정보보호론

1. 선택된 폴더의 데이터를 완전 백업(Full Backup)한 후, 다음번 완전 백업(Full Backup)을 시행하기 전까지는 변경, 추가된 데이터만 백업하는 방식은?

① 일반 백업(Normal Backup)
② 매일 백업(Daily Backup)
③ 복사본 백업(Copy Backup)
④ 차등 백업(Differential Backup)
⑤ 증분 백업(Incremental Backup)

2. 강화된 무선 네트워크 보안 기법으로서 기존 IEEE 802.11의 보안 취약성을 해결한 IEEE 802.11i 및 RSN 보안 기법에 해당하는 것은?

① ARIA
② AES
③ RC4
④ WPA2
⑤ EAP

3. 아래 표에서 ㉠과 ㉡의 특징을 갖는 주요 악성코드를 옳게 짝지은 것은?

㉠	㉡
컴퓨터 취약점을 이용하여 네트워크 통한 감염 및 실행	컴퓨터 사용 시 자동으로 광고를 표시하는 악성코드
자기복제: O	자기복제: X
독립적인 프로그램: O	독립적인 프로그램: X

	㉠	㉡
①	웜	애드웨어
②	트로이 목마	애드웨어
③	애드웨어	바이러스
④	바이러스	트로이 목마
⑤	웜	트로이 목마

4. 암호 알고리즘에 대한 설명으로 옳지 않은 것은?

① Adaptive Chosen-plaintext Attack은 Ciphertext-only Attack보다 공격자 입장에서 더 높은 자유도를 갖는다.
② Differential Cryptanalysis는 평문과 암호문 간의 차분 정보를 사용하는 암호 공격 기법이다.
③ Side-channel Attack은 소비 전력이나 실행 시간 등 암호의 구현상 특성을 활용하는 공격 기법이다.
④ Birthday Attack은 공개키 암호 알고리즘의 암호 안전도를 측정하는 데 사용된다.
⑤ 해시함수는 Collision Resistance를 가져야 한다.

5. 양자내성암호(Post-Quantum Cryptography)에 대한 설명으로 옳지 않은 것은?

① 양자컴퓨터의 실현 가능성이 높아짐에 따라 기존 대칭키 암호를 대체하는 목적으로 만들어지고 있다.
② RSA는 양자내성암호로 볼 수 없다.
③ 양자내성암호의 종류로는 격자 기반 암호, 코드 기반 암호, 해시 기반 암호 등이 있다.
④ 양자내성암호는 알고리즘의 종류에 따라 키 교환 목적, 전자서명 목적으로 사용된다.
⑤ 양자내성암호는 NIST에 의해 표준화가 진행되고 있다.

6. 다음에서 설명하는 DoS 공격 유형은?

> 패킷을 전송할 때 출발지 IP주소와 목적지 IP주소의 값을 똑같이 만들어서 공격대상에게 보낸다. 이때 조작된 목적지 IP주소는 공격대상의 IP주소이다. 이렇게 목적지 주소가 조작된 패킷을 공격대상에게 보내면 시스템은 공격자가 보낸 SYN패킷의 출발지 주소를 참조하여 응답패킷을 보내는데, 이때 패킷이 네트워크 밖으로 나가지 않고 자신에게 다시 되돌아오며, 돌아온 패킷의 출발지 IP주소에는 또다시 자신의 IP주소가 기록되어 시스템을 마비시키는 공격의 종류이다.

① Ping of Death
② Land Attack
③ SYN Flooding Attack
④ Smurf Attack
⑤ Mail Bomb

7. OSI 7 Layer 중 계층별 프로토콜의 연결이 옳지 않은 것은?

	OSI 모델	프로토콜
①	응용계층	HTTP, FTP
②	표현계층	MPEG, Telnet
③	전송계층	TCP, UDP
④	네트워크계층	IP, ICMP
⑤	데이터링크계층	Ethernet

8. IP주소에 대한 설명으로 옳지 않은 것은?

① IP주소는 TCP/IP 프로토콜로 접속된 네트워크에서 각 컴퓨터를 식별하는 데 사용하는 숫자이다.

② InterNIC에서 관리하는 IP주소는 네트워크와 호스트(노드)로 구성되어 있다.

③ IPv6는 IP주소 공간의 부족, 12개 필드로 구성된 IPv4 헤더 영역의 비효율적인 사용, 네트워크 프래그멘테이션 증가로 인한 스위칭의 비효율성 문제를 해결하기 위해 개발되었다.

④ IPv4 주소는 상위 4비트 값을 기초로 다섯 개의 클래스로 분류된다.

⑤ 클래스 D는 멀티캐스트용 주소이다.

