네트워크 보안 취약점 진단

네트워크 보안 취약점이란?

- **정의:** 네트워크 시스템, 장비, 애플리케이션 등의 설계, 구현, 설정, 운영상의 약점으로, 공격자가 이를 이용해 시스템에 침투하거나 정보 유출, 서비스 마비 등을 야기할 수 있는 부분.
- **예시:**
  - 취약한 비밀번호 사용
  - 업데이트되지 않은 소프트웨어 (알려진 보안 패치 누락)
  - 잘못된 방화벽 설정
  - 불필요하게 열려있는 포트
  - SQL Injection, XSS 등의 웹 애플리케이션 취약점
- **왜 중요한가?:** 취약점을 통해 데이터 유출, 시스템 파괴, 서비스 중단 등 막대한 피해 발생 가능성 설명

Kali Linux 소개 및 설치

- **Kali Linux란?:**
  - Debian 기반의 리눅스 배포판.
  - 모의 해킹(Penetration Testing) 및 디지털 포렌식(Digital Forensics)을 위한 수많은 도구들을 기본으로 포함.
  - 보안 전문가, 화이트 해커들이 주로 사용.
  - **설치 방법 (간략 설명):**
    - 가상 머신 (VirtualBox, VMware Workstation) 사용 권장.
    - ISO 이미지 다운로드 -> 가상 머신 생성 -> 설치 과정

기본 정보 수집 툴 1 (netstat)

- 네트워크 통계 (network statistics)" 의 줄임말로, 컴퓨터의 네트워크 활동을 보여주는 명령어 도구입니다.
- 내 컴퓨터가 다른 컴퓨터들과 어떻게 연결되어 있는지, 어떤 프로그램이 인터넷을 사용하고 있는지 등을 보여주는 "네트워크 현황판“

- 네트워크 문제 해결
- 보안 점검
- 네트워크 상태 확인

- **netstat ? Or netstat -h** 로 옵션 정보 확인 가능

Netstat 사용 예시

- netstat –an
- Proto Local Address Foreign Address State
- TCP 192.168.0.10:51234 125.209.222.141:80 ESTABLISHED
  - Proto: TCP (안정적인 웹 통신을 위해 사용)
  - Local Address: 내 컴퓨터의 IP 주소와 임시 포트 번호 (51234번은 웹 브라우저가 임시로 할당받은 포트)
  - Foreign Address: 네이버 서버의 IP 주소(125.209.222.141)와 웹 서비스 포트(80)
  - State: ESTABLISHED (네이버와 연결이 잘 되어 데이터를 주고받는 중이라는 뜻)

기본 정보 수집 툴 2 (nmap)

- **Nmap이란?:**
  - "Network Mapper"의 약자.
  - 네트워크 스캐닝 및 보안 감사에 사용되는 강력한 오픈 소스 도구.
  - 호스트 발견, 포트 스캐닝, 서비스 및 OS 감지 등의 기능 제공.
- 주요 기능:
  - **호스트 발견:** 네트워크 상의 활성 호스트 찾기.
  - **포트 스캐닝:** 대상 시스템에서 열려있는 포트 확인. (어떤 서비스가 실행 중인지 힌트 제공)
  - **서비스 및 버전 감지:** 포트에서 실행 중인 애플리케이션과 버전 정보 파악.
- **OS 감지:** 대상 시스템의 운영체제 종류 파악

Nmap 사용 예시

- **Nmap 기본 사용법:**
  - 터미널(Terminal)에서 nmap [옵션] [대상 IP 주소/도메인] 형식으로 사용.
    - **가장 기본적인 스캔:** nmap [대상 IP]
      - 예시: nmap 192.168.1.1
      - 결과: 열려있는 포트, 서비스 상태 등 출력.
    - **서비스 및 버전 감지:** -sV 옵션
      - 예시: nmap -sV 192.168.1.1
      - 결과: 포트별 서비스 이름 및 버전 정보 추가 출력.
    - **운영체제 감지:** -O 옵션
      - 예시: nmap -O 192.168.1.1
    - 결과: 대상 시스템의 운영체제 종류 추정.
- **자주 사용되는 Nmap 옵션:**
  - -sS: SYN 스캔 (가장 일반적이고 빠른 스캔)
  - -p [포트범위]: 특정 포트 또는 포트 범위 스캔 (예: -p 80,443 또는 -p 1-1024)
  - -A: Aggressive 스캔 (OS 감지, 버전 감지, 스크립트 스캔 등을 모두 수행)
  - -oN [파일이름]: 결과를 일반 텍스트 파일로 저장.

기타 정보 수집 툴 (OpenVAS, OWASP ZAP)

- **OpenVAS란?:**
  - "Open Vulnerability Assessment System"의 약자.
  - 종합적인 취약점 스캐너로, 네트워크 및 시스템의 알려진 취약점을 자동으로 식별.
  - 주요 기능:
    - 자동화된 취약점 스캔.
    - 스캔 결과 보고서 생성 (심각도별 분류).
    - 취약점 해결을 위한 권고 사항 제공
- **OWASP ZAP이란?:**
  - "Open Web Application Security Project Zed Attack Proxy"의 약자.
  - 웹 애플리케이션의 보안 취약점을 찾는 데 사용되는 오픈 소스 침투 테스팅 도구.
  - 웹 개발자 및 보안 전문가 모두에게 유용.
  - 주요 기능:
    - **프록시 기능:** 웹 브라우저와 웹 서버 사이에서 모든 HTTP/HTTPS 트래픽을 가로채고 수정.
    - **자동 스캔 (Automated Scan):** 웹 애플리케이션을 자동으로 탐색하고 취약점 스캔.
    - **수동 탐색 (Manual Explore):** 사용자가 직접 웹 사이트를 탐색하면서 ZAP이 트래픽을 기록하고 분석.
    - **강제 브라우징 (Forced Browse):** 웹 서버의 숨겨진 파일 및 디렉토리 탐색.
    - **퍼징 (Fuzzing):** 입력 값에 다양한 비정상 데이터를 주입하여 애플리케이션의 응답 확인.

주의사항 및 윤리적 해킹

- **윤리적 해킹 (Ethical Hacking)의 중요성:**
  - "아는 것이 힘이다." 이 지식을 선한 목적으로 사용해야 함.
  - 취약점 진단은 시스템의 보안 강화 목적.
  - **절대 지켜야 할 원칙:**
    - **사전 허가 (Prior Consent):** 모든 스캔 및 테스트는 반드시 시스템 소유자의 명시적인 허가(Written Consent)를 받은 후에만 수행해야 함.
    - **책임감 (Responsibility):** 잠재적인 시스템 손상이나 서비스 중단에 대한 책임을 이해하고 조심스럽게 수행.
    - **합법성 (Legality):** 모든 행위는 해당 국가의 법률을 준수해야 함