AWS Security Assessment

Pralhad Chaskar (@c0d3xpl0it)

Agenda

- Intro to Amazon Web Services (AWS)
- Infrastructure as Code
- Traditional Infrastructure vs AWS Pentesting
- Tools of Trade
- Privilege Escalations in AWS

Amazon Web Services (AWS)

- Amazon Web Services (AWS) is a subsidiary of Amazon that provides on-demand cloud computing platforms to individuals, companies and governments, on a metered pay-as-you-go basis.
- Amazon Web Services (AWS) offers reliable, scalable, and inexpensive cloud computing services. Free to join, pay only for what you use.

https://en.wikipedia.org/wiki/Amazon_Web_Services

Global Network of AWS Regions

The AWS Cloud spans 61 Availability Zones within 20 geographic Regions around the world, with announced plans for 12 more Availability Zones and four more regions in Bahrain, Cape Town, Hong Kong SAR, and Milan.

Explore Our Products


Analytics


Application Integration


AR & VR


AWS Cost Management


Blockchain


Business Applications


Compute


Customer Engagement


Database


Developer Tools


End User Computing


Game Tech


Internet of Things


Machine Learning


Management & Governance


Media Services


Migration & Transfer


Mobile


Networking & Content Delivery


Robotics


Satellite


Security, Identity & Compliance


Storage


See All Products

Is the Cloud Secure?

March 27, 2018
Contributor: Kasey Panetta

CLOUD INFRASTRUCTURE & OPERATIONS

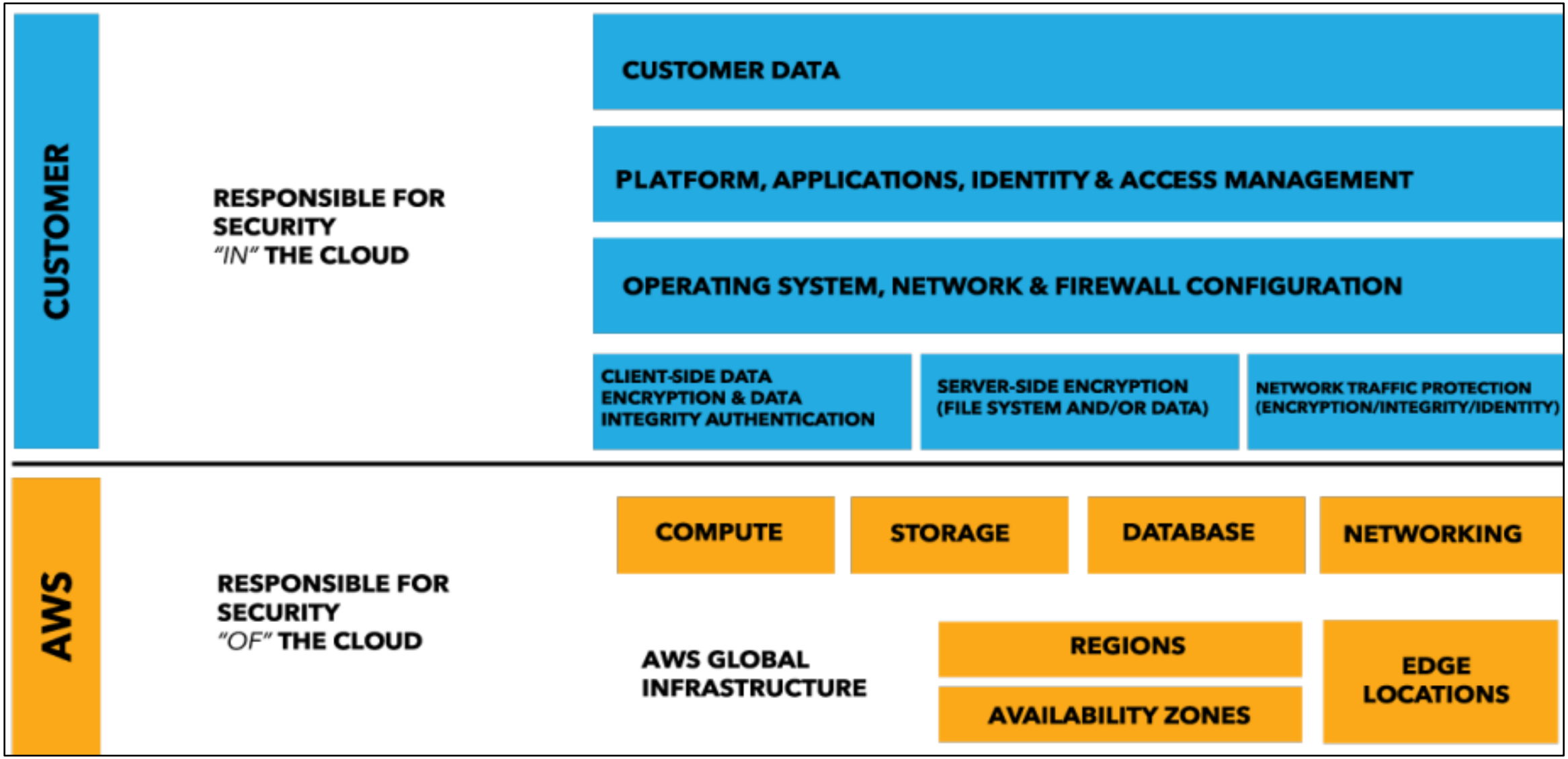
Recommendations for developing a cloud computing strategy and predictions for the future of cloud security.

