Pentesting AWS

Anand Varia
I am **NOT** being compensated by AWS or my employer to give this talk. I am expressing my own opinions here.

I’m sharing what I have learned. There are many others who know more about AWS than I do.
Agenda ~ 45 mins

- Evolution of Cloud
- About AWS
- Key AWS concepts
- Cloud Breaches
- Demo - Scenario 1
- Demo - Scenario 2
- Using AWS to secure AWS
- QnA
Evolution of cloud

- 1960: IBM virtualised operating systems
- 1965: Late Professor John McCarthy suggested computing would be sold as a utility
- 1970: ARPANET launched
- 1975: Queen Elizabeth II sends an email
- 1980: White House installed its first computers
- 1985: Storage tapes with capacity of 200 megabytes launched
- 1990: Nearly 100,000 computers connected to the Internet
- 1995: World Wide Web launched; 1 million computers connected to the Internet
- 2000: Professor Ramnath Chellapa mentions 'Cloud'
- 2005: 'Cloud' in an internal document in Compaq
- Amazon Web Service (AWS) launches public cloud
Evolution of cloud

- 2005: Sun Microsystems develops 'data centre in a box' concept
- 2006: Amazon launches Elastic Compute Cloud (EC2)
- 2007: Dropbox founded - cloud storage becomes a service
- 2008: AWS offers Service Level Agreement (SLA)
- 2009: Single provider services in multiple regions and data centers
- 2010: Spot bidding for instances launched by AWS
- 2011: NIST provides definition for Cloud computing
- 2012: Microsoft Azure launched
- 2013: Blockchain-as-a-service launched
- 2014: AWS launches Lambda for serverless applications
- 2015: European Grid Infrastructure (EGI) Federated Cloud launched
- 2016: Dell launches Hybrid Cloud System
- 2017: IBM Cognitive Cloud popularised
- 2018: IBM launches Internet of Things (IoT) platform available
- 2019: Amazon StepFunctions launched
- 2020: Microservices for Cloud application development

First Generation Cloud
Second Generation Cloud
Next Generation Cloud
Evolution of Amazon

Company milestones
- Amazon founded: July 5, 1994
- Amazon IPOs at $18.00/share: May 1997
- Acquires IMDb: Apr 1998
- Lawsuit against Barnes & Noble: Mar 2002
- Amazon Fresh: Aug 2007
- Amazon Prime: Feb 2005
- Amazon Kindle: Nov 2007
- Amazon S3: Mar 2006
- Amazon Instant Video: Feb 2011
- Acquires Kiva Systems: Mar 2012
- Amazon Launches in India: Jun 2013
- Amazon Underground: Aug 2015
- Amazon Prime Air: Dec 2016
- 23-year anniversary: July 5, 2017

Product launches
- Expands beyond books: Aug 1997
- Launches Amazon Music: Sep 2007
- Launches Amazon Mechanical Turk: Nov 2005
- Launches Amazon Appstore: Mar 2011
- Launches Amazon Elastic Compute Cloud: Aug 2006
- Acquires Zappos: Jul 2009
- Acquires Goodreads: Mar 2013
- Acquires Whole Foods: Nov 2016
- Opens its first physical store: Nov 2017
- Kindle Fire: Jul 2014
- Amazon Launches in India: Jun 2013
What is Cloud?
Amazon Web Services

Here services are terms used for various products it is offering like S3, EC2, RDS, Lambda, Polly, SNS, SQS etc.

There are 150+ services and are being added frequently.
**Region**: A geographical area designed to be isolated from all other Regions

- Isolated for fault tolerance and stability
- AWS has Global Services (like IAM) that apply to all Regions
- AWS also has Region-based Services

**Availability Zones** are separate locations within the Region

Site: https://infrastructure.aws/
About AWS: Shared Responsibility Model

**CUSTOMER**
- Responsibility for security ‘in’ the cloud

**AWS**
- Responsibility for security ‘of’ the cloud

**SOFTWARE**
- Compute
- Storage
- Database
- Networking

**HARDWARE/AWS GLOBAL INFRASTRUCTURE**
- Regions
- Availability Zones
- Edge Locations

**CUSTOMER DATA**
- Platform, Applications, Identity & Access Management

**OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION**
- Client-side data encryption & data integrity authentication
- Server-side encryption (file system and/or data)
- Networking traffic protection (encryption, integrity, identity)
About AWS: Shared Responsibility Model

Customer Responsibility

- Client Side Data Encryption & Data Integrity Authentication
- Network Traffic Protection (Encryption/ Integrity/Identity)

AWS Responsibility

- Platform & Application Management
- Operating System & Network Configuration

AWS Endpoints

- AWS Foundation Services
  - Compute
  - Storage
  - Database
  - Network

AWS Global Infrastructure

- Regions
- Availability Zones
- Edge Locations

Key Services : Elastic Cloud Compute(EC2)

- EC2 instance are traditional virtual servers present on cloud.
- AMI: Amazon Machine Image: Golden images to create Instances.
- There are Security Groups, Auto scaling groups, Elastic Ips.

