실전형 침투 테스트를 위한 오픈소스 C2 프레임워크 통합 아키텍처 설계

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

sjw91best@ajou.ac.kr, security@ajou.ac.kr

Design of an Integration of Open-Source C2 Frameworks for Practical Penetration Testing

Jeong-Won Seok[1], Jin Kwak[2]
[1]Dept. of Cyber Security, Ajou University
[2]Dept. of Cyber Security, Ajou University

요 약

최근 APT 와 같은 고도화된 사이버 공격의 증가로, 실전형 침투 테스트의 필요성이 강조되고 있다. 본 연구에서는 공격 시나리오의 자동화 및 탐지 회피성을 강화하여 침투 테스트의 실전성을 높이기 위해 주요 오픈소스 C2 프레임워크들의 특성과 한계를 분석하고, 각 프레임워크의 강점을 조합한 통합 아키텍처를 설계하여 제안한다.

1. 서론

침투 테스트는 정보 시스템에 존재하는 보안 취약점을 식별하고 이를 악용할 수 있는 공격 시나리오를 실험하는 과정으로, 시스템의 보안성을 평가하고 향상시키기 위한 필수적인 절차이다.

최근 APT(Advanced Persistent Threat)와 같은 고도화된 공격 활동이 증가하면서, 침투 테스트의 중요성이 더욱 부각되고 있다 [1]. 이에 따라 다양한 오픈소스 기반 C2(Command and Control) 프레임워크들이 등장하였으며, 침투 테스팅 환경을 구성하고 공격 시나리오를 실험하는 데 활발히 활용되고 있다.

각 프레임워크는 고유한 특성과 강점을 지니고 있지만 동시에 명확한 한계도 존재한다. 이러한 제약으로 인해 단일 프레임워크만으로는 고도화된 침투 테스트 시나리오를 완전하게 구현하기 어렵다.

본 연구에서는 다양한 오픈소스 C2 프레임워크의 장단점을 분석하고, 이를 기반으로 실전형 침투 테스트에 최적화된 통합 아키텍처를 설계하여 제안한다.

2. 오픈소스 C2 프레임워크 분석

현재 침투 테스트 및 레드팀 활동에서 널리 사용되는 오픈소스 C2 프레임워크인 Caldera, Sliver, Metasploit 을 대상으로 분석을 진행하였다.

2.1. 비교 항목 및 분석 결과

표 1 은 통합 아키텍처 설계에 필요한 C2 프레임워크 특성을 평가하기 위해, 다음과 같은 비교 항목을 선정하였다. 우선, 공격 세션 및 시나리오를 일관되게 관리할 수 있는 통합 제어 능력과, 초기 목표 시스템 접근 및 implant(침투용 에이전트) 배포를 평가하는 초기 침투 적합성을 기준으로 삼았다. 또한, 초기 침투 이후 추가적인 권한 상승이나 내부 확장 공격 수행 가능여부를 의미하는 후속 공격 적합성과, 공격 시나리오 실행 및 관리를 자동화할 수 있는 자동화 수준을 평가 기준으로 고려하였다. 그리고 implant 운영 시 다양한 네트워크 환경에서 공격을 은닉할 수 있는지를 나타내는 통신 채널 다양성과 표준화된 공격 전술(TTPs) 기반 시나리오 작성 및 통제 가능성에 대해 평가하는 MITRE ATT&CK 연계성도 함께 분석 항목 에 포함하였다.

(표 1) 각 C2 프레임워크 장단점 비교

	Caldera	Sliver	Metasploit
통합제어 능력	높음(공격 시나리오 자동화 및 세션 관리 지원)	낮음(implant 개별 관리 위주)	낮음(단일 세션 위주 관리)
초기침투	중간(시나리오	높음(implant	높음(다양한

적합성	기반 초기 접근 가능)	배포 및 초기 침투에 최적화)	초기 취약점 익스플로잇 지원)
후속공격 적합성	중간(전술 자동화 및 다단계 공격 지원)	중간(implant 기반 추가 명령 실행 가능)	높음(다양한 후속 익스플로잇, 권한 상승 공격 지원)
자동화 수준	높음(ATT&CK 기반 공격 시나리오 자동화 지원)	중간(implant 관리 자동화 일부 지원)	낮음(수동 모듈 기반 조작 필요)
통신채널 다양성	중간(HTTP 기반 기본 지원)	높음(gRPC, HTTP/2, mTLS 등 다양한 통신 지원)	낮음(기본적인 reverse shell 통신 지원)
MITRE 연계성	높음(ATT&CK 기반 시나리오 설계 지원)	낮음(공식 연계 없음)	낮음(개별 모듈 중심 사용)

위 분석 결과, Sliver 는 다양한 통신 채널(gRPC, HTTP/2, mTLS 등) 지원을 통해 초기 침투 과정에서 탐지 회피에 유리하며 [2], Metasploit 은 다양한 익스플로잇 모듈을 보유하여 후속 공격 수행에 강점을 가진다. Caldera 는 세션 통합 관리 및 MITRE ATT&CK 기반 공격 시나리오 자동화 설계 기능을 제공함으로써, 테스트 일관성과 효율성을 높일 수 있다 [3].

