클라우드 보안 - CloudGoat 오픈소스 실습

리더	정호심
구분	스터디
시즌	시즌 1
확정 멤버	김민석 안지현 수빈 김 진윤태 시온 강 SOOCHAN KWAK

1 주제

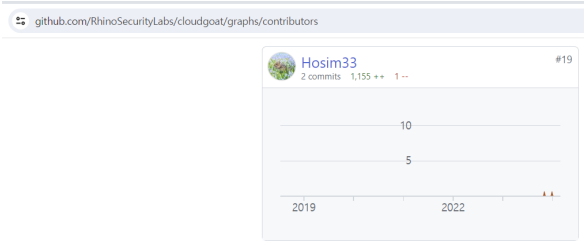
> 어떤 학습 자료 혹은 프로젝트를 진행하고 싶은지 설명해 주세요.

스터디 1주차 OT.pdf

CloudGoat 오픈소스 프로젝트의 시나리오를 6개 이상 실습합니다!

"설계상 취약한" AWS 배포 도구

GitHub - RhinoSecurityLabs/cloudgoat: CloudGoat is Rhino Security Labs' "Vulnerable by Design" AWS deployment tool
CloudGoat is Rhino Security Labs' "Vulnerable by Design" AWS deployment tool - RhinoSecurityLabs/cloudgoat
https://github.com/RhinoSecurityLabs/cloudgoat



2 대상

> 어떤 사람이 이 스터디/프로젝트를 따라오기 적절한지 알려주세요.

- 리더에게 뛰어난 보안 역량을 기대하지 않는 분
  - 저도 부족한 점이 있으니 와서 적극적으로 같이 공부합시다!!
- AWS 보안과 클라우드 보안을 이론이 아닌 실습으로 배우고 싶으신 분
- CloudGoat 오픈소스 컨트리뷰션에 관심이 있으신 분
- 보안에 대한 이해도를 가볍게 높이고 싶으신 분
- Terraform과 클라우드 보안을 같이 공부하고 싶으신 분

- 기술적인 해킹이나 공격보다 사람이 설정을 잘못해서 발생하는 클라우드 보안 문제가 대부분이라는 것을 이해하고 있고, 기술적인 실습만을 원하지 않는 분
    - 실제로 CloudGoat는 취약한 설정이 된 환경을 실습하는 것이라서 그 과정에서 공격을 하는 부분도 있겠지만 비중이 적기 때문에 이런 분이 오시면 실망할 수 있습니다...
- 해킹 대회, CTF와 유사한 방식으로 클라우드 보안을 공부하고 싶으신 분
    - 정답이 이미 다 공개되어 있기 때문에 너무 어려울 거라고 걱정하지 않으셔도 됩니다!
    - 처음부터 끝까지 답을 안 보고 풀기는 어렵기 때문에 꼭 내가 처음부터 풀어내고 싶고 정답은 안 본다 하시는 분은 맞지 않으실 수 있습니다. 실력의 문제가 아니라 AWS CLI 명령어가 길고 복잡하기 때문입니다.

3️⃣ 커리큘럼

> 8주 간의 커리큘럼을 설명해 주세요.

1주(3/5)

- 자기소개 및 아이스브레이킹
- 리더가 진행하는 CloudGoat 오픈소스 간단 설명 및 진행했던 프로젝트 돌아보기 (10분 정도)
    - 직접 BoB 12기 2차 프로젝트 기간 동안 CloudGoat 오픈소스에 4개의 시나리오를 팀원들과 함께 PR 하였고, 최종 MERGE 되었습니다.

2주(3/12)

- iam_privesc_by_rollback 시나리오 실습 후 내용 랜덤으로 1명이 발표
- Q&A
- 클라우드 보안 자유 주제 발표 미리 정한 1명

3주(3/19)

- lambda_privesc 실습 후 내용 랜덤으로 1명이 발표
- Q&A
- 클라우드 보안 자유 주제 발표 미리 정한 1명

4주(3/26)

- vulnerable_lambda 시나리오 실습 후 내용 랜덤으로 1명이 발표
- Q&A
- 클라우드 보안 자유 주제 발표 미리 정한 1명

5주(4/2)

- iam_privesc_by_key_rotation 실습 후 내용 랜덤으로 1명이 발표
- Q&A
- 클라우드 보안 자유 주제 발표 미리 정한 1명

6주(4/9)

- SQS_FLAG_SHOP 실습 후 내용 랜덤으로 1명이 발표
- Q&A
- 클라우드 보안 자유 주제 발표 미리 정한 1명

7주(4/16)

- 5~7주 중 논의해서 시험기간으로 1주 휴식
- 만약 쉴 필요 없는 사람들은 자유롭게 클라우드 보안 자유 주제 발표 미리 정한 2명

8주(4/23)

- cloud_breach_s3 시나리오 실습 후 내용 랜덤으로 1명이 발표
- Q&A
- 스터디 최종발표 준비 및 스터디 회고

4️⃣ 방식

> 이 스터디만의 규칙이나 진행 방식을 설명해 주세요.

- 어디서 진행하나?
  - 기본적으로 디스코드 진행 예정인데, 원하는 사람이 있다면 3분의1 정도는 오프라인 의향이 있습니다...
- 어떻게 흘러가나?
  - 모든 실습 과정을 개인 블로그나 노션에 남기고, 스터디 시작할 때 1명을 뽑아서 발표를 진행합니다.
  - 뽑았을 때 앞의 2번 스터디에서 발표하신 분의 경우는 제외합니다. (최대한 많은 사람이 발표하기 위함)
  - 실습 발표가 끝난 후 궁금한 점이나 나누고 싶은 이야기를 자유롭게 합니다.
  - 클라우드 보안에 대해 자유 주제로 미리 정한 사람이 발표를 진행합니다. (5~10분 정도 짧게)
  - 대학생을 고려해서 8주 중 5~7주에 1번 쉬어가는 주를 만들 예정인데, 원하지 않거나 스터디 하고 싶은 분들은 2명 정해서 클라우드 보안 자유 주제 발표하시면 될 것 같습니다.
- 언제 진행하나요?
  - 화요일 정규 스터디 시간을 생각하고 있는데, 오프라인 원하실 경우 같이 시간을 맞춰보면 좋을 것 같습니다.

5️⃣ 기록

> 스터디 내용을 기록 할 공간을 노션에서 따로 마련하거나, 외부 저장소 링크를 남겨주세요.

- 추후 인원 모이면 노션 페이지에 마련 예정인데, 개인 블로그에 해도 되고 자유롭게 가능합니다.

CloudGoat 스터디 기록

Aa 이름	담당자	상태
2주 - iam_privesc_by_rollback		진행 중
클라우드 보안 발표		진행 중

6️⃣ 출석부

> 3회 이상 불참시 5기를 수료할 수 없습니다.

1주(3/5)

불참 x

2주(3/12)

3주(3/19)

4주(3/26)

5주(4/2)

6주(4/9)

7주(4/16)

8주(4/23)