ISO

OSI 7계층

물리 계층: 실제 장치를 연결

데이터 링크 계층: 신뢰성 있는 전송을 보장

네트워크 계층: 경로를 찾아주는

전송 계층: 양 끝단의 사용자가 신뢰성 있는 데이터를 주고받게

세션 계층: 통신을 관리하는 방법을 제공

표현 계층: 코드 간 번역

응용 프로그램 계층: 일반적인 응용 서비스를 수행

CAT 1 아날로그

CAT 3 이더넷

CAT 7 10Gb 이더넷

UTP 전선과 피복, 절연의 구리선이 서로 꼬여

FTP 알루미늄 은박이 네 가닥의 선을 감싸, 공장 배선용

STP 연선, 외부의 노이즈를 차단하거나 전기적 신호의 간섭에 탁월

랜 케이블은 UTP 케이블 중 CAT 5 또는 CAT 6에 해당하는 선에 RJ 45 커넥터를 사용

MAC 주소는 ipconfig /all 명령으로 확인

MAC 주소는 12개의 16진수로 구성

앞쪽 6개의 12진수는 네트워크 카드를 만든 회사

뒤쪽 6개의 12진수는 시리얼

데이터 링크 계층의 대표적인 네트워크 장치는 스위치

MAC 계층에서 동작하는 대표적인 프로토콜은 이더넷

스위치 메모리에 포트별로 MAC 주소가 매칭된 테이블 존재

스위치는 IP 정보를 네트워킹에 활용하지 않음

1단계 전: 패킷 수신 컴퓨터의 MAC 주소 확인

1단계: 패킷 수신 컴퓨터의 MAC 주소를 적어 스위치로 보냄

2단계: 패킷의 MAC 주소를 확인한 후 해당하는 포트로 패킷을 흘려보냄

3단계: 해당하는 포트에 연결된 컴퓨터로 패킷이 흘러감

IP 주소는 8비트의 수 4개로 구성

TCP도 포트라는 주소를 가지고 있음

21 FTP

53 DNS

80 HTTP

3계층과 4계층 정보는 netstat -an 명령으로 확인

3-웨이 핸드셰이킹

연결 과정

클라이언트 SYN 보냄

서버 SYN+ACK 보냄

클라이언트 ACK 보냄

연결 해제 과정

클라이언트 FIN 보냄

서버 ACK 보냄

서버 FIN 보냄

클라이언트 ACK 보냄

서비스 거부 공격

취약점 공격형

TearDrop

시퀀스 넘버와 길이를 조작

랜드 공격

출발지 IP 주소와 목적지 IP 주소의 값을 똑같이 만듦

조작된 IP 주소의 값은 공격 대상의 IP 주소

자원 고갈 공격형

죽음의 핑 공격

초기의 DoS 공격

패킷을 최대한 길게

SYN 플러딩 공격

존재하지 않는 클라이언트

HTTP GET 플러딩 공격

HTTP의 GET 메소드로 특정 페이지를 무한대로 실행

HTTP CC 공격

캐시 기능을 사용하지 않도록 함

동적 HTTP 리퀘스트 플러딩 공격

차단 기법을 우회하고 웹 페이지를 요청

스머프 공격

패킷을 확장해 서비스 거부 공격

메일 폭탄 공격

스팸 메일

분산 서비스 거부 공격

공격자

마스터

핸들러

에이전트

데몬

스니핑 공격: 데이터 속에서 정보를 찾는 것

랜 카드의 프리미스큐어스 모드를 이용해 필터링을 해제

스니핑 공격의 탐지

ping을 이용한 탐지

ARP를 이용한 탐지

DNS를 이용한 탐지

유인을 이용한 탐지

ARP watch를 이용한 탐지

스푸핑 공격

ARP 스푸핑은 MAC 주소를 속이는 것

IP 스푸핑 공격은 트러스트 관계를 이용해야 함

ICMP 리다이렉트 공격

DNS 스푸핑 공격

세션 하이재킹 공격

세션 하이재킹은 세션 가로채기라는 뜻

AP 보안

물리적인 보안 및 관리자 패스워드 변경

SSID 브로드캐스팅 금지

바이러스

웜

트로이 목마

PUP

POST

CMOS

O/S 위치 정보 로드

암호형 바이러스

은폐형 바이러스

다형성 바이러스

매크로 바이러스

차세대 바이러스

매스 메일러형 웜

메일로 전파

SMTP 서버의 네트워크 트래픽 증가

시스템 공격형 웜

O/S 고유 취약점을 이용

과다한 TCP/135, 445 트래픽이 발생

네트워크 공격형 웜

특정 네트워크나 시스템에 대해 SYN 플러딩이나 스머프와 같은 DoS 공격을 수행

기호주의

연결주의

퍼셉트론

지도 학습은 분류나 회귀

비지도 학습은 군집과 차원 축소

강화 학습은 시행착오와 지연 보상

