

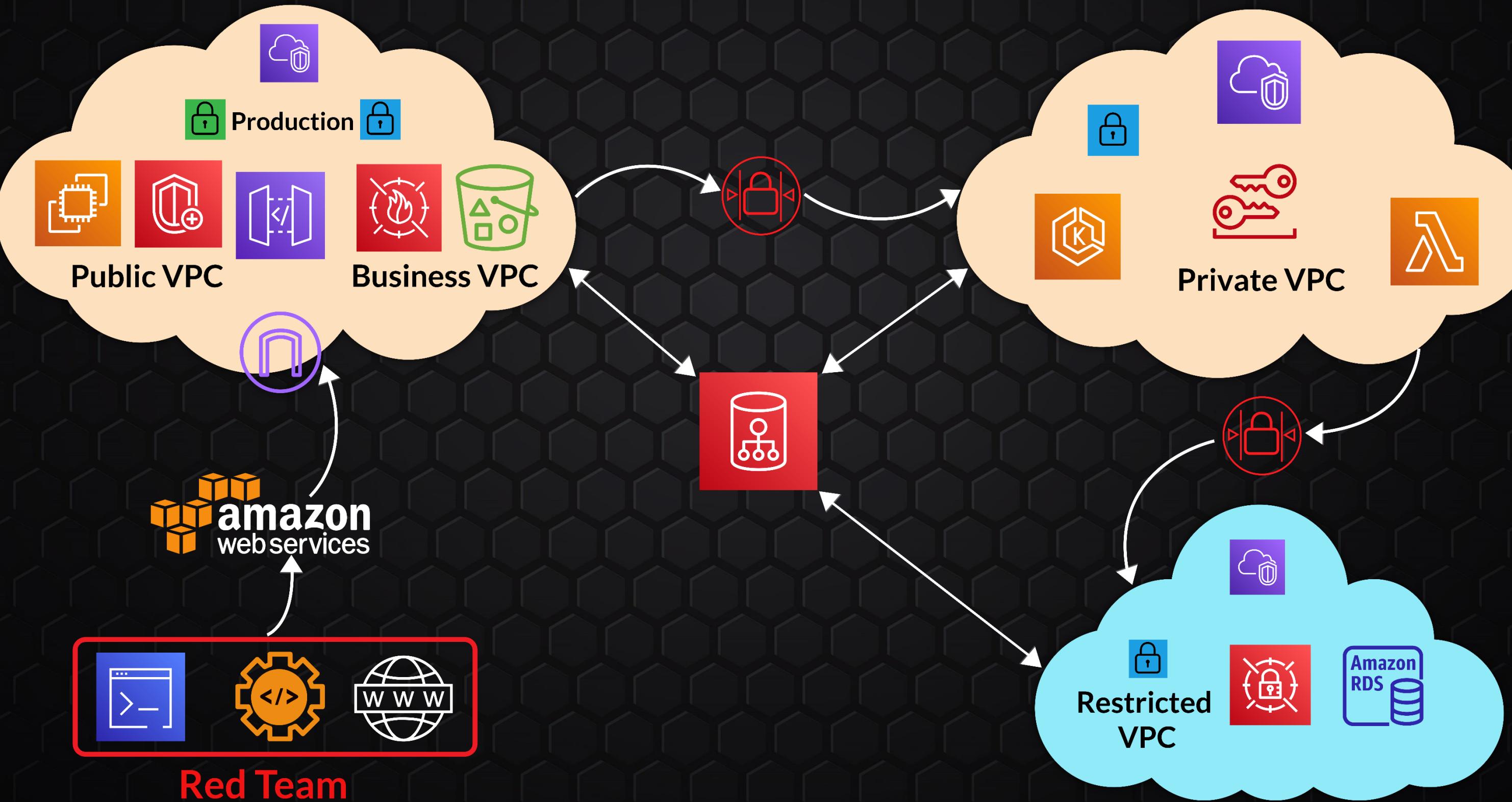


Certified AWS Cloud Red Team Specialist [CARTS]



