

네트워크 보안(9급)

(과목코드 : 142)

2022년 군무원 채용시험

응시번호 :

성명 :

1. 다음 중 통합보안관리시스템(Enterprise Security Management)의 특징에 대한 설명으로 가장 옳지 않은 것은?

- ① 공격의 효과적인 사전 탐지
- ② 보안 정책의 일관성 유지
- ③ 통합보안관리 인프라 구축
- ④ 침해사고에 효과적인 대응

2. 침입방지시스템(IPS, Intrusion Prevention System)에 대한 설명으로 가장 옳지 않은 것은?

- ① 침입에 대한 탐지와 차단기능을 수행한다.
- ② 탐지영역은 네트워크 계층과 전송계층이다.
- ③ 침입차단 시스템과 침입방지 시스템의 장점을 결합한 보안 시스템이다.
- ④ 외부로부터 유입되는 유해한 트래픽을 차단하기 위한 능동형 보안 솔루션이다.

3. 다음 중 Snort에 대한 설명으로 가장 옳은 것은?

- ① 실시간 트래픽분석과 IP 네트워크에서의 패킷 처리를 담당하는 공개 소스로 프로토콜 분석, 콘텐츠 검색 및 조합 작업을 할 수 있다.
- ② 오픈소스 웹 취약점 스캐너로 서버의 취약점을 찾아준다.
- ③ 비밀번호를 크래킹하는 tool로 망 패킷 스니핑, 사전 공격(dictionary attack) 등의 방법을 사용한다.
- ④ 수많은 해킹도구와 설명서를 포함한 모의 해킹 플랫폼이다.

4. 다음 중 DoS(Denial of Service) 공격에 대한 설명으로 가장 옳지 않은 것은?

- ① 루트권한을 획득하는 공격이다.
- ② 디스크, 데이터, 시스템을 파괴하는 파괴 공격도 가능하다.
- ③ 공격의 원인이나 공격자를 추적하기 힘들다.
- ④ 매우 다양한 방법으로 공격할 수 있다.

5. 다음은 TCP header Flag에 대한 설명이다. 옳은 것을 모두 고르시오.

- ㉠ URG: TCP가 즉시 이 메시지를 상위계층 프로세스에게 전달할 수 있게 한다.
- ㉡ ACK: Acknowledgment Number가 유효함을 표시한다.
- ㉢ RST: 연결을 Reset하도록 지시하는 Flag.
- ㉣ SYN: 연결시작을 나타내기 위해 사용하는 Flag.
- ㉤ FIN: 연결을 종료하도록 지시하는 Flag.

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

6. 다음 지문은 무엇에 대한 설명인가?

사용자 PC를 악성코드에 감염시켜 이용자가 인터넷 '즐거찾기' 또는 포털사이트 검색을 통하여 금융회사 등의 정상 홈페이지 주소로 접속하여도 가짜 사이트 홈페이지로 유도되어 해커가 금융거래정보 등을 편취하는 수법

- ① 파밍(Pharming)
- ② 애드웨어(Adware)
- ③ 크래킹(Cracking)
- ④ 백도어 공격(Backdoor Attack)

7. 다음 중 표준 인터넷 프레임의 길이에 대한 설명이 가장 옳은 것은?

- ① 최소 프레임 길이: 64byte,
최소 데이터 길이: 48byte
- ② 최대 프레임 길이: 1,524byte,
최대 데이터 길이: 1,500byte
- ③ 최대 프레임 길이: 1,518byte,
최대 데이터 길이: 1,500byte
- ④ 최소 프레임 길이: 56byte,
최소 데이터 길이: 48byte

8. 다음 지문에 대한 네트워크 공격으로 가장 적절한 것은?

공격대상의 주소로 소스 IP 주소를 만들고 임의의 브로드캐스트 주소로 ICMP echo 패킷을 전송하여 스푸핑된 IP 호스트는 ICMP reply 패킷을 동시 다발적으로 수신하여 시스템 부하를 증가시킨다.

- ① Teardrop
- ② Land Attack
- ③ Syn Flooding
- ④ Smurf Attack

9. 다음 중 분산서비스 거부공격(DDoS, Distributed Denial of Service)의 공격 도구에 해당하지 않는 것은?

- ① Trinoo Attack
- ② TFN Attack
- ③ Targa Attack
- ④ Stacheldraht

10. 어떤 네트워크 보안 모델은 다음 지문과 같이 5가지 원칙을 기반으로 하고 있다. 해당하는 보안 모델은 무엇인가?

