오답노트

시스템 보안

- **nfts 파일시스템의 메타 파일 (오답 : $bios는 메타파일 아님)**

파일명	설명
$MFT	**Master File Table**: NTFS의 모든 파일과 디렉터리에 대한 정보를 저장하는 핵심 테이블
$MFTMirr	$MFT의 첫 4개 레코드(중요 정보)의 백업본. $MFT 손상 시 복구용으로 사용
$LogFile	파일시스템 메타데이터 변경에 대한 트랜잭션 로그를 저장. 시스템 복구에 사용
$Volume	볼륨의 라벨, 버전, 플래그 등 볼륨 자체에 대한 정보 저장
$AttrDef	NTFS에서 사용하는 속성(Attributes) 정의 테이블
. (dot)	루트 디렉터리
$Bitmap	클러스터 사용 현황 비트맵(어떤 클러스터가 사용 중/비어있는지)
$Boot	부트 섹터(부팅 정보, BPB 등)
$BadClus	불량 클러스터 목록. 디스크의 손상된 영역 정보
$Secure	보안 정보(Access Control List, ACL 등) 저장
$UpCase	대소문자 구분 없는 비교를 위한 대문자 변환 테이블
$Extend	확장 기능(Quota, Object ID, Reparse Point, USN 저널 등) 디렉터리
$Quota	사용자별 디스크 사용량(쿼터) 정보
$ObjId	파일/폴더의 고유 식별자(Object ID) 정보
$Reparse	리파스 포인트(심볼릭 링크, 마운트 포인트 등) 정보
$UsnJrnl	파일 변경 이력(USN Change Journal), $Extend 하위에 위치

- 레이스 컨디션 공격
  - 두 프로세스간 자원 사용을 위해 경쟁하는 것을 이용한 공격으로, 시스템의 프로그램과 공격 프로그램이 경쟁상태가 되어 root권한으로 파일에 접근을 가능하게 하는 방법
- 미라이
  - ip카메라나 가정용 라우터같은 iot장치를 주요 공격 대상으로 삼는 ddos공격용 봇넷 악성코드

- 백오피리스
  - 원격제어 해킹 툴로 악성코드(멀웨어)
  - 원래는 윈도우 운영체제의 보안 취약점을 알리기 위해 공개됐지만, 실제로는 해킹·도청 등 악의적으로 많이 사용되어 **대표적인 트로이 목마 악성코드**로 분류
- 워너 크라이(wannacry)
  - 파일을 암호화하고 돈을 요구하는 악성코드(랜섬웨어),
  - **SMB(파일 공유) 취약점**을 이용해, 이메일 첨부파일이 아니라 네트워크만 연결돼 있어도 빠르게 전파
- 님다
  - 2001년 9월 전 세계적으로 대규모 피해를 일으킨 악성 컴퓨터 바이러스(웜). 단 22분 만에 인터넷상에서 가장 넓게 확산된 바이러스 중 하나로 기록되어 있습니다
- 스턱스넷
  - 2010년에 발견된 악성 컴퓨터 웜 바이러스로, 산업시설을 실제로 파괴할 목적으로 개발된 최초의 사이버 무기. 기존의 악성코드가 금전적 이득이나 정보 탈취를 목표로 했다면, 스턱스넷은 특정 산업 인프라를 물리적으로 손상시키는 것을 목표로 삼았다는 점에서 사이버 공격의 새로운 패러다임을 제시
  - 여러 개의 제로데이(Zero-day) 취약점, 합법적인 인증서로 서명된 드라이버, 루트킷 기능 등 다양한 첨단 기술이 결합된 복합 웜입니다. 자체적으로 업데이트되며, 감염 사실을 숨기기 위해 허위 피드백 신호를 보내기도 했습니다
- sql 슬래머
  - 2003년 1월 25일 전 세계적으로 대규모 피해를 일으킨 악성 웜 바이러스입니다. 마이크로소프트의 데이터베이스 관리 시스템인 SQL 서버의 버퍼 오버플로 취약점을 이용해 감염
- buffer overflow버퍼 오버플로
  - 리눅스 커널의 rtlwifi드라이버에서 **경계값** 체크가 미흡해서 발생.
  - 공격자는 **경계값을 넘어서는 길이**의 패킷을 전송해서 시스템 장애발생
- 슬랙
  - 하드디스크 구조에서 물리적으로는 할당받은 공간이지만, 논리적으로 사용할 수 없는 공간
- CHS

    - 컴퓨터 하드디스크의 물리적 주소 체계 중 하나인 **Cylinder-Head-Sector**의 약자입니다. CHS 방식은 하드디스크의 데이터를 읽고 쓸 때, 디스크의 위치를 실린더(Cylinder), 헤드(Head), 섹터(Sector)라는 세 가지 값으로 지정하는 방식
- 윈도우 레지스트리 키
    - hkey_classes_root : 파일의 각 확장자 정보와 프로그램 맵핑정보 저장
- tpm
    - 민감한 암호연산을 하드웨어로 이동함으로써 시스템 보안을 향상시키고, 인증된 부트, 인증, 암호화와 같은 기본적인 기능제공, 안전한 입출력에 사용되는 암호 프로세서를 제공
- srm, sam
    - srm : Storage Resource Management, 데이터 저장 자원을 효율적으로 관리하는 IT 프로세스입니다. 저장 용량의 모니터링, 백업, 확장, 장애 대응, 데이터 분산 등을 포함하며, 대규모 데이터 환경에서 저장 자원의 최적화와 안정성 확보에 중점
    - sam : Security Accounts Manager 윈도우os에서 사용자 계정과 암호 정보를 저장하는 데이터베이스 파일. 윈도우 로그인 시 입력한 사용자명과 암호를 SAM 데이터베이스와 비교하여 인증을 수행합니다. 이 파일은 보안을 위해 암호화되어 저장되며, 시스템의 중요한 보안 요소
- mkfs, mknod
    - mkfs : make filesystem"의 약자로, 디스크나 파티션에 새로운 파일 시스템을 생성(포맷)하는 명령어로 ext2, ext3, ext4, xfs, vfat, ntfs 등 다양한 파일 시스템을 지원
    - mknod : 특수 파일(주로 장치 파일, 디바이스 파일, FIFO 등)을 생성하는 명령어
        - `mknod /dev/myblock b 7 0` : 메이저 번호 7, 마이너 번호 0인 블록 디바이스 파일 생성
- 파일시스템
    - ext
        - Extended File System"의 약자로 리눅스 환경에 맞춰 설계됨
        - 모두 최대 크기가 2GB
        - **파일명 최대 255바이트** 지원(더 긴 파일명 가능)
        - **접근 제어, inode 수정, 타임스탬프 수정 등은 불가**(EXT1 기준)
        - **저널링 미지원**(EXT1 기준, EXT3부터 저널링 지원)

- fat16:
  • 주로
  DOS, Windows 초기 버전, 플로피디스크, USB 등에서 사용
  - 모두 최대 크기가 2GB
  - **클러스터 크기**가 2KB~32KB로, 파티션 크기에 따라 조정됨
  - **루트 디렉터리 엔트리 수 제한**(최대 512개 등)
  - **파일명**: 8.3 포맷(짧은 파일명, 예: FILENAME.TXT)
  - **저널링, 권한, 타임스탬프 등 고급 기능 없음**
  - **단순하고 호환성 높음**

- 로그
  - btmp: **/var/log/btmp,** 로그인 시도 중 **실패한 로그인** 내역을 기록하는 바이너리 로그 파일
  - wtmp: **모든 로그인 및 로그아웃** 기록, 시스템 부팅/종료 기록 등 사용자의 세션 이력을 저장하는 바이너리 로그 파일로, last 명령어로 조회가능
  - xferlog : ftp 접근 여부를 검토할 수 있는 로그
  - 윈도우 로그
    - 개체 액세스 감사 - 특정 파일이나 디렉터리, 레지스트리 키 등과 같은 객체에 대한 접근을 시도하거나 속성변경등을 탐지한다.
- 랜섬웨어
  - 페트야, 크립토월, 워너크라이
- 크립토재커
  - 다른 사람의 컴퓨터, 스마트폰, 서버 등 IT 기기의 **컴퓨팅 자원을 무단으로 빼앗아 암호화폐(가상화폐)를 채굴하는 사이버 범죄자 또는 악성코드, 악성프로그램**
  - 피해자의 시스템에 몰래 크립토마이닝(암호화폐 채굴) 소프트웨어를 설치
  - 이 프로그램은 백그라운드에서 CPU, GPU 등 컴퓨팅 자원을 사용해 암호화폐를 채굴하고, 채굴된 암호화폐는 공격자의 지갑으로 전송
- 파일시스템의 시간속성
  - **atime (Access Time)**: 파일에 마지막으로 접근(읽기)한 시간
  - **mtime (Modify Time)**: 파일의 내용이 마지막으로 수정된 시간

    - **ctime (Change Time)**: 파일의 메타데이터(권한, 소유자 등)가 마지막으로 변경된 시간
    - **crtime 또는 birth time**: 파일이 최초로 생성된 시간
- pam(pluggable Authentication Module)
    - 리눅스에서 시스템 관리자가 응용프로그램들이 사용자를 인증하는 방법을 선택할 수 있도록 해주는 공유 라이브러리 묶음으로 이것을 사용하는 응용프로그램을 재컴파일 하지 않고, 인증방법을 변경할 수 있다는 장점이 있다.
- rlogin접속 설정 파일 : /etc/hosts.equiv, /.rhost
    - hosts.equiv : 이 파일에 적어두면, 클라이언트가 패스워드 입력할 필요없이 로그인가능하게 해주는 서비스
- rpc
    - 원격제어를 위한 코딩없이 다른 주소공간에서 함수나 프로시저를 실행할 수 있게해주는 프로세스간 프로토콜
    - xml rpc라는 서비스는 xml기반의 분산시스템 호출방법으로 rpc호출에 대해 xml 형태로 매개변수나 리턴값을 반환
- sshd
    - SSH Daemon"의 약자로, **SSH(Secure Shell) 서버에서 동작하는 백그라운드 프로세스(데몬)**입니다.
    - **네트워크를 통해 들어오는 SSH 연결 요청을 24시간 대기하며, 사용자의 인증, 암호화된 통신, 터미널 연결, 파일 전송, 포트 포워딩 등 SSH 프로토콜의 서버 역할**
- drive by download
    - 해커가 홈페이지 해킹한 후, 취약점에 따른 exploit코드가 있는 악성 스크립트를 은닉시키고, 이용자가 접숙할 경우 악성코드가 다운로드되는 공격기법으로 사용자 개입없이 접속만으로 감염된다.
- snort
    - 실시칸 트래픽 분석과 패킷로깅이 가능한 가벼운 네트워크 **침입탐지시스템**이다.
    - 프로토콜 분석, 내용검색/매칭을 수행할 수 있으며, 다양한 공격과 스캔을 탐지할 수 있다.
    - **Snort의 threshold 옵션**
        - 네트워크 트래픽에서 과도한 이벤트 발생 시 경고(알림)나 로그의 남발을 방지하고, 이벤트 발생 빈도에 따라 탐지 동작을 제어하는 기능

        - 타입
            - `limit`: 지정된 시간(seconds) 동안 지정된 횟수(count)까지 action(알림 등)을 수행합니다. 즉, 설정한 횟수까지는 모두 탐지합니다.
            - `threshold`: 지정된 시간 동안 지정된 횟수마다 action을 수행합니다. 예를 들어, 60초 동안 100번 이벤트가 발생하면 1번, 200번이면 2번 탐지합니다.
            - `both`: 지정된 시간 동안 지정된 횟수에 도달할 때 한 번만 action을 수행합니다.
    - 탐지 옵션
        - **sid (Rule ID)**
            - 규칙을 고유하게 식별하기 위한 번호입니다. (예: `sid:20000001;`)
        - **nocase (Case Insensitive)**
            - 대소문자를 구분하지 않고 패턴을 탐지합니다. (예: `content:"USER root";` `nocase;`)
        - **depth**
            - **패킷 내에서 검색을 시작할 위치(바이트 시작점)를 지정**합니다.
                - **depth**: 검색 범위의 끝 위치를 지정 (예: `depth:20` → 20바이트까지 검색).
        - **distance**
            - **이전 content 패턴 매치 끝 지점 이후 몇 바이트부터 검색할지 지정**합니다.

              (예: 이전 패턴 끝에서 3바이트 뒤부터 검색 → `distance:3`)
- 리눅스 특수권한
    - root와 동일한 권한 = uid: 0, gid: 200
    - SetGID가 부여된 파일은 소유그룹의 실행권한이 x에서 s로 변경
    - SetUID가 부여된 파일은 소유자 실행권한이 x에서 s로 변경
        - **chmod 4755 파일명**
            - **4755**에서 첫 번째 숫자 4는 SetUID 비트로 설정하는 것임
            - 즉 파일을 실행하는 사용자에 상관없이 해당 파일은 소유자의 권한으로 실행된다.

        - SetUID가 설정된 실행 파일을 **누구든 실행하면, 그 실행은 파일의 소유자 권한으로 동작**합니다.
        - 대표적인 예로 `/usr/bin/passwd` 파일이 있습니다. 이 파일은 일반 사용자가 자신의 비밀번호를 변경할 때, 시스템의 중요한 파일을 수정해야 하므로 SetUID가 적용되어 있다.
    - Sticky bit
        - **공용 디렉터리(예: /tmp)**에 설정하는 특수 권한
        - /tmp와 같은 777 권한의 공용디렉터리에서 파일 삭제 문제를 해결
        - 이 권한이 설정된 디렉터리에서는 **누구나 파일을 생성하거나 읽을 수 있지만, 파일을 삭제하거나 이름을 바꿀 수 있는 사람은 그 파일의 소유자와 root(관리자)로 제한**
- **Null session 공유 취약점**
    - **윈도우 시스템에서 인증(사용자명, 비밀번호) 없이 네트워크 공유(특히 IPC$(Inter-Process Communication) 등)에 접속할 수 있는 보안 약점**
    - ipc란? 윈도우 시스템에서 프로세스 간 특별한 공유
- index.dat
    - ie 검색 히스토리 저장소
- 기억 장치의 메모리 반입 정책
    - 최초 적합(First fit) : 메모리 공간을 처음부터 탐색하여, 요청보다 크거나 같은 첫 번째 빈 공간에 할당
        - **장점:** 탐색 속도가 빠르고, 구현이 간단합니다.
        - **단점:** 공간이 많이 남아도 불필요하게 분할될 수 있습니다(외부 단편화 발생 가능).
    - 최상 적합(Best fit) :요청 크기와 가장 비슷한(차이가 가장 적은) 빈 공간을 찾아 할당합니다.
        - **장점:** 메모리 낭비가 적고, 효율적인 메모리 사용이 가능합니다.
        - **단점:** 작은 조각(외부 단편화)이 많이 발생할 수 있고, 탐색 시간이 길어질 수 있습니다.
    - 최악 적합(Worst fit) : 요청 크기와 차이가 가장 **큰(가장 큰) 빈 공간**에 할당합니다.
        - **장점:** 큰 공간을 남기지 않으므로, 큰 요청이 들어왔을 때도 대응할 수 있습니다.

        - **단점:** 여전히 외부 단편화가 발생할 수 있고, 실제로는 잘 사용되지 않습니다.
    - 다음 적합(Next fit) 마지막으로 할당한 위치에서부터 탐색을 시작하여, 요청 크기 이상의 첫 번째 빈 공간에 할당합니다.
        - **장점:** 탐색이 최초 적합보다 더 빠를 수 있습니다(특히 메모리가 많이 사용된 경우).
        - **단점:** 최초 적합과 마찬가지로, 공간 활용이 비효율적일 수 있습니다.
- 매크로 바이러스
    - **플랫폼과 무관하에 실행된다.**
    - **주로 이메일을 통해 감염된다. :** 이메일 첨부 파일, 네트워크 공유, 이동식 저장매체 등으로 전파되며, 실제로 이메일을 통한 감염이 매우 흔합니다
    - 매크로 바이러스는 문서 파일 내부의 매크로(스크립트)로 작성되며, EXE(실행 파일) 형태의 자동화된 기능을 포함하지 않습니다. 매크로 바이러스 자체가 EXE 파일은 아닙니다
- 파일시스템 터널링(File system tunneling) : Window에서 파일이 삭제된 직후 일정 시간(기본 15초)안에
  동일한 이름의 파일이 생성되는 경우 방금 삭제된 파일의 테이블 레코드를 재사용하는 경우
- 리눅스 Capabilities
    - **CAP_SYS_MODULE : 커널 모듈 동적 로드/언로드**: `insmod`, `modprobe`, `rmmod` 등의 명령어를 통해 커널 모듈을 추가하거나 제거. **루트 권한과 동등한 위험성**을 지니는 모듈.
    - **CAP_AUDIT_CONTROL**: 시스템 감시(audit) 설정 관리 권한.
    - **CAP_MAC_ADMIN**: MAC(Mandatory Access Control) 정책 관리 권한
- 시그니처(Signature) : 대부분의 응용 프로그램에서 생성된 파일은 항상 동일한 몇 바이트를 파일 내부의 특정 위치에 가지고 있다. 특정위치의 고정값
- SAM
    - **윈도우 시스템의 사용자 계정 및 패스워드를 암호화하여 보관**
    - HKEY_LOCAL_MACHINE\SAM에 저장되어있으며, 일반계정은 접근 불가
    - 운영체제가 작동하는 동안 접근할 수 없도록 잠겨있다. (종료하면 가능)
- SCAN

    - **디스크 스케줄링 알고리즘 중 엘리베이터 알고리즘으로 “디스크 헤드를 실린더 번호가 낮은 순서대로 이동시키다가, 디스크의 끝에 도달하면 방향을 바꿔 실린더 번호가 높은 순서대로 이동시키는 알고리즘”**
    - 다른 알고리즘
        - SSTF(Shortest Seek Time First)**: 디스크 헤드와 가장 가까운 실린더에 있는 요청을 먼저 처리하는 알고리즘
        - **C-SCAN(Circular SCAN)**: SCAN 알고리즘의 변형으로, 디스크 헤드가 디스크의 끝에 도달하면 다시 처음으로 돌아와 같은 방향으로 이동하는 알고리즘입니다.
        - **FCFS(First Come First Served)**: 요청이 들어온 순서대로 처리하는 알고리즘
- 무차별 공격 : id, 비번에 대해 도구를 이용하여, id, 비번을 자동으로 조합하여 크랙하는 공격
- **윈도우 시스템 암호화 방법에서 EFS(Encrypted File Service)**
    - **사용자 단위 데이터 암호화 기능을 제공한다.**
        - **해당 사용자의 인증서로만 복호화가 가능**
    - **컴퓨터 단일 또는 복수 사용자에게 대한 파일 및 폴더 단위 암호화를 지원**
- Adversarial 공격
    - AI나 머신러닝의 이미지 인식에 있어서 이미지 속에 인간이 감지할 수 없는 노이즈나 작은 변화를 주어 AI 알고리즘의 특성을 악용하여 잘못된 판단을 유도하는 공격
- **netstat 명령어를 통해 확인할 수 있는 정보 : 라우팅 테이블정보, 소켓을 열고있는 프로세스 id, 프로세스이름, 열린 포트 정보**
    - 오답: 데이터 패킷
- **Visual Basic 스크립트를 이용한 악성코드**
    - 확장자는 VBS 또는 JSE
    - 러그버그라고 불리는 이메일에 첨부되어 전파된 바이러스가 Visual Basic 스크립트로 개발되었다.
- lsof
    - **디바이스를 사용 중인 프로세스를 찾기 위해 사용할 수 있는 명령어**
        - 오답: ps, metstat

네트워크 보안

- **KRACK(Key Reinstallation Attack) 공격**
  - WPA2 프로토콜의 **4-Way Handshake 과정**에서 키 재설정 취약점을 악용
  - **TCP 연결 하이재킹 :** 암호화 키를 탈취해 TCP 세션을 장악하고 통신을 가로챌 수 있.
  - **HTTP 컨텐츠 인젝션 :** 암호화된 트래픽을 복호화한 뒤, 악성 코드나 랜섬웨어를 웹사이트에 주입할 수 있다.
  - **Wi-Fi 패킷 재전송 :** 핸드셰이크 메시지(특히 3단계 메시지)를 재전송해 키를 재설치하고 암호화를 무력화
  - 오답 : **SSID 브로드캐스팅이랑은 무관하다.**
- firewall, ids, ips 차이
  - firewall, ips만 패킷차단 가능
  - ids, ips만 이상탐지 가능
  - firewall(침입**차단** 시스템)
    - 내부 네트워크 주소와 인터넷 주소를 변환시켜주는 기능을 설치하여 운영할 수 있다
    - 사용자 인증기능이 있다
    - 데이터 축약기능은 없다
    - 동작방식
      - Stateful Inspection방식
        - 패킷의 헤더 내용을 분석하여 순서에 위배되는 패킷 차단
        - 패킷 필터링 방식에 비해 세션 추적 기능 추가
        - 데이터 내부에 악의적인 정보를 포함할 수 있는 프로토콜에 대한 대응이 어려움
  - ids(intrusion detection system 침입탐지시스템)는 실시간 탐지=경보장치
    - 비정상적이거나, 악의적인 활동, 보안위배 등을 실시간 감지
    - 사용자에게 경고 보내지만, 차단하진 못한다.
    - 주로 방화벽 뒤
    - 침입 경로를 찾을 수 있도록 탐지대상으로부터 생성되는 **로그를** 제공한다.

        - 문자열을 비교하여 네트워크 패킷을 검사하는 방법은 Signature-based Detection의 일종이다.
        - 시그니처 기반 탐지(Signature-based Detection)**가 오직 "이미 알려진 공격
        - **데이터 수집 → 데이터 가공 및 축약 → 침입분석 및 탐지 → 보고 및 대응**
        - Anomaly Detection은 정상 행위를 규정하여 공격을 탐지하는 방법이다.
    - ips(intrusion prevention system 침입 방지 시스템)는 세션기반 탐지=경보+문단속
        - ids보다 더 나아가 차단까지 가능. 즉각 대응해서 피해 예방
        - 주로 방화벽 뒤 또는 네트워크 중간
        - 침입방지시스템은 침입자에게 시스템이나 네트워크를 사용하지 못하게 하는 등 능동적인 기능을 수행할 수 있다.
- dns 싱크홀
    - DNS 싱크홀은 악성코드 감염 PC가 해커에게 가지 못하게 '가짜 길'을 만들어주는 우회로
    - 감영경로 추척에 활용
    - 해커를 막는 보안기술
- HSM
    - hardware security module 암호화에 사용되는 암호키를 보관하고 관리하는 하드웨어 장치
    - 은행 등에서 사용
- TCB
    - trusted computing base 신뢰할 수 있는 컴퓨팅 기반으로 보안을 책임지는 핵심 하드웨어, 소프트웨어, 펌웨어 집합을 말한다.
- 비트라커
    - 윈도우os에 내장된 디스크를 전체 암호화하는 기능을 말한다.
    - aes알고리즘으로 암호화한다.
- spi(stateful packet inspection), dpi(deep packet inspection)
    - dpi는 심층 패킷 분석 방식으로, 패킷 내의 바이러스등 악성코드를 검사할 수 있다. spi보다 진보된 기술로 데이터 내용(페이로드)까지 분석한다. 내용/출처/목적지 등

심층검사하며 tcp 전계층에 대해 탐지 차단가능하다. 정밀한 만큼 느리고 비용이 크다

    - spi는 상태 기반 패킷 검사로, 주로 패킷 헤더와 세션정보를 확인하고 의심스러우면 트래픽 차단한다.. (즉 데이터 내용(페이로드)는 보지 않는다), 빠른 속도로 대용량 트래픽 처리가 가능하다. 어플리케이션 계층까지의 정밀분석은 어렵다.