[Diagram: Amazon EC2: Instance Types]

https://microage.com/blog/aws-ec2-pricing-models/
Security Groups are individual enclaves bordered with stateful firewalls
- Can specify separate (or even multiple) Security Groups for each host
- Filtering rules can be set up for inbound and outbound traffic
  - Can specify allowed source/destination IPs and ports
  - If not otherwise specified, all outbound traffic is permitted
  - Implicit DENY of all traffic not explicitly ALLOWed

VPCs are like VLANs, a private network

VPC Endpoints: VPC Endpoints allow private connections between the AWS back-end and your VPC
Key Services: Simple Storage Service S3

- S3 is an Object-based storage service where you can practically store unlimited files.
- They have a bad reputation because people leave them world-readable.
Key Services: CloudTrail vs CloudWatch

- **CloudTrail** is a webservice recording all the API activity, whereas **CloudWatch** is a monitoring service for AWS resources and applications.

- **CloudTrail/Watch** gets enabled by default, for CloudWatch supports certain services and basic monitoring is free, for detailed one you will need to pay.

- **CloudTrail** helps you in ensure compliance & regulatory requirements, **CloudWatch** logs details which provides information on what happens with data.

- **CloudTrail**: Deliver events within 15 mins of API Call

- **CloudWatch**: For basic monitoring delivers data in 5 mins, for detailed monitoring 1 mins.
Key Services: Identity & Access Management

- Not granting access to any services, user will be allowed to stare at the screen
Key Services: Identity & Access Management

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::confidential-data"
        },
        {
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::confidential-data/*"
        }
    ]
}
```

Tag: a metadata key (value is optional) that can be attached to AWS resources.

- Limit access to resources based on Tags:
  
  "Secrets manager:ResourceTag/Project": "${aws:PrincipalTag/Project}"

API Access : AWS CLI, AWS Provided Libraries

- Access Key ID
- Secret Access Key

Cloud Formation: “Infrastructure as a code”, another example is “Terraform”
Common Failures: Accessible API Keys, Excessive Permissions

- Your AWS API keys allow people to impersonate you, get access to your resources, and use your AWS account to mine for bitcoin.
- There are tools like truffleHog and git-secrets available to audit any GitHub repositories to find AWS Keys, passwords, and other sensitive data.
- Public buckets: not even once, until authorized by management.
- Use bucket lifecycles for data retention.
- “Authenticated Users” group means anyone who has logged in to any AWS account, not just yours!
- Set your S3 buckets to be encrypted by default. It has zero impact on your workflow and makes your auditors happy.
- While encrypting take care of “Old Data” and all previous versions

“Demo”
Demo - 1 Poorly configured S3 buckets

flAWS.cloud
Excessive permission can lead to ...
Demo – 3 misconfigured EC2 instance

Who can access “meta-data”
Cloud Breaches

Former AWS Engineer Arrested as Capital One Admits Massive Data Breach

Over 540 million Facebook records found on exposed AWS servers
Leak originated at two third-party companies that had collected Facebook data on their own servers.

AWS Data Leaks Persist

In addition to the aforementioned Microsoft data leak, several Amazon Web Services (AWS) data leaks recently were discovered, including:

- **Alteryx**: Misconfigured AWS cloud storage, exposing personal information from 123 million U.S. households.
- **Verizon**: Suffered two AWS-related leaks: a [Verizon Wireless leak](#) and a second exposure in which [14 million Verizon records were leaked](#).
- **Time Warner Cable**: Leaked 4 million customer records.
- **WWE**: Exposed 3 million customer records.

Ford, TD Bank Affected by Cloud Data Breach

BY CHRIS BRUNAU
Cybersecurity

JUN 28, 2019

An unprotected [Microsoft](#) cloud server database has exposed sensitive data from more than 80 million American households, hacktivists Noam Rotem and Ran Locar told [vpnMentor](#). Microsoft has notified the database owner, and the database has been removed.
On July 29th, a story broke about a hacker who extracted data from CapitalOne's infrastructure, Credit card application data from 2005-2019 was taken.

There were 140,000 Social Security Numbers and 80,000 bank numbers included in this data.

The source of the data was an S3 bucket, but this was not a public S3 bucket.

Facts: WAF IAM role from accessible ec2 instance with having access “sync” S3 buckets

The report to the Law enforcement agency contains details about WAF IAM role being used to infiltrate the data from an EC2 instance
Cloud Breach – EBS Public Snapshots

- At **DEFCON**, Ben Morris from Bishop Fox announced that he had discovered that many Elastic Block Store (EBS) snapshots are set to public.
  - Elastic Block Store is a virtual hard drive for your EC2 Instances.
  - Backups of these virtual hard drives are done via Snapshots.
- If Snapshots are in Public mode, they are open to everyone.
- Anything that might be on your system might be in an EBS Snapshot (Code, AWS Keys, log data, company confidential information).
- You can audit your snapshots to figure out if they’re Public or not via the Console or the AWS CLI, or set up AWS Config rules to audit and enforce Private snapshots.
Using AWS to secure AWS

- Make use of **Trusted Advisor** at least for public S3, any to any traffic present in **SG**.
- Make separate accounts for infrastructure like **Production, SIT, UAT, Staging, Test, Hacking etc.**
- Make use of **AWS Organizations, AWS Control Tower**
- **Least Privileges, IAM Hygiene, Restricted IAM Roles**
- Make use of **AWS Systems Manager**
- Make use of **AWS Config, Amazon Macie as well as Guard Duty**
- **Do not rely on your bill** to know which resources you are/were using. Have **inventory**
For demo purpose I have used the following:

- http://flAWS.cloud
- Cloudgoat by Rhino security labs

Tools reference link:

- https://github.com/0xVariable/AWS-Security-Tools
Questions?
Thank you!
Email: anandjvaria@gmail.com