학습을 하는 시스템을 에이전트라고 부름

회피 공격

학습 과정에서 무작위의 오류가 존재하는 노이즈를 고의적으로 추가

중독 공격

악의적인 데이터를 이용해 인공지능 시스템이 오작동

전도 공격

인공지능에서 사용하는 데이터 자체를 탈취

나이브 베이즈 분류기

최초의 스팸 메일 솔루션

BERT

구글에서 개발한 NLP 사전 훈련 기술

전문가 시스템

기호주의의 한 분야

사전 대응 -> 침해 사고 발생 -> 사고 탐지 -> 대응 -> 제거 및 복구 -> 후속 조치 및 보고

침해 대응 체계 점검 사항

보안 정책에 대해 알고 있는가?

침해 사고 발생 시 누구에게 보고하고 언론 대응은 어떻게 해야 하는지 충분히 인지하고 있는가?

침해 사고 발생 시 처리해야 할 기술적 절차에 대해 충분히 이해하고 있는가?

정해진 절차에 따라 주기적으로 훈련을 수행하고 있는가?

침해 사고 식별 과정에서 확인할 사항

발생 시점은 언제인가?

누가 침해 사고를 발견하고 보고했는가?

어떻게 발견되었는가?

발생 범위는 어느 정도인가? 다른 곳이 손상되지는 않았는가?

기업의 서비스 능력이 손상되었는가?

공격자의 규모와 공격 능력은 어느 정도인가?

침해 사고 보고서 항목

침해 사고 발생 일지

사고 원인

초기 대처

복구 현황

대처 오류 및 해결 방안

디지털 포렌식

포렌식의 증거

직접 증거

간접 증거

인적 증거

물적 증거

포렌식으로 수집된 증거는 간접 증거로 정확히 표현하면 전문 증거이다

기본 원칙

정당성의 원칙

재현의 원칙

신속성의 원칙

연계 보관성의 원칙

무결성의 원칙

포렌식 수행 절차

수사 준비

증거물 획득

보관 및 이송

분석 및 조사

보고서 작성

최량 증거 원칙

포렌식 증거를 관리할 때는 최량 증거 원칙을 따름

보안 거버넌스: 조직의 보안을 달성하기 위한 구성원 간의 지배 구조

구현의 어려움

조직 구성의 어려움

성과 측정의 어려움

조직의 무관심

구현 요건

전략적 연계

위험 관리

자원 관리

성과 관리

가치 전달

ISMS: 기업이 민감한 정보를 안전하게 보존하도록 관리할 수 있는 체계적인 경영 시스템

PDCA: 계획, 수행, 점검, 조치를 반복적으로 순환하여 수행

계획: ISMS 수립 단계

수행: ISMS 구현과 운영 단계

점검: ISMS 모니터링, 검토 단계

조치: ISMS 관리와 개선 단계

K-ISMS: ISO 27001의 국제 표준을 포함하고 우리나라 상황에 맞는 보안 요건을 강화

정보 보안 책임자

적정 예산 확보하여 지원

정보 보안 관리자

정보 보안 업무 기획, 점검

정보 보안 담당자

전체 시스템의 보안 관리

보안 조직을 구성할 때 고려 사항

기업의 크기

시스템 환경

기업의 조직 및 관리 구조

운영 사이트의 수와 위치

사이트 간의 상호 연결 형태

IT 예산

접근 제어 모델

기밀성과 무결성 확보가 접근 제어의 주목적

임의적 접근 제어 모델

정보 소유자가 정보의 보안 레벨을 결정하고 접근 제어 설정

강제적 접근 제어 모델

중앙에서 정보를 수집, 분류하여 접근 제어 수행

벨 라파둘라 모델

정보의 기밀성에 따라 상하 관계가 구분된 정보를 보호

비바 모델

정보의 무결성을 높일 때 사용

RBAC

사람이 아닌 직책에 권한 부여

최소 권한

필요한 권한 이상을 부여받으면 안 된다는 개념

직무 분리

하나의 업무 절차를 두 사람 이상이 수행하도록 업무를 분리

TCSEC

오랜 역사를 가진 인증으로 지금까지도 보안 솔루션을 개발할 때 기준

ITSEC

유럽에서 발전한 보안 표준

기밀성만을 강조한 TCSEC와 달리 무결성과 가용성을 포괄하는 표준안

CC

TCSEC와 ITSEC는 CC라는 기준으로 통합되고 있음

개인 정보란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보를 말한다

PIMS

기관 및 기업이 개인 정보 보호 관리 체계를 갖추고 체계적이고 지속적으로 보안 업무를 수행하는지 심사하여 기준을 만족하면 인증을 부여하는 제도