Chapter 03 네트워크 보안

**01. 네트워크의 이해**

OSI 7계층: 국제표준화기구(ISO)는 다양한 네트워크 간의 호환을 위해 OSI 7계층이라는 표준 네트워크 모델을 만듦

1계층 물리 계층(physical layer): 실제 장치를 연결하기 위한 전기적·물리적 세부 사항을 정의한 계층

2계층 데이터 링크 계층(data link layer): 두 지점 간의 신뢰성 있는 전송을 보장하기 위한 계층

3계층 네트워크 계층(network layer): 여러 개의 노드를 거칠 때마다 경로를 찾아주는 계층

4계층 전송 계층(transport layer): 양 끝단에 사용자가 신뢰성 있는 데이터를 주고받게 하여 상위 계층이 데이터 전달의 유효성이나 효율성을 신경 쓰지 않게 해주는 계층

5계층 세션 계층(session layer): 양 끝단의 응용 프로세스가 통신을 관리하는 방법을 제공하는 계층

6계층 표현 계층(presentation layer): 코드 간 번역을 담당하는 계층

7계층 응용 프로그램 계층(application layer): 응용 프로세스와 직접 관계하여 일반적인 응용 서비스를 수행하는 계층

**물리 계층(1계층)**

- 시스템 간의 연결을 의미하는 것으로 전자 파장을 전달하는 공간 또는 물질 자체가 물리 계층임

- 물리 계층이 쓰이는 케이블을 데이터의 속도에 따라 분류 이때 CAT 1부터 CAT 7은 케이블의 굵기와 구리선의 가닥수로 구분

CAT 최대 속도 용도

CAT 1 1Mbps 미만 아날로그 음성(일반적인 전화 서비스)

CAT 3 16Mbps 이더넷상의 데이터 및 음성 전송에 사용

CAT 7 10Gbps 10Gb 이더넷

- 케이블 내 구리선의 보호 방법이나 꼬임 방법에 따라서 케이블을 분류하기도 함

케이블 선 설명

UTP 제품 전선과 피복만으로 구성되어 있으며, 두 선 사이의 전자기 유도를 줄이기 위해 절연의 구 리선이 서로 꼬여 있다

FTP 알루미늄 은박이 네 가닥의 선을 감싸고 있으며, UTP보다 절연 기능이 탁월하여 공장배선용으로 많이 사용한다

STP 차폐재는 접지 역할을 하므로 외부의 노이즈를 차단하거나 전기적 신호의 간섭에 탁월하다

- 인터넷에 쓰는 랜 케이블은 UTP 케이블 중 CAT 5 또는 CAT 6에 해당하는 10/100/1000 BASE-T(IEEE802.3) 선에 RJ 45 커넥터를 사용

**데이터 링크 계층(2계층)**

- 두 포인트(Point to Point) 간 신뢰성 있는 전송을 보장하기 위한 계층

- 상호 통신을 위해 할당 받는 MAC 주소는 ipconfig /all 명령으로 확인할 수 있음

- MAC 주소는 총 12개의 16진수 숫자로 구성

앞쪽 6개의 16진수는 네트워크 카드를 만든 회사를 나타내는 것으로 OUI라고 함

뒤쪽 6개의 16진수는 각 회사에서 임의로 붙이는 일종의 시리얼을 나타내는 것으로 Host Identifier라고 함

- 데이터링크 계층의 대표적인 네트워크 장비는 스위치, MAC 계층에서 동작하는 대표적인 프로토콜은 이더넷(Ethernet)

스위치의 동작 원리

- 스위치 메모리에 포트별로 MAC 주소가 매칭된 테이블 존재, 매칭 정보 업데이트 가능

- 일반적으로 잘못 이해할 수 있는 스위치의 구조

스위치 메모리 테이블에 네트워크 계층 정보인 IP 주소와 MAC 주소가 매칭되어 저장된다고 잘못 생각하는 경우 많음

스위치(데이터 링크 계층 장비)는 IP정보(네트워크 계층)를 네트워킹에 활용하지 않음

- 패킷 송신 컴퓨터 -> 패킷 수신 컴퓨터까지의 흐름 메커니즘

1단계 전: 패킷 송신 컴퓨터가, 패킷 수신 컴퓨터의 MAC 주소 확인

1단계: 패킷의 목적지 MAC 주소 부분: 패킷 수신 컴퓨터의 MAC 주소를 적어 스위치로 보냄

2단계: 스위치에서 2번 포트로 수신된 패킷의 목적지 MAC 주소가, 3번 포트와 연결된 컴퓨터임을 메모리에서 확인 후, 패킷을 3번 포트로 흘려 보냄

3단계: 3번 포트에 연결된 컴퓨터로 패킷이 흘러감

**네트워크 계층(3계층)**

- 여러 개의 노드를 거칠 때마다 경로를 찾아주는 역할을 하는 계층

- 다양한 길이의 데이터를 네트워크를 통해 전달하며 그 과정에서 라우팅, 흐름 제어, 세그멘테이션, 오류 제어 등을 수행

- 네트워크 계층에서 여러 개의 노드를 거쳐 경로를 찾기 위한 주소는 IP로 대표됨

- IP 주소는 8비트의 수 4개로 구성(32자리의 2진수로 8자리마다 점을 찍어 구분)

- IP 주소는 A, B, C, D, E 클래스로 구분

A 클래스: 첫 번째 자리가 네트워크 주소, 나머지 세 자리는 호스트 주소

B 클래스: 두 번째 자리까지 네트워크 주소, 나머지 두 자리는 호스트 주소

C 클래스: 세 번째 자리까지 네트워크 주소, 나머지 두 자리는 호스트 주소

네트워크 클래스의 구분

시작 주소 클래스 설명

0 A 클래스 00000000번부터 01111111(127)번까지의 네트워크이다

네트워크 크기가 가장 큼

10 B 클래스 10000000(128)번부터 10111111(191)번까지의 네트워크이다

110 C 클래스 11000000(192)번부터 11011111(223)번까지의 네트워크이다

네트워크 크기가 가장 작음

1110 D 클래스 11100000(224)번부터 1110111(239)번까지의 네트워크이다

멀티미디어 방송을 할 때 자동으로 부여된다

E 클래스 11110000(240)번부터 1111111(255)번까지의 네트워크이다

테스트를 위한 주소 대역이며 사용하지 않는다

- 사설 IP 주소가 필요한 이유

기존의 IP 주소가 부족하므로, 서브넷(외부에 노출할 필요가 없는 컴퓨터)에 사설 IP 주소를 부여해, IP 주소 고갈을 해결하기 위함

- 클래스별 사설 네트워크 범위

클래스 지정된 사설 네트워크

A 클래스 10.0.0.0~10.255.255.255

B 클래스 172.16.0.0~172.31.255.255

C 클래스 192.168.0.0~192.168.255.255

- 2계층과 3계층에서의 패킷 흐름(OSI 7계층에 따른 패킷 흐름)

시스템에서 송신 패킷이 처음 생성되어, 스위치를 지나 라우터를 거쳐 인터넷으로 가는 과정

- 네트워크 계층에서의 패킷 전달 구조

1) 출발지의 IP와 MAC 주소가 기록됨

2) 목적지 IP 주소 입력

3) 목적지 MAC 주소에는 랜을 벗어나기 위한 가장 일차적인 목적지, 즉 게이트웨이의 MAC 주소

4) 라우터에서 사용한 2계층 정보를 벗겨냄

5) 다음 라우터까지의 2계층 정보를 패킷에 덧씌움

**전송 계층(4계층)**

- 양 끝단(End to end)의 사용자들이 신뢰성 있는 데이터를 주고받을 수 있도록 함

- 상위 계층이 데이터 전달의 유효성이나 효율성을 신경 쓰지 않도록 해 줌

- 가장 잘 알려진 전송 프로토콜은 TCP(Transmission Control Protocol)

- TCP도 포트라는 주소를 가지고 있음

MAC 주소가 네트워크 카드의 고유 식별자, IP가 시스템 주소라면

포트는 시스템에 도착한 수, 패킷이 찾아갈 응용 프로그램과 통하는 통로 번호로 볼 수 있음

- 시스템에서 구동되는 응용 프로그램은 네트워킹을 하기 위해 자신에게 해당되는 패킷을 식별할 필요가 있음

이때 사용하는 것이 포트이며, 포트는 0번부터 65.535번까지 존재함

- 주요 포트와 서비스

포트 서비스

21 FTP

53 DNS

80 HTTP

- 3계층과 4계층 정보는 netstat -an 명령으로 쉽게 확인할 수 있음

- 3-웨이 핸드셰이킹(3-way handshaking)

1단계: 두 시스템이 통신을 하기 전에 클라이언트는 포트가 닫힌 Closed 상태, 서버는 해당 포트로 항상 서비스를 제공할 수 있는 Listen 상태

2단계: 클라이언트가 처음 통신을 하려면 임의의 포트 번호가 클라이언트 프로그램에 할당되고, 클라이언트는 서버에 연결하고 싶다는 의사 표시로 SYN Sent 상태가 됨

3단계: 클라이언트의 연결 요청을 받은 서버는 SYN Received 상태가 되고, 클라이언트에 연결을 해도 좋다는 의미로 SYN + ACK 패킷을 보냄

4단계: 클라이언트는 연결 요청에 대한 서버의 응답을 확인했다는 표시로 ACK 패킷을 서버로 보냄

- TCP 연결 해제 과정

1단계: 통신 중에는 클라이언트와 서버 모두 Established 상태

2단계: 통신을 끊으려는 클라이언트가 서버에 FIN(Finish) 패킷을 보내고 클라이언트는 Close Wait 상태가 됨

3단계: 서버는 클라이언트의 연결 종료 요청을 확인하고 응답으로 클라이언트에 ACK 패킷을 보내면 서버도 클라이언트의 연결을 종료하겠다는 의미로 FIN 패킷을 보내고 Close Wait 상태가 됨

4단계: 클라이언트는 연결 종료를 요청한 것에 대한 서버의 응답을 확인했다는 표시로 ACK 패킷을 서버로 보냄

**세션 계층(5계층)**

- 양 끝단의 응용 프로세스가 통신을 관리하기 위한 방법을 제공

- 전송 계층이 종단 간의 논리적인 설정을 담당한다면 세션 계층은 이런 연결에 정보 교환을 효과적으로 할 수 있게 추가 서비스를 함

**표현 계층(6계층)**

- 코드 간의 번역을 담당함

- 사용자 시스템에서 데이터 구조를 하나의 통일된 형식으로 표현하며 응용 계층의 데이터 형식 차이로 인한 부담을 덜어줌

**응용 프로그램 계층(7계층)**

- 사용자나 응용 프로그램 사이에 데이터 교환이 가능하게 하는 계층

- HTTP, FTP, 터미널 서비스, 메일 프로그램, 디렉터리 서비스 등을 제공

**02. 서비스 거부 공격(DoS, Denial of Service)**

**1) 취약점 공격형**

(1) Boink, Bonk, TearDrop 공격

- 프로토콜의 오류 제어 로직을 악용해 시스템 자원을 고갈시키는 방식

TCP 패킷 안에는 각 패킷이 데이터의 어느 부분을 포함하는지 표시하기 위하여 시퀀스 넘버가 기록되어 있는데, 시스템의 패킷 재전송과 재조합에 과부하가 걸리도록 시퀀스 넘버를 속이는 공격임

즉, 공격 대상이 반복적인 재요청, 수정을 계속하게 하여, 시스템 자원을 고갈시킴

- TCP가 제공하는 오류 제어 기능

패킷 순서가 올바른지 확인

중간에 손실된 패킷이 없는지 확인

손실된 패킷의 재전송을 요구

**TearDrop**

- 패킷의 시퀀스 넘버와 길이를 조작하여, 패킷 간의 데이터 부분이 겹치거나 빠진 패킷을 전송하는 공격

- 이러한 공격에 의한 취약점은 패치를 통해 제거하는데, 과부하가 걸리거나 계속 반복되는 패킷은 무시하고 버리도록 처리함

**랜드 공격**

- 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소의 값을 똑같이 만들어서 공격 대상에게 보내는 것

