제로트러스트 클라우드 보안 연구센터

MITRE ATT&CK based Penetration Testing Tool for Security System Demonstration

보안 시스템의 실증을 위한 MITRE ATT&CK 프레임워크 기반의 침투 테스트 도구

적용분야

Zero Trust | Multi Cloud | 기업/공공 자산 | 네트워크 보안

연구목적

· 사이버 보안 공격의 고도화에 따라, 보안 시스템의 취약점을 효과적으로 진단하고 강화하기 위해 다양한 공격을 수행할 수 있는 침투 테스트 도구의 필요성이 부각됨

· 실제 사이버 공격을 기반으로 정리한 **MITRE ATT&CK 프레임워크를 활용한 공격**, 각 시스템의 **알려진 취약점(CVE)을 스캔 및 악용**, HashValue 크래킹과 접근 권한 탈취를 위한 무차별 대입 공격으로 구성함

· 기존 ATT&CK 기반 정형화된 공격 수행 구조에 **LLM Agent 기반 지능형 의사결정 모듈**을 추가하여, 공격 기법 선택 및 공격 계획, 우선 순위 판단 등을 **자동화하고 환경 반응에 따라 공격 전략을 동적으로 조정**할 수 있도록 확장함

연구내용

· AI Agent 기반 공격

자율적 의사결정 기반 공격 시나리오 생성 및 실행

- 취약점 및 악용 공격 시나리오를 Attack Tree 구조로 구현
- LLM의 공격 설계 성능 향상을 위해 RAG 기반 외부 지식 확장 메커니즘을 적용
- 공격 수행 결과를 반영하여 공격 경로를 반복적으로 확장 및 최적화

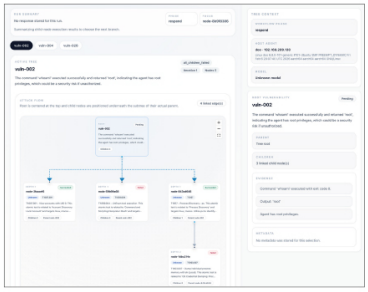
· MITRE ATT&CK 기반 공격

TTPs를 기반으로 구현된 약 1,200개 공격 자동화 및 결과 보고

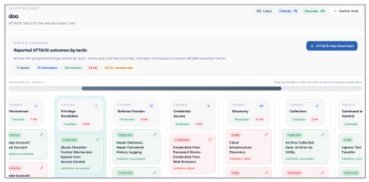
· CVE 스캐닝 및 Exploitation

포트 스캐닝 및 알려진 취약점(CVE) 탐색 시도 및 악용 공격

- 무차별 대입 공격을 통한 Credential Access 및 Hash Cracking을 포함



공격 유형 1. AI Agent 기반 공격



공격 유형 2. MITRE ATT&CK 기반 공격

공격 유형 3. CVE 스캐닝 및 Exploitation

기술 경쟁력

기존기술	기술 차별성	대상기술

· 사전 정의된 공격 시나리오 및 규칙(rule)에 따라 침투테스트를 수행하는 방식으로, 공격 절차가 고정되어 있음

· MITRE ATT&CK과 같은 프레임워크를 활용하더라도 실제 테스트는 미리 설계된 순서에 따라 단계적으로 실행

기술적 한계

· 환경 변화에 대응하는 동적 공격 수행 불가
· 공격 간 연계 부족으로 전체 공격 흐름 파악이 어려움
· 사용자 의존도가 높아 자동화 수준의 제한
· 공격 결과를 활용한 지속적 의사결정 기능 부재

· LLM 기반 AI Agent가 탐색 결과를 분석하여 취약점을 자동으로 판단 및 Attack Tree 구조로 공격 계획 구성

· RAG 기반 MITRE ATT&CK TTP 검색 및 공격 수행 결과 피드백을 통한 공격 경로 동적 생성 및 확장

기술적 우위

· 환경 변화를 반영한 자율적 공격 의사결정 가능
· 공격 흐름의 가시성 및 확장성 확보 (Attack Tree 구조화)
· RAG를 통한 공격 지식 활용으로 공격 설계 정확도 향상
· 공격 계획-실행-분석 전 과정 자동화로 사용자 개입 최소화

지식재산권

SW 명칭	출원(등록)번호	출원(등록)일자
PoC(Proof of Concept) 구현을 통한 클라우드 보안 공격 자동화 플랫폼	C-2024-042500	2024.10.30

제로트러스트 클라우드 보안 연구센터 ZeroTrust Cloud Security Research Center
부산대학교 PUSAN NATIONAL UNIVERSITY
문의처 제로트러스트 클라우드 보안 연구센터 csrc@pusan.ac.kr 051.510.7212