9. RSA 암호 시스템에서 오일러 Totient 함수는 $\varnothing(n)$={n보다 작은 양의 정수 중에서 n과 서로소인 양의 정수의 개수}로 정의할 수 있다. p와 q가 각각 서로 다른 소수(Prime Number)라고 가정할 때, 옳지 않은 것은?

① $\varnothing(p) = p - 1$

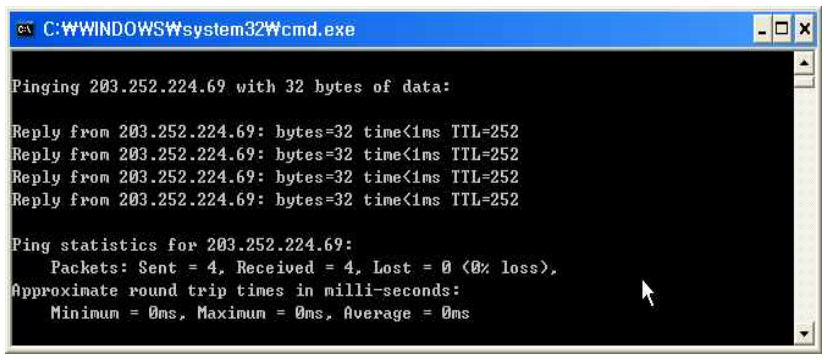
② $\varnothing(p \cdot q) = \varnothing(p)\varnothing(q)$

③ $a^{\varnothing(2 \cdot p)} \not\equiv a^{\varnothing(p)} (\mathrm{mod}\, p)$: 만일 p가 2보다 큰 소수이고, a는 p에 의하여 나누어지지 않는 양의 정수일 때

④ $a^{\varnothing(n)} \equiv 1 (\mathrm{mod}\, n)$: 서로소인 a와 n에 대하여

⑤ $\varnothing(35) = 24$

10. 다음은 ping 명령을 실행한 것이다. TTL이 의미하는 것은?



① 해당 IP주소 서브넷의 대표 주소이다.

② 전송 속도를 보여주며, 단위는 ms이다.

③ 전송된 패킷의 바이트 크기이다.

④ 해당 패킷의 생명주기이다.

⑤ 발신 패킷과 수신 패킷 간의 손실률을 보여준다.

11. 「개인정보보호법」상 민감정보에 해당하지 않는 것은?

① 건강 및 성생활에 관한 정보

② 사상, 신념 및 정치적 견해

③ 유전정보

④ 인종, 민족에 관한 정보

⑤ 사번, 학번, 법인등록번호, 사업자등록번호에 관한 정보

12. 다음과 관련된 디지털 포렌식의 기본 원칙은?

> ○ 적법한 절차를 따르지 않고 수집한 증거는 위법수집 증거에 해당되기 때문에 이를 사용할 수 없다.
>
> ○ 독수독과이론(Fruit of the Poisonous Tree) 또는 독과수이론

① 기밀성의 원칙

② 무결성의 원칙

③ 정당성의 원칙

④ 가용성의 원칙

⑤ 연계보관성의 원칙

13. SSL Record 프로토콜의 처리 순서가 올바른 것은?

① 압축 → 단편화 → 암호화 → MAC → 전송

② 압축 → 단편화 → MAC → 암호화 → 전송

③ MAC → 암호화 → 압축 → 단편화 → 전송

④ 암호화 → MAC → 단편화 → 압축 → 전송

⑤ 단편화 → 압축 → MAC → 암호화 → 전송

14. 인터넷 환경에서 많이 사용 중인 보안 프로토콜에 대한 설명으로 옳지 않은 것은?

① ISAKMP 프로토콜은 IPsec에서 보안 연관을 생성하기 위해 사용된다.

② IPsec은 IPv4와 IPv6에서 사용할 수 있는 보안 프로토콜이므로 상위계층 보안이 필요한 VPN을 제공하지 못한다.

③ IPsec에서 제공하는 Transport 모드는 두 엔드포인트 장치 간에 Point-to-point 연결을 제공한다.

④ IPsec은 데이터 보호를 위해 AH와 ESP 보안 프로토콜을 제공한다.

⑤ IPsec는 상호간 안전한 키 분배를 위해 Diffie-Hellman 키 분배 프로토콜을 사용할 수 있다.

15. Kerberos 보안 프로토콜에 대한 설명으로 옳지 않은 것은?

① 발급 받은 TGT(Ticket Granting Ticket)는 일회성으로 재사용이 불가능하다.

② Kerberos의 정상적인 동작을 위해서는 관련된 호스트의 시간 동기화가 필요하다.

③ Kerberos는 SSO(Single Sign On)와 상호 인증 기능을 제공한다.

④ Kerberos에 참여하는 인증서버는 클라이언트에 TGT(Ticket Granting Ticket)를 발급한다.

