

# DEV SEC OPS

DOMINIK



# NARZĘDZIA DO AUDYTU SECURITY

## AWS GOAT - SYSTEM DO TESTOWANIA

- 1) POTRZĘBUJEMY TERRAFORM
- 2) GIT CLONE LINE-LABS/AWS-GOAT.GIT
- 3) TERRAFORM INT
- 4) TERRAFORM APPLY

PMAPPER - STOSY DO SPRAWDZENIA, CZY  
JAKIS USERDOWNNIU NIE MOŻE WYSKACZOWAĆ  
SWOICH UPRAWNIEN DO POLICJI AŁO ROLI ADMINA

- 1) PIP INSTALL PRINCIPALMAPPER
- 2) AWS CONFIGURE

Zadanie	Komenda
Pobranie danych IAM z AWS	pmapper aws-fetch
Stworzenie grafu IAM	pmapper graph create
Sprawdzenie, kto może zostać administratorem	pmapper query "Who can assume Administrator role?"
Sprawdzenie, kto może tworzyć role	pmapper query "Who can create roles?"
Sprawdzenie, kto może przekazywać role (PassRole)	pmapper query "Who can call iam:PassRole?"
Sprawdzenie, kto może eskalować swoje uprawnienia	pmapper query "Can user user123 escalate privileges?"
Sprawdzenie, kto może modyfikować polityki IAM	pmapper query "Who can modify policies?"
Wizualizacja IAM w terminalu	pmapper visualize
Eksport wyników do JSON (dla Viz)	pmapper visualize --format json > iam_permissions.json

VIZ - WIZUALIZACJA ŚCIĘZEŃ ATAKU, DODAĆ DO PMAPPER

## PROWLER

AWS CONFIGURE - USTAWIENIE DOMYŚLNEGO CONFI  
AWS STS GET-CALLER-IDENTITY

PROWLER - P DEFAULT  - M HTML - O NAZWA

NAZWA UŻYTKOWNIKA

DO SKANUJEMY - BOSTE CYCŁI WSLYSIDŁO  
- SERVICE IAM

ROZSZERZENIE PLIKU WYJĘCIOWEGO

- HTML
- CSV
- JSON-ASTF - DZIAŁA INFO
- JSON-OCFS - LATWIEJSZY DO EKSPANIA

NAZWA PLIKU WYJĘCIOWEGO

# POSTĘPNE ZAGROŻENIA

## CHMURA

- \* NIEAUTORYZOWANY DOSTĘP - KTOŚ PREZYTAT NAJĘ W KONTO ADMINA - MFA, LEAST PRIVILEGE
- \* PUBLICZNY DOSTĘP DO DANYCH - S3 LUB RDS SA PUBLICZNE - UŻYWANIE VPC, AWS SECRET MANAGER
- \* PRZECIHWYTAWANIE RUCHU - NIESZYFROWANE DANE MOGĄ BYĆ PODSTYCHANE - HTTPS CZYLI CERTYFIKATY, ENCRYPTION W RDS
- \* BRAK KOPII ZAPASOWYCH - BEZDŁ CZELOWEKA - BACKUPS, SNAPSHOT
- \* WŁI W KONFIGURACJI - BEZDŁ KONFIGURACJA - SLANY MAŁY I INNYMI NARZĘDZIAMI

## CICD

- \* KONTROLA DOSTĘPU DO JENKINS ITP - MFA, LEAST PRIVILEGE
- \* OCHRONA KWCZY - AWS SECRET MANAGER
- \* ANALIZA KODU - SONAR QUBE
- \* BEZ PIECZNE KONTENERY - POPPIŚYWANIE OPERAŻÓW, WŁOŻYSKIAMIĘ 2 AUTORYZOWANYCH
- \* LOGI

CLOUD TRAIL - STUŻY DO MONITOROWANIA  
DZIAŁAŃ W DARMOWA

SECURITY HUB - KONTROLA Z DANYCH MONITO-  
Ringu, GENEROWE ALERTY

# INTERVIEW

## 1) NADWAŻNIE ŚŁÓW ZASADY:

- TESTY DAWINNY BYCĘ YAN NAJWŚZOSZYJĄ
- AUTOMATYZACJA CIĄGŁOŚĆ TESTÓW
- LEASE PRIVILEGE & ZERO TRUST
- CIĄGŁE MONITOROWANIE I REAKCYA
- WSZYSTKI ODPOWIADAJĄ ZA PRZECIĘNIŚTWO

