DREAMLABS COLLECTOR

I Built an AI Agent That Hacks for Me | OpenClaw + Kali Linux

zSecurity 채널의 이 영상은 Kali Linux 클라우드 서버에서 OpenClaw 라는 자율 AI 해킹 에이전트를 구축하는 과정을 시연합니다 . 이 에이전트는 일반 AI 챗봇과 달리 Nmap, Metasploit, 웹 브라우저와 같은 도구에 직접 접근하여 실제 해킹 작업을 실행할 수 있습니다 . 영상은 클라우드 인프라 설정부터 AI ' 두뇌 ' (Claude 4.6 Opus 또는 DeepSeek 모델 사용) 연결 , 그리고 Telegram 을 통한 모바일 보고 설정까지 전 과정을 다룹니다 . CCTV 카메라 위치 파악 및 자동화된 OSINT, 취약점 스캐닝과 같은 실제 시연을 포함하며 , 모든 내용은 교육 목적으로만 제공됨을 강조합니다 . 이 기술은 보안 전문가와 학생들에게 AI 에이전트의 역량을 이해하고 시스템을 보호하는 방법을 배우는 데 유용합니다 .

CHANNEL

zSecurity

VIDEO ID

C5ir_rQ4L4g

source: https://www.youtube.com/watch?v=C5ir_rQ4L4g | video_id: C5ir_rQ4L4g | generated: 2026-06-13T15:43:26Z

Executive Summary

영상 시청 전 빠른 정보 습득을 위한 요약

SUMMARY

zSecurity 채널의 이 영상은 Kali Linux 클라우드 서버에서 OpenClaw 라는 자율 AI 해킹 에이전트를 구축하는 과정을 시연합니다 . 이 에이전트는 일반 AI 챗봇과 달리 Nmap, Metasploit, 웹 브라우저와 같은 도구에 직접 접근하여 실제 해킹 작업을 실행할 수 있습니다 . 영상은 클라우드 인프라 설정부터 AI ' 두뇌 ' (Claude 4.6 Opus 또는 DeepSeek 모델 사용) 연결 , 그리고 Telegram 을 통한 모바일 보고 설정까지 전 과정을 다룹니다 . CCTV 카메라 위치 파악 및 자동화된 OSINT, 취약점 스캐닝과 같은 실제 시연을 포함하며 , 모든 내용은 교육 목적으로만 제공됨을 강조합니다 . 이 기술은 보안 전문가와 학생들에게 AI 에이전트의 역량을 이해하고 시스템을 보호하는 방법을 배우는 데 유용합니다 .

source: https://www.youtube.com/watch?v=C5ir_rQ4L4g | video_id: C5ir_rQ4L4g | generated: 2026-06-13T15:43:26Z

Video Structure

영상 구성과 논리 흐름

01

OpenClaw 소개 및 Kali Linux 사용 이유 (0:00 - 1:35)

02

클라우드 VPS 설정 및 서버 보안 강화 (2:12 - 7:44)

03

OpenClaw 설치, 구성 및 AI 두뇌 (OpenRouter) 연결 (7:44 - 11:50)

04

Telegram 봇 생성 및 보안을 위한 허용 목록 설정 (11:50 - 14:15)

05

에이전트 활성화, 필수 스킬 설치 및 '전문 해커' 시스템 프롬프트 설정 (14:15 - 19:00)

06

CCTV 카메라 위치 파악 및 자동화된 OSINT/취약점 스캐닝 시연 (19:00 - 22:50)

source: https://www.youtube.com/watch?v=C5ir_rQ4L4g | video_id: C5ir_rQ4L4g | generated: 2026-06-13T15:43:26Z

Key Ideas

정보게시물로 전환할 핵심 아이디어

01

자율 AI 에이전트를 활용한 공격적 보안 (Offensive Security) 개념 구현 (메타데이터 기반 추론)

02

OpenClaw 프레임워크를 통한 AI 에이전트의 직접적인 도구 접근 및 실행 능력 (메타데이터 기반 추론)

03

클라우드 기반 Kali Linux 환경 구축의 이점 및 방법론 (메타데이터 기반 추론)

04

Claude 4.6 Opus, DeepSeek 등 고급 LLM 을 AI 에이전트의 ' 두뇌 ' 로 활용하는 방안 (메타데이터 기반 추론)

05

자동화된 OSINT 및 취약점 스캐닝을 통한 보안 작업 효율성 증대 (메타데이터 기반 추론)

06

AI 에이전트의 역할과 행동을 정의하는 시스템 프롬프트 엔지니어링의 중요성 (메타데이터 기반 추론)

source: https://www.youtube.com/watch?v=C5ir_rQ4L4g | video_id: C5ir_rQ4L4g | generated: 2026-06-13T15:43:26Z

DreamLabs Application

DreamLabs 내부 적용 관점

01

DreamLabs 내부 시스템의 자동화된 보안 취약점 진단 및 모의 침투 테스트에 OpenClaw 또는 유사 프레임워크 적용 가능성 검토

02

위협 인텔리전스 (Threat Intelligence) 수집 및 분석 자동화를 위한 AI 에이전트 활용 방안 연구

03

보안관제센터 (SOC) 운영 효율성 증대를 위해 AI 에이전트의 초기 분석 및 대응 지원 역할 탐색

04

AI 에이전트 자체의 보안 취약점 및 오용 가능성에 대한 선제적 연구 및 방어 전략 개발

05

AI 기반 보안 기술 교육 콘텐츠 개발 시 본 영상의 구축 방법론을 참고하여 실습 환경 구성

source: https://www.youtube.com/watch?v=C5ir_rQ4L4g | video_id: C5ir_rQ4L4g | generated: 2026-06-13T15:43:26Z

Verification Required

모델 추론 /metadata 한계 / 원본 확인 필요

01

OpenClaw 프로젝트의 현재 상태, 오픈소스 여부 및 커뮤니티 지원 수준 확인

02

Claude 4.6 Opus 또는 DeepSeek 과 같은 특정 LLM 이 복잡한 해킹 시나리오에서 보이는 실제 성능 및 한계 평가

03

영상에서 제시된 '전문 해커' 시스템 프롬프트가 다양한 실제 환경에서 얼마나 효과적으로 작동하는지 검증

04

자율 AI 에이전트 배포 시 발생할 수 있는 잠재적 보안 위험 (예: 의도치 않은 행동, 권한 오용) 에 대한 심층 분석

05

Hostinger VPS 할인 코드 'ZSECURITY' 의 유효성 및 적용 조건 확인

source: https://www.youtube.com/watch?v=C5ir_rQ4L4g | video_id: C5ir_rQ4L4g | generated: 2026-06-13T15:43:26Z

Source & Download Metadata

게시물과 문서 산출물 추적 정보

METADATA

Title: I Built an AI Agent That Hacks for Me | OpenClaw + Kali Linux
Channel: zSecurity
Video ID: C5ir_rQ4L4g
Source URL: https://www.youtube.com/watch?v=C5ir_rQ4L4g
Playlist ID: PLHwM6idVO2zyqi2IZeDAiP5QBqRXd2Zyh
Generated at: 2026-06-13T15:43:26Z
Source basis: metadata_and_model_inference