Pusan National University
Computer Science and Engineering
Technical Report 2024-10

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

201824441 김승혁

201824507 송재홍

202145827 정재영

지도교수 최 윤 호

목 차

1. 서론

1.1. 연구 배경

클라우드 마이그레이션은 기존 시스템에 있는 데이터, 소프트웨어, 디지털 서비스를 클라우드로 옮기는 활동을 말한다. 이를 통해 유연성과 확장성, 비용 효율성 등의 이점을 얻을 수 있다. SNS인사이더가 추산한 글로벌 클라우드 마이그레이션 서비스 시장의 규모는 2021년 기준 9.2억 달러이다. 또 2028년에는 45.11억 달러에 이를 것으로 예측했다.[1] 행정안전부는 전국 행정기관과 공공기관이 운영 중인 모든 정보시스템 1만 9천개를 2025년까지 클라우드로 전면 전환 및 통합하겠다고 밝혔다.[2] 이는 많은 기업이 기존 시스템을 클라우드 환경으로 전환하고 있음을 의미한다.

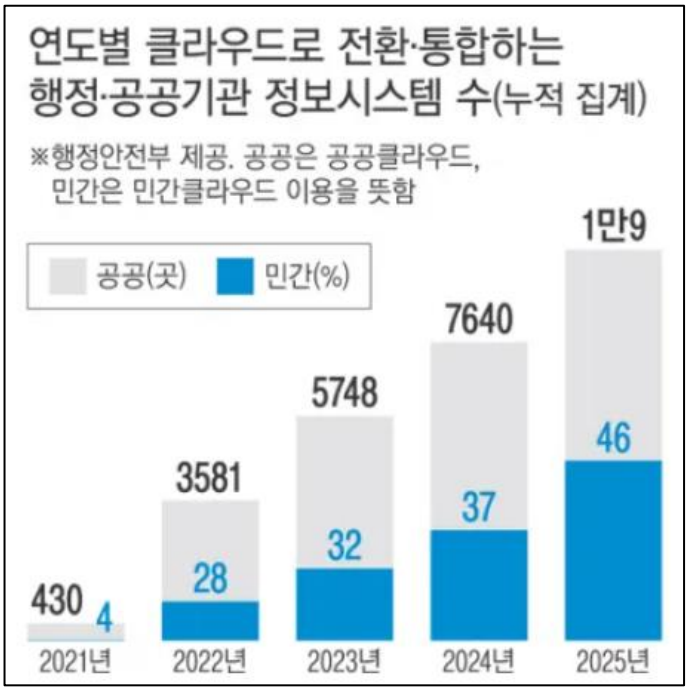


그림 1 클라우드로 전환하는 공공 부문 정보시스템 수

클라우드 환경은 많은 이점을 제공하지만, 동시에 새로운 보안 위협을 초래하기도 한다. 트렌드마이크로가 발표한 '클라우드 보안 위협' 보고서에 따르면 클라우드 보안 문제의 주요 원인은 설정 오류이다.[3] 이는 클라우드를 안전하게 사용하기 위해 사용자가 사

[1] 참고 문헌 [1]

[2] 참고 문헌 [2]

[3] 참고 문헌 [3]

전에 클라우드 환경에 대한 충분한 지식을 갖춰야 함을 말한다. 또한, 클라우드 환경의 복잡성으로 인해 기존의 보안 장비나 솔루션만으로는 완전한 보안 평가가 어려워 새로운 형태의 보안 문제가 발생할 수 있다. 본 과제는 이러한 문제를 해결하기 위해 MITRE ATT&CK 기반의 침투 테스트 자동화 도구를 개발하고자 한다. MITRE ATT&CK은 새로운 공격 기법이 발견될 때마다 데이터를 업데이트하여 해당 도구가 최신 공격에 신속하게 대응할 수 있으며, 공격 자동화를 통해 사용자에게 클라우드 환경에 대한 사전 지식이 없어도 효과적인 보안 검사를 제공할 수 있도록 지원한다.

1.2. 기존 문제점

클라우드 환경에서는 전통적인 보안 모델이 충분하지 않기 때문에, 새로운 보안 전략과 도구가 요구된다. 특히, CVE(Common Vulnerabilities and Exposures)와 MITRE ATT&CK 프레임워크를 기반으로 한 공격 시나리오는 클라우드 보안의 주요 위협 요소로 떠오르고 있다. 이러한 공격들을 사전에 탐지하고 방어하기 위해서는 공격 기법을 이해하고, 이를 시뮬레이션 할 수 있는 PoC(Proof of Concept)를 구현하는 것이 중요하다. 이를 통해 클라우드 환경에서의 취약점을 실질적으로 확인하고, 개선 방안을 도출할 수 있다.

1.3. 연구 목표

본 과제의 목표는 클라우드 보안을 강화하기 위해 MITRE ATT&CK 프레임워크를 기반으로 클라우드 보안 공격 자동화 도구를 개발하는 것이다. 클라우드 환경으로 완전한 전환이 아닌 하이브리드 클라우드 환경을 사용하는 사용자를 위해 온프레미스(On-premise) 환경의 공격도 지원하도록 설계한다.

MITRE ATT&CK은 새로운 공격 기법이 발견될 때마다 데이터가 업데이트되어 최신 공격에 대해 신속하게 대응할 수 있는 장점이 있다. 이 과제에서는 클라우드 및 온프레미스 환경에서 발생할 수 있는 다양한 보안 취약점과 공격 기법을 분석하고, 관련 CVE를 통해 취약점을 파악한다. 이후 분석된 정보를 바탕으로 공격 시나리오를 설계한다. 이때, 공격 시나리오는 '공격 대상 시스템에서 특정 목표를 달성하기 위한 일련의 과정'으로 정의하며, MITRE ATT&CK에서 제공하는 Tactic의 순서를 기반으로 자동 생성되는 기능을 포함하고자 한다. 모의 해킹이 끝나면 사용자는 공격 결과와 과 공격 시나리오에 대한 설명 및 공격을 예방할 수 있는 방어책을 제공받을 수 있다.

2. 연구 배경

2.1. 침투 테스트

침투 테스트란 시스템의 취약점을 찾기 위해 모의 사이버 공격을 실행하는 보안 테스트이다. 해킹 도구 및 기술을 사용하여 윤리적 해킹을 하는 침투 테스터가 가짜 공격을 준비하여 보안 팀이 중요한 보안 취약점을 발견하고 대처할 수 있도록 한다. 침투 테스터는 먼저 대상 시스템에 대한 정보 수집을 시작한다. 이때 얻은 지식을 활용해 시스템의 취약점을 찾아낸다. 예를 들어 포트 스캐닝을 했을 때 악성 코드를 보낼 수 있는 열린 포트를 찾을 수 있다. 취약점을 발견했다면 테스트 범위 내에서 다양한 공격을 시도한다. 모의 공격이 끝나고 난 뒤 침투 테스터는 자신이 남긴 로그 및 도구, 임의로 변경한 구성 등의 흔적을 없애고 공격에 대한 보고서를 쓴다. 보안 팀은 해당 보고서를 참고하여 실제 공격에 대한 방어를 강화한다.[4]

2.2. MITRE ATT&CK 프레임워크

MITRE ATT&CK은 실제 관찰을 기반으로 공격자의 Tactic과 Technique에 대한 전 세계적으로 접근 가능한 지식 기반이다.[5] MITRE ATT&CK의 ATT&CK은 악의적 전술(Adversarial Tactics), 기법 및 일반 지식(Technique & Common Knowledge)의 약자이다. ATT&CK은 MITRE에서 공격에 대한 Tactic과 Technique을 문서화하는 것으로 시작되었으나 이후 공격자들의 행동 패턴 분석을 기반으로 TTPs(Tactics, Techniques, Procedures) 정보를 매핑하여 공격자의 행위를 식별할 수 있는 프레임워크로 발전하였다.[6]

[4] 참고 문헌 [4]

[5] 참고 문헌 [5]

[6] 참고 문헌 [6]

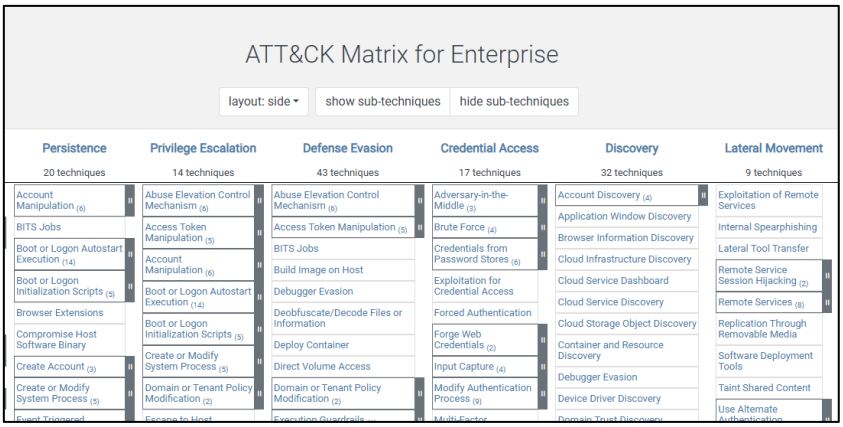


그림 2 MITRE ATT&CK Matrix 일부 (출처: https://attack.mitre.org/)

2.3. CVE (Common Vulnerabilities and Exposures)

CVE는 공개적으로 알려진 컴퓨터 보안 결함 목록이다.[7] MITRE에서 CVE 목록을 유지 및 관리한다. CVE를 통해 여러 보안 전문가들은 동일한 문제를 논의하고 해결하기 위해 노력할 수 있다. CVE 웹사이트에 아이디를 검색하면 취약점에 대한 설명과 CWE(Common Weakness Enumeration), CVSS(Common Vulnerability Scoring System) 등 관련 정보가 표시된다.