- ospf (open shortest path first)
    - anycast dns에서 경로를 동적으로 광고하고, 최적의 dns서버로 트래픽 유도하는 역할을 한다. anycast dns구축시 ospf를 사용하는 것이 일반적이다.
    - 기업이나 기관에서 사용하는 동적 라우팅 프로토콜로 최단 경로 찾아서 데이터 전달해주는 동적 라우팅 프로토콜
    - 다익스트라 알고리즘 사용, hop수에 제한이 없다. 대규모 네트워크에서도 안정적
- anycast dns
    - 여러 지리적 위치에 동일한 ip를 가진 dns서버를 배치하고, 라우팅 프로토콜을 이용해서 클라이언트가 가장 가까운 서버로 접속하게 하는 방식
    - 서비스 가용성,성능에도 좋고, ddos공격에도 좋다.
    - 라우팅 프로토콜 표준은 bgf(border gateway protocol)방식이다.(ospf아님)
- siem(security information and event management 보안 정보 및 이벤트 관리)
    - 조직의 인프라에서 발생하는 로그와 이벤트를 수집,저장,분석해서 보안위협을 실시간탐지하고 대응하는 통합 보안 관리 솔루션
    - 네트워크 포렌식과 보안관련 준수성에 중요한 역할 담당
- syn flooding, land, smurf
    - syn flooding
        - 3way handshaking tcp연결중 half-open연결이 가능하다는 취약점을 이용한 공격
        - 증폭(Amplification)으로 공격하는것이 아님. 증폭 공격은 DNS/ICMP 리플렉션 공격의 특징
        - 서버 측의 대기 큐의 크기를 늘리는 방법이 대응 방법
        - **nmap의 TCP Half Open 스캔과 TCP FIN/NULL/XMAS 스캔**
            - TCP FIN/NULL/XMAS 스캔은 열린 포트에서 **응답이 없다.**
            - 닫힌포트에 대해서 Half Open 스캔은 `RST-ACK`, FIN 계열은 `RST`로 응답

- `SYN-ACK`는 Half Open 스캔에서만 발생
- **참고) 열린 포트(Open Port) :**네트워크 장비(서버, PC 등)에서 특정 포트 번호로 서비스(예: 웹 서버, 메일 서버 등)가 실행 중이며, 외부에서 해당 포트로 접속 요청이 들어오면 응답할 준비가 되어 있는 상태입니다.
  - **특징**:
    - 외부에서 해당 포트로 접속하면 정상적으로 통신이 이루어집니다.
    - 예를 들어, 웹 서버(HTTP)는 기본적으로 80번 포트를 열어두고, 클라이언트가 접속하면 웹 페이지를 제공합니다.
    - 포트 스캔 시, SYN 패킷을 보내면 **SYN+ACK** 응답이 오면 열린 포트임을 알 수 있습니다
  - **닫힌 포트(Closed Port)**
    - 해당 포트 번호로 서비스가 실행되고 있지 않거나, 방화벽 등 보안 장치에 의해 차단되어 외부에서 접속해도 응답하지 않거나 연결이 거부되는 상태입니다.
    - **특징**:
      - 외부에서 해당 포트로 접속하면 응답하지 않거나, 연결이 즉시 거부됩니다.
      - 포트 스캔 시, SYN 패킷을 보내면 **RST(Reset)** 또는 **RST+ACK** 응답이 오면 닫힌 포트다

- 받을수 있는 공격
  - Half Open Connection 공격
  - 분산 DOS 공격
  - **Reflector공격 (**공격자가 피해자의 IP 주소를 스푸핑하여 다수의 서버(반사체, Reflector)에 SYN 패킷을 대량으로 보내고, 이 서버들이 피해자에게 SYN-ACK 응답을 집중적으로 보내게 하는 **분산 서비스 거부(DDoS) 공격)**
  - 오답: **Teardrop 공격(이건 syn flooding 공격이 아니다)**
    - 공격자가 **조각화된 IP 패킷**을 보낼 때, **오프셋(시작 위치)** 값을 조작해 패킷이 중첩되도록 합니다.
    - 피해 시스템은 이를 재조립하려 시도하지만, 오류로 인해 크래시되거나 과부하가 발생

        - **반사체를 사용하지 않으며**, 단일 타깃에 직접 공격
    - 소스 IP를 스푸핑(IP Spoofing)하여 서버에 다수의 SYN 패킷을 보내는 방식이 일반적이다.
  - land 공격
    - 출발지와 목적지 IP/포트를 **동일하게** 공격대상ip로 설정한 패킷을 전송해 시스템의 TCP/IP 스택을 혼란시키는 공격입니다.
  - smurf : icp request 메시지를 이용해서 대량의 메시지를 전송하는 공격으로 라우팅 테이블의 패킷전달 기능을 악용한 방법이다. 출발지 주소를 자신의 아이피가 아닌 공격대상 ip로 변조하면 라우터가 이를 모든 네트워크에 다 보내게 되는 공격으로
    - ICMP Echo Request(ping)**를 브로드캐스트 주소로 전송해 다수의 응답을 유발하는 **ICMP 기반 증폭 공격**
    - 방지 방법: direct broadcast를 disable시킨다, ping reply 금지, 라우터의 ingress filtering을 이용해서 spoof된 패킷을 막는다(spoof된 패킷을 막는다 = **"위조된 정보(예: 출발지 IP 주소, MAC 주소 등)를 가진 가짜 패킷이 네트워크에 들어오거나 전달되는 것을 차단")**
- **Boink 공격**
  - **IP 단편화(Fragmentation)** 과정에서 시퀀스 번호를 비정상적으로 조작해 패킷 재조립 오류를 유발하는 공격(중간에 패킷 시퀀스 번호를 비정상적인 상태로 전송하는 공격)
- **HTTP Slowloris 공격 : "동시 사용자 수 제한"공격으로HTTP 계층에서 다수의 연결을 오래 유지하며 서버 자원을 고갈시키는 공격으로, IP Spoofing과는 직접적인 관련이 없다.**
- heartbleed
  - OpenSSL 라이브러리에서 발견된 심각한 보안 취약점, SSL/TLS에서 발생하는 취약점
- ssl 보안 프로토콜
  - record 프로토콜 : **Record 프로토콜**은 SSL/TLS에서 데이터를 안전하게 전송하기 위해 데이터를 단편화, 압축, MAC 생성, 암호화, 헤더 추가
  - 그리고 전송 및 수신 시 복호화와 무결성 검증을 수행하는 **핵심 보안 계층**입니다

    즉, SSL/TLS의 데이터 보호(기밀성, 무결성, 인증)의 실질적인 처리를 담당하는 프로토콜

- memcached ddos(네트워크 공격), meltdown spectre(하드웨어 취약점), shell shock(**소프트웨어 버그)**
  - memcached ddos : 취약한 **Memcached 서버**를 향해 **UDP 프로토콜**을 통해 위조된 대량의 트래픽을 증폭시켜 특정 표적을 공격하는 **분산 서비스 거부(DDoS) 공격**
    - 이로 인해 표적의 서버나 네트워크가 과부하되어 정상 서비스가 중단됩니다.
    - memcached는 **인터넷 속도 향상을 위한 캐싱 시스템(Memcached)**
  - meltdown spectre
    - 현대 프로세서(CPU)의 설계 결함에서 비롯된 **하드웨어 취약점으로** 패치로 완화 가능하지만, 성능 저하가 발생할 수 있습니다.
    - **Meltdown**: 사용자 프로그램이 운영체제 커널 메모리에 접근해 민감한 데이터(비밀번호, 암호화 키 등)를 유출시킵니다.
    - **Spectre**: 정상 프로그램을 속여 다른 프로그램의 메모리 데이터를 유출시킵니다. 두 취약점 모두 **추측 실행(Speculative Execution)** 기능을 악용합니다. 이건 **하드웨어** 취약점
  - shell shock
    - **Unix Bash 셸**의 보안 결함으로, 원격 코드 실행이 가능한 취약점
    - 환경 변수를 조작해 Bash가 의도하지 않은 명령어를 실행하도록 유도합니다.
    - 공격자가 서버를 장악하거나 봇넷을 구축하는 데 활용되었습니다.
    - Apache 웹 서버, OpenSSH, Qmail 등 다양한 시스템에서 위협이 확인
  - icmp 메시지 타입
    - 이 중 0, 8번이 ping

타입 번호	메시지 이름	설명
0	**Echo Reply**	Ping 요청에 대한 응답 메시지 (Echo Request의 응답)
3	Destination Unreachable	목적지 도달 불가 (네트워크, 호스트, 포트, 프로토콜 등)
4	**Source Quench**	네트워크 폭주로 데이터 손실 유실(혼잡 제어, 현재는 거의 사용하지 않음)
5	Redirect	더 나은 경로가 있을 때 경로 재지정 안내
8	**Echo Request**	Ping 요청 메시지(네트워크 연결 진단용)

9	Router Advertisement	라우터가 자신을 네트워크에 광고
10	Router Solicitation	호스트가 라우터를 찾기 위한 요청
11	Time Exceeded	**TTL(Time To Live) 초과**, 패킷이 너무 오래 네트워크에 머문 경우
12	Parameter Problem	잘못된 헤더 매개변수 발견 시 알림
13	Timestamp Request	시간 동기화 요청
14	Timestamp Reply	시간 동기화 응답
15	Information Request	정보 요청(거의 사용하지 않음)
16	Information Reply	정보 요청에 대한 응답(거의 사용하지 않음)
17	Address Mask Request	서브넷 마스크 요청
18	Address Mask Reply	서브넷 마스크 응답
30	Traceroute	경로 추적(Traceroute)

- wep, wpa, wpa2
  - wep에서는 인증이나 암호화에 사전 공유키를 사용할 수 있지만 wpa나 wpa2처럼 동적으로 암호화 키를 변경하는것은 안된다.
    - wep는 무선랜 통신을 위한 암호화 기술 중 가장 기본적인 방 법이다. 무선 단말에서 무선 AP와 통신을 위해 인증 요청을 보내고, 요청을 받은 무선 AP에서는 중간에 키를 계속 가로챌 경우 키 생성 순서를 예측하는 것을 방지하기 위해 랜덤하게 Initial Vector를 생성하여 무선 단말기에 보낸다.
  - wep에서는 암호 강도가 높지 않은 rc4를 암호화 알고리즘으로 사용했으며 암호화 키 길이는 64비트 또는 128비트이 다. aes기반의 강력한 암호화방식을 의무화한것은 wpa에서부터이다.
  - **WEP**는 RC4 암호화 알고리즘을 사용한 것
  - WEP 인증은 데이터 암호화와 사용자 인증 기능을 제공한다.
  - **WPA**에서는 기본적으로 **TKIP** 암호화 방식을 사용하며, **AES 기반 암호화는 '선택적'**, AES를 사용할 수는 있었지만, **의무화(필수)는 아니었습니다**
  - **AES 기반의 암호화(CCMP)를 '의무화'한 것은 WPA2부터** AES 암호화가 필수로 적용
  - EAP 인증을 통해 공격자의 패킷 도청을 방어할 수 있다.

- 802.11 무선 표준에서는 무선랜의 구성에 따라 2개의 구성유형이 제시되고 있다. 첫 번째는 **Infrastructure** 모드로 무선 AP와 무선 단말기로 구성되는 방식과, 두 번째는 무선 단말기 사이에 직 접 통신이 이뤄지는 **Ad Hoc** 모드이다.
- L2TP
    - data link layer
    - (Layer 2 Tunneling Protocol, 계층 2 터널링 프로토콜)는 **가상 사설망(VPN) 구축에 널리 사용되는 터널링 프로토콜**
- cdr (content disaram & reconstruction) : 파일내의 악성코드를 분해해서 제거하고 콘텐츠는 원본관 동일하게 생성해서 새로운 파일을 만드는 솔루션
- 내부공격자 위험을 줄이기 위해서는 보안설정을 white list로 해야한다.
- bpfdoor(Berkeley Packet Filter) 취약점
    - **리눅스 시스템을 겨냥한 고도화된 백도어 악성코드**입니다. 이 악성코드는 SKT의 핵심 서버(HSS, 홈 가입자 서버)에 침투해 가입자 USIM 정보 등 민감한 데이터를 유출하는 데 사용된 것으로 확인
    - **패시브 백도어**로 분류되며, 일반적인 악성코드와 달리 시스템에 거의 흔적을 남기지 않고, 포트 바인딩 없이 동작합니다. 즉, netstat, ss 등으로도 쉽게 탐지되지 않습니다
    - **네트워크 방화벽이나 보안 장비를 우회**할 수 있고, TCP, UDP, ICMP 등 다양한 프로토콜을 통해 명령을 수신합니다.
    - SKT 사건에서 BPFdoor는 **VPN 장비 등 외부 접속 경로의 취약점**을 통해 침투한 것으로 추정되며, 보안 장비 우회와 은폐 능력 때문에 탐지와 대응이 매우 어려웠던 것으로 분석
- Promiscuous mode
    - 스니퍼 탐지 도구는 로컬 네트워크 상의 호스트들에서 네트워크 인터페이스 카드의 Promiscuous mode 여부를 검사함으로써 스니퍼가 수행되고 있는지를 확인할 수 있다.
    - Promiscuous Mode(프로미스큐어스 모드, 무차별 모드)**는 네트워크 카드(NIC)가 네트워크에 흐르는 모든 패킷을 받아들이는 동작 모드입니다. 원래 네트워크 카드는 자기 MAC 주소로 도착한 패킷만 받아들이고, 나머지는 무시합니다. 하지만 Promiscuous Mode를 활성화하면, 목적지와 상관없이 네트워크 상의 모든 패킷을 수신할 수 있습니다
- Duplex Mode

    - 네트워크 장비(예: 컴퓨터, 스위치, 라우터)끼리 데이터를 주고받는 방식, 즉 송신과 수신이 어떻게 이루어지는지를 나타내는 통신 모드
    - **Half Duplex (반이중)**
        - *한 번에 한 방향으로만 데이터 전송이 가능*합니다.
        - 즉, 데이터를 보낼 때는 받을 수 없고, 받을 때는 보낼 수 없습니다.
        - 무전기(워키토키)처럼 "내가 말할 땐 상대방이 들을 수만 있다"는 방식입니다.
    - **Full Duplex (전이중)**
        - **동시에 양방향 데이터 전송이 가능합니다.**
        - 데이터를 보내면서 동시에 받을 수 있습니다.
        - 전화기처럼 "서로 동시에 이야기하고 듣는 것"과 같습니다.
        - 스위치 기반의 현대 네트워크 환경에서는 거의 대부분 Full Duplex를 사용합니다
    - **Simplex (단방향)**
        - 한쪽에서만 보내고, 다른 쪽은 받기만 하는 방식입니다.
        - 라디오, TV 방송이 대표적인 예입니다
    - *Duplex Mode가 맞지 않으면 네트워크 속도 저하, 충돌(Collision), 통신 오류*가 발생
- ARP (Address Resolution Protocol, 주소 결정 프로토콜))
    - 네트워크에서 IP 주소(논리 주소)를 실제 컴퓨터의 물리 주소인 MAC 주소로 변환해주는 프로토콜입니다. 쉽게 말해, "이 IP 주소를 가진 컴퓨터의 MAC 주소가 뭐야?"라고 물어보고, 그 답을 받아오는 역할
- 무선 네트워크 아이디(SSID)
    - 무선랜의 전송 패킷에 덧붙여지는 32bytes 길이의 고유 식별자로서, 무선장치들이 BSS(Basic Service Set)에 접속할 때 패스워드같이 사용되는 코드
    - **SSID 브로드캐스팅**은 단순히 Wi-Fi 네트워크 이름을 노출시키는 설정
    - SSID(네트워크 이름)를 알고 있다면, 브로드캐스팅하지 않아도 **수동으로 SSID와 암호를 입력해 AP에 접속할 수 있다.**
- SDN(Software Defined Networking)
    - 폐쇄적이었던 네트워크 장비들을 열린 구조로 바꾸고 소프트웨어로 제어할 수 있는 기능성을 통해서 네트워크 구조의 새로운 패러다임을 이끌고 있으며 네트워크의 관

리적인 측면에서 많은 발전을 이루고 있다. 트래픽의 미세흐름 조정을 통해 네트워크의 효율성을 높이고, 지금까지 어려웠던 QoS 보장 기술을 확보하며, 손쉬운 장비 관리 등 네트워크의 성능 과 관리성을 향상시킬 수 있다.

- 지능형 지속 위협(Advanced Persistent Threat, APT)
  - 특정 목표를 정하고, 오랜 시간 동안 다양한 방법과 고도의 기술로 은밀하게 침투해 정보를 빼내거나 시스템을 장악하려는 공격입니다
  - 공격자는 다양한 수법과 맞춤형 악성코드, 여러 단계의 공격을 사용하며, 탐지를 피하기 위해 지속적으로 방법을 바꿈. 그래서 공격자의 비용이 크다
  - 이 때문에 **시스템 관리자는 모든 종류의 여러방법으로 공격 시나리오를 고려해야 하며, 방어가 매우 어렵고 복잡**
- TCP의 3-Way Handshaking을 통해 서버와 연결을 설정할 때, **클라이언트 측의 연결 상태 변화 순서**
  1. **CLOSED :** 연결 시도 전, 클라이언트의 초기 상태입니다
  2. **SYN_SENT :** 클라이언트가 서버로 SYN 패킷(연결 요청)을 보낸 후, 응답을 기다리는 상태입니다
  3. **ESTABLISHED :** 서버로부터 SYN+ACK 패킷(연결 수락 및 응답)을 받고, 클라이언트가 ACK 패킷을 보내 연결이 완전히 성립된 상태입니다. 이 상태에서 데이터 송수신이 가능
- SOAR
  - 다양한 보안 위협에 대한 대응 프로세스를 자동화해 낮은 수준의 보안 이벤트는 사람의 도움 없이 처리하고, 보안사고 발생 시 표준화된 업무 프로세스에 따라 담당자가 쉽게 대응할 수 있는 차세대 보안 솔루션
- 스푸핑 공격
  - 공격자가 자신을 다른 존재로 속여 시스템이나 사용자를 기만하는 공격 방식
  - 대표적인 스푸핑 공격 종류
    - **ARP 스푸핑**: ARP 프로토콜을 속여 네트워크 내에서 자신의 MAC 주소로 트래픽을 유도하는 공격
    - **IP 스푸핑**: 자신의 IP 주소를 다른 사람의 IP로 위장하여 공격하는 방식
    - **DNS 스푸핑**: DNS 응답을 조작해 사용자가 잘못된(공격자가 원하는) IP로 접속하게 만드는 공격으로
      - hosts 파일을 통해 도메인 이름에 대한 IP 주소를 적어두면 대응가능하다

- traceroute
  - 패킷이 목적지까지 도달하는 동안 거치는 라우터 IP를 확인하는 도구이다. 이 도구는 udp와 icmp, ip의 ttl 값을 이용한다. 상대방의 IP 주소를 알고 있는 상태에서 상대방에게 인터넷 서비스를 제공하고 있는 회사를 알아내는 데 사용
  - traceroute 프로그램과 연관이 있는 ICMP 메시지는 시간초과(time exceeded)와 *에코(echo)*
  - **시간초과(Time Exceeded, Type 11)**
    - traceroute는 각 패킷의 TTL(Time To Live) 값을 1부터 시작해 하나씩 늘리며 목적지로 전송합니다.
    - 중간 라우터는 TTL이 0이 된 패킷을 폐기하고, **ICMP Time Exceeded** 메시지로 응답합니다.
    - traceroute는 이 메시지를 받아 해당 라우터의 주소를 기록해 경로를 추적합니다
  - **에코(Echo, Type 8/0)**
    - 일부 운영체제(특히 Windows의 tracert)는 UDP 대신 ICMP Echo Request(핑) 패킷을 사용합니다.
    - 목적지에 도달하면, 목적지 호스트는 **ICMP Echo Reply**(Type 0)로 응답합니다.
    - traceroute는 이 응답을 받아 최종 목적지에 도달했음을 확인합니다
- 서비스 거부 공격
  - **HTTP GET Flooding Attack : 최상위 계층 layer7에서 발생**
  - **ICMP Flooding Attack : Layer 3(네트워크 계층)**
  - **LAND Attack : Layer 4(전송 계층)**
    - TCP 패킷의 출발지와 목적지 IP/포트를 동일하게 설정해 시스템의 TCP 연결 처리를 혼란스럽게 만듭니다.
  - **Teardrop Attack : Layer 3(네트워크 계층)**
    - 조각화된 IP 패킷의 오프셋 값을 조작해 시스템이 패킷 재조립에 실패하도록 하는 공격
- VPN
  - SSL VPN은 별도의 클라이언트 프로그램 설치 없이 웹브라우저만으로도 접속할 수 있어 사용가능

- **IPSec VPN은 네트워크 계층에서 안전하게 정보를 전송하는 방법이다.**
- IPSec VPN은 OSI 7계층 중 네트워크 계층(Layer 3)에서 동작하며, IP 패킷 자체를 암호화하여 안전하게 정보를 전송
- IPSec VPN은 **트랜스포트 모드와 터널 모드 모두 지원**
- 암호화 프로토콜로 ESP(Encapsulating Security Payload)와 AH(Authentication Header)를 모두 사용가능
  - **ESP를 설정하면 데이터 기밀성을 제공하여 데이터가 노출되는 것을 차단할 수 있다**
  - **AH를 설정할 시 데이터가 수정되지 않았음을 보장할 수 있다. - AH(Authentication Header)는 데이터의 무결성과 송신자 인증을 보장**
- **기본적으로 SSL VPN과 IPSec VPN은 데이터의 기밀성과 무결성이 동일하며, 단지 데이터의 암호화 구현 방식 및 적용계층에 차이가 있다.**
- **VPN 터널링에 사용되는 프로토콜**
  - **PPTP (Point-to-Point Tunneling Protocol) :**마이크로소프트가 개발한 가장 오래된 VPN 터널링 프로토콜 중 하나입니다. 데이터를 캡슐화하여 안전하게 전송할 수 있도록 해줍니다
  - **L2F (Layer 2 Forwarding) :**시스코가 개발한 터널링 프로토콜로, 데이터 링크 계층에서 동작하며 VPN 터널을 생성합니다
  - **IPSec (Internet Protocol Security) :**IP 계층에서 동작하는 표준 터널링 프로토콜로, 데이터의 암호화와 인증을 제공
- **IPSec의 두 가지 모드**
  - **Tunnel Mode**:
    - 전체 IP 패킷을 새 IP 헤더로 감싸 암호화
    - **게이트웨이(방화벽, 라우터) 간 VPN**에서 표준적으로 사용됨
    - 내부 네트워크 전체를 보호할 수 있음
    - Site-to-Site VPN(사설망-사설망 연결) 등에 적합
  - **Transport Mode**:
    - 원래 IP 헤더는 그대로 두고, 페이로드(TCP/UDP 포함)만 암호화
    - **엔드-투-엔드(호스트-호스트) 통신**에 적합
    - 즉, 두 서버 또는 클라이언트-서버 간 직접 통신에 사용

