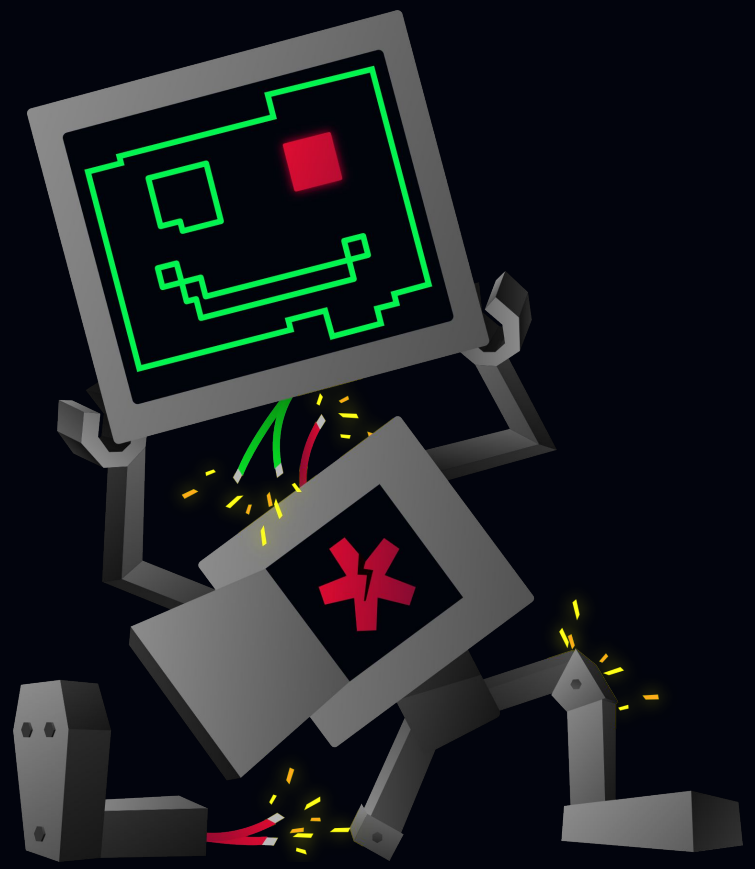
THE H@CK SUMMIT

C:\>

Entering the Cloud Kingdom with keys from Webapps



Karan Raheja
Senior Security Engineer, Razorpay
@5h4d0w_hun73r1, github/cryptic-hunter

Simardeep Singh
Network Engineer, Hughes Systique
github/tombstoneghost

thehacksummit.com

19-20/10/2023

PGE Narodowy
+ Online

ORGANIZERS:

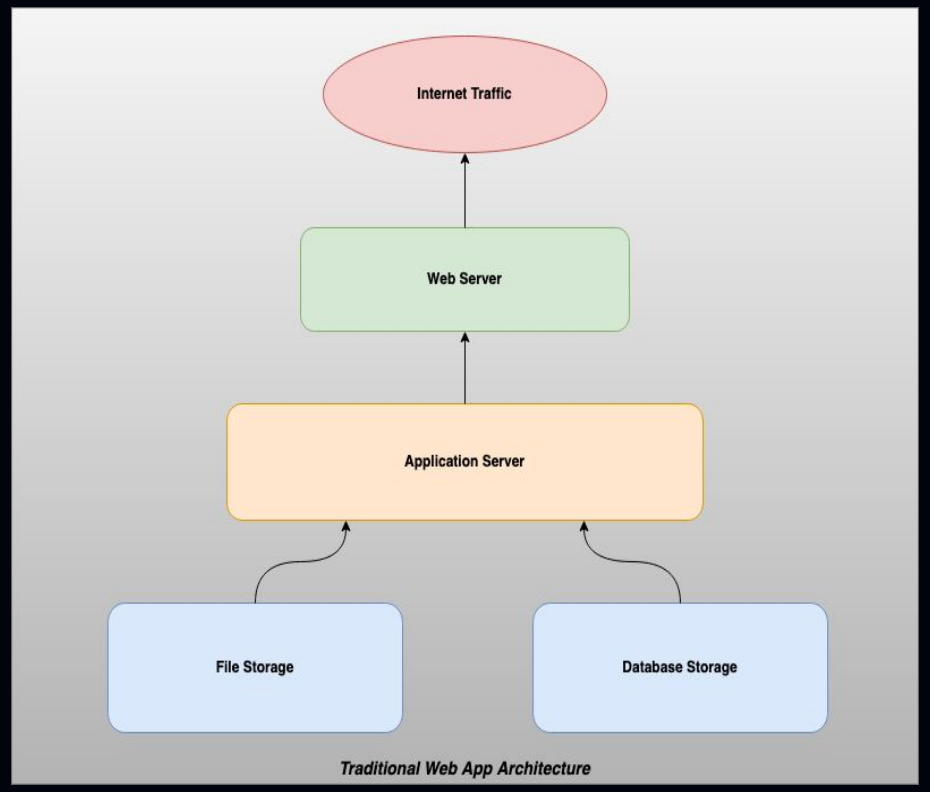
ACADEMIC PARTNERS

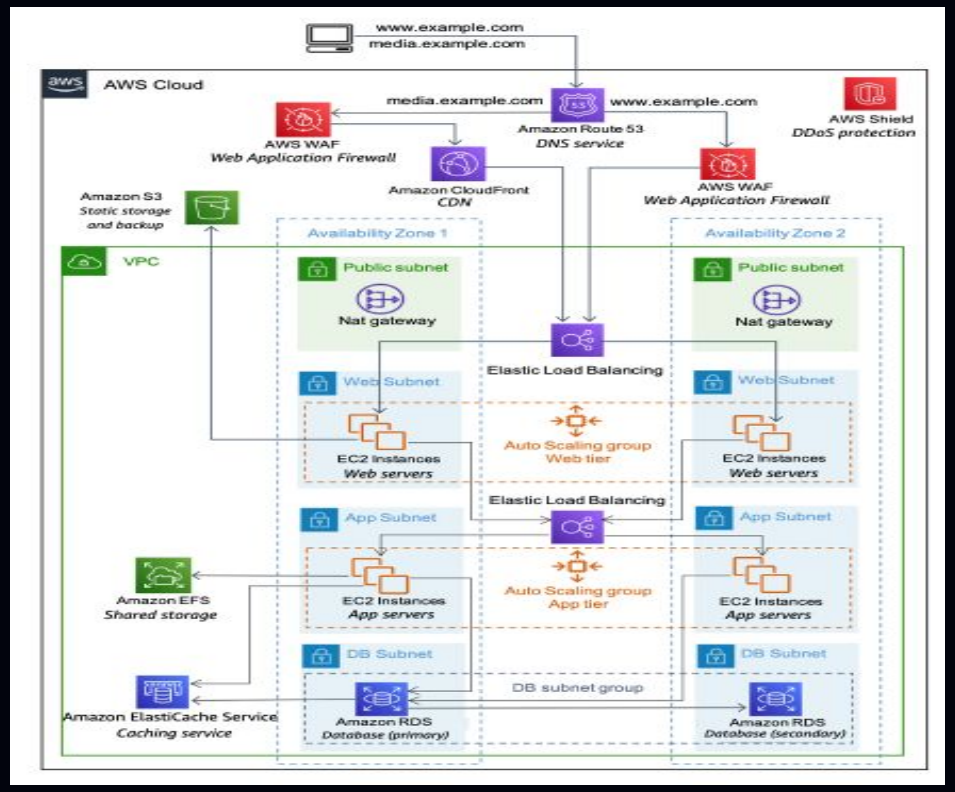
speaker1> whoami
output> Karan Raheja \
4+ years experienced in IT Security \
Security @ Razorpay, worked for multiple clients from different domains in the past \
Mostly working on Web, Cloud and Network Security

speaker2> whoami
output> Simardeep Singh \
Network Automation @ HSC, automating tasks and building secure APIs, dashboards for NOC.
Mostly working on Web, Cloud and Network Infra.

