**정보 수집**

정보 수집 단계는 모의해킹의 대상을 정하고 나면 가장 처음 수행하게 되는 단계

수집할 정보:

1. 웹 애플리케이션을 서비스하기 위한 호스트 환경 (운영체제, 웹 서버, 웹 프레임워크)

-> 알려진 취약점을 쉽게 찾아 공격

2. 웹 애플리케이션 자체에 대한 정보

-> 웹 애플리케이션 매핑을 통해 정보 수집 후 구조 파악하여 공격 지점 찾기

**1. 배너를 통한 정보 수집**

- 웹 서버와 관련된 정보를 가장 간단하게 확인할 수 있는 방법 -> 응답 메시지의 서버 헤더

- 서버 응답을 통한 정보 수집 방법 -> 배너 그래빙(banner grabbing)

- 서버 헤더를 통해 아파치 웹 서버 버전 정보, 운영체제, PHP 버전 정보, OpenSSL 등 정보 수집

- 서버 헤더 이외 X-Powered-By, X-ASPNET-VERSION과 같은 헤더들이 호스트 환경의 정보 노출

- 이와 같은 응답 헤더의 정보는 웹 브라우저의 개발자 도구에서 확인 가능

- Burp Suite의 Proxy 히스토리 기능으로도 확인 가능

텍스트, 스크린샷, 소프트웨어, 멀티미디어 소프트웨어이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 번호, 폰트이(가) 표시된 사진

자동 생성된 설명

**2. 기본 설치 파일을 통한 시스템 정보 수집**

- 웹 애플리케이션 운영 위한 웹 서버와 웹 프레임워크, 기타 구성 요소 설치시, 기본 설치 파일로 인해 호스트 환경에 대한 정보 노출

(ex. PHP의 경우, phpinfo.php라는 기본 설치 파일을 통해 PHP 환경에 대한 정보, 환경 변수, 그 밖의 다양한 호스트 관련 정보가 노출될 수 있음.)

텍스트, 전자제품, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

**3. 웹 취약점 스캐닝**

- 자동화된 프로그램을 이용하여 웹사이트의 여러 가지 정보 수집 및 취약점 파악

- 많은 트래픽 유발로 인해 모의 해킹할 때, 담당자의 허가 후에 진행

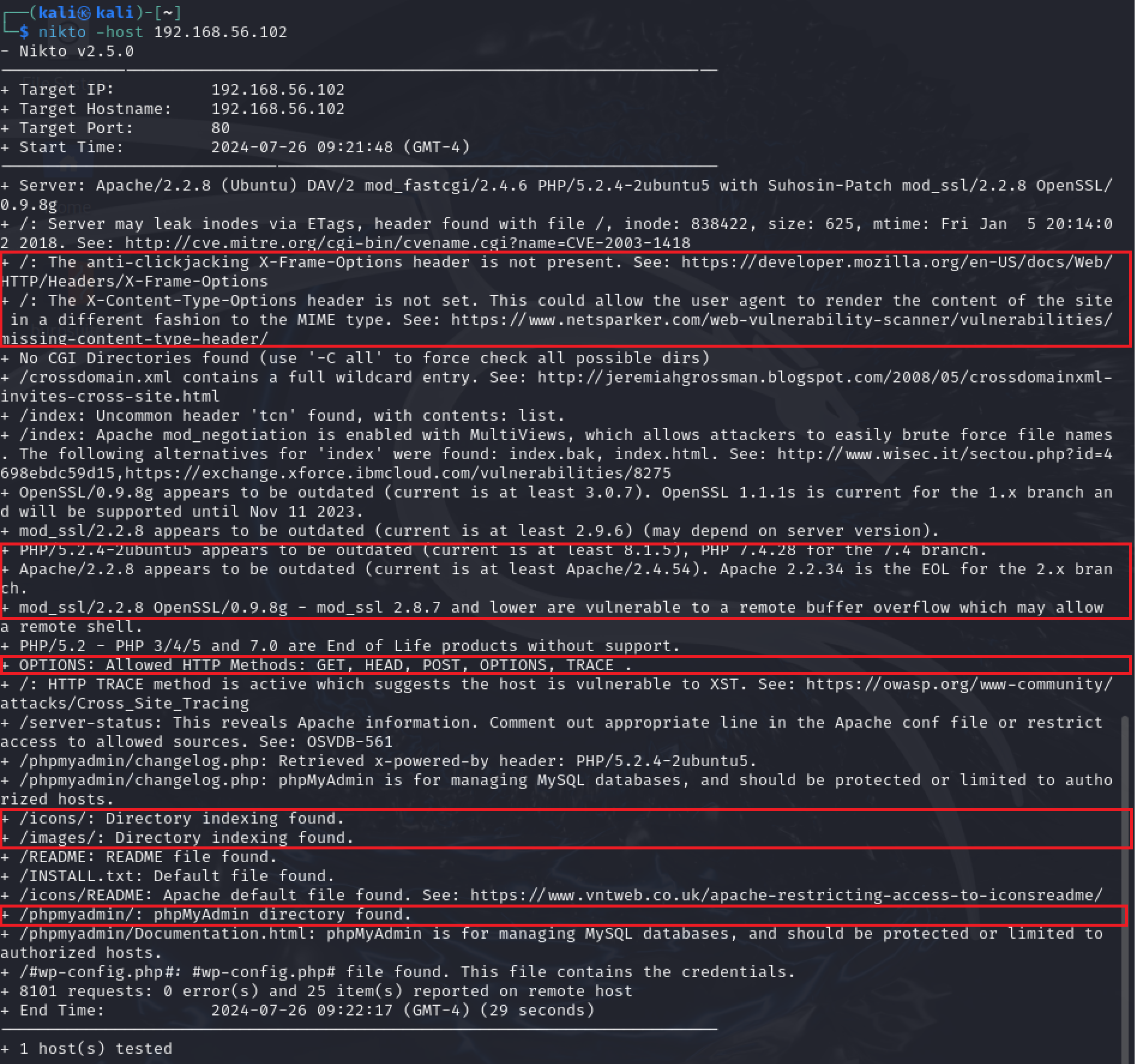
- 칼리 리눅스에 기본으로 설치된 웹 스캐닝 프로그램인 “nikto”로 정보 쉽게 수집 가능