- ㉠ 네트워크의 모든 사용자는 항상 위험하다고 가정
- ㉡ 외부 및 내부 위협이 네트워크에 항상 존재
- ㉢ 네트워크의 신뢰 여부를 결정할 때 네트워크의 위치는 충분하지 않음
- ㉣ 모든 디바이스, 사용자, 네트워크를 인증하고 권한 확인
- ㉤ 최대한 많은 데이터 소스를 기반으로 자동적인 정책 수립

- ① 경계면 보안
- ② 엣지 보안
- ③ 제로 트러스트 보안
- ④ 공격표면 보안

11. 다음 중 OWASP TOP 10 2021에 새롭게 포함되지 않는 웹 취약점으로 가장 적절한 것은?

- ① 소프트웨어 및 데이터 무결성 오류
(Software and Data Integrity Failures)
- ② 안전하지 않은 설계(Insecure Design)
- ③ 서버 측 요청 위조
(Server-Side Request Forgery)
- ④ Identification and Authentication Failures
(식별 및 인증 오류)

12. 기존 IP 기반 인터넷의 주소 고갈 문제를 해결하기 위해 IPv4에서 IPv6로의 전환이 이루어지고 있다.

하지만 인터넷상의 모든 시스템이 IPv4에서 IPv6로 전환하기 위해서는 상당히 많은 시간이 소요된다. 이와 같은 문제를 해결하기 위해, IETF에서 IPv4와 IPv6 시스템 사이에 문제가 없도록 전환을 돕는 전략을 사용하고 있다. 다음 중 이에 해당하지 않는 것은?

- ① 터널링(tunneling)
- ② 라우터 간청(router-solicitation)
- ③ 헤더 변환(header translation)
- ④ 이중 스택(dual stack)

13. ICMP는 발신지 IP주소를 사용하여 오류 메시지를 데이터그램의 발신지로 보낸다. 오류 보고 과정을 단순화하기 위해 ICMP 보고 메시지가 따르는 규칙으로 가장 옳지 않은 것은?
- ① 현재 호스트(this host) 또는 루프백(loopback)과 같은 특수주소를 가지는 데이터그램에 대해서는 ICMP 오류 메시지가 생성되지 않는다.
 - ② 처음 단편이 아닌 단편화된 데이터그램에 대해서는 ICMP 오류 메시지가 생성되지 않는다.
 - ③ 어떤 ICMP 오류 메시지도 ICMP 오류 메시지를 전달하는 데이터그램의 응답으로 생성되지 않는다.
 - ④ 어떤 ICMP 오류 메시지도 유니캐스트 주소를 가진 데이터그램을 위해서 생성되지 않는다.
14. 다음 중 IPSec의 전송모드에 대한 설명으로 가장 옳은 것은?
- ① IP패킷 전체를 보호한다.
 - ② IP헤더를 보호하지 않으며 전송층에서 발송한 정보만 보호한다.
 - ③ IP패킷 전체를 보호한 후에 새로운 IP헤더를 추가한다.
 - ④ 전송층에서 온 정보에 IP헤더만 추가하고 IPSec헤더를 나중에 추가한다.
15. 다음 중 전자우편용 보안서비스인 S/MIME (Secure/Multiple Internet Mail Extension) 프로토콜에 대한 설명으로 가장 옳지 않은 것은?
- ① MIME 프로토콜에 보안성을 강화한 프로토콜이다.
 - ② ASCII 코드로된 메시지만 전송할 수 있다.
 - ③ MIME에 기밀성과 무결성 같은 보안서비스를 위해 암호메시지구조문(CMS, Cryptography Message Syntax)을 정의한다.
 - ④ 암호알고리즘으로는 대칭암호와 비대칭암호를 모두 사용할 수 있다.
16. 다음 중 SSL/TLS에서 사용하는 4가지 프로토콜을 나열한 것으로 가장 옳은 것은?
- ① Authentication Header, ClientKeyExchange, Peer Certificate, Alert
 - ② Authentication Header, SessionID, Handshake, Peer Certificate
 - ③ SessionID, Record, ClientkeyExchange, ChangeCipherSpec
 - ④ Record, Handshake, ChangeCipherSpec, Alert
17. 데이터를 전용선(leased line)으로 전송하면 보안적 측면이나 속도면에서 좋지만 회선 사용료가 고가이며, 미사용 시간이 길어 대역폭 낭비가 발생할 수 있다. 다음 중 대안으로 가장 적합한 기술은 무엇인가?
- ① OSPF(Open Shortest Path First)
 - ② EIGRP(Enhanced Interior Gateway Routing Protocol)
 - ③ 가상사설망(VPN, Virtual Private Network)
 - ④ 가상랜(VLAN, Virtual LAN)
18. 다음 중 HTTPS를 활성화 하면 데이터는 대칭암호 시스템으로 전송하게 되는데 송신자와 수신자가 이 대칭키를 공유하는 안전한 방법에 대한 설명으로 가장 옳지 않은 것은?
- ① 공개키 암호화 방식으로 대칭키를 공유한다.
 - ② 송신자인 브라우저는 서버의 공개키로 대칭키를 암호화해서 서버로 송신한다.
 - ③ 송신자와 수신자가 확보한 공유 대칭키로 메시지를 암호화하여 상호 간에 전송한다.
 - ④ 서버는 인증기관의 공개키로 송신자가 보내준 공인인증서를 복호화하여 대칭키를 확보한다.