THE H@CK SUMMIT

Traditional Web App vs Cloud Hosted Web Apps

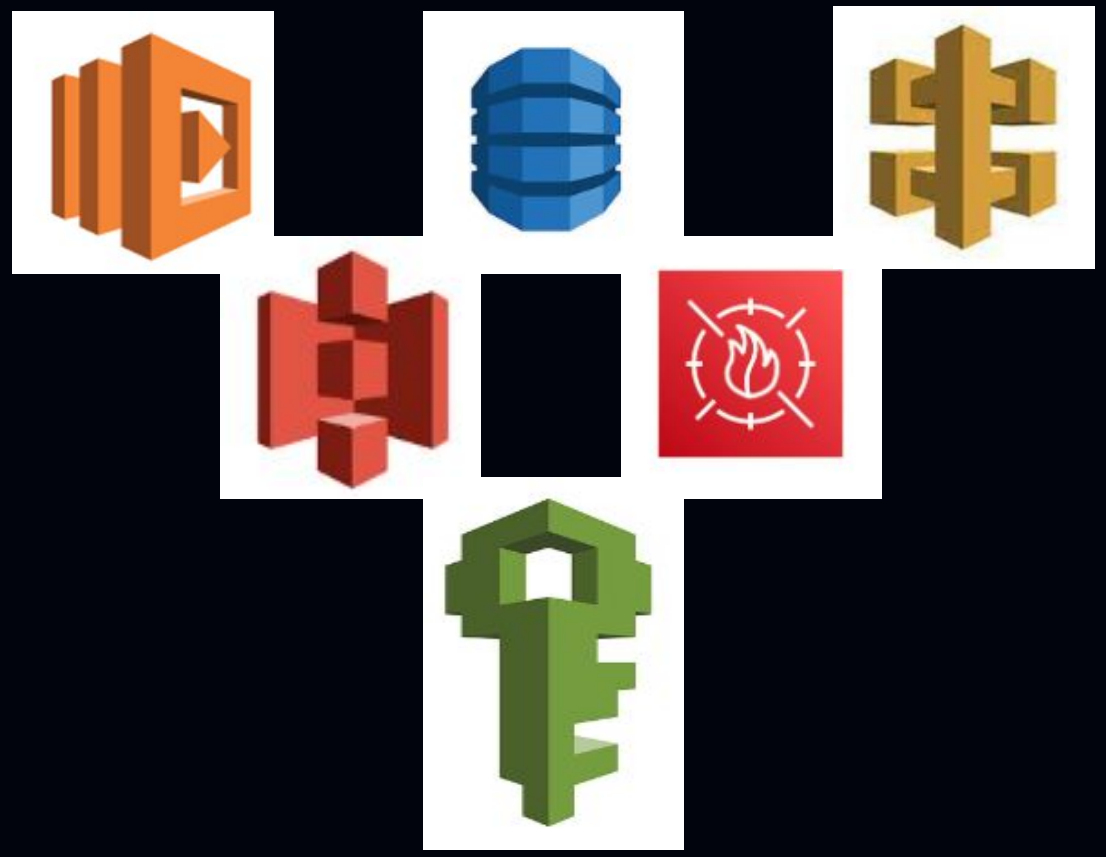




THE H@CK SUMMIT

Web Application Stack - AWS

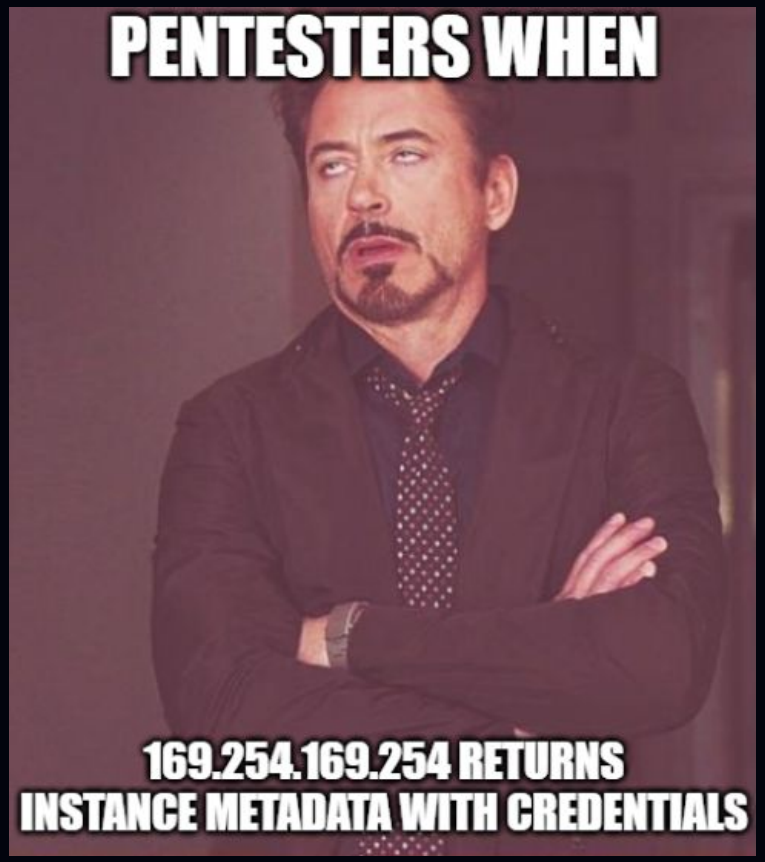
- ★ AWS EC2
- ★ AWS S3
- ★ AWS DynamoDB/RDS/Aurora
- ★ AWS WAF
- ★ AWS IAM/AWS Cognito
- ★ AWS API Gateway/Route53
- ★ AWS CloudFormation
