Sheffield CompSoc

SHEFFIELD ETHICAL STUDENT HACKERS

AWS Workshop

What is it, why is it useful and how can we get started with it?

Collection of services

EC2 - Virtual Servers
RDS - Managed Relational Database Service
S3 - Scalable Storage

And many more specialised services...

EC2

Easy to deploy, easy to manage and easy to upgrade virtual servers

Allows for easy setup of essential features such as auto scaling, automated backups and status alarms

RDS

Easy to *securely* connect to your EC2 instances

Easy to create clusters of databases so that your service is always available

Built in features to automatically backup and more importantly, restore backups

S3

Easily scalable storage

Simple to adapt storage towards fast reads (more expensive) or longer term archival storage (less expensive)

Can easily connect to other services to provide storage for a web app or store machine learning models

Other Services

Device Farm - Allows you to test Android, iOS and Web Apps on real devices in the cloud

Elastic Transcoder - Easy to use scalable media transcoding

IoT tools - More than 10 services to help connect, monitor and control IoT devices

Machine Learning - Image Recognition, Speech Synthesis and Generative AI tools are just a few examples of Machine Learning tools offered by AWS

How to setup an EC2 Instance

Ethical Student Hackers

AWS Security

The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

- Relevant UK Law: https://www.legislation.gov.uk/ukpga/1990/18/contents

Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.

- If you have any doubts or need anything clarified, please ask a member of the committee.

- Breaching the Code of Conduct = immediate ejection and further consequences.

- Code of Conduct can be found at https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf

Incidents

https://www.techradar.com/news/this-new-open-source-tool-is-hunting-for-public-aws-s3-buckets-to-spy-on

- check s3 buckets for “BlockPublicAcls”, “BlockPublicPolicy”, “IgnorePublicAcls”, “RestrictPublicBuckets”
- Download and scan for credentials, access tokens and PII

https://www.theregister.com/2022/09/01/mobile_apps_leaked_biometrics/

- hardcoded values stored in code by dependencies

https://www.theregister.com/2022/06/20/captial_one_wire_fraud/

- misconfigured web application firewall
- Put stolen credit card info on github
- Used data to get into accounts and mine bitcoin

https://www.pentestpartners.com/security-blog/unclamping-the-barnacle/

- Endpoint leaked S3 keys
- Accepted test credit cards

Firewalls

In cloud so things can be much more publicly accessible.

Firewalls can be used to block traffic leaving and entering your virtual network.

Filter based on:

- AWS services
- IP addresses
- Domains
- Ports
- Protocols

Allow only the traffic that is needed to pass through the firewall.

Public and private subnetting

AWS Virtual Private Cloud - Virtual network within AWS

Subnets - range of addresses within the VPC

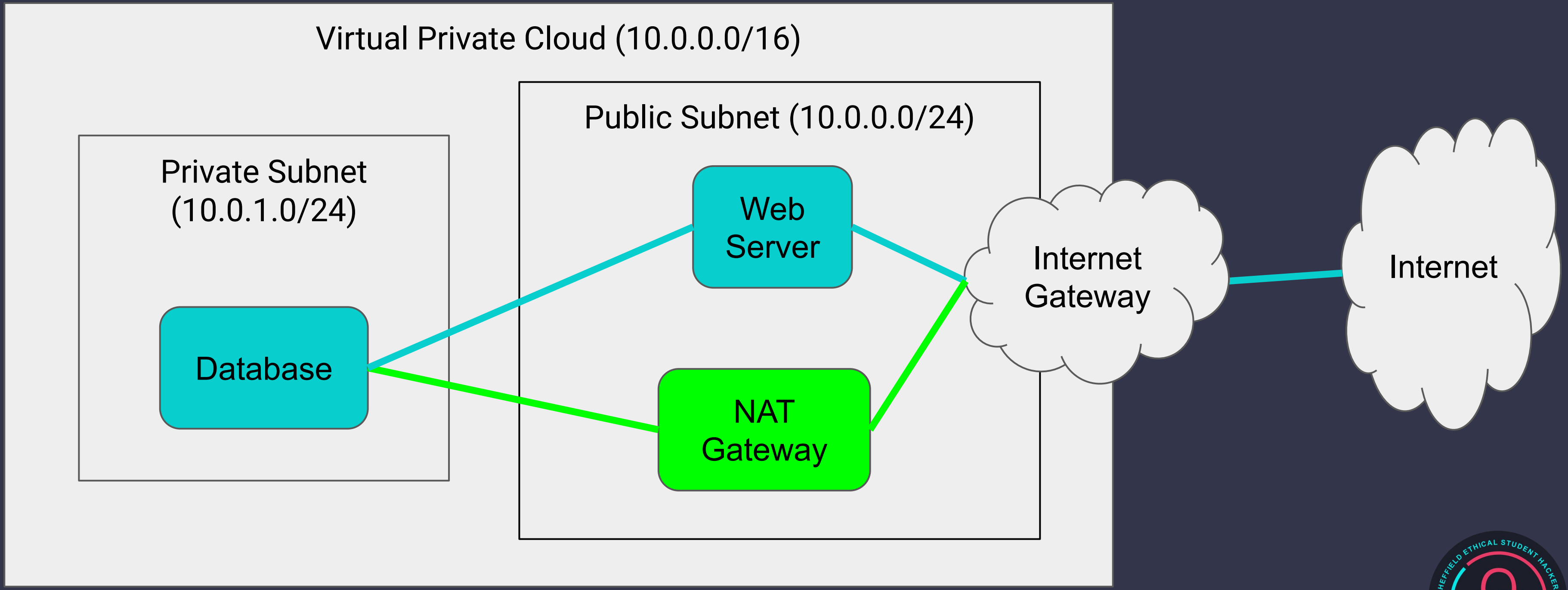
- Public - has internet gateway so direct internet access
- Private - no direct internet access

