Chapter 03 네트워크 보안

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

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

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 비지도 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)

정상메일인 텍스트에 포함된 모든 단어의 개수

= 0

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

스팸메일인 텍스트에 포함된 모든 단어의 개수

= 0.27

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

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 보안 관리

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