- ★ AWS Cloudwatch
- ★ .....



THE H@CK SUMMIT

Web Application Vulnerabilities

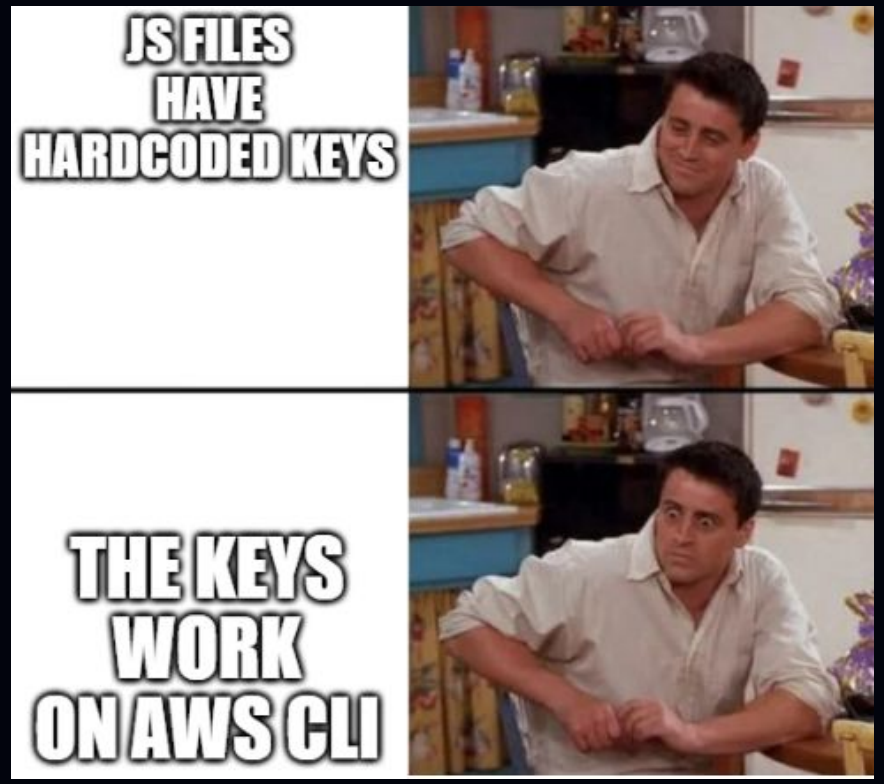
- ★ SQL Injection
- ★ Server Side XSS
- ★ XML External Entities
- ★ Server Side Template Injection
- ★ Server Side Request Forgery
- ★ Remote Code Execution
- ★ Insecure Deserialization
- ★ API Misconfigurations