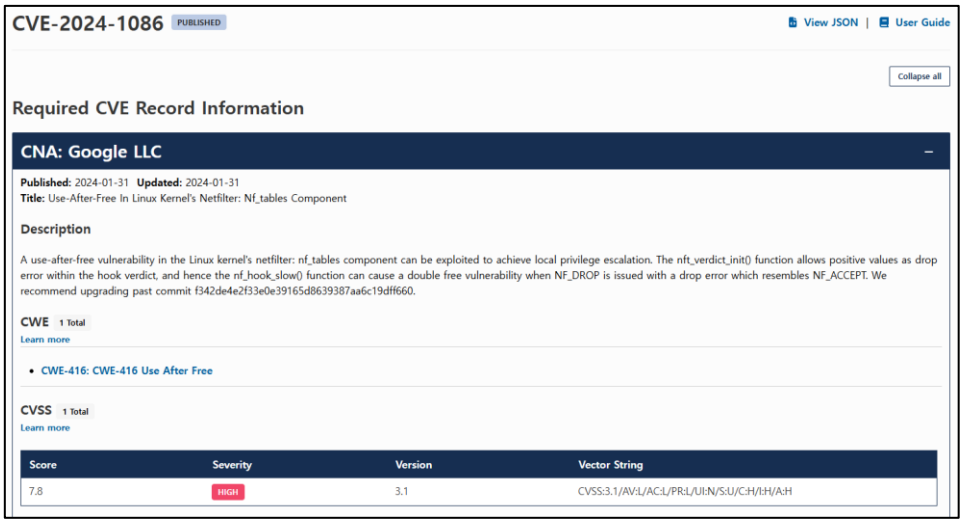


그림 3 특정 CVE 검색 결과

[7] 참고 문헌 [7]

3. 연구 내용

3.1. 시스템 전체 구상도

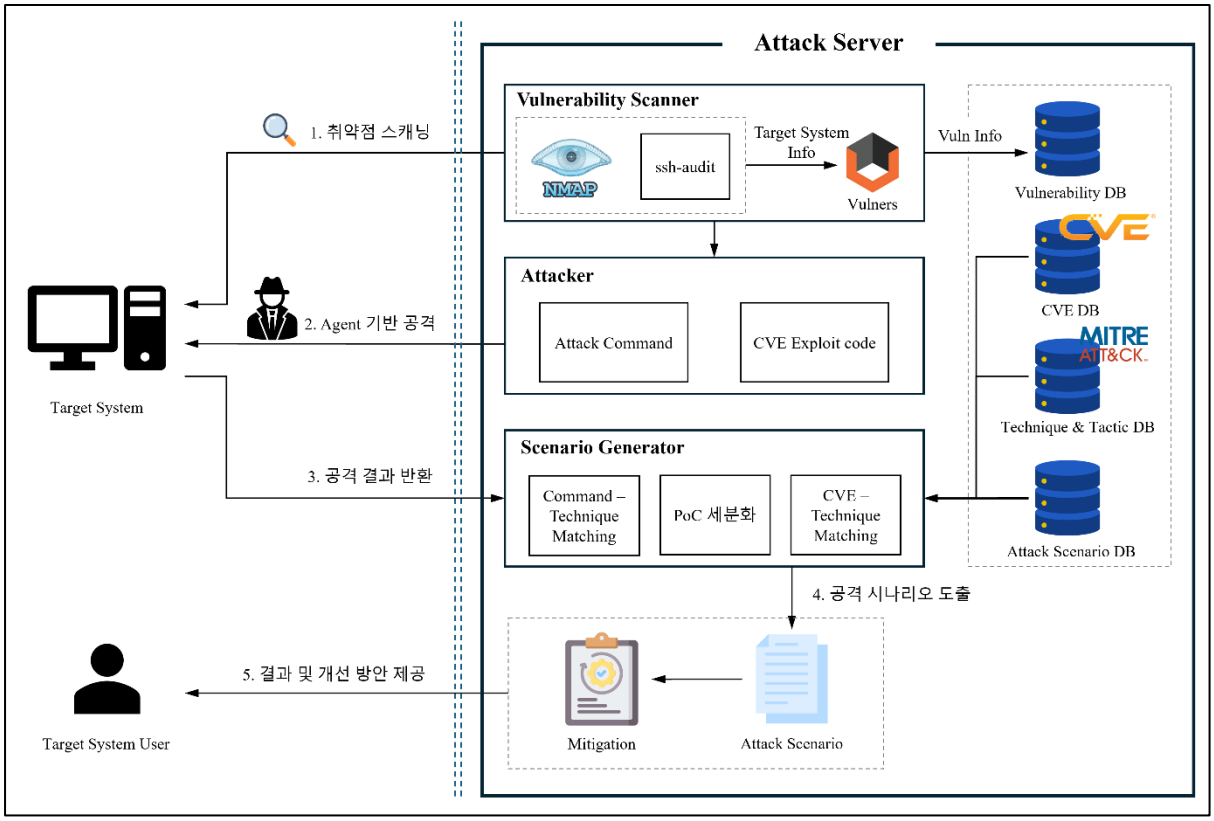


그림 4 MITRE ATT&CK 기반 침투 테스트 자동화 플랫폼 서비스 아키텍처

위 그림은 개발한 플랫폼의 서비스 아키텍처이다. 해당 플랫폼의 Attack Server는 본 과제의 핵심적인 기능을 담당하며, Attack Server는 Vulnerability Scanner, Attacker, Scenario Generator로 구성되어 있다. 각 모듈에 대한 자세한 설명은 아래에 기술한다.

- **Vulnerability Scanner**

  Nmap[8], ssh-audit[9] 등의 툴을 이용하여 대상 시스템을 스캔한다. 스캔한 정보 및 Vulners [10] 를 이용하여 대상 시스템이 가지고 있는 CVE 목록을 추출한 후,

[8] 참고 문헌 [8]

[9] 참고 문헌 [9]

[10] 참고 문헌 [10]

Vulnerability DB에 저장 및 Attacker 모듈에 전달한다.

- **Attacker**

  MITRE ATT&CK의 Technique과 매핑한 CMD 명령어와 CVE Exploit code를 CVE DB, Technique & Tactic DB에서 가져온다. Agent를 통해 해당 공격 명령어로 대상 시스템을 공격하고, 공격 성공 여부를 파악한다.

- **Scenario Generator**

  공격이 성공한 CMD 명령어 및 CVE Exploit code와 매핑된 MITRE ATT&CK Technique을 기반으로 공격 시나리오를 Attack Scenario DB에서 도출한다. 이후 도출된 공격 시나리오와 이에 대한 개선 방안을 대상 시스템 사용자에게 제공한다.

3.2. 공격 시나리오 구현

APT3 공격 사례에서 사용된 Technique별 Windows CMD 명령어를 정리한 자료를 토대로 총 25가지 공격에 해당하는 명령어(하나의 Technique에 중복되는 명령어 존재)를 구현하였으며, 총 8개의 공격 시나리오를 구현했다. 그 중 3개는 CVE의 공개된 PoC를 이용한 시나리오이고 5개는 Windows 환경의 CMD 명령어를 통해 구성된 시나리오이다. 시나리오에 대한 구체적인 설명은 아래에 기술했으며, 시나리오에 사용된 각 Technique은 'Tactic – Technique 이름 (Technique ID)' 형식으로 명시한다.

- **Wi-Fi DoS(Denial-of-Service) 공격 시나리오**

  Wi-Fi DoS 공격 시나리오는 대상 시스템의 Wi-Fi 기능을 차단시킨다. 이 공격 시나리오가 완료되면 사용자는 Wi-Fi 기능을 사용하지 못하게 된다. 해당 시나리오에 사용된 Technique은 다음과 같다.

