

1. <보기>의 패킷 로그가 검출된 공격은?

Source: 203.211.11.11
Destination: 203.211.11.11
Protocol: 6
Src Port: 21845
DST Port: 21845

- ① Teardrop
- ② Land attack
- ③ Ping of Death
- ④ SYN flooding

2. 유럽의 정보보호 전문기관인 ENISA(European Network and Information Society Agency)에서 분류한 SNS 관련 보안 위협 중 <보기>에서 설명하는 것으로 가장 옳은 것은?

- SNS를 이용한 스팸 증가
- 크로스 사이트 스크립팅 및 웹·바이러스 등에 대한 취약성 증가
- 다양하게 통합되는 SNS 포털들이 정보수집기로 이용되어 보안 취약성이 증가

- ① 프라이버시 보안 위협
- ② 네트워크 상의 보안 위협
- ③ ID 관련 보안 위협
- ④ 사회적 위협

3. 정보보안의 위협 관리 과정에서 조직의 보안 요구사항에 대한 효과적인 식별 및 효율적인 위협의 감소를 실현하기 위해 세부적인 위협 분석 방법들이 존재한다. <보기>에서 설명하는 (가)에 해당하는 위협 분석 방법으로 가장 옳은 것은?

(가)은 모든 시스템에 대하여 표준화된 보안 대책을 제시하며 체크리스트 형태로 보안 대책이 있는지 없는지를 판단하여 적용되어 있지 않은 보안대책을 적용하는 방법으로 수행하는 위협 분석 방법

- ① 비정형 접근법
- ② 복합 접근법
- ③ 상세위험 분석
- ④ 베이스라인 접근법

4. 「개인정보 보호법 시행령」에서 규정한 개인정보 영향평가 대상에 대한 설명으로 가장 옳지 않은 것은?

- ① 5만 명 이상의 정보주체에 대한 민감 정보 또는 고유식별 정보의 처리가 수반되는 개인정보파일
- ② 내부 또는 외부에서 구축·운용하는 다른 개인정보파일과 연계하려는 경우, 연계 결과 10만 명 이상의 정보주체에 관한 개인정보파일
- ③ 100만 명 이상의 정보주체에 관한 개인정보파일
- ④ 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하는 경우, 변경된 부분

5. 해시 알고리즘의 특징에 대한 설명으로 가장 옳은 것은?

- ① 해시 값이 같으면서 입력 값이 서로 다른 충돌 쌍을 찾는 것은 계산상 불가능하다.
- ② 고정길이의 입력 메시지를 임의 길이의 출력 값으로 압축 시킨 함수이다.
- ③ 주어진 해시 값 y에 대해서 hash(x)=y 식을 만족하는 x를 찾는 것이 계산적으로 가능하다.
- ④ 메시지의 거대화 방지 및 데이터의 은닉에 사용된다.

6. 소프트웨어 취약점 공격에 해당하지 않는 것은?

- ① 버퍼 오버플로우 공격
- ② 힙 버퍼 오버플로우 공격
- ③ 크로스 사이트 스크립팅 공격
- ④ 웹 세션 하이재킹

7. 메시지 송수신 상황에서 <보기>의 조치를 취했을 경우에 지켜질 수 있는 정보보호 서비스로 옳은 것끼리 짝지어진 것은?

송신자 앨리스는 밥에게 보낼 메시지를 먼저 자신의(앨리스) 개인키로 암호화하였다. 이렇게 암호화된 암호문을 수신자인 밥의 공개키로 한 번 더 암호화를 한 뒤에 수신자인 밥에게 보냈다.

- ① 무결성, 인증, 부인방지
- ② 기밀성, 무결성, 부인방지
- ③ 기밀성, 무결성, 인증, 부인방지
- ④ 무결성, 인증, 가용성, 부인방지

8. 공인인증서에 대한 설명으로 가장 옳은 것은?

