

2024.03.05 클클 5기 시즌1 스터디 소개

클라우드 보안 스터디

CloudGoat 실습

목차

a table of contents

1

스터디 개요

2

CloudGoat 간단 소개

3

CloudGoat 컨트리뷰션 후기

STEP 1 정해진 시나리오 실습해와서 랜덤 뽑기로 1명이 발표하기

* 3주차부터 이전 2번의 스터디에서 발표했던 사람은 제외하고 랜덤 뽑기함



STEP 2 발표를 듣고 궁금한 점이나 다 같이 이야기해보고 싶은 거 Q&A



STEP 3 클라우드 보안 관련 내용 저번 주에 정한 1명이 발표하기 (5~10분)

* 다음 주에 하실 분..? 없으면 랜덤 뽑기합니다... / 발표자료 없어도 됨 그냥 노션페이지나 찾은 링크 화면공유하면서 설명하면 됨

예상되는 총 소요시간 **30분** 이내
짧다고 생각하시는 분?

#클라우드 보안 관련 발표 주제

- 클라우드 보안 사고 사례
- AWS 보안 서비스 소개
(ex. Macie, Detective, Shield...)
- 클라우드 보안이랑 온프레미스 보안 차이
- Azure 보안 서비스 소개
- GCP 보안 서비스 소개
- 발표할 거 떨어지면 클라우드 관련 아무거나

#5~7주 중에 1번 쉬는 거 반대하시는 분?

직장인은 관계 없는 이야기긴 한데요...

사실 우리 막학기라 시험 많이 안 보긴 해?

근데 그냥 쉬고 싶어

싫음 말구... 공부하든가... 저는 빼고 ㅎ

**#실습에서 과금 될 수 있음...
미안... 지원해주는 줄 알았음!!**

#빨리 실습하고 삭제하면 거의 안 될 거임...진짜로!

#클클 자금 사정이 안 좋아졌음...T

Q&A

질의 응답 시간

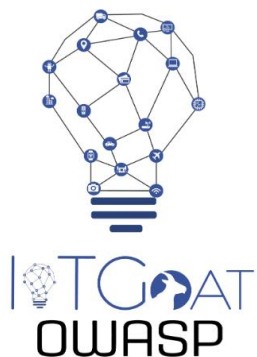
Part 2



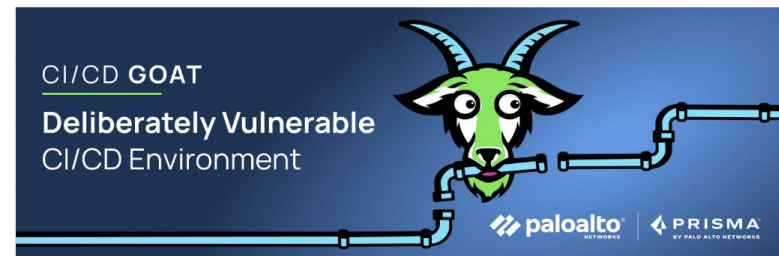
CloudGoat 간단 소개

오픈소스 소개 + 환경 설정 및 실습 진행 방법

Part 2 | CloudGoat 간단 소개



Kubernetes Goat



Goat

일부러 취약한 환경을 구성해서 모의 침투 테스트를 할 수 있도록 하는 도구

* 외국에서는 꽤 알려져 있는 거 같은데 한국에서는...

Part 2 | CloudGoat 간단 소개



리눅스 가상머신 필요



AWS 개인 계정 필요

Part 2 | CloudGoat 간단 소개

 README  BSD-3-Clause license

CloudGoat (🐘🌥️)


 rhino  vulnerable | tool  python 3.6+  license BSD  PRs  welcome

CloudGoat is Rhino Security Labs' "Vulnerable by Design" AWS deployment tool.



Quick reference

- Where to get help: [the Rhino Security Labs Discord](#), or [Stack Overflow](#)
- Where to file issues: <https://github.com/RhinoSecurityLabs/cloudgoat/issues>
- Maintained by: [the CloudGoat Community](#)

 Rhino Security Labs

cloudgoat

CloudGoat is Rhino Security Labs' "Vulnerable by Design" AWS deployment tool. It allows you to hone your clo...