  ◦ **Discovery – System Network Configuration Discovery (T1016)**

    공격자는 접근하는 시스템의 네트워크 구성 및 설정(예: IP 주소 혹은 MAC 주소 등)에 대한 세부 정보를 찾거나 원격 시스템의 정보 검색을 통해 찾을 수 있다. 또한, 네트워크 장치에서 네트워크 장치 CLI(Command-Line Interface)를 활용하여 정보를 얻을 수 있다. 얻은 정보들을 바탕으로 공격자들은 후속 공격 여부를 결정할 수 있다.

    해당 공격으로 시스템이 Wi-Fi를 사용하고 있는지 확인할 수 있다. 이를 통해 Wi-Fi를 사용하는 것이 확인되었다면 시나리오의 다음 공격을 진행할 수 있다.

◦ **Privilege Escalation – Abuse Elevation Control Mechanism: Bypass User Access Control (T1548.002)**

공격자는 사용자 계정 컨트롤(User Account Control, UAC) 메커니즘을 우회하여 시스템에서 프로세스 권한을 상승시킬 수 있다. UAC는 프로그램의 권한을 상승시켜 관리자 권한으로 작업을 수행할 수 있다. UAC 보호 수준이 가장 높은 수준이 아닌 다른 수준으로 설정된 경우, 특정 Windows 프로그램은 사용자에게 알림 없이 권한을 상승시키거나 일부 상승된 COM(Component Object Model) 객체를 실행할 수 있다.

본 시나리오에서는 Akagi64.exe라는 UAC 우회 도구를 사용한다. Akagi64.exe를 실행시키면 관리자 권한이 있는 CMD가 실행된다. Agent를 통해 Akagi64.exe를 대상 시스템에 업로드 한 뒤, 해당 실행 파일을 실행시킨다.

◦ **Impact – Endpoint Denial of Service (T1499)**

공격자는 사용자에게 제공되는 서비스의 가용성을 저하시키거나 차단하기 위해 Endpoint DoS 공격을 수행할 수 있다. Endpoint DoS는 시스템 리소스를 고갈시키거나 시스템을 악용하여 지속적으로 충돌하게 하여 수행될 수 있다. Endpoint DoS는 서비스에 대한 액세스를 제공하는 데 사용되는 네트워크를 포화시키지 않고 서비스의 가용성을 거부한다.

해당 공격으로 Wi-Fi 모듈이 작동하지 않도록 만들 수 있다. 이는 관리자 권한을 요구하며 아래 그림은 Wi-Fi DoS 공격 시나리오가 진행된 후의 네트워크 구성 상태에서 Wi-Fi 항목이 사라진 모습을 보여준다.

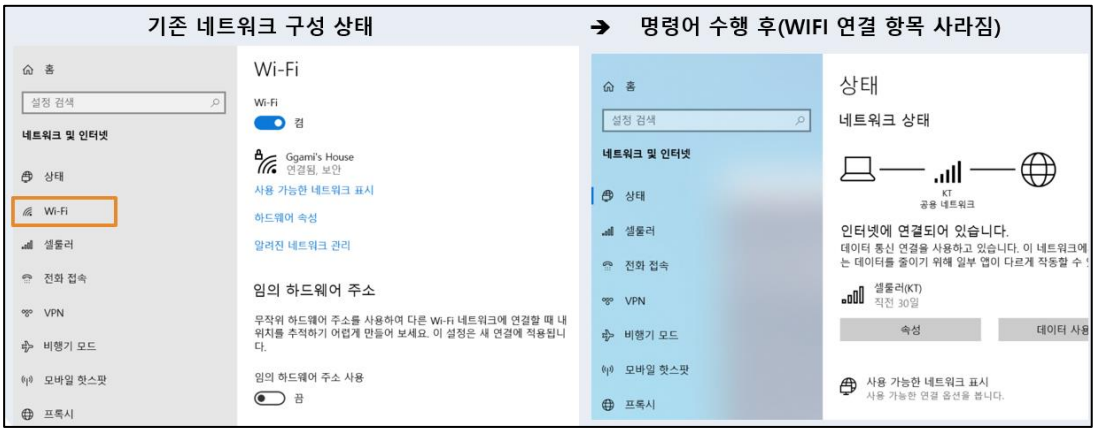


그림 5 Wi-Fi DoS 공격 전후 비교

- **파일 추출 공격 시나리오**

  이 공격 시나리오는 대상 시스템에서 파일을 추출한다. 해당 시나리오에 사용된 Technique은 다음과 같다.

  ◦ **Collection – Data Staged: Local Data Staging (T1074.001)**

  공격자는 Exfiltration(유출) 단계 전에 로컬 시스템의 중앙 위치 혹은 디렉토리에 수집한 데이터를 저장할 수 있으며 CMD와 bash의 기능을 사용하여 데이터를 임시 저장 위치로 복사할 수 있다. 공격자는 여러 위치에서 수집한 데이터를 한곳으로 모아두고 유출하기 쉽도록 준비한다.

  해당 공격으로 대상 시스템에 임의로 폴더를 생성할 수 있다.

  ◦ **Collection – Data from Local System (T1005)**

  공격자는 파일 시스템 및 구성 파일 혹은 로컬 데이터베이스 같은 로컬 시스템 소스를 검색하여 Exfiltration 전에 관심 있는 파일과 민감한 데이터를 찾을 수 있다. CMD 혹은 네트워크 장치 CLI를 사용하여 파일 시스템과 상호 작용하여 정보를 수집할 수 있다.

  해당 공격으로 C:₩Users 하위 경로에서 특정 파일을 찾아낼 수 있다.

  ◦ **Collection – Data Staged: Local Data Staging (T1074.001)**

  해당 공격으로 위에서 찾은 특정 파일을 공격자가 원하는 폴더에 복사하여 추출을 위한 준비를 할 수 있다.

  ◦ **Collection – Archive Collected Data: Archive via Utility (T1560.001)**

  공격자는 Exfiltration 전에 수집된 데이터를 압축하거나 암호화할 수 있다. 데이터를 압축하면 수집된 데이터를 난독화하고 네트워크를 통해 보내지는 데이터 양을 최소화할 수 있다. 또한, 암호화를 통해 탐지 혹은 검사 시에 추출되는 데이터를 숨길 수 있다.

  해당 공격으로 공격자가 수집한 파일이 있는 폴더를 압축하여 추출을 위한 준비를 할 수 있다.

  ◦ **Exfiltration – Exfiltration Over C2 Channel (T1041)**

  공격자는 기존 명령 및 제어 채널을 통해 데이터를 훔칠 수 있다.

  해당 공격을 통해 파일을 지정한 주소로 보낸다. 이를 통해 공격자는 앞서 찾

은 파일을 마음대로 추출할 수 있다.

본 시나리오를 통해 공격자는 대상 시스템에서 원하는 파일을 추출하여 자신의 서버로 전송할 수 있다.

- **사용자 비밀번호 임의 변경 공격 시나리오**

  이 공격 시나리오는 사용자 계정의 암호를 현재 모르더라도 임의로 바꿀 수 있다. 해당 시나리오에 사용된 Technique은 다음과 같다.

  ◦ **Discovery – System Owner/User Discovery (T1033)**

  공격자는 계정 사용자 이름을 검색하거나 OS Credential Dumping(OS 캐시, 메모리 등에서 얻을 수 있는 자격 증명을 탈취) 등을 이용하여 기본 사용자, 현재 로그인한 사용자, 일반적으로 시스템을 사용하는 사용자가 시스템을 적극적으로 이용하고 있는지 식별할 수 있다. 사용자 정보를 통해 후속 동작 여부를 결정할 수 있다.

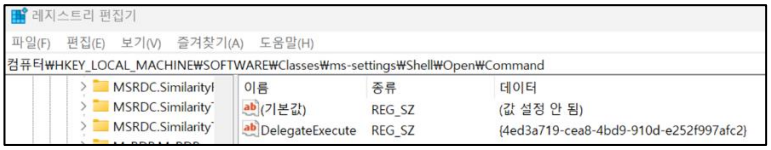
  해당 공격으로 현재 사용자 계정 이름을 알 수 있다. 바꾸고자 하는 사용자 계정을 파악한다.

  ◦ **Privilege Escalation – Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)**

  해당 Technique은 Wi-Fi DoS 공격에서도 다뤘던 권한 상승 Technique이다. Akagi64.exe 도구를 통해 해도 되지만, 여기서는 또 다른 방법인 Fodhelper와 관련된 레지스트리 키를 수정하여 UAC를 우회한다. Fodhelper.exe가 저장된 경로는 다음과 같다.

  C:₩Windows₩System32₩fodhelper.exe

  Windows에서 기본적으로 System32 폴더 내부에 저장된 프로그램은 Microsoft가 신뢰하는 파일로 인식하여 자동으로 권한이 상승되어 실행되는데, Fodhelper는 실행 시 HKCU:₩Software₩Classes₩ms-settings₩shell₩open₩command 키의 Default 값에 저장된 명령도 실행된다. 이 또한 마찬가지로 관리자 권한으로 실행된다.



