50 PoC(Proof of Concept) 구현을 통한 클라우드 보안 공격 자동화 도구 개발

소속 정보컴퓨터공학부 분과 D 팀명 417호 참여학생 김승혁, 송재홍, 정재영 지도교수 최윤호

과제 개요

배경 및 목표

- 기업 및 기관의 클라우드 마이그레이션이 증가함에 따라 클라우드 보안의 중요성이 강조됨
- 클라우드 환경의 보안을 강화하기 위해 MITRE ATT&CK 프레임워크를 기반으로 보안 공격 자동화 플랫폼 개발
- 해당 플랫폼은 대상 시스템의 취약점을 이용하여 시스템을 공격한 후 사용자에게 그 결과를 알려주어 보안을 강화할 수 있도록 도움
- 공격 자동화를 통해 사용자가 클라우드 환경에 대한 사전 지식 없이 보안 검사가 가능함

과제 내용

공격 시나리오 생성

- 공격 대상 시스템에서 특정 목표를 달성하기 위한 일련의 과정을 '공격 시나리오'라고 정의
- 공격 시나리오는 MITRE ATT&CK 프레임워크의 Technique으로 구성

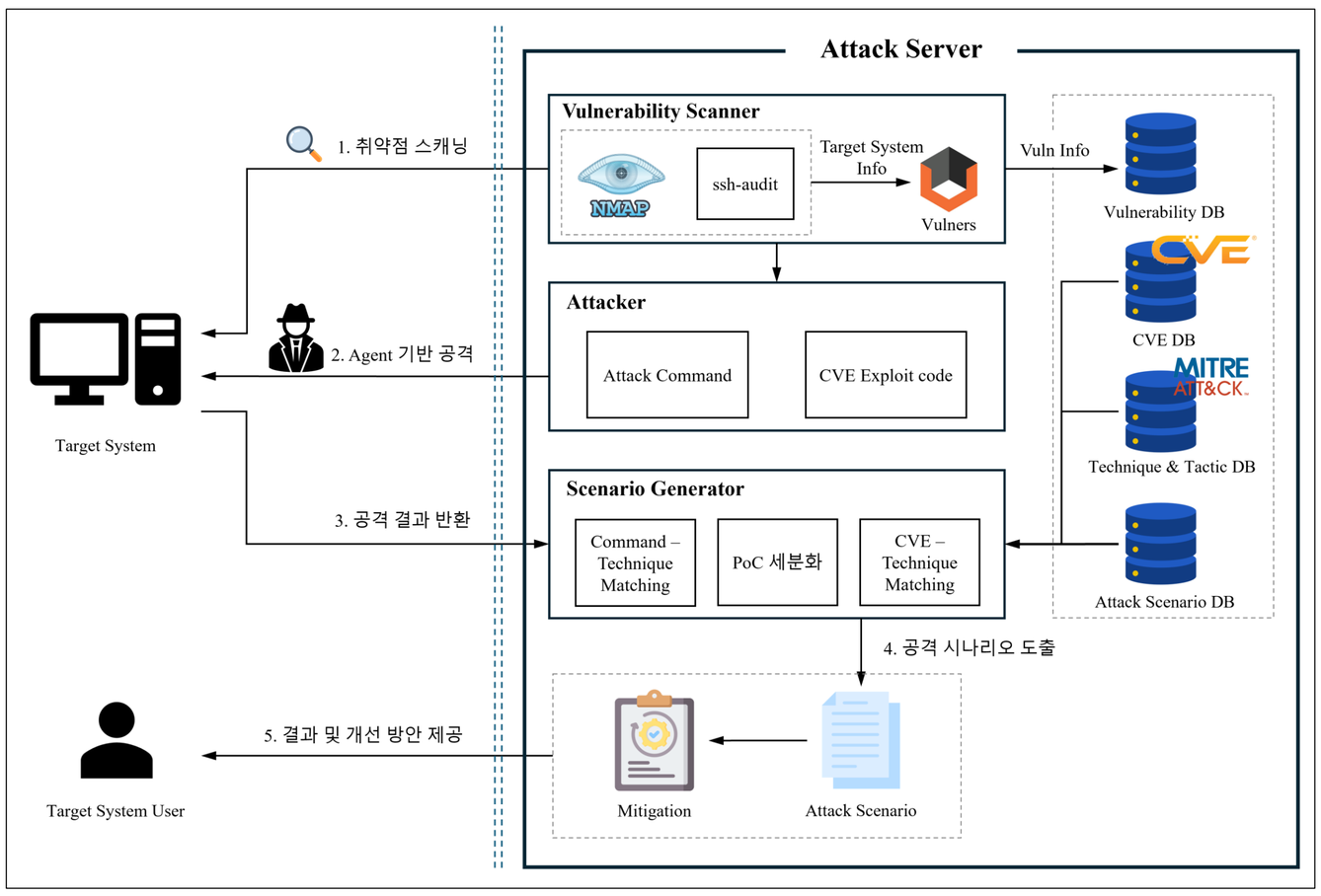
MITRE ATT&CK 기반 침투 테스트

- MITRE ATT&CK 프레임워크에서 정의한 공격 기법들을 구현하고 그 기법들을 연결하여 공격 시나리오 구현
- Agent를 이용하여 대상 시스템을 공격하고 그 결과 값을 기반으로 시스템을 공격할 수 있는 시나리오 도출

CVE Exploit 기반 침투 테스트

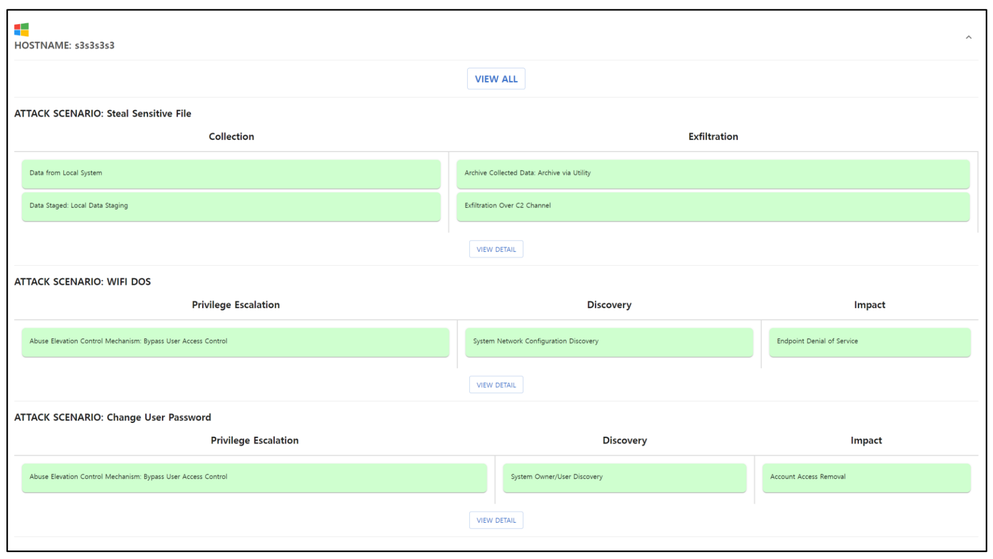
- CVE(Common Vulnerabilities and Exposures)의 알려진 PoC의 동작 흐름과 MITRE ATT&CK의 Technique과 매핑하여 공격 시나리오 구성
- 대상 시스템의 IP 주소 혹은 Agent를 이용하여 해당 시스템에서 발견된 CVE 목록과 Exploit 성공한 CVE를 출력

Service Architecture



결과

MITRE ATT&CK



CVE ATTACK