In a world where security breaches dominate the headlines, the ambiguity that surrounds cloud computing can make securing the enterprise seem daunting. Concerns about security have led some CIOs to continue inhibiting their organizational use of public cloud services.

The challenge exists not in the security of the cloud itself, but in the policies and technologies for security and control of the technology. In nearly all cases, it is the user — not the cloud provider — who fails to manage the controls used to protect an organization's data.

> " Through 2022, at least 95% of cloud security failures will be the customer's fault"

Shared Responsibility Model



Permission for Penetration Testing

Customer Service Policy for Pen Testing

Private Preview and NDA – We're currently operating a preview program for security assessments of the services below. Before conducting such assessments, please contact pen-test-nda@amazon.com to complete an NDA:

o Amazon Cloudfront

Permitted Services – You're welcome to conduct security assessments against AWS resources that you own if they make use of the services listed below. We're constantly updating this list; click here to leave us feedback, or request for inclusion of additional services:

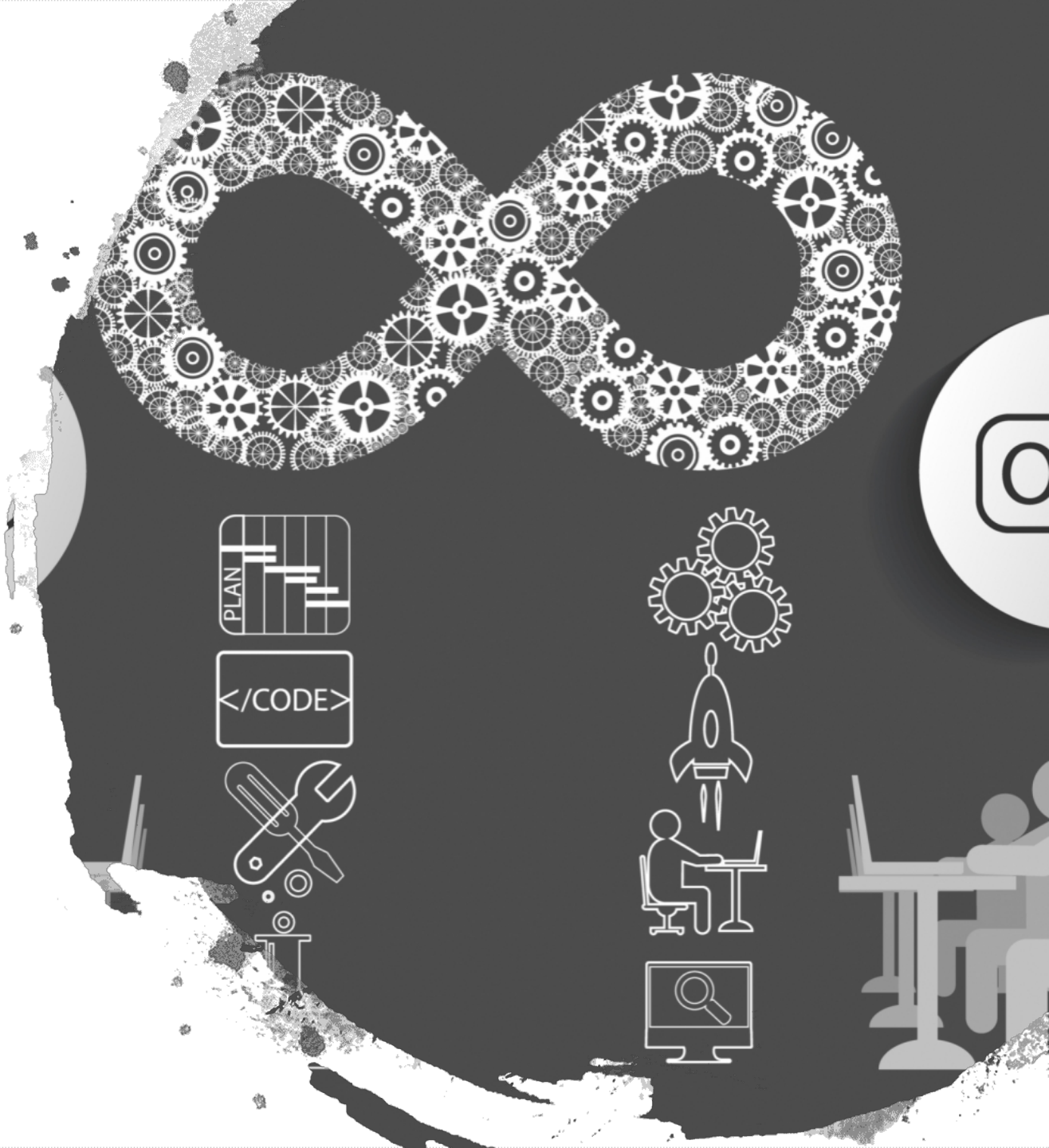
o Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers
o Amazon RDS
o Amazon CloudFront
o Amazon Aurora
o Amazon API Gateways
o AWS Lambda and Lambda Edge functions
o Amazon Lightsail resources
o Amazon Elastic Beanstalk environments