  여기서 (기본값)으로 표시된 것을 C:₩Windows₩System32₩CMD.exe 로 바꾼

뒤, Fodhelper를 실행시키면 UAC를 우회할 수 있다.

참고로, Fodhelper는 Windows에서 기본으로 제공하는 "선택적 기능"에 해당한다. 아래 그림은 Fodhelper 화면을 나타낸다.

그림 6 Fodhelper 화면

◦ **Impact – Account Access Removal (T1531)**

공격자는 사용자의 계정에 대한 액세스를 방해하여 시스템 및 네트워크 리소스의 가용성을 방해할 수 있다. 계정 삭제, 잠금, 조작(예: 자격 증명 변경) 등을 통해 액세스를 방해할 수 있으며, 이를 통해 로그오프하거나 시스템을 종료 혹은 재부팅할 수 있다.

해당 공격을 통해 사용자 계정 비밀번호를 임의로 변경할 수 있다. 참고로, 제어판 - 사용자 계정에서 비밀번호를 변경하려면 아래 그림과 같이 현재 암호를 필요로 한다. 현재 암호를 모르더라도 공격자가 원하는 암호로 변경할 수 있기에 치명적이다.

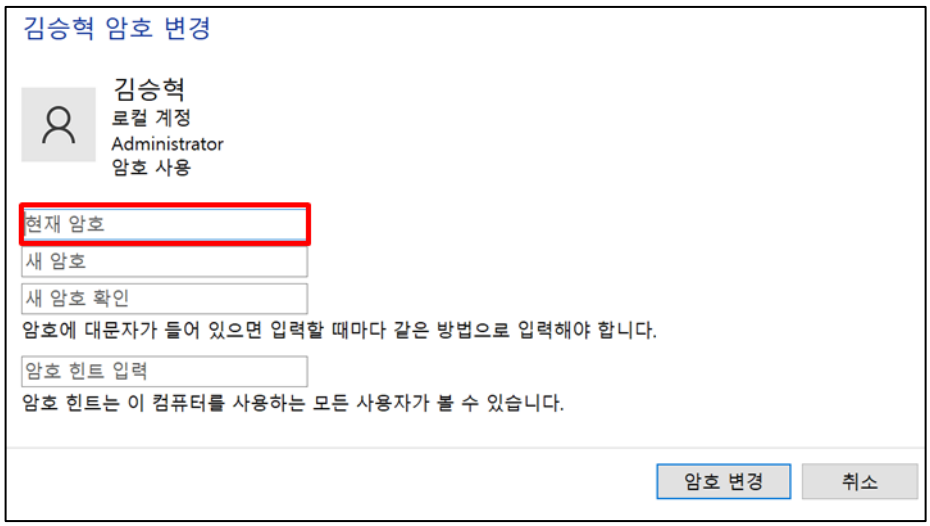


그림 7 제어판 - 사용자 계정 암호 변경

- **실행 파일을 특정 process id에 강제 주입하는 공격 시나리오**

  이 공격 시나리오는 소유자가 현재 사용자인 Process에 실행 파일을 주입한다. 해당 시나리오에 사용된 Technique은 다음과 같다.

  ◦ **Discovery – Process Discovery (T1057)**

  공격자는 실행 중인 시스템에 대한 정보를 얻으려 시도할 수 있다. 얻은 정보를 사용하여 대상을 완전히 감염시키거나 특정 작업 시도 여부 등의 후속 동작을 결정할 수 있다.

  이 공격을 통해 소유자가 현재 사용자의 프로세스 목록을 JSON 형태로 가져올 수 있다.

  ◦ **Defense Evasion – Process Injection: Portable Executable Injection (T1055.002)**

  공격자는 프로세스 기반 방어를 회피하고 권한 상승을 위해 프로세스 내에 실행 파일(Portable Executable, PE)을 주입할 수 있다. PE 주입을 통해 특정 프로세스 주소 공간 내에서 임의의 프로세스를 실행한다.

  해당 공격은 특정 서버 URL로부터 파일을 다운로드 받아 특정 프로세스 ID에 강제로 실행 파일을 주입시키는 공격이다. 현재 사용자가 소유자인 프로세스 ID를 요구하므로 이전 공격에서 출력된 값을 바탕으로 공격을 진행한다.

- **원격으로 연결된 host shell 획득 공격 시나리오**

  PsExec.exe를 통해 원격에 있는 다른 대상 시스템으로의 shell을 얻는 공격 시나리오이다. 이 과정에서 brute-force 공격과 조합하여 대상 시스템과 연결된 원격 시스템의 계정 정보를 알아내고 해당 시스템의 Shell 권한을 획득할 수 있다.

  ◦ **Command and control - Ingress Tool Transfer (T1105)**

  공격자는 도구나 다른 파일을 외부 시스템에서 손상된 환경으로 전송한다. 손상된 환경 내에서 피해자 장치 간에 도구를 전송 및 확산할 수 있다.

  본 시나리오에서는 PsExec.exe가 포함된 PsTool을 강제로 설치하여 공격을 시작한다. PsTool은 Microsoft에서 제공하는 Sysinternals Suite의 일부로, 시스템 관리 및 진단을 위한 다양한 도구를 포함한다. 주로 원격 프로세스 실행, 프로세스 관리, 시스템 정보 수집 등 다양한 기능을 제공하여 IT 관리자들이 시스템을 효율적으로 관리하는 데 도움을 준다.

◦ **Discovery - System Network Connections Discovery (T1049)**

공격자는 네트워크를 통해 정보를 쿼리하여 현재 액세스 중인 시스템에 네트워크 연결 목록을 얻을 수 있다. 클라우드 기반 환경의 일부인 시스템에 접근하는 공격자는 가상 사설 클라우드(Virtual Private Clouds) 또는 가상 네트워크(Virtual Networks)를 매핑하여 연결된 시스템과 서비스를 확인한다.

해당 공격을 통해 원격으로 연결된 대상 시스템의 정보를 획득한다.

◦ **Lateral Movement - Remote Services (T1021)**

공격자는 합법적인 애플리케이션(소프트웨어 배포 도구 및 기타 관리 프로그램)을 통해 원격 연결을 허용하는 서비스에 로그인할 수 있다. 그 다음 로그인한 사용자로 작업을 수행한다.

해당 공격에서는 brute-force 공격을 통해 원격으로 연결된 대상 시스템으로 접속한다.

CVE를 공격하는 시나리오는 각 CVE의 PoC 코드를 분석한 후 동작 흐름을 파악하여 MITRE ATT&CK의 Technique을 매핑하여 공격 시나리오를 구현했다. 총 3개의 리눅스 커널 관련 CVE를 분석하고 각각의 PoC를 시나리오로 구현하였다. 해당 시나리오는 모두 공개된 PoC를 기반으로 하며, PoC를 최신화하고 개발한 플랫폼의 사용 방식에 맞게 수정하였다. PoC의 동작 흐름에 따라 아래는 특정 CVE의 PoC를 분석한 그림이다.

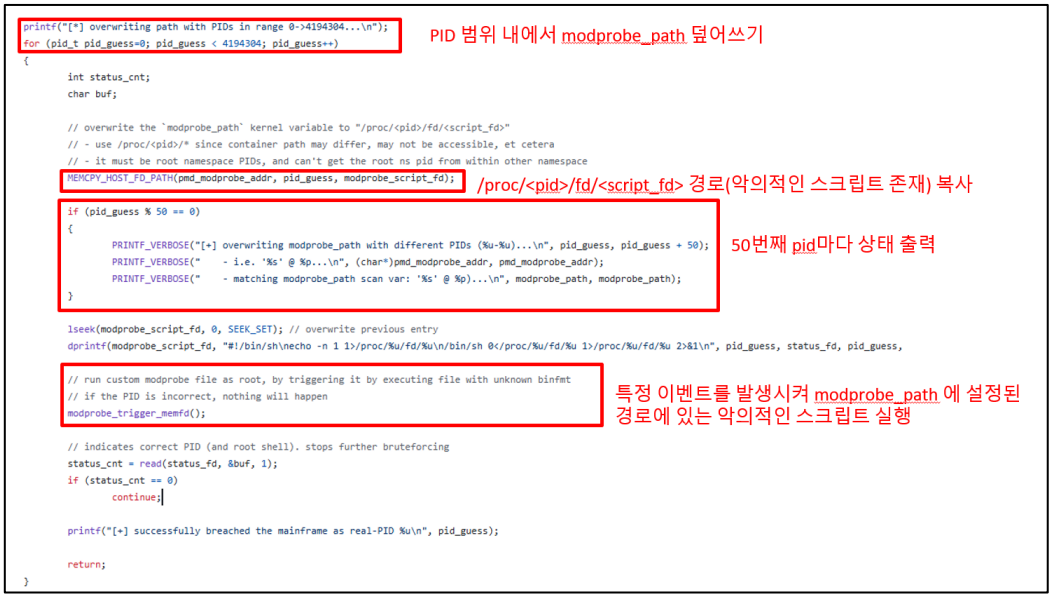


그림 8 CVE 2024-1086의 PoC 분석

아래는 분석한 PoC의 동작 흐름에 따라 MITRE ATT&CK의 Technique을 매핑한 그림이다.