- 조작된 IP 주소의 값은 공격 대상의 IP 주소임

- CPU 부하를 올려서, 시스템이 금방 지쳐버리게 만듦

- 랜드 공격의 보안 대책은 운영체제의 패치 관리나 방화벽과 같은 보안 솔루션을 이용

**2) 자원 고갈 공격형**

- 네트워크 대역폭, 시스템의 CPU, 세션 등의 자원을 소모시키는 형태

**죽음의 핑 공격**

- 시스템을 파괴하는 데 가장 흔히 쓰인 초기의 DoS 공격

- 네트워크에서 패킷을 전송하기 적당한 크기로 잘라서 보내는 특성을 이용한 공격

- 네트워크의 연결 상태를 점검하는 ping 명령을 보낼 때 패킷을 최대한 길게(최대 65,500바이트) 보냄

수백 수천 개의 패킷으로 잘게 쪼개져 보내짐

공격 대상 시스템은 대량의 작은 패킷을 수신하면서 네트워크가 마비됨

- 이 공격을 막으려면 ping이 내부 네트워크에 들어오지 못하도록 방화벽에서 ping이 사용하는 프로토콜인 ICMP를 차단해야 함

- 윈도우 95, 98, 리눅스 6.0 이하의 버전에서 유효함

**SYN 플러딩 공격**

- 네트워크에서 서비스를 제공하는 시스템에 걸려있는 사용자 수 제한을 이용한 공격

- 존재하지 않는 클라이언트가 서버별로 한정된 접속 가능 공간에 접속한 것처럼 속여 다른 사용자가 서비스를 제공받지 못하게 함

- TCP의 연결 과정인 3-웨이 핸드셰이킹의 문제점을 악용한 공격

- 공격 대응책은 SYN Received의 대기 시간을 줄이는 것

- 침입 방지 시스템과 같은 보안 시스템으로도 공격을 쉽게 차단할 수 있음

**HTTP GET 플러딩 공격**

- 공격 대상 시스템에 TCP 3-웨이 핸드셰이킹 과정으로 정상 접속한 뒤 HTTP의 GET 메소드로 특정 페이지를 무한대로 실행하는 공격

- 공격 패킷을 수신하는 웹 서버는 정상적인 TCP 세션과 정상으로 보이는 HTTP GET을 지속적으로 요청하므로 시스템에 과부하가 걸림

**HTTP CC 공격**

- HTTP 1.1 버전의 CC(Cache-Control) 헤더 옵션

- 자주 변경되는 데이터에 새로운 HTTP 요청 및 응답을 요구하기 위해, 캐시 기능을 사용하지 않도록 함

- 캐시 기능을 사용하지 않음으로 인해, 웹 서비스의 부하를 증가시키는 공격

**동적 HTTP 리퀘스트 플러딩 공격**

- 웹 방화벽을 통해 특징적인 HTTP 요청 패턴을 방어 가능함

- 이러한 차단 기법을 우회하기 위해, 지속적으로 요청 페이지를 변경하여 웹 페이지를 요청하는 공격 기법

**스머프 공격**

- ICMP 패킷과 네트워크에 존재하는 임의의 시스템으로 패킷을 확장해 서비스 거부 공격을 수행하는 것으로, 네트워크 공격에 많이 사용함

**메일 폭탄 공격**

- 메일 폭탄(mail bomb)은 스팸 메일과 같은 종류

- 메일이 폭주하여 디스크 공간을 가득 채우면 받아야 할 메일을 받을 수 없으므로 스팸 메일을 서비스 거부 공격으로 분류

**분산 서비스 거부 공격(DDoS)**

- 분산 서비스 거부 공격의 기본 구성

공격자(attacker): 공격을 주도하는 해커 컴퓨터

마스터(master): 공격자에게 직접 명령을 받는 시스템으로 여러 대의 에이전트를 관리

핸들러(handler) 프로그램: 마스터 시스템의 역할을 수행하는 프로그램

에이전트(agent): 직접 공격을 가하는 프로그램

데몬(daemon) 프로그램: 에이전트 시스템의 역할을 수행하는 프로그램

**03. 스니핑 공격**

**스니핑 공격의 원리**

- 스니핑 공격: 데이터 속에서 정보를 찾는 것으로 공격 시 아무것도 하지 않고 조용히 있는 것만으로도 충분하여 수동적 공격이라 함

- 스니핑 공격자는 가지지 말아야 할 정보까지 모두 볼 수 있어야 하므로 랜 카드의 프러미스큐어스(promiscuous) 모드를 이용해 데이터 링크 계층과 네트워크 계층의 정보를 이용한 필터링을 해제함

**스니핑 공격의 탐지**

**ping을 이용한 스니퍼 탐지**

- 의심이 가는 호스트에 네트워크에 존재하지 않는 MAC 주소를 위장해서 ping을 보내면 스니퍼 탐지 가능. 존재하지 않는 MAC 주소를 사용했으므로 스니핑을 하지 않는 호스트라면 ping request를 볼 수 없는 것이 정상이기 때문

**ARP를 이용한 스니퍼 탐지**

- 위조된 ARP request를 보냈을 때 ARP response가 오면 되돌려 보냄

- 프러미스큐어스 모드로 설정된 것이므로 탐지 가능

**DNS를 이용한 스니퍼 탐지**

- 스니핑한 시스템의 IP 주소에 DNS의 이름 해석 과정인 Reverse-DNS lookup을 수행

- 대상 네트워크로 ping sweep를 보내고 들어오는 Reverse-DNS lookup을 감시하면 스니퍼 탐지 가능

**유인을 이용한 스니퍼 탐지**

- 가짜 아이디와 패스워드를 네트워크에 계속 뿌려서 공격자가 이를 이용해 접속을 시도하면 스니퍼 탐지 가능

**ARP watch를 이용한 스니퍼 탐지**

- ARP watch는 MAC 주소와 IP 주소의 매칭 값을 초기에 저장하고 ARP 트래픽을 모니터링하여 이를 변하게 하는 패킷이 탐지되면 알려주는 툴. 대부분의 공격 기법은 위조된 ARP를 사용하기 때문에 쉽게 탐지 가능

**04. 스푸핑 공격**

**스푸핑 공격의 종류**

**ARP 스푸핑 공격**

- ARP 스푸핑은 MAC 주소를 속이는 것

- 로컬에서 통신하는 서버와 클라이언트의 IP 주소에 대한 데이터 링크 계층의 MAC 주소를 공격자의 MAC 주소로 속여 클라이언트에서 서버로 가는 패킷이나, 서버에서 클라이언트로 가는 패킷이 공격자에게 향하게 하여 랜의 통신 흐름을 왜곡하는 공격

- 패킷 확인 후, 원래 목적지로 향하도록 다시 돌려보내어, 연결 유지시키는 공격

**IP 스푸핑 공격**

- 1) 트러스트 관계(신뢰 관계)를 맺고 있는 서버와 클라이언트를 확인한 후

- 2) 클라이언트에 서비스 거부 공격을 하여 연결을 끊음

- 3) 클라이언트의 IP 주소를 확보한 공격자는 실제 클라이언트처럼 패스워드 없이 서버에 접근함

트러스트: 서버에 미리 정보가 기록된 클라이언트가 접근하면 아이디와 패스워드 입력 없이 로그인을 허락하는 인증법

- 유닉스에서는 트러스트 인증법을 주로 사용하지만 윈도우에서는 액티브 디렉터리(Active Directory)를 사용함

- IP 스푸핑 공격 대응책은 트러스트를 이용하지 않는 것이며 트러스트를 사용하려면 트러스트로 묶는 구성 서버에 취약한 패스워드가 없어야 함

**ICMP 리다이렉트 공격**

- 네트워크 계층에서 스니핑 시스템을 네트워크에 존재하는 또 다른 라우터라고 알림으로써 패킷의 흐름을 바꾸는 공격

**DNS 스푸핑 공격**

- 실제 DNS 서버보다 빨리 DNS response 패킷을 보내어 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격

- DNS 스푸핑 공격을 막으려면 중요 서버에 대해 DNS query를 보내지 않으면 되는데 이를 위해서는 중요 접속 서버의 URL에 대한 IP를 hosts 파일에 등록해야 함

- 모든 서버의 IP를 등록하는 것은 무리이므로 모든 서버의 DNS 스푸핑을 막기는 어려움

**05. 세션 하이재킹 공격**

**세션 하이재킹**

- 세션 가로채기라는 뜻으로 세션은 사용자와 컴퓨터 또는 두 컴퓨터 간의 활성화된 상태이므로 세션 하이재킹은 두 시스템 간의 연결이 활성화된 상태, 즉 로그인된 상태를 가로채는 것

**TCP 세션 하이재킹**

- TCP의 고유한 취약점을 이용하여 정상적인 접속을 빼앗는 방법

- 서버와 클라이언트에 각각 잘못된 시퀀스 넘버를 사용해서 연결된 세션에 잠시 혼란을 준 뒤 자신이 끼어 들어가는 방식

**세션 하이재킹 대응책**

- 텔넷과 같은 취약한 프로토콜을 이용하지 않고 SSH와 같이 세션 인증 수준이 높은 프로토콜로 서버에 접속해야 함

- 또는 클라이언트와 서버 사이에 MAC 주소를 고정해야 함

**06. 무선 네트워크 공격과 보안**

**무선 랜**

- 유선 랜의 네트워크를 확장하려는 목적으로 사용되며 이를 위해서는 내부의 유선 네트워크에 APAccess Point 장비를 설치해야 함

- 확장된 무선 네트워크는 AP를 설치한 위치에 따라 통신 영역이 결정되며 보안이 설정되어 있지 않으면 공격자가 통신 영역 안에서 내부 사용자와 같은 권한으로 공격 가능

- 주요 무선 랜 프로토콜

무선과 관련된 프로토콜은 무조건 802.11로 시작

시기 프로토콜 설명

1997년 7월 802.11 최초의 무선 랜 프로토콜

1999년 9월 802.11b 와이파이라고 하며 WEP 방식의 보안을 구현한다

802.11a 와이파이5라고 하며, 전파 투과성과 회절성이 떨어짐

2003년 6월 802.11g 802.11b에 802.11a의 속도 성능을 추가한 프로토콜

2004년 6월 802.11i 802.11b 표준에 보안성을 강화한 프로토콜

2007년 802.11n 대역폭 손실을 최소화하고 최대 속도는 600Mbps

2012년 802.11ac 802.11n과의 호환성을 위해 40MHz까지 대역폭을 지원

2014년 802.11ad 대용량 데이터나 무압축 HD 비디오 등 동영상 스트리밍에 적합

**AP 보안**

- 물리적인 보안 및 관리자 패스워드 변경

AP는 전파가 건물 내에서 한정되도록 전파 출력을 조정, 창이나 외부에 접한 벽이 아닌 건물 안쪽 중심부의 눈에 쉽게 띄지 않는 곳에 설치, 설치 후에는 AP의 기본 계정과 패스워드를 반드시 재설정

- SSID 브로드캐스팅 금지

무선 랜 네트워크를 검색 시 확인할 수 있는 AP 목록에 표시된 이름이 SSID

높은 수준의 보안 권한이 필요한 무선 랜은 AP의 존재를 숨기고 SSID 브로드캐스팅을 막아 사용자가 SSID를 입력해야 AP에 접속할 수 있게 함. 이때 SSID는 AP 접근을 위한 일차적인 패스워드로 사용 가능

**무선 랜 통신의 암호화**

- WEP: 128비트 키까지 암호화 키 제공

WEP(Wired Equivalent Privacy)는 무선 랜 통신을 암호화하기 위해 802.11b 프로토콜부터 적용되기 시작, 1987년에 만들어진 RC 4(Ron’s Code 4) 암호화 알고리즘을 기본으로 사용

- WPA-PSK: WEP 방식 보안의 암호화 취약점을 해결한 암호화 방식

WAP-PSK(Wi-Fi Protected Access Pre-Shared Key) WEP 방식 보안의 문제점을 해결하기 위해 만들어짐

WPA 규격은 WPA-개인과 WPA-엔터프라이즈로 각각 규정. WPA-개인은 PSK(Pre-Shared Key) 모드를 사용하는 경우, WPA-엔터프라이즈는 RADIUS 인증 서버를 사용하는 경우임

- EAP와 802.1x 암호화

WPA-EAP(Extensible Authentication Protocol)로 불리는 WPA-엔터프라이즈 방식은 인증 및 암호화를 강화하기 위해 다양한 보안 표준 및 알고리즘을 채택

EAP: 무선 랜 클라이언트와 RADIUS 서버 간의 통신을 가능하게 하는 프로토콜

802.1x: 포트에 대한 접근을 통제하는 프로토콜

연습문제

01 TCP/IP의 4계층에 해당하지 않는 것은? (4)

(1) 인터넷 계층 (2) 전송 계층

(3) 응용 계층 (4) 물리 계층

02 MAC 주소는 무엇으로 이루어져 있는가? (3)

(1) 6개의 16진수 (2) 12개의 8진수

(3) 12개의 16진수 (4) 6개의 8진수

03 공인 IP 주소로 가장 많은 호스트를 구성할 수 있는 네트워크는? (1)

(1) A 클래스 (2) B 클래스

(3) C 클래스 (4) D 클래스

04 다음 중 네트워크 서비스와 포트가 잘못 연결된 것은? (4)

(1) FTP: 21 (2) DNS: 53

(3) HTTP: 80 (4) SMTP: 63

05 3-웨이 핸드셰이킹에 대해 설명하시오.