Prohibited Activities – The following activities are prohibited at this time:

o DNS zone walking via Amazon Route 53 Hosted Zones
o Denial of Service (DoS), Distributed Denial of Service (DDoS), Simulated DoS, Simulated DDoS
o Port flooding
o Protocol flooding
o Request flooding (login request flooding, API request flooding)

IAC

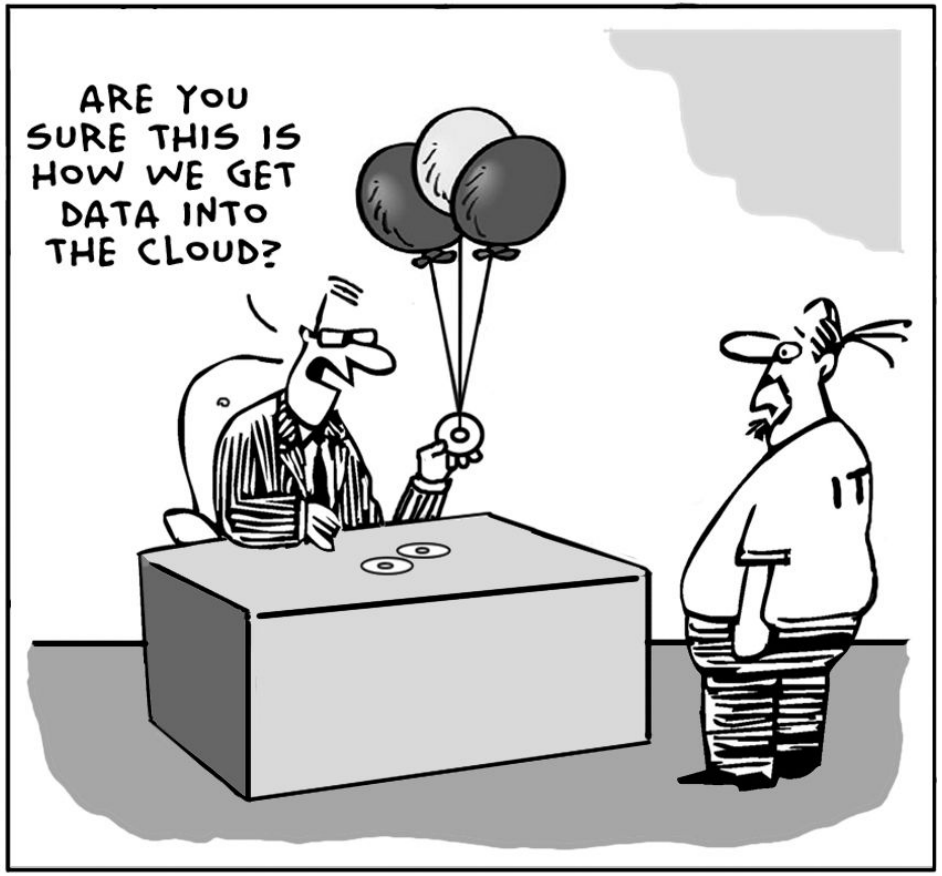
Infrastructure as code (IaC) is the process of managing and provisioning computer data centers through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools.



Terraform

- Terraform is an open-source **Infrastructure as Code** software tool created by HashiCorp.
- It enables users to define and provision a datacenter infrastructure using a high-level configuration language known as Hashicorp Configuration Language (HCL), or optionally **JSON**.
- Terraform supports a number of cloud infrastructure providers such as **Amazon Web Services**, IBM Cloud, **Google Cloud Platform**, Linode, **Microsoft Azure**, Oracle Cloud Infrastructure, or VMware vSphere as well as OpenStack

Any idea how much time it takes to facilitate any infra on Cloud compared to traditional datacenter based infra ?



Lets facilitate CloudGoat

CloudGoat is ‘Vulnerable-by-Design’ AWS Environment

https://rhinosecuritylabs.com/aws/cloudgoat-vulnerable-design-aws-environment/

Lets facilitate below infra in AWS

CloudGoat launches the following resources into your AWS account (currently into us-west-2 where possible):

- 1 CloudTrail trail
- 1 GuardDuty detector
- 1 Lambda function
- 2 S3 buckets
- 1 Elastic Load Balancer
- 1 EC2 instance
- 3 EC2 security groups
- 3 IAM users
- 3 IAM roles
- 1 IAM group
- 1 IAM instance profile
- 1 Lightsail instance
- 1 CodeBuild project
- 1 Glue Development Endpoint (Disabled by default)

DEMO !!