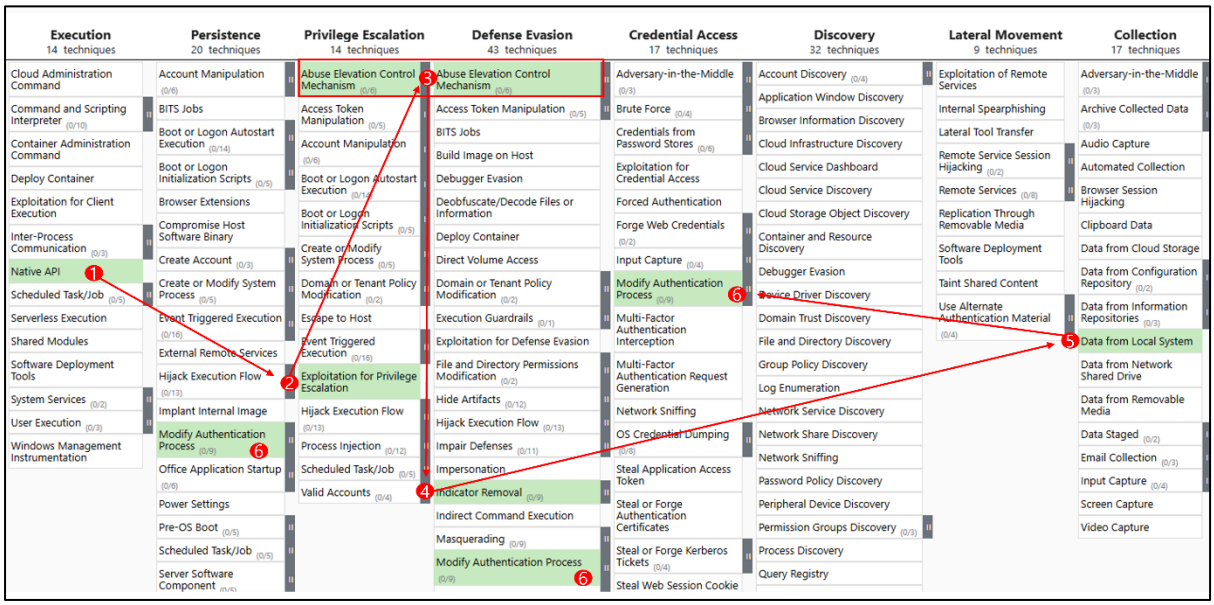


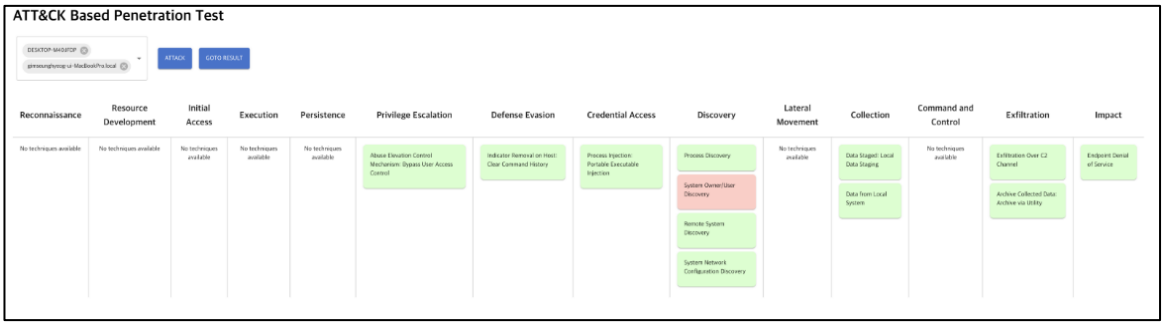
그림 9 CVE 2022-0847 PoC와 매핑된 Technique

대상 시스템에서 PoC를 실행했을 때 루트 권한 탈취 등 의도했던 공격이 성공한다면 시스템이 해당 Exploit이 성공했다고 판단한다. CVE ATTACK을 통해 밝혀낸 CVE 목록 중에 해당하는 CVE 정보가 있다면 Exploit을 실행한다.

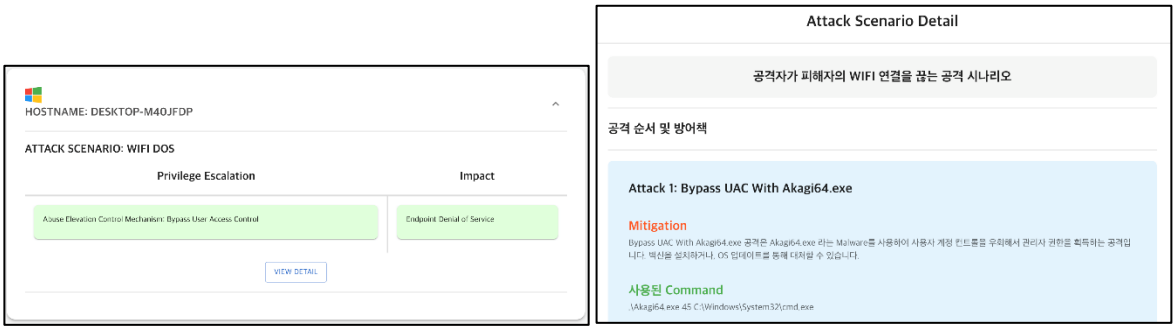
3.3. 침투 테스트

3.3.1. MITRE ATT&CK 기반 침투 테스트

본 기능은 MITRE ATT&CK 프레임워크에서 정의한 Technique에 해당하는 명령어들을 대상 시스템의 Agent를 통해 실행하는 방식으로 동작한다. 각 명령어가 실행되면, 반환된 값을 파싱하여 해당 데이터가 다음 공격 단계에 활용될 수 있는지를 판단한다. 이때 진행 과정은 MITRE ATT&CK의 Tactic 순서에 따라 체계적으로 이루어지며, 각 Tactic 단계에서 명령어들의 결과를 사용하여 특정 공격 시나리오를 구성한다. 생성된 시나리오에 사용된 Technique가 초록색 블록으로 표현되어, 시나리오 전체의 흐름에서 어느 지점에서 어떤 Technique이 적용되었는지 파악할 수 있다.



결과 창으로 이동하면 대상 시스템에서 식별된 취약점을 활용한 다양한 공격 시나리오가 표시된다. 각 시나리오에는 설명과 더불어, 해당 취약점에 대한 구체적인 방어책 및 공격 과정에서 사용된 명령어 목록이 포함되어 있다. 아래 그림은 결과 화면에서 보여지는 시나리오 설명 및 방어책이다.



3.3.2. CVE Exploit 기반 침투 테스트

본 기능에서는 먼저 대상 시스템의 IP 주소 또는 Agent를 이용해 취약점 탐색 과정을 수행한다. 탐색 단계에서 대상 시스템을 Nmap, ssh-audit 등 포트 스캐닝 및 취약점 스캐닝 도구(혹은 오픈 소스)를 사용하여 스캔한다. 스캐닝을 통해 알아낸 정보를 토대로, VulnersDB에 APIkey를 사용하여 CVE 목록을 검색한다. 그림 10은 해당 공격의 간단한 순서도를 나타낸다.

