

네트워크 보안

문 1. ㉠ ~ ㉣에 들어갈 용어를 바르게 연결한 것은?

- OSI 7계층에서 (㉠)은 물리 계층으로부터 제공되는 물리적 특성을 이용하여 인접한 두 장치 간에 데이터 송·수신을 수행한다.
- (㉠)은 (㉡)와 (㉣)라는 두 개의 부계층으로 나뉜다.

㉠

㉡

㉣

- | | | |
|------------|--------|--------|
| ① 데이터링크 계층 | 논리링크제어 | 오류제어 |
| ② 데이터링크 계층 | 논리링크제어 | 매체접근제어 |
| ③ 네트워크 계층 | 흐름제어 | 오류제어 |
| ④ 네트워크 계층 | 흐름제어 | 매체접근제어 |

문 2. ㉠ ~ ㉣에 들어갈 용어를 바르게 연결한 것은?

- (㉠) 기법은 이미 알려진 공격 패턴을 근거로 침입을 탐지하는 기법
- (㉡) 기법은 정상적인 활동에 대한 프로파일을 생성하고, 이 프로파일과 확률적으로 비교하여 벗어나는 행위를 탐지하는 기법
- (㉣) IDS(Intrusion Detection System)는 네트워크 상의 모든 패킷을 캡처링한 후 이를 분석하여 침입을 탐지하는 시스템

※ 이상탐지 : Anomaly Detection, 오용탐지 : Misuse Detection

㉠

㉡

㉣

- | | | |
|--------|------|---------|
| ① 이상탐지 | 오용탐지 | 네트워크 기반 |
| ② 이상탐지 | 오용탐지 | 호스트 기반 |
| ③ 오용탐지 | 이상탐지 | 네트워크 기반 |
| ④ 오용탐지 | 이상탐지 | 호스트 기반 |

문 3. 다음에서 설명하는 보안 공격 유형은?

- 먼저 목표를 정하여 사전 조사를 실시한다.
- 조사를 바탕으로 공격 대상 컴퓨터에 악성코드를 감염 시킨다.
- 내부 인프라로 서서히 침투하여 몰래 드나들 수 있도록 백도어 및 톨을 설치한다.
- 내부 인프라 접속 권한을 상승시키고 정보를 탈취하기 시작한다.
- 이후 장기간에 걸쳐 내부 인프라를 장악한 후, 더 많은 정보를 유출하거나 시스템을 파괴하는 등 또 다른 보안 사고를 유발한다.

- ① 루트킷(Rootkit) 공격
- ② 랜섬웨어(Ransomware) 공격
- ③ 지능적 지속 위협(APT) 공격
- ④ 블루스나프(BlueSnarf) 공격

문 4. 다음에서 설명하는 네트워크는?

- 일반적으로 안전하지 않은 공용 네트워크를 이용하여 사설 네트워크를 구성하는 기술로서, 전용선을 이용한 사설 네트워크에 비해 저렴한 비용으로 안전한 망을 구성할 수 있다.
- 공용 네트워크로 전달되는 트래픽은 암호화 및 메시지 인증 코드 등을 사용하여 기밀성과 무결성을 제공한다.

- ① LAN(Local Area Network)
- ② WAN(Wide Area Network)
- ③ MAN(Metropolitan Area Network)
- ④ VPN(Virtual Private Network)

문 5. 다음의 실행 결과를 제시하는 명령어는?

프로토콜	로컬 주소	외부 주소	상태
TCP	111.111.111.111:49217	222.222.222.221:ms-sql-s (중략)	ESTABLISHED
TCP	111.111.111.111:49216	222.222.222.222:ftp	TIME_WAIT

- ① nslookup
- ② route
- ③ tracert
- ④ netstat

문 6. 패킷 필터 방화벽이 네트워크 계층에서 검사할 수 없는 정보는?

