant Infrastructures
- Addressing Compliance Regulations From the Get-Go

# Avoiding AWS Security Pitfalls

SYNERCOMM

AWS metadata endpoint

S3 Buckets

Credential management

Route 53 domain takeovers

# Pentest findings common in AWS

SYNERCOMM

# SSRF & AWS Metadata
# - Capital One -

SYNERCOMM

Insider threat

Capital one was subjected to this type of attack in conjunction with an SSRF ( Server Side Request Forgery)

Once the SSRF was completed the AWS metadata endpoint could be compromised.

AWS metadata endpoint is in every AWS environment and has information to help authenticate

# SSRF Example

hack-box-01 $ curl http://web-server.com:4567/\?url\=http://10.0.0.2/

RESPONSE: <html><head><title>Internal admin panel</title></head>...</html>

SYNERCOMM

# AWS Metadata Information

SYNERCOMM

| |
|---|
| ami-id |
| ami-launch-index |
| ami-manifest-path |
| block-device-mapping/ |
| events/ |
| hostname |
| iam/ |
| instance-action |
| instance-id |
| instance-type |
| local-hostname |
| local-ipv4 |
| mac |
| metrics/ |
| network/ |
| placement/ |
| profile public-hostname |
| public-ipv4 |
| public-keys/ |
| reservation-id |
| security-groups |
| services/ |

# Lessons Learned

SYNERCOMM

AWS metadata is needed but should be secured from access from SSRF's using host based firewalls, whitelisting, and GPOs (Not just Security Groups)

SSRF's should be tested for on all external facing applications and corrected once found.

"Dangling" CName entries

Happens when using AWS DNS servers

Associated name servers do not have zone files

E.g. Deleted or Removed zones without removing a pointer at the domain registrar.

# Route 53 Zone Takeovers

SYNERCOMM

Remove nameserver entries corresponding to the deleted zone in AWS from the domain registrar

AWS zones should be monitored for removal activities and trigger alerts or remediation actions

# Remediation of Zone Takeovers

SYNERCOMM

# Credential Management

SYNERCOMM

- Use of hard-coded passwords
- Plaintext storage of passwords
- J2EE Misconfiguration
- Hard-coded credentials
- Insufficientally protected credentials

# Remediation

SYNERCOMM

AVOID RISKY CODE PRACTICES

NEVER STORE SENSITIVE INFORMATION IN EASILY ACCESSIBLE FORMATS OR LOCATIONS

ALWAYS USE ENCRYPTION WHEN DEALING WITH CREDENTIALS

LIMIT PERMISSIONS OF CREDENTIALS TO ONLY WHAT IS NEEDED.

# Mismanaged S3 Buckets

- Publicly accessible buckets with information stored that should not be
- Uses common names that are easily guessable
- No use of access controls or permissions
- Data not encrypted
- No visibility into access

SYNERCOMM

Public buckets should always have permissions and restrictions associated with

No sensitive information should be stored on a bucket that is not controlled

Buckets should be monitored for activity

IAM roles should be applied on a per bucket or buckets basis that restricts information

Encryption should always be considered for the information inside a bucket.

# Remediation

SYNERCOMM

# THANK YOU!

Questions?