WELCOME

announcements

rules

intros

socials

casual

giveaway-entries

PENTESTING

general

training-certifications

infosec-news

aws-pentest

azure-pentesting

gcp-pentesting

pm-operations

Lounge

RHINO TOOLS

cloudgoat

pacu

other-tools

@Andrew Issue with rds_snapshot seems like it got "merged" and it still has some issues that have not been addressed <https://github.com/>

Tyler R 2023.12.18, 오후 12:00

@John Doe -- Do you have any insight into this?

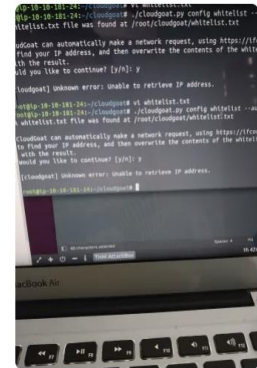
2023년 12월 19일

Do Kyu Park 님이 Issue with rds_snapshot 스레드를 시작하셨습니다(스레드 모두 보기). 2023.12.19, 오전 7:37

2024년 2월 12일

Namita 2024.02.12, 오전 6:48

Hey guys, I'm getting this error. AWS tryhackme cloudpentest Unable to locate ip



I'm not able to configure Solus profile

© 2023. Saebyeol Yu. all rights reserved.

Part 2 | CloudGoat 간단 소개

cloudgoat Public

master 19 Branches 0 Tags

jdearmas Remove publicly exposed by default

.github Refactor/cloud

core Remove public

scenarios Format vulnera

.gitignore Resolve local e

Dockerfile Fix dockerfile's

LICENSE Initial commit

README.md This commit ac

RhinoSecurityLabs / cloudgoat

<> Code Issues 11 Pull requests 14 Actions Security Insights

Files

master + Q

Go to file t

- > .github
- > core
- > scenarios
 - > cicd
 - > cloud_breach_s3
 - > codebuild_secrets
 - > detection_evasion
 - > ec2_ssrf
 - > ecs_efs_attack
 - > ecs_takeover
 - > glue_privesc
 - > iam_privesc_by_attachment
 - > iam_privesc_by_key_rotation
 - > iam_privesc_by_rollback
 - > lambda_privesc
 - > rce_web_app
 - > rds_snapshot
 - > sqs_flag_shop
 - > vulnerable_cognito
 - > vulnerable_lambda
- .gitignore
- Dockerfile
- LICENSE

cloudgoat / scenarios /

andrew-aiken Format vulnerable lambda (#229)

Name

- ..
- cicd
- cloud_breach_s3
- codebuild_secrets
- detection_evasion
- ec2_ssrf
- ecs_efs_attack
- ecs_takeover
- glue_privesc
- iam_privesc_by_attachment
- iam_privesc_by_key_rotation
- iam_privesc_by_rollback
- lambda_privesc
- rce_web_app
- rds_snapshot
- sqs_flag_shop
- vulnerable_cognito

총 17개 중 6개

Part 2 | CloudGoat 간단 소개

아키텍처 크기?

사용되는 서비스의 양? / 난이도

Rarge / Hard

Medium / Moderate

vulnerable_lambda (Small / Easy)

```
$ ./cloudgoat.py create vulnerable_lambda
```

In this scenario, you start as the 'bilbo' user. You will assume a role with more privileges, discover a lambda function that applies policies to users, and exploit a vulnerability in the function to escalate the privileges of the bilbo user in order to search for secrets.

[Visit Scenario Page.](#)

Part 2 | CloudGoat 간단 소개

실습할 시나리오 6개

iam_privesc_by_rollback (Small / Easy)

```
$ ./cloudgoat.py create iam_privesc_by_rollback
```

Starting with a highly-limited IAM user, the attacker is able to review previous IAM policy versions and restore one which allows full admin privileges, resulting in a privilege escalation exploit.

