

네트워크 보안

1. 국내에서 개발된 대칭키 암호화 알고리즘이 아닌 것은?

- ① AES
- ② LEA
- ③ ARIA
- ④ SEED

2. OSI 7계층 중 네트워크 계층에 포함되지 않는 프로토콜은?

- ① ARP
- ② UDP
- ③ OSPF
- ④ RARP

3. (가) ~ (다)에서 설명하는 네트워크 장비를 바르게 연결한 것은?

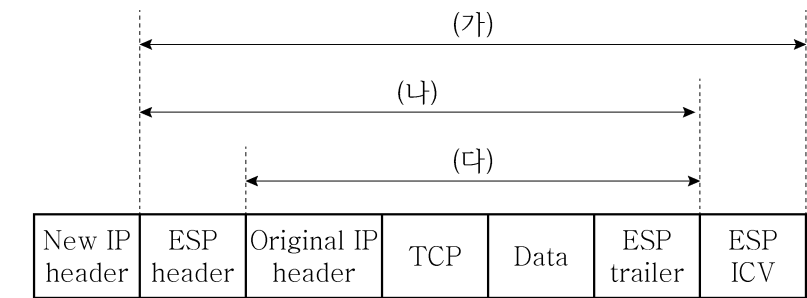
(가) 물리 계층에서 동작하며 수신된 프레임을 모든 포트에 브로드캐스팅하는 장비

(나) 데이터 링크 계층에서 MAC 주소를 기반으로 특정 포트에 프레임을 전달하는 장비

(다) 네트워크 계층에서 네트워크 주소(IP 주소)를 확인하고 다른 네트워크와 연결하는 장비

- | (가) | (나) | (다) |
|-------|-----|-----|
| ① 라우터 | 스위치 | 허브 |
| ② 허브 | 라우터 | 스위치 |
| ③ 스위치 | 허브 | 라우터 |
| ④ 허브 | 스위치 | 라우터 |

4. 다음 IPSec ESP(Encapsulating Security Payload)에서 터널모드의 암호화 및 인증 범위를 바르게 연결한 것은?



- | 암호화 범위 | 인증 범위 |
|--------|-------|
| ① (가) | (나) |
| ② (가) | (다) |
| ③ (다) | (가) |
| ④ (다) | (나) |

5. SSLv3(Secure Sockets Layer version 3)에서 서버와 클라이언트가 서로 인증하고, 암호와 MAC 알고리즘과 암호키를 협상하는 역할을 하는 프로토콜은?

- ① Alert Protocol
- ② Record Protocol
- ③ Handshake Protocol
- ④ Change Cipher Spec Protocol

6. 디지털 포렌식에서 다음에 해당하는 것은?

불법 해킹 용의자의 해킹 툴이 증거 능력을 갖추기 위해서는 같은 상황의 피해 시스템에 툴을 적용할 경우 피해 상황과 일치하는 결과가 나와야 한다.

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

7. XSS 취약점 공격의 수행 단계를 순서대로 바르게 나열한 것은?

(가) 사용자 시스템에서 XSS 코드가 실행된다.
(나) 웹 서버는 XSS 코드가 포함된 게시판의 글을 사용자에게 전달한다.
(다) 사용자는 공격자가 작성해 둔 XSS 코드가 포함된 게시물을 클릭한다.
(라) 임의의 XSS 취약점이 존재하는 서버에 XSS 코드가 포함된 게시물을 작성하여 저장한다.
(마) XSS 코드가 실행된 결과는 공격자에게 전달되고 공격자는 공격을 종료한다.

- ① (나) → (가) → (다) → (라) → (마)
- ② (나) → (가) → (라) → (다) → (마)
- ③ (라) → (나) → (가) → (다) → (마)
- ④ (라) → (다) → (나) → (가) → (마)

8. TCP 세션 하이재킹 공격에 대한 설명으로 옳지 않은 것은?

- ① 공격자는 적절한 시퀀스 넘버를 얻기 위해 스니핑을 한다.
- ② TCP 세션 하이재킹은 공격자가 동기화 상태를 무너뜨리는 것에서 시작한다.
- ③ 공격자는 네트워크에서 직접 클라이언트의 세션 ID를 수정하여 새로운 세션을 생성한다.
- ④ 서버와 클라이언트의 통신 시에 시퀀스 넘버의 제어에 문제점이 있음을 파악하고 악용한다.

9. (가), (나)에 들어갈 내용을 바르게 연결한 것은?

nmap 명령어의 옵션에서 (가)는 TCP SYN을 스캔하고, (나)는 스캔 결과를 상세히 출력한다.

- | (가) | (나) |
|-------|-----|
| ① -sS | -v |
| ② -sS | -A |
| ③ -sT | -v |
| ④ -sT | -A |

10. 암호화 단계에서 현재의 평문 블록을 바로 직전의 암호 블록과 XOR한 것을 암호 알고리즘 입력으로 사용하는 블록 암호 운영 모드는?