- ① 공인인증서는 공개키와 소유자를 연결시켜주는 전자 문서로 오늘날 사용되는 대부분의 인증서는 X.509 인증서(버전3)를 표준으로 따른다.
- ② 공인인증서의 기본 영역은 버전, 일련번호, 서명 알고리즘, 발급자, 주체, 주체키 식별자, 기관 정보 액세스, 키 사용 용도, 인증서 정책 등을 포함하고 있다.
- ③ 누구나 사용자의 인증서를 획득하고, 공개키를 획득할 수 있으며 누구나 자유롭게 인증서를 수정/발급할 수 있다.
- ④ 인증서 폐기 목록은 보통 폐기된 인증서에 관한 정보만 유지하는데, 이를 나쁜 목록(bad-list) 방법이라고 한다. 나쁜 목록 방법은 좋은 목록(good-list) 방법보다 안전하지만 상대적으로 용량이 매우 크다.

9. 보안 등급 평가 기준인 TCSEC(Trusted Computer System Evaluation Criteria)에 대한 설명으로 가장 옳은 것은?

- ① E1~E6까지 6등급으로 구분한다.
- ② 기밀성, 무결성, 가용성을 평가한다.
- ③ 유럽의 신뢰성 있는 컴퓨터 시스템 평가기준이다.
- ④ 각 클래스별로 기능 요구사항과 보증 요구사항을 정의·포함한다.

10. 이메일 보안의 사실상의 표준으로 사용되고 있는 PGP (Pretty Good Privacy)에 대한 설명으로 가장 옳은 것은?

- ① RSA, DSA 등의 알고리즘을 사용한 디지털 서명을 통해 보낸 사람에 대한 인증과 부인방지 기능을 제공한다.
- ② AES, IDEA 등의 대칭키 암호화 알고리즘을 사용하여 이메일의 내용이 외부에 노출되는 것을 방지하는 기밀성은 제공하나, 이메일의 내용이 전송 중에 변경되지 않았다는 무결성은 보장하지 못한다.
- ③ PGP는 송신자의 대용량 이메일을 작은 메시지로 분할하지 않고 수신자에게 전송한다.
- ④ PGP는 이메일의 내용만 암호화하고, 첨부되는 문서는 암호화하지 못하여 다른 기법을 추가로 사용해야 한다.

11. <보기>에서 설명하는 시스템 공격에 해당하는 것으로 가장 옳은 것은?

—<보기>—

2014년 4월에 발견된 오픈 소스 암호화 라이브러리인 OpenSSL의 소프트웨어 버그로 전 세계 웹 사이트 가운데 2/3 정도가 사용하는 OpenSSL에서 발견된 치명적인 결함을 말한다. 이 공격은 주로 아이디, 비밀번호, 주민등록번호 등 개인정보와 SSL 서버 비밀키, 세션키, 쿠키 등을 탈취한다.

- ① 스쿨버스
- ② 루트킷
- ③ 하트블리드 공격
- ④ 무차별 공격

12. 위협(Threats), 취약성(Vulnerability), 자산가치(Asset Value), 위험(Risk)의 상관관계 표현으로 가장 옳은 것은?

- ① 위험=자산가치/위협×취약성
- ② 위험=위협/취약성×자산가치
- ③ 위험=위협×취약성/자산가치
- ④ 위험=위협×취약성×자산가치

13. 컴퓨터 및 네트워크에서 서비스가 더 이상 진행되지 못하도록 하는 경우로써 <보기>에서 설명하고 있는 공격 방법으로 가장 옳은 것은?

—<보기>—

- 핑(ping)을 사용하여 현재 동작 중인 노드가 에코 메시지를 보내게 한다.
- 공격자가 발신주소를 공격하고자 하는 목적지의 IP주소로 위장하여 ICMP 에코 메시지를 요청하여 다량의 패킷이 목적지로 전송되도록 한다.
- 목표시스템은 과부하가 발생하여 정상적인 서비스가 불가능하게 된다.

- ① 스머프(smurf) 공격
- ② 중간자(man-in-the-middle) 공격
- ③ 포맷 스트링(format string) 공격
- ④ 프래글(fraggle) 공격

14. <보기>에서 설명하는 포렌식(Forensic)의 기본 원칙에 해당하는 것으로 가장 옳은 것은?

—<보기>—

증거는 획득하고 난 뒤 '이송·분석·보관·법정 제출'이라는 일련의 과정이 명확해야 하며, 이러한 과정에 대한 추적이 가능해야 한다. 이를 만족하려면 증거를 전달하고 전달받는 데 관련한 담당자와 책임자를 명시해야 한다.