- TCP에서 가상 경로를 설정할 때 연결을 설정하는 과정을 말한다

06 SYN 패킷만 보내어 서버를 점유함으로써 다른 사용자가 서버를 사용할 수 없게 하는 공격은? (1)

(1) SYN 플러딩 공격 (2) 랜드 공격

(3) 분산 서비스 거부 공격 (4) 스머프 공격

07 다음 중 랜드 공격의 출발지 주소와 목적지 주소가 바르게 묶인 것은? (3)

[출발지 주소] [목적지 주소]

(1) 공격 대상의 클라이언트 IP 주소 공격 대상의 서버 IP 주소

(2) 공격 대상의 서버 IP 주소 공격 대상의 클라이언트 IP 주소

(3) 공격 대상의 서버 IP 주소 공격 대상의 서버 IP 주소

(4) 공격자의 IP 주소 공격 대상의 서버 IP 주소

08 스머프 공격은 ICMP echo request를 이용하는 것이다. 이 echo request 패킷을 에이전트에 뿌리기 위해 라우터에서 지원해야 하는 것은?

- 다이렉트 브로드캐스트

09 프러미스큐어스 모드에 대해 설명하시오.

- 스니핑을 수행하는 공격자는 자신이 가지지 말아야 할 정보까지 모두 볼 수 있어야 하기 때문에 데이터 링크 계층과 네트워크 계층의 정보를 이용한 필터링은 방해물이다. 이때, 두 계층의 필터링을 해제하는 랜 카드의 모드를 말한다

10 스위칭 환경에서 스니핑을 수행하기 위한 공격이 아닌 것은? (3)

(1) ARP 스푸핑 (2) ICMP 리다이렉트

(3) IP 스푸핑 (4) 스위치 재밍

11 ARP 스푸핑은 몇 계층 공격에 해당하는가? (2)

(1) 1계층 (2) 2계층

(3) 3계층 (4) 4계층

12 IP 스푸핑 공격을 수행하기 위해 공격 대상이 사용하고 있어야 하는 것은? (2)

(1) SSO (2) 트러스트

(3) DRM (4) 웹 서비스

13 스위칭 환경에서 스니핑을 하기 위한 공격과 가장 거리가 먼 것은? (1)

(1) DNS Spoofing (2) ARP Broadcast

(3) ARP Jamming (4) Switch Jamming

14 이메일과 관련된 프로토콜이 아닌 것은? (2)

(1) SMTP (2) SNMP

(3) POP3 (4) IMAP

15 다음 중 무선 랜 구축 시 보안 고려 사항으로 가장 적절하지 않은 선택은? (4)

(1) SSID를 숨김 모드로 사용

(2) 관리자용 초기 ID/Password 변경

(3) 무선 단말기의 MAC 주소 인증 수행

(4) 보안성이 우수한 WEP(Wired Equivalent Privacy) 사용

16 DNS 정보를 요청한 클라이언트 측면에서 DNS 스푸핑이 가능한 가장 큰 요인을 설명하시오.

- 공격자는 로컬에 존재하므로 지리적으로 DNS 서버보다 가깝다. 따라서 DNS 서버가 올바른 DNS response 패킷을 보내주기 전에 클라이언트에 위조된 DNS response 패킷을 보낼 수 있다

17 세션 하이재킹을 하기 위해 서버 측에 최초로 보내는 TCP 패킷은? (2)

(1) SYN (2) RST

(3) FIN (4) ACK

18 다음 중 무선 랜 보안 시 확인할 사항이 아닌 것은? (1)

(1) SSID 브로드캐스팅 허용 (2) WEP 키 설정

(3) WPA-PSK 키 설정 (4) 802.1x 솔루션 도입

Chapter 06 악성코드

제작자가 의도적으로 사용자에게 피해를 주기 위해 만든 모든 악의적 목적을 가진 프로그램 및 매크로, 스크립트 등으로 컴퓨터에서 작동하는 실행 가능한 모든 형태

01. 악성코드

+ 동작에 의한 분류

- 바이러스: 사용자의 컴퓨터 내에서 프로그램이나 실행 가능한 부분을 몰래 변형하여 자신 또는 자신의 변형을 복사하는 프로그램. 복제와 감염으로, 다른 컴퓨터로 스스로 전파되지 않음

- 웜: 인터넷 또는 네트워크를 통해 컴퓨터에서 컴퓨터로 전파되는 악성 프로그램. 윈도 또는 응용 프로그램의 취약점을 이용하거나 이메일 또는 공유 폴더, p2p를 통해 전파됨. 스스로 전파 가능

- 트로이 목마: 바이러스나 웜처럼 컴퓨터에 직접적인 피해를 주지 않지만, 악의적인 공격자가 침투하여 사용자의 컴퓨터를 조종하는 프로그램. 다른 파일에 복사하지 않고 전파되지 않음

- PUP: 잠재적으로 원하지 않는 불필요한 프로그램이란 뜻으로 사용자에게 치명적인 피해를 주지 않지만 불편함을 주는 악성 코드. 프로그램 설치 시 사용자에게 직간접적인 동의를 구하지만 용도를 파악하기 어렵다

+ 목적에 의한 분류

- 다운로더(downloader): 네트워크를 통해 어떤 데이터나 프로그램 등을 내려받는 것이 목적으로, 내려받은 데이터나 프로그램이 추가 공격을 위한 악성 코드이거나 악성 코드 작성자의 명령 집합인 경우다

- 드로퍼(dropper): 자신 안에 존재하는 데이터로부터 새로운 파일을 생성하여 공격을 수행하는 것이 목적이다. 압축되어 있어 실행해 보지 않고서는 확인이 어렵다

- 런처(launcher): 다운로더, 드로퍼 등으로 생성돼 파일을 실행하기 위해 관련 기능을 포함하고 있다

- 애드웨어(adware): 광고가 포함된 s/w로 자체에 광고를 포함하거나 같이 묶어 배포한다. 압축 또는 동영상 재생 프로그램과 같은 프리웨어 설치 시에 동의 항목에 포함되어 설치 및 실행되는 경우가 많다. 사용자의 인식 없이 설치된 애드웨어는 인터넷 시작 페이지 변경, 광고와 관련된 알림 창 띄우기, 바탕화면에 광고 페이지의 바로가기 지속 생성이 목적이다

- 스파이웨어(spyware): 개인이나 기업의 정보를 몰래 수집하여 동의 없이 다른 곳에 보내는 것이 목적이다. 자신의 존재를 숨긴 채 사용자의 컴퓨터 조작 방해, 사용자의 컴퓨터 지켜보기, 사용자의 정보(검색 흔적, 사용자 로그인 정보, 은행이나 신용 계좌 정보, 은행 등) 수집한다. 패스워드 스틸러, 키로거 등으로 세분화됨

- 랜섬웨어(ransomware): 인질의 몸값을 나타내는 ransom 과 s/w의 합성어로 사용자에 의해 랜섬웨어가 실행되면 파일 암호화가 진행되어 사용자가 실행하거나 읽을 수 없게 하고 돈을 요구. 거의 복구 불가능 / 백업 필요

- 백도어(backdoor): 원래 시스템의 유지 보수나 유사시 문제 해결을 위해 시스템 관리자가 보안 설정을 우회한 다음 시스템에 접근할 수 있도록 만든 도구인데, 백도어를 악의적인 목적을 가진 공격자가 시스템에 쉽게 재 침입하는 데 이용하는 경우를 의미함. 백도어는 비인가된 접근을 허용하는 것으로 공격자가 사용자 인증 등의 절차를 거치지 않고 프로그램이나 시스템에 접근할 수 있도록 지원한다

- 익스플로잇(exploit): OS나 특정 프로그램의 취약점을 이용하여 공격하는 악성 코드. 기존 코드는 공격자가 직접 공격을 수행했으나 최근에는 악성 코드로 제작 및 배포하여 자동으로 공격 확산을 수행하는 경우가 많다

- 봇(bot): DDoS 공격 시 지정된 공격을 수행하도록 하는 악성 코드. 수많은 봇이 모여 대규모 공격을 수행하는 봇넷 구성

- 스캐어웨어(scareware): 겁주다와 s/w의 합성어로 사용자를 놀라게 하거나 겁주는 목적이다. 악성코드에 감염되지 않았는데도 악성 코드를 탐지했다고 겁을 주고 자사의 안티바이러스 제품으로 제거해야 한다는 식으로 구매를 유도함

+ 감염 증상

시스템: 시스템 설정 정보 변경(레지스트리 키 값을 변경하여 시스템 정보를 변경한다)/FAT 파괴(시스템의 파일 시스템을 파괴함)/CMOS 변경(CMOS 내용을 변경하여 부팅 시 오류를 발생시킴)/CMOS 정보 파괴/기본 메모리 감소/속도 저하/프로그램 자동 실행(레지스트리 값을 변경하여 시스템 부팅 시 특정 프로그램을 자동으로 실행)/프로세스 종료

네트워크: 메일 발송/정보유출/속도 저하/메시지 전송/특정 포트 오픈

하드디스크: 포맷/부트섹터 파괴

파일: 생성/삭제/감염/손상/암호화

특이점: 이상 화면 출력/특정 음 발생/메시지 상자 출력/증상 없음

02. 바이러스

1. 원시 바이러스

- 단순하게 자기 복제 기능과 데이터 파괴 기능만을 가지고 있음

+ 부트 바이러스(몽키, 브레인, 미켈란젤로)

: 플로피디스크나 하드 디스크의 부트 섹터에 감염되는 바이러스로 MBR과 함께 PC 메모리에 저장되어 부팅 시 자동으로 동작하여 부팅 후에 사용되는 모든 프로그램을 감염시킨다

- 컴퓨터 부팅 순서

1단계: POST(Power On Self Test)

POST(BIOS(Basic input/output System)에 의해 실행됨)는 O/S와 관련 없지만 O/S를 설치할 때 H/W자체가 시스템에 문제가 없는지 기본사항을 스스로 확인하는 POST 과정을 항상 거친다

메인보드는 LED로 문제 표시, 컴퓨터 조립 시 PCI 카드 제대로 안 끼우면 경고음

2단계: CMOS(Complementary Metal-Oxide Semiconductor)

PC 부팅 시 ESC 또는 F2를 누르면 CMOS에 들어갈 수 있다. CMOS에는 기본 장치에 대한 설정과 부팅 순서를 정할 수 있으며 이런 설정 사항을 BIOS가 읽어 시스템에 적용

3단계: O/S 위치 정보 로드

윈도 부트 매니저가 실행되는 단계이다. bootmgr.exe가 실행되고 부트 설정 데이터(BCD Boot Configuration Data)를 읽어 실행 가능한 운영체제 목록을 보여준다. 부트 바이러스는 이 3단계에서 동작한다

+ 파일 바이러스(예루살렘, 선데이, 스코피온, 크로, FCL…)

: 파일을 직접 감염시키는 것으로 하드디스크로 부팅하는 것이 일반화되면서 부트 바이러스 대안으로 등장.

일반적으로 COM이나 EXE와 같은 실행 파일과 오버레이 파일, 디바이스 드라이버 등에 감염되어 전체 바이러스의 80% 이상으로 바이러스에 감염된 실행 파일이 바이러스 코드를 실행한다. (프로그램을 덮어쓰는 경우, 프로그램의 앞부분에 실행 코드를 붙이는 경우, 프로그램 뒷부분에 바이러스 코드를 붙이는 경우가 있음)

2세대 암호형 바이러스(슬로, 캐스케이드, 원더러, 버글러…)

: 바이러스 코드를 쉽게 파악하여 제거할 수 없도록 암호화한 바이러스. 1세대 바이러스는 패턴이 있어서 백신에 막히기 때문에 백신을 우회하기 위해 만듦

ex) 바이러스 코드 -> 암호화 -> 복호화 알고리즘/암호화된 바이러스 코드/복호화 키

3세대 은폐형 바이러스(브레인, 조시, 512, 4096 바이러스)

: 2세대는 감염된 파일이 일정 기간의 잠복기를 가지도록 만들어진 것으로 감염이 돼도 실제 바이러스가 동작하기 전까지 그 존재를 파악하기 어려움

4세대 다형성 바이러스

: 백신은 바이러스 안의 특정한 식별자로 감염 여부를 판단하는데 이를 우회하기 위해 만듦.

코드 조합을 다양하게 할 수 있는 조합(mutation) 프로그램을 암호형 바이러스에 덧붙여 감염시키기 때문에 프로그램이 실행될 때마다 바이러스 코드 자체를 변경하여 식별자 구분이 어렵게 함

5세대 매크로 바이러스(워드 콘셉트, 와쭈, 엑셀-라룩스, 멜리사…)

: 주로 MS 오피스 프로그램의 매크로 기능을 통해 감염되는 바이러스. (스크립트 형태의 실행환경을 이용)

-> 증상 – 문서가 정상적으로 열리지 않거나 암호가 설정되어 있음/문서 내용에 깨진 글자나 이상한 문구가 포함/매크로 메뉴가 실행할 수 없게 잠겨 있다/엑셀이나 워드 작업 중 VB 편집기의 디버그 모드가 실행된다.