THE H@CK SUMMIT

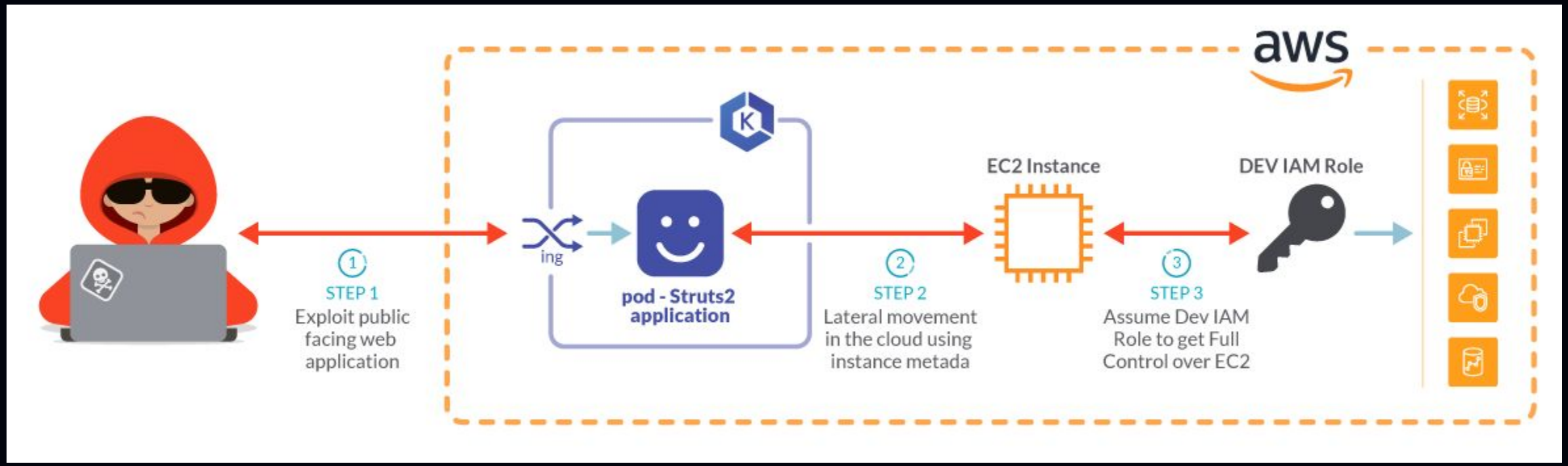
Gaining Access to the kingdom

- ★ Vulnerable Application running on kubernetes inside AWS environment
- ★ Static files/resources associated with web applications.
- ★ Web Application Vulnerabilities such as SQLi, XXE, SSRF, SSTI etc.
  - ✓ Includes applications running on lambda
- ★ Supply Chain, because, we are living in open-source world!
- ★ Misconfigured IAM and Role Policies