[Visit Scenario Page.](#)

lambda_privesc (Small / Easy)

```
$ ./cloudgoat.py create lambda_privesc
```

Starting as the IAM user Chris, the attacker discovers that they can assume a role that has full Lambda access and pass role permissions. The attacker can then perform privilege escalation using these new permissions to obtain full admin privileges.

vulnerable_lambda (Small / Easy)

```
$ ./cloudgoat.py create vulnerable_lambda
```

In this scenario, you start as the 'bilbo' user. You will assume a role with more privileges, discover a lambda function that applies policies to users, and exploit a vulnerability in the function to escalate the privileges of the bilbo user in order to search for secrets.

[Visit Scenario Page.](#)

iam_privesc_by_key_rotation (Small / Easy)

```
$ ./cloudgoat.py create iam_privesc_by_key_rotation
```

Exploit insecure IAM permissions to escalate your access. Start with a role that manages other users' credentials and find a weakness in the setup to access the "admin" role. Using the admin role, retrieve the flag from secretsmanager.

Contributed by [infrasec.sh](#).

[Visit Scenario Page.](#)

Scenario : SQS_FLAG_Shop

Size: Medium Difficulty: Easy

Command:

```
$ ./cloudgoat.py create sqs_flag_shop
```

Scenario Resources

cloud_breach_s3 (Small / Moderate)

```
$ ./cloudgoat.py create cloud_breach_s3
```

Starting as an anonymous outsider with no access or privileges, exploit a misconfigured reverse-proxy server to query the EC2 metadata service and acquire instance profile keys. Then, use those keys to discover, access, and exfiltrate sensitive data from an S3 bucket.

[Visit Scenario Page.](#)

이번 주에 실습할 시나리오

iam_privesc_by_rollback (Small / Easy)

```
$ ./cloudgoat.py create iam_privesc_by_rollback
```

Starting with a highly-limited IAM user, the attacker is able to review previous IAM policy versions and restore one which allows full admin privileges, resulting in a privilege escalation exploit.

[Visit Scenario Page.](#)