(Traditional Infrastructure vs AWS) Pentesting

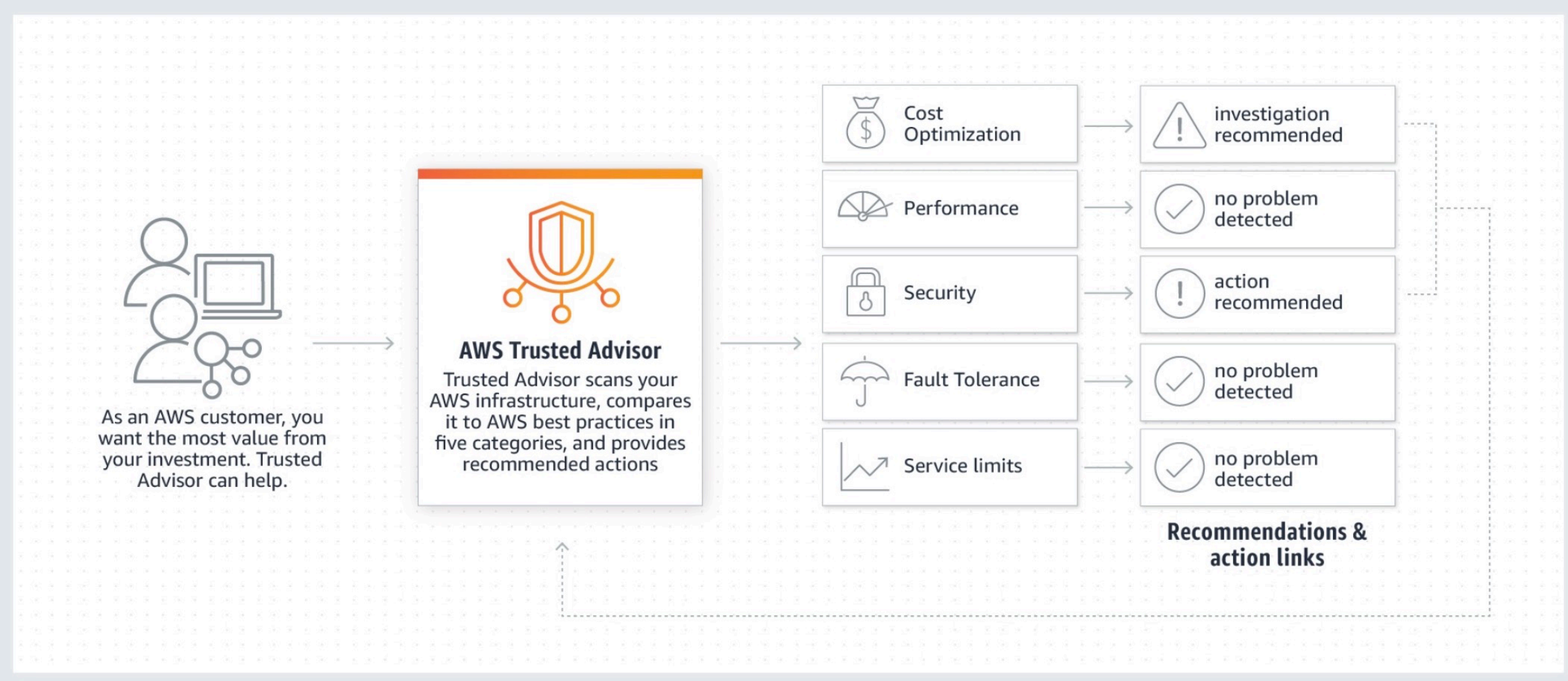
- Ownership varies
- In cloud, auditor queries the AWS API to find vulnerabilities and bad practices
- Some attacks cant be carried out (e.g.; ARP Poisoning, DOS, etc)

Responsibility	#	Layer	Examples
Customer	7	Application	Web requests, documents, application load balancers, WAF, DNS
	6	Presentation	Translation between network and application layers
	5	Session	Stateful firewall – tracks all the packets in a particular session.
	4	Transport	TCP, UDP protocols (with ports), load balancers, stateless firewalls
Cloud Provider	3	Network	IP Protocol (no ports), IP routers
	2	Data Link	Ethernet, 802.11, Mac Layer
	1	Physical	Network interface card and other hardware

https://rhinosecuritylabs.com/assessment-services/aws-cloud-penetration-testing/
https://www.slideshare.net/TeriRadichel/are-you-ready-for-a-cloud-pentest

Tools of Trade

AWS Trusted Advisor



https://aws.amazon.com/premiumsupport/technology/trusted-advisor/

AWS Inspector

Amazon (AWS) Inspector service allows you to configure a vulnerability scanner to identify and flag vulnerabilities in your server environment.

Install

Install the AWS agent on your EC2 instances.