- ① TCP 연결 상태
- ② 송·수신지 IP주소
- ③ 송·수신지 포트 번호
- ④ TCP 플래그 비트

문 7. 무선랜의 보안을 강화하기 위한 대책으로 안전하지 않은 것은?

- ① 무선랜 AP 접속 시 데이터 암호화와 사용자 인증 기능을 제공하도록 설정한다.
- ② 무선랜 AP에 지향성 안테나를 사용한다.
- ③ 무선랜 AP에 MAC 주소를 필터링하여 등록된 MAC 주소만 허용하는 정책을 설정한다.
- ④ 무선랜 AP의 이름인 SSID를 브로드캐스팅하도록 설정한다.

문 8. IPSec 프로토콜의 인증 헤더(AH)와 보안 페이로드 캡슐화(ESP)에서 제공하는 보안서비스 중 ESP에서만 제공하는 보안서비스는?

- ① 재전송 공격 방지(Replay Attack Protection)
- ② 메시지 기밀성(Confidentiality)
- ③ 메시지 무결성(Integrity)
- ④ 개체 인증(Entity Authentication)

문 9. NAT(Network Address Translation)에 대한 설명으로 옳지 않은 것은?

- ① 한정된 공인 IP주소 부족 문제의 해결이 가능하다.
- ② 공인 IP와 NAT IP의 매핑이 1:1만 가능하다.
- ③ 주소 변환 기능을 제공한다.
- ④ 내부 시스템에 네트워크 구조를 노출하지 않는 보안상의 이점을 제공한다.

문 10. SSL(Secure Socket Layer)의 레코드 프로토콜에서 응용 메시지를 처리하는 동작 순서를 바르게 나열한 것은?

※ MAC: Message Authentication Code

- ① 압축→단편화→암호화→MAC 첨부→SSL 레코드 헤더 붙이기
- ② 압축→단편화→MAC 첨부→암호화→SSL 레코드 헤더 붙이기
- ③ 단편화→MAC 첨부→압축→암호화→SSL 레코드 헤더 붙이기
- ④ 단편화→압축→MAC 첨부→암호화→SSL 레코드 헤더 붙이기

문 11. ㉠과 ㉡에 들어갈 용어를 바르게 연결한 것은?

- (㉠)는(은) 네트워크 중간에서 상대방의 패킷 정보를 도청하는 수동적 공격이다.
○ (㉡) 공격의 대응 방안으로 텔넷의 경우 원격 접속 시 평문 패킷의 암호화를 지원하기 위해 (㉢)를(을) 사용한다.

㉠

㉡

- | | |
|-------------|-----|
| ① ARP watch | SSH |
| ② ARP watch | PGP |
| ③ Sniffing | SSH |
| ④ Sniffing | PGP |

문 12. 정보보호 시스템들의 로그를 수집하여 분석 및 모니터링을 통해 전사적 차원의 정보시스템 보안성을 향상시키고 안전성을 높이는 시스템은?

- ① ESM(Enterprise Security Management)
- ② NAC(Network Access Control)
- ③ MAM(Mobile Application Management)
- ④ MDM(Mobile Device Management)

문 13. 방화벽의 구축 형태 중 베스천 호스트 방식에 대한 설명으로 옳지 않은 것은?

- ① 외부와 내부 네트워크를 연결해주는 역할을 수행한다.
- ② 외부에서 내부 네트워크로 접속할 때 원하지 않는 접근은 차단할 수 없다.
- ③ 로그인 정보가 누출되면 내부 네트워크를 보호할 수 없다.
- ④ 베스천 호스트가 손상되면 내부 네트워크를 보호할 수 없다.

문 14. <보기 1>의 보안 위협과 <보기 2>의 그에 대한 설명을 바르게 연결한 것은?