Q&A

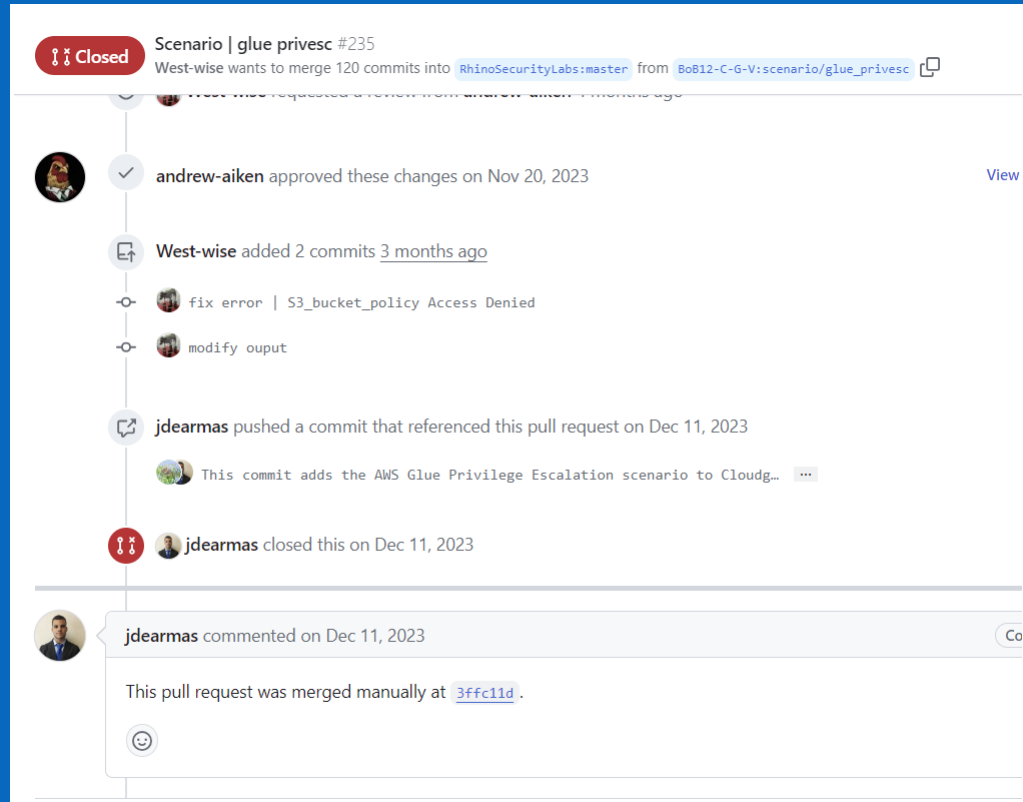
질의 응답 시간

Part 3

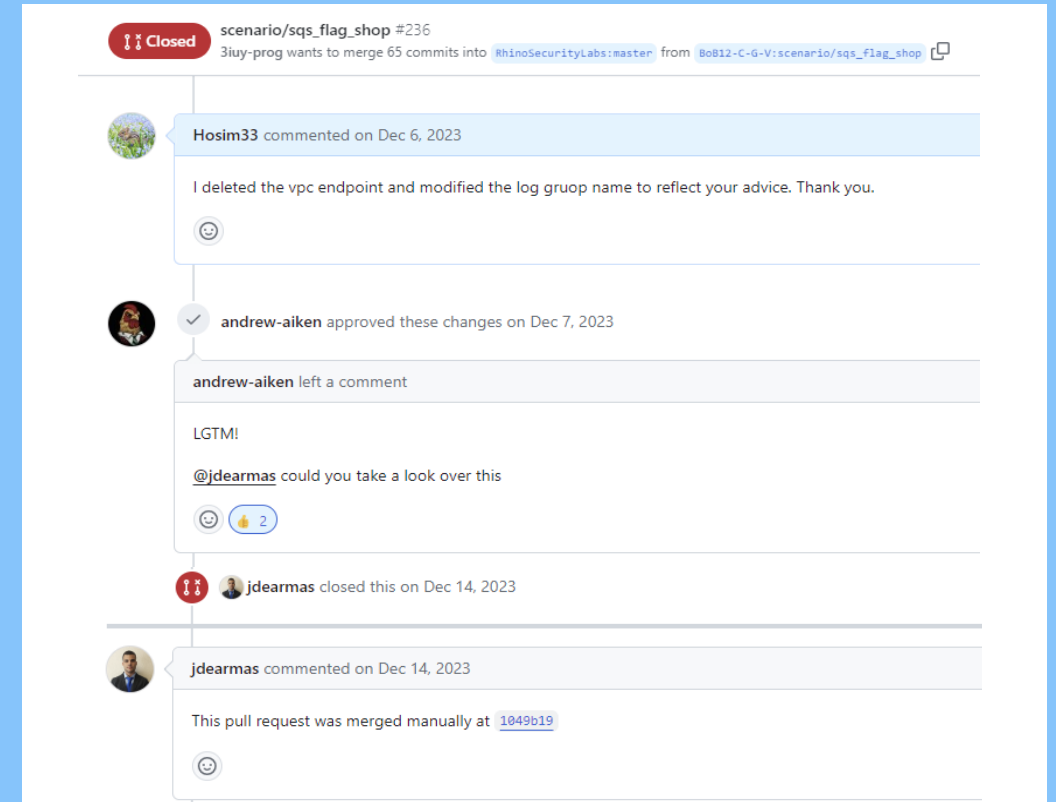
CloudGoat 컨트리뷰션 후기

총 4개의 시나리오를 PR하였고 최종 Merge 3개

Part 3 | CloudGoat 컨트리뷰션 후기

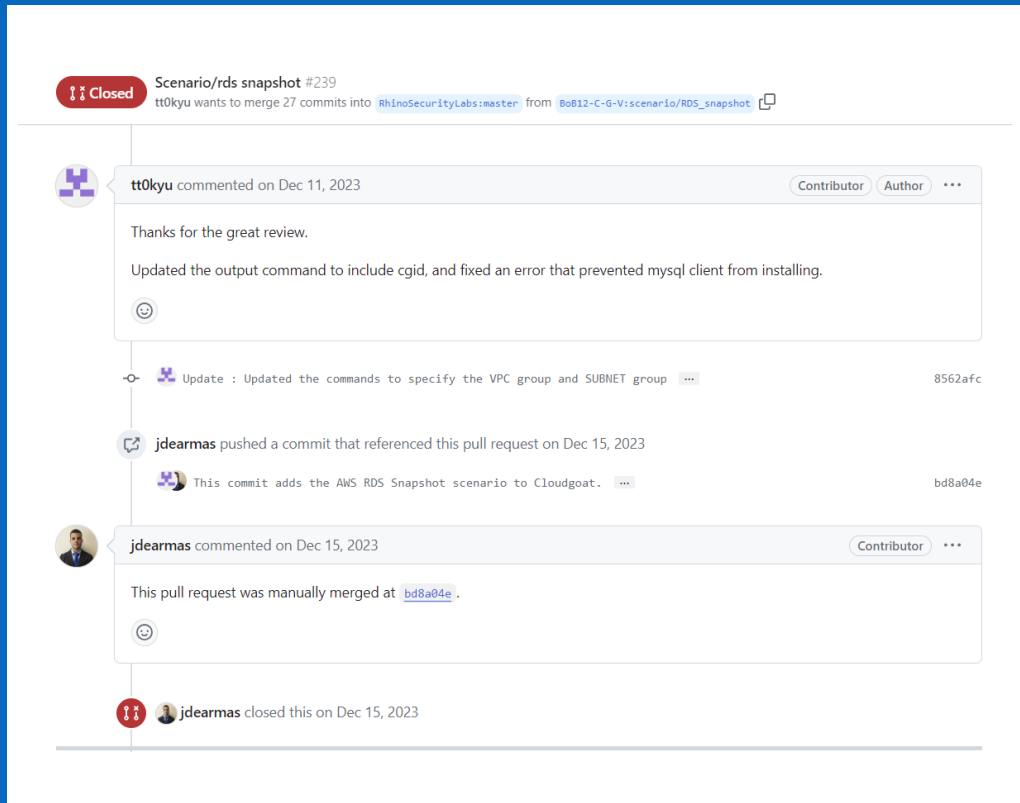


glue_privesc



sqs_flag_shop

Part 3 | CloudGoat 컨트리뷰션 후기



This screenshot shows the GitHub interface for pull request #239, titled "Scenario/rds snapshot". The status is "Closed". The pull request was created by tt0kyu and merged into the RhinoSecurityLabs:master branch. The commit message is "Updated the output command to include cgid, and fixed an error that prevented mysql client from installing." The pull request was manually merged by jdearmas on Dec 15, 2023. The commit hash is bd8a04e.

Scenario/rds snapshot #239
Closed
tt0kyu wants to merge 27 commits into RhinoSecurityLabs:master from Bo812-C-G-V:scenario/RDS_snapshot

tt0kyu commented on Dec 11, 2023
Thanks for the great review.
Updated the output command to include cgid, and fixed an error that prevented mysql client from installing.