Learn more

Run

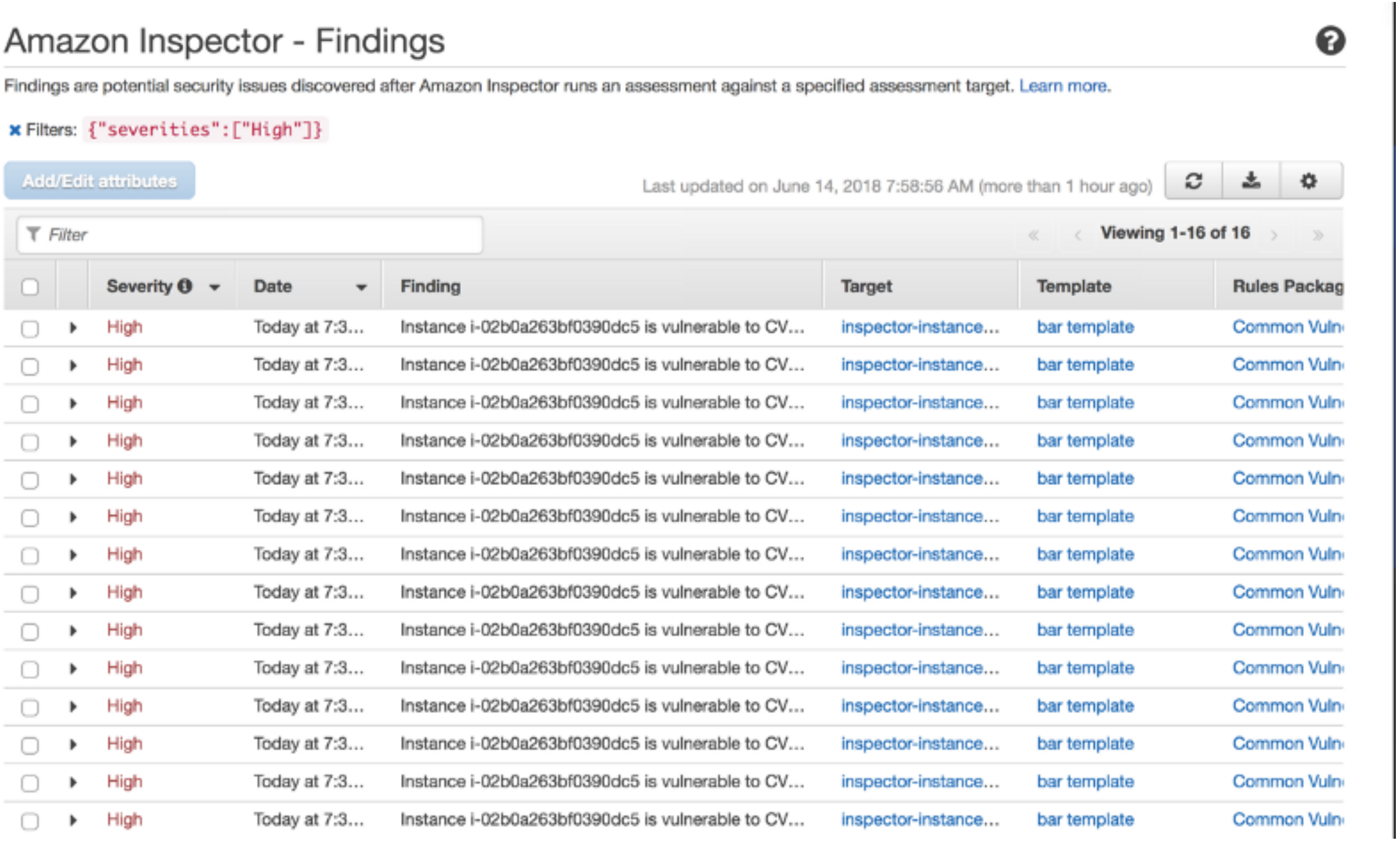
Run an assessment for your assessment target.

Learn more

Analyze

Review your findings and remediate security issues.

