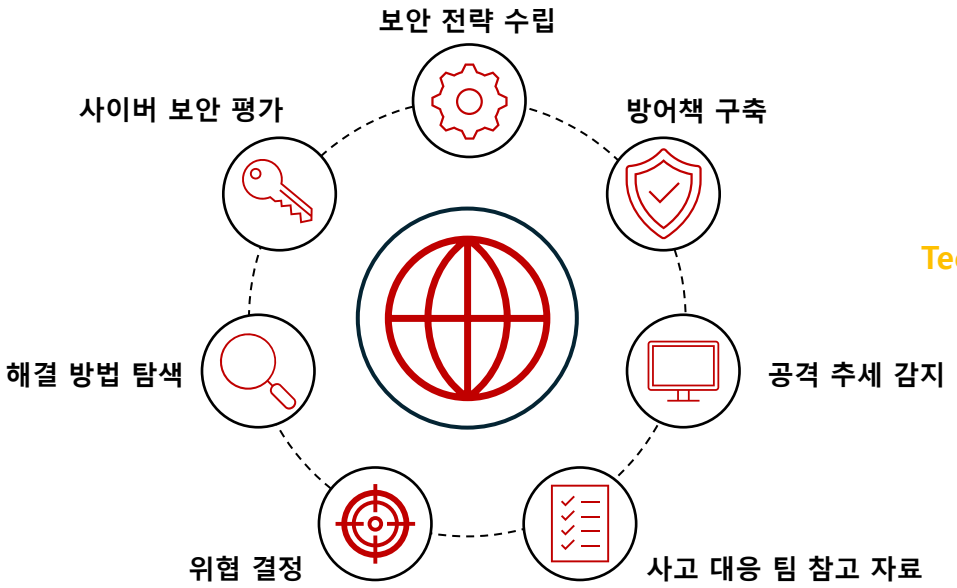
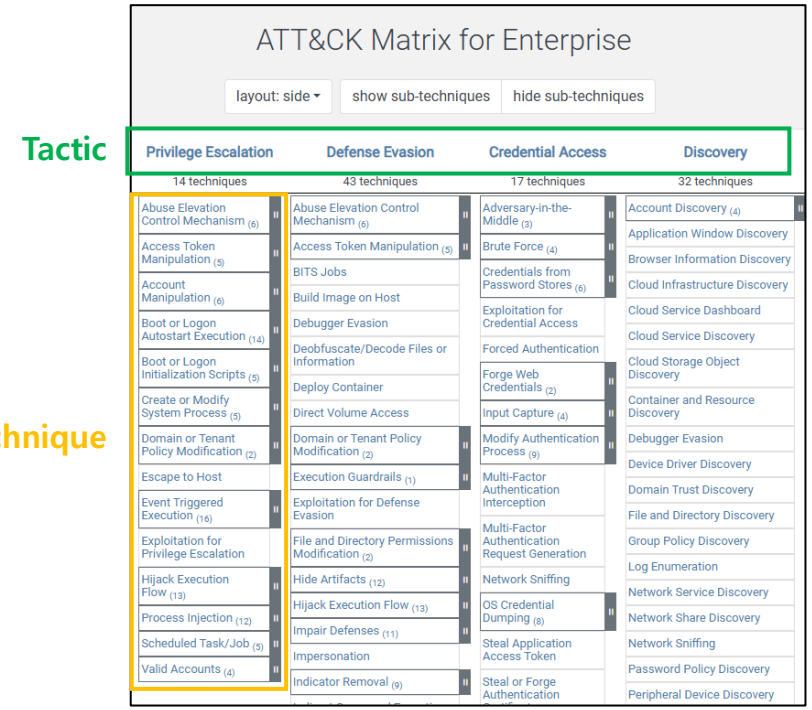
PoC 구현을 통한 클라우드 보안 공격 자동화 도구 개발

201824441 김승혁
201824507 송재홍
202145827 정재영

연구 배경

- **MITRE ATT&CK 프레임워크**
  - 사이버 공격 기술과 방어 방법을 체계적으로 정리한 지식 기반 (Knowledge Base)
    - ❖ 지식 기반: 모든 정보 또는 지식을 저장, 조직화하고 고객, 직원 및 파트너와 공유할 수 있는 저장소
  - 공격 방법(Tactic)과 기술(Technique)을 분석하여 다양한 해킹 기법을 문서화하고 분류한 프레임워크

