**1과목 : 과목 구분 없음**

1. ICMP(Internet Control Message Protocol)의 기능으로 옳지 않은 것은?

① 네트워크 데이터 전송 오류 보고
❷ 멀티캐스트 그룹 멤버십 보고
③ 네트워크 혼잡 보고
④ Timeout 보고

2. 다음에서 설명하는 방화벽 구성 방법은?

> 네트워크로 들어오는 트래픽에 대해서 스크리닝 라우터는 패킷 필터링으로 1차 방어를 하고, 베스천 호스트로 단일 홈 게이트웨이에서 프록시 등으로 2차 방어를 한다. 또한, 베스천 호스트는 스크리닝 라우터를 거치지 않은 모든 접속을 거부하며, 스크리닝 라우터도 베스천 호스트를 거치지 않은 모든 접속을 거부하도록 설정한다.

❶ 스크린된 호스트 게이트웨이 ② 스크리닝 라우터
③ 단일 홈 게이트웨이 ④ 이중 홈 게이트웨이

3. OSI 7계층과 각 계층에서 송수신되는 프로토콜 데이터 단위(PDU)를 바르게 연결한 것은? (순서대로 ㄱ, ㄴ, ㄷ)

> ㄱ. 전송 계층 ㄴ. 네트워크 계층
> ㄷ. 데이터링크 계층

① 프레임, 세그먼트, 패킷 ② 프레임, 패킷, 세그먼트
③ 세그먼트, 프레임, 패킷 ❹ 세그먼트, 패킷, 프레임

4. ㉠~㉣에 들어갈 윈도우 명령어를 바르게 연결한 것은? (순서대로 ㉠, ㉡, ㉢, ㉣)

> - ( ㉠ )은(는) 도메인 네임을 얻거나 IP주소 매핑을 확인하기 위해 DNS에 질의할 때 사용하는 명령
> - ( ㉡ )은(는) 지정한 IP주소의 통신 장비 접속성을 확인하기 위한 명령
> - ( ㉢ )은(는) 패킷이 목적지까지 도달하는 동안 거쳐 가는 라우터의 IP주소를 확인하는 명령
> - ( ㉣ )은(는) 전송 프로토콜, 라우팅 테이블, 네트워크 인터페이스, 네트워크 프로토콜 통계를 위한 네트워크 연결 상태를 보여주는 명령

① ping, tracert, netstat, nslookup
② nslookup, ping, netstat, tracert
③ ping, nslookup, tracert, netstat
❹ nslookup, ping, tracert, netstat

5. IPsec에 대한 설명으로 옳지 않은 것은?

① AH(Authentication Header)－IP 패킷에 대한 인증과 무결성을 제공하지만, 기밀성은 제공하지 않는다.
② ESP(Encapsulating Security Payload)－IP 패킷에 대한 기밀성, 인증, 무결성을 제공하며 IPsec의 전송 모드와 터널 모드에서 모두 동작 가능하다.
❸ IKE(Internet Key Exchange)－IPsec의 보안 연관(security association)을 수립하고 필요한 보안키 교환 기능을 제공하지만, 인증서를 통한 개체 인증은 제공하지 않는다.
④ MIB(Management Information Base)－IPsec의 보안 정책이나 관리 정보를 저장하는 데 사용될 수 있는 자료구조이다.

6. 다음에서 설명하는 스위치 패킷 전송 방식은?

> 수신한 프레임의 목적지 주소를 확인하고 목적지 주소의 포트로 프레임을 즉시 전송하는 방식으로 지연 시간이 최소화되나 수신한 프레임에 오류가 발생할 때는 목적지 장치에서 폐기하는 방식이다.

❶ 컷스루 방식(cut-through) ② 저장 후 전송 방식
③ 반이중 방식 ④ 전이중 방식

7. 네트워크 접근 제어(NAC) 시스템에 대한 설명으로 옳지 않은 것은?

① 네트워크에 접근하는 단말기의 보안정책 준수 여부를 검사하여 네트워크 접속을 통제할 수 있다.
② 보안정책에서 필요에 따라 특정 단말기에 보안 소프트웨어 설치를 유도할 수 있다.
❸ DHCP를 이용한 방식은 공인인증서 기반으로 단말기에 URL을 할당하여 네트워크 접속을 통제한다.
④ 네트워크 접근 시 인증을 위해 Active Directory, Kerberos, LDAP 등을 사용한다.

