Red Team 2.0: Adapting Traditional Red Team to Cloud (AWS) Red Team

// Hack Space Con 2023

HALBORN

aws sts get-caller-identity

@carlospolopm

// CARLOS POLOP

- **Cloud, Infra & WebApp Team Lead in Halborn.**
- **Pentester/Red Teamer. Several Certifications.**
- **Captain of the Spanish team in ECSC2021 & member of the Team Europe in ICSC2022.**
- **Author of Hacktricks & PEASS-ng.**

Índice

Cyber Kill Chain

1- Enumeration

2 Exploitation

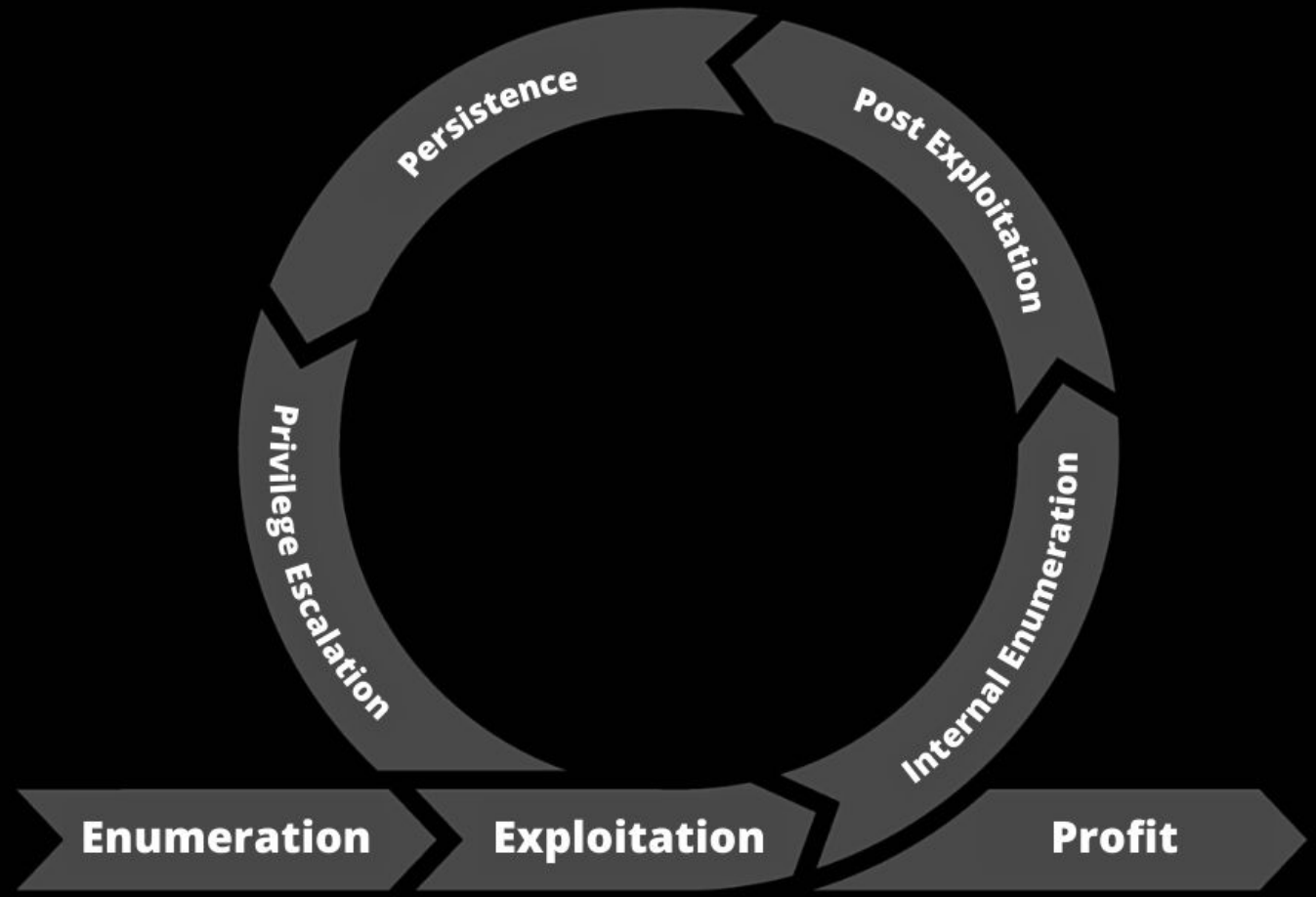
3- Internal Enumeration

4- Post exploitation

5- Persistence

6- Privilege Escalation

7- Profit



Discovery & Enumeration

- OSINT
  - Github Leaks
- Open Buckets
  - Spidering
  - Brute-Force
- Open ports
  - Exploits
  - Brute-Force credentials
- Web
  - SSRF
- Public AMIs, EBS Snapshots, RDS Snapshots
- Roles & Usernames enumeration
- Cognito Credentials
- Federated Identities

Attack: We found some Cognito misconfiguration

Exploitation

- **OSINT**
  - **Github Leaks**
  - **https://book.hacktricks.xyz/generic-methodologies-and-resources/external-recon-methodology/github-leaked-secrets**
- **Open Buckets**
  - **Spidering**
  - **Brute-Force**
  - **https://cloud.hacktricks.xyz/pentesting-cloud/aws-pentesting/aws-unauthenticated-enum-access/aws-s3-unauthenticated-enum**
- **Open ports**
  - **Exploits**
  - **Brute-Force credentials**
- **Web**
  - **SSRF**
  - **https://book.hacktricks.xyz/pentesting-web/ssrf-server-side-request-forgery/cloud-ssrf**
- **Public AMIs, EBS Snapshots, RDS Snapshots**
  - **https://cloud.hacktricks.xyz/pentesting-cloud/aws-pentesting/aws-unauthenticated-enum-access/aws-ec2-unauthenticated-enum**
- **Roles & Usernames enumeration (demo)**
- **Cognito Credentials (demo)**
- **Federated Identities**