Put resources on private subnet unless they need internet access to reduce attack surface.

Allow traffic from public subnet to private subnet by adding public subnet ip range to private subnet security group.

Allow private subnet internet access by allowing and configuring traffic to access NAT gateway (special configuration for IPv6).

Public and private subnetting


Virtual Private Cloud (10.0.0.0/16)
Public Subnet (10.0.0.0/24)
Private Subnet (10.0.1.0/24)
Web Server
Database
NAT Gateway
Internet Gateway
Internet

Green used for updates and other connections initiated from the private subnet.

Securing S3 Storage

Access Control Lists:

- Each object has an ACL with the one who uploaded it being the owner (not necessarily who created the the S3 bucket)
- They can grant access to other users and groups
- Set individual actions or FULL_CONTROL:
  - READ
  - WRITE
  - READ_ACP
  - WRITE_ACP
- Can be disabled to use object ownership

```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy
xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Owner>
    <ID>Owner-canonical-user-ID</ID>
    <DisplayName>display-name</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="CanonicalUser">
        <ID>Owner-canonical-user-ID</ID>
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>

    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="CanonicalUser">
        <ID>user1-canonical-user-ID</ID>
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>WRITE</Permission>
    </Grant>
```

Securing S3 Storage

Object Ownership:

- Bucket owner owns all the objects
- Access dependent on:
  - IAM Policy
  - Bucket Policy
  - VPC endpoint
  - AWS Organization Service Control Policies

```
PUT HTTP/1.1
        Host: bucketname.s3.eu-west-2.amazonaws.com
        x-amz-date: Mon, 14 Nov 2022 17:00:00 GMT
        Authorization: authorization string
        x-amz-grant-write: emailAddress="user1@example.com", emailAddress="user2@example.com"
```

Securing S3 Storage

Encryption:

- Server side - data encrypted at rest after entering AWS
  - Prevents directly reading from disk
  - Transparent to clients
  - Keys held by AWS (keys are used following any authenticated request)
- Client side - Encrypt data before it is sent to the S3 storage
  - Prevents data from being read in transport and at rest
  - Requires the keys to be stored on every client consuming that data
  - Or can use AWS Key Management Service (similar risks to SSE)

Bucket Versioning

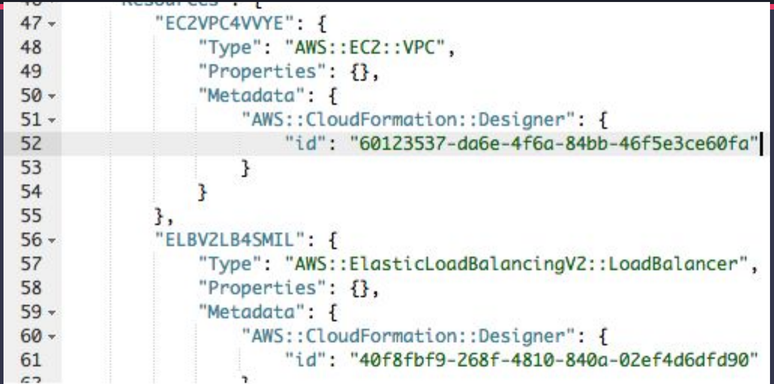
Templates/Automation

Security in templates or other automation allow for consistent deployment with all the security that you have designed and is less likely to have mistakes.