## 2) LIFE CYCLE KODU

PROGRAMISCI PISIAJĄ KOD - SAST / SCA  
CI/CD - SAST, DAST, SCA, CONTAINER SCANNING  
TESTOWANIE APLIKACYJ - DAST, IAST  
WDRÓŻENIE NA PRODUKCJĘ - RASP, WAF, COGS,  
SIEM

DEVELOPMENT  
SAST, SCA

MONITORING  
SIEM, THREAT INTELLIGENCE

BUILD & CI/CD  
DAST, CONTAINER SCAN

DEPLOYMENT  
RASP, WAF

PRE-DEPLOYMENT  
IAST, FUZZING

SAST - ANALIZA KODU ZRODŁOWEGO  
SDNAR QUBĘ

SCA - ANALIZA BIBLIOTEK

DAST - TESTY DYNAMICZNE

IAST - ANALIZA APLIKACJI W TRAKCIE  
DZIAŁANIA

RASP - DZIAŁAJSĄCY AGENT, KTÓRY WYSWIETLA  
I USUWA ZAGROŻENIA

WAF - FILTRUJĄCY RUCH HTTPS

SIEM - CLOUD TRAIL

THREAT INTELLIGENCE + SECURITY HUB

3) REAKCJA NA WYKRYCIE INCYDENTU

- KRYTYCZNOŚĆ
- ZŁOŻECZO
- SAKA CZĘŚCI CPKLU - DOKUMENT (PP.)
- IZOLACJA
- ODŁĘCIE OD NIECZYSTYCH ZASOBÓW
- KOREKCJA
- ANALIZA i PREZENCIOWANIE RÓWNOKI

# 6) KOMPLETNY MODEL ZAGROŻEŃ

- PREGAŁ DYSKONU - JAKIE APLIKACJE  
DANEG CHRONIĘ
- DIAGRAM PRZEPŁYWU DANYCH - JAK APLI-  
KACJA KOMUNIKUJE SIĘ Z INNYMI SYSTEWA-  
MI
- LISTA ZAGROŻEŃ - STRIDE
- OCENA RYZYKA - PREAD
- SPRAWNI ZARAPCZE
- TESTOWANIE + CI/CD SECURITY
- MONITOROWANIE + REAKCJA

S - POISZKIWAŃIE SIE  
T - MANIPULACJA DANYMI  
R - BRAĆ WOGÓW  
I - WYCIOUJ DANYCH  
O - ODOB  
E - PODNIESIĆ MIE UPRAWNIEŃ

D - JANIE SŁUPODY WYRZĄDZI, A JAK  
R - JAN TATTO MOŻNA GO PAMIĘTAĆ  
E - JAN TATTO MOŻNA GO WYSKRYSIĄC  
A - W OŚPIEWNIAŃ DORYCZY  
O - JAN TATTO A JAKUSZCI MĄDREĆ CÓW

5) RÓŻNICA POMIEDZY SKAKOWANIEM  
PODAJNOŚĆĄ TESTAMI, PENERACYJĄ I M/  
SŁAN PODAJNOŚCI - SPRAWDZA WĘDUG  
ZALECENI - BIBLII CIS

TESTY PENERACYJNE - REALNY A İAD DLA  
SPRAWDZENIA

6) HASŁOWANIE A SZYFROWANIE

HASŁOWANIE - GENERUJE CIĄG Znaków,  
KTÓRY BĘDZIE 2AWSZI SAMOCZAIĆ JEGO  
WARTOSCI, NASTĘPMIE JEGO PACZUNKU

SZYFRANIE - 2 KŁUCZE DO SZYFRUWAŃIA  
I ODSZYFROWANIA

7) JAK ZABEZPIECZYĆ KONTENERY

- SKANOWANIE PODATNOŚCI

- UŻYWAĆ NIE ROOT

- UŻYWAĆ RODZIAŁ NA SECJĘ

- AWS SECRETS MANAGER

- MONITOROWANIE W CZASIE RZECZYWISTYM

- POLITYKI BĘDZIĘCZEŃSTWA

- AUTORIZACJA I ROZACZĄ

8) BĘDZIĘCZEŃSTWO DANYCH AT REST  
IN TRANSIT (PRZESYŁKI)

IN REST - SZYFROWANIE

IN TRANSIT - TLS (HTTPS)

8) TCP A UDP

TCP - POCZTOWE - EMAIL, STRONY WIELKIE

UDP - BĘDZIĘCZNIAWE, SŁYBSZE - FILMY, GRY, VIDEO

LINUX

APROPOS

>

>>

LINUX