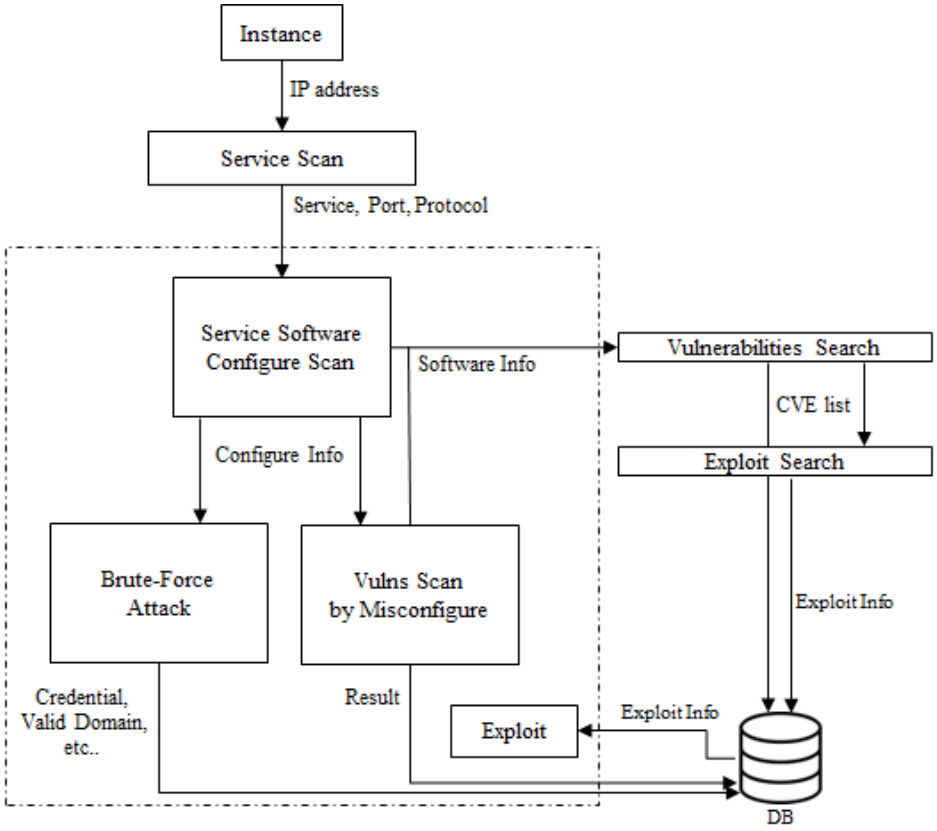


그림 10 CVE Exploit 기반 침투 테스트의 순서도

이때 확인된 CVE 목록 중에서 Exploit 가능성이 있는 항목을 식별하고 해당 Exploit code를 실행한다. 의도한 결과가 나오면 대상 시스템이 해당 CVE 공격 시나리오에 취약하다고 판단한다. 아래는 Exploit이 성공한 CVE들의 목록을 CVE ID, 사용된 Technique, Mitigation 정보와 함께 제공하는 결과 화면이다.

CVE List

CVE ID	Used Technique	Mitigation
CVE 2024-1086	T1068 T1543 T1547 T1059 T1203	If you are using Linux kernel version 3.15 ~ 6.1.76 / 6.2 ~ 6.6.15 / 6.7 ~ 6.7.3, update the kernel to the latest version
CVE 2021-44228	T1190 T1059 T1203 T1068 T1105 T1071	Log4j 2.15.0 has been released to address the vulnerability

그림 11 대상 시스템에 공격 성공한 CVE 목록

3.4. GUI 개발

3.4.1. 메인 화면

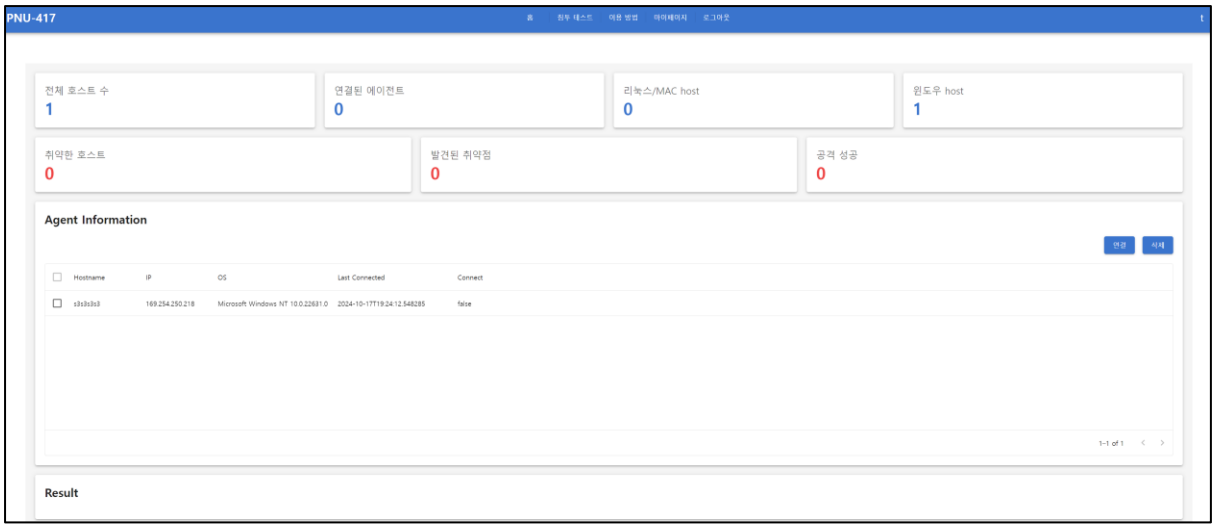


그림 12 메인 화면

로그인 직후 화면으로 사용자가 연결한 호스트의 요약 정보 및 침투 테스트 결과를 간략하게 정리하여 표시해주는 페이지이다.

3.4.2. 침투 테스트 진행 페이지

3.4.2.1. Agent 관리

그림 13 Agent 관리 화면

상단 메뉴바에 있는 침투 테스트 버튼을 통해 침투테스트 화면으로 넘어올 수 있다. 가장 먼저 Agent를 관리할 수 있는 화면이 표시된다. 해당 페이지에서는 침투 테스트를 진행할 PC에 Agent를 연결하거나 삭제할 수 있으며 연결상태 등을 확인할 수 있다. 연결 버튼을 누르면 Agent 연결을 위한 가이드라인을 제시해준다.

여기서, Agent는 공격 대상 시스템에 실행되는 프로그램으로, 침투 테스트 플랫폼과 http 프로토콜을 사용해서 연결되어 공격을 진행하는데 있어 도움을 준다.

3.4.2.2. MITRE ATT&CK 기반 침투 테스트

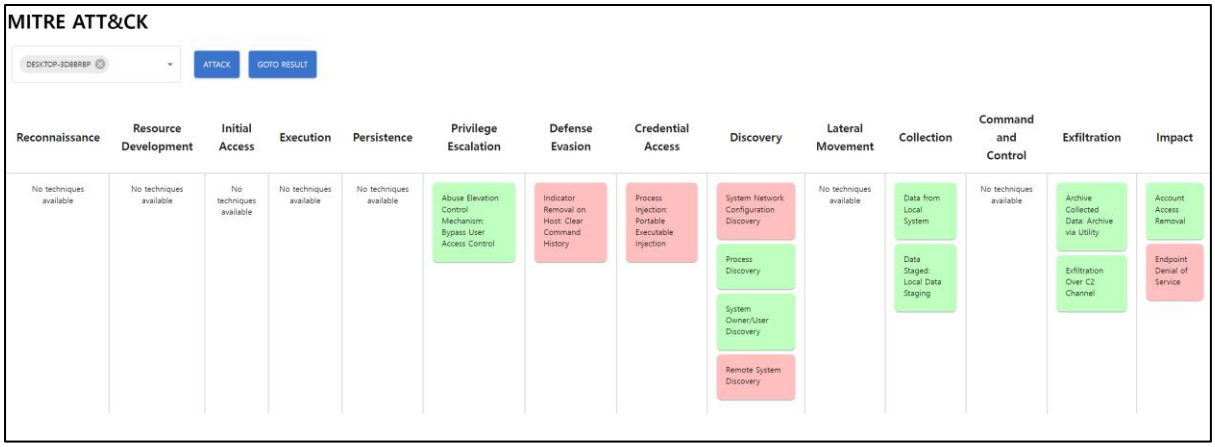


그림 14 MITRE ATT&CK 기반 침투 테스트 화면

앞서 연결한 Agent에 대해서 MITRE ATT&CK 기반 침투 테스트를 진행할 수 있는 화면이다. MITRE ATT&CK 프레임워크를 기반으로 다양한 형태의 공격을 진행한다. 각 Tactic에 따른 일정 Technique을 나타내며 연결된 Agent를 선택 후 ATTACK을 클릭하여 자동으로 침투 테스트를 진행할 수 있다. 성공한 공격에 대해서는 초록색, 실패한 공격은 빨간색으로 표시되어 사용자가 공격 경과를 한 눈에 알아보기 쉽도록 구성하였다.