Learn more


Amazon Inspector - Findings
Findings are potential security issues discovered after Amazon Inspector runs an assessment against a specified assessment target. Learn more.
Filters: {"severities":["High"]}
Add/Edit attributes
Last updated on June 14, 2018 7:58:56 AM (more than 1 hour ago)
Filter
Viewing 1-16 of 16
Severity
Date
Finding
Target
Template
Rules Packag
High
Today at 7:3...
Instance i-02b0a263bf0390dc5 is vulnerable to CV...
inspector-instance...
bar template
Common Vuln
High
Today at 7:3...
Instance i-02b0a263bf0390dc5 is vulnerable to CV...
inspector-instance...
bar template
Common Vuln
High
Today at 7:3...
Instance i-02b0a263bf0390dc5 is vulnerable to CV...
inspector-instance...
bar template
Common Vuln
High
Today at 7:3...
Instance i-02b0a263bf0390dc5 is vulnerable to CV...
inspector-instance...
bar template
Common Vuln
High
Today at 7:3...
Instance i-02b0a263bf0390dc5 is vulnerable to CV...
inspector-instance...
bar template
Common Vuln
High
Today at 7:3...
Instance i-02b0a263bf0390dc5 is vulnerable to CV...
inspector-instance...
bar template
Common Vuln
High
Today at 7:3...
Instance i-02b0a263bf0390dc5 is vulnerable to CV...
inspector-instance...
bar template
Common Vuln
High
Today at 7:3...
Instance i-02b0a263bf0390dc5 is vulnerable to CV...
inspector-instance...
bar template
Common Vuln
High
Today at 7:3...
Instance i-02b0a263bf0390dc5 is vulnerable to CV...
inspector-instance...
bar template
Common Vuln
High
Today at 7:3...
Instance i-02b0a263bf0390dc5 is vulnerable to CV...
inspector-instance...
bar template
Common Vuln
High
Today at 7:3...
Instance i-02b0a263bf0390dc5 is vulnerable to CV...
inspector-instance...
bar template
Common Vuln
High
Today at 7:3...
Instance i-02b0a263bf0390dc5 is vulnerable to CV...
inspector-instance...
bar template
Common Vuln
High
Today at 7:3...
Instance i-02b0a263bf0390dc5 is vulnerable to CV...
inspector-instance...
bar template
Common Vuln
High
Today at 7:3...
Instance i-02b0a263bf0390dc5 is vulnerable to CV...
inspector-instance...
bar template
Common Vuln

Prowler

Prowler is a command line tool for AWS Security Best Practices Assessment, Auditing, Hardening and Forensics Readiness Tool.

The following AWS Managed Policies can be attached to the principal used to run Scout in order to grant the necessary permissions:

- SecurityAudit

https://github.com/toniblyx/prowler

ScoutSuite

- Scout Suite is a multi-cloud security auditing tool, which enables assessing the security posture of cloud environments. Using the APIs exposed by cloud providers, Scout gathers configuration data for manual inspection and highlights risk areas.

- The following AWS Managed Policies can be attached to the principal used to run Scout in order to grant the necessary permissions:
- ReadOnlyAccess
- SecurityAudit

- https://github.com/nccgroup/ScoutSuite

CloudMapper

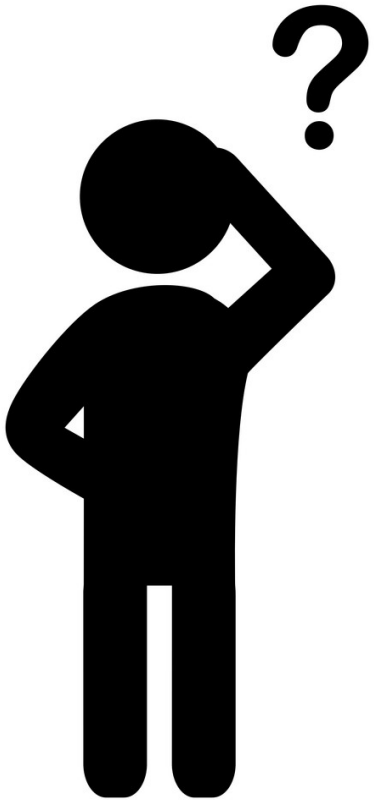
- CloudMapper helps you analyze your Amazon Web Services (AWS) environments. The original purpose was to generate network diagrams and display them in your browser. It now contains much more functionality, including auditing for security issues.

The following AWS Managed Policies can be attached to the principal used to run Scout in order to grant the necessary permissions:

- ViewOnlyAccess
- SecurityAudit

- https://github.com/duo-labs/cloudmapper

Privilege Escalation in AWS ?



Allows Read and Write Access to Objects in an S3 Bucket

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ListObjectsInBucket",
            "Effect": "Allow",
            "Action": ["s3:ListBucket"],
            "Resource": ["arn:aws:s3:::bucket-name"]
        },
        {
            "Sid": "AllObjectActions",
            "Effect": "Allow",
            "Action": "s3:*Object",
            "Resource": ["arn:aws:s3:::bucket-name/*"]
        }
    ]
}
```

Administrator users policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
    ]
}
```

There are 52 known Policies which can be abused by attacker to gain Root level permissions on account.

https://github.com/RhinoSecurityLabs/pacu/blob/master/modules/iam__privesc_scan/main.py#L76

Pacu

Pacu is an open source AWS exploitation framework, designed for offensive security testing against cloud environments.

Pacu allows penetration testers to exploit configuration flaws within an AWS account, using modules to easily expand its functionality.

Current modules enable a range of attacks, including user privilege escalation, backdooring of IAM users, attacking vulnerable Lambda functions, and much more.