- ① CFB
- ② CBC
- ③ OFB
- ④ CTR

11. TCP/IP 프로토콜에 대한 설명으로 옳지 않은 것은?
- ① SMTP는 네트워크의 두 메일 서버 간에 이메일을 송수신할 때 사용되는 프로토콜이다.
 - ② DHCP는 네트워크의 각 노드에 IP 주소를 자동으로 할당하고 관리한다.
 - ③ ARP를 이용하여 LAN에 연결되어 있는 다른 노드의 포트 번호를 획득할 수 있다.
 - ④ ICMP의 송신지 억제(Source Quench) 메시지는 송신 노드에 혼잡 가능성을 알리고 전송 속도를 늦출 것을 요구한다.
12. 네트워크 공격 기술에 대한 설명으로 옳지 않은 것은?
- ① 랜드 공격은 패킷을 전송할 때 출발지 MAC 주소와 목적지 MAC 주소의 값을 같게 만들어서 공격 대상에게 보내는 공격이다.
 - ② 스위치 재밍 공격은 스위치가 MAC 주소 테이블을 기반으로 패킷을 포트에 스위칭할 때 정상적인 스위칭 기능을 마비시키는 공격이다.
 - ③ IP 스푸핑은 신뢰 관계에 있는 두 개의 호스트 사이에서 하나의 시스템을 마비시킨 후 자신이 신뢰 관계에 있는 호스트인 것처럼 속이는 공격이다.
 - ④ HTTP GET 플러딩은 웹서버에서 처리할 수 없는 최대 성능 이상의 과도한 HTTP GET 요청을 전송함으로써 웹 서버가 자원을 모두 소비하여 정상적인 기능을 발휘하지 못하도록 하는 공격이다.
13. 스크리닝 라우터와 배스천 호스트에 대한 설명으로 옳지 않은 것은?
- ① 배스천 호스트는 내부 네트워크와 외부 네트워크 간의 게이트웨이 역할을 한다.
 - ② 스크리닝 라우터는 배스천 호스트에 비하여 통과하거나 거절당한 패킷의 기록을 관리하기 쉽다.
 - ③ 스크리닝 라우터는 네트워크 계층과 전송 계층에서 동작하는 프로토콜인 IP, TCP 또는 UDP의 헤더에 포함된 내용을 분석한다.
 - ④ 배스천 호스트가 손상되면 내부 네트워크를 보호할 수 없다.
14. ICMP 리다이렉트 공격이 성공했을 경우의 상황으로 옳은 것은?
- ① 호스트의 ARP 캐시가 업데이트된다.
 - ② 특정 호스트의 MAC 주소가 도용된다.
 - ③ 스위치의 주소 테이블이 가득 차게 된다.
 - ④ 호스트의 라우팅 테이블 정보가 업데이트된다.
15. 프로토콜별 통계 현황을 출력하는 netstat 명령어 옵션은?
- ① -i
 - ② -p
 - ③ -r
 - ④ -s

16. IP에 대한 설명으로 옳지 않은 것은?
- ① IPv4에서 192.168.0.0은 사설 주소 영역에 해당된다.
 - ② IPv4에서 IP 데이터그램의 최대 길이는 65,535바이트이다.
 - ③ IPv6에서 주소 FCBB:0000:0000:0000:0000:1ABC:BBCB는 FCBB:0:0:0:0:1ABC:BBCB으로 축약할 수 있다.
 - ④ IPv6에서 홑 제한은 패킷이 라우터에 의해 중개될 때마다 1씩 증가하여 128을 넘는 순간 패킷을 폐기한다.
17. 『OWASP Top 10 for LLM Applications 2025』에서 정의한 「LLM03:2025 공급망」에 대한 항목에 해당하지 않는 것은?
- ① 타사 모델을 선택할 때는 포괄적인 AI 레드팀 및 평가를 수행한다.
 - ② 취약하거나 오래된 구성 요소를 완화하기 위해 패치 정책을 구현한다.
 - ③ 모델이 의도하지 않은 데이터 소스에 접근하는 것을 방지하기 위해 인프라를 충분히 제어해야 한다.
 - ④ 협업 모델 개발 환경에 대한 엄격한 모니터링 및 감사 관행을 구현하여 남용을 방지하고 신속하게 탐지한다.
18. SNMP(Simple Network Management Protocol) version 1에서 매니저와 에이전트 간의 통신에 사용되는 메시지에 대한 설명으로 옳지 않은 것은?
- ① trap 메시지를 이용하여 매니저가 에이전트에게 특정 상황 발생을 알린다.
 - ② setRequest 메시지를 이용하여 매니저가 특정 변수값의 변경을 요청한다.
 - ③ getResponse 메시지를 이용하여 에이전트가 매니저의 요청에 해당하는 변수값을 전송한다.
 - ④ getRequest 메시지를 이용하여 매니저가 변수값을 읽어올 수 있다.
19. CIDR 방식으로 표현한 203.237.10.0/25에 대한 설명으로 옳은 것은?
- ① 203.237.10.128은 브로드캐스트 주소이다.
 - ② 3개의 서브넷을 만들 수 있다.
 - ③ 서브넷 마스크는 255.255.255.128이다.
 - ④ 서브넷의 호스트 가용 IP 주소는 124개이다.
20. X.509 버전 3 인증서의 확장 필드에 대한 설명으로 옳지 않은 것은?
- ① Basic Constraints: 인증 주체가 CA인지를 식별한다.
 - ② Authority Key Identifier: 인증서를 서명하는 데 사용하는 공개 키를 식별한다.
 - ③ Key Usage: 인증서에 있는 암호화, 서명, 인증서 서명과 같은 키의 목적을 정의한다.
 - ④ Subject Alternative Name: 인증서의 발급자에 대한 다양한 대체 이름을 제공하는 역할을 한다.