3.4.2.3. CVE Exploit 기반 침투 테스트

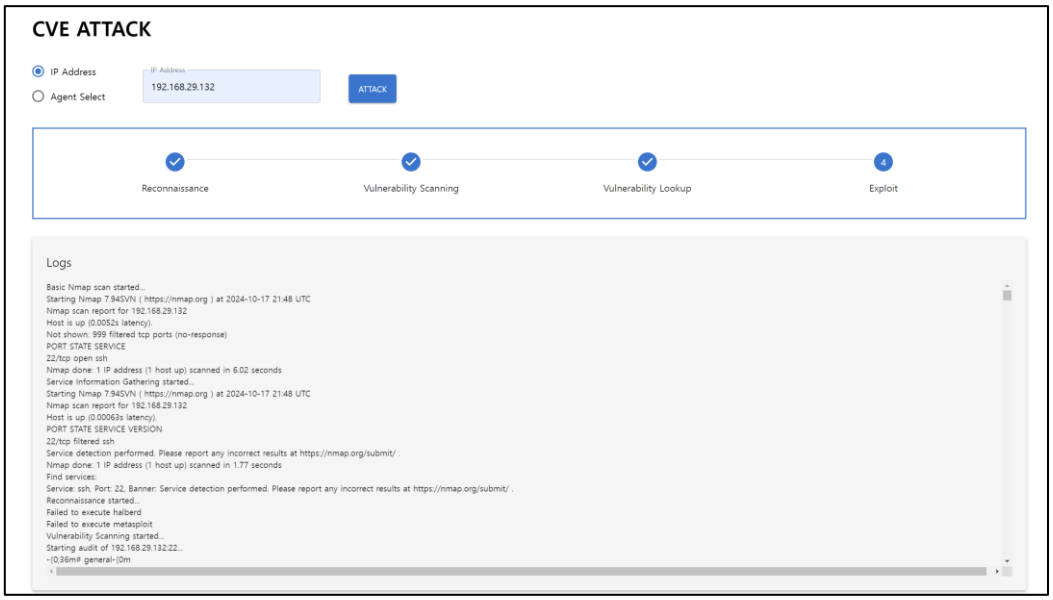


그림 15 CVE ATTACK 화면

해당 화면에서는 Agent의 연결 없이도 IP 주소만으로 해당 시스템의 알려진 취약점

(CVE)을 탐색할 수 있다. 침투 테스트 경과에 따라 아래 log가 표시된다. 찾아낸 CVE 중 구현된 Exploit PoC가 있을 경우 Exploit 공격으로 이어질 수 있다.

3.4.3. 결과 페이지

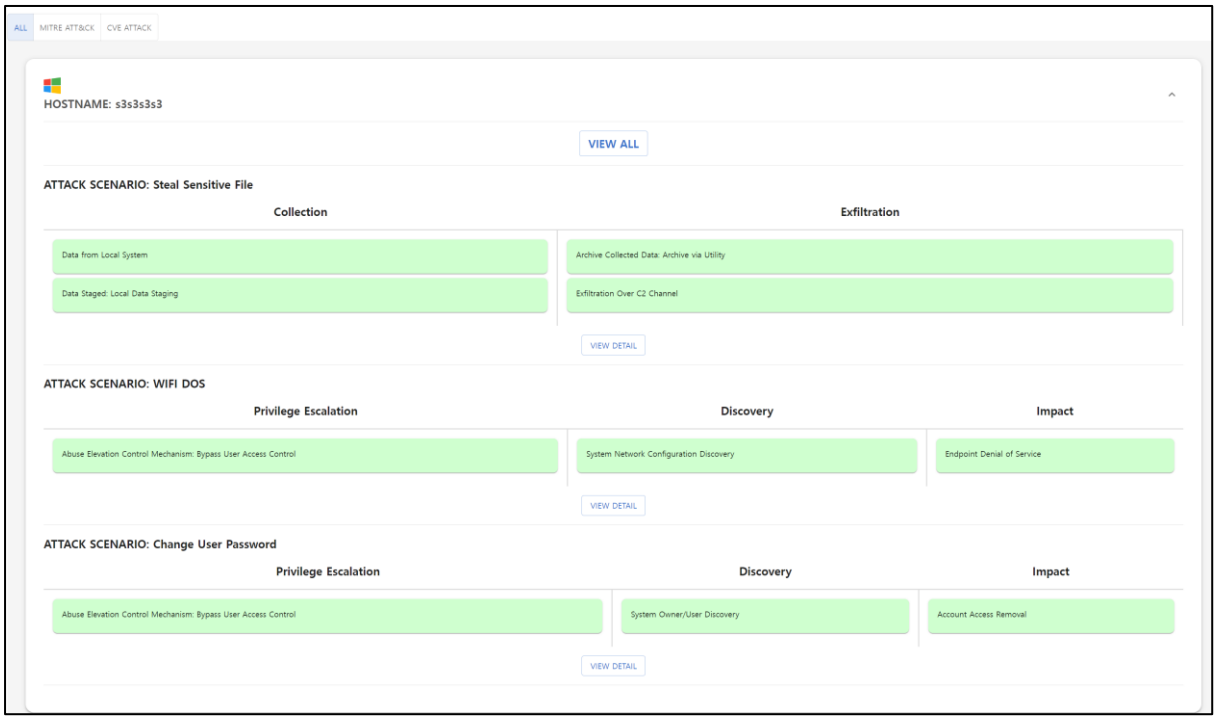


그림 16 침투 테스트 결과 화면 1

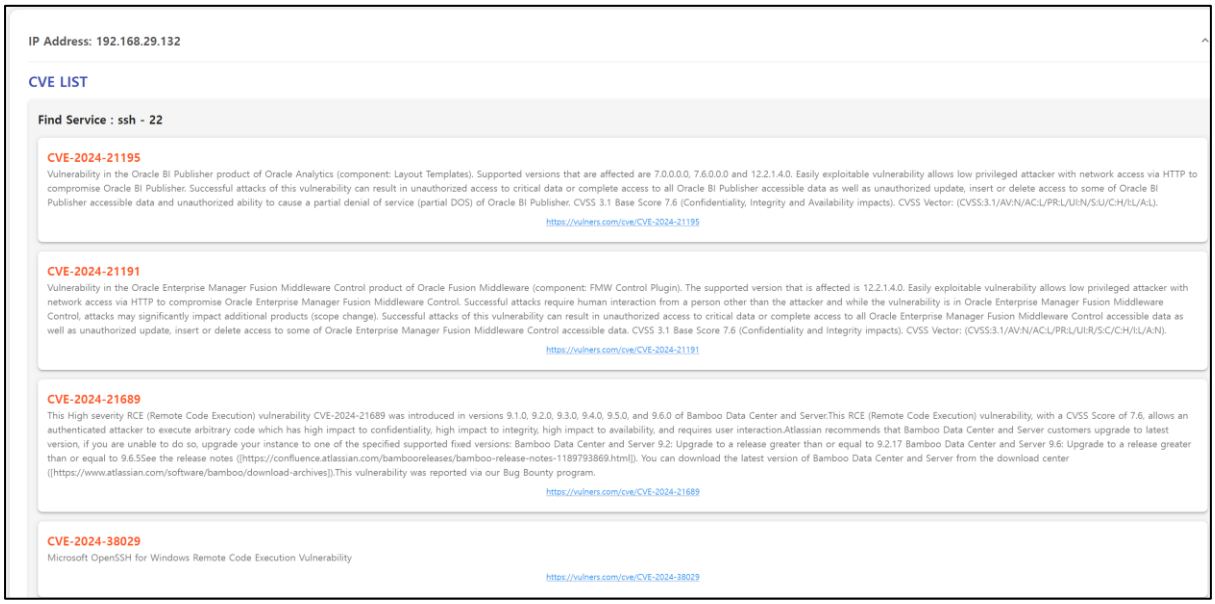


그림 17 침투 테스트 결과 화면

해당 화면에서는 앞서 실시한 침투 테스트에 대한 결과를 보고서 형식으로 확인할 수 있는 페이지이다. 그림 16은 MITRE ATT&CK 기반의 침투 테스트 결과를 나타낸다. View Detail을 눌러서 각 항목에서 어떤 공격이 수행되었고 그에 대응하는 완화 방법이 무엇인지 알 수 있다. 그림 17은 CVE ATTACK에서 실시한 침투 테스트 결과를 나타내며 IP 주소에 따른 CVE List를 나타낸다.

4. 연구 결과 분석 및 평가

4.1. MITRE ATT&CK 기반 공격 시나리오 평가

MITRE ATT&CK 기반 공격 평가는 Windows 10 운영체제를 사용하는 노트북과 VM을 Target System으로 설정하였다. 또한 노트북 환경에서는 Windows Defender를 종료했을 때와 실행 중일 때 공격이 어떻게 수행되는지 분석하였다. 각 공격 시나리오에 대해 성공 여부는 공격을 모두 실행 후 Target System의 반응을 기반으로 평가하였다. Wi-Fi DoS는 Wi-Fi 항목이 차단되는지 여부, 파일 추출은 C:₩Users 하위 폴더에 있는 pdf 파일 하나를 추출했는지 여부, 사용자 비밀번호 변경은 비밀번호 변경 여부, 프로세스 강제 주입은 대상 프로세스에 주입 성공 여부, 원격 호스트 Shell 획득 여부를 평가하여 성공, 실패를 각각 O, X 로 표시하였다.

각 공격 시나리오에 대한 평가 표는 다음과 같다.