———— <보기 1> ————

- ㄱ. 방해(Interruption)
ㄴ. 가로채기(Interception)
ㄷ. 변조(Modification)

———— <보기 2> ————

- A. 송신측에서 수신측으로 메시지를 전송할 때 제3자가 수신측과 연결할 수 없도록 하는 행위
B. 송신측과 수신측이 메시지를 주고받는 사이에 제3자가 도청하는 행위
C. 송신측에서 수신측으로 메시지를 전송할 때 제3자가 일부 또는 전부를 변경하여 수신측에 전송하는 행위

ㄱ

ㄴ

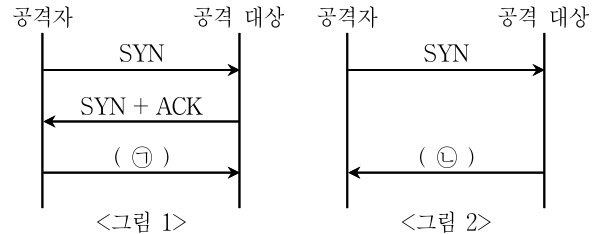
ㄷ

- | | | |
|-----|---|---|
| ① A | B | C |
| ② A | C | B |
| ③ B | A | C |
| ④ B | C | A |

문 15. HTTPS에 대한 설명으로 옳지 않은 것은?

- ① HTTPS 연결로 명시되면 포트 번호 443번이 사용되어 SSL을 호출한다.
- ② HTTPS는 웹 브라우저와 웹 서버 간의 안전한 통신을 구현하기 위한 것이다.
- ③ HTTPS는 HTTP over TLS 표준 문서에 기술되어 있다.
- ④ HTTPS 사용 시 요청된 문서의 URL은 암호화할 수 없다.

문 16. 다음 그림은 TCP half open 스캔 절차이다. ㉠과 ㉡에 들어갈 패킷을 바르게 연결한 것은?



※ <그림 1>은 공격 대상 서버의 포트가 열린 경우이고, <그림 2>는 공격 대상 서버의 포트가 닫힌 경우임.

㉠

㉡

- | | |
|-------|-----------|
| ① ACK | ACK |
| ② ACK | RST |
| ③ RST | RST + ACK |
| ④ RST | SYN + ACK |

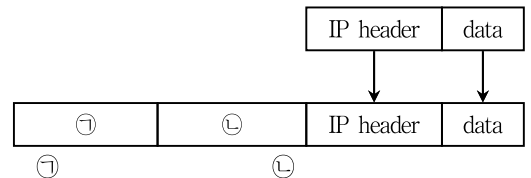
문 17. 네트워크 보안 공격에 대한 설명으로 옳은 것은?

- ① Smurf 공격은 공격대상의 IP주소로 위장된 다량의 ICMP echo reply 패킷을 전송하여 서비스를 거부하는 공격이다.
- ② MITM 공격은 네트워크에 여러 메시지를 전송하거나 네트워크 흐름을 통제하는 공격이다.
- ③ Salami 공격은 위조된 ARP reply 패킷을 전송하여 서비스를 거부하는 공격이다.
- ④ Teardrop 공격은 출발지와 목적지의 IP주소가 동일하게 위조된 SYN 패킷을 전송하는 공격이다.

문 18. ARP Spoofing 공격에 대응하기 위한 명령어로 옳은 것은?

- ① arp -a IP주소 MAC주소
- ② arp -d IP주소 MAC주소
- ③ arp -s IP주소 MAC주소
- ④ arp -v IP주소 MAC주소

문 19. 다음은 IPSec 터널모드에서 IP 패킷을 암호화하고 인증 기능을 수행하는 그림이다. ㉠과 ㉡에 추가되는 헤더 정보를 바르게 연결한 것은?



- | | |
|-----------------|---------------|
| ① new IP header | ESP/AH |
| ② ESP/AH | new IP header |
| ③ IKE header | new IP header |
| ④ new IP header | IKE header |

문 20. OSI 계층구조와 계층별로 사용되는 보안 프로토콜의 연결이 옳지 않은 것은?

- ① 네트워크 계층 - IPsec
- ② 응용 계층 - SSH
- ③ 데이터링크 계층 - TLS
- ④ 전송 계층 - SSL