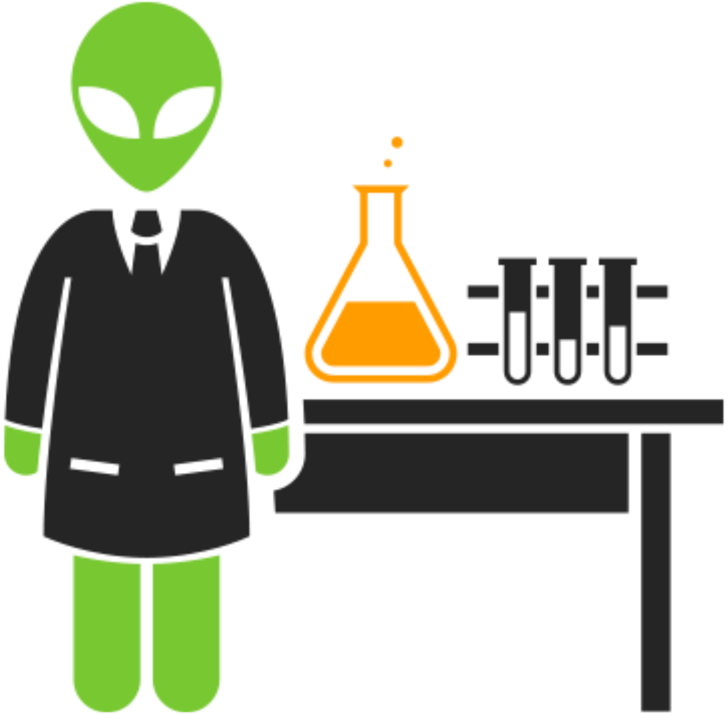
Cloudy with a Chance of Persistence

AWS Post Compromise primer by Peter Ewane

DEFCON - WALL OF SHEEP 2017

I am Peter therefore I am

- Security Researcher at AlienVault
- Cocktail and weird wine aficionado
- Native Texan
- @eaterofpumpkin



Itinerary

- Intro to AWS
- Infection Vectors
- Hiding Techniques
- Persistence Techniques
- AWS Hardening Tips

What is a “AWS”

- Who is Amazon and what are their web services?
- Why should you care?

User Based AWS Compromise Vectors

- Infected Machines
- Phishing
- Credential Leakage
  - BitBucket
  - Github
- Social Engineering

Service Based AWS Compromise Vectors

- 3rd Party Monitoring Services
- MetaData Leakage
- AMI Poisoning
- Instance Profiles
- Public EBS Snapshots

Hiding in AWS

- CloudTrail Alteration
  - Log Deletion
  - Stopping Logging
- S3 Trail Storage Alteration
  - Altering the log rotation / retention policy
  - Changing the location of log writes
- AWS Key Management Service (KMS)
  - Encrypt the log files

Persistence

- Creating a New User
  - Typo Squatting
- Creating Temporary User
- Creating New User Access Keys
- Backdoor Existing Roles
- Backdooring AMIs
- Modification of Default Security Groups

Attempting to be More Secure

- Use IAMs instead of the Root Account
- Utilize the Least Privilege Model
- Use Instance Profiles
- Audit Everything
  - AWS CloudTrail
  - AWS Config
  - AWS CloudWatch

Questions?

- Ask them if you have them

References

- https://danielgrzelak.com/disrupting-aws-logging-a42e437d6594
- https://danielgrzelak.com/backdooring-an-aws-account-da007d36f8f9
- https://www.blackhat.com/docs/us-16/materials/us-16-Amiga-Account-Jumping-Post-Infection-Persistency-And-Lateral-Movement-In-AWS.pdf
- https://www.blackhat.com/docs/us-14/materials/us-14-Riancho-Pivoting-In-Amazon-Clouds-WP.pdf
- https://aws.amazon.com/documentation/cloudwatch/
- https://aws.amazon.com/documentation/cloudtrail/
- https://aws.amazon.com/documentation/config/
- https://www.nvteh.com/news/problems-with-public-ebs-snapshots

ALIEN VAULT™

Thank you