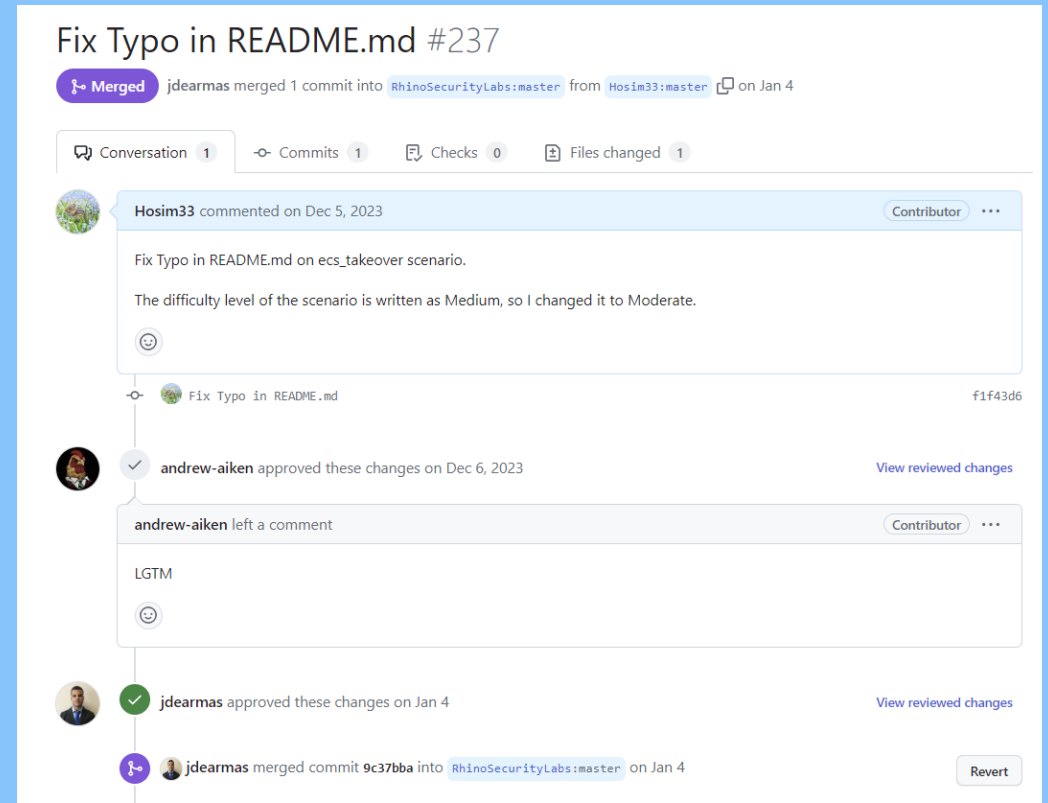
Update : Updated the commands to specify the VPC group and SUBNET group
8562afc

jdearmas pushed a commit that referenced this pull request on Dec 15, 2023
This commit adds the AWS RDS Snapshot scenario to Cloudgoat.
bd8a04e

jdearmas commented on Dec 15, 2023
This pull request was manually merged at bd8a04e.

jdearmas closed this on Dec 15, 2023

rds_snapshot



This screenshot shows the GitHub interface for pull request #237, titled "Fix Typo in README.md". The status is "Merged". The pull request was created by Hosim33 and merged into the RhinoSecurityLabs:master branch. The commit message is "Fix Typo in README.md on ecs_takeover scenario. The difficulty level of the scenario is written as Medium, so I changed it to Moderate." The pull request was manually merged by jdearmas on Jan 4. The commit hash is 9c37bba.

Fix Typo in README.md #237
Merged
jdearmas merged 1 commit into RhinoSecurityLabs:master from Hosim33:master on Jan 4

Hosim33 commented on Dec 5, 2023
Fix Typo in README.md on ecs_takeover scenario.
The difficulty level of the scenario is written as Medium, so I changed it to Moderate.