매크로 사용에 대한 설정 보기 [옵션-보안센터-설정-매크로 설정]

6. 차세대 바이러스

최근에는 매크로 바이러스에서 네트워크와 메일을 이용하여 전파시킨다. 데이터 파괴 + 시스템 장악을 위한 백도어 기능을 가진 웜의 형태로 진화

03. 웜

웜은 벌레와 증식을 뜻하는 말로 IT에서는 인터넷 또는 네트워크를 통해 컴퓨터에서 컴퓨터로 전파되는 프로그램을 의미

- 다른 컴퓨터의 취약점을 이용하여 스스로 전파되거나 메일로 전파되지만, 다른 파일을 감염시키는 컴퓨터 바이러스와는 다르다. 컴퓨터 바이러스 – 부트 영역에 침입하거나, 메모리에 상주하거나, 정상 파일에 침입…

웜 – 스스로 증식하는 것이 목적

1. 매스 메일러형 웜(소빅, 두마루, 넷스카이, 베이글…)

: 자기 자신을 포함하는 대량 메일을 발송하여 확산되는 것. 전체의 40% 정도로 제목이 없는 메일이나 특정 제목의 메일을 전송하고 사용자가 이를 읽었을 때 감염

- 특징 및 증상

메일로 전파. 감염된 시스템이 많으면 SMTP 서버(25번)의 네트워크 트래픽이 증가

출처나 내용이 확인되지 않은 메일을 열었을 때 확산됨

베이글 웜은 웜 파일을 실행할 때 Can’t find a viewer associated with the file 같은 가짜 오류 메시지를 출력

넷스카이 웜은 윈도 시스템 디렉터리 밑에 CSRSS.exe 실행파일을 만듦

변형된 종류에 따라 시스템에 임의의 파일을 생성

2. 시스템 공격형 웜(아고르, 블래스터 웜, 웰치아…)

O/S 고유 취약점을 이용하여 내부 정보를 파괴하거나 컴퓨터를 사용할 수 없는 상태로 만들거나 외부의 공격자가 시스템 내부에 접속할 수 없도록 악성 코드를 설치하는 것

- 특징

전파할 때 과다한 TCP/135, 445 트래픽이 발생

Windows, windows/system32, winnt, winnt/system32 폴더에 SVCHOST.EXE 파일을 설치

공격 성공 후 UDP/5599 등의 특정 포트를 열어 외부 시스템과 통신

시스템 파일 삭제 또는 정보 유출 가능

# 웰치아 동작 – ICMP 패킷을 전송하면서 살아 있는 시스템을 찾고 컴퓨터에 설정된 시스템 IP를 기준으로 B클래스의 주소를 고정시킨 뒤 C클래스 대역의 IP를 계속 증가시키면서 ICMP 패킷을 전송한다

시스템을 찾았으면 TCP/135번의 RPC DCOM 취약점을 이용하여 공격을 시도함으로써 네트워크에 장애를 발생시키고 시스템을 비정상적으로 종료시킴

3. 네트워크 공격형 웜(클레즈)

: 특정 네트워크나 시스템에 대해 SYN 플러딩이나 스머프와 같은 DOS 공격을 수행. 시스템 공격형 웜과 네트워크 공격형 웜은 버퍼 오버플로나 포맷 스트링과 같은 취약점을 주로 이용

- 주요 증상

네트워크가 마비되거나 급격히 느려짐/장비가 비정상적으로 동작

04. 트로이목마

: 악성 루틴이 숨어 있는 프로그램. 겉으론 멀쩡해 보이는데 안에는 악성 코드가 실행. 보통 다른 파일에 삽입되거나 스스로 전파되지 않고 백도어(원래 운영체제나 프로그램을 생성할 때 정상적인 인증 과정을 거치지 않아도 접근할 수 있도록 만든 통로=trap door, administrative hook)를 활용

프로그램 개발된 후 완전히 삭제되어야 하지만 그래도 남아 있는 경우도 있다

05. PUP

: (Potentially Unwanted Program) 사용자에게 직간접적으로 동의를 구하긴 하지만 용도를 파악하기 어려운 상태에서 설치되는 프로그램. 언제 설치했는지 모르는 프로그램들. 포르노나 크랙 사이트에 접속할 때 설치되는 경우도 있고 악성코드에 의해 설치되는 경우도 있다

06. 악성코드 탐지 및 대응책

1. 네트워크 상태 점검하기

악성코드가 외부 공격자와의 통신이나 dos 신호를 수신하기 위해 생성한 서비스 포트를 확인한다

2. 정상적인 프로세스와 비교하기

정상적인 프로세스와 네트워크 상태에서 확인한 프로세스를 비교/분석한다. 악성코드는 주로 iexplorer, csrr, svchost 등을 이용

3. 악성 코드와 실제 파일 확인하기

네트워크 상태와 프로세스 분석을 통해 파악한 악성 코드의 실제 파일을 확인한다

4. 시작 프로그램과 레지스트리 확인하기

악성 코드는 레지스터를 이용하는 경우가 많으므로 악성 코드를 삭제할 때 시작 프로그램과 레지스트리의 내용을 확인한다

5. 악성 코드 제거하기

악성 코드 프로세스 중지하기 -> 악성 코드 파일 삭제하기 -> 레지스트리 삭제하기

연습문제

01 컴퓨터 (바이러스)란 자기 자신을 복제하여 대상 프로그램에 포함시킴으로써 해당 프로그램을 감염시키는 프로그램이다.

02 바이러스와 웜의 차이를 설명하시오.

웜은 스스로 전파하지만 바이러스는 다른 컴퓨터로 전파하지 않음

03 다음 중 악성 코드에 속하지 않는 것은? (4)

(1) 바이러스 (2) 스파이웨어

(3) 트로이 목마 (4) 자바스크립트

04 다음 중 시스템의 부팅 순서가 올바르게 나열된 것은? (4)

(1) MBR 로드 – CMOS 로드 – POST – 운영체제 정보 로드

(2) POST – MBR 로드 – CMOS 로드 – 운영체제 정보 로드

(3) CMOS 로드 – POST – MBR 로드 – 운영체제 정보 로드

(4) POST – CMOS 로드 – MBR 로드 – 운영체제 정보 로드

05 부팅 단계에서 부트 바이러스가 시스템에 감염되는 단계에 해당하는 것은? (3)

(1) CMOS 내의 설정 사항을 로드하는 단계

(2) 시스템의 이상 여부를 확인하기 위한 POST 단계

(3) 마스터 부트 레코드(MBR)를 메모리에 저장하는 단계

(4) 운영체제와 관련된 기본 정보를 메모리에 저장하는 단계

06 다음 중 바이러스가 감염시키는 파일 확장자를 모두 고르시오. (1), (4)

(1) com (2) hwp

(3) txt (4) exe

07 파일 바이러스가 프로그램 뒷부분에 위치할 때의 프로그램 실행 순서를 설명하시오.

프로그램 시작 지점에서 점프하여 프로그램 종료 뒤에 바이러스 코드를 심고 다시 점프하여 프로그램을 실행한다.

08 암호형 바이러스를 치료하는 방법을 간단히 설명하시오.

바이러스가 동작할 때 메모리에 올라오는 과정에서 암호화가 풀린다. 이를 이용해 메모리에 실행되어 올라온 바이러스와 감염 파일을 분석하고 치료

09 다음 중 컴퓨터 바이러스에 대한 설명으로 옳지 않은 것은? (2)

(1) 부트 바이러스는 플로피 디스크나 하드디스크의 부트 섹터를 감염시키는 바이러스다.

(2) 파일 바이러스는 숙주 없이 독자적으로 자신을 복제하고 다른 시스템을 자동으로 감염시켜 자료를 유출ˑ변조ˑ삭제하거나 시스템을 파괴한다.

(3) 이메일 또는 프로그램 등의 숙주를 통해 전염되어 자료를 변조ˑ삭제하거나 시스템을 파괴한다.

(4) 최근 들어 암호화 기법을 기반으로 구현된 코드를 감염 시마다 변화시킴으로써 특징을 찾기 어렵게 하는 다형성(Polymorphic) 바이러스로 발전하고 있다.

10 코드 조합을 다양하게 할 수 있는 조합 프로그램을 암호형 바이러스에 덧붙여 감염시키기 때문에 프로그램이 실행될 때마다 바이러스 코드 자체를 변경하여 식별자를 구분하기 어렵게 하는 바이러스는? (3)

(1) 암호형 바이러스 (2) 은폐형 바이러스

(3) 다형성 바이러스 (4) 매크로 바이러스

11 매크로 바이러스의 공격 대상을 모두 고르시오. (3), (4)

(1) 웹 브라우저 (2) HWP

(3) MS 워드 (4) MS 엑셀

12 시스템 공격형 웜에 대해 간단히 설명하시오.

O/S 고유의 취약점을 이용하여 내부 정보를 파괴하거나 컴퓨터를 사용할 수 없는 상태로 만들거나 외부의 공격자가 시스템 내부에 접속할 수 있도록 악성 코드를 설치하는 것

13 악성 루틴이 숨어 있는 프로그램으로, 겉보기에는 정상적인 것 같지만 사용자가 실행하면 악성 코드를 실행하는 것은? (2)

(1) 바이러스 (2) 트로이 목마

(3) 스파이웨어 (4) 자바스크립트

14 다음 중 트로이 목마(Trojan)의 일반적인 특징 및 기능으로 옳지 않은 것은? (2)

(1) 패스워드 가로채기 (2) 악성 코드 전파

(3) 파일 파괴 (4) 원격 조정

15 (PUP)는 사용자가 설치할 의도가 없으나 용도를 쉽게 파악하기 어려운 상태에서 직간접적으로 사용자에게 동의를 구하여 설치되는 프로그램이다.

16 다음 중 악성 코드를 탐지하기 위해 확인하는 사항에 속하지 않는 것은? (4)

(1) 네트워크 상태 (2) 프로세스

(3) 파일 (4) 디스크 상태

17 윈도우 시스템이 동작하기 위한 기본 프로세스에 대한 설명을 바르게 연결하시오.

cross.exe: 윈도우 콘솔을 관장하고 스레드를 생성 및 삭제하며 32비트 가상 MS-DOS 모드를 지원한다

lsass.exe: winlogon 서비스에 필요한 인증 프로세스를 담당한다

smss.exe: 사용자 세션을 시작하는 기능을 담당한다. 이 프로세스는 winlogon, win32(csrss.exe)를 구동하고 시스템 변수를 설정한다. 또한 smss는 winlogon이나 csrss가 끝나기를 기다려서 정상적인 winlogon, csrss 종료 시 시스템을 종료한다