THE H@CK SUMMIT

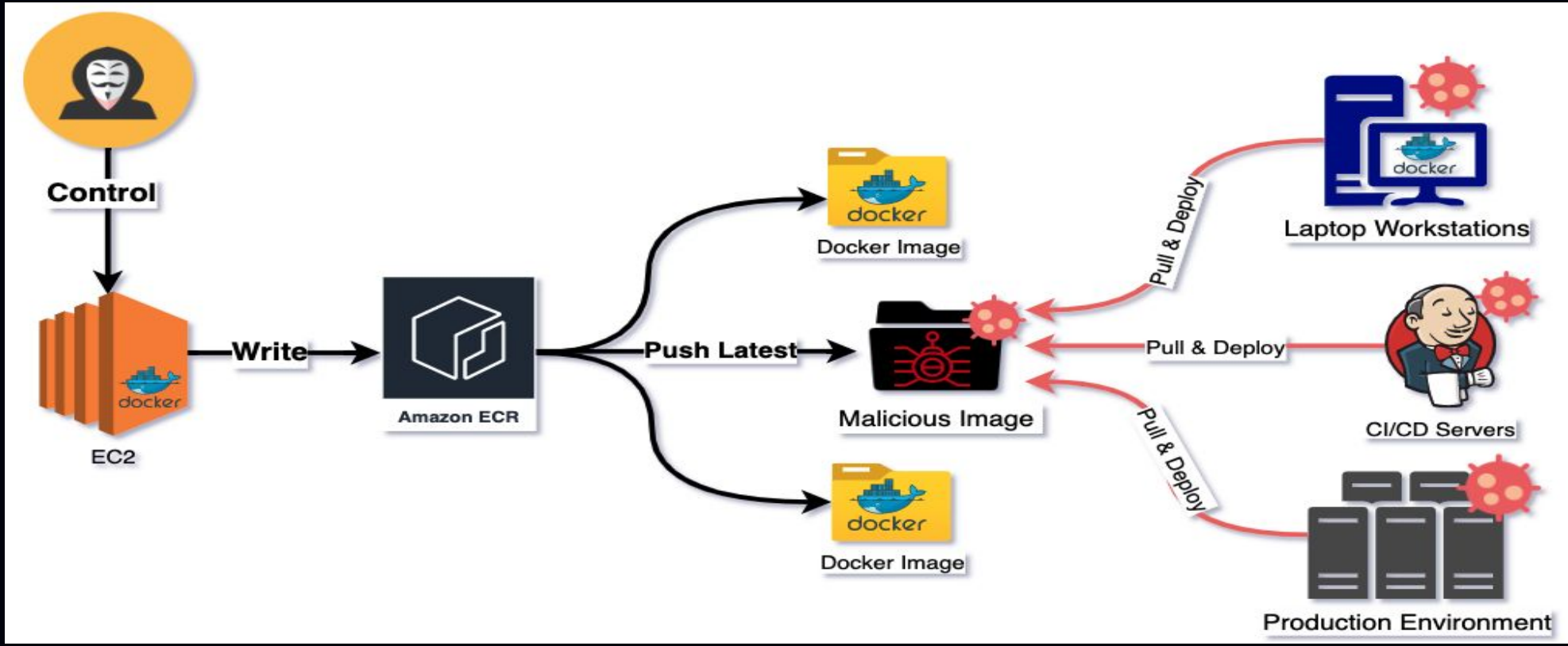
Gaining Access to the kingdom - Webapp -> K8s -> AWS -> 1337



https://sysdig.com/blog/lateral-movement-cloud-containers/

THE H@CK SUMMIT

Gaining Access to the kingdom - Webapp -> ECR -> AWS -> 1337



THE H@CK SUMMIT

Traditional Web Application Attacks:

Slides about the Web Application attacks in on-prem infrastructure and the damage caused by them.

Added risk factor

- Lateral Movement (VPC Configuration) (trust required)
- Data Exfiltration
- Persistence/Backdoors/CryptoMiners
- DDoS Amplification/Resource Exhaustion
- Privilege Escalation

Lateral Movement

- Cross Account Roles
- Recon for further network movement - requires some kind of trust
  - Can enumerate networks with readonly role
- AWS Organizations compromise
- IAM Permissions Abuse
- AWS EC2 IAM Instance Profiles
- AWS SSM exploitation

THE H@CK SUMMIT

Data Exfiltration

THE H@CK SUMMIT

Persistence/Backdoors

THE H@CK SUMMIT

DDoS Amplification/Resource Exhaustion

Privilege Escalation

- Vertical Privilege Escalation - A user role above current privileges
- Lateral Privilege Escalation - An identity accessing functions/resources reserved for other identities

THE H@CK SUMMIT

APT Actors in action

TeamTNT Continues Attack on the Cloud, Targets AWS Credentials

While investigating the team's activities, we found a binary containing a hardcoded shell script designed to steal AWS credentials, which provided us a lead on the scope of the attack.

HOW CYBER CRIMINALS ARE HACKING INTO AWS FARGATE, EKS & EVADING CLOUDTRAIL LOGS DETECTION

Scarleteel Cloud Attack: Hackers Use Kubernetes and AWS to Steal Source Code

Researchers warn Amazon's AWS System Manager agent can be used as a RAT

Cryptominer Found Embedded in AWS Community AMI

Old Services, New Tricks: Cloud Metadata Abuse by UNC2903

THE H@CK SUMMIT

Exploiting Fargate for Crypto Profits

thehacksummit.com

19-20/10/2023

PGE Narodowy
+ Online

ORGANIZERS:

ACADEMIC PARTNERS

Moving to the demos.