Fix Typo in README.md
f1f43d6

andrew-aiken approved these changes on Dec 6, 2023
View reviewed changes

andrew-aiken left a comment
LGTM

jdearmas approved these changes on Jan 4
View reviewed changes

jdearmas merged commit 9c37bba into RhinoSecurityLabs:master on Jan 4
Revert

fix_typo

Chapter.02 - 프로젝트 수행 과정

시나리오 상세

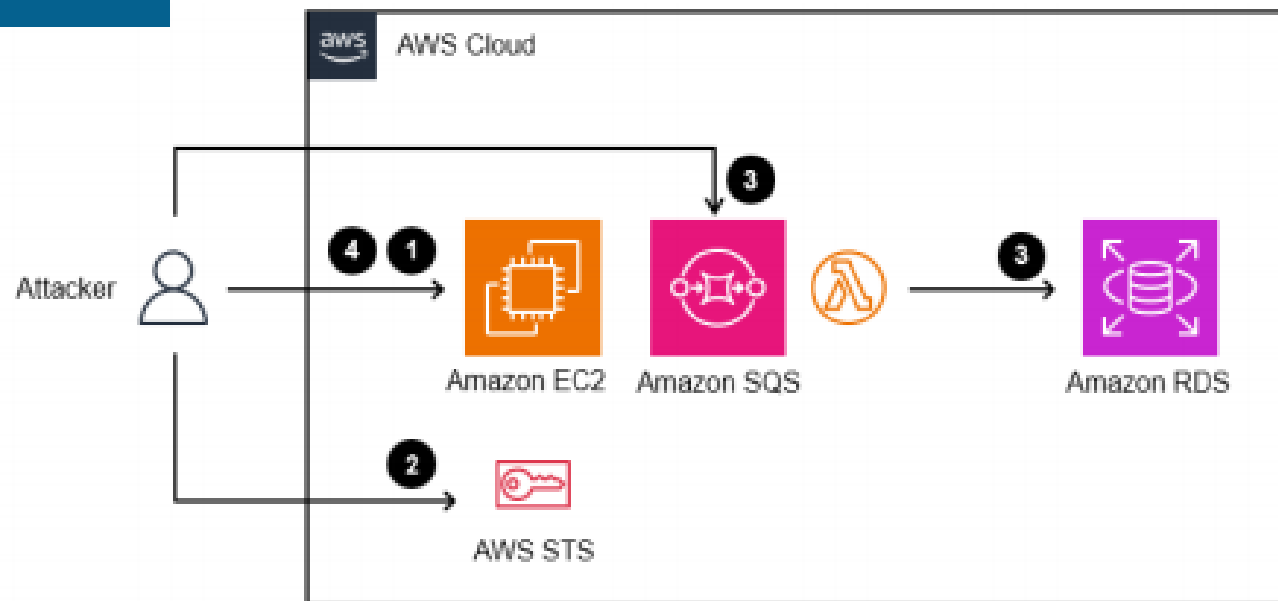
SQS_FLAG_SHOP

주요한 구성 오류

- 웹 서비스 취약한 소스코드 노출
- 부적절한 IAM 권한 설정

시나리오 진행

- 웹 서비스에 사용되는 취약한 소스코드 노출
- 공격자에게 부여된 권한 확인 및 권한 상승
- 공격자는 SQS 대기열에 위조된 메시지 전송
- FLAG 구매 후 시나리오 종료



주요 관계자



andrew-aiken



활발하게 활동하는 컨트리뷰터



Andrew 2023.12.13. 오전 3:29

New CloudGoat Scenario: Glue Privilege Evasion

Created by the Best of the Best 12th CGV Team (Yong Siwoo, Park Do Kyu, Park Seo Hyun, Jung Ho Shim, Chae Jinsoo)

<https://github.com/BoB12-C-G-V>

https://github.com/RhinoSecurityLabs/cloudgoat/tree/master/scenarios/glue_privesc (수정됨)



jdearmas



라이노 시큐리티 랩스 CloudGoat 오픈소스 담당자



John Doe 2023.12.09. 오전 4:22

I'm currently having trouble spinning up the scenario. I got an "Access Denied" error when applying the S3 Bucket Policy.



Tyler R 2023.11.21. 오전 1:15

Yes I notified Rhino team! I'm on PTO this week though but will plan on checking it out myself when back!



라이노 시큐리티 랩스 직원인데 윗 사람보다 높은 느낌(?)

Part 3 | CloudGoat 컨트리뷰션 후기

Chapter.02 - 프로젝트 수행 과정

PR 과정

Kyu 2023.11.14, 오후 12:54

Hello, Tyler, we have a PR request for a new scenario. A reviewer named Andrew gave us some feedback, which we've incorporated. We look forward to Rhino final review!

<https://github.com/RhinoSecurityLabs/cloudgoat/pull/233>



Tyler R 2023.11.14, 오후 1:24

Hey - fantastic! Thank you so much for reaching out. I'll share this with the rest of the Rhino team in the morning so we can begin reviewing it!

