MITRE ATT&CK 기반의 자동화된 Red Team 공격 시뮬레이션 설계 및 구현

오윤경 [1], 곽진 [2]
[1] 아주대학교 사이버보안학과 학부생
[2] 아주대학교 사이버보안학과 교수

charming2005@ajou.ac.kr, security@ajou.ac.kr

Design and Implementation of Automated Red Team Attack Simulation Based on MITRE ATT&CK Framework

Yun-Gyeong Oh
Dept. of Cyber Security, Ajou University

요 약

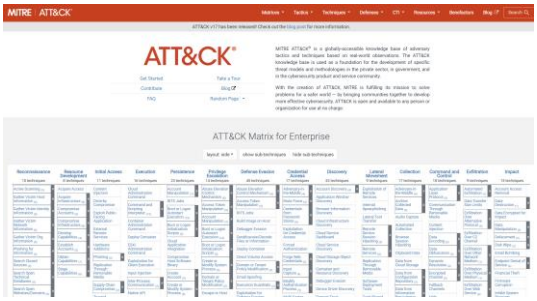
본 연구는 최근 증가하는 고도화된 사이버 위협에 대응하기 위하여 MITRE ATT&CK 프레임워크를 기반으로 Red Team 공격 시나리오의 자동화 방법을 제시한다. 이를 위해 공격 자동화 플랫폼인 Caldera 와 오픈 소스 프레임워크 Metasploit, Sliver 를 활용하여 공격 시나리오를 설계하고 구현하였다.

1. 서론

사이버 공격이 점차 고도화되고 다양화됨에 따라 기존의 방어체계만으로는 복합적인 공격을 탐지하고 대응하기 어려워지고 있다. 이에 따라 공격자의 관점에서 보안 취약점을 선제적으로 식별하고 대응하는 Red Team 의 필요성이 대두되고 있다. 이번 연구는 MITRE ATT&CK 프레임워크를 기반으로 구체적이고 표준화된 공격 시뮬레이션 시스템을 설계하고 이를 자동화하여 Red Team 의 효율성과 정확성을 향상시키는 동시에 보안 체계를 강화하는 것을 목표로 한다.

2. Red Team 과 MITRE ATT&CK 프레임워크

Red Team 은 실제 공격자의 관점에서 모의 공격을 수행하여 시스템의 보안 취약점을 식별한 뒤 보안 체계의 한계점을 분석하여 개선을 지원하는 역할을 한다. 이러한 모의 공격을 체계화하기 위해 MITRE ATT&CK 프레임워크가 주목받게 되었는데, MITRE ATT&CK 프레임워크는 공격자가 사용하는 다양한 방법론을 문서화하기 위해 고안된 프레임워크이다. 실제 공격 사례에서 수집된 전술(Tactics), 기법(Techniques), 절차(Procedures), 방어 전략(Defenses) 등을 구조화하여 제공한다. 하지만 수작업으로 이루어지는 전통적인 모의 공격은 시간과 인력 소모가 크고, 다양한 시나리오를 충분히 반복 적용하기엔 어려움이 있다. 따라서 표준화된 공격 데이터를 이용한 공격 자동화(BAS, Breach and Attack Simulation)를 통해 반복적인 공격을 신속하게 수행하고 다양한 시나리오를 적용함으로써 수작업 대비 높은 효율성을 확보할 수 있다.



(그림 1) MITRE ATT&CK 프레임워크 사진

3. 자동화 공격 시뮬레이션 설계

본 연구에서는 오픈소스 기반의 공격 시뮬레이션 및 침투 테스트 도구인 Caldera, Metasploit, Sliver 를 사용하였다. Caldera 는 MITRE 기관에서 개발한 공격 자동화 프레임워크로, ATT&CK 프레임워크에 기술된 다양한 공격 전술과 기법을 자동화된 시나리오 형태로 수행할 수 있도록 개발되었다. 해당 프레임워크는 대상 시스템에 배포된 Agent 를 통해 공격을 수행하며, 체계적이고 반복적인 공격 테스트를 지원한다. Metasploit 은 다양한 취약점 공격 및 침투 테스트

기능을 제공하는 프레임워크로, Caldera 와 연계하여 고도화된 공격을 수행하는 데 활용된다. Sliver 는 Command and Control(C2) 프레임워크로서 공격자가 대상 시스템에 대해 안정적이고 지속적인 통제 및 관리를 수행할 수 있도록 지원한다. 이러한 세 가지 도구를 연계하여 공격자의 내부 정보 수집, 권한 상승 등 일련의 공격 단계를 자동화하고 현실적인 공격 시나리오를 설계하였다.

