MITRE ATT&CK REDTEAM 기술 연구

91913098 강민영

Contents

Ⅰ. 연구 개요

1.1 연구 소개

1.2 연구 추진 방안

I 연구 개요 01. 연구 소개

연 구 소개

연구 배경

지속적인 사이버 공격 증가

기업을 대상으로 하는
표적형 공격 및 랜섬웨어 등
악의적인 공격으로부터
조직 보호 필요

사이버 공격에 대응하기 위한
사이버 훈련장 시스템 필요

연구 필요성

기존 사이버 훈련장 보완

기존 사이버 훈련장 시스템은
사용자의 개입이 필요하여
비용적인 측면에서 비효율적

MITRE ATT&CK 프레임워크를 사용하여
자동화 도입

연구 목적

MITRE ATT&CK 프레임워크를 사용하여
사이버 훈련
공격팀/방어팀 자동화 시스템 개발

I 연구 개요 02. 연구 추진 방안

담 당 연 구

공격 기법 확인

- 총 14단계의 전술 및 여러 기법 존재
- 공격 기법 모두 파악
- MITRE ATT&CK에서 지원하지 않는 공격 기법은 직접 개발

구현

- MITRE ATT&CK에서 지원하는 공격 기술은 테스트 진행
- 공격 기술에 알맞은 환경 셋팅
- 구성한 환경에 테스트

개발

- 공격 기술에 알맞은 환경 셋팅
- Technique에 해당되는 공격 기술 개발

문서화

- 구현 및 개발이 완료된 공격은 문서화

Ⅱ. 연구 내용

2.1 Red Team 기술 절차

Ⅱ 연구 내용 01. Red Team 기술 연구 내용 (1/4)

연 구 절 차

내용

환경 구성

Windows

Active Directory

Cloud

Linux

Techniques 확인

MITRE ATT&CK™

1. Reconnaissance
⋮
14. Impact

공격 Command 존재 여부 확인

Command 구현 Command 개발

공격 Command 테스트

Command 구현

알맞은 환경에 **CLI 테스트 진행**

Tool을 사용하여 **공격 성공 확인**

Command 개발

알맞은 환경에 **CLI 개발**

Tool을 사용하여 **공격 성공 확인**

파일화

Command 구현 Command 개발

YML

구현 및 개발된 Command **YAML 문서화**

보고서 작성

Red Team 공격 대응 및 탐지 연구 최종 보고서 작성

Ⅱ 연구 내용 01. Red Team 기술 연구 내용 (2/4)

연 구 절 차

내용

환경 구성 → Techniques 확인

Windows

Active Directory

Cloud

Linux

MITRE ATT&CK

1. Reconnaissance
⋮
14. Impact

공격 Command 존재 여부 확인

Command 구현 / Command 개발

세부 내용

1 환경 구성

- Vmware, Virtual Box 사용
- 모든 운영체제 구축은 비효율적
  환경 구성이 다른 서버만 구축

2 Techniques 확인

- 총 14단계의 전술의 YAML 파일 확인
- YAML 파일 구성: TTPs, 상세 설명, 공격 CLI
- 공격 Command 존재 여부에 따라 구현 or 개발

Ⅱ 연구 내용 01. Red Team 기술 연구 내용 (3/4)

연 구 절 차

세부 내용

3 Command 구현

- YAML 파일에 명시된 공격 CLI 테스트
- Tool을 사용하여 공격 성공 확인

3 Command 개발

- YAML 파일의 전술, 상세 설명을 참고하여 공격 CLI 개발
- Tool을 사용하여 공격 성공 확인

공격 Command 테스트

Command 구현

알맞은 환경에 **CLI 테스트 진행**

Tool을 사용하여 **공격 성공 확인**

Command 개발

알맞은 환경에 **CLI 개발**

Tool을 사용하여 **공격 성공 확인**

파일화

Command 구현 Command 개발

구현 및 개발된 Command **YAML 문서화**

세부 내용

4 파일화

- 구현 및 개발에 성공한 CLI, 전술, CLI에 대한 누구나 이해할 수 있도록 상세 설명을 추가하여 YAML 문서화

Ⅱ 연구 내용 01. Red Team 기술 연구 내용 (4/4)

연 구 절 차

내용

환경 구성

Windows

Active Directory

Cloud

Linux

Techniques 확인

MITRE ATT&CK

1. Reconnaissance
⋮
14. Impact

공격 Command 존재 여부 확인

Command 구현 Command 개발

공격 Command 테스트

Command 구현

알맞은 환경에 **CLI 테스트 진행**

Tool을 사용하여 **공격 성공 확인**

Command 개발

알맞은 환경에 **CLI 개발**

Tool을 사용하여 **공격 성공 확인**

파일화

Command 구현 Command 개발

YML

구현 및 개발된 Command **YAML 문서화**

보고서 작성

Red Team 공격 대응 및 탐지 연구 최종 보고서 작성

Ⅲ. 추후 연구

3.1 연구 추진 일정

Ⅲ 추후 연구 01. 연구 추진 일정

연구 추진 일정

- MITRE ATT&CK 프레임워크 1-14단계의 TTPs **공격 구현 및 개발**

- MITRE ATT&CK 프레임워크 1-14단계의 TTPs **1차 검증**
- MITRE ATT&CK 프레임워크 1-14단계의 TTPs **2차 검증**

2022년 2023년 2024년 • • •


Q&A