Kyu 2023.11.14, 오후 4:00

Hello Tyler,

I hope you had a pleasant time off. I am a member of the CGW team, and I've been working on writing a scenario about Glue, ECS, and SQS. (Discord link: [Rhino Security Labs](#) -> [Glue Privacy Scenario](#))

I'm reaching out to you today to inquire about the status of the Pull Request for our scenario. Usually, I'd patiently wait while working on other tasks until the PR is completed. But given our project deadline is not far away (-Dec 15, 2023), I'm a bit concerned and felt the need to check in.

You may check our team organization here: <https://github.com/Bodhi-C-G-V>

Looking forward to your response.

Best regards,
(Do Kyu Park)

John Doe 2023.11.14, 오후 4:00

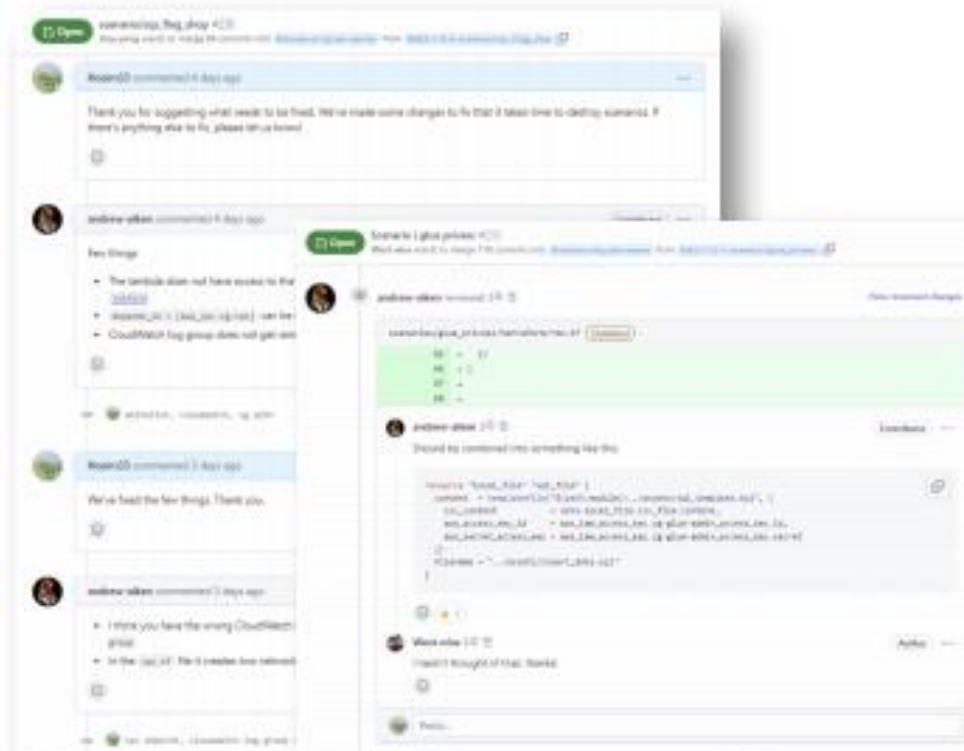
Hello Kyu,

Yes, I'm currently prioritizing and reviewing your scenario. I should be done with my review within the next few days.

Your scenario is more time-consuming due to the zip file. External zipfiles require extra care. I'm sure you understand 😊

Thank you for taking the time to contribute to an open-source project. It's organizations such as yourselves that help provide this common good to everyone.

1. RhinoSecurityLabs 담당자와 Discord로 소통하며
팀소개 및 PR 리뷰 지속적으로 요청



2. CloudGoat 오픈소스 컨트리뷰터에게
시나리오 별로 피드백을 받아 코드 수정

#PR할 때 커밋 기록을 깔끔하게 하자

#외국 사람들 게으르다

#오픈소스 컨트리뷰션은 생각보다 안 어렵다(?)

Q&A

질의 응답 시간