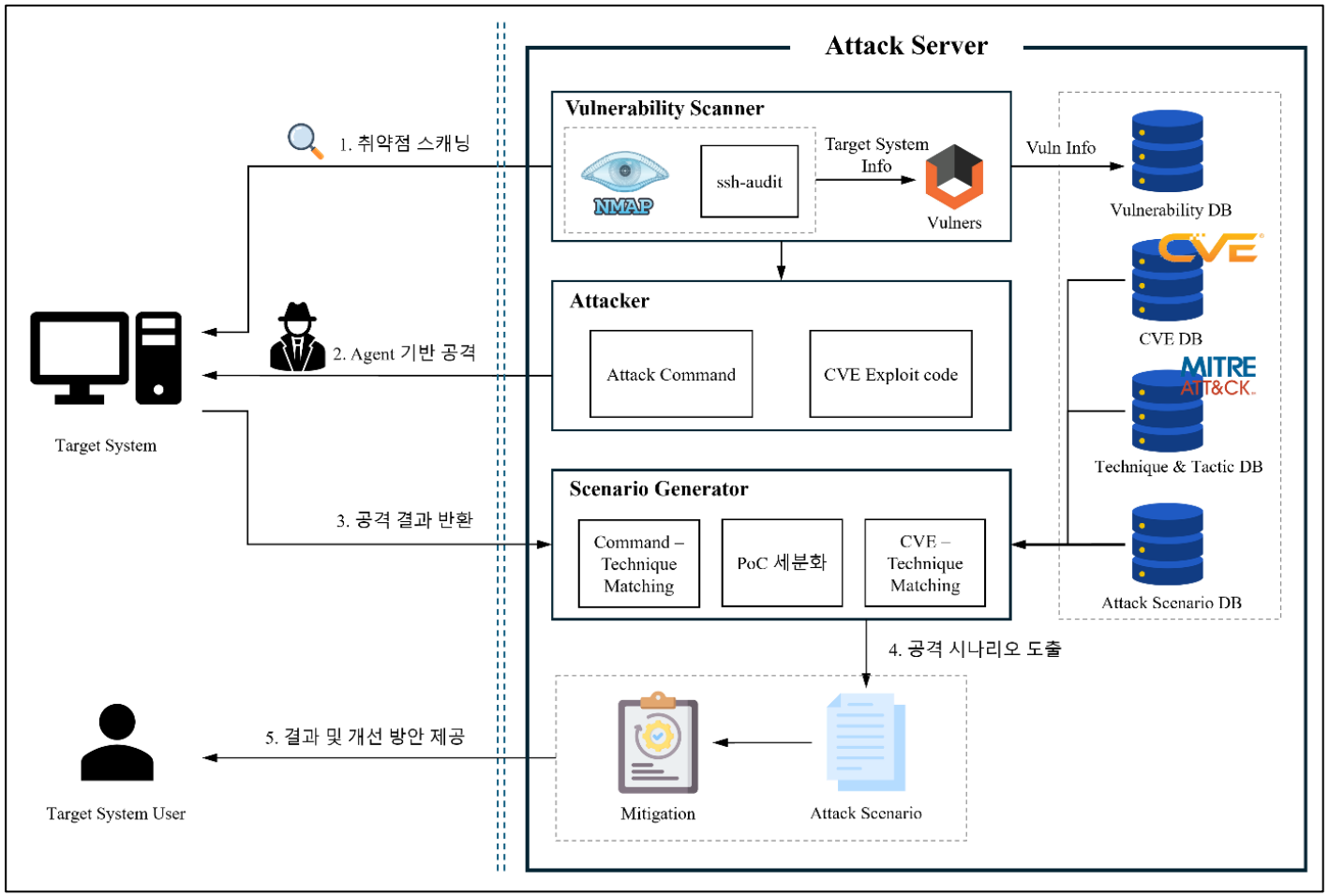




Examples of Tactic & Technique in MITRE ATT&CK Matrix

연구 내용

▪ 전체 시스템 구상도



Architecture

연구 내용

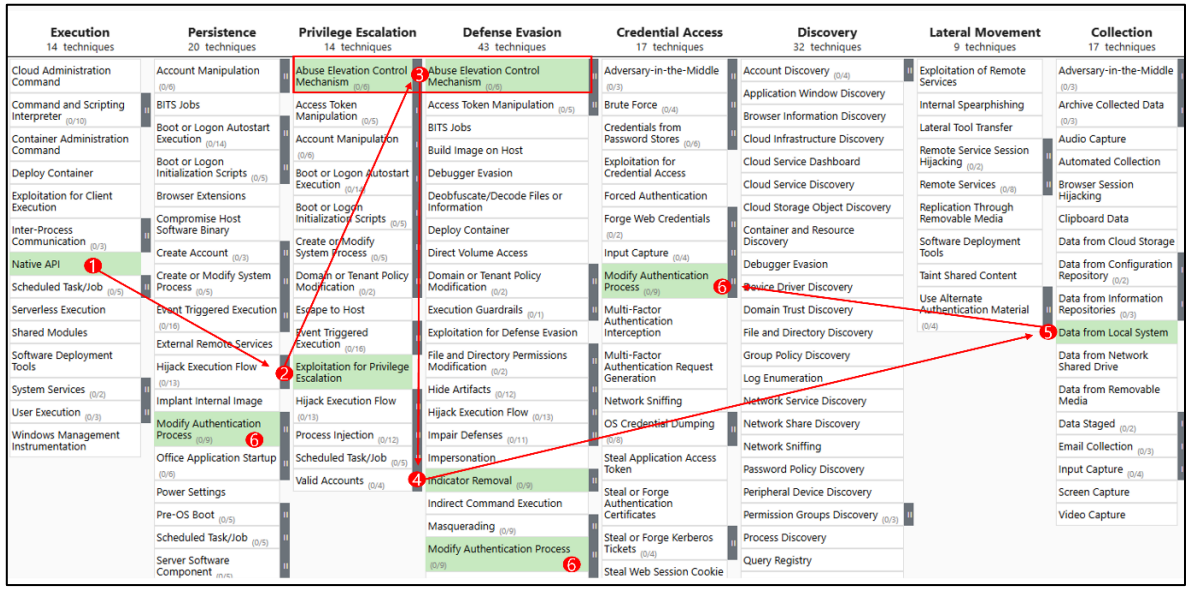
- **공격 시나리오 설계**
  - MITRE ATT&CK의 Technique과 그에 해당하는 CMD 명령어를 매핑하여 시나리오 설계
  - CVE (Common Vulnerabilities and Exposures) PoC의 흐름과 MITRE ATT&CK의 Technique과 매핑하여 시나리오 설계
  - 설계한 시나리오를 기반으로 자동화된 침투 테스트 기능 구현
    1. MITRE ATT&CK 기반 침투 테스트
    2. CVE Exploit 기반 침투 테스트

◆ **CVE-2022-0847 (Dirty Pipe)**

– MITRE ATT&CK 매트릭스와 매핑

- T1106 - Native API (Execution)
  - 공격을 수행하기 위해 native OS API 와 상호작용
  - splice, write, pipe, open, fstat 등의 리눅스 시스템 호출
- T1068: Exploitation for Privilege Escalation (Privilege Escalation)
  - 공격자는 권한을 상승시키기 위해 소프트웨어 취약점을 악용
  - /etc/passwd 파일을 덮어쓰고 이를 통해 시스템의 루트 계정 비밀번호를 설정하여 루트 권한을 획득
- T1548: Abuse Elevation Control Mechanism (Privilege Escalation, Defense Evasion)
  - 공격자는 더 높은 권한을 얻기 위해 권한 상승을 제어하도록 설계된 메커니즘 우회
  - /etc/passwd 파일을 수정하여 시스템의 사용자 계정을 수정하여 권한을 상승
- T1070: Indicator Removal (Defense Evasion)
  - 공격자가 자신의 흔적을 지우기 위해 시스템 내에 생성됐던 artifact를 삭제 또는 수정
  - /etc/passwd 파일의 원본을 /tmp/passwd.bak에 백업하고 공격 수행 후 원본 파일 복구
- T1005: Data from Local System (Collection)
  - 취약한 데이터를 찾기 위해 로컬 시스템 자원을 검색
- T1556: Modify Authentication Process (Credential Access, Defense Evasion, Persistence)
  - 인증 메커니즘 및 사용자의 자격 증명 접근 과정 수정