8. 안전한 해시함수(SHA)에 대한 설명으로 옳은 것은?

① 한 블록을 처리할 때 SHA-512는 SHA-384보다 많은 라운드(round)를 거친다.
❷ SHA-1의 메시지 다이제스트(message digest) 길이는 160bits이다.
③ SHA-256의 입력메시지 최대 길이는 2128bits이다.
④ SHA-512의 입력메시지 최대 길이는 2512bits이다.

9. TCP 헤더의 제어용 플래그(control flags, 1: on, 0: off) 6bits에 할당된 값 010001이 의미하는 것은?

① SYN(synchronization)과 RST(reset) 값이 1이다.
❷ ACK(acknowledgment)와 FIN(finish) 값이 1이다.
③ URG(urgent)와 PSH(push) 값이 1이다.
④ SYN(synchronization)과 PSH(push) 값이 1이다.

10. 무선랜 보안에 대한 설명으로 옳은 것만을 모두 고른 것은?

> ㄱ. 802.11b에서 사용된 WEP는 RC4 암호화 알고리즘을 기본으로 사용한다.
> ㄴ. WEP는 사전에 공유된 비밀키를 인증에 사용한다.
> ㄷ. RADIUS 프로토콜은 엑세스 포인트(access point)와 무선 단말기 사이에 사용되는 프로토콜이다.
> ㄹ. 802.1X는 포트 기반 접근제어 기능을 제공하며 인증자(authenticator)는 RADIUS 서버이다.

❶ ㄱ, ㄴ ② ㄱ, ㄷ
③ ㄴ, ㄷ ④ ㄷ, ㄹ

11. 포트 스캔 공격에 대한 설명으로 옳지 않은 것은?

① TCP Full Open 스캔에서 대상 시스템의 포트가 열린 경우 공격자는 TCP Three-way handshaking의 모든 과정을 거친다.

② TCP Half Open 스캔에서 대상 시스템의 포트가 열린 경우 공격자가 SYN 세그먼트를 보내면 대상 시스템이 SYN+ACK 세그먼트로 응답하고 공격자는 즉시 RST 세그먼트를 보내 연결을 끊는다.

❸ NULL, FIN, XMAS 스캔에서 대상 시스템의 포트가 열린 경우에만 공격자에게 RST 세그먼트가 되돌아오고, 닫힌 경우에는 아무런 응답이 없다.

④ UDP 스캔에서 대상 시스템의 포트가 닫힌 경우 대상 시스템은 공격자에게 ICMP unreachable 패킷을 보내지만, 열린 경우에는 아무런 응답이 없다.

**12. DoS(Denial of Service) 공격 유형에 해당하는 것은?**

① Eavesdropping 공격 ② Man-In-The-Middle 공격
❸ Smurf 공격 ④ Stealth Scan 공격

**13. 보안 솔루션에 대한 설명으로 옳지 않은 것만을 모두 고른 것은?**

> ㄱ. SSO(Single Sign On)는 하나의 인증 시스템을 통해 인증 시스템과 연결된 다른 시스템에 추가적인 인증 과정 없이 로그인하는 기능을 제공한다.
> ㄴ. PKI(Public Key Infrastructure)는 네트워크 보안을 제공하기 위해 패킷을 분석하고 정상적인 패턴이 아닌 경우 차단 등의 기능을 제공한다.
> ㄷ. FDS(Fraud Detection System)는 다양한 네트워크 기기의 인증을 통합 제어하는 기능을 제공한다.
> ㄹ. DRM(Digital Rights Management)은 문서 열람, 편집, 출력 등에 관한 접근 권한을 설정하는 기능을 제공한다.

① ㄱ, ㄷ ❷ ㄴ, ㄷ
③ ㄴ, ㄹ ④ ㄷ, ㄹ

**14. 다음에서 설명하는 보안 프로토콜의 특성은?**

> 공격자에게 비밀키 혹은 패스워드가 노출되더라도 그 후에 키분배 과정을 거쳐 새롭게 생성되는 세션키(session key)를 알 수 없다.