        - 게이트웨이 장비(방화벽, 라우터) 간의 네트워크 전체 보호에는 부적합
        - **트랜스포트 모드 AH헤더는 IP헤더와 IP페이로드 사이에 삽입된다**
    - **방화벽 장비에서의 적용 제한**
        - 방화벽(게이트웨이) 장비는 **네트워크 전체의 트래픽을 보호**하기 위해 패킷 전체를 암호화해야 한다..
        - **Transport Mode는 패킷의 페이로드만 보호**하고, 원래 IP 헤더는 암호화하지 않으므로, 게이트웨이-게이트웨이 간 VPN(즉, 방화벽 장비 간 VPN)에는 보안상 부적합하며, 실제로 대부분의 방화벽 장비는 Tunnel Mode만 지원한다.
    - Transport Mode는 **호스트-호스트** 또는 **특정 상황에서만 제한적으로** 사용
- **RSVP (Resource ReSerVation Protocol) :**RSVP는 네트워크에서 대역폭 등 리소스 예약을 위해 사용되는 프로토콜로, 즉, VPN 터널링 프로토콜이 아닙니다.
- Null Routing
    - 라우터나 스위치에서 DDoS 또는 DoS를 차단하는 경우 패킷이 특정 인터페이스로 보내져 패킷이 필터링 될 때마다 패킷의 출발지 ip로 ICMP Unreachable이라는 에러 메시지를 보 내게 되는데, 필터링 하는 패킷이 많을 경우에는 라우터나 스위치에 과부하를 유발할 수 있 기 때문에 ICMP 에러 메시지를 보내지 않도록 이것을 설정하는 것이 좋다.
- null 스캔
    - TCP 플래그 값을 모두 off(비활성화)한 패킷들을 이용하여 스캔하는 기법
- Cyber Kill Chain
    - 사이버 공격을 프로세스 상으로 분석해 각 공격 단계에서 조직에 가해지는 위협 요소들을 파악하고 공격자의 목적과 의도, 활동을 분쇄 완화해 조직의 회복 탄력성을 확 보하는 전략이다. 한마디로 공격자의 관점에서 사이버 공격 활동을 파악, 분석해 공격 단 계별로 조직에 가해지는 위협 요소를 제거하거나 완화하자는 것이다.
- 이터널블루 공격(EternalBlue Attack)
    - 윈도우의 소프트웨어 취약점을 악용하는 것으로 NSA가 개발한 것으로 추정되는 공격도 구로서 섀도 브로커스에 의해 2017년도에 공개되었다. 이는 미국 볼티모어시 정부에 대 한 랜섬웨어 공격에서 다시금 부상하게 되었다. 문제는 많은 컴퓨터가 구식의 윈도우 운 영체제를 계속 사용하고 있다는 것이다. 마이크로소프트의 SMB 구현의 취약점을 공격 한다.
- **익스플로잇(Exploit)**

    - 익스플로잇은 컴퓨터 시스템, 소프트웨어, 하드웨어, 네트워크 장비 등에 존재하는 **보안 취약점(버그, 약점)**을 악용해 공격자가 원하는 동작을 하도록 만드는 **공격 행위** 또는 **공격 도구/코드**
    - 대표적으로 시스템 권한 탈취, 악성코드 설치, 서비스 거부(DoS), 데이터 유출 등이 있습니다
- 스위칭 환경에서 시도할 수 있는 스니핑(네트워크 도청) 공격 유형
    - 스위칭 환경에서 스니핑 공격을 하기 때문에 관련된것들로, 스위치 환경은 기본적으로 목적지 MAC 주소를 가진 포트로만 트래픽을 전달하므로, 일반적으로 스니핑이 어렵지만 아래와 같은 공격을 통해 스위치 환경에서도 스니핑이 가능
        - switch jamming**(MAC Flooding)** : 스위치의 MAC 주소 테이블을 가득 채워 정상 동작을 방해하고, 결국 스위치가 허브처럼 모든 포트로 브로드캐스트하게 만들어 트래픽을 스니핑할 수 있게한다.
        - icmp redirect : ICMP Redirect 메시지로 라우팅 테이블을 변조, 트래픽이 공격자에게 오도록 하여 스니핑할수있다.
        - arp spoofing : 공격자가 ARP 패킷을 위조해 희생자의 트래픽이 공격자에게 가도록 유도, 스니핑이 가능
        - arp direct : ARP 스푸핑하고 유사,
        - **ARP Direct/Redirect/스푸핑/포이즈닝**: 다 같음
    - 오답 :
        - syn flooding은 스위칭이랑 관련없음. syn flooding은 서버 자원을 고갈시켜 서비스 거부를 유발하는 것으로 패킷을 도청하거나 트래픽을 가로채는 것이 아니다.
        - ip spoofing : **IP 스푸핑**은 공격자가 자신의 컴퓨터에서 보내는 패킷의 출발지 IP 주소를 **다른 사람의 IP 주소로 위조(변조)**하여, 마치 신뢰받는 다른 시스템이나 사용자인 것처럼 속이는 네트워크 공격 기법
- 스푸핑 (위장, 사칭) spoofing
    - **IP 스푸핑**: 자신의 IP 주소를 다른 사람의 IP로 위장
        - **RST를 이용한 접속 끊기**: 위조된(스푸핑된) RST 패킷을 이용해 정상 연결을 강제로 종료시키는 공격입니다. IP Spoofing과 관련이 있습니다
        - **순서번호 추측**: TCP 시퀀스 번호를 추측해 스푸핑된 패킷을 보내는 공격입니다. IP Spoofing이 필수적으로 사용됩니다
    - **이메일 스푸핑**: 발신자 주소를 위조해 신뢰받는 사람인 척 메일 발송

    - **ARP 스푸핑**: 네트워크 내에서 자신의 MAC 주소를 다른 장치의 주소로 속임
    - **DNS 스푸핑**: DNS 응답을 조작해 사용자가 잘못된 사이트로 접속하도록 유도
- CIDR
    - IPv4의 IP 주소 고갈 및 라우팅 테이블 대형화에 대한 해소책으로 기존의 클래스 기반 IP 주 소 체계를 벗어나 서브넷 마스크 정보를 IP 주소와 함께 라우팅 정보로 사용할 수 있게 만든 IP 주소 지정 방식
- 분산서비스 거부공격(DDoS)의 구성요소
    - 공격자(attacker)
    - 마스터(master) 또는 명령제어서버(c&c)
    - 에이젼트 또는 좀비 : 악성코드에 감염된 일반 사용자의 컴퓨터로, 마스터의 명령에 따라 실제로 공격 트래픽을 발생시키는 역할을 합니다.
    - 공격대상(victim) :에이전트로부터 실제 공격을 받는 서버, 네트워크, 서비스 등 목표 시스템입니다.
- TTL
    - TTL은 "**라우팅 정보가 잘못되어 발생하는 패킷 무한 반복을 제어하기 위한 값**" = **패킷이 네트워크에서 무한히 순환하는 것을 방지**하는 것
- NAC
    - 네트워크에 접근하는 접속 단말의 보안성을 검증하여 보안성을 강제화하고 접속을 통제할 수 있는 보안 인프라이다. 사용 단말이 내부 네트워크에 접속하기 전에 보안 정책을 준수했는지 여부를 검사해 네트워 크 접속을 통제하는 보안 솔루션이다.
    - 주요 기능으로는 접근제어/인증, PC 및 네트워크 장비 통제, 해킹, 웜, 유해 트래픽 탐지 및 차단 등이 있다.
- **SSL Handshake 프로토콜**
    - **Cipher Suite은 공개키(키 교환 알고리즘) 암호 시스템, 대칭키 암호 시스템, 해시 알고리즘 등 3개의 정보로 구성된다**
    - **SSL Handshake 프로토콜 동작과정을 통해 SSL 클라이언트와 서버가 공유하는 암호 알고리즘들과 키 값들이 생성된다.**
    - **SSL 클라이언트는 통신 상대인 서버의 신원확인을 위해 전자인증서 기반의 인증을 수행한다 = 서버는 SSL 인증서를 클라이언트에 제공하며, 클라이언트는 CA(Certificate Authority)를 통해 인증서의 유효성을 검증**

    - SSL 인증서는 비대칭키 암호 시스템을 기반으로 동작하며, 대칭키는 세션 데이터 암호화에만 사용됩니다.
        - 전자인증서는 **비대칭키 암호 시스템(공개키/개인키)**을 사용
- 계층
    - **이더넷(네트워크 인터페이스 카드)**:
        - *물리 주소(MAC 주소)**를 사용하며, **6바이트(48비트)**입니다
    - **인터넷 계층(IP 계층)**:
        - *논리 주소(IP 주소)**를 사용하며, **4바이트(32비트)**입니다
    - **전송 계층**:
        - *포트 주소(Port 번호)**를 사용하며, **2바이트(16비트)**
- DHCP
    - DHCP에서는 전송계층으로 udp프로토콜을 사용하는데, 서버는 잘 알려진 67번 포트를 사용하고, 클라이언트는 잘 알려진 68번 포트를 사용한다.
- Sandbox
    - Anti APT 제품군에 사용되는 기술로 실제 환경과 동일한 조건으로 만든 가상환경에서 의심 스러운 요소를 실행시킨 후 공격으로 의심되는 행위가 발생한다면 해당 요소를 침입으로 판 단한다.
- SCADA
    - 산업제어시스템(Industrial Control System)에 대한 공정, 기반 시설, 설비 를 바탕으로 한 작업공정을 감시하고 제어하는 컴퓨터 시스템으로, 최근 이를 대상으로 이루 어진 사이버 공격으로 인해 전력공급체계 등 사회기반시설 운영에 피해가 발생하고 있다.
- ftp
    - **포트 21만 열면 명령은 주고받을 수 있지만, 파일 전송(데이터 채널)이 불가능하므로 FTP 서비스가 제대로 작동하지 않습니다**
    - 파일 전송까지 원활하게 하려면, 사용하는 모드(액티브/패시브)에 따라 추가로 필요한 포트(포트 20 또는 서버/클라이언트의 임의 고포트)를 방화벽에서 열어야 한다.
- UDP Flooding의 대응 방안
    - **미사용 프로토콜 필터링**
    - **출발지 IP당 패킷 전송률(PPS)을 제한 (도착지에 대해 나오면 오답)**

    - **패킷 크기 기반 차단**
    - **Anycast를 이용한 대응 :** Anycast는 트래픽을 여러 서버로 분산시켜 단일 지점의 과부하를 방지합니다. 이는 대규모 DDoS 공격에 효과적인 대응 전략
- **스니핑 모니터링 프로그램인 sentinal을 이용하여 스니퍼를 탐지**
    - **./sentinel –a –t 211.47.65.4 : ARP 테스트를 수행하여 스니핑(프로미스큐어스 모드) 여부를 확인**
        - 프로미스큐어스 모드 : 일반적으로 네트워크 카드는 자신에게 온 패킷만 받아들이지만, 프로미스큐어스 모드에서는 목적지에 관계없이 모든 패킷을 받아서 상위 계층(운영체제)으로 전달
    - **./sentinel –d –f 1.1.1.1 –t 211.47.65.4 : 존재하지 않는 호스트(1.1.1.1)에 대한 DNS 질의를 대상 서버(211.47.65.4)로 보내, DNS 응답이 오는지 확인하여 스니핑 여부를 탐지**
    - **./sentinel–e –t 211.47.65.4 : Etherping 테스트를 수행하여 스니핑 여부를 확인**
        - **Etherping**은 스니핑 탐지 기법 중 하나로, 공격 대상(의심 시스템)에 ICMP Echo 요청(Ping) 패킷을 보낼 때, 목적지 IP는 정상이지만 목적지 MAC 주소는 존재하지 않는 값으로 위조하여 전송합니다. 정상적인 시스템은 자신의 MAC 주소와 맞지 않는 패킷을 무시하지만, 프로미스큐어스 모드가 활성화된 시스템은 MAC 주소에 상관없이 패킷을 받아들여 응답할 수 있습니다
    - **./sentinel–t 211.47.65.4 –f 1.1.1.1 –d –a - :** `–d –a –e` 옵션을 모두 사용하면 **DNS, ARP, Etherping 세 가지 테스트를 동시에 수행**
- 시스코 라우터에서 cpu 평균 사용률 보기 위해 show precess실행하고, 라우터 인터페이스 하드웨어 정보를 보기 위해 show controllers로 조회하고, 메모리 용량, 사용량 등을 확인하기 위해 show memory함
- Developed Kiddie 해커
    - 해킹 수행 코드가 적용될 수 있는 취약점을 발견할 때까지 여러 번 시도하여 시스템 침투에 성공할 수 있는 능력이 있다.
    - 새로운 취약점을 직접 발견하거나 최근 발견된 취약점을 주어진 상황에 맞게 수정해서 활용할 만한 실력은 없다
- **SNMP 커뮤니티 스트링**
    - SNMP 커뮤니티 스트링(Community String)은 SNMP에서 네트워크 장비(Agent)와 관리 시스템(Manager) 간의 통신 인증을 위해 사용하는 일종의 비밀번호 역할을 하는 문자열입니다

    - 관리 시스템이 네트워크 장비에 접근해서 정보를 요청하거나 설정을 변경할 때, 양쪽에서 동일한 커뮤니티 스트링을 사용해야만 정상적인 통신이 이루어집니다. 만약 커뮤니티 스트링이 다르면 장비는 요청을 거부
    - SNMP 커뮤니티 스트링은 기본적으로 public(읽기), private(쓰기)로 설정
    - **모든 서버 및 클라이언트에서 동일한 커뮤니티 스트링을 사용해야만 한다.**
    - **MIB 정보를 주고 받기 위하여 커뮤니티 스트링을 사용**
    - 커뮤니티 스트링 변경은 시스템 설정 파일(예: `/etc/snmp/snmpd.conf`)을 수정해야 하며, 이 파일 수정에는 일반적으로 관리자(root) 권한이 필요
    - SNMP(Simple Network Management Protocol)는 **네트워크 장비(서버, 라우터, 스위치 등)를 효율적으로 관리하고 모니터링하기 위한 표준 프로토콜**
    - TCP/IP 기반 네트워크에서 네트워크 장치로부터 정보를 수집하거나, 원격으로 장치의 설정을 변경할 수 있도록 설계되었으며, 주로 **UDP 포트 161을 사용**
- ids에서 이상 탐지 방법
    - **예측 가능한 패턴 생성 : 정상적인 네트워크/시스템 활동의 패턴을 학습하여 미래의 동작을 예측**
    - **통계적 접근법 : 통계적 모델을 기반으로 과거 경험적인 자료를 토대로 처리, 행동에 대한 프로파일을 생성데이터의 분포를 분석하여 정상 범위를 벗어난 값을 이상으로 판단**
- 다익스트라(Dijkstra) 알고리즘을 사용하는 라우팅 프로토콜
    - 다익스트라 알고리즘은 **링크상태(Link-State) 알고리즘**에 속하며, **OSPF**에서 사용된다.
    - **대규모 망에 적합한 알고리즘이**
    - 오답
        - **커리벡터 알고리즘**은 **거리-벡터(Distance-Vector) 알고리즘**(예: RIP)을 의미합니다.
        - 거리-벡터 알고리즘은 이웃 라우터와의 거리(홉 수)를 기반으로 경로를 계산하며, 벨만-포드(Bellman-Ford) 알고리즘을 사용합니다.
        - **링크상태 알고리즘**은 전체 네트워크 토폴로지 맵을 구성한 후 다익스트라 알고리즘으로 최단 경로를 계산합니다.
- 모바일 가상화(Hypervisors
    - BYOD(Bring Your Own Device)의 보안 기술 중 모바일 기기 보안 기술

- IPSec(Internet Protocol Security)의 SA(Security Association) 매개변수
  - ipsec이란 **네트워크 계층(IP 계층)에서 IP 패킷을 보호하기 위한 표준 보안 프로토콜 모음**
  - **AH Information**: 인증 헤더(Authentication Header) 관련 정보
    - 헤더에는 무결성, 인증을 위한 데이터가 포함되지 않는다.
    - ah가 적용되어 sa(security association)를 식별할 수 있다.
  - **IPSec Protocol Mode**: 전송(Transport) 모드 또는 터널(Tunnel) 모드 등 IPSec 동작 모드
  - **Sequence Number Counter**: 패킷 순서 번호 카운터
- 해킹도구
  - **넷버스(Netbus) , 백오리피스, 스쿨버스 :원격 제어 및 침해를 위한 트로이목마**
  - **키로그23(Keylog23) : 사용자의 키보드 입력을 몰래 기록해 아이디, 비밀번호 등 민감 정보를 탈취하는 악성 소프트웨어**
- **RFID 보안 기술에서 암호 기술을 사용하는 보호대책**
  - **XOR(Exclusive OR) 기반 원타임 패드 기법 : 데이터를 암호화하여 저장 및 전송하는 데 사용되는 암호 기술로, XOR 연산과 원타임 패드(일회용 키)를 결합해 데이터를 보호**
- nmap
  - TCP/IP 프로토콜 표준이 명시하지 않은 패킷 처리 기능의 운영체제별 구현 : map의 OS 탐지는 TCP/IP 스택 핑거프린팅을 기반으로 하며, 운영체제마다 TCP/IP 프로토콜 구현에서 차이가 나는 부분을 활용해 다양한 테스트 패킷을 보내고, 그 응답 패턴을 분석하여 운영체제를 식별
  - 즉, 표준이 명확히 정의하지 않은 부분이나 구현에 따라 다를 수 있는 동작을 활용하는 것이 Nmap OS 탐지의 핵심
- **MRTG(MultiRouter Traffic Grapher) - 트래픽을 분석**
  - 필요한 것 : **C Compiler, perl, gd library**
- **Libpcap : 네트워크 패킷 캡처 도구(예: tcpdump, wireshark)에 쓰인다.**
- nac(**네트워크 접근 제어, Network Access Control) 보안시스템)**
  - 조직의 네트워크에 접속하려는 사용자와 장치(엔드포인트)를 식별하고, 사전에 정의된 보안 정책에 따라 네트워크 접근을 허용하거나 차단하는 보안 솔루션

    - 인증, 인가, 감사, 모니터링, 제어, 신원확인, 정책준수 검사
    - 일반적으로 mac주소를 기반으로 수행
- smtp.rez.command==’EHLO’
    - 이메일 서비스 확장 지원 세션을 시작하는 명령어로 필터하기 위한 것
    - 순서 : EHLO＞AUTH＞RCPT＞MAIL＞DATA＞QUIT
- 리버싱 도구
    - 리버싱(Reverse Engineering)은 소프트웨어나 하드웨어의 구조, 기능, 동작 원리를 역으로 분석하여 설계 의도나 구현 방식을 이해하는 기술
    - Procexp (Process Explorer) : 시스템에서 실행 중인 프로세스와 관련된
    - OllyDbg - 디버깅 시 프로그램의 실행을 단계별로 추적,
- **ARP 스푸핑(Spoofing) 방지방법**
    - **arp –s [ip주소] [mac 주소] 명령을 통해 ARP 테이블을 관리한다.** → 이 명령은 사용자가 직접 ARP 테이블에 IP와 MAC 주소의 매핑을 '정적(static)'으로 추가하는 방법입니다. ARP 스푸핑 방지 방법 중 하나로, 중요한 서버나 장비에 대해 정적 ARP 엔트리를 등록해 공격을 예방할 수 있습니다
        - 원래 ARP 테이블은 기본적으로 정적으로 관리된다.
    - 이너넷 환경에서 공객대상자의 캐시 테이블에 공격자가 원하는 ip에 대한 mac주소 쌍을 업데이트해서 공격대상자의 패킷 흐름을 공자가 원하는 방향으로 조절해서 공격
- 포트 미러링 : tcpdump를 사용한 패킷 스니핑에서 동일 세그먼트 내 패킷을 복제하여 정보를 수집할때를 말한다.
- **정찰공격(reconnaissance attack) 도구**
    - **핑 스윕(Ping sweep) :** 네트워크 내 활성화된 호스트를 식별하기 위한 정찰(정보수집) 도구입니다. ICMP 패킷을 여러 IP에 보내 응답하는 시스템을 찾습니다
    - **포트 스캔(Port scan) :** 대상 시스템의 열린 포트를 탐색하여 어떤 서비스가 운영 중인지 확인하는 대표적인 정찰 도구입니다
    - **패킷 스니퍼(Packet sniffer) :** 네트워크 상의 패킷을 수집·분석하여 시스템 및 서비스 정보를 수집하는 정찰(정보수집) 도구입니다. 패시브(수동) 정찰에 주로 사용
    - **오답 : 포트 리다이렉션(Port redirection) :** 이는 정찰이 아니라, 이미 침투한 시스템에서 공격자가 다른 시스템으로 트래픽을 우회하거나 내부망으로 이동(pivoting)

할 때 사용하는 공격 기법입니다. 즉, 정보수집(정찰)이 아니라 공격·침투 단계에서 활용

- **VLAN 오/남용을 경감시키기 위한 방법**
  - **모든 포트에 동적 트렁킹 프로토콜(DTP)을 꺼 놓는다.**
  - 신뢰할 수 없는 장치가 트렁크 포트에 연결되면 VLAN 호핑 공격 가능하기때문에 신뢰불가 네트워크는 vlan에 붙이지 않는다
  - native vlan에는 접근제한을 둬서 경감시킨다
  - 오답 : VMPS 사용. 이건 동적 VLAN 할당을 위한 도구로 위험성 증가
- 서비스별 포트
  - | 138 | NetBIOS 데이터그램 서비스 | UDP |
    | 139 | NetBIOS 세션 서비스 | TCP |
    | 110 | POP3 | TCP |
    | 143 | IMAP | TCP |
- trojan : 악의적인 프로그램을 건전한것처럼 속여서, 실행시키고, 특정 포트를 열어서 공격자 침입을 돕고, 정보를 유출하고 자신을 숨긴다.
- Enhanced Open
  - Wi-Fi Alliance가 정의한 무선 LAN 보안 규격입니다.
  - 패스프레이즈와 같은 인증없이 단말과 액세스 포인트간의 무선 통신을 암호화하는 방식을 제공합니다.
- BLP) 모델과 비바(Biba) 모델의 비교
  - **공통점**
    - **강제적 접근통제(MAC)** 기반
    - **등급(Label) 시스템** 사용 (BLP: 보안 등급, Biba: 무결성 등급)
    - **수학적 검증**을 거친 최초의 모델
  - 차이점