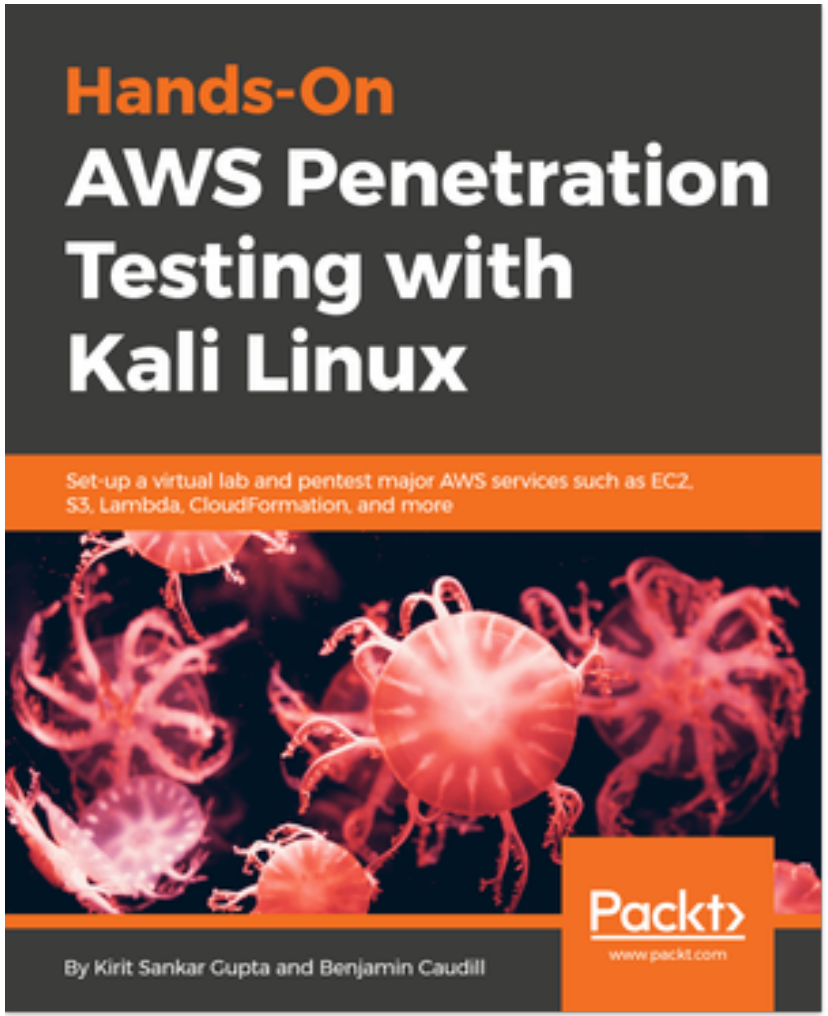
https://github.com/RhinoSecurityLabs/pacu

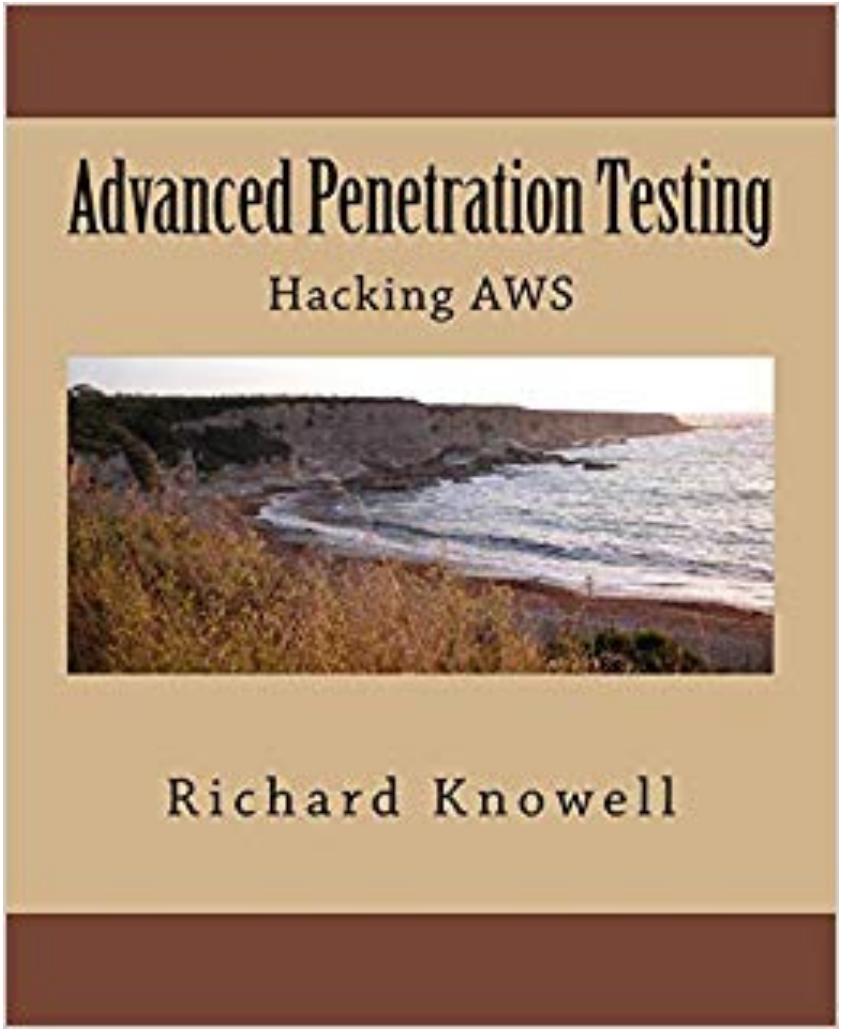
DEMO !!