- ① 정당성의 원칙
- ② 재현의 원칙
- ③ 연계 보관성의 원칙
- ④ 무결성의 원칙

15. <보기>에서 설명하고 있는 시스템 관련 보안으로 가장 옳은 것은?

—<보기>—

시스템은 계정과 패스워드 관리, 권한 관리, 접근 제어 등의 다양한 시스템 관련 보안 기능을 충분히 갖추고도 보안적인 문제가 발생할 수 있는데, 이는 컴퓨터의 하드웨어 또는 소프트웨어의 결함이나 운영체제 설계상의 허점으로 인한 것이다. 이러한 시스템 자체의 결함을 체계적으로 관리하는 통합적인 개념이다.

- ① 세션 관리
- ② 로그 관리
- ③ 취약점 관리
- ④ 패치 관리

16. 악성코드에 대한 설명으로 가장 옳은 것은?

- ① 바이러스(virus)는 다른 프로그램을 감염시키지는 않지만 네트워크를 통해 자기 복제를 하며 전파된다.
- ② 트로이목마(Trojan horse)는 자기 복제 능력은 없으면서 정상적인 기능을 하는 프로그램 속에 숨어서 정보를 빼내거나 사용자 PC를 원격으로 제어할 수 있게 한다.
- ③ 애드웨어(adware)는 사용자의 브라우저를 원하지 않은 사이트로 이동시키면서 팝업창을 띄운다.
- ④ 드로퍼(dropper)는 사용자의 동의를 얻어 설치되었으나 프로그램 목적과 상관없이 시작 페이지 변경, 광고 노출, 과도한 리소스 사용으로 시스템 성능 저하를 가져오거나 존재하지 않는 위험을 가지고 사용자를 위협하여 결제를 유도한다.

17. <보기>에서 설명하는 정보 은닉 기술로 가장 옳은 것은?

—<보기>—

비밀 정보를 기존의 이미지 파일, 음악 파일, 동영상 파일 등에 숨겨서 전송하는 정보 은닉(information hiding) 기술의 일종이다. 이 기술은 저작권 보호보다는 정보를 은밀하게 전달하기 위한 목적이 크다.

- ① 워터마크(watermark)
- ② 스테가노그래피(steganography)
- ③ 스파이웨어(spyware)
- ④ 섀도(shadow)

18. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정한 정보보호 최고책임자의 업무로 규정되지 않은 것은?

- ① 침해사고 대응
- ② 침해사고 정보 전파
- ③ 정보보호 사전보안성 검토
- ④ 정보보호 취약점 분석 및 개선

19. <보기>에서 설명하고 있는 APT(Advanced Persistent Threats) 공격 기법으로 가장 옳은 것은?

<보기>

조사된 정보를 바탕으로 정보시스템, 웹 어플리케이션 등의 알려지지 않은 취약점 및 보안시스템에서 탐지되지 않는 악성코드 등을 감염시키는 것이다. 해당 취약점에 의해 악성 코드에 감염된 PC는 동일한 취약점을 보유하고 있는 PC를 스캔하여 감염시킨다.

- ① 사전조사(Reconnaissance)
- ② 사회 공학(Social engineering)
- ③ 제로데이(Zero-day) 공격
- ④ 적응(Adaption)

20. 전자정부 소프트웨어 개발 시 비밀번호를 설계할 때 고려해야 할 사항으로 가장 옳지 않은 것은?

- ① 패스워드를 설정할 때 한국인터넷진흥원 『암호이용안내서』의 패스워드 설정규칙을 적용해야 한다.
- ② 패스워드 저장 시 솔트(salt)가 적용된 안전한 해시함수를 사용해야 하며 해시함수 실행은 클라이언트에서 해야 한다.
- ③ 네트워크를 통해 패스워드를 전송하는 경우 반드시 패스워드를 암호화하거나 암호화된 통신 채널을 이용해야 한다.
- ④ 패스워드 재설정·변경 시 안전하게 변경할 수 있는 규칙을 정의해서 적용해야 한다.

이 면은 여백입니다.