텍스트, 스크린샷이(가) 표시된 사진

자동 생성된 설명

<터미널에서 nikto의 옵션을 확인한 모습>

- “-host” 옵션 뒤에 스캐닝할 IP 주소만 입력해주면 스캐닝을 실행하여 많은 정보 수집



<실습용 가상 머신의 IP 주소를 입력하여 실행한 화면>

- 서버 헤더 및 PHP, 아파치, mod\_ssl 등의 버전이 오래되었다.

- 보안 관련 헤더가 설정되어 있지 않다.

- 허용된 메소드 목록 정보

- /icons/, /images/ 경로에서 디렉토리 인덱싱이 발견되었다.

- phpMyAdmin 디렉토리가 발견되었다.

- 이와 같은 정보는 모의해킹을 수행하는 과정에서 공격에 중요한 단서가 될 수 있다.

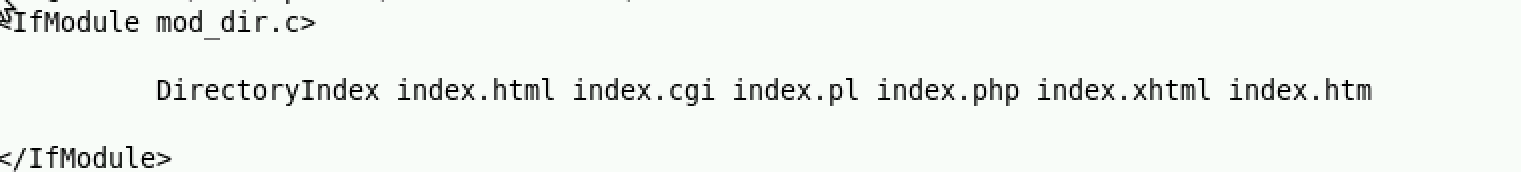
- 오래된 버전을 사용하는 소프트웨어에는 이미 알려진 취약점들이 존재할 수 있어, 이 취약점을 활용하여 쉽게 공격 성공할 수 있다.

**4. 디렉토리 인덱싱**

- 웹 서버의 잘못된 설정으로 웹 서버 디렉토리의 파일들이 노출되는 취약점

- 디렉토리 리스팅 취약점이라고도 부르며, 과거 국가정보원 8대 홈페이지 취약점으로도 선정되었다.

- 디렉토리 목록 출력은 원래 웹 서버가 지원하는 기능



<디렉토리의 기본 출력파일을 설정하는 mod\_dir 아파치 모듈>

- 사용자가 웹 브라우저의 주소로 디렉토리 경로(ex. /images/) 요청시, 해당 디렉토리에 위 사진과 같은 파일이 존재하면 해당 파일 출력

- 지정된 파일들이 모두 디렉토리에 존재하지 않으면 해당 디렉토리의 모든 파일 출력 -> 문제

- 아파치와 같은 일부 웹 서버의 경우, 소프트웨어 설치시 기본으로 디렉토리 인덱싱 설정

텍스트, 전자제품, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

- 이전 스텝에서 “nikto”로 /icons/에 디렉토리 인덱싱 발견을 토대로 웹 브라우저에 검색하면 디렉토리 파일 목록 출력

- web.confg.bak, wp-config.bak과 같은 백업 파일을 통해서도 중요한 정보 노출 가능

**5. 수동 매핑**