svchost.exe: DLL에 의해 실행되는 기본 프로세스다. 한 시스템에서 여러 개의 svchost 프로세스를 볼 수 있다

services.exe: 시스템 서비스를 시작 및 정지하고 그것들 간에 상호작용하는 기능을 수행

Chapter 10 IoT 보안과 AI 보안

1. IoT 보안

- IoT의 개념

인터넷에 연결되는 것을 의미

MIT auto-ID 센터 설립자인 케빈 애시턴이 1999년 사물 인터넷의 개념과 용어를 처음으로 제안

이미 상용화된 IoT 기기로는 전구, 자동차, 냉장고, 보일러, 자물쇠, 칫솔, 개인 비서, 프린터 등

매우 다양하지만, 물건에 시스템을 결합한 형태라는 점은 동일

- IoT는 물건이 인터넷에 연결되는 ‘사물 인터넷’을 의미

- IoT 기기는 대부분 와이파이나 블루투스를 통신에 사용하므로 관련 취약점을 그대로 지니게 됨

- 한국인터넷진흥원(KISA)에서 수립한 IoT 공통 보안 7대 원칙

1) 정보 보호와 프라이버시 강화를 고려한 IoT 제품과 서비스 설계

2) 안전한 소프트웨어와 하드웨어 개발 기술 적용 및 검증

3) 안전한 초기 보안 설정 방안 제공

4) 보안 프로토콜 준수와 안전한 파라미터 설정

5) IoT 제품과 서비스의 취약점 보안 패치 개발 및 업데이트 지속 이행

6) 안전한 운영·관리를 위한 정보 보호 및 프라이버시 관리 체계 마련

7) IoT 침해 사고 대응 체계 및 책임 추적성 확보 방안 마련

02. AI에 대한 이해

**AI의 역사**

AI의 시작

1943년 논리학자인 월터 피츠와 신경외과의인 워렌 맥컬럭의 논문에서 최초의 인간 두뇌에 관한 모델이 등장

1950년 영국의 수학자 앨런 튜링의 논문에서 ‘생각하는 기계’에 대해 기술

1956년 존 매카시 교수가 ‘다트머스 AI 컨퍼런스’를 개최하면서 초청장 문구에 ‘AI’라는 용어를 처음으로 사용

AI의 발전

1950년대의 인공지능 연구는 크게 기호주의와 연결주의의 두 분야로 전개

- 기호주의: 인간의 지능과 지식을 기호화해 매뉴얼화하는 접근법

- 연결주의: 1943년 월터 피츠와 워렌 맥컬럭이 연구한 뇌 신경 네트워크의 재현을 목표로 하는 접근법

퍼셉트론은 인간의 사진을 대상으로 남자와 여자를 구별해내면서 뉴욕 타임즈에 등장

- 퍼셉트론: 인공 신경망(딥 러닝)의 기본이 되는 알고리즘

AI의 빙하기

마빈 민스키는 제자 시모어 페퍼트와 퍼셉트론의 한계를 수학적으로 증명

퍼셉트론이 무너지고 설상가상으로 2년 뒤인 1971년에 로젠블랫이 사망하며 신경망 열기가 급격히 냉각

로젠블랫의 퍼셉트론으로는 XOR 같은 비선형 문제는 해결할 수 없음

AI의 부활

제프리 힌튼 교수는 다층 퍼셉트론, MLP과 역전파 알고리즘을 실험을 통해 증명하여 XOR 문제를 해결

하버드대학 풀 워보스가 다층 퍼셉트론 환경에서 학습을 가능하게 하는 역전파 알고리즘으로 박사 학위 논문 발표

1986년 데이빗 럼멜하트와 제프리 힌튼이 최적의 신경망 변수들을 찾아내는 적합을 증명

AI의 2차 빙하기

기울기 소실과 과적합문제로 2차 빙하기를 맞이함

기울기 소실

- 다층 신경망의 은닉층을 늘리면 신경망의 깊이가 깊어질수록 오히려 기울기가 사라져 학습이 되지 않는 문제

과적합

- 신경망이 깊어질수록 너무 정교한 패턴을 감지하게 되어 새로운 데이터에 대해서는 정확성이 떨어지는 문제

딥 러닝의 시작

제프리 힌튼은 가중치의 초깃값을 제대로 설정한다면 깊은 신경망을 통한 학습이 가능하다는 것을 밝혀냄

인공 신경망이라는 단어가 들어간 논문을 학회에 투고하면 제목만 보고 거절당하거나 사람들의 관심을 끌지 못하기 때문에 제프리 힌튼은 이 논문에 deep을 붙인 DNN이라는 용어를 사용

**AI 기술의 분류**

AI가 곧 딥 러닝은 아니며 아직 AI 관련 용어에 대한 정의가 명확하지 않고 혼용되는 경우가 많음

AWS에 나타난 AI의 정의

- 인공지능은 학습, 문제 해결, 패턴 인식 등과 같이 주로 인간 지능과 연결된 인지 문제를 해결하는 데 주력하는 컴퓨터 공학 분야

머신 러닝의 분류

머신 러닝 역시 상당 부분 통계학적인 기술을 포함

- 지도 학습: 분류나 회귀에 사용

- 비지도 학습: 군집에 사용

- 강화 학습: 환경에서 취하는 행동에 대한 보상을 이용하여 학습을 진행

지도 학습

답이 있는 데이터를 활용해 학습시키는 방법

입력 값(X이 주어지면 입력 값에 대한 라벨(Y)을 주어 학습

분류

- 주어진 데이터를 정해진 레이블(범주)에 따라 나누는 것

- 범주가 2개이면 이진 분류, 3개 이상이면 다중 클래스 분류

회귀

- 어떤 데이터들의 특징을 토대로 값을 예측하는 것

- 결과 값은 실수 값을 가질 수 있음

비지도 학습

지도 학습과 달리 답이 없는 데이터를 비슷한 특징끼리 군집화하여 새로운 데이터에 대한 결과를 예측하는 것

군집

- 특정 기준에 따라 유사한 특성의 데이터를 각각의 그룹으로 분류

- 고유한 패턴 또는 특성을 찾기 위해 클러스터링을 사용

차원 축소

- 많은 변수 중에 유의미한 변수들을 식별하여 개수를 줄이는 작업

- 일부 변수가 중복되거나 작업과 아무 관련이 없는 경우가 많기 때문

- 변수를 줄이면 잠재되어 있는 진정한 관계를 도출하기가 용이

강화 학습

지도·비지도 학습과는 다른 종류의 알고리즘

학습하는 시스템을 ‘에이전트’라고 부르며, 환경을 관찰해서 행위를 수행하고 보상을 받음

시간이 지나면서 가장 큰 보상을 얻기 위해 ‘정책’이라고 부르는 최상의 전략을 스스로 학습

정책은 주어진 상황에서 에이전트가 어떻게 행동해야 하는지를 판단하는 것

기계는 최대의 보상을 산출하는 행위를 발견하기 위해 서로 다른 시나리오를 시도

시행착오와 지연 보상은 다른 기법과 구별되는 강화 학습만의 특징

3. AI의 취약점 유형과 대안

**데이터 변조 공격과 대안**

회피 공격

학습 과정에서 데이터에 무작위의 오류가 존재하는 노이즈를 고의적으로 추가하면 인공지능은 다른 이미지로 판단

기존 해킹 방법이 유무선 네트워크나 단말기의 취약점을 이용, 인공지능에 대한 해킹은 인공지능 자체의 취약점을 이용

데이터가 변조되었다면 변조 공격을 학습 데이터에 포함해 훈련시키는 방법으로 대응할 수 있음

중독 공격

악의적인 데이터를 이용해 인공지능 시스템이 오작용을 일으키도록 하는 공격

- 예) 스캐터랩의 ‘이루다’는 일부 사용자들이 이루다에게 욕설, 인종 차별 및 성 차별 발언, 정치적 발언 등 악의적인 발언들을 훈련시키면서 정상적인 서비스가 불가능해짐

부정적인 데이터에 대한 사전 학습으로 대응할 수 있음

사전 학습된 단어들과 비교하여 추가 학습이 불가하거나 답변을 우회하도록 프로그램을 설계하는 방법도 고려

**데이터 추출 공격**

전도 공격

데이터 추출 공격은 인공지능에서 사용하는 데이터 자체가 탈취하는 공격

인공지능에 수많은 쿼리를 한 후, 산출된 결과를 분석해 인공지능에서 사용된 데이터를 추출하는 공격

데이터 추출 공격에는 질의 횟수를 조정하는 것으로 대응할 수 있음

4. AI를 이용한 보안

**스팸 메일 탐지**

나이브 베이즈 분류기

최초의 스팸 메일 솔루션에 일반적으로 적용된 알고리즘

인공 신경망 알고리즘에는 속하지 않지만 머신 러닝의 주요 알고리즘으로 분류되어 있고 준수한 성능을 보임

베이즈의 정리

- P(A)가 A가 일어날 확률, P(B)가 B가 일어날 확률

- P(B|A)는 A가 일어난 뒤 B가 일어날 확률

- P(A|B)는 B가 일어난 뒤 A가 일어날 확률

입력 테스트가 정상 메일인지 스팸 메일인지 구분하기 위한 확률

- P(정상 메일|텍스트) = (P(텍스트|정상 메일) \* P(정상 메일)) / P(텍스트)

- P(스팸 메일|텍스트) = (P(텍스트|스팸 메일) \* P(스팸 메일)) / P(텍스트)

P(정상 메일|텍스트)가 P(스팸 메일|텍스트)보다 크다면 정상 메일이라고 볼 수 있으며, 그 반대라면 스팸 메일

BERT

구글에서 개발한 NLP 사전 훈련 기술로 모든 자연어 처리 분야에서 좋은 성능을 내는 범용 언어 모델

딥러닝에서 인공 신경망의 뉴런과 유사한 역할을 하는 어텐션 알고리즘

위키피디아나 소셜 같은 막대한 양의 텍스트를 이용하여 모델을 훈련

최근 BERT를 활용한 스팸 메일 솔루션은 90% 후반대의 정확도를 보임

**네트워크 침입 탐지**

전문가 시스템

- 특정 응용 분야 전문가의 지식 및 능력을 체계적으로 잘 조직하여 컴퓨터 시스템에 입력해 해당 분야의 비전문가라도 전문가에 상응하는 능력을 발휘할 수 있도록 쉽고 빠르게 도움을 주는 시스템

- 전문가 시스템은 앞서 AI의 역사에서 언급한, 논리적인 체계로 문제를 푸는 기호주의의 한 분야에 속함

**악성 코드 탐지**

- 기존에는 악성 코드를 탐지하기 위해 악성 코드의 일부분을 매칭해보거나 특정 부분의 해시 값을 생성하여 비교해보는 등의 방법이 사용

- 최근에는 이런 탐지 방법을 회피한 고도화된 방식으로 다양한 신·변종 악성 코드가 나타나 탐지가 어려움

- 현재는 프로그램이 지닌 일반적인 특징들을 변수화하여 이를 기반으로 악성 코드와 정상 코드를 머신 러닝 모델에 학습시켜 악성 코드를 탐지하는 방법이 제안 및 연구

- 최근에 응용 프로그램의 행위에 기반한 특징을 분석해서 이를 변수로 두고 악성 코드를 탐지하는 기술이 적용되고 있는데, 이는 상당한 정확도를 보여줌

**CCTV**

- 물리적 보안에서 중요한 역할을 담당하는 CCTV에도 머신 러닝이 적용

- CCTV에 찍히는 영상을 AI 기술로 실시간 처리하여 무단 침입과 같은 침해 사고를 감지

- 다국적 정유 기업인 쉘은 각 주유소에 설치된 CCTV로 모니터링하여 이 영상 데이터를 애저 클라우드 환경에서 분석하여 주유소와 관련한 위험 요인을 탐지

연습문제

01 IoT 보안에 있어서 초기 설치 단계와 고장 수리 후 재설치 단계에서 보안 프로토콜들에 기본으로 설정하는 파라미터 값이 가장 안전한 설정이 될 수 있도록 설계되어야 한다는 원칙은? (2)

(1) Secure by Default (2) Security by Design

(3) Privacy by Design (4) Privacy by Default

02 다음 중 뇌 신경 네트워크의 재현을 목표로 하는 AI 접근법은? (2)

(1) 기호주의 (2) 연결주의

(3) 이산주의 (4) 논리주의

03 (퍼셉트론)은 인공 신경망(딥 러닝)의 기본이 되는 알고리즘으로 월터 피츠와 워렌 맥컬럭의 뇌 모델과 1949년에 발표된 도널드 헵의 <헵의 학습 이론>에 힌트를 얻어 가중치를 추가한 업그레이드 버전이었다.

04 다음 중 비지드 학습에 속하는 두 가지는? (3), (4)

(1) 분류 (2) 회귀

(3) 클러스터링 (4) 차원 축소

05 다음 학습 데이터와 나이브 베이즈 분류기를 활용하여, “you free ticket”이 정상 메일일 확률과 스팸 메일일 확률을 각각 구하시오.

P(정상메일|단어) = P(you|정상메일) \* P(free|정상메일) \* P(ticket|정상메일) \* P(정상메일)

= 1/3 \* 2/3 \* 0/3 \* 3/6

= 0

P(스팸메일|단어) = P(you|스팸메일) \* P(free|스팸메일) \* P(ticket|스팸메일) \* P(스팸메일)

= 1/3 \* 2/3 \* 2/3 \* 3/6

= 0.07

06 실제로는 공격이 아닌데 공격이라고 탐지하는 것은? (1)

(1) 거짓 양성(False Positive) Type 1 에러

(2) 거짓 음성(False Negative) Type 2 에러

(3) 거짓 음성(False Negative) Type 1 에러

(4) 거짓 양성(False Positive) Type 2 에러

07 수많은 쿼리를 한 후, 산출된 결과를 분석해 인공지능에서 사용된 데이터를 추출하는 공격은? (3)

(1) 회피 공격(Evasion Attack)

(2) 중독 공격(Poisoning Attack)

(3) 전도 공격(Inversion Attack)

(4) 재전송 공격(Replay Attack)

Chapter 11 침해 대응과 디지털 포렌식

CERT: 범죄자나 의심스러운 사람이 건물에 들어오면 검사해 범죄자면 체포하는 역할

01. 침해 대응

\* CERT 침해 대응 절차

사전 대응 -> 침해 사고 발생 -> 사고 탐지 -> 대응(단시, 백업 및 증가 확보, 시스템 복구) -> 제거 및 복구 -> 후속 조치 및 보고

