# 네트워크보안

1. 다음은 OSI 7계층에 대한 설명 중 해당 계층끼리 올바르게 짝지어진 것은?

| |
|---|
| ㄱ. 경로설정, 데이터 교환 및 중계, 트래픽 제어, 패킷정보 전송 |
| ㄴ. 정보형식(포맷), 코드 변환, 데이터 암호화, 데이터 압축, 구문검색, 문맥관리 |
| ㄷ. 프로토콜 방식 PPP, PPTP, L2F, HDLC, SDLC 등 |

| | ㄱ | ㄴ | ㄷ |
|---|---|---|---|
| ① | Network Layer | Session Layer | Data link Layer |
| ② | Network Layer | Session Layer | Transport Layer |
| ③ | Session Layer | Network Layer | Data link Layer |
| ④ | Session Layer | Network Layer | Physical Layer |

2. IDS 공격탐지 방법 중 오용탐지에 대한 설명으로 가장 틀린 것은?

① 시그니처 기반으로 동작한다.
② 속도가 빠르며, 구현이 쉽다.
③ 이미 정립된 공격패턴을 미리 입력하고 매칭하여 침입을 판단한다.
④ 정상인지, 비정상인지 결정하는 임계치 설정이 어렵다.

3. Windows 시스템 명령창에서 netstat -an 명령을 수행한 결과의 일부이다. 구동 중인 서비스로 가장 옳지 않은 것은?

| 프로토콜 | 로컬주소 | 외부주소 | 상태 |
|---|---|---|---|
| TCP | 0.0.0.0:21 | 0.0.0.0:0 | LISTENING |
| TCP | 0.0.0.0:25 | 0.0.0.0:0 | LISTENING |
| TCP | 0.0.0.0:80 | 0.0.0.0:0 | LISTENING |

① FTP
② Telnet
③ SMTP
④ HTTP

4. UDP 포트 스캐닝을 수행할 때 해당 포트에 서비스가 없을 경우 되돌아오는 메시지는 무엇인가?

① ICMP Unreachable
② UDP Unreachable
③ Reset
④ SYN+ACK

5. 다음에서 설명하는 보안 공격 기법은?

| |
|---|
| ㄱ. 두 프로세스가 자원을 서로 사용하려고 하는 것을 이용한 공격이다. |
| ㄴ. 시스템 프로그램과 공격 프로그램이 서로 자원을 차지하기 위한 상태에 이르게 하여 시스템 프로그램이 갖는 권한으로 파일에 접근을 가능하게 하는 공격방법을 말한다. |

① Buffer Overflow 공격
② Format String 공격
③ MITB(Man-In-The-Browser) 공격
④ Race Condition 공격

6. NIC(Network Interface Card)에 대한 설명으로 올바르지 않은 것은 무엇인가?

① 네트워크 정보를 전송하기 위해서 병렬구조로 데이터를 바꾼다.
② 빠른 전송을 위해서 데이터를 코딩 및 압축한다.
③ 목적지 장비의 NIC는 데이터를 수신하고 CPU로 데이터를 전달한다.
④ 네트워크 장비와 LAN 사이의 통신을 준비한다.

7. IDS 탐지기능에서 False Negative의 의미로 가장 올바른 것은 무엇인가?

① false(+)로 표현되고, 공격이 아닌데도 공격이라고 오판
② false(-)로 표현되고, 공격인데도 공격이 아니라고 오판
③ false(+)로 표현되고, 공격인데도 공격이 아니라고 오판
④ false(-)로 표현되고, 공격이 아닌데도 공격이라고 오판

8. 다음은 어느 포렌식 도구에 대한 설명인가?

| |
|---|
| ㄱ. 유닉스 운영체제에서 실행되는 도구 |
| ㄴ. Dan Farmer와 Wietse Venema가 개발 |
| ㄷ. 라이브 시스템에서 현재 상태정보를 캡쳐하고 분석할 수 있는 뛰어난 도구 |
| ㄹ. 법원에서 증거로 채택하기 위해 데이터를 모으는 것이 아니라 어떻게 시스템을 손상시켰는지 알아내도록 돕기 위한 것 |

① Encase
② TCT
③ FTK
④ Safeback

9. 다음 중 동적 라우팅(Dynamic Routing)의 특징에 대한 설명이 아닌 것은?
① 대부분 라우터에서 사용되며 환경이 수시로 변화하는 환경에 적합
② 네트워크 환경 변경 혹은 트래픽이 변경되는 경우에 자동으로 경로변경
③ 패킷을 전달할 경로가 여러 개 있을 경우 가장 큰 효과가 있음
④ 환경 변화가 적거나 상호 연결 네트워크가 적은 형태에 적합

10. 다음 중 FTP 서버에 대한 Bounce Attack의 설명으로 옳지 않은 것은?
① FTP 프로토콜 구조의 허점을 이용한 공격 방법이다.
② Active, Passive 모드를 임의로 변경할 수 있다.
③ FTP Bounce Attack을 이용하면 근원지(Source)를 알 수 없는 전자 메일(Fake Mail)을 보낼 수 있다.
④ FTP 클라이언트가 실행되는 호스트가 아닌 다른 호스트를 지정하더라도 서버는 충실하게 지정된 곳으로 정보를 보낸다.

11. 다음에서 설명하는 침입 차단 시스템(Firewall)의 유형은?

ㄱ. 종단-대-종단 TCP 연결을 허용하지 않는다.
ㄴ. 시스템 관리자가 내부 사용자를 신뢰할 경우 일반적으로 사용한다.
ㄷ. 두 개(자신과 내부 호스트 사용자 간, 자신과 외부 호스트 TCP 사용자 간)의 TCP 연결을 설정한다.
ㄹ. 내부 IP 주소를 숨길 수 있다.