Attack: We got Cognito credentials

Internal Enumeration

- Console (web)
- Steampipe
  - https://github.com/turbot/steampipe-mod-aws-perimeter
  - https://github.com/turbot/steampipe-mod-aws-insights
- AWS cli
- Current privileges BF (demo):
  - https://github.com/carlospolop/bf-aws-permissions
  - https://github.com/carlospolop/aws-Perms2ManagedRoles
  - https://github.com/carlospolop/bf-aws-perms-simulate
  - https://github.com/carlospolop/Cloudtrail2IAM
  - https://github.com/carlospolop/tfstate2IAM
  - https://github.com/carnal0wnage/weirdAAL
  - https://github.com/andresriancho/enumerate-iam

Attack: We found interesting privileges

IAM Privilege Escalation

- HackTricks has hundreds of documented permissions that can be used to escalate privileges:
  - https://cloud.hacktricks.xyz/pentesting-cloud/aws-pentesting/aws-privilege-escalation
- iam:CreateAccessKey (demo)

Attack: We escalated to Administrator

Internal Enumeration

- IAM recon (demo)
  - https://github.com/carlospolop/aws_sensitive_permissions
- Org recon (demo)

Attack: We found children accounts

Org Compromise

- By default the Management Account has Admin permissions on child accounts through the OrganizationAccountAccessRole role. (demo)
  - https://cloud.hacktricks.xyz/pentesting-cloud/aws-pentesting#compromising-the-organization

Attack: We moved to Administrator in a child account

Post exploitation

- **Confused Deputy**
  - https://cloud.hacktricks.xyz/pentesting-cloud/aws-pentesting/aws-post-exploitation/aws-iam-post-exploitation
- **Steal Lambda Requests**
  - https://cloud.hacktricks.xyz/pentesting-cloud/aws-pentesting/aws-privilege-escalation/aws-lambda-privesc/aws-warm-lambda-persistence
- **Get Console Access (demo)**
- **Stealing credentials from Code Build (demo)**

Attack: We obtained a sensitive token to access Github

Persistence

- **Secrets Rotation Lambda**
  - **https://cloud.hacktricks.xyz/pentesting-cloud/aws-pentesting/aws-persistence/aws-secrets-manager-persistence**
- **Lambda Layers Persistence**
  - **https://cloud.hacktricks.xyz/pentesting-cloud/aws-pentesting/aws-persistence/aws-lambda-persistence/aws-lambda-layers-persistence**
- **Backdoor Role Trust Policies**
- **Role Chain Juggling (demo)**

Attack: We set some persistence

“Profit”

- Crypto mining
- Dump everything
- Kill everything (DoS)
- Change KMS keys - Ransomware
  - Or give yourself access to the clients KMS keys and remove it from him (--bypass-policy-lockout-safety-check)

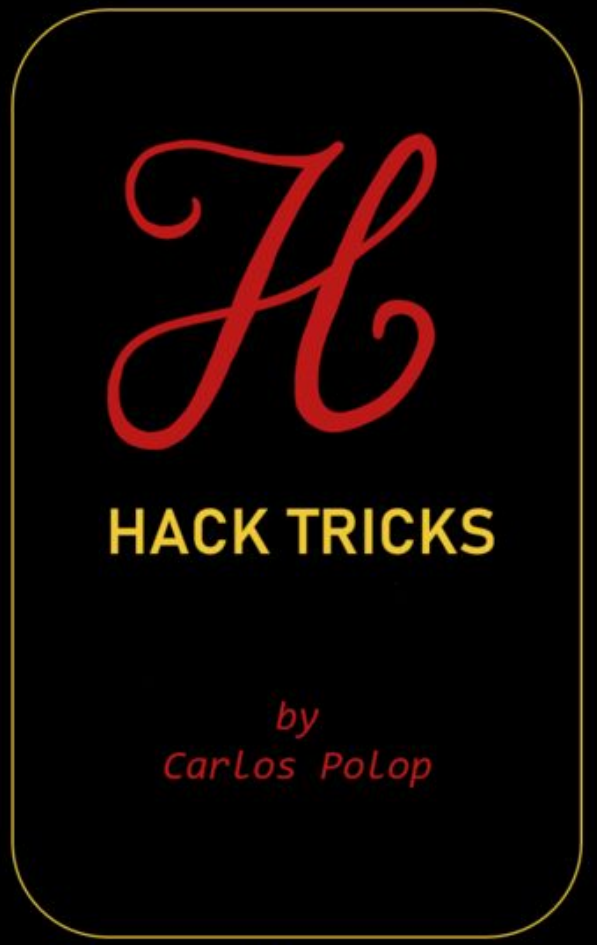
I don’t support doing any of these things without permission, neither I recommend it!

Want to learn more??

HackTricks Team is preparing Cloud Red Team certifications.

Follow me in twitter or linkedin for updates.

The first one, HackTricks AWS Red Team Expert (HackTricks ARTE), on presale next month.



*Use responsibly

¡Thank You!

Carlos Polop

HALBORN