References

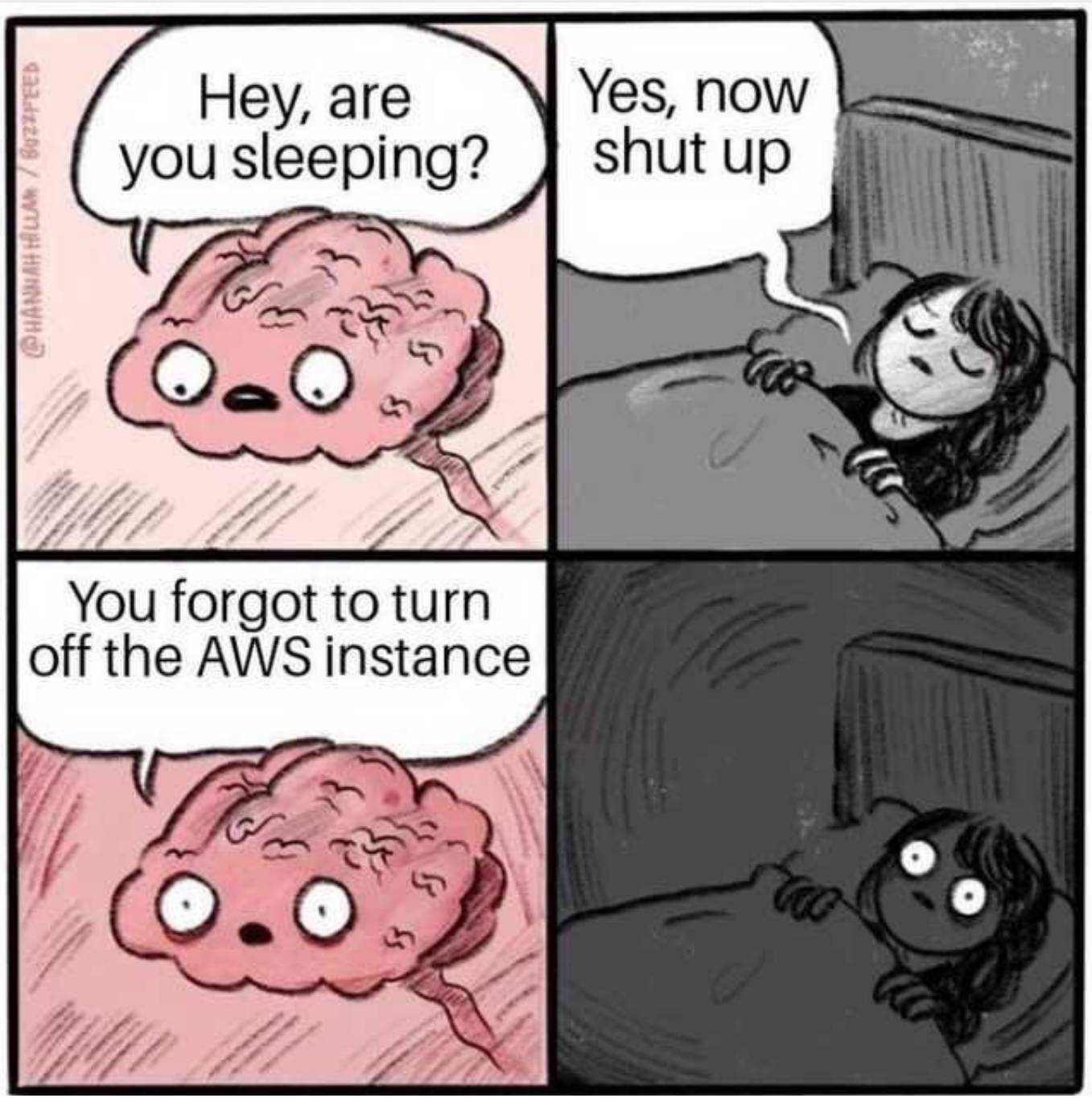
- https://rhinosecuritylabs.com/assessment-services/aws-cloud-penetration-testing/
- https://github.com/toniblyx/my-arsenal-of-aws-security-tools
- https://github.com/RhinoSecurityLabs/pacu
- https://github.com/toniblyx/prowler
- https://github.com/nccgroup/ScoutSuite
- https://github.com/duo-labs/cloudmapper
- https://andresriancho.com/automated-security-analysis-aws-clouds/
- https://www.cyberark.com/threat-research-blog/cloud-shadow-admin-threat-10-permissions-protect/
- https://www.cloudconformity.com/conformity-rules/

Book (if required)





Word of Caution !!



Questions ?