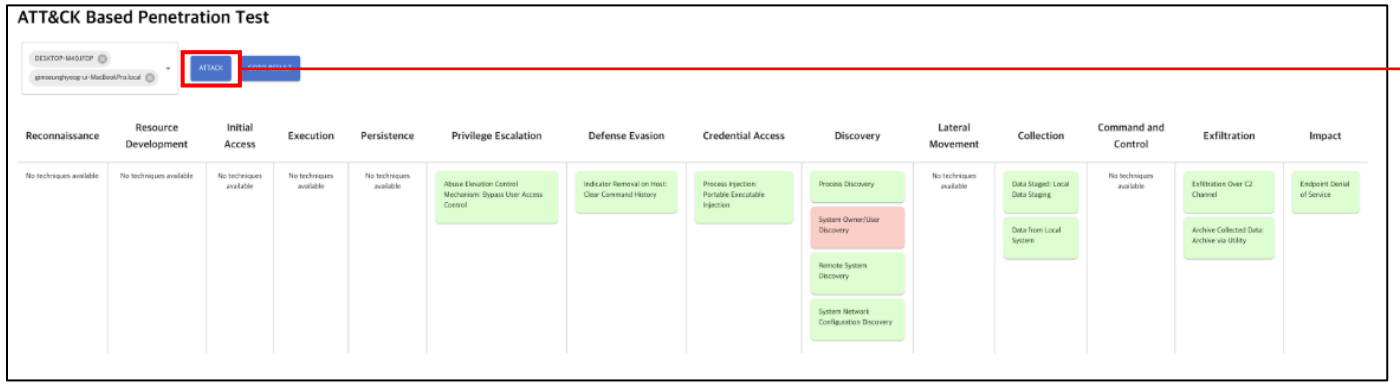
CVE 2022-0847의 PoC 분석



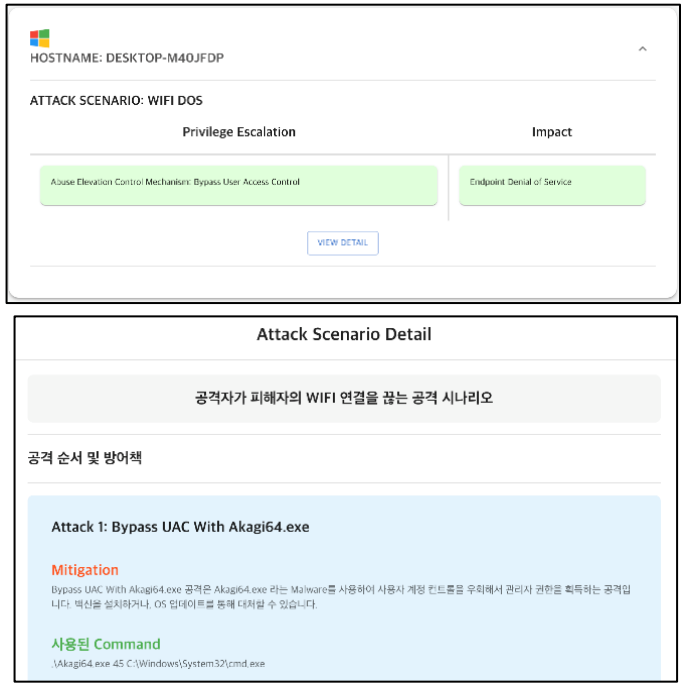
CVE 2022-0847의 PoC와 매핑된 Technique

연구 내용

- **침투 테스트**
  1. **MITRE ATT&CK 기반 침투 테스트**
     - ① MITRE ATT&CK 기반으로 모의 해킹을 수행
     - ② 성공한 공격 시나리오에 대한 결과 및 Mitigation 제공
  2. **CVE(Common Vulnerabilities and Exposures) Exploit 기반 침투 테스트**