⑤ Kerberos는 대칭키 암호 기반의 인증 프로토콜로 신뢰할 수 있는 제3자를 필요로 한다.

16. <보기>에 해당하는 계층별 보안 프로토콜과 세부 프로토콜은?

<보 기>

이 프로토콜의 각 메시지는 2바이트로 되어 있으며, 첫 바이트는 발생한 메시지 오류의 심각성을 알려주기 위해 경고(warning) 또는 치명적(fatal) 값을 가진다. 만약 레벨이 치명적이라면, 계층 보안 프로토콜은 즉시 연결을 종결시킨다. 동일 세션상의 다른 연결들은 지속될 수 있지만, 이 세션에서 새로운 연결이 만들어질 수는 없다. 두 번째 바이트에는 구체적인 경보를 나타내는 코드가 들어있다.

① IPsec에서의 경보 프로토콜(Alert Protocol)

② SSL에서의 경보 프로토콜(Alert Protocol)

③ SSH에서의 경보 프로토콜(Alert Protocol)

④ S/MIME에서의 경보 프로토콜(Alert Protocol)

⑤ SSH에서의 연결 프로토콜(Connection Protocol)

17. 다음 네트워크 기반과 호스트 기반 IDS(침입탐지시스템)의 특징 중 옳지 않은 것만을 모두 고르면?

<네트워크 기반(Network-based)>

ㄱ. 전체 네트워크에 대한 침입탐지가 가능하다.

ㄴ. 탐지된 침입의 실제 공격 성공 여부를 네트워크단에서는 알지 못한다.

ㄷ. 기존 네트워크 환경을 크게 변경하여야만 설치가 가능하다.

<호스트 기반(Host-based)>

ㄹ. 네트워크 기반 IDS가 탐지 불가능한 로컬 시스템에 대한 공격을 탐지할 수 있다.

ㅁ. 모든 개별 호스트에 대한 설치 및 관리를 하기 때문에 네트워크 기반 IDS 보다 설치 및 관리가 쉽다.

ㅂ. 고부하·스위치 네트워크에서도 적용이 가능하며, 우회 가능성이 거의 없다.

① ㄱ, ㄹ

② ㄴ, ㅁ

③ ㄴ, ㅂ

④ ㄷ, ㅁ

⑤ ㄷ, ㅂ

18. 재해복구시스템의 복구 수준별 유형을 비교한 설명으로 옳지 않은 것은?

① Mirror Site는 주센터와 동일한 수준의 정보 기술 자원을 원격지에 구축하고 Active-Active 상태로 운영한다.

② Hot Site는 주센터와 동일한 수준의 정보 기술 자원을 원격지에 구축하여 대기(Standby) 상태로 유지한다.

③ Warm Site는 중요성이 높은 정보기술 자원만 부분적으로 재해복구센터에 보유한다.

④ Cold Site는 데이터만 원격지에 보관하고 이의 서비스를 위한 정보자원을 확보하지 않거나 장소 등 최소한으로만 확보한다.

⑤ 재해발생시 RTO(Recovery Time Objective)가 빠른 것은 Hot Site → Mirror Site → Warm Site → Cold Site 순서이다.

19. 악성코드에 대한 설명으로 옳지 않은 것은?

① Backdoor는 비인가된 접근을 허용하는 것으로 공격자가 사용자 인증 과정 등의 정상 절차를 거치지 않고 프로그램이나 시스템에 접근하도록 지원한다.

② Rootkit은 보안 관리자나 보안 시스템의 탐지를 피하면서 시스템을 제어하기 위해 공격자가 설치하는 악성파일이다.

③ Ransomware는 사용자의 파일을 암호화하여 사용자가 실행하거나 읽을 수 없도록 한 뒤 자료복구 대가로 돈을 요구한다.

④ Launcher는 Downloader나 Dropper 등으로 생성된 파일을 실행하는 기능을 가지고 있다.

⑤ Exploit은 악성코드에 감염되지 않았는데도 악성코드를 탐지했다고 겁을 주어 자사의 안티바이러스 제품으로 제거해야 한다는 식으로 구매를 유도한다.

20. NAT(Network Address Translation)에 대한 설명으로 옳지 않은 것은?

① 사용자에게 투명성을 제공함으로써 처리 속도가 빠르다.

② 한정된 공인 IP주소 부족 문제의 해결이 가능하다.

③ 주소 변환 기능을 제공한다.

④ 외부 컴퓨터에서 사설 IP를 사용하는 호스트에 대한 접근이 어려워 보안 측면에서 장점을 제공한다.

⑤ 외부 컴퓨터에 네트워크 구조를 노출하지 않는 보안상의 이점을 제공한다.