제로 트러스트 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

적용 분야

- 보안 시스템 실증
- 취약점 분석
- 보안 위협 시각화
- 공격 시뮬레이션

연구 목적

- 사이버 보안 공격의 고도화에 따라, 실제 공격자들의 공격을 방어하는 데 어려움이 존재하고 이에 따라 보안 시스템 실증을 위해 다양한 공격을 사전에 시도할 수 있는 침투 테스트의 필요성이 부각됨
- 실제 사이버 공격을 기반으로 정리한 MITRE ATT&CK 프레임워크를 활용하여 보안 시스템을 체계적으로 테스트하고, 다양한 공격 기법을 자동화된 방식으로 시뮬레이션할 수 있는 도구를 개발함
- MITRE ATT&CK 프레임워크의 다양한 공격 기법(TTPs)을 활용하여 보안 시스템에 대한 실질적인 공격 시뮬레이션을 진행하고, 이를 바탕으로 공격자의 행동 패턴을 예측하며, 시스템 취약점에 대한 구체적인 대응 방안을 제시하고자 함

연구 내용

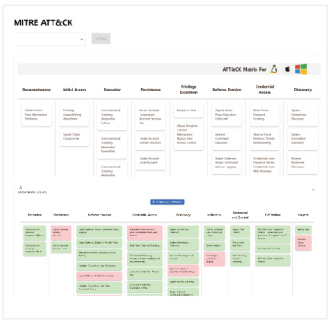
MITRE ATT&CK기반공격 | TTPs를 기반으로 구현된 약 1,200개 공격 자동화 및 결과 보고

ATT&CK Matrix 형태로 결과를 제공하여 대상 시스템에 수행된 공격 흐름 시각화 / Atomic Red Team의 공격 소스를 95% 이상 반영하여 자동화

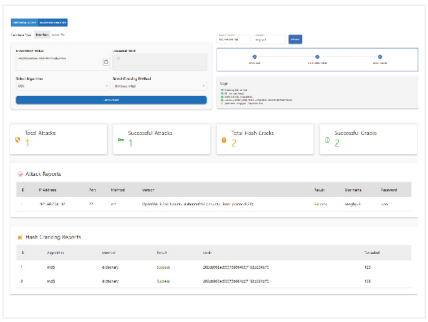
Brute Force | 무차별 대입 공격을 통한 Credential Access 및 Hash Cracking

Credential Access : Brute Force 공격을 통한 접근 권한 탈취 시도 / Password Cracking : 해시 처리된 비밀번호를 입력받아 원래 비밀번호 찾기 시도

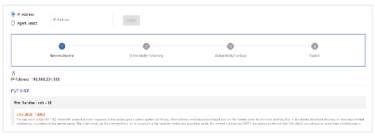
CVE 스캐닝 및 Exploitation | 포트 스캐닝 및 알려진 취약점(CVE) 탐색 시도 및 악용 공격



공격유형 1. MITRE ATT&CK 기반 공격



공격유형 2. Brute Force



공격유형 3. CVE 스캐닝 및 Exploitation

시스템 취약점 통계치 제공

기술 경쟁력

기존기술	기술 차별성 ▶▶	기존기술
• 공격 수행 후 공격의 전반적인 맥락과 공격 경로에 대한 시각화 부재 •일부 공격 기법만을 집중적으로 다루어 사용자가 공격 프로세스를 직접 설계해야 함		• MITRE ATT&CK Matrix 형태로 공격 결과를 제공하여 공격의 전반적인 맥락을 시각화 • 다양한 공격 프로세스 통합 및 사용자 친화적인 GUI 제공으로 자동화된 공격 수행 가능
기술적 한계 • 제한적인 공격 기법 • 수동적 테스트 및 복잡한 설정을 요구 • 공격 결과 분석 및 시각화 부족 • 사용자 친화성 부족		기술적 우위 • 다양한 공격 기법 통합 지원 및 자동화 • MITRE ATT&CK 프레임워크 기반의 공격 흐름 시각화 • 사용자 친화적인 인터페이스 제공

지식재산권

발명의 명칭	출원(등록)번호	출원(등록)일자
PoC(Proof of Concept) 구현을 통한 클라우드 보안 공격 자동화 플랫폼	C-2024-042500	2024. 10. 30.

문의처 | 제로트러스트 클라우드 보안 연구센터 csrc@pusan.ac.kr 051. 510. 7212