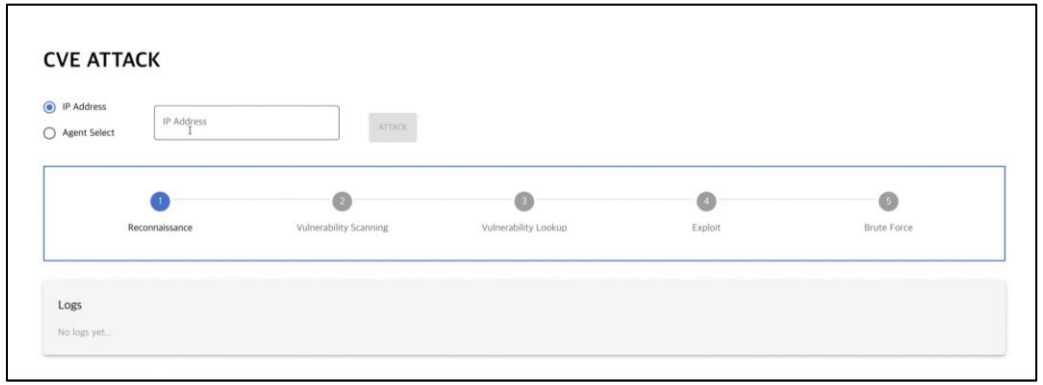
시스템에 대한 침투 테스트 수행 결과 화면



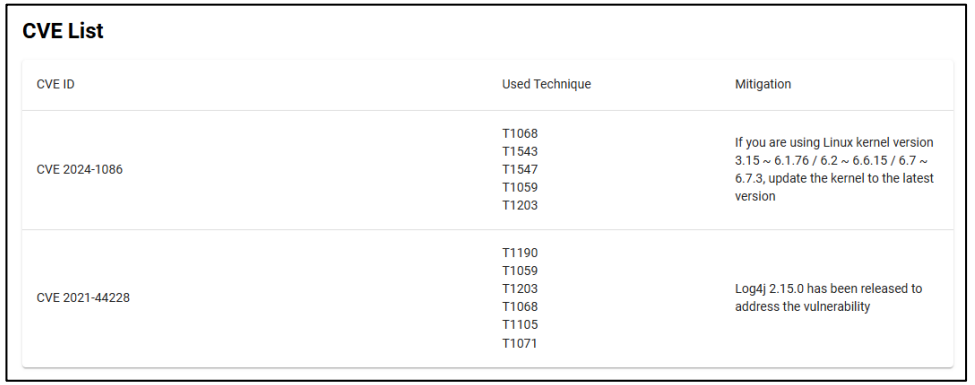
성공한 공격 시나리오 및 완화 방법 제시 화면

연구 내용

- **침투 테스트**
  1. **MITRE ATT&CK 기반 침투 테스트**
  2. **CVE(Common Vulnerabilities and Exposures) Exploit 기반 침투 테스트**
     - ① 대상 시스템에 대한 CVE 탐색
     - ② Exploit으로 연결될 수 있다면 공격을 수행
     - ③ 각 CVE에 대한 MITRE ATT&CK의 Technique과 매핑한 결과 제공
     - ④ Cloud RMF의 CVE ATTACK과의 차이점
       - Cloud RMF에서는 CVE 목록을 출력하고 공격은 수행하지 않음
       - 해당 플랫폼에서는 CVE 목록을 탐색한 이후 시스템 **공격 시도**