THE H@CK SUMMIT

Exploiting Lambda Function to gain RCE

THE H@CK SUMMIT

SQLi on RDS Database

THE H@CK SUMMIT

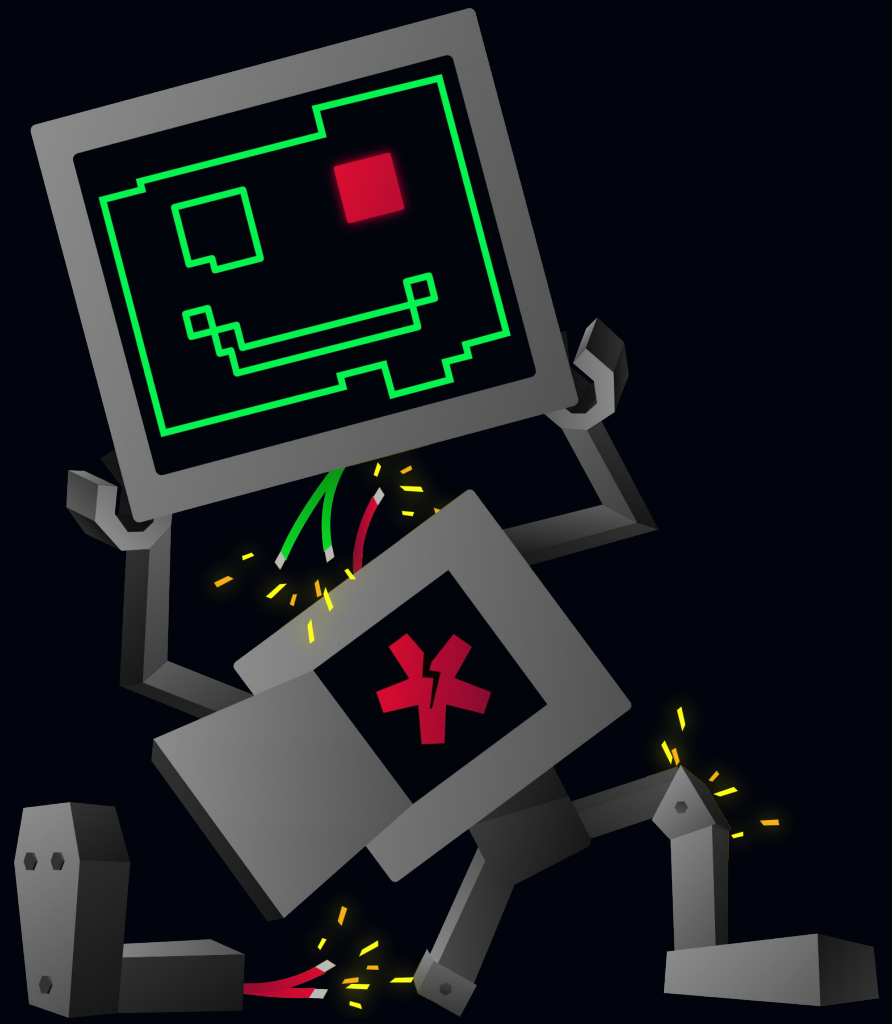
SSRF on Web App hosted on EC2

THE H@CK SUMMIT

Defending web applications hosted on Cloud

- Implement IMDS v2
- Maintain the list of dependencies of your application. (3rd Party / Open Source)
- Conduct regular security assessments for the applications deployed on cloud.
- Always configure all AWS resources and policies with the Principle of Least Privileges.
- Maintain a regular check on the AWS Security Hub Reports

THE H@CK SUMMIT



Thank you for watching!

Remember to leave your questions and rate the presentation in the section below.

thehacksummit.com

19-20/10/2023

PGE Narodowy
+ Online

ORGANIZERS:

ACADEMIC PARTNERS

THE H@CK SUMMIT

Reach out to the speakers

Karan Raheja:
LinkedIn:
https://www.linkedin.com/in/karan-raheja-796015110/

Simardeep Singh:
LinkedIn:
https://www.linkedin.com/in/simardeepsingh99/