@CyberWarFare Labs

Certified AWS Cloud Red Team Specialist Architecture



INTRODUCTION TO AWS RED TEAM SPECIALIST

Module 1

Introduction to AWS Cloud

1.1 AWS Cloud Overview

1.2 Classification of AWS Cloud Bases of Service Models

1.3 Classification of AWS Cloud Bases of Service Uses

Module 2

AWS Cloud Services Functionalities & Exploitation

2.1 Introduction about IAM

2.2 IAM Components Explanations

A. Users

B. Groups

C. Roles

D. Policies

a. Managed Policy

I. AWS Managed Policy

II. Customer Managed Policy

b. Inline Policy

E. Security Token Service (STS)

2.3 Exploitation

A. Enumeration

B. Initial Access

C. Persistence

D. Privilege Escalation

E. Credential Access

Module 3

Virtual Private Cloud (VPC)

3.1 Introduction about VPC

3.2 VPC Components Explanations

- A. VPC**
- B. Subnets**
- C. Routing Tables**
- D. Internet Gateway (IGW)**
- E. NAT Gateway**
- F. VPC Peering**
- G. VPC Endpoints**
- H. Network ACLs**

3.3 Exploitation A. Lateral Movement / Pivoting

Module 4

Elastic Compute Cloud (EC2)

4.1 Introduction about EC2

4.2 EC2 Components Explanation

A. Amazon Machine Image (AMIs)

- AWS AMIs
- Custom AMIs

B. EC2 Instance Access

- SSH
- EC2 Instance Connect
- SSM

C. Security Group (External Firewall)

4.3 Exploitation

A. Initial Access

B. Persistence

C. Credential Access

D. Privilege Escalation

Module 5

Lambda Function

5.1 Introduction about Lambda

5.2 Lambda Components Explanation

A. Lambda Function

B. API Gateway

C. Lambda Invocation / Trigger

- API Gateway
- AWS Services
- Event Source Mapping

5.3 Exploitation

A. Initial Access

B. Credential Access

C. Persistence

D. Privilege Escalation

Module 6 Containers

6.1 Introduction about Containers

6.2 Container Components Explanation

- A. Elastic Container Service (ECS)
- B. Elastic Kubernetes Service (EKS)
- Control Plane
- Nodes
 - EC2
 - Fargate
- C. Container Registry
 - AWS Registry (ECR)
 - Docker Hub
 - Self Hosted Registry

6.3 Exploitation

- A. Initial Access
- B. Persistence
- C. Credential Acces

Module 7

Simple Storage Service (S3)

7.1 Introduction about S3

7.2 S3 Components Explanation

A. S3 Resources

- Buckets
- Objects
- Keys
- Regions

B. S3 Access Policies

- Resource Based Policies
- Public Access
- ACLs – Bucket & Object Level
- Bucket Policies – Only for Bucket Level
- Time Limited URLs
- User Based Policies – IAM

7.3 Exploitation

A. Credential Access

B. Data Exfiltration

Module 8

Relational Database Service (RDS)

8.1 Introduction about RDS

8.2 RDS Components Explanation

A. RDS Authentication Method

- Password Based
- Password + IAM Based
- Password + Kerberos Based

B. RDS Access Restriction

- IAM Level Access Restriction
- Network Level Access Restriction

C. RDS Proxy

8.3 Exploitation

A. Credential Access

B. Data Exfiltration

Module 9

Elastic Block Store (EBS)

9.1 Introduction about EBS

9.2 EBS Components Explanation

- A. Volumes**
- B. Snapshots**
- C. Encryption**

9.3 Exploitation

- A. Credential Access**
- B. Data Exfiltration**

Module 10

Secret Manager

10.1 Introduction about Secret Manager

10.2 Secret Manager Components Explanation

A. Secret Manager

B. Key Management Server (KMS)

- AWS KMS Key
- Customer Master key (CMK)

10.3 Exploitation

A. Credential Access

Module 11

Single Sign on (SSO)

11.1 Introduction about SSO

Module 12

AWS Security Services

- 12.1 AWS CloudTrail
- 12.2 AWS Shield
- 12.3 AWS Web Application Firewall (WAF)
- 12.4 AWS Inspector
- 12.5 AWS GuardDuty

Red Team Operations in AWS Cloud Environment

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Credential Access
- Discovery
- Lateral Movement
- Data Exfiltration



Thank You

Cyberwarfare.live