① 패킷 필터링(Packet Filtering) 침입 차단 시스템
② 회로 레벨 프록시(Circuit – Level Proxy) 침입 차단 시스템
③ 응용 프록시(Application Proxy Gateway) 침입 차단 시스템
④ 스테이트풀 패킷 검사(Stateful Packet Inspection) 침입 차단 시스템

12. 다음 중 사용자 패스워드의 보안을 강화하기 위한 솔트(Salt)에 대한 설명으로 가장 옳지 않은 것은?
① 여러 사용자에 의해 중복 사용된 동일한 패스워드가 서로 다르게 저장되도록 한다.
② 솔트 값은 보안 강화를 위하여 암호화된 상태로 패스워드 파일에 저장되어야 한다.
③ 한 사용자가 동일한 패스워드를 두 개 이상의 시스템에 사용해도 그 사실을 알기 어렵게 한다.
④ 해시(Hash) 연산 비용이 증가되어 오프라인의 사전 공격을 어렵게 만든다.

13. <보기>의 설명에 해당하는 네트워크 보안 솔루션은?

ㄱ. 사용자 컴퓨터 및 네트워크 단말기가 네트워크에 접근하기 전에 보안정책을 준수했는지 여부를 검사하여 네트워크 접속을 통제하는 기술
ㄴ. 네트워크 접근제어 기술을 이용하여 내부 네트워크의 자원을 관리하고, 네트워크 내의 장애 및 사고 원인을 예방·탐지하고 제거하여 안정적인 네트워크 운영·관리가 가능

① 역추적 시스템 ② NAC
③ UTM ④ ESM

14. 다음 중 비밀키 시스템에 대한 설명으로 맞는 것은 몇 개 인가?

ㄱ. 암호화 키와 복호화 키가 다름
ㄴ. 암호화 과정이 복잡하여 속도가 느림
ㄷ. 디지털 서명이 어려움
ㄹ. 평문을 암호화하는데 가장 많이 사용됨
ㅁ. RSA, PGP 암호 알고리즘이 가장 대표적임

① 2 ② 3 ③ 4 ④ 5

15. 다음 중 세션 하이재킹(Session Hijacking)에 대한 설명으로 틀린 것은?
① TCP의 취약점을 이용한 능동적 공격 방법이다.
② Telnet, FTP 등 TCP를 사용한 모든 세션의 갈취가 가능하다.
③ TCP의 Sequence Number를 이용한 공격이다.
④ TCP의 취약점을 이용하여 클라이언트와 서버 양쪽 모두 데이터 전송을 못하게 하는 공격이다.

16. 다음 중 DNS 레코드에 대한 설명으로 가장 옳지 않은 것은?

① CNAME 레코드 : 여러 개의 호스트가 같은 IP 주소로 응답할 경우 설정이 용이하다.
② MX 레코드 : 메일 서버가 이메일을 전달하기 위해 DNS에서 읽어오는 레코드이다.
③ NS 레코드 : 역방향 영역 안에서 IP를 도메인 주소로 변경하기 위한 호스트 등록작업을 한다.
④ A 레코드 : 호스트는 각 영역별로 중복될 수는 있지만 같은 영역 안에 중복된 호스트가 있으면 안된다.

17. 다음에서 설명하는 것은 무엇인가?

ㄱ. 초기에는 PPP(Point to Point Protocol)에서 사용하기 위해 개발되었으나, 현재는 무선랜 표준인 IEEE 802.1x에서 사용자 인증 방법으로 사용
ㄴ. 어떤 링크에도 접속이 가능한 단순한 캡슐화 개념의 프로토콜로 모든 링크에 적용될 수 있으며 다양한 인증 방법을 사용 할 수 있도록 설계됨
ㄷ. 네트워크 접근을 위한 인증 서버와 무선장비 사이에 상호 인정을 허용

① SSID
② WEP
③ EAP
④ MAC

18. 다음에서 설명하고 있는 서비스 공격기법에 해당하는 것은?

ㄱ. TCP의 3-Way Handshake의 취약점을 이용한 공격
ㄴ. 출발지 IP주소를 존재하지 않는 IP주소로 변조한 후 다량의 SYN패킷을 전송하여 공격대상 시스템의 백로그 큐(Backlog Queue)를 가득 채워 시스템을 마비시키는 공격
ㄷ. 시스템은 백로그 큐의 모든 자원을 소모하여 정상적인 서비스 불가능

① Smurfing
② SYN Flooding
③ LAND Attack
④ Teardrop

19. 다음은 보안시스템들에 대한 설명이다. (가), (나)에 들어갈 용어로 알맞은 것은?

(가)은(는) 외부 침입에 대한 정보를 수집하고 분석하여 침입활동을 탐지해 이에 대응하도록 보안 담당자에게 통보하는 기능을 수행하는 네트워크 보안 시스템이다. (나)은(는) 침입을 탐지했을 경우에 이에 대한 대처까지 수행한다.
즉, (나)은(는) 예방적이고 사전에 조치를 취하는 기술이고, (가)은(는) 탐지적이고 사후에 조치를 취하는 기술이다.

① (가) IDS (나) Firewall
② (가) IDS (나) IPS
③ (가) Firewall (나) IPS
④ (가) Firewall (나) IDS

20. 다음에서 설명하고 있는 네트워크 공격 기법은 무엇인가?

ㄱ. 공격자는 출발지 IP로 스푸핑하여 SYN패킷을 공격 경유지 서버로 전송한다.
ㄴ. SYN패킷을 받은 경유지 서버는 스푸핑된 IP의 타깃 서버로 SYN/ACK를 전송한다.
ㄷ. 타깃 서버는 수많은 SYN/ACK를 받아 다운된다.

① DoS
② DDoS
③ DRDos
④ SYN Flooding