비교 항목	BLP 모델 (Bell-LaPadula)	Biba 모델 (Biba Integrity)
주요 목표	**기밀성** (정보 유출 방지)	**무결성** (정보 변조 방지)
핵심 규칙	- No Read Up (상향 읽기 금지)- No Write Down (하향 쓰기 금지)	- No Write Up (상향 쓰기 금지)- No Read Down (하향 읽기 금지)

정보 흐름	정보가 **높은 등급 → 낮은 등급**으로 흐르는 것 차단	정보가 **낮은 등급 → 높은 등급**으로 흐르는 것 차단
주요 적용 분야	군사·정부 기밀 문서 관리	금융·의료 데이터 등 무결성이 중요한 시스템
대표적 문제점	무결성 보장 불가 (Blind Write 가능)	기밀성 보장 불가

- **find / -perm -4000**
  - **퍼미션 중에 SetUID 비트(4000)가 설정된 파일**
  - SetUID는 파일 실행 시 소유자의 권한으로 동작하게 하는 특수 권한
- **-perm +4000**
  - 파일의 권한 중 **4000 비트(SetUID)가 하나라도 포함**된 파일을 찾습니다.
  - `-perm +6000` 은 SetUID(4000) 또는 SetGID(2000) 중 하나라도 있으면 포함

어플리케이션 보안

- SOAR
  - (Security Orchestration, Automation, and Response)은 보안 오케스트레이션, 자동화, 대응을 의미하는 보안 기술로, 보안 운영팀이 다양한 보안 도구와 시스템을 하나의 중앙 플랫폼에서 통합·연동하고, 반복적인 작업을 자동화하며, 보안 인시던트에 신속하게 대응할 수 있도록 지원하는 **솔루션(플랫폼)**
  - 수집된 로그 및 이벤트를 바탕으로 위협 인텔리전스와 능동적 탐지를 통해 침해정보와 영향도 도출하고 개선하기 위해 시스템 변경을 자동화한다.
  - SOA, SIRP, TIP을 폭넓게 포함하는 개념
- SIEM
  - (Security Information and Event Management, 보안 정보 및 이벤트 관리)은 조직의 IT 인프라 전반에서 발생하는 다양한 로그와 이벤트 데이터를 **중앙에서 수집·통합·분석**하여, 보안 위협을 실시간으로 탐지하고 대응할 수 있도록 지원하는 보안 **솔루션**
  - 이벤트 간의 상관관계 분석을 통해 복합적인 공격 시나리오를 식별하고, 신속한 사고 대응과 포렌식
- SET 대칭키 암호화 방식
  - 송수신간 비밀키 교환을 하는 방식

    - A가 B에게 비밀키와 B의 공개키를 기반으로 만든 전자봉투를 생성해서 전송
- CSRF(Cross-Site Request Forgery, 사이트 간 요청 위조)
    - 웹 보안 취약점 중 하나로, 공격자가 사용자의 **인증 정보를 악용해** 사용자가 의도하지 않은 요청을 특정 웹사이트에 보내도록 **유도**하는 공격 방식.
    - 즉, 사용자가 로그인된 상태에서 공격자가 만든 악성 사이트나 이메일 링크를 클릭하면, 사용자의 권한으로 원치 않는 작업(예: 송금, 비밀번호 변경 등)이 실행될 수 있다.
    - 이 공격은 웹 애플리케이션이 요청이 실제 사용자에 의해 발생했는지 제대로 검증하지 않을 때 발생합니다. 대표적인 **방어 방법**으로는 CSRF 토큰 사용, Referrer 검증, CAPTCHA 적용 등이 있습니다
- XSS(크로스 사이트 스크립팅, Cross-Site Scripting)
    - 웹 애플리케이션의 취약점을 이용해 공격자가 악의적인 스크립트(주로 자바스크립트)를 웹사이트에 삽입하고, 이를 방문한 사용자의 브라우저에서 실행되도록 하는 공격.
    - 이로 인해 공격자는 사용자의 세션 쿠키, 개인정보 등 민감한 정보를 탈취하거나, 사용자의 권한으로 악의적인 행동을 수행할 수 있습니다
- **디지털 포렌식 5대 원칙**
    - **1. 정당성의 원칙 :** 증거는 반드시 적법한 절차에 따라 수집되어야 하며, 위법하게 수집된 증거는 법적 효력을 인정받지 못합니다. 이를 '위법수집증거배제법칙'이라 하며, 위법 증거를 통해 얻어진 2차 증거도 증거능력이 부정됩니다(독수독과 이론)
    - **2. 무결성의 원칙 :** 수집된 디지털 증거는 어떠한 변조나 손상 없이 원본 상태를 유지해야 하며, 이를 입증하기 위해 해시(Hash) 값을 활용합니다. 수집 시점과 법정 제출 시점의 해시값이 일치하면 무결성이 보장된 것으로 인정됩니다
    - **3. 재현의 원칙 :** 동일한 조건과 환경에서 동일한 분석 과정을 반복했을 때 항상 같은 결과가 나와야 합니다. 이는 증거의 신뢰성과 객관성을 확보하기 위한 원칙입니다
    - **4. 신속성의 원칙:** 디지털 증거는 휘발성 특성(시간 경과에 따라 쉽게 손실되는 정보)이 있으므로, 증거 수집과 분석 절차를 지체 없이 신속하게 진행해야 합니다
    - **5. 절차 연속성의 원칙 (연계 보관성의 원칙) :**증거의 획득부터 이송, 분석, 보관, 법정 제출에 이르기까지 모든 단계에서 담당자와 책임자를 명확히 하고, 증거가 손상되지 않도록 체계적으로 관리해야 합니다. 이를 통해 증거의 신뢰성을 유지합니다
- white box testing

    - 개발된 소스 코드를 살펴보고 코드 취약점을 찾는 방식
- dnskey, rrsig, nsec/nsec3 : dnssec의 전자서명과 서명검증 절차를 지원하기 위해 추가한 신규 리소스 레코드와 관련된 것
- dnssec(Domain Name System Security Extensions)
    - 인터넷에서 도메인 이름을 IP 주소로 바꿔주는 기술입니다. 기존의 DNS는 보안 기능이 부족해 공격자가 DNS 데이터를 위조하거나 변조할 수 있는데, DNSSEC는 이런 "데이터 위조·변조 공격"을 막기 위해 만들어졌습니다
    - DNSSEC는 DNS 스푸핑(위조)이나 캐시 포이즈닝(잘못된 정보로 DNS 서버를 속이는 공격) 같은 위협을 효과적으로 방어합니다. 하지만 피싱이나 DDoS 공격 등에는 직접적인 방어 효과가 없습니다
    - DNSSEC의 핵심은 DNS 응답 데이터에 전자서명(디지털 서명)을 추가하는 것. 이 서명은 **공개키** 암호화 방식을 사용해 생성되며, 사용자는 DNS 응답이 실제로 해당 도메인 소유자가 보낸 것인지, 중간에 변조되지 않았는지 검증할 수 있습니다. 즉, 사용자가 접속하려는 웹사이트의 IP 주소 정보가 신뢰할 수 있는지 확인해주는 역할을 합니다.
    - dnssec이 받을 수 있는 공격 유형 : 파밍, 피싱, ddos 공격
        - 웜바이러스에 의한 hosts 파일 안의 정보 변조 (x) —> 틀린값
- 파밍(Pharming)
    - 사용자가 정상적인 웹사이트에 접속하려고 할 때, **DNS(Domain Name System) 등의 취약점을 악용하거나 악성코드를 이용해** 사용자를 가짜(사기) 웹사이트로 자동 리디렉션시켜 **개인정보, 금융정보 등 민감한 정보를 탈취하는 사이버 공격**입니다
    - **악성코드 감염**: 사용자의 컴퓨터에 악성코드를 설치해 호스트 파일을 변조, 사용자가 정상 주소를 입력해도 가짜 사이트로 이동하게 만듭니다
    - **DNS 변조(DNS 포이즈닝)**: DNS 서버의 정보 자체를 조작해, 다수의 사용자가 특정 도메인에 접속할 때 공격자가 만든 가짜 사이트로 이동하도록 합니다
    - 파밍은 피싱과 달리, 사용자가 정상적인 URL을 직접 입력해도 공격자가 만든 가짜 사이트로 이동할 수 있어 **피해자가 인지하기 어렵고, 대규모 피해로 이어질 수 있습니다**
- 공개키(비대칭키) vs 대칭키
    - 공개키 알고리즘으로 암호화에 사용하는 키는 **수신자의 공개키**이고, 서명검증에 사용하는 키는 **송신자의 공개키**이다
    - 대칭키(블록암호)

        - **암호화와 복호화에 동일한 키를 사용**합니다.
        - 즉, 데이터를 암호화할 때 쓴 키와, 암호화된 데이터를 다시 원래대로 복호화할 때 쓰는 키가 같습니다
        - 이 키는 송신자와 수신자 모두가 알아야 하므로, 안전하게 키를 서로 전달하는 것이 매우 중요합니다.
        - 대칭키 배송문제 해결 방법 (**대칭키 암호 방식에서 송신자와 수신자가 동일한 비밀키를 안전하게 공유해야 하는데, 이 비밀키를 안전하게 전달(배송)하는 과정에서 발생하는 보안상의 문제)**
            - diffie-hellman 키 교환방법에 의한 해결
            - 키 분배 센터에 의한 해결
            - 공개키 암호에 의한 해결
            - 오답: 전자서명 (이건 비대칭키 기술로 주로 무결성과 신원인증에 관한 기능)
        - 블록암호(Block Cipher)는 **일반적으로 대칭키 암호화 방식**을 의미합니다.
            - 블록암호란, 평문을 고정된 길이의 블록 단위로 나누어 각 블록을 **같은 키(대칭키)**로 암호화하는 알고리즘. 암호화와 복호화에 동일한 키 사용
            - 대표적인 블록암호로는 **AES, DES, SEED, ARIA** 등
            - 블록암호 = 대칭키인 이유
                - 공개키(비대칭키) 암호화 방식은 보통 블록 단위로 동작하지 않고, 키 교환, 전자서명, 소규모 데이터 암호화에 사용됩니다.
        - 장점: 암호화·복호화 속도가 빠르고, 구현이 쉽습니다.
        - 단점: 키를 안전하게 공유(키 교환)하는 것이 어렵고, 사용자가 많아질수록 관리해야 할 키의 수가 기하급수적으로 늘어납니다
        - **예시**: AES(고급 데이터 암호화 기법), DES, SEED, ARIA 등
    - 비대칭키
        - **암호화와 복호화에 서로 다른 키(쌍으로 된 공개키와 개인키)를 사용**합니다
        - 공개키는 누구나 알 수 있도록 공개하고, 개인키는 본인만 보관합니다.
        - 데이터를 암호화할 때는 상대방의 공개키를 사용하고, 복호화할 때는 상대방만 가진 개인키를 사용합니다.
        - 부인방지 및 인증지원

        - 키를 미리 안전하게 교환할 필요가 없으므로, 대칭키 방식의 키 교환 문제를 해결할 수 있습니다.
        - 장점: 키 분배가 쉽고, 인증·전자서명 등 다양한 보안 기능을 지원합니다.
        - 단점: 암호화·복호화 속도가 느리고, 연산이 복잡합니다
        - **예시**: RSA, ECC, Diffie-Hellman, ElGamal(타원곡선 암호 적용) 등
- 공개키 암호화 방식
    - 두 개의 **정수** P, q를 선택하여 n= **p x q** 를 계산한다. 이때, P, q를 알고 있는 사람은 n을 계 산하기 쉽지만, n만 알고 있는 사람은 n으로부터 p, q를 찾는 것은 어렵다. 이를 **소인수분해 문제**라고 한다. 이에 기반한 대표적인 공개키 암호 알고리즘은 **RSA, Robin암호**이다.
    - RSA 공개키 암호를 이용하여 송신자(A) 와 수신자(B) 간에 비밀 세션키를 공유하는 키분배 방식을 지원하고 있다. 이때, 송신자(A)가 수 신자(B)에게 전달하는 **세션키를** 암호화할 때 필요로 하는 키 정보는 **수신자(b)의 공개키**가 된다,
- **공개키 기반구조(PKI)와 인증서**
    - 구성요소
        - ca, ra, 공개키 인증서의 소유자
    - 인증서는 사용자의 공개키에 대해 인증기관이 인증해 주는 전자문서
    - 인증서는 **공개키만 포함**하며, 개인키는 절대 포함되지 않습니다
    - 공개키는 평문으로 저장되며, 인증기관(CA)의 전자서명으로 보호됩니다
    - 개인키는 사용자(또는 장치)가 별도로 보관하며, 인증서와 분리되어 관리됩니다
        - 개인키가 유출되면 인증서의 신뢰성이 완전히 무너지므로, 인증서 내에 포함되지 않습니다
        - CA도 개인키를 알 수 없으며, 사용자만이 생성하고 관리
- FTP
    - 디폴트는 **active** 모드이며, passive 모드로의 변경은 FTP **클라이언트가** 결정한다.
    - passive 모드
        - 서버에서 클라이언트를 접속해야하는 모순을 해결하기 위해 고안된 방식
        - 보안을 위해 서버에서는 passive 모드로 사용할 포트를 제한한다.
        - 제어 전송은 21번 포트

        - 클라이언트가 서버의 21번 포트(명령 채널)로 접속합니다.
    - FTP 클라이언트가 서버에 접속할 때 데이터 전송을 위한 연결 방향을 바꿔, 방화벽이나 NAT 환경에서 발생하는 연결 문제를 해결하기 위해 사용되는 방식
    - 서버는 데이터 전송을 위해 사용할 임의의 포트 번호(보통 1024번 이상의 비특권 포트)를 클라이언트에게 알려줍니다.
    - 클라이언트는 서버가 알려준 해당 포트로 직접 접속해 데이터 전송 채널을 엽니다.
    - 이후 이 데이터 채널을 통해 파일 전송 등 데이터가 오갑니다
    - 데이터 채널 연결이 "클라이언트 → 서버" 방향으로 이뤄집니다.
    - 클라이언트 측 방화벽이나 NAT 환경에서도 별도의 추가 설정 없이 파일 전송이 가능합니다.
    - 서버는 데이터 전송용 포트(1024~65535 중 임의)를 열어야 하므로, 서버 방화벽에서 해당 포트 범위를 허용해야 합니다
    - Active 모드와 달리 서버가 클라이언트로 직접 접속하지 않기 때문에, 클라이언트 보안 환경에서 더 유리합니다.
    - 정리 : Passive 모드는 클라이언트가 서버에 명령 채널(21번 포트)로 접속한 뒤, 서버가 지정한 데이터 포트로 클라이언트가 다시 접속해 데이터 채널을 여는 방식입니다. 이로 인해 클라이언트가 방화벽이나 NAT 뒤에 있어도 FTP 파일 전송이 원활하게 동작합니다
- ftp 바운스 공격
    - ftp 서버가 데이터를 데이터 포트 20번으로 전송할때 목적지가 어딘지 검사하지 않는 취약점 공격하는 유형으로 익명ftp서버를 이용해서 공격자가 port명령을 조적해서 피해서버의 네트워크 및 포트스캔, 데이터 전송등이 가능하며, 방화벽 내부에 ftp서버가 있으면 방화벽 패킷필터링을 무시하고 여러 공격이 가능하다.
- tftp(Trivial File Transfer Protocol)
    - 네트워크 상에서 간단하게 파일을 전송하기 위해 설계된 매우 단순한 파일 전송 프로토콜입니다. FTP보다 기능이 훨씬 제한적이며, 주로 임베디드 시스템, 네트워크 장비의 펌웨어 업로드, 네트워크 부팅 등 복잡한 인증이나 고급 기능이 필요 없는 환경에서 사용됩니다
    - TFTP는 매우 단순하고 가벼운 파일 전송 프로토콜로, 인증이나 보안이 필요 없는 환경에서 빠르게 파일을 주고받을 때 유용합니다. 하지만 보안 기능이 없으므로 외부망이나 중요한 데이터 전송에는 적합하지 않습니다

        - **주요 특징**
            - **UDP 기반**: TFTP는 전송 계층에서 UDP(포트 69)를 사용. TCP 기반의 FTP보다 전송이 빠르지만, 신뢰성(재전송, 흐름제어 등)은 UDP에 의존하기 때문에 데이터 손실에 취약
            - **비연결형**: 클라이언트와 서버 간에 영구적인 연결을 유지하지 않고, 각 파일 전송이 독립적으로 진행
            - **간단한 구조**: 디렉터리 목록 조회, 사용자 인증, 암호화 등 부가 기능이 없습니다. 오직 파일 읽기/쓰기만 지원합니다
            - **작은 규모**: 구현이 간단하고, 메모리 요구량이 적어 임베디드 시스템이나 부트로더 등 리소스가 제한된 환경에 적합
            - **보안 취약**: 인증이나 암호화 기능이 없어 보안에 취약. 민감한 데이터 전송에는 부적합하며, 신뢰할 수 있는 내부망에서만 사용하는 것이 권장
        - **동작 방식**
            - 클라이언트가 서버에 파일 읽기(**RRQ**) 또는 쓰기(**WRQ**) 요청 →
            - 서버는 요청을 수락하면 데이터(DATA) 패킷을 전송하고, 클라이언트는 각 데이터 블록마다 확인 응답(ACK)을 보냅니다.
                - ack메시지는 클라이언트와 서버 모두 사용한다.
            - 데이터 블록 크기는 일반적으로 **512**바이트이며, 마지막 블록이 512바이트보다 작으면 전송이 종료
                - 데이터 메시지는 클라이언트와 서버 모두 사용한다.
            - 오류 발생 시 ERROR 메시지가 전송됩니다.
        - **주요 사용 사례**
            - 네트워크 장비(스위치, 라우터 등) 펌웨어 업로드
            - 임베디드 시스템의 운영체제 이미지 다운로드
            - 네트워크 부팅(예: PXE 부팅) 시 부트 이미지 전송
- HTTP
    - cache-control : 특정 웹 리소스의 캐싱이 되지 않게 하며, 악용되어 사용될 경우 서버에 부하가 발생하는 공격으로 사용가능
- SET
    - 이중 서명

        - set에서 도입된 기술로 상점이 카드 사용자의 계좌번호와 같은 정보를 알수 없고 은행도 사용자가 상점에서 물건을 샀는지를 알수 없게 하지만, 결제대금만큼은 정확하게 보증하는 방법
    - 전자상거래 송신측 암호화 절차
        - 송신자 메시지 압축 → 송신자의 **개인키**로 암호화 → 전자서명 생성
        - 원문메시지에 전자서명 첨부해서 **대칭키**로 암호화
        - **대칭키**를 다시 수신자의 **rsa공개키**로 암호화 한후 암호문과 함께 전송
- dns
    - 구성요소
        - **도메인 네임 스페이스(Domain Name Space) :** DNS가 저장·관리하는 계층적 구조로, 도메인 이름을 트리 형태로 조직화하여 각 도메인과 그 하위 도메인 정보를 계층적으로 관리합니다. 이 구조 덕분에 전 세계적으로 분산된 환경에서도 효율적으로 도메인 정보를 찾을 수 있습니다
        - **네임 서버(Name Server) :** 도메인 이름과 IP 주소를 매핑하는 정보를 실제로 저장하고 관리하는 서버입니다. 사용자가 요청한 도메인 이름에 대한 IP 주소 정보를 찾아 리졸버(Resolver)에게 전달하는 역할을 합니다. 네임 서버는 루트 네임 서버, TLD(최상위 도메인) 서버, 권한 있는 네임 서버 등 여러 종류가 있습니다
        - **리졸버(Resolver) :** 사용자의 요청을 받아 적절한 네임 서버에 질의하고, 그 결과(도메인 이름에 해당하는 IP 주소)를 사용자에게 반환하는 역할을 합니다. 일반적으로 PC나 스마트폰 등에서 DNS 요청을 보내는 클라이언트 프로그램 또는 운영체제의 일부
    - 공격유형
        - dns하이재킹 : 해커가 dns 서버를 해킹하거나 패킷 조작해서 특정 도메인에 대응하는 ip주소를 해커가 원하는 ip주소로 위조하는 기법
- otp
    - otp는 7계층 중 **응용 계층에서** 사용된다.(mime, pgp도 동일)
    - 이론적으로 전수공격(Brute Force Attack)에 가장 강한 암호기법
        - 전수공격(Brute Force Attack) : 무차별 대입 공격은 암호, 비밀번호, 암호화 키 등과 같이 보호된 정보를 알아내기 위해 가능한 모든 조합을 체계적으로 시도하는 해킹 기법입니다. 공격자는 자동화된 도구를 사용해 모든 가능한 문자, 숫자, 기호의 조합을 입력해 정답을 찾을 때까지 반복적으로 시도합니다

    - 질의/응답 방식으로 생성된다. : 사용자가 OTP 인증 요청 시 인증서버로부터 받은 질의값을 직접 OTP 토큰에 입력하 여 응답값(난수 형태)을 생성한다.
    - OTP 토큰과 인증서버 간에 동기화해야 할 기준 정보가 없기 때문에, 동기화할 필요가 없다.
    - 사용자와 서버 간에 상호 인증을 제공하는 방식으로 쉽게 확장이 가능하다.
    - 인증서버도 해당 사용자의 질의값을 관리해야 하는 부담이 있다.
- db암호화 방식
    - **API 방식 :**애플리케이션 서버에서 암·복호화를 수행하는 방식입니다. 응용프로그램이 암호화 모듈(API)을 호출해 데이터를 암호화한 뒤 DB에 저장합
        - 장점: DB 서버에 부하가 적고, 성능 저하가 적음
        - 단점: 애플리케이션 수정이 필요하며, DB 내부 연산에서 암호화된 데이터 처리에 한계가 있음
    - **플러그인(Plug-in) 방식**
        - DBMS에 암·복호화 모듈을 플러그인 형태로 설치해 DB 서버에서 암호화를 처리합니다.
        - 장점: 애플리케이션 수정이 최소화됨
        - 단점: DB 서버 부하가 증가할 수 있고, 대용량 처리 시 성능 저하가 발생할 수 있음
    - **인플레이스(In-place) 방식**
        - DB 엔진 내부에서 암·복호화 기능을 수행하는 방식으로, 플러그인 방식보다 더 깊이 통합되어 있습니다.
        - 장점: 완전한 독립성, 빠른 암호화 성능
        - 단점: DB 보안 기능 추가 시 별도 패키지 필요
    - **하이브리드(Hybrid) 방식**
        - API와 플러그인 방식을 혼합해, 성능과 보안 요구에 따라 유동적으로 적용하는 방식입니다.
        - 장점: 환경에 따라 적합한 방식을 선택해 적용 가능
        - 단점: 구축이 복잡할 수 있음
    - **TDE(Transparent Data Encryption) 방식**
        - DBMS 자체 기능을 이용해 데이터 파일 저장 시 암호화를 수행합니다.