4. 공격 시나리오 구현 및 실험

본 연구에서는 피싱, 악성코드 감염 등으로 인해 초기 침투가 이루어진 상황을 가정하고 실험을 시작하였다. 먼저 Sliver 를 이용하여 대상 시스템에 Caldera Agent 를 설치한 뒤, Caldera 를 통해 대상 시스템의 커널 버전, 라이브러리(glibc, pip 등) 버전 등을 확인한다. 이후 수집한 버전을 바탕으로 Python 스크립트와 Vulners API 등을 활용하여 CVE(Common Vulnerabilities and Exposures)를 검색하고 취약점의 존재 여부를 파악한다. 이때 취약점이 존재하는 경우 Sliver 와 Metasploit 을 이용하여 권한 상승, 임의 코드 실행 등의 공격을 수행한다. 또한 Caldera 를 이용하여 대상 시스템의 디렉토리를 탐색하고 정보를 수집하는 악성코드를 설치한다.

```
    - sh:
      platform: linux
      command: |
        echo -n 'id result : '; id
750b245c-ba22-4e13-b62c-d7a28bcc72c8:
  name:  execute_groups
  tactic:  discovery
  technique_name:  "Permission Groups Discovery: Local Groups"
  technique_id:  T1069.001
  executors:
    - sh:
      platform: linux
      command: |
        echo -n 'groups result : '; groups
b2c16a35-b580-4ce8-8b0c-ed6db95ef332:
  name:  execute_sudo_l
  tactic:  privilege-escalation
  technique_name:  "Abuse Elevation Control Mechanism: Sudo and Sudo Caching"
  technique_id:  T1548.003
  executors:
    - sh:
      platform: linux
      command: |
        echo -n 'sudo -l result: '; sudo -l
```

(그림 2) Caldera 를 이용해 기본적인 리눅스 명령어를 이용하여 Discovery 를 수행하는 YAML 소스 코드

5. 결론

본 연구를 통해 MITRE ATT&CK 프레임워크를 기반으로 Caldera, Sliver, Metasploit 을 통해 현실적인 자동화 공격 시나리오를 구축할 수 있음을 확인하였다. 특히 Caldera 를 활용하여 대상 시스템의 커널 및 라이브러리 버전 등을 자동으로 수집하고, 이를 기반으로 취약점을 신속하게 식별함으로써 수작업에 비해 훨씬 효율적인 진단이 가능했다. 향후 연구에서는 더욱 체계적인 공격 기법과 보안 탐지 우회 기술을 통합하여 더욱 정교하고 고도화된 자동화 시나리오를 개발할 예정이다. 이를 통해 기존 보안 체계의 취약점을 보다 정밀하게 평가 및 개선하고 나아가 APT 공격과 같은 복합적 공격에 대한 대응 능력을 향상시키는데 기여할 수 있을 것으로 전망된다.

참고문헌

[1] MITRE Corporation, 2013, “MITRE ATT&CK Framework”, 2025 년 04 월 26 일 검색, https://attack.mitre.org/

[2] MITRE Corporation, (n.d.), “CALDERA”, 2025 년 04 월 26 일 검색, https://caldera.mitre.org/

[3] Rapid7, (n.d.), “Metasploit”, 2025 년 04 월 26 일 검색 https://www.metasploit.com/

[4] BishopFox, (n.d.), “sliver”, 2025 년 04 월 26 일 검색, https://github.com/BishopFox/sliver