정보보호론

1. 다음 설명에서 제시하는 공격의 명칭은?

> 사용자가 특정 웹 사이트에 접속하기 위해 올바른 URL을 입력하였지만, 실제로는 해커가 만들어 놓은 웹 사이트에 접속되었다. 해커의 웹 사이트에서는 불법적으로 개인정보가 수집되고 있었다. 사용자의 컴퓨터는 공격자에게 점유되어 정상적인 URL을 입력해도 이에 해당하는 IP 주소가 공격자의 웹 서버로 연결되도록 되어 있었다.

① Pharming
② Smishing
③ QRshing
④ Phishing
⑤ SQL Injection

2. 네트워크 보안과 관련된 다음 설명에서 ㉠, ㉡에 들어갈 용어는?

> 네트워크 인터페이스 카드가 가지고 있는 모드 중 (㉠) 모드를 설정하여 네트워크 인터페이스 카드를 거치는 모든 데이터를 확인하는 스니핑 공격을 수행할 수 있다. 이 모드 설정을 위해서 Linux 환경에서는 (㉡) 명령어를 활용한다.

㉠	㉡
① non-promiscuous	netstat
② promiscuous	netstat
③ non-promiscuous	ifconfig
④ promiscuous	ifconfig
⑤ non-promiscuous	ipconfig

3. RSA 암호 시스템에서 밥이 앨리스의 공개키 (e, N)= (11, 143)을 취득하여 앨리스에게 평문 4를 암호화하여 보내고자 한다. 이때 전송되는 암호문은?

① $11^4 \bmod 143$
② $4^{11} \bmod 143$
③ $4^{143} \bmod 11$
④ $11^{143} \bmod 7$
⑤ $4^{143} \bmod 7$

4. 다음과 같은 정보보안 요구사항이 존재할 때 필요한 정보보호 시스템들을 짝지은 것으로 옳은 것은?

> 공인 IP 주소 자원의 효율적인 관리를 위해 사설 IP와의 연계를 수행하고 조직 내부의 네트워크 구조를 외부에서 알 수 없도록 하고 싶다. 또한, 내부에서 외부로의 정보유출을 탐지하여 개인정보 및 민감 정보의 유출을 차단하고자 한다.

① NAT-VPN
② IPS-DLP
③ NAT-SSL
④ IPS-SSL
⑤ NAT-DLP

5. 커버로스(Kerberos)에 대한 설명으로 옳지 않은 것은?

① 신뢰받는 제3자인 키 배포 기관이 구성원들 중간에 개입하는 방법이다.
② 커버로스는 세션 키를 이용한 티켓 기반 인증 기법을 제공한다.
③ 토큰을 이용한 인증 프로토콜이다.
④ 인증 서버가 사용자에게 발급한 티켓(즉, 티켓-승인 티켓)은 유효기간 내에 재사용할 수 있다.
⑤ 분산 시스템 환경에서 SSO(Single Sign On) 시스템을 구축할 수 없다.

6. 다음 설명에서 제시하는 목적으로 활용되는 네트워크 보안 기술은?

> 조직 내에 운영되는 다양한 정보보안 장비 및 IT 시스템들의 이벤트 로그를 수집, 분석하여 이상 징후 및 위험사항을 파악한다. 이렇게 파악된 결과를 인지하기 쉬운 형태로 가공하여 경영진에 보고하기도 한다. 이상 징후의 도출에 전문가의 경험을 활용하거나 인공지능 기술을 활용한다.

① SIEM
② DLP
③ VPN
④ NAT
⑤ IPS

7. 보안 프로토콜에 대한 설명으로 옳지 않은 것은?

① 경량 프로토콜인 CoAP는 DTLS를 사용하여 보안성을 제공한다.
② 사물인터넷 프로토콜인 MQTT는 TLS 프로토콜을 사용한다.
③ TLS 프로토콜은 UDP 상에서 동작하므로 많은 인터넷 응용에서 사용된다.
④ HTTPS는 HTTP 프로토콜에 SSL/TLS를 적용한 것이다.
⑤ SSH은 TCP 프로토콜 상에서 사용되며, telnet의 안전성 보장에 사용된다.

8. 블록 암호(Block Cipher) 모드에 대한 설명으로 옳지 않은 것은?

① ECB(Electronic CodeBook) 모드는 평문 블록을 암호화한 것이 그대로 암호문 블록이 된다.

② CBC(Cipher Block Chaining) 모드는 암호화 전에 XOR 연산을 수행한다.

③ CFB(Cipher FeedBack) 모드는 평문 블록을 암호 알고리즘으로 직접 암호화한다.

④ OFB(Output FeedBack) 모드는 암호 알고리즘의 출력을 암호 알고리즘의 입력으로 피드백한다.

⑤ CTR(CounTeR) 모드는 스트림 암호의 일종으로 카운터의 값이 암호화의 입력이 된다.

9. 파일을 실행시킬 때 사용자의 권한이 아닌 일시적으로 파일 소유자(특히 관리자)의 권한을 가지기 때문에 공격에 많이 사용되는 것은?

① setuid

② setgid

③ uid

④ gid

⑤ sticky bit

10. 개인정보 비식별화 조치로 볼 수 없는 것은?

① 가명 처리

② 총계 처리

③ 데이터 값 삭제

④ 범주화 수행

⑤ 공개키 암호 기반 서명값 생성

11. TCP/IP 기반의 네트워크에서 목적지 호스트까지의 경로를 파악하기 위해서 데이터그램의 TTL 값과 ICMP Time Exceeded 메시지를 기반으로 동작되는 도구는?

① ipconfig

② traceroute

③ nslookup

④ netstat

⑤ telnet

12. 공공기관의 보안성 강화를 위한 망분리 기술에 대한 설명으로 옳지 않은 것은?