        - 장점: 애플리케이션 수정이 불필요하고, DBMS 엔진에 최적화
        - 단점: 지원되는 DBMS에 한정됨
    - **파일 암호화 방식**
        - 운영체제 수준에서 DB 파일 전체를 암호화하는 방식입니다.
        - 장점: 비정형 데이터도 암호화 가능, 애플리케이션 수정 불필요
        - 단점: OS 의존성이 크고, 서버 부하가 발생할 수 있음
    - 어플리케이션 수정없이 사용될 수 있는 유형 : tde방식-파일암호화
- pgp(Pretty Good Privacy)
    - 전자우편 보안 시스템으로
    - 제공 기능
        - **기밀성(Confidentiality)**

          메시지를 암호화하여 네트워크를 통해 전송되는 전자우편의 내용을 외부에서 볼 수 없도록 보호. **대칭키(세션키)** 암호화 방식을 사용해 메시지를 암호화하고, 이 대칭키는 수신자의 공개키로 암호화
        - **무결성(Integrity)**

          메시지에 해시 함수를 적용해 메시지가 전송 중에 변경되거나 위조되지 않았음을 확인할 수 있습니다. 주로 MD5, SHA와 같은 **해시 알고리즘**을 사용합니다
        - **인증(Authentication) = 전자서명**

          디지털 서명을 통해 메시지의 송신자가 누구인지를 확인할 수 있습니다. 송신자가 자신의 개인키로 메시지 해시값을 암호화해 서명하고, 수신자는 송신자의 **공개키로** 이를 검증합니다
        - **부인방지(Non-repudiation)**

          송신자가 메시지를 보냈다는 사실을 부인할 수 없도록 보장합니다. 디지털 서명 기능을 통해 송신자가 메시지를 보냈음을 증명할 수 있습니다. (수신 부인방지는 아님. 헷갈리지 말것)
        - **압축(Compression)**

          메시지를 암호화 또는 서명한 후 압축하여 전송함으로써, 전송 효율을 높이고 추가적인 보안 효과도 얻을 수 있습니
        - **전자우편 호환성(E-mail compatibility)**

바이너리 데이터를 ASCII 코드로 변환하는 Radix-64 인코딩을 사용해 다양한 이메일 시스템과 호환되도록 지원합니다

- **키 관리 및 분산 인증**

  PGP는 중앙집중식 인증기관(PKI) 대신 **'Web of Trust'라는 분산된 키 인증 방식**을 사용합니다. 사용자는 서로의 공개키에 서명하여 신뢰를 확장합니다

- 단편화
  - 전자우편 시스템은 한 번에 전송할 수 있는 메시지 크기에 제한(예: 약 50KB)이 있습니다. PGP는 이 제한을 넘는 큰 메시지를 여러 개의 작은 블록으로 나누어(단편화하여) 전송
- 재조립
  - 수신자는 여러 개의 블록으로 나누어져 도착한 메시지를 원래의 하나의 메시지로 다시 합칩니다

- 인터넷 메일 구조

메일 사용자 에이전트	Mail User Agent (MUA)	사용자가 메일을 작성, 송신, 수신, 읽기, 관리하는 클라이언트(예: 아웃룩, Gmail
메일 제출 에이전트	Mail Submission Agent (MSA)	MUA가 작성한 메일을 받아, 올바른 형식과 인증을 확인한 뒤 MTA에 전달
메일 전송 에이전트	Mail Transfer Agent (MTA)	메일을 인터넷 상에서 다른 메일 서버로 송수신, 라우팅 및 중계. 메시지가 목적지 mda에 도달할때까지 중계역할한다.
메일 배달 에이전트	Mail Delivery Agent (MDA)	MTA가 받은 메일을 최종적으로 수신자의 메일박스에 저장. 메시지를 mhs에서 ms로 메시지 전달

- 웹 방화벽(WAF, Web Application Firewall)의 주요기능
  - 파일업로드 제어 및 검사 기능
  - http공격 패킷 탐지 및 차단
  - 웹서버 오류 필터링 및 기밀 정보 유출차단
  - ip주소와 포트기반 패킷탐지 및 차단 → 이건 **네트워크 방화벽** 기능 아님. 오답. 이유는 WAF의 보호 범위와 동작 계층이 네트워크 방화벽과 다르기 때문
    - WAF는 OSI 7계층 중 **응용 계층(7계층)**에서 동작하며, 주로 HTTP/HTTPS 트래픽을 분석하고 웹 애플리케이션에 대한 공격(예: SQL 인젝션, XSS 등)을 탐지·차단합니다. 반면, 네트워크 방화벽은 **3계층(네트워크**

계층, IP 주소) 및 **4계층(전송 계층, 포트 번호)**에서 동작하며, IP 주소, 포트, 프로토콜 등 네트워크 패킷 정보를 기반으로 접근을 제어

- XML 기반의 보안 기술
  - XML signature : 무결성 및 부인방지 기능
  - xkms : pki 서비스 기능
  - xacml : 접근 제어기능
  - SAML :**인증(Authentication)과 권한부여(Authorization) 정보를 안전하게 교환**하는 데 사용됩니다.
    - **싱글사인온(SSO)** 지원: 한 번의 인증으로 여러 서비스에 접근 가능하게 함
    - **인증 및 권한 정보 전달**: IdP(Identity Provider)와 SP(Service Provider) 간에 사용자의 인증 및 권한 정보를 안전하게 주고받음
    - **무결성, 인증, 부인방지** 등 보안성 강화
- WPKI
  - (Wireless Public Key Infrastructure)는 **무선 인터넷 환경**에서 안전한 인증과 통신을 가능하게 해주는 **무선 공개키 기반 구조**입니다. 쉽게 말해, 스마트폰이나 **무선 단말기**에서 인터넷 뱅킹, 모바일 결제, 주식 거래 등 중요한 서비스를 사용할 때 외부 침입이나 정보 유출로부터 사용자를 보호하는 보안 시스템
  - **무선 환경에 최적화**

    기존의 PKI(공개키 기반 구조)를 **무선 기기**의 작은 메모리, 낮은 CPU 성능, 제한된 네트워크 환경에 맞게 경량화하여 적용한 구조입니다.
  - 구성요소
    - ca (인증기관) : 인증서 발급 및 **폐지**
      - 인증서 폐지 목록 저장 : CA는 인증서가 폐지(해지)될 때마다 해당 정보를 CRL에 기록하고, 이 목록을 주기적으로 갱신하여 공개 디렉토리(웹, LDAP 등)에 게시
    - ra (Registration Authority(등록기관 또는 등록대행기관)) : ca에 인증서 폐지 **요청**,
      - 인증요청서 보관
      - 공개키와 인증서 소유자 관계 확인 및 인증서 발급 대행
      - **사용자의 신원 확인**: 인증서를 신청하는 사용자의 신원을 확인합니다

- **인증서 발급 요청 대행**: 신원이 확인된 사용자의 인증서 발급 요청을 ca에 전달합니다
- **CA와 사용자 간 중개 역할**: 사용자가 직접 CA에 접근하지 않고, RA가 중간에서 신원 검증과 요청을 대행함으로써 전체 인증 프로세스의 신뢰성을 높입니다
  - RA는 CA 대신 신원 검증만 수행하며, 인증서 발급 권한은 없습니다
- **WPKI에서의 역할**: 무선 환경에서도 RA는 사용자의 인증서 신청 및 신원 확인, 그리고 CA로의 요청 전달이라는 기본 역할을 수행합니다

정리하면, **RA는 사용자의 신원을 검증하고, 그 결과를 바탕으로 인증서 발급을 CA에 요청하는 중개 기관**입니다. CA가 인증서를 실제로 발급하는 주체라면, RA는 "신원 확인 및 등록"을 담당하는 기관

- client(사용자) : 인증서 발급 및 관리에 대한 요청
- directory : ca가 발행한 인증서 정보 저

- TLS 공격대상과 공격방법
  - DHE export key - Logjam
  - CBC mode encryption - BEAST
  - CBC mode encryption + padding - 패딩 오라클 공격
  - openssl(ssl3.-) -heartbleed
- DLP(Data loss Prevention)
  - 잠재적인 데이터나 정보 유출 전송을 감지해서, 사용중 또는 이동 중 정지 상태에 있는 멘감한 데이터 또는 정보를 모니터링 하거나 감지/차단함으로써 이를 방지한다. = 데이터 유출(누출) 방지, 데이터 이동 경로 감시 및 차단
  - drm과 다름 (drm 은 문서·파일 자체 암호화, 권한 관리 및 사용 통제)
- DRM
  - 구성요소
    - 클리어링 하우스 : 콘텐츠를 이용하는 사용자에 대해 정해진 정책에 따라 사용권한을 결정하고, 부여된 사용권한에 따라 라이선스의 발급 및 그 내역을 관리하는 시스템
    - **콘텐츠 제공자(Contents Provider) :** 저작권을 가진 자로, 보호할 디지털 콘텐츠(음악, 영상, 문서 등)를 제공

        - **패키저(Packager) :** 콘텐츠를 메타데이터와 함께 암호화하여 배포 가능한 형태로 묶는 역할
        - **콘텐츠 분배자(Contents Distributor) :**암호화된 콘텐츠를 실제로 유통하는 주체(예: 온라인 쇼핑몰, 스트리밍 서비스 등)입니다
        - **콘텐츠 소비자(Contents Customer) :** DRM 보호 콘텐츠를 구매하거나 이용하는 사용자입니다
        - **DRM 컨트롤러(DRM Controller) :**배포된 콘텐츠의 이용 권한을 실제로 통제하는 **소프트웨어 또는 시스템**
        - **보안 컨테이너(Security Container) :** 암호화된 콘텐츠 원본을 안전하게 유통하기 위한 전자적 보안 장치
- 전자메일
    - 헤더
        - Received : 실제 발송자를 추적하기 위해 사용
- 디지털 포렌식
    - 정당성의 원칙 : 적법절차로 수집되었는가에 대한 것 (위법수집증거배제법칙)
    - 연계보관성 : 증거물 획득, 이송, 분석, 법정 제출의 각 단계에서 담당자 및 책임자를 명확히 하는 것
    - 증거 식별, 수집, 획득, 보존, 분석 등의 과정을 거친다.
- 쿠키
    - **웹 서버**에 저장된 쿠키값은 개인정보보호를 위해 정기적으로 삭제해야 한다 **→ (x) 쿠키는 클라이언트 부라우저에 저장되는 것.**
- mssql 서버 인증
    - sqlserver의 기본인증모드는 윈도우 인증이다.
    - 윈도우 인증모드가 적용되어 있을 경우, sql 서버 인증을 이용할 수 없다.
    - 혼합 인증모드가 적용되어있을 경우, 둘다 사용가능
    - **윈도우 인증이 더 안전한 인증 방법(sql 서버인증보다)**
- PGP(Pretty Good Privacy)에서 **디지털 서명 기능을 위해 사용되는 알고리즘**
    - **DSS/SHA**
        - DSS(Digital Signature Standard, 즉 DSA)는 디지털 서명에 사용되며, SHA는 메시지 해시(다이제스트) 생성에 사용

    - rsa란
        - RSA 공개키 알고리즘 역시 PGP에서 디지털 서명에 사용
        - 메시지 해시를 RSA로 암호화(서명)하여 서명을 생성
    - diffie-hellman
    - 오답 : aes
- **Radix-64: 이진 데이터를 ASCII로 변환하는 인코딩 방식으로, 암호화나 서명과는 무관**
- **OS command injection**
    - 웹 페이지에 입력한 문자열이 Perl의 system함수나 PHP의 exec함수 등에 전달되어, 부정하게 쉘 스크립트(시스템 명령)가 실행되는 공격
- **Session hijacking:** 세션 정보를 탈취하여 권한을 빼앗는 공격
- **다크웹(Dark Web)**
    - **공공인터넷을 사용하는 오버레이 네트워크(예: Tor, I2P) 위에 구축된다**
    - **다크웹이 딥웹의 일부**이며, 딥웹이 더 큰 개념
    - **토르(TOR)같은 특수한 웹브라우저를 사용해야만 접근가능**
    - **다크넷에 존재하는 웹사이트를 의미**
- **DDos 공격 형태 중 자원 소진 공격**
    - **SYN Flooding, ACK Flooding, DNS Query Flooding은 각각 연결 큐, 상태 확인, DNS 서버 처리 능력 등 특정 자원 소진**
    - 오답 : **ICMP Flooding은 네트워크 대역폭 고갈이다(자원(대역폭, CPU 등) 소진 공격)**
- **MS SQL 서버의 인증 모드**
    - **기본 인증 모드는 Windows 인증**
    - **트러스트되지 않은 연결(SQL 연결)은 SQL Server 인증(혼합 모드)에서만 가능하다. 윈도우 인증에서는 불가능**
    - 윈도우즈 인증 로그온 추적시 SID 값을 사용
- **버퍼오버플로우에 대한 보안 대책**
    - **경계 검사를 하는 컴파일러 및 링크 사용**
    - **스택내의 코드 실행 금지**

- 오답: 포맷 스트링 취약점을 방지하기 위한 대책으로, 버퍼오버플로우와 관련없다. (포맷스트링 취약점이란 사용자 입력이 printf, sprintf 등에 그대로 전달될 때 발생하는 별도의 취약점)

- **SSO(Single Sign On)**
  - **Delegation 검사 :** SSO에서 공식적으로 사용하는 용어는 **Delegation(위임, 인증 대행) 방식**
  - **Propagation 방식: SSO의 대표적 구현 방식 중 하나로, 인증 정보(토큰)를 전달하는 모델**
- **S/MIME의 주요 기능**
  - S/MIME의 주요 기능은 **메시지 암호화(봉인된 데이터, Enveloped Data)**, **전자 서명(서명 데이터, Signed Data)**, **서명 및 암호화(서명 및 봉인된 데이터, Signed-and-Enveloped Data)**
  - **봉인된 데이터(Enveloped data)**
  - **서명 데이터(Signed data)**
  - **순수한 데이터(Clear-signed data)**
- **DNS**
  - **ISP 등이 운영하는 캐시 네임서버가 관리하는 DNS 캐시에 IP 주소, UDP 포트번호, DNS 메시지 ID값이 조작된 정보를 추가함으로써 DNS 캐시 포이즈닝(poisoning) 공격이 가능**
    - DNS 캐시 포이즈닝 공격은 캐시 네임서버의 캐시에 **잘못된 IP 주소(혹은 RR, Resource Record)**를 심는 것
  - DNSSEC은 **무결성, 출처 인증** 기능을 제공하지만, **비밀성(기밀성)**은 제공하지 않습니다.
- **무선 인터넷 보안 기술**
  - **WSP(Wireless Session Protocol) - 장시간 활용하는 세션을 정의하고 세션 관리를 위해 Suspend/Resume 기능과 프로토콜 기능에 대한 협상이 가능**
  - **WAP(Wireless Application Protocol) - 무선 인터넷 접속을 위한 전체적인 통신 규약이지 전송계층 보안이 아님**
  - WTLS는 무선 환경에서 데이터의 보안(암호화, 무결성, 인증)을 제공하는 전송계층 보안 프로토콜이지 인터넷접속을 위한 것이 아님

    - WTP는 WAP 환경에서 트랜잭션(데이터 교환)을 관리하는 프로토콜로 인증이나 암호화와 관련없음
- /etc/ftpusers : 익명 FTP를 사용할 수 있는 계정을 제한하는 파일
- /etc/pam.d/ftp : 익명 FTP에 대한 인증을 설정하는 파일
- /bin/etc/pub : 익명 FTP에서 공유할 수 있는 파일의 목록을 저장하는 파일
- **안드로이드 시스템 권한**
    - **ACCESS_CHECKIN_PROPERTIES : 체크인 데이터베이스의 속성테이블 액세스 권한**
    - **LOADER_USAGE_STATS : 액세스 로그 읽기 권한**
    - **SET_PROCESS_LIMIT : 제한처리 지정 권한**
    - **CHANGE_COMPONENT_ENABLED_STATE : 컴포넌트의 사용 여부를 변경하는 권한**
- **DNS 증폭 공격(DNS Amplification DDoS Attack)**
    - DNS 질의는 DNS 질의량에 비하여 DNS 서버의 응답량이 훨씬 크다는 점을 이용
    - 공격자가 소량의 DNS 요청 패킷을 여러 공개 DNS 서버에 보내고, 이때 출발지 IP를 피해자의 IP로 위조(스푸핑)하여, DNS 서버들이 대량의 응답을 모두 피해자에게 전송하도록 유도하는 공격
    - **오픈 리졸버(Open DNS Resolver) 악용**: 누구나 접근 가능한 DNS 서버(오픈 리졸버)를 활용해 공격 효과를 극대화
- ltrace : **어플리케이션의 공유 라이브러리에 대한 호출을 확인하기 위해 사용되는 리눅스의 디버깅 유틸리티**
- log4j 로그레벨 순서
    - ALL < DEBUG < INFO < WARN < ERROR < FATAL < OFF

정보보호일반

- 중요정보란
    - 개인정보, 인증정보, 권한으로 보호되어야 할 페이지 URL/IP 정보, 서버 절대경로, 자격증명 Key 등
- 개인정보란
    - 개인을 식별할 수 있는 정보(예: 고유식별정보, 금융정보, 민감정보, 위치정보 등)

- 민감정보 : 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보
  - **사상이나 신념에 관한 정보**: 개인의 가치관, 종교적 신념, 이데올로기 등
  - **노동조합·정당의 가입·탈퇴에 관한 정보**: 노동조합 또는 정당에 가입하거나 탈퇴한 사실 및 이를 유추할 수 있는 정보(예: 회비 납입내역)
  - **정치적 견해에 관한 정보**: 특정 정치 사안에 대한 입장, 지지 정당 등
  - **건강 및 성생활에 관한 정보**: 과거 및 현재의 병력, 신체적·정신적 장애, 성적 취향 등 (하지만 혈액형은 아님)
  - **유전정보**: 유전자 검사 결과 등 개인의 유전적 특징과 관련된 정보
  - **범죄경력자료**: 법에 따라 관리되는 범죄경력에 관한 정보
  - **개인의 신체적, 행동적 특징에 관한 정보**: 지문, 홍채, 얼굴 등 생체정보
  - **인종이나 민족에 관한 정보**: 개인의 인종, 민족적 배경 등
- BS7799
  - 영국표준협회(BSI, British Standards Institution)가 1995년에 제정한 정보보호 관리체계(Information Security Management System, ISMS) 국제 표준
  - 이후 국제표준화기구(ISO)로 이관되어, Part 1은 ISO/IEC 17799(현 ISO/IEC 27002), Part 2는 ISO/IEC 27001로 발전
- **ITSEC, TCSEC, CC 평가인증제도**
  - **ITSEC (Information Technology Security Evaluation Criteria)**
    - 유럽에서 개발된 정보보호 평가 기준으로, 제품 또는 시스템의 보안 기능과 보증성을 별도로 평가
    - 평가 등급(E0~E6)과 기능 등급(예: F-C1~F-B3 등)을 구분하며, 평가 대상(TOE: Target of Evaluation)의 보안 목표(Security Target)를 중심으로 평가가 이루어집니다.
    - ITSEC은 TCSEC의 한계를 보완하고, 기능성과 보증성을 독립적으로 평가하는 점이 특징
  - **TCSEC (Trusted Computer System Evaluation Criteria, 오렌지북)**
    - 미국 국방부가 제정한 컴퓨터 시스템 보안성 평가 기준으로, 오렌지북(Orange Book)으로도 불립니다.
    - 보안 등급을 D(최소 보호)~A1(검증된 설계)까지 계층적으로 구분하며, 각 등급은 임의적/강제적 접근제어, 감사, 식별, 보증 등 다양한 보안 요구사항을 포함합니다.