3. 통합 아키텍처 제안

본 장에서는 2 장에서 분석한 결과를 바탕으로, 각 프레임워크의 강점을 통합함으로써, 단일 프레임워크로는 구현이 어려운 복합적이고 고도화된 침투 테스트 시나리오의 자동화 및 탐지 회피성 강화를 목표로 하는 통합 아키텍처를 제안하고자 한다.

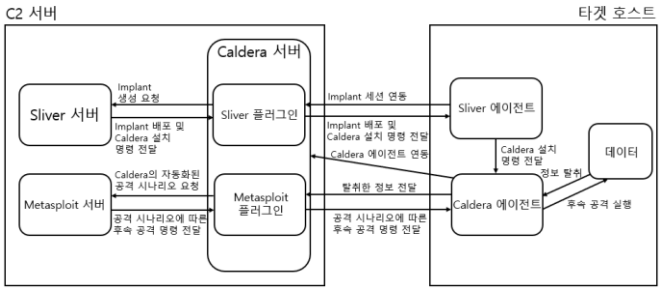
3.1. 제안 아키텍처 개요

제안하는 통합 아키텍처는 Caldera 를 메인 컨트롤러로 설정하여 침투 테스트 시나리오의 자동화를 수행하고, Sliver 를 통해 초기 침투를 위한 implant 생성과 고성능 통신 및 은닉 채널을 관리하는 구조를 설계하였다. 추가 공격 단계에서는 Metasploit 을 활용하여 다양한 후속 공격을 전개할 수 있도록 계획하였다.

Caldera 는 고도로 모듈화된 플러그인 기반 아키텍처를 채택하고 있어, 다양한 C2 프레임워크와의 유연한 연동이 가능하다. 본 연구에서는 Sliver 와 Metasploit 각각에 대해 implant 생성 API, gRPC 를 활용한 별도의 Caldera 플러그인 설계를 제안하였으며, 이를 통해 implant 생성 및 추가 공격 단계를 Caldera 내부에서 통합 관리할 수 있도록 하였다.

공격 흐름은 다음과 같다. Implant 생성 및 배포 과정은 Caldera Sliver 플러그인 내에서 자동화되며, implant 가 타겟에 연결되면 Sliver 세션을 통해 Caldera 에이전트를 설치하도록 구성하였다. 이후 추가 공격이 필요한 경우, Caldera Metasploit 플러그인을 활용하여 Metasploit RPC 를 통해 익스플로잇 모듈을 호출하고 공격 시나리오를 확장하는 방식을 제안한다. 이를 통해 침투 테스트 수행자는 최소한의 수작업 개입으로 다양한 고도화된 공격 시나리오를 연속적으로 수행할 수 있을 것으로 기대된다.

(그림 1) 통합 아키텍처 구성도



4. 결론

본 연구에서는 실전형 침투 테스트를 위한 오픈소스 C2 프레임워크 통합 방안을 제안하였다. 주요 오픈소스 C2 프레임워크들의 장단점을 분석하고, Caldera 를 중심으로 Sliver, Metasploit 등의 강점을 결합한 통합 아키텍처를 설계하였다.

제안한 통합 아키텍처는 기존 단일 C2 프레임워크의 한계를 극복하고, 복합적이고 탐지 회피를 수행하는 공격 시나리오를 자동화하여 침투 테스트 및 레드팀 활동의 효율성을 크게 향상시킬 수 있다.

향후 연구에서는 다양한 공격 벡터를 추가로 통합하고, 방어 측 탐지 시스템과의 상호작용을 고려한 통합 전략 수립이 필요하다. 또한, AI 기반 기법을 활용하여 시나리오를 자동으로 생성하고 최적화하는 방안에 대해서도 연구를 확장할 수 있을 것이다.

참고문헌

[1] Abdul Basit Ajmal et al, "Toward Effective Evaluation of Cyber Defense: Threat Based Adversary Emulation Approach," IEEE Access, 2023.

[2] E. Chatzoglou et al, "Bypassing antivirus detection: old-school malware, new tricks," in Proc. 18th Int. Conf. Availability, Reliability and Security (ARES '23), ACM, 2023.

[3] M. Landauer et al, "Red team redemption: A structured comparison of open-source tools for adversary emulation," in Proc. 2024 IEEE 23rd Int. Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2024.