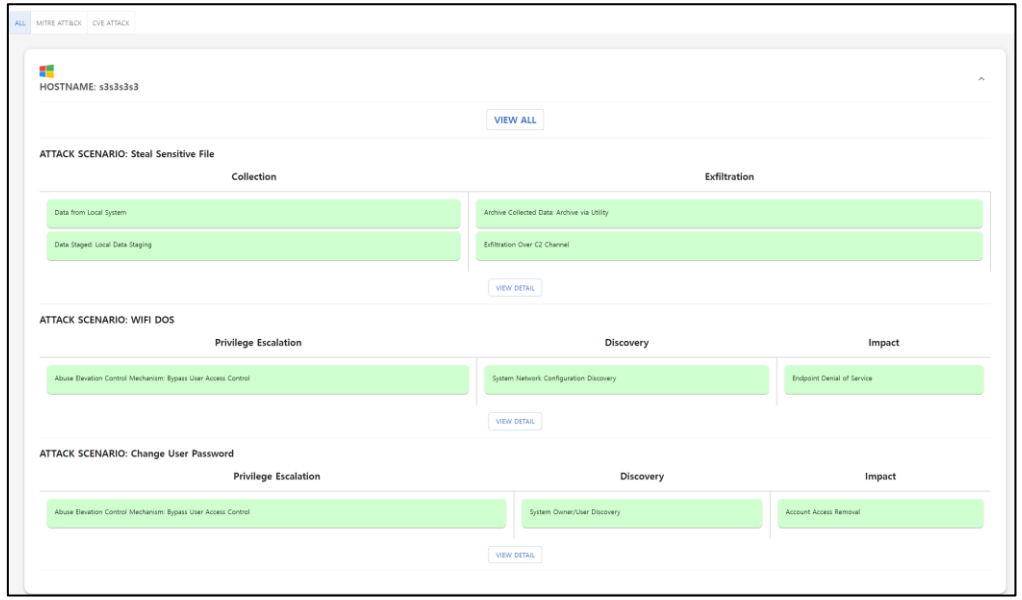
CVE ATTACK 초기 화면



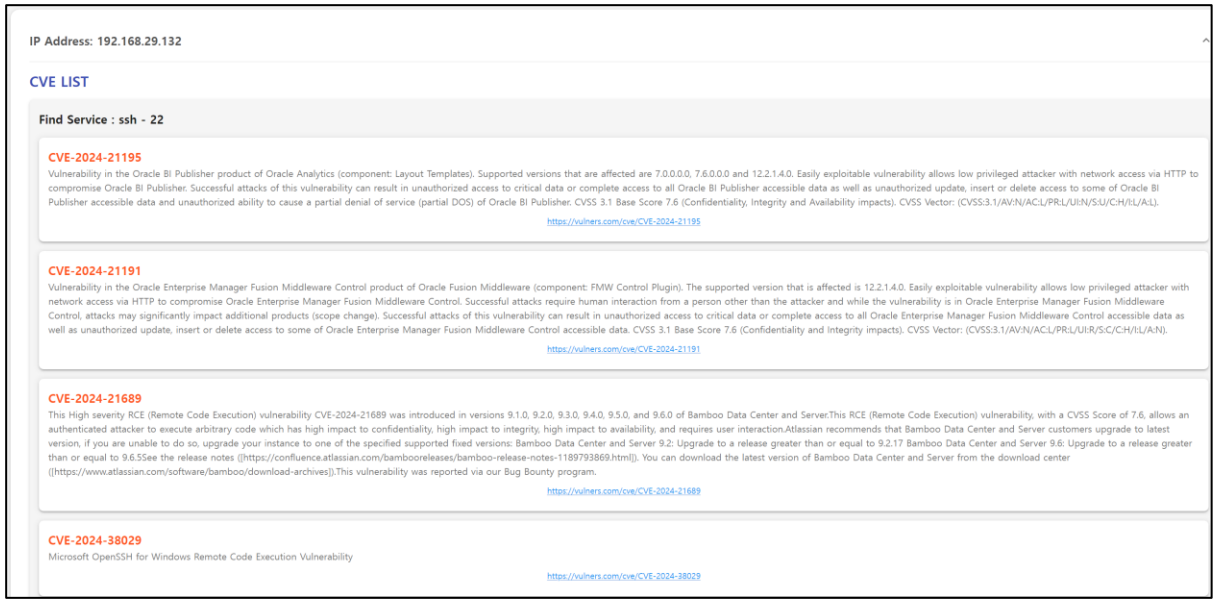
해당 시스템 대상 CVE 리스트 출력

연구 내용

- **침투 테스트 – 결과**
  - 대상 시스템에 수행된 공격 결과와 이에 대응하는 완화 방법 출력
  - 관련 CVE 목록 출력



결과 화면



해당 시스템 대상 CVE 리스트 출력

감사합니다