        - 주로 운영체제와 기밀성 중심으로 평가하며, 네트워크 보안이나 가용성 등은 상대적으로 미흡
    - **CC (Common Criteria, 공통평가기준)**
        - ITSEC, TCSEC 등 기존 평가 기준을 통합·발전시킨 국제 표준(ISO/IEC 15408)입니다.
        - 보안 기능 요구(SFR)와 보증 요구(SAR)를 분리하여, 평가 대상(TOE)의 보안 목표(Security Target) 및 보호 프로파일(PP)에 따라 평가가 이루어집니다.
        - 평가 보증 등급(EAL1~EAL7)로 **7개로** 세분화되고 기본은 **11개의** 클래스로 구성되어 있으며, 다양한 IT 제품과 시스템에 적용 가능하며, 국제적으로 상호 인증이 이루어집니다
    - 인가
        - 정보를 전송하는 과정에서 송신자와 수신자가 해당 자원에 대한 사용이 정당한지를 확인하는 절차
    - Users 그룹
        - 이 그룹의 구성원은 자신의 모든 데이터 파일 및 레지스트리에서 자신이 속하는 부분(hkey_current_user)를 완전하게 제어할 수 있다
    - iptables, ipfwadm, ipchains : 세개 모두 리눅스용 패킷 필터 기반 시스템 접근 통제 도구
    - modesecurity
        - (줄여서 ModSec)는 오픈소스 웹 애플리케이션 방화벽(WAF, Web Application Firewall)입니다. 원래는 아파치(Apache) 웹 서버의 모듈로 개발되었으나, 현재는 Nginx, Microsoft IIS 등 다양한 웹 서버에서 사용가능
    - 리눅스 명령어
        - 60일마다 비밀번호 변경 설정
            - passwd -x 60 user아이디
- **인증서 폐지 목록(CRL)**
    - 인증서 폐지 메커니즘은 X.509에 정의된 인증서 폐지 목록(CRL)으로 관리한다.
    - 폐지된 인증서의 목록은 디렉터리에 보관하여 공개하고 네트워크를 통해 접속하여 확인할 수 있다.
    - 인증서 폐지 주체

        - 소유자 본인뿐만 아니라, 인증기관이나 대리인 등 여러 주체가 다양한 사유로 신청하거나 직권으로 처리 가능(소유자 본인, 대리인, 인증기관 모두가 폐지 신청 및 처리 가능)
        - **소유자(가입자) 본인**이 직접 폐지를 신청할 수 있습니다. 예를 들어, 개인키 분실, 퇴직, 정보 변경, 사용 중단 등 개인적인 사유가 있을 때 본인이 폐지 요청을 할 수 있다
        - *인증기관(CA)**이 직권으로 폐지가능 (소유자 동의없이)
            - 인증서가 부정하게 발급된 사실이 확인된 경우
            - 인증서 내 정보가 변경된 경우
            - 보안 정책 위반, 약관 위반, 신원확인 미비 등 객관적 사유가 발생한 경우
            - 기타 보안상 더 이상 신뢰할 수 없다고 판단되는 경우
        - **대리인**이 소유자의 사망, 실종, 법적 무능력 등으로 인해 적법한 서류를 갖춰 폐지를 신청할 수도 있다.
    - 인증기관은 폐지된 인증서 목록(CRL)을 주기적으로 갱신하여 누구나 폐지 사실을 확인할 수 있도록 공고한다.
    - 오답 : **사용자의 인증서에 인증기관의 올바른 전자서명이 붙어 있고 인증서의 유효기간이 유효하면 인증서를 신뢰한다. —> "전자서명 + 유효기간"만으로 인증서를 신뢰하는 것은 불완전한 설명**입니다. 반드시 **해지(폐지) 여부**까지 확인해야만 인증서를 신뢰할 수 있다.
    - **버전(Version)**: CRL의 형식 버전을 나타냅니다.
    - **서명 알고리즘(Signature Algorithm)**: CRL에 서명할 때 사용된 알고리즘의 식별자입니다.
    - **발급자(Issuer)**: CRL을 발급한 인증기관(CA)의 DN(Distinguished Name)입니다.
    - **발급일자(This Update)**: 해당 CRL이 발급된 시점(갱신 시점)입니다.
    - **다음 발급일자(Next Update)**: 다음 CRL이 발급될 예정 시점입니다.
    - **폐지된 인증서 목록(Revoked Certificates)**: 폐지된 인증서의 일련번호(Serial Number), 폐지 시각 등
    - **발급자 서명(Signature)**
    - 오답 : 유효기간
- 보안커널(괄호는 다 보안커널)

    - 주체가 특정 객체에 접근을 요청하면 (⑦)은(는) 이를 가로챈다.
    - (⑦)은(는) 자신이 가지고 있는 기본규칙에 따라 접근권한(조직이 정의한 정책에 따라 설 정됨)을 결정한다.
    - (⑦)은(는) 정의된 접근규칙에 따라 접근을 허가 혹은 거부한다.
    - (⑦)에서 처리되는 모든 접근 요청은 이후의 추적 및 분석을 위해 기록된다.
- IDEA
    - 대칭키 암호 알고리즘
    - 128비트의 키를 사용하여 64비트의 평문을 8라운드를 걸쳐 64비트 암호문으로 만든다. 모든 연산이 16비트 단위로 이루어지도록 하여 16비트 프로세서에서 구현이 용이한 암호알고리즘이다.
- LEA
    - 국가보안기술연구소에서 2013년 개발한 경량 블록 암호 알고리즘으로 2019년 국제표준으 로 제정되었다. 특징으로는 AES 암호알고리즘에 대비하여 경량 암호로 높은 처리량, 낮은 전력소비로 사물인터넷 암호화에 적합한 알고리즘이다.
- kerberos
    - Kerberos 키 분배 프로토콜의 기반 기술 : Needham-Schroeder 프로토콜 (**Kerberos가 Needham-Schroeder의 취약점을 개선한 프로토콜)**
        - Needham-Schroeder 프로토콜
            - 키 분배 센터를 이용하는 키 분배 방법이다.
            - 질의응답(Challenge-Response) 방식을 이용하여 설계되었다.
            - 재전송 공격(Replay attack)에 취약하다. : **공격자가 이전에 유효했던 메시지(특히 세션키가 포함된 메시지)를 저장해 두었다가 나중에 그대로 재전송해도 프로토콜이 이를 구분하지 못하기 때문으로 이유는 Needham-Schroeder 프로토콜은 **타임스탬프(시간 정보)**를 사용하지 않고, Nonce(난수)만을 사용하기 때문이다**
                - 재전송공격을 방어는 방법 : 순서번호, 타임스탬프, 비표
    - 비밀키 암호작성법에 기초를 둔 온라인 암호키 분배방법이다.
    - **Kerberos의 핵심 목적이 바로 '인증되지 않은 사용자의 서비스 접근을 차단하고, 반드시 인증된 사용자만 서비스에 접속할 수 있도록 하는 것**
    - kerberos 프로토콜 시스템 특징

        - **기밀성(Confidentiality):** 네트워크 상에서 암호화를 통해 인증 정보와 티켓이 노출되지 않도록 보호합니다.
        - **무결성(Integrity):** 메시지 인증 코드(MAC) 등을 통해 데이터가 위조되거나 변조되지 않았음을 보장합니다.
        - **인증(Authentication):** 사용자와 서버가 서로의 신원을 확인할 수 있도록 합니다.
        - 오답 : 가용성(kdc 중단되면 전체 서비스 마비), 부인방지(kerberos는 대칭키 기반이기 때문에 부인방지 불가. 즉 사용자가 메시지를 보냈다는 사실을 증명할 수 없다)
- X.509 확장 영역에 속하는 것
    - **키와 정책 정보 : 공개키/확장키 사용목적, 인증서 정책**
    - **식별자: 인증서 발급자(기관키)/ 소유자(사용자키) 식별자**
    - **이름 및 대체 이름: 인증서 발급자(기관키)/ 소유자(사용자키) 대체 이름**
    - **제약 조건 및 정책:** 인증서가 CA인지 여부, 인증 경로 길이 제한, 소유자명 및 대체 명칭의 사용 범위 제한, 인증서 정책 검사 및 매핑에 대한 제한, 인증서간 정책
    - **인증서 관리 및 유효성 :** CRL 배포 지점 인증서 폐지 목록(CRL) 위치 정보, 인증서 발급자 정보 및 OCSP(온라인 인증서 상태 프로토콜) 경로, 개인키 사용 기간(전자서명 생성키의 유효기간)
    - X.509 v3는 확장 필드를 통해 유연한 인증서 관리를 지원
- 접근통제
    - 임의적 (DAC)
        - 객체에 대한 소유권을 기반으로 소유권을 갖는 주체가 객체에 대한 권한의 일부 또는 전부를 다른 주체에게 부여할 수 있다
        - **권한을 가진 주체(IT팀 내 직원)가 자율적으로 접근 권한을 관리**하고, 그 결과에 따라 특정 사용자의 접근 가능 여부가 결정되는 구조로 임의적으로 저 폴더에 권한을 누구는 주고 안주고를 결정
    - 강제적 (MAC)
        - 시스템 관리자가 보안 레이블(등급)을 기반으로 엄격하게 권한을 통제
        - 보안관리자 주도하에 중앙집중적 관리가 가능
        - 군사/정부 기관, 고보안 시스템
        - **장점**: 보안성이 매우 높음.

        - **단점**: 유연성이 낮고 관리가 복잡함
    - 규칙기반**(Rule-Based)**
        - 미리 정의된 규칙(예: 시간, IP 주소)에 따라 접근을 허용/차단
        - 방화벽 정책, 시간대별 접근 제한
        - **장점**: 일관된 정책 적용 가능.
        - **단점**: 동적 변경이 어렵고 복잡한 규칙 관리 필요
    - 역할기반 (RBAC)
        - 직무나 역할 기반 그룹화해서 관리 (기업 시스템(개발자, 회계팀 등 역할별 권한))
        - **장점**: 관리 효율성 ↑, 최소 권한 원칙 적용.
        - **단점**: 초기 역할 설계가 중요함
        - **최소 권한 원칙:** 사용자에게는 반드시 필요한 최소한의 권한만 부여됩니다.→ **과도한 권한 부여를 방지** 목표
        - RBAC는 역할을 세분화해 권한을 엄격히 제한 → 과도한 권한 내지 불필요한 권한을 가질 가능성은 매우 낮다
        - **추상화 작업 요구**: RBAC 구현 시 역할을 추상화(예: "관리자", "일반 사용자")하는 과정이 필수적
        - **Non-DAC 모델**: RBAC는 임의적 접근통제(DAC)와 달리 역할에 기반하므로 Non-DAC로 분류
- 키변경 기능(Key Change Function)
    - 기존의 암호키를 이용하여 새로운 암호키를 생성하는 방법을 키 갱신이라고 한다.
        - **키 갱신 방식은 기존 키가 안전하게 보관될 때만 안전**
        - **기존 키가 이미 노출된 경우에는 키 갱신이 아니라, 기존 키와 무관하게 완전히 새로운 키를 생성(키 교체)**
    - 기존의 암호키와는 독립적인 방법으로 새로운 암호키를 생성하는 방법을 키 교체라고 한다.
    - 암호키의 노출이 확인되거나, 노출의 위협이 있는 경우 혹은 암호키 유효 기간의 만료가 가까워지는 경우 암호키를 안전하게 변경해야 하며, 암호키를 변경한 이후에는 기존의 암호키를 정지단계로 전환해야 한다.
- MD 계열 해시함수의 특징

    - **데이터 무결성을 위해 메시지 압축·축약을 하는 해시 알고리즘이다 (MD 계열은 임의 길이의 입력을 고정된 크기의 해시값으로 축약하며, 데이터 무결성 검증에 사용)**
    - **해시 충돌 방지 확률은 약 1.47×10^{-29}이다**
    - MD 계열은 **128-bit** 출력을 사용합니다.
    - **MD 계열의 출력 크기**
        - **MD4**: 128-bit 해시값 생성 (16바이트, 16진수 32자리), **MD4의 경우, 속도가 빠른 반면에 안정성에서 뒤떨어진다.(그래서 현재 사용안함)**
        - **MD5**: 128-bit 해시값 생성 (MD4의 개선판)
        - **MD6**: 224/256/384/512-bit 지원 (MD5 이후 개발됨)

          → **160-bit 출력은 MD 계열의 특징이 아닙니다. (160-bit 해시값을 생성하는 알고리즘은 SHA-1로** MD 계열과 SHA 계열은 별개)
- 해시함수
    - 일방향성, 충돌 회피, 효율성의 특징이 있다.
    - 해시함수를 인증에서 증명 용도로 사용될 수 있다"**는 설명이 틀린 이유는 **해시 함수 단독으로는 인증(authentication)을 제공할 수 없기 때문.** 해시 함수는 **무결성(integrity) 검증**에는 적합하지만, **인증**을 위해서는 반드시 추가적인 암호학적 메커니즘이 필요
    - 임의의 유한 길이의 비트 스트링을 고정된 길이의 비트 스트링으로 변환하는 함 수이다.
    - 효율적 전자서명 생성을 위해 전자서명 생성 과정에서 해시함수가 사용된다.
- 대칭키 암호화와 MAC(Message Authentication Code)으로 해결할 수 없는 보안서비스
    - 메시지 부인방지: 대칭키 자체가 부인방지가 안됨.
- RSA 암호화 방식에서 공개키가 (7,33), 개인키가 (3,33)일 경우, 공개키로 암호화 한 값이 3이 라고 할 때 이를 복호화 한 값은 ?
    - 암호문 3의 개인키3 승한것을 33으로 나눴을때 나머지 = 27
- SSO 방식
    - 오답: RADIUS
    - SPNEGO, Kerberos, SESAME
- RADIUS 프로토콜

    - RADIUS는 네트워크 접근 제어를 위해 다음 세 가지 주요 기능 제공
        - **인증(Authentication): :**사용자의 신원을 확인합니다. 사용자가 네트워크에 접속하려 할 때, 사용자 이름과 비밀번호 등의 정보를 검증합니다.
        - **권한 부여(Authorization):** 인증된 사용자가 어떤 네트워크 자원이나 서비스를 사용할 수 있는지 결정합니다. 예를 들어, 접속 시간, 사용 가능한 서비스 종류 등을 제어합니다.
        - **계정 관리(Accounting):** 사용자의 네트워크 사용 내역을 기록합니다. 접속 시간, 데이터 사용량, 세션 종료 시간 등 다양한 정보를 로그로 남겨 과금이나 통계, 네트워크 관리에 활용합니다
        - 다만, RADIUS는 패킷의 무결성이나 메시지 인증을 완벽하게 보장하지 않으며, 로그 위변조나 세부 행위 추적 등 책임추적성의 모든 요건을 충족하지 않습니다. 즉 책임추적은 안됨
- 디바이스 인증 vs 사용자 인증
    - 디바이스 인증
        - 네트워크에 연결되는 "디바이스"의 신원을 확인하고, 인가된 디바이스만 네트워크에 접속할 수 있도록 제한하는 것이 목적 → 비인가된 디바이스의 접속 방지
        - 네트워크 참여 디바이스의 신뢰성 확보
    - 사용자 인증
        - **사용자 인증**은 **네트워크나 시스템**에 접근하는 "사람"의 신원을 확인하고, 인가된 사용자만 사용권을 갖도록 제한합
- 대칭키 암호화에서 10명의 사용자가 서로 암호화된 메시지를 교환할 때 필요한 **서로 다른 대칭키의 개수 계산 = 답은 45**
    - 대칭키 암호화에서는 **각 사용자 쌍(2명)마다 고유한 키가 필요**
    - **n명의 사용자가 있을 때 필요한 키의 총 개수 =** $n(n-1)/2$
- 암호 알고리즘 공격방법
    - 선택 암호문 공격
        - 먼저 암호 알고리즘의 비선형 요소에 대해 평문의 차분과 암호문의 차분 사이의 관계에 대한 차분 분포표를 구성한다. 그 후 차분 분포표에서 높은 확률을 갖는 공격에 필요한 평문 목록 을 구성하고, **암호문**을 선택하고 그에 대응하는 평문을 **얻어** 키의 특정 비트 정보를 찾는다.

    - 선택 평문 공격 : 암호 해독자가 사용된 암호기에 접근할 수 있어 평문에 해당하는 암호문을 얻을 수 있는 상 황에서 키를 추정하여 암호를 해독하는 방법이다.
    - 기지 평문 공격 : 암호화 키를 알아내거나, 다른 암호문들에 대응되는 평문을 **추정**하는 방법 암호 해독자는 일정량의 알려진 평문에 대응하는 암호문을 알고 있음
    - 비교
        - **기지평문공격:** 이미 주어진 평문-암호문 쌍을 분석
        - **선택암호문공격:** 공격자가 원하는 암호문을 복호화해서 평문을 직접 얻어볼 수 있음
- WPA3
    - 순방향 기밀성을 갖는다 :
        - 즉, 현재 사용되는 세션키나 마스터키가 노출되더라도 예전에 암호화된 트래픽의 기밀성에 영향 을 미치지 않는다. = **과거 트래픽 보호**: 현재 키가 유출되더라도 **이전 세션의 암호화된 데이터는 복호화할 수 없습니다**
        - **세션별 독립 키 생성**: 각 통신 세션마다 고유한 암호화 키를 생성합니다. 예를 들어, Wi-Fi에서 장치가 연결될 때마다 새로운 키가 자동으로 생성
        - **장기 키와 분리**: 마스터키(예: Wi-Fi 비밀번호)가 유출되어도 세션 키와 무관하므로 과거 트래픽은 안전
- 메시지 인증
    - 블록 암호 운영 모드 중 CBC는 CBC-MAC 등으로 메시지 인증에 사용될 수 있습니다. CTR은 단독으로 메시지 인증에 사용할 수 없으며, 별도의 인증 절차(HMAC 등)가 필요
    - CBC (Cipher Block Chaining) 모드
        - **메시지 인증에 사용 가능:** CBC 모드는 메시지 인증 코드(MAC)를 생성하는 방식인 CBC-MAC에 활용됩니다. CBC-MAC은 입력 메시지를 CBC 방식으로 암호화한 뒤, 마지막 블록을 MAC 값으로 사용
    - CTR (Counter) 모드
        - **메시지 인증에 직접 사용 불가:** CTR 모드는 본질적으로 메시지 인증(무결성 보장) 기능이 없습니다. CTR은 스트림 암호처럼 동작하여, 오직 기밀성(암호화)만 제공합니다. 메시지의 무결성이나 인증을 보장하지 않는다
        - **운영 방식:** 각 블록마다 증가하는 카운터 값을 암호화하여, 이를 평문과 XOR하여 암호문을 생성합니다.

        - **인증 필요:** CTR 모드로 암호화한 후, 별도의 메시지 인증 코드(HMAC 등)를 추가로 적용해야 무결성과 인증이 보장됩니다
    - CFM(암호 피드백 모드)
        - 초기값을 암호화한 값과 평문 블록을 XOR하여 암호문 블록을 생성하고, 그 암호문을 입력 으로 사용하여 다시 암호화한 값과 평문 블록을 XOR하여 암호문 블록을 생성하는 작업을 **반복**하는 방식이다. 암호화에서는 특정 평문 블록이 이후의 모든 암호문 블록에 영향을 미치지 만, 복호화에서는 특정 암호문 블록 오류의 영향이 국지적이라는 특성을 갖는다.
    - OFB모드(Output Feedback)
        - 블록 암호를 **스트림 암호처럼** 사용하는 암호화 운영 모드
        - 다음 블록의 키 스트림은 **이전 키 스트림을 암호화해서** 계속 만들어집니다
        - **오류 전파 없음**: 암호문 일부가 깨져도 해당 블록만 영향, 평문이나 암호문의 오류가 후속 블록에 영향을 미치지 않음
        - **병렬 처리 불가**: 이전 키 스트림의 결과를 다음 키 스트림 생성에 사용하므로, 순차적으로 처리해야 합니다16.
        - **암호화와 복호화 방식이 동일**: 암호문과 키 스트림을 XOR하면 평문이 바로 복원
- HMAC
    - 용도는 메시지 인증
    - HMAC(Hash-based MAC)는 **메시지 무결성**과 **인증**을 제공하기 위해 해시 함수를 기반으로 하는 MAC 방식
    - 특징
        - **해시 함수 교체 용이성**
            - 내장된 해시 함수를 **보안 취약성 발생 시 쉽게 교체**할 수 있어야 함
            - 예: SHA-1이 취약해지면 SHA-256으로 교체 가능
        - **원본 해시 함수 성능 유지**
            - HMAC 연산이 해시 함수의 **기본 동작 성능을 저하시키지 않음**
            - 예: SHA-256 단독 사용 대비 HMAC-SHA256의 성능 차이 미미
        - **암호학적 안전성 보장**
            - 해시 함수의 충돌 저항성 등 암호학적 특성을 활용하여 안전성 유지

- AES
  - 256 비트 키 길이의 AES 알고리즘의 라운드의 개수는 14개
    - 128비트 키로 충분한 보안성을 확보한 뒤, 키가 32비트씩 늘어날 때마다 라운드를 2개씩 추가하는 구조(128비트가 10, 192가 12, 256이 14)
    - (비트/32)+6
- **긴 메시지에 해시를 적용한 후 전자서명하는 근본적 이유**
  - 전자서명 알고리즘의 특성상 전자서명 및 검증속도가 데이터량에 따라 많은 영향을 받기 때문이다.
  - 긴 메시지를 **직접 서명하지 않고 해시값을 서명**하는 방식은 **전자서명 알고리즘의 연산 효율성 문제(**RSA, ECC 등 공개키 암호 기반 전자서명 알고리즘은 **대량의 데이터 처리에 비효율적)와**
  - **암호학적 연산 부하 감소 (**공개키 암호화는 모듈로 지수 연산 등 복잡한 수학적 연산을 필요로 하며, 데이터 크기가 커질수록 연산량이 기하급수적으로 증가한다) 해시값 서명은 이러한 부하를 해시 함수의 빠른 처리 성능으로 상쇄
- 전자서명
  - 전자서명은 서명문의 위조 불가, 서명한 행위의 부인 방지를 제공
  - 은닉서명은 서명자가 서명문의 내용을 알지 못하는 상태에서 서명하도록 한 방식으로 서명자 의 익명성이 보장된다.
    - 신원노출문제를 해결하는 전자서명 기술
  - DSA 알고리즘은 이산대수 문제의 어려움에 기반을 두고 있는 대표적인 전자서명
  - 서명자를 누구든지 검증할 수 있다.
  - 개인키를 알고 있는 서명자만 서명을 생성할 수 있다.
  - 전자서명에서 서명 재사용 불가능 이유
    - **서명이 특정 문서의 해시값에 종속적이기 때문**입니다.
    - **서명 생성**: 문서의 해시값을 발신자의 **개인키로 암호화**하여 서명을 생성합니다.
      - 예: 문서 A → 해시값 H(A) → 개인키로 암호화 → 서명 Sig(H(A)).
      - **검증**: 수신자는 문서의 해시값 H(A')을 계산하고, 서명 Sig(H(A))을 발신자의 **공개키로 복호화**하여 H(A)를 얻습니다.
        - H(A') ≠ H(A) → 서명 무효.
    - **서명 재사용 시 발생하는 문제**

        - 다른 문서(B)에 서명(Sig(H(A)))을 재사용하면:
        - 문서 B의 해시값 H(B) ≠ H(A) → 복호화된 H(A)와 H(B)가 일치하지 않습니다.
        - 검증 시 **H(B) ≠ H(A)**로 판별되어 서명이 즉시 무효화됩니다
    - **해시 함수의 충돌 저항성**: 서로 다른 문서(A, B)가 동일한 해시값(H(A) = H(B))을 생성할 확률은 극히 낮습니다.
    - **디지털 서명의 무결성 보장**: 서명 재사용 시도는 해시값 불일치로 인해 **변조 시도로 감지**됩니다.
  - 알고리즘 : **dsa**, kcdsa, ecdsa
- 스트림 암호
  - LFSR(선형 피드백 시프트 레지스터) 기반 스트림 암호는 **긴 주기**와 높은 선형 복잡도를 요구한다
  - 일회성 패드(One-Time Pad)의 이론을 기반으로 하며, 실제 적용을 위해 의사난수 생성기로 확장한 방식이다
  - 스트림 암호는 비트/바이트 단위 실시간 처리로 블록 암호보다 일반적으로 빠르다
  - 블록암호인 OFB(Output Feedback) 모드는 블록 암호를 스트림 암호와 유사하도록 설계된 모드
- BLP 모델 핵심 규칙 요약
  - **Simple Security Property (No-read-up):** 낮은 등급 주체 → 높은 등급 객체 **읽기 불가**
  - **Star Property (No-write-down):** 높은 등급 주체 → 낮은 등급 객체 **쓰기 불가**.
- **Hybrid 암호화 시스템**
  - **대칭키 암호**와 **공개키 암호**의 장점을 결합한 방식
  - **대칭키 암호시스템의 역할**
    - **데이터 암호화**: 1회용 세션키(대칭키)로 대용량 데이터를 빠르게 암호화합니다.
  - **공개키 암호시스템의 역할**
    - **세션키 분배**: 수신자의 공개키로 세션키(대칭키)를 암호화하여 안전하게 전달합니다.
  - 하이브리드 시스템 흐름
    1. **세션키 생성**: 송신자가 임의의 대칭키(세션키) 생성.