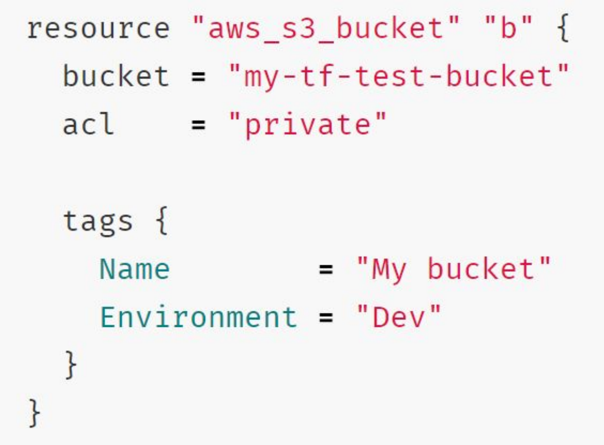
Cloudformation (native)

Terraform (Cross platform including GCP, Azure, Digital Ocean)

Scanning tools such as AWS Inspector provides reports on where there are configuration issues in your cloud resources.



```
        "EC2VPC4VVYE": {
            "Type": "AWS::EC2::VPC",
            "Properties": {},
            "Metadata": {
                "AWS::CloudFormation::Designer": {
                    "id": "60123537-da6e-4f6a-84bb-46f5e3ce60fa"
                }
            }
        },
        "ELBV2LB4SMIL": {
            "Type": "AWS::ElasticLoadBalancingV2::LoadBalancer",
            "Properties": {},
            "Metadata": {
                "AWS::CloudFormation::Designer": {
                    "id": "40f8fbf9-268f-4810-840a-02ef4d6dfd90"
```



```
resource "aws_s3_bucket" "b" {
  bucket = "my-tf-test-bucket"
  acl    = "private"

  tags {
    Name        = "My bucket"
    Environment = "Dev"
  }
}
```

adinermie.com

Denial of Service/Resilience

Availability Zones & Regions - Natural Disasters

AWS Shield - DDoS

Load balancers

Amazon CloudFront - CDN

Authentication

Identity and Access Management

Request details:

- Principle - authenticated person or application making request
- Resources - what resource (sometimes specifically
- Actions - what you are doing to the resource
- Environment data - IP address, user agent, SSL, time

AWS checks checks these against policies:

- Identity-based policies
- Resource-based policies
- IAM permissions boundaries
- AWS Organizations service control policies
- Session policies

The request is only fulfilled if there is no policy to deny it. There are explicit allow/deny policies that override other decisions. If these conflict the request is denied.

Authentication

Protect your account:

- Strong password
- Use 2FA (can be enforced as policy)

Protect root:

- Create an administrative user and assign administrative access
- Don’t login - most things don’t require root
- https://docs.aws.amazon.com/accounts/latest/reference/root-user-tasks.html

API keys:

- Keep repositories private unless needed if likely to contain keys
- Automatic repository scanner with key invalidation (many services require opt in)
- Key management to keep keys out repositories (prevents accidental disclosure and follows ACLs)

Organisation

Listed ownership of resources:

- Clearly stored
- Accessible
- Backup contact

When deploying systems or client applications:

- Ensure test credentials are removed for minimal application specific keys
- Replace any services, resources or files used for development or testing

Onboarding/Offboarding:

- Clear steps following SOP
- Only give what is required
- Integrate into an RBAC system to minimise mistakes

Final Extra Resources

AWS Best Practices

- https://aws.amazon.com/blogs/security/getting-started-follow-security-best-practices-as-you-configure-your-aws-resources/
- https://aws.amazon.com/architecture/security-identity-compliance/

Configuring IAM:
https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

CloudWatch:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch_architecture.html

Using CloudFormation:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/GettingStarted.Walkthrough.html

Guide to Availability Zones:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

Configuring Account / Organisation Policies:
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies.html

Encrypting S3:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingEncryption.html

Upcoming Sessions

What's up next?

www.shefesh.com/sessions

21/11/22 - Networking

28/11/22 - Hack the Box

05/12/22 - Christmas CTF

Any Questions?

www.shefesh.com

Thanks for coming!