① 물리적 망분리와 논리적 망분리 기법이 존재한다.

② 물리적 망분리가 되었다 하더라도 USB와 같은 저장 매체를 통한 악성 코드 침입이 가능하다.

③ 논리적 망분리 기법으로는 SBC 및 CBC 기반의 망분리 기법이 존재한다.

④ 애플리케이션 가상화 및 데스크톱 가상화를 통해 물리적 망분리 실현이 가능하다.

⑤ 데이터 다이오드 기반 데이터 일방향성을 이용하여 망분리 실현이 가능하다.

13. 다음 설명에서 제시하고 있는 공격기법과 연관된 네트워크 프로토콜은?

> 중간자(MITM: Man-In-The-Middle) 공격의 일종으로 같은 네트워크에 설치된 컴퓨터에 “피해 대상 IP 주소를 소유한 컴퓨터의 MAC 주소”를 “공격자의 MAC 주소”로 대체하는 공격을 수행한다. “피해 대상 컴퓨터”로 전달되는 메시지는 “공격자 컴퓨터”를 통해서 “피해 대상 컴퓨터”에 전달된다.

① TCP

② IP

③ ARP

④ ICMP

⑤ HTTP

14. 전문가의 경험과 지식을 활용하여 빠르게 진행되는 위험 분석 접근법은?

① 비정형 접근법(Informal Approach)

② 상세 위험 분석 접근법(Detailed Risk Analysis)

③ 기준 접근법(Baseline Approach)

④ 수학 공식 접근법(Math Formula Approach)

⑤ 단위 접근법(Unit Approach)

15. PGP(Pretty Good Privacy)에 대한 설명으로 옳지 않은 것은?

① 사용할 수 있는 대칭 암호 알고리즘에는 IDEA, CAST, 트리플 DES 등이 있다.

② 공개키의 취소 증명서를 발행할 수 있다.

③ 데이터의 압축은 ZIP 형식을 사용한다.

④ RSA, MD5 등의 알고리즘을 이용하여 전자서명을 한다.

⑤ 한 명의 사용자는 다수의 공개키/개인키 쌍을 사용할 수 없다.

16. 공개키 암호 시스템과 대칭키 암호 시스템의 장점을 조합한 하이브리드 암호 시스템에 대한 설명으로 옳지 않은 것은?

① 메시지 자체를 암호화 또는 복호화할 때는 속도가 빠른 대칭키 암호 시스템을 사용한다.
② 암호화에 사용된 대칭키(세션키)를 상대방에게 전달할 때 상대방의 공개키를 사용한다.
③ 하이브리드 암호 시스템은 대칭키 암호의 키 교환 문제가 존재한다.
④ 공개키 알고리즘을 사용하여 공개키와 개인키를 생성하고, 공개키를 상대방에게 전달한다.
⑤ 수신자는 암호화된 대칭키를 수신자의 개인키로 복호화할 수 있다.

17. <보기>에서 XSS 공격을 수행하는 과정을 나타낸 설명 중 옳지 않은 것은?

<보 기>

ㄱ. 공격자는 XSS 코드를 포함한 게시판의 글을 웹 서버에 저장한다.
ㄴ. 웹 사용자는 공격자가 작성해 놓은 XSS 코드를 포함한 게시판의 글에 접근한다.
ㄷ. XSS 코드를 포함한 게시판의 글이 웹 서버에서 사용자에게 전달된다.
ㄹ. 웹 서버에서 XSS 코드가 실행된다.
ㅁ. 공격 결과가 공격자에게 전달된다.

① ㄱ
② ㄴ
③ ㄷ
④ ㄹ
⑤ ㅁ

18. CEK(Contents Encrypting Key)와 KEK(Key Encrypting Key)에 대한 설명으로 옳지 않은 것은?

① KEK를 이용하여 지켜야 할 키의 개수를 줄일 수 있다.
② 통상적으로 CEK에는 세션 키(Session Key)가, KEK에는 마스터 키(Master Key)가 사용된다.
③ 암호문과 KEK만 있다면 원래의 콘텐츠를 알 수 있다.
④ KEK를 이용하여 CEK를 암호화한다.
⑤ KEK의 기밀성을 유지하기 위하여 PBE(Password Based Encryption)를 이용하기도 한다.

19. '개인정보의 안전성 확보 조치 기준' 고시에서 5만 명의 고유식별정보를 공공기관의 내부망에 저장할 경우, 해당 고유식별정보의 암호화 의무 여부를 결정하기 위해 필요한 조치에 해당하는 용어는?

① ISMS
② 취약점 점검
③ 침투 테스트
④ 개인정보 영향평가
⑤ 자산 평가

20. 「개인정보 보호법」 제38조 권리행사의 방법 및 절차에 대한 설명으로 옳지 않은 것은?

① 정보주체는 제35조에 따른 열람, 제36조에 따른 정정·삭제, 제37조에 따른 처리정지 등의 요구(이하 "열람등요구"라 한다)를 문서 등 대통령령으로 정하는 방법·절차에 따라 대리인에게 하게 할 수 있다.
② 만 14세 미만 아동의 법정대리인은 개인정보처리자에게 그 아동의 개인정보 열람등요구를 할 수 없다.
③ 개인정보처리자는 열람등요구를 하는 자에게 대통령령으로 정하는 바에 따라 수수료와 우송료(사본의 우송을 청구하는 경우에 한한다)를 청구할 수 있다.
④ 개인정보처리자는 정보주체가 열람등요구를 할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다.
⑤ 개인정보처리자는 정보주체가 열람등요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.