2. **세션키 암호화**: 수신자의 **공개키**로 세션키를 암호화.
3. **데이터 암호화**: 세션키로 **대칭키 암호화 알고리즘**을 사용해 데이터 암호화.
4. **전송**: 암호화된 세션키 + 암호화된 데이터를 수신자에게 전송.
5. **복호화**:
    - 수신자는 자신의 **개인키**로 세션키 복호화.
    - 복호화된 세션키로 데이터 복호화.

- 단일 치환 암호
    - 해독방법은 빈도 분석법 : **평문에 등장하는 각 문자의 빈도(출현 비율)가 암호문에서도 그대로 유지되기 때문**
        - **단일 치환 암호**는 평문의 각 알파벳을 치환표에 따라 다른 알파벳으로 바꿉니다.
        - 예를 들어, 평문의 'E'가 암호문의 'X'로 바뀌면, 평문에 'E'가 10번 나오면 암호문에도 'X'가 10번 나옵니다
- 해시함수의 분류 중 MDC(Modification Detection Cryptography)에 포함되는 알고리즘은? - MD(Message Digest), SHA(Secure Hash Algorithm), LSH(Lightweight Secure Hash)
- **실시간으로 인증서 유효성을 검증하는 OCSP(Online Certificate Status Protocol)의 서비스**
    - RFC 6960으로 묘사되며, 인터넷 표준의 경로가 된다.
    - **OCSP는** X.509를 이용한 전자 서명 인증서의 폐지 상태를 파악하는데 사용되는 인터넷 프로토콜이다.
    - **CRL : 인증서 폐지 목록 확인서비스** CRL은 실시간이 아닌, 주기적으로 갱신되는 목록을 통한 인증서 유효성 확인 방식
    - 상태값 : good, revoked, unknown (오답 : bad)
    - **DPD(대리인증 경로 발견 서비스)**: 클라이언트 대신 서버가 인증 경로를 찾아주는 실시간 서비스
    - 그밖에 ors(온라인 취소상태 확인서비스), dpv(대리인증 경로 검증서비스)
- CRL(Certificate Revocation List, 인증서 폐지 목록에 포함되는 정보
    - **폐기된 인증서의 일련번호**
    - **폐기 일자**

    - **폐기 사유(선택적)**
    - **CRL 발행자 정보:** 해당 CRL을 발행한 인증기관(CA)의 정보가 포함
    - **CRL 발행 일자 및 다음 갱신 일자**
    - **CRL 버전 정보**
    - **CRL 자체의 서명 및 서명 알고리즘 정보:** 발행자의 전자서명과 서명 알고리즘 정보
    - **(선택적) 폐기된 인증서의 공개키**
- 전자서명인증업무지침에 따라 공인인증기관이 지켜야 할 구체적인 사항이 아닌 것
    - **공인인증기관 지정 절차**
- IAM
    - 사용자가 로그인할 때 본인임을 증명하는 과정은 '인증
    - 인가는 인증 이후 사용자가 어떤 자원에 어떤 권한으로 접근할 수 있는지 결정하는 과정
    - 사용자가 시스템을 사용하기 위해 로그인 ID를 발급하는 과정을 프로비저닝
- 전자서명 사용 예
    - **Code Signing**: 소프트웨어 코드에 전자서명을 적용하여 코드의 무결성과 출처를 검증
    - **X.509 Certificate**: X.509 인증서는 전자서명 사용하여 인증서의 진위와 무결성을 보장
    - **SSL/TLS Protocol**: SSL/TLS 프로토콜은 X.509 인증서의 전자서명을 이용
    - 오답 : Kerberos는 대칭키 기반의 비밀키 암호화 방식을 사용하여 인증을 수행하며, 전자서명을 사용하지 않는다
- Needhan-Schroeder 프로토콜
    - 대칭키 암호 방식과 키 분배 센터(KDC)를 이용
    - 세션키 탈취 시 재사용 공격(replay attack)에 취약
    - 보완하기 위해 KDC와 난수(또는 타임스탬프)를 이용해 인증 방식을 도입 → 나중에 Kerberos 등으로 발전
    - A(사용자)가 KDC를 통해 세션키를 발급받고, 이 키로 상호 인증을 수행
    - 절차
        1. A가 KDC에 A와 B의 ID, 난수(N1)를 전송합니다.

2. KDC는 세션키, B의 ID, N1, 그리고 B에게 전달할 세션키 정보를 포함해 A에게 응답합니다.
3. A는 KDC로부터 받은 세션키 정보를 B에게 전달합니다.
4. B는 A에게 새로운 난수(N2)를 세션키로 암호화해 보냅니다.
5. A는 N2+1을 세션키로 암호화해 B에게 회신

- **RSA를 이용하여 키를 공유하는 방법**
  - RSA는 MIT의 Rivest, Shamir, Adelman이 개발한 공개키 암호화 방식
  - **A가 암호화 되지 않은 평문으로 A의 공개키를 B에게 전송 (RSA 방식에서 공개키는 안전하게 공개가능)**
  - **B는 세션키(공유 비밀키)를 생성, A에게서 받은 A의 공개키로 암호화 전송 → A는 A만 자신의 개인키로 이를 복호화**
- 은닉서명 : RSA 전자서명 환경에서 메시지 **M**에 대해 **난수 r**과 공개 검증키 **e**를 사용해 **$r^eM \bmod n$** 값을 서명자에게 전송하는 기법
- 알려진 평문 공격(Known-Plaintext Attack)
  - **암호문에 대응하는 일부 평문이 가용한 상황에서의 암호 공격방법 (일부 평문 쌍을 알고 있을 때)**
- 공개키 암호의 필요성(장점)
  - 무결성, 인증, 부인방지
  - 오답 : 키 관리 문제 대칭키 암호 방식의 단점
- **커버로스(Kerberos)의 구성요소**
  - **KDC(Key Distribution Center)**: Kerberos의 중앙 서버로, 인증 서버(AS)와 티켓 부여 서버(TGS)로 구성
  - **AS(Authentication Service/Server)**: 사용자의 신원을 확인, 티켓 부여 티켓(TGT)을 발급
  - **TGS(Ticket Granting Service/Server)**: 서비스 티켓을 발급
- **공개키 암호 알고리즘**
  - **RSA(Rivest, Shamir, Adelman) : 공개키와 개인키 쌍을 기반으로 작동**
  - **ECC(Elliptic Curve Cryptography)**: 타원곡선 기반의 공개키 암호 시스템으로, RSA보다 짧은 키 길이로 동일한 보안 수준을 제공
  - **ElGamal**: Diffie-Hellman 키 교환을 기반으로 한 공개키 암호 시스템

    - 오답: **Rijndael(**AES 기반이 되는 **대칭키 암호 알고리즘)**
- **키를 분배하는 방법**
    - **KDC, 공개키 암호시스템, Diffie-Hellman**
    - 오답 : **Kerberos(키 분배 프로토콜)**
- 해시함수 특징
    - 두 번째 역상저항성 :주어진 **x**에 대해 **x′ ≠x**이면서 **h(x) = h(x′)**인 **x′**를 찾기 어려운 특성
    - **충돌 저항성:** 임의의 두 입력 $\mathbf{x_1}$, $\mathbf{x_2}$에 대해 **$h(x_1) = h(x_2)$**를 만족하는 쌍을 찾기 어려운 특성
    - **압축성**: 해시 함수가 임의 길이 입력을 고정 길이 출력으로 변환하는 특성
    - **일방향성**: 해시값 **h(x)**에서 원본 입력값 **x**를 역추적할 수 없는 특성
- 하이브리드 암호 시스템
    - **대칭키 암호화와 공개키(비대칭키) 암호화의 장점을 결합**
    - 동작 원리
        - **메시지 암호화**: 실제 데이터는 빠르고 효율적인 대칭키 암호화(예: AES)로 암호화합니다.
        - **세션키 분배**: 이때 사용된 대칭키(세션키)는 수신자의 공개키로 암호화하여 함께 전송합니다.
        - **복호화 과정**: 수신자는 자신의 개인키로 세션키를 복호화한 뒤, 이 세션키로 실제 메시지를 복호화
- **메시지 출처 인증(Message Origin Authentication)에 활용되는 암호 기술 중 대칭키 방식**
    - 메시지 인증 코드(Message Authentication Code, MAC)
- 해시값과 mac(메시지 인증코드)
    - HMAC은 메시지 송수신자는 비밀키(Encryption Key) 또는 세션키(session Code)를 사전에 안전한 채널을 통해 공유해야 한다.
- 전자서명, 이중서명은 공개키(비대칭키)방식
- SSL/TSL 1.3을 사용하면 통신의 기밀성을 확보할 수 있다.
- **OTP와 HSM(Hardware Security Module)**

    - OTP는 일반적으로 대칭키(공유 비밀) 기반의 알고리즘(HOTP, TOTP 등)을 사용한다. (공개키인 pki방식은 사용하지 않음)
    - **HSM의 안정성 인증 적용 표준은 FIPS 140-2**
    - **HSM은 공개키를 사용**
- **신규 OTP 기술**
    - MicroSD OTP : 휴대폰이 아닌 별도의 외장 저장장치 카드에 OTP 모듈을 내장하여 사용
    - 스마트 OTP : IC칩 기반의 스마트카드와 NFC 기능을 지원하는 스마트폰에 OTP를 발생
    - USIM OTP: 사용자의 휴대폰의 USIM내에 OTP모듈 및 주요정보를 저장
- **빅데이터 비식별화 처리기법 중 가명처리 방법**
    - **휴리스틱 가명화**
        - 일정한 규칙이나 알고리즘(예: 이름을 임의의 규칙으로 변환)으로 식별자를 대체합니다.
        - 예시: "홍길동" → "임꺽정", "USER_A" 등
    - **암호화(Encryption)**
    - **토큰화 :** 식별 정보를 의미 없는 임의의 토큰(값)으로 대체합니다.
    - **일련번호 부여**
- I-PIN는 지식기반 인증방식으로 'ID/PW'와 주민번호를 대체하기 위하여 만들어졌다.
- 사이드채널 공격 : 암호화 알고리즘의 구현 과정이나 환경에서 발생하는 물리적 또는 전기적 신호를 측정하여 비밀 정보를 추출하는 공격입니다. 측정되는 신호에는 전력 소모, 전자기파, 열, 소음 등
- 스마트카드
    - 접촉식 스마트카드는 리더기와 스마트카드의 접촉부(CHIP) 사이의 물리적 접촉에 의해 작동하는 스마트카드이다.
    - 스마트카드의 인증 데이터 저장을 위해 서명된 정적 응용 프로그램 데이터와 인증기관(CA)의 개인키로 발행자의 공개키를 암호화된 데이터를 스마트카드에 저장

정보보호 관리 및 법규

- 정보통신기반 보호법

    - **정보통신기반** 보호법」 제16조에 따르면, 금융·통신 등 분야별 정보통신기반시설을 보호하기 위해 구축·운영할 수 있는 조직은 **"정보공유·분석센터(ISAC, Information Sharing and Analysis Center)"다. → 사이버 안전센터는 오답. 사이버 안전센터라는 것은 없다.**
- 개인정보보호법상 개인정보처리 위탁
    - *"개인정보처리자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 **위탁에** 대해 정보주체의 동를 받아야 한다.(x) —>* **정보주체의 동의를 받을 필요는 없고, 고지(알림)만 하면 됩니다.**
        - 동의가 필요한 것은 "**제3자 제공**"의 경우이며, "위탁"은 동의가 아니라 고지 의무가 적용됩니다
    - 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 일정한 내용이 포함된 문서에 의하여야 한다.
- 주요정보통신기반시설 **취약점의** 분석 및 평가
    - **의무제도**이다.(자율제도 아님)
    - 의뢰기관
        - 한국인터넷 진흥원
        - 정보보호 전문서비스 기업
        - 한국전자통신 연구원
        - 정보공유, 분석센터
        - 오답 : **한국정보화진흥원**
- 정보통신기반보호위원회 기능 (위원회는 **정책의 조정, 계획의 종합·조정 및 추진 실적 심의** 등 '조정'과 '심의' 역할을 담당)
    - 주요정보통신기반시설의 지정 및 지정 취소
    - 주요정보통신기반시설 보호정책의 조정
    - 주요정보통신기반시설에 관한 보호계획의 종합. 조정
    - 오답 : 주요정보통신기반시설 보호대책의 수립(이건 틀린값. 이건 해당 시설을 관리하는 공공기관 또는 기업이 담당)
- 공공기관에서 개인정보파일을 운용하는 경우에 보호위원회에 등록해야 하는 사항
    - 개인정보파일의 명칭
    - 개인정보파일의 운영 근거 및 목적

    - 개인정보파일에 기록되는 개인정보의 항목
    - 개인정보의 처리방법
    - 개인정보의 보유기간
    - 개인정보를 **통상적 또는 반복적으로** 제공하는 경우에는 그 제공받는 자
    - 그 밖에 대통령령으로 정하는 사항
    - 오답: 개인정보를 **일시적으로** 제공하는 경우 그 제공받는 자
- 개인정보 영향평가(PIA)를 하는 경우에 고려할 사항
    - (처리하는) 개인정보 수
    - 제3자 제공 여부
    - 권리 침해 가능성 및 위험
    - 민감정보/고유식별정보 처리 여부
    - 보유기간
    - 기타 안전조치 및 처리방법의 적정성
    - 오답 : 개인정보처리의 위탁여부(x)
- 위험관리의 정보자산 식별활동
    - 조직의 **업무특성**에 따라 식별/분류하고, **중요도**를 산정한 후 그 목록을 최신으로 관리해야한다.
- 정량적 vs 정성적 위험분석 (장점만)
    - **정량적 위험분석의 장점**
        - **객관적이고 신뢰성 있는 결과 :** 수치 데이터와 통계적 분석에 기반하므로, 평가 결과의 신뢰성이 높고 객관적입니다
        - **금전적 가치 등 구체적인 수치 제공:** 위험의 발생 확률과 손실 규모를 금전적 가치, 백분율, 확률 등으로 산출하여 의사결정에 직접 활용할 수 있습니다
        - **재무적·전략적 의사결정에 유용 :**예상 손실 비용, 기대값 등 구체적 수치를 제공해 자원 배분이나 투자 우선순위 결정에 실질적인 근거가 됩니다
        - **시뮬레이션과 다양한 시나리오 분석 가능 :**몬테카를로 시뮬레이션, 민감도 분석 등 다양한 수학적 기법을 통해 복잡한 위험 상황도 정밀하게 분석할 수 있습니다
    - **정성적 위험분석의 장점**

        - **빠르고 쉽게 적용 가능 :**복잡한 계산이나 방대한 데이터가 없어도 전문가의 판단, 경험, 시나리오 분석 등으로 신속하게 위험 평가가 가능합니다
        - **데이터가 부족한 상황에서도 활용 가능 :**과거 데이터가 부족하거나 수치화가 어려운 위험(예: 평판, 조직 문화 등)도 평가할 수 있습니다
        - **현장 경험과 직관 반영 :**전문가의 경험, 직관, 다양한 이해관계자의 의견을 반영하여 실제 현장 상황에 맞는 평가가 가능합니다
        - **우선순위 도출 및 커뮤니케이션에 용이:** 위험을 등급(고, 중, 저)이나 점수로 분류해 우선순위를 쉽게 파악하고, 조직 내 의사소통이 원활합니다
- 세이프 가드
    - **위험분석에서 확인된 위협과 취약점**에 대응하기 위해 도입하는 각종 통제, 보호조치, 대응책을 의미
    - 위협이 가해질 때 특정 위협이 나 위협 그룹에 관련된 위험을 제거하기 위해 적용된 통제나 대응방안 =**위험을 줄이기 위한 구체적이고 실질적인 보호조치**
    - **주요 특징**
        - **위험 감소 목적**
            - 세이프가드는 자산의 취약성을 줄이고, 위협이 실제 피해로 이어질 가능성을 낮추는 역할을 합니다.
            - 예를 들어, 방화벽 설치, 접근통제 정책, 백업 시스템, 보안 교육 등이 모두 세이프가드에 해당합니다
        - **다양한 형태:** 세이프가드는 단순한 기술 장치뿐 아니라, 정책, 절차, 교육, 조직적 조치 등 다양한 형태
        - **비용-효과 분석의 대상**세이프가드의 가치=도입 전 예상 연간 손실(ALE)−(도입 후 ALE+세이프가드 연간 운영비
        - 세이프가드 도입 전후의 위험 감소 효과와 도입·운영 비용을 비교하여, 경제적으로 타당한지 평가합니다.
    - **법적·윤리적 책임 이행**

      적절한 세이프가드를 마련하지 않아 실제 위협이 현실화될 경우, 조직은 법적 책임을 질 수 있습니다.

      따라서 세이프가드는 의무적 관리책임(Do care) 이행의 수단이기도 합니다
- ALE 계산
    - 위험분석의 정량적 방법

    - 특정 자산에 대해 연간 어느 정도의 금전적 손실이 예상되는지 산출하는 공식
    - **SLE(Single Loss Expectancy, 단일 예상 손실액) 계산**$SLE = AV \times EF$
        - AV(Asset Value): 자산가치
        - EF(Exposure Factor): 노출계수(위험 발생 시 손실 비율)
    - **ARO(Annual Rate of Occurrence, 연간 발생률) 산정**
        - 일정 기간 내 위험이 발생할 확률(예: 5년에 1번 발생 → 0.2)
    - **ALE 계산**$ALE = SLE \times ARO ALE = (AV \times EF) \times ARO$
        - **자산가치(AV)**: 1억 원
        - **노출계수(EF)**: 30% (0.3)
        - **연간 발생률(ARO)**: 0.2 (5년에 1번)

          =3천만원×0.2=6백만원 = 따라서, 이 자산에 대해 연간 6백만 원의 손실이 예상된다는 의미
- 자동화된 위험 분석 도구
    - 단점: 위험분석에 소요되는 시간과 비용을 절감할 수 없다. 초기 투자와 도입비용이 크고, 데이터 품질 및 통합이 어려우며(자동화분석 오류 발생)
- 100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업의 내부관리계획의 내용에 포함할 내용
    - 100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업은 「개인정보의 안전성 확보조치 기준」상 **유형2(표준)**에 해당하며, 내부관리계획을 반드시 수립해야 합니다
    - 개인정보 보호 조직의 구성 및 운영에 관한 사항
    - 개인정보 보호책임자의 자격요건 및 지정에 관한 사항
    - 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
    - 개인정보취급자에 대한 관리·감독 및 교육에 관한 사항
    - 접근 권한의 관리에 관한 사항
    - 접근 통제에 관한 사항
    - 개인정보의 암호화 조치에 관한 사항
    - 접속기록 보관 및 점검에 관한 사항
    - 악성프로그램 등 방지에 관한 사항

    - 개인정보의 유출·도난 방지 등을 위한 취약점 점검에 관한 사항
    - 물리적 안전조치에 관한 사항
    - 개인정보 내부관리계획의 수립, 변경 및 승인에 관한 사항
    - 100만명 미만 정보주체 개인정보를 보유한 중소기업은 위에 명시한 항목을 내부관리계획에 포함해야 하며, 일부 고도화된 항목(유출사고 대응계획 등)은 필수사항이 아닙니다.
    - 1만명 미만의 소상공인, 개인, 단체는 내부관리계획 수립 자체가 생략될 수 있지만, **중소기업**은 반드시 수립해야 합니다
- 베이스라인 접근법
    - 모든 시스템에 대해 표준화된 보호(보안) 대책의 세트를 **체크리스트** 형태로 제공하고, 이를 기준으로 해당 대책이 실제로 구현되어 있는지 점검하는 방식
    - 사전에 정의된 보안대책(예: ISO27001, ISMS 등)을 체크리스트로 만들어, 조직 내 시스템에 해당 대책이 적용되어 있는지 여부를 확인
- **개인정보의 안정성 확보조치 기준(고시)의 제7조(개인정보의 암호화)에 따라 반드시 암호화 하여 저장해야하는 개인정보**
    - **주민등록번호**
    - **여권번호**
    - **운전면허번호**
    - **외국인등록번호**
    - **신용카드번호**
    - **계좌번호**
    - **생체인식정보(바이오정보)**
    - **비밀번호** (단, 비밀번호는 복호화가 불가능한 일방향 암호화로 저장)
    - 오답 : 전화번호는 아님
- ISMS(정보보호 관리체계)와 ISMS-P(정보보호 및 **개인정보보호** 관리체계)의 차이
    - **ISMS**는 조직의 정보자산을 안전하게 보호하는 체계(정보보호)에 초점을 맞춘 인증입니다. 개인정보 보호에 관한 별도의 요구사항은 포함되어 있지 않습니다
    - **ISMS-P**는 ISMS의 정보보호 기준에 더해, 개인정보의 수집·보유·이용·제공·파기 등 개인정보 처리 단계별 보호조치 요구사항이 추가된 통합 인증입니다. 즉, 정보보호와 개인정보보호를 모두 포괄합니다

        - 관리체계 수립 및 운영 4단계 중 위험 관리 단계의 통제항목 : 정보자산 식별, 현황 및 흐름 분석, 위험 평가
    - **인증 범위**도 ISMS는 정보시스템, 조직, 물리적 위치 등 정보서비스 운영 전반에 한정되지만, ISMS-P는 여기에 개인정보 처리와 관련된 시스템, 인력, 장소까지 모두 포함합니
    - **인증 항목 수** 역시 ISMS-P가 더 많으며, 개인정보보호 관련 항목이 추가되어 심사 기준이 더 엄격
    - 정보보호 관리체계는 통상적으로 PDCA 사이클을 기반으로 실행된다.
        - pdca란?
            - Plan(계획) – Do(실행) – Check(점검/평가) – Act(개선/조치)**의 네 단계로 구성된, 경영 및 품질관리에서 널리 쓰이는 **지속적 개선을 위한 관리 방법론**
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률(정보통신망법)**에서 정의하는 용어 설명
    - 전자문서 : **컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적 형태로 작성·송수신 또는 저장된 정보로서, 그 내용이 확인될 수 있는 것으로**
        - **“암호화”가 될 필요없고, “표준화”될 필요도 없다. —> 있으면 오답**
- 「개인정보보호법」 제34조 및 관련 시행령에 따른 개인정보 유출 통지 및 신고
    - 통지 : **지체 없이** 정보주체(당사자)에게 유출 사실을 통지
    - 신고 : **보호위원회(또는 전문기관)이** 아래 중 하나에 해당하면 **72시간 이내**에 **개인정보보호위원회 또는 한국인터넷진흥원(KISA)**에 신고해야 함
        - 1,000명 이상의 정보주체에 관한 개인정보가 유출된 경우
        - 민감정보 또는 고유식별정보가 유출된 경우
        - 개인정보처리시스템 또는 정보기기에 대한 불법 접근으로 개인정보가 유출된 경우
    - 예외
        - **유출된 개인정보를 회수·삭제 등으로 권익 침해 가능성이 현저히 낮아진 경우 신고하지 않을 수 있음**
- 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공 (공유를 포함한다. 이하 같다)할
    - 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우