① Inverse Cipher
② Zero-Knowledge Authentication
❸ Perfect Forward Secrecy
④ Second Preimage Resistance

**15. 블록암호 운영모드 중 암호화 알고리즘과 복호화 알고리즘이 둘 다 필요한 것은?**

❶ Cipher Block Chaining ② Cipher Feedback
③ Output Feedback ④ Counter

**16. DNS 서버로부터 얻을 수 있는 레코드 종류와 그 내용이 옳지 않은 것은?**

① NS(Name Server)-각 도메인에 한 개 이상 있어야 하며, DNS 서버를 가리킨다.
② MX(Mail Exchanger)-도메인 이름으로 보낸 메일을 받는 호스트 목록을 지정한다.
❸ PTR(Pointer)-도메인 이름에 IP주소를 매핑하는 역할을 한다.
④ CNAME(Canonical Name)-호스트의 다른 이름을 정의하는 데 사용된다.

**17. TCP 세션 하이재킹(session hijacking) 공격의 보안 대책으로 옳지 않은 것은?**

❶ Inverse DNS Lookup 탐지
② ACK Storm 탐지
③ 패킷 유실과 재전송 증가 탐지
④ TCP 순서 번호(sequence number) 비동기 상태 탐지

**18. 인터넷 보안 위협에 대한 설명으로 옳지 않은 것은?**

① 이블 트윈 공격(evil twin attack)은 사회관계망에서 공격 대상의 지인 또는 특정 유명인으로 위장해 공격 대상으로부터 중요한 정보를 획득하는 데 사용된다.
❷ Man-In-The-Browser 공격은 웹브라우저 내에 악성코드를 설치하여 웹브라우저에서 표시되는 웹페이지 내용을 도청하거나 위·변조하는 공격으로 SSL/TLS 등을 통해 통신구간을 암호화하지 않으면 대응하기 힘들다.
③ 피싱(phishing)이란 진짜 웹사이트와 거의 동일하게 꾸며진 가짜 웹사이트를 통해 개인정보를 탈취하는 것이다.
④ 파밍(pharming)이란 도메인을 탈취하거나 악성코드를 통해 DNS의 이름을 속여 사용자가 진짜 웹사이트로 오인하게 만들어 개인정보를 탈취하는 것이다.

**19. 침입탐지 시스템에 대한 설명으로 옳은 것만을 모두 고른 것은?**

> ㄱ. 호스트 기반 침입탐지 시스템은 내부 호스트에서 동작하는 악성코드의 스택 오버플로(stack overflow) 공격을 막기 위해 스택 영역을 실행 불가능하게 만든다.
> ㄴ. 오용 탐지(misuse detection)는 정립된 공격 패턴을 활용해 제로데이(zero day)와 같은 새로운 형태의 공격을 탐지하는 데 사용된다.
> ㄷ. 이상 탐지(anomaly detection)는 호스트 기반과 네트워크 기반 침입탐지 시스템에 모두 적용될 수 있는 탐지 방법으로 오랜 기간 수집된 올바른 사용자 행동패턴을 활용해 통계적으로 공격을 탐지하는 데 사용된다.
> ㄹ. False Negative는 실제 공격임에도 공격을 탐지하지 못하는 것을 의미한다.

① ㄱ, ㄴ ② ㄱ, ㄷ
③ ㄴ, ㄷ ❹ ㄷ, ㄹ

**20. 다음에서 설명하는 웹 보안 취약점은?**

> 악성 스크립트가 포함된 웹사이트에 방문한 사용자가 악성 스크립트에 의해 공격자가 의도한 행위를 수행하는 것이다. 이러한 악성 스크립트는 사용자의 웹브라우저에서 실행되지 않고 웹사이트에서 실행된다.

① SQL 명령 삽입

② 안전하지 않은 직접 객체 참조
③ 취약한 인증 및 세션 관리
❹ 크로스 사이트 요청 변조



| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| ② | ① | ④ | ④ | ③ | ① | ③ | ② | ② | ① |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| ③ | ③ | ② | ③ | ① | ③ | ① | ② | ④ | ④ |