1. 사전 대응

: 침해 사고에 대한 기본적인 사전 대응은 침해 대응 체계를 구축하는 것이고 가장 먼저 할 일은 CERT를 구성하는 것

\* 필요한 구성원

# 시스템 운영 전문가 – 침해 사고가 발생한 시스템을 효율적으로 복구하기 위해 서비스와 시스템의 관계를 명확하게 이해하고 조치를 취한다

# 대외 언론 및 외부 기관 대응 전문가 – 침해 사고를 이해하고 언론 및 사이버안전국, 경찰에 적절한 방법으로 대응

# 법률 팀 – 침해 사고 대응 과정에서 법적인 문제가 발생했을 때 이에 대한 판단을 내리고 법적인 후속 절차를 밟음

# 인사 팀 – 조직 내 구성원의 권리와 책임을 파악하고 침해 사고 대응 과정에서 적절한 조직원을 찾도록 지원

\* CERT 대응 등급

· 1등급 상황

- DDoS로 정상적인 동작이 불가능

- 침입자에 의해 서버의 중요한 파일이 삭제되고 있다

- 트로이 목마 등의 악성 프로그램이 실행되어 정상적인 접근 제어를 실시해도 다른 경로를 통해 침입자가 지속적인 공격을 시도

- 침입자의 공격에 대한 대응 수단이 없는 그 외의 경우이다

· 1등급 대응 절차

- 침해사고 발생 상황으로 판단되면 시스템 담당자가 CERT 팀장에게 즉시 보고

- 긴급 상황 시에 피해를 최소화하기 위해 네트워크의 인터페이스 단절, 전원 공급 중단 등의 조치를 먼저 수행

· 2등급 상황

- 비인가자에 의해 관리자 명령이 실행되고 있다

- 시스템 자원을 불법적으로 사용하는 프로그램이 실행되고 있다

- 일반 사용자의 홈 디렉터리에 시스템 파일이 존재

- 일반적이지 않은 숨김 파일 또는 디렉터리가 존재

- 시스템 담당자가 알지 못하는 사용자가 추가되거나 사용자 권한이 임의로 변경

· 3등급 상황

- 외부 또는 내부에서 취약점 수집(scanning) 행위가 계속 발견된다

- 외부 또는 내부에서 불법적인 접근 시도가 계속 발견된다

- 외부 또는 내부에서 비정상 패킷의 전송량이 증가한다

- 확산 속도가 빠른 바이러스가 외부에서 발생한다

· 2/3등급 대응 절차

- 시스템 담당자가 비인가 접근 시도 및 정보 수집 행위를 발견하면 CERT와 함께 해당 단말기 또는 IP를 조사하여 소속 네트워크와 조직을 파악

- 내부 시스템에서 침입 시도가 발생한 경우에는 시스템 위치를 확인하여 책임자와 접속 경위 등을 조사한다. 외부 네트워크에서 침입 시도가 발생한 경우 해당 조직의 시스템 담당자 또는 보안 담당자에게 해당 IP로부터 불법적인 접근 시도가 발생했음을 통보하고 협조를 구한다

- 외부 네트워크의 침입 시도에 대한 적절한 조치가 이루어지지 않고 위협이 심각한 경우 대외기관(경찰, 검찰 등)에 조사를 의뢰

- 침입 시도에 대한 대응이 종료되면 CERT 팀장이 침입 시도 방법, 침입 시도 대응책 등이 포함된 ‘침입 시도 대응 보고서’를 작성하여 관련 담당자에게 전달

· 침해 대응 체계가 잘 구축되었는지 확인 방법

- 조직의 모든 사람이 보안 정책에 대해 알고 있는가?

- CERT의 모든 구성원은 침해 사고 발생 시 누구에게 보고하고 언론 대응은 어떻게 해야 하는지 충분히 인지하고 있는가?

- CERT의 모든 구성원은 침해 사고 발생 시 처리해야 할 기술적 절차에 대해 충분히 이해하고 있는가?

- 침해 사고 대응과 관련한 모든 구성원은 정해진 절차에 따라 주기적으로 훈련을 수행하고 있는가?

2. 사고 탐지

: 어떤 문제가 발생했을 때 운영상의 오류와 같은 일반적 문제인지 침해 사고가 발생했는지 확인하는 단계

- 이 단계에서 침해 사고로 확인되면, 로그 파일, 오류 메시지 등을 확보하고 방화벽, IDS 등을 통해 특정한 절차를 수행해야 하고 내부의 보고 체계에 따라 책임자에게 보고하고, 언론에 대한 대응이 필요한 경우 대응책을 마련

\* 침해 사고 식별 과정

- 침해 사고 발생 시점은 언제인가?

- 누가 침해 사고를 발견하고 보고했는가?

- 침해 사고가 어떻게 발견되었는가?

- 침해 사고의 발생 범위는 어느 정도인가? 이로 인해 다른 곳이 손상되지는 않았는가?

- 침해 사고로 인해 기업의 서비스 능력이 손상되었는가?

- 공격자의 규모와 공격 능력은 어느 정도인가?

-> 침해 사고 발생을 실시간으로 식별하는 과정은 주로 IDS나 IPS, 네트워크 트래픽 모니터링 장비(MRTG), 네트워크 관리 시스템(NMS)으로 이루어진다

ex) kt 홈페이지에 APT(지능적 지속 위협) 공격으로 긴 시간 동안 조심스럽게 이루어진 침해 사고(1200만 정보 유출)

방법: 공격자는 웹 프록시를 이용하여 홈페이지의 이용 대금 조회란에 고유 숫자 9개를 무작위로 자동 입력하는 프로그램을 작성하여 가입 고객의 아홉 자리 고유 번호를 맞혀 개인 정보를 탈취

성공률이 높을 때는 하루에 20~30만 개의 개인 정보 탈취했고 이런 정보는 휴대전화 개통 및 판매 영업에 활용되었다고…

3. 대응

: 침해 사고로 인한 손상을 최소화하고 추가 피해를 막기 위한 대응으로 3단계로 수행된다.

1) 단기 대응

: 손상을 최소화하기 위한 기본적인 단계로 침해 사고가 발생한 시스템이나 네트워크를 식별하고 통제할 수 있는 경우에는 해당 시스템이나 네트워크의 연결을 해제하거나 차단

추가로 침해 사고가 발생하는 경우 이 과정을 반복하여 단기 대응 수단으로 네트워크 케이블을 뽑는 것과 같은 물리적 대응을 포함하여 방화벽 설정 변경 및 침해 사고 룰 업데이트, 백신 업데이트, 시스템 종료 등이 있다

2) 백업 및 증거 확보

: 침해 사고 발생 후 후속 처리를 위해 침해 사고 발생 시스템을 초기화하는데, 그전에 백업을 하고 포렌식 절차에 따라 시스템 이미지를 획득하는 과정

포렌식으로 획득한 증거가 법적인 효력을 지니려면 증거 획득과 처리 과정이 적법한 절차를 거쳐야 한다

3) 시스템 복구

: 백도어 등의 악성 코드 제거, 시스템 계정 및 패스워드 재설정, 보안 패치 적용 작업을 거친 뒤 다시 서비스가 가능하도록 시스템을 네트워크에 연결하는 과정

4. 제거 및 복구

: 최초 침해 사고가 발생한 시스템 및 네트워크 외에 추가로 발생한 곳이 있는지 모두 확인하고 조치하는 단계

모든 조치가 완료되어 서비스를 완전하게 복구하는 과정에서 보안 툴을 설치하고 로그 설정을 강화하여 침해 사고가 다시 발생하는지 여부를 모니터링하는 것이 중요하다

따라서 발생한 침해 사고의 유형에 따라 시스템과 네트워크를 어떤 방식과 주기로 모니터링할지 결정한 뒤 완전한 복구를 진행해야 한다

제거와 복구가 매우 중요한 침해 사고의 유형으로 랜섬웨어가 있다. 랜섬웨어는 사용자 데이터 또는 시스템 데이터의 암호화로 데이터 손실이 발생하는 경우가 많고 암호를 풀려면 해커에게 돈을 지불하는 것 말고 다른 방법이 없기 때문이다

5. 후속 조치 및 보고

정해진 기록 문서에 따라 침해 사고 식별과 대응 과정에 대해 작성해야 한다

02. 포렌식

: 포렌식(FORENSIC)은 고대 로마 시대의 포럼(forum)이라는 라틴어에서 유래한 말로 ‘법의학적인, 범죄 과학 수사의, 법정의, 재판에 관한’이라는 의미다

- 일반적인 법적 변론을 위한 과학으로 법정 과학이나 법과학이라는 개념으로 사용되며, 최근에는 범죄 수사 및 민형사 소송 등 법정에서 사용되는 증거의 수집, 보존, 분석을 위한 응용과학 분야를 통칭하는 용어로 사용되고 있다

- 디지털 포렌식: 법정 제출을 전제로 디지털 환경과 장비를 이용하여 디지털 증거 자료를 수집, 분석하는 기술로 1991년 국제컴퓨터 수사전문가협회에서부터 처음 사용됨

1. 포렌식의 증거

- 범인을 잡을 때뿐만 아니라 기술 유출, 해킹, 위조, 사이버 테러, 명예훼손이나 업무상 과실, 내부 감사 등에도 사용

법적 효력을 가진 증거란?

요증 사실: 소송에서 당사자의 입증을 필요로 하는 사실

+ 증거의 종류

- 직접 증거: 요증 사실(증거에 의한 증명을 요하는 사실)을 직접적으로 증명하는 증거(범행 목격자, 위조지폐 등)

- 간접 증거: 요증 사실을 간접적으로 추측하게 해주는 증거(범죄 현장에 남아 있는 지문이나 알리바이 등)

- 인적 증거: 증인의 증언, 감정인의 진술, 전문가의 의견

- 물적 증거: 범행에 사용한 흉기, 사람의 신체 등

-> 포렌식으로 수집된 증거는 간접 증거에 속하는데 간접 증거를 더 정확히 표현하여 ‘전문 증거’

전문 증거: 사실 인정의 기초가 되는 실험을 실험자 자신이 법원에 직접 보고하지 않고 진술서나 진술 기재서를 통해 간접적으로 보고하는 것

ex) 증인이 직접 법정에 나서지 않고 수사관이 “제가 증인에게 들은 얘기인데, 누가 도둑질하는 걸 봤답니다”라고 대신 증언하는 경우

대륙법에서 전문 증거란 증인 자신이 체험한 사실이 아니라 타인에게 진술하는 증언이고

영미법에는 반대 신문을 거치지 않은 진술 및 그 진술을 대신하는 서면이라고 하며 증거로 채택하지 못하게 한다

=> 이를 전문 법칙 또는 전문 증거 배척의 원인이라 한다 [한국은 전문 법칙을 따르는 중]

· 증거 개시 제도

정식 재판이 진행되기 전 공판 준비 절차 단계에서 민사소송은 원고와 피고가, 형사 공판은 검사와 피고인이 각자 가지고 있는 증거를 동시에 개시하는 것으로 미리 제시하지 않은 증거는 법정에서 사용하지 못하게 하는 제도

2. 포렌식의 기본 원칙

- 포렌식으로 획득한 증거가 법적 효력을 가지기 위해서 증거를 발견하고, 기록하고, 획득하고, 보관하는 절차가 중요

하위 다섯 가지 원칙을 지키면서 포렌식이 이루어져야 한다

\* 5가지 원칙

· 정당성의 원칙

모든 증거는 적법한 절차를 거쳐서 얻은 것이어야 하며 위법한 절차로 획득한 증거는 증거 능력이 없다

예로 불법 해킹으로 시스템 내부에서 획득한 증거. 최면술

· 재현의 원칙

증거는 절차를 통해 정제되는 과정을 거칠 수 있다. 예로 시스템에서 삭제된 파일이나 손상된 파일을 복구하는 과정

이 증거를 법정에 제출하려면 같은 환경에서 같은 결과가 나오도록 재현할 수 있어야 하며 수행할 때마다 다른 결과가 나온다면 증거로 제시할 수 없다

· 신속성의 원칙

컴퓨터 내부의 정보는 휘발성을 가진 것이 많기 때문에 신속성이 필요하다. 예로 살인 사건 = 주변의 출입을 통제하고 지문이나 흔적이 사라지기 전에 최대한 빠른 시간 내에 수사 작업을 수행한다. 마찬가지로 시스템 안의 디스크 또는 메모리나 응용 프로그램 등의 정보를 얻기 위해서는 신속하고 정확하게 움직여야 한다

· 연계 보관성의 원칙

(chain of custody): 증거를 확보한 뒤에는 이송, 분석, 보관, 법정 제출이라는 일련의 과정이 명확해야 하며 이런 과정을 추적할 수 있어야 한다

· 무결성의 원칙

수집된 증거는 연계 보관성을 가지고 각 단계를 거치는 과정에서 위/변조되어서는 안 되며 이러한 사항을 매번 확인해야 한다. 하드디스크의 경우에는 해시 값을 구해서 각 단계마다 값을 확인하여 무결성을 입증할 수 있다

3. 포렌식 수행 절차

\* 수사 단계별 절차

1) 수사 준비

수사를 준비할 때는 장비와 툴을 확보하고 적절한 법적 절차를 거쳐 피의자 또는 수사 대상에 접근해야 한다

2) 증거물 획득

증거물을 획득할 때에는 증거를 획득하는 사람과 이를 감독하는 사람, 그리고 인증하는 사람이 있어야 한다. 그리고 이 세 사람의 참관 하에 다음과 같은 절차를 수행해야 한다

