

(과목코드 : 142)

성명 :

- 네트워크 보안(9급) 3 - 1

11. 다음 중 응용계층 방화벽에 대한 설명으로 가장 적절하지 않은 것은?

- ① 응용계층에서의 메시지 내용을 기반으로 필터링할 수 있다.
- ② 내부 시스템이 외부 시스템에 직접적으로 연결되는 것을 방지한다.
- ③ 내부의 민감정보가 외부로 유출되는 것을 막는 데에 활용한다.
- ④ 여러 응용 프로토콜에 대해 하나의 응용계층 방화벽으로 보호할 수 있다.

12. 다음 중 네트워크 진단 도구인 traceroute에 대한 설명으로 가장 적절하지 않은 것은?

- ① 송신지와 목적지 사이에 L3 라우터 상태를 확인하기 위해 사용한다.
- ② 중계노드 수, IP 주소, 응답시간을 확인할 수 있다.
- ③ 4개의 UDP 패킷의 TTL을 하나씩 증가시키면서 순차적으로 전송한다.
- ④ 운영체제에 따라 traceroute는 ICMP, TCP를 선택적으로 사용할 수 있다.

13. 다음 중 스위칭 환경에서 수행할 수 있는 스니핑 공격에 해당하는 것을 모두 고르면?

- (㉠) Teardrop Attack
- (㉡) TCP SYN Flooding Attack
- (㉢) ARP 스푸핑
- (㉣) ICMP 리다이렉트
- (㉤) 스위치 재밍

- ① (㉠), (㉡), (㉢), (㉣), (㉤) ② (㉡), (㉢), (㉣), (㉤)
- ③ (㉢), (㉣), (㉤) ④ (㉣), (㉤)

14. 포트 스캔을 통해 얻을 수 있는 정보 중 가장 적절하지 않은 것은?

- ① 시스템의 논리 주소
- ② 시스템의 동작 여부
- ③ 시스템의 제공 서비스
- ④ 방화벽의 필터링 규칙

15. 다음 중 포트 스캐닝 결과에 대한 신뢰도가 가장 낮은 스캐닝 방법으로 옳은 것은?

- ① TCP ACK scan ② UDP scan
- ③ ICMP Sweep ④ TCP SYN scan

16. 다음 중 무선랜 보안 기술 규격인 WPA-Personal의 PSK 인증에 대한 설명으로 가장 적절하지 않은 것은?

- ① 인증서버가 설치되지 않은 환경에서 동작 가능
- ② AP와 단말기의 인증 과정 중 3-way handshake 수행
- ③ AP와 단말기가 사전에 공유된 키(PSK)와 802.1x에 규정된 EAPoL-Key 프레임을 활용하여 인증 수행
- ④ 인증 후 공유키로부터 256비트 길이의 임시 암호키(PMK) 생성

17. 다음 중 ICMP 패킷의 크기를 기준 크기보다 크게 증가시키고, 더 많은 조각으로 단편화하여 공격 대상에게 전송하는 공격으로 가장 적절한 것은?

- ① Ping of Death ② SMURF Attack
- ③ DDoS ④ Teardrop Attack

18. 공격자가 발신지 주소를 공격 대상의 IP로, 목적지 주소를 직접 브로드캐스트 주소(Directed Broadcast Address)로 설정한 Ping 메시지를 통해 증폭 네트워크(Amplifier network)의 시스템들이 공격 대상에게 Ping 응답 메시지를 동시에 전송하도록 만드는 공격으로 가장 적절한 것은?

- ① Land Attack
- ② TCP SYN Flooding Attack
- ③ SMURF Attack
- ④ DDoS

19. 이더넷에서 사용되는 매체 접근 방식 중 호스트가 채널의 상태를 감지하여 충돌을 회피하는 방식으로 옳은 것은?

- ① Token Ring ② CSMA/CA
- ③ CSMA/CD ④ Token Bus

20. 다음 IDS의 탐지 유형 중 지식기반 탐지 기법에 해당하지 않는 것은?

- ① 전문가 시스템(Expert System)
- ② 시그니처 분석(Signature-based Detection)
- ③ 페트리넷(Petri-nets)
- ④ 통계적 분석

21. 다음 무선랜 보안 기법 중 짧은 길이의 IV 값으로 인해 공격자가 쉽게 암호키를 예측하는 것이 가능한 기법에 해당하는 것은?
- ① WEP ② WPA-1
 - ③ WPA-2 ④ 802.1x/EAP
22. 다음 중 세션 하이재킹에 대한 설명으로 가장 적절하지 않은 것은?
- ① 인증 과정을 마치고 생성된 정상 세션의 연결을 가로채는 공격이다.
 - ② 인증 과정에 포함된 절차를 모두 우회하는 것이 가능하다.
 - ③ TCP의 취약점을 이용한 공격이다.
 - ④ TCP로 연결된 송신자와 수신자의 세션을 차단하는 것이 목적이다.
23. 다음 중 Land Attack에 대한 대응책으로 가장 적절한 것은?
- ① egress filtering 적용
 - ② TCP 패킷의 소스 IP가 내부 IP인 외부 패킷 차단
 - ③ SYN 쿠키 기법 적용
 - ④ TCP 패킷의 소스 IP가 외부 IP인 내부 패킷 차단
24. 다음 중 IPsec의 AH(Authentication Header) 프로토콜과 가장 거리가 먼 것은?
- ① AH Header
 - ② Next Header
 - ③ Padding
 - ④ SPI(Security Parameter Index)
25. 다음 중 암호화 통신과 인증을 제공하는 원격 접속 프로토콜로 가장 적절한 것은?
- ① SSH ② Rlogin
 - ③ SNMP ④ Telnet