	노트북 + Windows Defender	노트북 No Defender	Windows VM No Defender
Wi-Fi DoS	X	O	X
파일 추출	O	O	O
사용자 비밀번호 변경	X	O	X
프로세스 강제 주입	O	O	O
원격 호스트 Shell 획득	X	O	O

그림 18 MITRE ATT&CK 공격 시나리오 평가 표

해당 결과를 통해 Windows Defender가 권한 상승을 요구하는 공격을 수행했을 때 감지하여 차단하는 것을 확인하였다. 조사 결과, Windows Defender는 권한 상승을 요구하는 공격에 대해 UAC (User Account Control) 모니터링을 통해 탐지 및 차단하는 것으로

나타났다. 이는 공격 실행 시 관리자 권한 요청이 발생할 때, 공격자의 활동을 중단시키는 역할을 한다. 따라서 권한 상승을 요구하는 공격인 Wi-Fi DoS, 사용자 비밀번호 변경, 원격 호스트 Shell 획득 등의 공격이 모두 실패하는 것을 확인하였다.

그리고 노트북에서는 인터넷 연결을 WI-FI를 통해서 했지만 VM의 경우 WI-FI로 연결된 것이 아니어서 Wi-Fi DoS 공격에서 실패한 것을 확인할 수 있었다. 또한 VM의 경우 VMware Workstation Pro 17을 사용하여 Windows 10 VM을 생성하였는데, 사용자 비밀번호를 변경할 때, 관리자 권한을 획득 했음에도 변경할 권한이 없다는 출력 값을 반환하였다. VMware 환경에서 사용자 비밀번호 변경 공격이 실패한 이유는 VMware의 보안 정책으로 인해 운영 체제 내 특정 권한이 제한되었기 때문이다. 이는 VM 내부의 프로세스가 하이퍼바이저에서 별도의 보안 제어를 받아 사용자 계정 관련 권한이 제약되는 사례로 분석되었다.

침투 테스트 플랫폼의 결과 화면에서도 그림 18의 내용과 같은 결과를 보여주는 것을 확인했다.

4.2. CVE 스캐닝 평가

Ubuntu 18.04 데스크톱 버전에 ssh 서버를 설치하여 Target System으로 설정한 뒤 평가를 진행하였다.

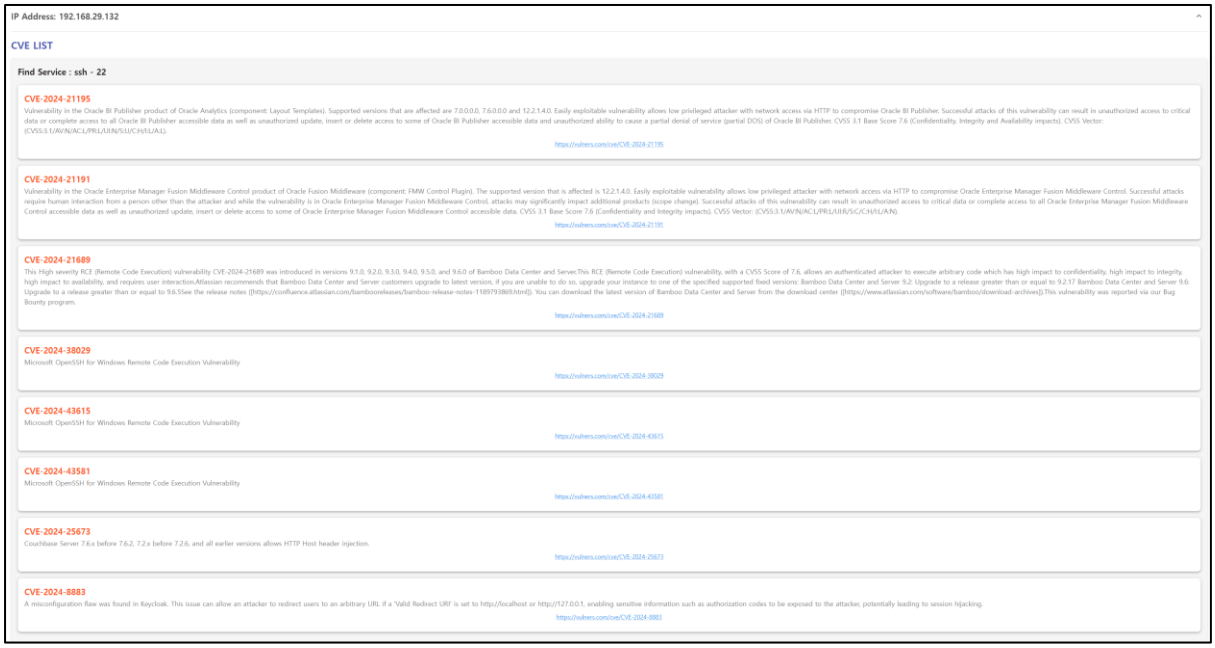


그림 19 Ubuntu 18.04 대상 CVE 스캐닝 결과

그림 19는 해당 IP 주소에 대응하는 서비스와 그에 해당하는 CVE 목록을 나타낸다. 적절하게 수행된 것으로 확인했다.

4.3. Exploit 평가

위에서 CVE 목록을 읽고 Exploit으로 구현된 CVE-2024-1086, CVE-2021-44228 등이 발견될 경우, Exploit으로 연결되는 지 평가한다. CVE ATTACK에서 바로 해당 Exploit을 실행할 수 있거나, CVE ATTACK으로 CVE 목록을 탐색한 뒤, MITRE ATT&CK 기반 침투 테스트를 실행하여 Exploit PoC를 Agent를 통해 해당 PC에 업로드 한 뒤 진행하는 것을 확인하였다.

4.4. 멘토 의견서 대응 방안

- **클라우드 환경에서 테스트를 하지 않은 점이 아쉬움**

  기존 목표인 클라우드 환경이 아닌 VM을 선택한 이유는 실제 퍼블릭 클라우드 서비스에 협력을 구해야 하는 제약사항 때문이다. 최대한 비슷한 환경을 생각하여 VMware 기반으로 VM을 생성하여 테스트 환경을 구축하였다. 해당 제약사항으로 인한 문제는 향후 연구를 진행하면서 퍼블릭 클라우드 서비스에 침투 테스트 관련 협력을 요청하여 승인받아 상용되는 클라우드 서비스(AWS, Azure, GCP 등)에서 진행할 수 있을 것이다.

5. 결론 및 향후 연구 방향

본 과제에서는 클라우드 및 온프레미스 환경에서의 보안 공격 자동화 도구를 개발했다. 이 도구는 Agent를 설치하거나 시스템의 IP 정보를 통해 대상 시스템에 자동으로 침투 테스트를 진행한다. 각 Technique에 해당하는 명령어를 실행한 결과를 바탕으로 공격 시나리오를 생성하고 이에 대한 정보를 사용자에게 제공한다. 또한 대상 시스템에 대한 CVE를 탐색한 후, 탐색 결과를 기반으로 Exploit을 진행하여 두 정보를 종합한 공격 가능 시나리오를 도출한다. 이를 통해 사용자들은 자신의 시스템의 취약점을 파악하고 사전에 예방할 수 있다. 또한, 시나리오를 보여줌으로써 취약점을 통해 최종적으로 어떤 공격이 이루어질 수 있는지 쉽게 파악할 수 있다.

현재 MITRE ATT&CK 프레임워크에 등록되어 있는 Technique은 대략 400개이다. 하지만 본 과제는 25개의 Technique만을 구현하여 탐지하지 못하는 취약점들이 많고, 생성할

수 있는 시나리오에도 한계가 있다.

향후에는 클라우드 환경 대상의 시나리오를 추가하고, 추가적인 Technique 구현을 통해 더 많은 시나리오를 생성할 것이다.

6. 참고 문헌

[1] 송현경. 클라우드 마이그레이션 산업 및 기술 동향. TTA Journal vol.203, 2022. SEP/OCT
[2] 조미덥. (2021, Dec 12). 국내 클라우드 '공공' 타고 뜬다. Available: https://www.khan.co.kr/economy/economy-general/article/202112122122005#c2b
[3] 뉴시스. (2020, April 15). "클라우드 보안 문제 주요 원인은 '설정 오류' … 사이버 범죄 주의". Available: https://www.newsis.com/view/NISX20200415_0000994898
[4]홍은주. (2022, April 6). 디지털 전환의 시작, 클라우드 마이그레이션 - 1 성장하는 시장. Available: https://www.samsungsds.com/kr/insights/cloud_migration.html
[5] 박재현. (2021, Mar 31). [초점] '클라우드 전환' 관심은 높지만 실행은 '주춤'. Available: https://www.comworld.co.kr/news/articleView.html?idxno=50164
[6] IBM. 침투 테스트란 무엇인가요?. Available: https://www.ibm.com/kr-ko/topics/penetration-testing
[7] The MITRE cooperation. ATT&CK. Available: https://attack.mitre.org/
[8] https://nmap.org/
[9] https://github.com/jtesta/ssh-audit
[10] https://vulners.com/