- 컴퓨터의 일반적인 하드 드라이브를 검사할 때는 컴퓨터 시스템 정보를 기록한다

- 복제 작업을 한 원본 매체나 시스템의 디지털 사진을 찍는다

- 모든 매체에 적절한 증거 라벨을 붙인다

3) 보관 및 이송

획득한 증거는 연계 보관성을 가진 채 보관 및 이송되어야 한다. 증거가 연계 보관성을 가지려면 우선 안전한 장소(evidence safe)에 보관되어야 하며, 이송하거나 담당자 또는 책임자가 바뀔 때 문서에 그 종적을 남겨야 한다

4) 분석 및 조사

포렌식 증거를 관리할 때 최량 증거 원칙(the best evidence rule)을 따른다

최량 증거 원칙: 복사본 등의 이차적인 증거가 아닌 원본을 제출하도록 요구하는 영미 증거법상의 원칙

원본이 존재하지 않으면서 가장 유사하게 복사한 최초 복제물이라도 증거로 제출해야 한다. 따라서 법원에 제출하는 원본 또는 최초의 복제물은 기본적으로 보관하고 이를 다시 복사한 것을 분석 및 조사해야 한다

5) 보고서 작성

분석을 마친 뒤에는 분석에 사용한 증거 데이터, 분석 및 조사 과정에서 증거 수집을 위해 문서화한 무결성과 관련된 정보, 스크립트 수행 결과를 보고서로 작성하여 증거와 함께 제출

4. 사이버 수사 기구

- 국가정보원 국가사이버안전센터

\* 주요 업무

국가 사이버 안전 정책 총괄

사이버 안전 예방 활동(모의 훈련, 정보통신망 보안성 검토)

국가 사이버 위협 정보 종합 수집, 분석, 전파

침해사고 긴급 대응, 조사 및 복구

국내외 사이버 위협 정보 공유 및 공조 대응

- 대검찰청 첨단범죄 수사과

기술유출범죄수사지원센터

인터넷 관련 범죄 수사팀

회계 분석 팀

범죄 수익 환수 팀

자금세탁 수사 및 범죄 수익 환수 전담반

첨단 범죄 수사 전문 아카데미

- 경찰청 사이버테러대응센터

03. 증거 수집

1. 네트워크 증거 수집

· 보안 솔루션 이용

네트워크와 관련된 증거를 수집할 때 우선 고려할 수 있는 것은 IDS이다. IDS는 공격자가 공격 대상에 침투하기 위한 스캐닝이나 접근 제어를 우회한 반복적인 접근 시도에 대한 기록이 남아 있을 수 있기 때문

그 밖엔 네트워크 링크의 트래픽 부하를 감시하는 툴(MRTG)이다. 라우터에서 가져온 모든 데이터 로그를 보관하고 200개 이상의 네트워크 링크를 즉시 감시할 수 있어 DOS 공격의 증빙으로 유용

· 네트워크 로그 서버 이용

네트워크 로그 서버를 별도로 운영하는 경우는 도움이 된다. (많이 안 씀)

· 스니퍼 운용

증거를 수집하기 위해 일시적으로 스니퍼를 네트워크 탐지용으로 운용함. 공격자가 네트워크에 백도어 등을 설치하면 스니퍼는 해당 패킷을 잡아내어 백도어를 탐지하고 공격자의 위치를 탐색할 수 있다. 그리고 웜이나 바이러스로 피해를 입은 경우에는 발원지와 감염된 PC를 구분하는 데 사용

2. 시스템 증거 수집

법원에 주로 제출되는 정보

· 활성 데이터 수집

활성 데이터 수집(live data collection): 정보는 시스템에서도 쉽게 사라지기 때문에 확인한 증거는 화면 캡처 등으로 남기는 것. 경우에 따라 카메라로 녹화

- 윈도 시스템

: 현재 해커의 세션이 시스템에 남아 있는지 확인한다. (not session으로 확인 = 윈도에서 NetBIOS로 현재 세션이 형성되어 있는 사용자를 확인하는 명령어)

# net session 명령어: 현재 세션이 형성되어 있는 사용자를 확인

# query user 명령어: 시스템의 사용자 정보 확인

# query session 명령어: 시스템의 사용자 세션 정보 확인

- 리눅스 시스템

w, who, last 명령으로 현재 세션 보여줌

· 시스템 로그 분석

: 공격자에 의해 삭제될 수 있지만 침해 사고가 발생했을 때 가장 먼저 살펴보아야 할 기본 항목

시스템 로그가 삭제되는 것을 막기 위해 네트워크에 로그 서버를 별도로 둘 수 있다

· 저장 장치 분석

증거 파일을 PC에 보관하거나 관련 증거를 얻기 위해 저장 장치를 분석한다. + 삭제된 데이터도 분석

하드디스크를 떼어낸 뒤 복사. (원본 보존을 위해서)

이미지 획득 작업은 저장 매체의 모든 정보를 비트 단위로 복사하는 것으로 획득한 이미지는 별도 포렌식 이미지 전용 툴로 분석하며 이를 통해 삭제된 파일도 일부 복구할 수 있다. (운영체제에 파일 삭제 시 실제로 해당 데이터를 모두 삭제하는 것이 아니라 해당 파일에 대한 링크 값을 삭제하고 파일이 저장된 공간에 다른 파일로 덮어쓰기가 가능한 공간임을 표시해줄 뿐 진정한 의미의 파일 삭제는 아니다.) 그러므로 덮어쓰기가 되어 있지 않은 파일은 복구 가능

-> abcd.txt 파일 삭제 시 운영체제가 FAT(File Allocation Table)에서 abcd.txt 파일 이름이 첫 번째 바이트 값을 (-0xe5)로 바꾼다. abcd.txt는 \_bcd.txt로 바뀌고 파일 시스템에서는 이 동작만으로 파일이 지워진 것으로 간주. [EnCase, ilook, 검찰 디지털 증거 분석 시스템으로 복구 가능]

3. 데이터 및 응용 프로그램 증거 수집

· 이메일 분석

여러 사람이 조직적으로 사건을 모의하는 것처럼 피의자가 여러 명일 때는 서로 주고받은 이메일을 분석하여 범죄의 증거를 확보할 수 있다. 일반적으로 각 피의자가 PC를 수거하여 이미지 획득 작업을 거친 뒤 각 PC에서 이메일 관련 파일을 획득한다. 이런 과정이 가능하려면 각 피의자는 아웃룩(Outlook)이나 노츠(Notes)와 같이 PC에 전송된 이메일이 저장되는 형태의 이메일 프로그램을 사용해야 한다. 저장된 메일은 쉽게 찾고 분석할 수 있도록 다시 데이터베이스화 하여 분석자에게 제공됨

· 인터넷 분석

인터넷 분석에는 시스템에 저장되어 있는 인터넷 브라우저의 쿠키나 index.dat 파일, temp 등을 이용해 방문 사이트의 정보를 획득하고 작업 내용을 파악할 수 있다. WFA(Window File Analyzer)로 index.dat 파일 열람

연습문제

01 다음 중 침해 사고에 대응하기 위해 만들어진 조직은? (4)

(1) IACIS (2) CAAT

(2) DARPA (4) CERT

02 침해 대응 절차의 순서대로 번호를 쓰시오.

(2) 침해 사고 발생

(3) 사고 탐지

(5) 제거 및 복구

(1) 사전 대응

(4) 대응

(6) 후속 조치 및 보고

03 침해 사고를 이해하고 언론 및 사이버안전국, 경찰 등에 대해 적절한 방법으로 대응하는 역할을 하는 구성원은? (2)

(1) 시스템 운영 전문가 (2) 대외 언론 및 외부 기관 대응 전문가

(3) 법률 팀 (4) 인사 팀

04 침해 사고 중 위험 등급이 가장 낮은 상황은? (2)

(1) 분산 서비스 거부 공격으로 정상적인 동작이 불가능한 경우

(2) 일반적이지 않은 숨김 파일 또는 디렉터리가 존재하는 경우

(3) 트로이 목마 등의 악성 프로그램이 실행되어 정상적인 접근 제어를 실시해도 다른 경로를 통해 침입자가 지속적인 공격을 시도하는 경우

(4) 침입자에 의해 서버의 중요한 파일이 삭제되고 있는 경우

05 사실 인정의 기초가 되는 실험을 실험자 자신이 법원에 직접 보고하지 않고 진술서나 진술 기재서를 통해 간접적으로 보고하는 경우의 증거를 무엇이라고 하는가?

- 전문 증거

06 포렌식으로 증거를 획득할 때 지켜야 할 기본 원칙 중 같은 환경에서 같은 결과가 나오도록 재현할 수 있어야 한다는 원칙은? (2)

(1) 정당성의 원칙 (2) 재현의 원칙

(3) 신속성의 원칙 (4) 연계 보관성의 원칙

(5) 무결성의 원칙

07 포렌식으로 증거를 획득할 때 지켜야 할 기본 원칙 중 증거의 이송, 분석, 보관, 법정 제출 과정이 명확해야 한다는 원칙은? (4)

(1) 정당성의 원칙 (2) 재현의 원칙

(3) 신속성의 원칙 (4) 연계 보관성의 원칙

(5) 무결성의 원칙

08 포렌식에서 사용하는 증거 라벨의 구성 요소에 대해 간단히 설명하시오.

- 증거 획득 날짜, 피의자 동의 여부, 사건 번호, 라벨 번호, 증거를 획득한 사람, 감독한 사람, 검토 책임자

09 복사본 등의 이차적인 증거가 아닌 원본을 제출하도록 요구하는 영미 증거법상의 원칙은?

- 최량 증거 원칙

10 삭제된 파일을 복구할 수 있는 이유를 알 수 있도록 파일 삭제 과정을 간단히 설명하시오.

- 파일 삭제 시 운영체제가 FAT(File Allocation Table)에서 파일 이름의 첫 번째 바이트 값을 (-0xe5)로 바꾸는데 파일 시스템에서는 이 동작만으로 파일이 지워진 것으로 간주. (링크 정보만 삭제) 끊어진 링크만 연결하면 복구 가능

Chapter 13 보안관리

01. 정보 보안 거버넌스

1. 구현의 어려움

· 조직 구성의 어려움

CSO를 CTO(Chief Technology Officer)나 CIO(Chief Information Officer) 밑에 두는 것이 효율적인지 동등하게 두는 것이 효율적인지 결정하기 어렵다

중앙집중화 vs 연방 체제

· 성과 측정의 어려움

정보 보안의 성격상 투자 성과를 측정하기가 힘들다. 보안에는 상당한 비용이 들어가지만 보안 사고가 일어나지 않는 한 그 성과를 측정하는 데 어려움이 있다

· 조직의 무관심

보안에 무관심한 경영진과 조직 구성원은 효율적인 보안 거버넌스를 구성하는 데 장애물임

2. 구현 조건

\* 5가지 필수 조건

· 전략적 연계

정보 보안 거버넌스는 비즈니스와 IT 기술의 목표, 정보 보안 전략이 서로 연계되어야 한다. 이를 위해 최상위 정보보안 운영위원회의 역할과 책임을 명시하고 정보보안 보고 체계의 합리화를 이뤄야 한다

· 위험 관리

정보 보안 사고의 잠재적 위험을 줄이려면 조직에 적합한 위험 관리 체계를 수립하고 이를 지속적으로 관리하여 수용 가능한 수준으로 위험을 낮춰야 한다. 또한 확인된 위험은 적절한 자원을 할당하여 관리해야 한다

· 자원 관리

정보 보안 지식과 자원을 효율적으로 관리하기 위해 중요한 정보 자산과 인프라를 포함하는 전사적 정보 보안 아키텍처를 확보해야 한다. 또한 정책과 절차에 따른 정보 보안 아웃소싱을 수행하고 아웃소싱 정보 보안 서비스와 통제에 책임을 명시 및 승인하며 기업의 정보 보안 아키텍처와 전사적 아키텍처를 연계해야 한다

· 성과 관리

정보 보안 거버넌스의 효과적인 운영을 위한 척도로 모니터링이나 보고 및 평가에 따른 성과 평가 체제를 운영하고 비즈니스 측면도 고려하여 성과를 평가해야 한다

· 가치 전달

정보 보안 투자의 효과를 높이기 위해서는 구성원들에게 정보 보안의 중요성과 가치를 교육해야 한다. 또한 국제 표준을 기준으로 정보 보안 관리 체계를 갖추어 운영하고 자본의 통제 및 투자에 관한 프로세스를 정보 보안과 통합해야 한다

3. 점검사항

- 보안 거버넌스가 잘 운영되고 있는 기업의 특징 11가지

· 사업 전반의 이슈: 보안은 사업 전반을 관통하는 이슈(enterprise-wide issue)로 조직 전반에 걸쳐 종적/횡적으로 관리해야 한다. 그러므로 보안 관리 프로그램(ESP-Enterprise Security Program)은 인력, 제품, 공장, 프로세스, 정책, 시스템, 기술, 네트워크, 정보를 포함하고 있어야 한다

· 경영진의 책임 의식: 경영진은 조직과 주주 및 공동체의 보안뿐만 아니라 경제적 국가적 보안사항에 대한 책임 의식을 가져야 한다. 이를 위해 적절한 재무 지원 및 관리, 정책과 감사를 수행해야 한다.