    - 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
    - 오답 : 정보주체와의 불가피함
- **클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률**
    - 서비스 중단이나 침해사고, 개인정보 유출 등이 발생한 경우 **클라우드컴퓨팅서비스 제공자는 우선적으로 해당 사실을 '이용자'에게 지체 없이 통지해야 하는 의무**
    - **과학기술정보통신부장관에게 직접 신고(통지)해야 하는 의무는 개인정보 유출 등 이용자 정보가 유출된 경우, 즉시 알린다.**
    - **사전예고 없이 서비스가 중단된 경우에도, 우선적으로 이용자에게 통지**해야 하며, 천재지변 등 불가피한 사유로 이용자 통지가 곤란한 경우에만 장관에게 통보하는 예외적 절차가 있다. 무조건 장관에게 보고하지 않음
- **수집한 개인정보를 파기 방법 중, 하이래밸은 기술적 한계가 있어서, 쉽게 복구되므로 사용하면 안됨. 로우레벨로 포맷해야한다. (로우레벨 포맷**: 디스크 섹터를 물리적으로 초기화해 데이터 복구를 방지)
    - 하이레벨 포맷으로 파기할 경우 **"개인정보 미파기"로 간주**되어, **3천만 원 이하의 과태료**가 부과
- 업무연속성계획(BCP)의 접근 5단계 방법론
    - 프로젝트의 범위•설정•기획 > 사업영향평가 -> 복구전략개발 〉 복구계획수립 > 프로젝트의 수행 테스트 및 유지보수
    - 업무 연속성 계획(BCP, Business Continuity Plan)은 자연재해, 시스템 장애, 사이버 공격, 팬데믹 등 각종 재난이나 비상 상황이 발생해도 기업의 핵심 업무가 중단되지 않도록 **사전에 준비하는 종합적인 대응 계획**
- 위험관리
    - 조직의 정보자산을 보호하기 위하여 정보자산에 대한 위협과 취약점을 분석하여 비용 대비 적절한 보호 대책을 마련함으로써 위험을 감수할 수 있는 수준으로 유지하는 일련의 과정
- 위험 구성요소
    - **위험(Risk) = 자산(Asset) + 위협(Threat) + 취약점(Vulnerability)**
    - 위협 = 조직이나 시스템에 손실을 유발시킬 수 있는 **잠재적 위험 요소** 또는 **원치 않는 사건의 잠재적 원인이나 행위자** 집합이다. 해킹(해커), 악성코드, 파손 행위, 화재, 내부 직원의 실수, 시스템 결합
    - 위험 = 위협이 실제로 취약점을 이용하여 자산에 **피해를 입힐 수 있는 가능성** 또는 **손실의 가능성**

    - 위험은 단순히 위협이 존재한다고 해서 발생하는 것이 아니라, **취약점(약점)**이 존재하고, 그 취약점을 위협이 실제로 악용할 수 있을 때 발생
- 정보보호관리를 이행하기 위해서 조직은 정보보호 정책 및 조직수립, 범위설정 및 정보자산 식별, 위험관리, 구현, 사후관리활동으로 구성된 5단계의 논리적이고 체계적인 정보보호관리 프레임워크를 수립하고,기획,관리하여야 한다.
- OECD 개인정보보호 8개 원칙
    - 안정석 확보의 원칙: 개인정보 침해, 누설, 도용을 방지하기 위한 물리적 조직적• 기술적인 안전조치를 확보
- 전자서명법
    - 전자서명 검증 : 서명된 전자문서와 전자서명, 그리고 공개키(전자서명검증키)를 이용하여 해당 전자서명이 진짜(위·변조되지 않았음)임을 확인하고 서명자가 해당 전자문서에 실제로 서명했음을 확인하는 행위
    - 전자서명 검증 과정에서는 개인키의 소유 여부를 직접적으로 확인하지 않습니다.
    - 송신자(서명자)의 고유한 정보(예: 개인키)**를 사용하여 서명을 생성
    - 전자서명은 송신자의 신원을 보장하고, 서명 행위의 부인을 방지하기 위해 **송신자만이** 소유한 개인키 등 송신자 정보에 의존 (수신자가 아님)
    - 기억장소에 전자서명의 복사본을 유지하는 것이 실용적이어야 한다.
- 정보보호 위원회
    - 조직 내 정보보호 정책, 표준, 대책, 실무 및 절차 등에 대해 **심의·의결하고, 경영진에게 보고하는 역할**을 담당
    - 정보보호 관련 주요 사안에 대해 **검토, 승인, 의사결정**을 수행하는 조직 내 **의사결정기구**
    - 오답 : **독립적인 입장에서 관리자에게 보증 —> 이건 감사팀 또는 외부 감사인 역할**
- 해시함수가 적용되는 분야
    - 전자서명
    - 메시지인증
    - 패스워드기반 암호화
    - 오답 : 압축은 아님
    - 해시함수 h와 주어진 입력값 x에 대해 h(x)=h(x')을 만족하는 x'(tx)를 찾는 것이 계산적으로 불가능한 것을 **두번째 역상저항성**이라 한다.

- 강한 충돌 저항성이란?
  - **암호학적 해시 함수에서 서로 다른 두 입력값 X, Y에 대해 H(X) = H(Y)가 되는 경우(충돌)를 찾는 것이 계산적으로 매우 어려워야 한다**는 성질
- 약한 충돌 저항성이란?
  - "특정 입력 X가 주어졌을 때, H(X) = H(Y)가 되는 X ≠ Y를 찾는 것이 어렵다"는 성질로, 강한 충돌 저항성보다 요구 조건이 약합니다
- 동형(Homomorphic) 암호
  - 평문에 대한 연산을 수행하여 암호화한 결과와 암호문에 대한 연산을 수행한 결과가 동일한 암호방식으로, 암호화된 데이터를 복호화하지 않고 데이터에 대한 연산이 가능하다. 금융, 의료분야에서 개인정보에 대한 빅데이터 처리를 위해 유용한 암호화 방식이다.
- 블록체인 암호화
  - 해시 함수(무결성), 공개키 암호화**(비대칭키 암호화)(신원 확인과 부인방지)**, 전자서명(거래 위조와 변조를 막고, 거래의 신뢰성을 높인다) 등 암호학적 기법을 활용해 데이터의 위·변조 방지, 신원 인증, 거래 부인방지, 네트워크 합의 등을 구현하는 기술
  - 블록체인은 중앙 기관 없이도 안전하고 신뢰할 수 있는 분산 시스템을 구축할 수 있습니다
- 사전(Dictionary)
  - 사용자는 기억하기 쉬운 단어를 패스워드로 사용할 가능성이 높다. 이런 이유로 공격자는 패 스워드로 사용될 가능성이 높은 단어를 적절히 선별할 경우 패스워드 공격의 성공 확률을 높 일 수 있으며, 이렇게 선별된 단어 모은 것
- 이산대수 문제에 기반한 공개키 알고리즘
  - Diffie-Hellman
    - 키 사전 분배 방식은 Diffie-Hellman의 키 교환 방식을 응용한 방식으로 이산대수문제를 기반으로 구성된다. 키 분배 센터는 큰소수 P를 선정하고 가입자는 개인키를 선정하여 공개키를 계산하여 공개한다.
    - 양자 간에 완성된 키를 교환하지 않고, 서로가 주고받은 특정 정보로 양자가 동일한 키를 계 산하여 키를 분배한다.

Diffie-Hellman	키 교환
ElGamal	암호화/서명

DSA	전자서명
ECDSA/ECDH	서명/키 교환
ECC	

- **메시지 인증 코드의 구조적 제약사항에 따른 재전송 공격을 막는 방법**
  1. **Sequence Number (순차 번호)**
     - 각 메시지에 고유한 순차 번호를 할당합니다.
     - 수신측은 이 번호를 검증하여 중복된 번호가 오면 재전송으로 판단합니다.
     - 예: TCP 프로토콜에서 패킷 순서 관리
  2. **Nonce (일회용 난수)**
     - 매 세션마다 새로운 난수를 생성하여 메시지에 포함시킵니다.
     - 이미 사용된 Nonce가 재전송되면 시스템이 차단합니다.
     - 예: OTP(일회용 비밀번호)
  3. **Timestamp (타임스탬프)**
     - 메시지 생성 시간을 기록하고, 수신측에서 유효 시간 범위를 검증합니다.
     - 예: 5분 이내의 메시지만 허용하는 경우, 오래된 메시지는 자동 폐기
  4. **오답 : Hash (해시) - 해시는 재전송 공격을 막을 수 없다.**
     - 메시지의 무결성을 보장하기 위해 해시값을 생성하지만, **재전송 자체를 차단하지는 않습니다**.
     - 재전송된 메시지의 해시값이 동일하면 무결성 검증을 통과하므로 공격에 취약합니다.
     - 예: HMAC은 무결성 검증은 가능하지만, 재전송 방지에는 추가 메커니즘 필요
- 확산
  - Shannon은 순환과 대치를 반복적으로 사용하여 평문과 암호문 사이의 관계 파악을 어렵게 만드는 합성암호를 소개하며, 암호문의 각각의 비트나 문자가 평문의 모든 비트나 특정 비트 에 종속적으로 결정되어 암호문에 대한 통계적인 테스트를 통하여 평문을 찾고자 하는 공격 자를 좌절시키는 개념을 소개하였다.

기타

- RTP(Real-time Transport Protocol, 실시간 전송 프로토콜)

- 네트워크에서 오디오, 비디오 등 다양한 미디어 데이터를 한 엔드포인트에서 다른 엔드포인트로 실시간으로 전송하기 위해 사용되는 표준 프로토콜입니다 TP는 주로 인터넷 전화(VoIP), 영상 회의, 인터넷 방송, 스트리밍 서비스 등 실시간 멀티미디어 데이터 전송에 널리 활용
- 전송 계층 프로토콜로 주로 **UDP** 위에서 동작하며, 빠른 데이터 전달을 우선시함
- RTCP(RTP Control Protocol)와 함께 사용되어 전송 품질 모니터링 및 세션 제어 기능 제공
- 국제 인터넷 표준화 기구(IETF)에 의해 표준화되었으며, RFC 3550에 정의

- **2024년 3월 개정 개인정보보호법 핵심 내용**
  - 인공지능(AI)을 이용한 자동화된 결정(예: 신용평가, 채용)이 개인의 권리·의무에 중대한 영향을 미치는 경우, 정보주체는 해당 결정을 거부하거나 설명을 요구할 수 있음
    - **특징**:
      - **거부권**: AI 시스템의 결정 결과를 수락하지 않을 권리 보장.
      - **설명 요구권**: 결정 근거, 알고리즘 작동 방식 등을 요청 가능
  - **개인정보보호책임자(CPO) 자격 강화**
    - 연 매출 1,500억 원 이상 기업 중 100만 명 이상 개인정보 처리자 또는 5만 명 이상 민감정보 처리자
    - CPO는 **독립적 역할** 수행이 가능한 경력자로, 이해관계 충돌 방지를 위해 내부 감사·법무 부서 소속 금지
  - **개인정보 국외 이전 규정 완화**
    - 기존에는 **정보주체 동의**만 허용 → 변경) **국제기구 또는 국가의 보호 수준 인정** 시 추가 이전 가능
    - 예: EU GDPR과 동등한 수준의 국가로 이전 가능
  - **생성형 AI(GenAI)**
    - 대규모 데이터 학습을 통해 텍스트, 이미지, 코드 등 **새로운 콘텐츠를 생성**하는 인공지능 기술
    - **주요 모델**:
      - **LLM(대규모 언어 모델)**: ChatGPT, GPT-4 등
      - **GAN(생성적 적대 신경망)**: 이미지·동영상 생성

- **악용 사례**:
  - **딥페이크**: 실제와 유사한 가짜 영상 생성
  - **사회공학 공격**: AI가 생성한 신뢰도 높은 피싱 메일·문서
  - **코드 생성**: 악성코드 자동 생성
- **대응 방안**:
  - **DLP(데이터 유출 방지)**: 민감 정보 업로드 차단
  - **AI 탐지 기술**: 생성 콘텐츠의 위조 여부 식별

◦ AI 기반 공격

- **딥페이크(Deepfake) 공격**
  - **설명**: AI를 활용해 실제 인물의 얼굴, 음성, 행동을 합성하여 가짜 영상이나 오디오를 제작하는 기술입니다.
  - **특징/위협**: 유명인이나 임직원을 사칭한 영상·음성으로 피싱, 사기, 사회적 혼란 유발 등 다양한 공격에 활
- **AI 기반 피싱(Phishing) 및 BEC(Business Email Compromise)**
  - **설명**: 생성형 AI 또는 챗봇을 이용해 개인화된 피싱 이메일, 문자, 메시지를 자동으로 생성하고, 임직원 사칭(BEC) 공격에 활용합니다.
  - **특징/위협**: FraudGPT, WormGPT 등 AI 피싱 도구로 더욱 정교하고 대규모의 공격이 가능해졌으며, 공격 성공률이 높아집니
- **적응형 멀웨어(Adaptive Malware)**
  - **설명**: AI가 보안 시스템의 탐지 패턴을 학습하여, 탐지를 우회하거나 환경에 맞춰 스스로 변형하는 악성코드
  - **특징/위협**: 실시간 데이터 분석을 통해 탐지 회피, 자동화된 변종 생성 등으로 방어가 어려워집니다
- **자동화된 취약점 탐지 및 공격**
  - **설명**: AI가 시스템, 네트워크, 소프트웨어의 취약점을 자동으로 분석·탐지하고, 최적의 공격 시나리오를 도출합니다.
  - **특징/위협**: 공격 준비 및 실행 속도가 빨라지고, 기존에 알려지지 않은 취약점(제로데이)까지 노릴 수 있습니다
- **하이브리드 공격(랜섬웨어+DDoS)**

        - **설명**: AI가 네트워크 취약점 분석, 공격 타이밍 최적화 등으로 DDoS(분산 서비스 거부)와 랜섬웨어를 결합해 복합적으로 공격합니다.
        - **특징/위협**: 서비스 마비 후 데이터 암호화, 금전 요구, 추가 협박 등 다중 피해를 유발합니다
    - **사회공학적 해킹**
        - **설명**: AI가 특정 집단의 언어, 문화, 심리까지 분석해 신뢰를 유도하는 맞춤형 공격(예: 피싱, 사칭, 가짜 뉴스 유포 등)을 수행합니다.
        - **특징/위협**: 공격 대상의 특성에 맞춘 정교한 접근이 가능해져 성공률이 높아집니다
    - **악성코드 자동 생성 및 확산**
        - **설명**: AI가 다양한 악성코드(바이러스, 트로이목마 등)를 자동으로 생성하고, 확산 경로를 최적화합니다.
        - **특징/위협**: 전문 지식이 부족한 공격자도 손쉽게 악성코드를 제작·배포할 수 있습니다

1. 기존의 암호키를 이용하여 새로운 암호키를 생성하는 방법을 키 갱신이라고 한다.
2. 기존의 암호키와는 독립적인 방법으로 새로운 암호키를 생성하는 방법을 키 교체라고 한다.
3. 갱신된 암호키가 노출된 경우, 갱신되기 이전의 암호키에 대한 정보는 노출되지 않으므로, 기존의 암호키가 노출되면 노출된 암호키를 변경하기 위해 키 갱신을 사용한다.
4. 암호키의 노출이 확인되거나, 노출의 위협이 있는 경우 혹은 암호키 유효 기간의 만료가 가까워지는 경우 암호키를 안전하게 변경해야 하며, 암호키를 변경한 이후에는 기존의 암호키를 정지단계로 전환해야 한다.

- 국내대리인의 필수 공개 정보 (국외사업자가 국내대리인 지정했을때)
    - 법인명, 대표명, 주소, 이메일
    - 오답 : 고객센터 연락처
- 주요정보통신기반시설을 지정할때 고려사항
    1. **관리기관 업무의 국가사회적 중요성**
    2. **업무의 정보통신기반시설에 대한 의존도**
    3. **다른 정보통신기반시설과의 상호연계성**
    4. **침해사고 발생 시 국가안전보장·경제사회적 피해 규모 및 범위**

5. **침해사고 발생 가능성 또는 복구 용이성**
    - 오답: 개인정보 보유 건수 (이건 필요없음)

- 위험평가방법 중 기준선 접근법
    - 최소 보호수준(베이스라인)을 기준으로 한다.
    - **시간·비용 절감 효과가 있다: 조직의 자산, 위협, 취약점 등을 개별적으로 상세 분석하지 않고, 공통적으로 필요한 보호대책을 일괄 적용하므로**
    - **체크리스트 활용**
    - 소규모 조직에 적합
    - **과보호·부족보호 가능성이 있다**
- **CTCPEC (시스템 보안평가 기준)**
    - 기능성(Functionality)과 보증성(Assurance) 요구사항으로 구성
    - **기능 기준**: 비밀성(Confidentiality), 무결성(Integrity), 가용성(Availability), 책임성(Accountability) 등 4가지 보안 목표를 명확히 제시
    - **보증 평가 등급**: T0~T7까지 총 8단계로 세분화하여, 각 등급별로 구조, 개발환경, 개발증거, 운영환경, 보안환경, 보안시험 등 6가지 요구사항을 평가
- TCSEC은 오렌지북, ITSEC은 유럽
- **개인정보 : 생존한 개인에 대한 정보임(사망한 개인은 포함안됨)**
- ISO27014 : 정보보호 거버넌스 국제 표준이다
    - ISO/IEC 27001은 정보보안경영시스템(ISMS)에 대한 국제 표준
- **정보의 수집·가공·저장·검색·송신·수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단인 정보보호 의 목적**
    - 기밀성, 무결성, 가용성
- **정보보호의 예방대책**
    - 관리적 예방대책: 조직의 정책, 절차, 규정, 표준화, 인력 관리 등 제도적·관리적 측면에서의 보안 대책 (문서처리 순서 표준화)
    - 기술적 예방대책: 시스템, 네트워크, 소프트웨어 등 기술적 수단을 활용한 보안 대책 (암호화, 방화벽, 침입차단, VPN 등), 패스워드 안전한것으로 강제 사용
- 개인정보보호 법령에 따른 영상정보처리기기(CCTV) 설치·운영 안내판에는 다음과 같은 사항을 기재해야 합니다.

- 설치 목적, 설치 장소. 촬영 범위 및 시간, 관리책임자(또는 담당부서)의 연락처

- 위험분석 방법

  1. 정량적 분석
     ① 과거자료 분석법 : 과거자료를 통해 위험발생 가능성 예측,
     ② 수학공식법 : 위험 정량화하여 간결하게 표현가능, 기대손실을 추정하는 자료의 양이 적다는 단점
     ③ 확률분포법 : 미지의 사건 추정시 확률적 편차를 이용하여 최저, 보통, 최고 위험평가 예측, 정확성 낮음
     ④ 점수법 : 위험발생 요인에 가중치를 두어 위험 추정, 소요 시간 적고 분석해야 할 자원 양 적음, 정확도 낮음

  2. 정성적 분석
     ① 델파이법 : 전문가 집단이 위험 분석 및 평가, 정확도 낮음
     ② 시나리오법 : 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거, 적은 정보를 가지고 전반적인 가능성 추론, 이론적 추측에 불과하고 정확도 등이 낮음
     ③ 순위결정법 : 비교우위 순위결정표에 위험항목들의 서술적 순위 결정(우선순위 도출), 소요시간 및 분석 자원 양 적다는 장점, 정확도 낮음
     ④ 퍼지 행렬법 : 정성적인 언어로 표현된 값을 사용하여 기대손실을 평가

- 디지털 포렌식

  - 연계보관성의 원칙

    - **증거물의 획득, 이송, 분석, 보관, 법정 제출** 등 모든 단계에서 **각 단계별 담당자와 책임자를 명확히 기록·관리**하여, 증거물이 처음부터 끝까지 어떻게, 누구에 의해, 어떤 방식으로 처리되었는지 추적이 가능하도록 하는 원칙

  - 정당성 : 적법절차 수집. 위법수집증거배제법칙

- 클라우드컴퓨팅 전담기관

  - 한국지능정보사회진흥원, 한국지역정보개발원, 한국인터넷진흥원

- **과학기술정보통신부장관이 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 법에 정한 기준에 적합한지에 관하여 인증을 할 수 있도록 하는 정보보호 관리체계 인증(ISMS)을 명시한 법률 : 정보통신망 이용촉진 및 정보보호 등에 관한 법률**

- **CERT가 정의하는 보안사고**

  - 일반 보안사고

    - 악성 소프트웨어(웜, 바이러스, 백도어, 트로이 목마 등)에 의한 침해

    - 네트워크 및 시스템에 대한 비인가된 침해 및 시도

        - 일반 자산의 도난, 분실, 파손 및 파괴
        - 보안취약점으로 정보 시스템의 정상적인 운영에 지장을 초래한 사건
        - 정보의 비인가자 사용, 승인되지 않은 개인에게 정보 접근 허용
        - 비인가자의 보안 구역 접근 시도
        - 조직이나 업무 등에 파급효과가 없는 단순히 개인에 국한된 사고는 보안사고의 - 범주에서 제외하여 단순사고로 처리 가능
    - 중대 보안사고의 정의
        - 정보시스템이 비인가 접근에 의해 변조, 파괴되어 정상적인 서비스를 제공하지 못하는 경우
        - 중요도 등급이 1등급(예 : 중요도 1/2/3 등급)인 정보자산 또는 비밀문서가 외부로 누출된 경우
        - 정보자산의 오용으로 인하여 조직의 대외 이미지에 중대한 손상을 끼친 경우
        - 관련 법규 및 규정 저촉으로 인하여 사회적 물의를 일으키는 경우
        - 기타 고의 또는 과실에 의해 조직의 정상적 업무에 심각한 지장을 초래하는 경우
        - 보안 장치의 변경이나 파괴 : 출입보안, 침입탐지시스템, 잠금장치, 보안 카메라 등
    - **정보보호관리체계 인증 범위 내 필수적으로 포함해야 할 자산**
        - DMZ 구간 내 정보시스템
        - 개발서버, 테스트서버
        - 관리자 PC, 개발자 PC:
        - 오답 : ERP, DW, GroupWare
- ISMS(정보보호관리체계) 인증을 **의무적으로 받아야 하는 기관(사업자)
    - **정보통신서비스 제공자(ISP)**
    - **집적정보통신시설 사업자(IDC)**
    - **매출액 또는 이용자 수 기준 충족 사업자**
        - **정보통신서비스 부문 전년도 매출액이 100억 원 이상인 자**
        - **전년도 일일평균 정보통신서비스 이용자 수가 100만 명 이상인 자**
        - **연간 매출액 또는 세입이 1,500억 원 이상인 자** 중 다음에 해당하는 경우