· 사업의 필요조건: 보안은 사업의 필요조건(viewed as a business requirement)으로 소모되어 사라지는 비용이 아니라 회사의 가치를 높이기 위한 원가 요소로 이해해야 한다

· 위험관리: 보안의 중요성은 노출된 위험의 크기에 좌우되므로 위험 관리(risk based)가 필요하다

· 역할과 책임: 경영진은 운영 조직과 R&P(Role & Responsibility)과 SoD(Segregation of Dutied Defined)가 명확해야 한다

· 정책과 절차: 보안과 관련된 정책과 절차(address and enforced in policy)는 잘 정비되어 있고 엄격하게 지켜져야 한다

· 능력과 권한: 보안 조직에 속한 인원은 적합한 능력과 권한(adequate resources committed)을 가져야 한다

· 교육과 훈련: 모든 직원이 보안 인식을 갖추고 보안 교육과 훈련(staff aware and trained)을 받아야 한다

· 프로그램 개발 및 변경: 개발 및 변경과 같은 시스템과 소프트웨어의 생명주기에 따른 보안 통제가 이루어져야 한다

· 계획, 수행 및 평가: 사업의 전략 및 계획을 수립할 때 보안을 고려해야 한다

· 검토와 감사: 주기적인 검토와 감사(review and audited)를 통해 보안 사항을 확인하고 개선해야 한다

02. 보안 프레임워크

- 보안 프레임워크는 조직 구성원 모두가 전문가가 아니더라도 조직의 보안 수준을 유지 및 향상하기 위한 체계로 대표적인 것이 ISO 27001 표준

1. ISMS와 PDCA 모델

(Information Security Management System: ISMS) – 기업이 민감한 정보를 안전하게 보존하도록 관리할 수 있는 체계적인 경영 시스템. PDCA를 통해 발전시킬 수 있다. 계획, 수행, 점검, 조치를 반복 순환하는 모델

1) 계획: ISMS 수립

2) 수행: ISMS 구현과 운영

3) 점검: ISMS 모니터링과 검토

4) 조치: ISMS 관리와 개선

K-ISMS

ISO 27001의 국제 표준을 포함하고 우리나라 상황에 맞는 보안 요건을 강화한 정보 보호 관리 체계

03. 보안 조직

· 보안 팀의 역할

- 정보 보안 업무를 기획하고 각종 통제 사항을 관리

- 모니터링과 위협 분석 등을 통해 평시 정보 보안 관리를 이행

- 임직원에 대한 정보 보안 교육을 시행

- 긴급 사항에 대처하기 위한 비상 계획을 수립하고 운영을 지원

· 보안 조직 구성 시 고려 사항

- 기업의 크기

- 시스템 환경

- 기업의 조직 및 관리 구조

- 운영 사이트의 수와 위치

- 사이트 간의 상호 연결 상태

- IT 예산

04. 보안 정책과 절차

· 보안 정책의 특성

- 규칙으로서 지켜져야 할 정책(regulatory)

- 하려는 일에 부합하는 정책이 없을 때 참고하거나 지키도록 권유하는 정책(advisory)

- 어떠한 정보나 사실을 알리는 데 목적이 있는 정책(informative)

05. 접근 제어 모델

- 보안의 세 가지 목적 중 기밀성과 무결성 확보가 접근 제어의 주목적

· 임의적 접근 제어 모델(Discretionary Access Control)

: 정보 소유자가 정보의 보안 레벨을 결정하고 이에 대한 접근 제어도 설정하는 모델

· 강제적 접근 제어 모델(Mandatory Access Control)

- 벨 라파둘라 모델: 정보의 기밀성에 따라 상하 관계가 구분된 정보를 보호하기 위해 사용

- 비바 모델: 정보의 무결성을 높이기 위해 사용

· RBAC(Role-Based Access Control)

각 직책에 대한 권한 세트를 미리 만들어 두고 새로운 사람이 오면 권한을 부여

06. 내부 통제

내부 통제(internal control): 효과적이고 효율적인 업무 운영과 정확하고 신뢰성 있는 재무 보고 체계 유지, 관련 법규와 내부 정책 및 절차를 준수하는 등의 목적을 달성하여 기업이 건전하고 안정적으로 운영되도록 조직의 이사회, 그 외 구성원들이 지속적으로 실행하는 일련의 통제 과정

· 최소 권한(least privilege)

: 한 사람이나 조직이 수행하는 업무에 필요한 이상을 부여받으면 안 된다는 개념

· 직무 분리(segregation of duties)

: 하나의 업무 절차를 두 사람 이상이 수행하도록 업무를 분리한다는 개념

07. 보안 인증

보안 인증: 소프트웨어나 시스템에 대한 품질 표시 마크

· TCSEC

: 오랜 역사를 가진 인증으로 지금까지도 보안 솔루션을 개발할 때 기준이 됨

· ITSEC

: 기밀성만을 강조한 TCSEC와 달리 무결성과 가용성을 포괄하는 표준안 제시

· CC

: 최근에 TCSEC와 ITSEC는 CC(Common Criteria)라는 기준으로 통합되고 있음

08. 개인 정보 보호

- 개인정보는 다음과 같이 정의한다

개인정보 보호법 제2조 1항 – 개인 정보란 살아 있는 개인에 관한 정보로서, 성명, 주민등록번호 및 영상 등을 통해 개인을 알아볼 수 있는 정보

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 6항 – 개인 정보란 생존하는 개인에 관한 정보로서, 성명, 주민번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호, 문자, 음성, 음향 및 영상 등의 정보

개인 정보의 예

신분 관계: 성명, 주소, 본적, 가족관계, 주민번호

개인 성향: 사상, 종교, 가치관, 성향

심신 상태: 건강, 신체적 특징, 장애정도

사회 경력: 학력, 직업, 자격, 전과 여부

경제 관계: 소득 규모, 재산 보유현황, 신용 정보

기타: 홍채, 지문, 위치정보

· OECD 개인 정보 보안 원칙

1) 수집 제한의 법칙: 개인 정보는 적법하고 공정한 방법을 통해 수집되어야 한다

2) 정보 정확성의 원칙: 이용 목적상 필요한 범위 내에서 개인 정보의 정확성, 완전성, 최신성이 확보되어야 한다

3) 목적 명시의 원칙: 개인 정보는 수집 과정에서 수집 목적을 명시하고 명시된 목적에 적합하게 이용되어야 한다

4) 이용 제한의 원칙: 정보 주체의 동의가 있거나 법 규정이 있는 경우를 제외하고 목적 외에 이용하거나 공개할 수 없다

5) 안전성 확보의 원칙: 개인정보의 침해, 누설, 도영 등을 방지하기 위한 물리적, 조직적, 기술적 안전 조치를 확보해야 한다

6) 공개의 원칙: 개인정보의 처리 및 보호를 위한 정책 및 관리자에 대한 정보는 공개되어야 한다

7) 개인 참가의 원칙: 정보 주체의 개인정보 열람/정정/삭제 청구권은 보장되어야 한다

8) 책임의 원칙: 개인정보 관리자에게 원칙 준수 의무 및 책임을 부과해야 한다

연습문제

01 정보 보안 거버넌스의 구현 요건과 설명을 바르게 연결하시오.

(1) 가치 전달: 정보 보안 투자의 효과를 높이기 위해서는 구성원들에게 정보 보안의 중요성과 가치를 교육하고 국제 표준을 기준으로 정보 보안 관리 체계를 갖추어 운영해야 한다

(2) 전략적 연계: 정보 보안 거버넌스는 비즈니스와 IT 기술의 목표, 정보 보안 전략이 서로 연계되어야 한다

(3) 자원 관리: 정보 보안 지식과 자원을 효율적으로 관리하기 위해 중요한 정보 자산과 인프라를 포함하는 전사적 정보 보안 아키텍처를 확보해야 한다

(4) 위험 관리: 정보 보안 사고의 잠재적 위험을 줄이려면 조직에 적합한 위험 관리 체계를 수립하고 이를 지속적으로 관리해야 한다

(5) 성과 관리: 정보 보안 거버넌스의 효과적인 운영을 위한 척도로 모니터링이나 보고 및 평가에 따른 성과 평가 체계를 운영하고 비즈니스 측면도 고려하여 성과를 평가해야 한다

02 다음 중 정보 보안 거버넌스의 점검 사항으로 옳지 않은 것은? (1)

(1) 능력과 권한: 보안과 관련된 모든 권한은 최고경영자에게 있다.

(2) 위험 관리: 보안의 중요성은 노출된 위험의 크기에 좌우된다.

(3) 정책과 절차: 보안과 관련된 정책과 절차를 잘 정비하고 엄격하게 지켜야 한다.

(4) 역할과 책임: 경영진과 운영 조직의 R&R과 SoD가 명확해야 한다

03 ISMS를 발전시키기 위한 PDCA 모델에 대해 설명하시오.

- ISO 27001에서는 PDCA 모델을 통해 ISMS를 발전시켜 나갈 수 있다고 하는데, 여기서 PDCA는 계획, 수행, 점검, 조치를 반복적으로 순환하여 수행하는 모델을 말한다

04 회사의 보안 조직을 구성할 때 고려하는 사항을 세 가지 이상 쓰시오

- 기업의 크기

- 시스템 환경

- 기업의 조직 및 관리 구조

- 운영 사이트의 수와 위치

- 사이트 간의 상호 연결 상태

- IT 예산

05 영미권의 보안 정책에서 조직의 보안 정책이 어떤 원칙과 목적을 가지고 있는지를 밝히는 문서는 무엇인가? (4)

(1) Standards (2) Baselines

(3) Guidelines (4) Security Policy

06 벨 라파둘라 모델과 비바 모델의 차이를 설명하시오.

- 정보의 무결성을 높이려면 비바 모델, 기밀성을 높이려면 벨 라파둘라 모델

07 벨 라파둘라 모델에서 기밀성을 확보하기 위한 규칙으로 옳지 않은 것은? (3)

(1) 상위 문서 읽기 금지 (2) 하위 문서 읽기 허락

(3) 상위 문서 쓰기 금지 (4) 하위 문서 쓰기 금지

08 다음에서 설명하는 접근 통제 모델로 알맞은 것은? (2)

미 국방부 지원 보안 모델로 보안 요소 중 기밀성을 강조한다. 최초의 수학적 모델로 강제적 정책에 의한 접근을 통제한다. 보안 정책은 정보가 높은 레벨에서 낮은 레벨로 흐르는 것을 방지하며 No Read Up, No Write Down으로 표현된다.

(1) 비바 모델 (2) 벨-라파둘라 모델

(3) 만리장성 모델 (4) 클락윌슨 모델

09 직무 분리의 개념을 간단히 설명하시오.

- 직무 분리: 하나의 업무 절차를 두 사람 이상이 수행하도록 업무를 분리한다.

10 시스템 내의 보안 정책을 적용할 수 있고 각 데이터의 보안 레벨 설정이 가능한 TCSEC 등급은 무엇인가? (4)

(1) A1 (2) B3

(3) B2 (4) B1

11 개인 정보를 간단히 정의하시오.

- 개인정보 보호법 제2조 1항 – 개인 정보란 살아 있는 개인에 관한 정보로서, 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보

12 OECD 개인 정보 보안 8원칙을 간단히 설명하시오.

1) 수집 제한의 원칙: 개인 정보는 적법하고 공정한 방법을 통해 수집되어야 한다

2) 정보 정확성의 원칙: 이용 목적상 필요한 범위 내에서 개인 정보의 정확성, 완전성, 최신성이 확보되어야 한다

3) 목적 명시의 원칙: 개인 정보는 수집 과정에서 수집 목적을 명시하고 명시된 목적에 적합하게 이용되어야 한다

4) 이용 제한의 원칙: 정보 주체의 동의가 있거나 법 규정이 있는 경우를 제외하고 목적 외에 이용하거나 공개할 수 없다

5) 안전성 확보의 원칙: 개인정보의 침해, 누설, 도용 등을 방지하기 위한 물리적, 조직적, 기술적 안전 조치를 확보해야 한다

6) 공개의 원칙: 개인정보의 처리 및 보호를 위한 정책 및 관리자에 대한 정보는 공개되어야 한다

7) 개인 참가의 원칙: 정보 주체의 개인정보 열람/정정/삭제 청구권은 보장되어야 한다

8) 책임의 원칙: 개인정보 관리자에게 원칙 준수 의무 및 책임을 부과해야 한다