19. 다음 중 커beros(Kerberos)에 대한 설명으로 가장 옳은 것은?

- ① 네트워크 그룹을 이동시켜야 할 때 물리적 장비를 옮기는 과정 없이 스위치 설정만으로 조정할 수 있게 하는 서비스이다.
- ② 네트워크를 구성하는 LAN 내의 장비 간에 원활한 패킷 전송을 위한 서비스이다.
- ③ 네트워크상에서 키를 분배하고 사용자를 인증하는 서비스이다.
- ④ 네트워크 내의 데이터 무결성을 보장하기 위한 해시함수 중의 하나이다.

20. 다음 중 네트워크 접근에서 서버에 접근하는 요청으로부터 보안을 강화하는 방법에 대한 설명으로 가장 거리가 먼 것은?

- ① DNS 서버를 활용해 접근 제어를 강화하는 방식으로 IP주소를 할당한다.
- ② 가상랜(VLAN)을 활용해 접근 요청자에 대한 보안요구 사항에 따라 어떤 가상랜에 접근을 허가할지 결정한다.
- ③ 침입차단시스템(Firewall)을 이용해 네트워크 내부와 외부 사이의 트래픽을 허가하거나 거절하는 방식으로 접근을 강화한다.
- ④ IEEE 802.1X의 확장인증 프로토콜로 인증 절차를 수행한다.

21. 다음 중 네트워크 명령어 traceroute에 대한 설명으로 가장 옳지 않은 것은?

- ① 지정한 호스트까지의 경로를 조사한다.
- ② 네트워크 장애 시, 어느 라우터에 문제가 발생했는지 확인한다.
- ③ TCP 시간초과 메시지 및 TCP 포트 도달 불가 오류 메시지를 이용해 구현한다.
- ④ Windows 명령어는 tracert이고, Linux 명령어는 traceroute이다.

22. 다음 중 HTTPS를 사용해서 암호화하는 통신 요소를 나열한 것에서 가장 옳지 않은 것은?

- ① 서버의 공개키 인증서
- ② 브라우저와 서버 간의 쿠키
- ③ HTTP 헤더 내용
- ④ 요청한 URL

23. 다음 중 침입탐지시스템에 활용하는 기법으로 임계값 탐지와 프로파일 기반 변형 탐지를 활용하는 탐지 방법을 가장 적절하게 설명한 것은?

- ① 규칙기반 탐지(Rule-based Detection)
- ② 통계적 변형 탐지(Statistical Anomaly Detection)
- ③ 감사 기록 탐지(Audit Record Detection)
- ④ 분산 침입 탐지(Distributed Intrusion Detection)

24. 다음 중 침입차단시스템의 유형으로 가장 옳지 않은 것은?

- ① 패킷-필터링 침입차단시스템 (Packet-Filtering Firewall)
- ② 스테이트풀 검사 침입차단시스템 (Stateful Packet Inspection Firewall)
- ③ 회선-레벨 게이트웨이 (Circuit-Level Gateway)
- ④ 하이재킹 침입차단시스템(Hijacking Firewall)

25. 다음 중 TCP 헤더의 Control Flag 필드에 대한 설명으로 가장 옳지 않은 것은?

- ① 플래그 비트 중 SYN만 전송해 대상 서버에서 SYN+ACK로 응답하는 경우 포트가 오픈 상태로 있는 것을 판단할 수 있다.
- ② FIN 플래그만 전송하면 대상 포트가 닫혀있는 경우 RST 플래그가 세팅된 패킷이 수신된다.
- ③ 플래그 하위 비트 6개를 모두 0으로 전송하면 대상 포트가 닫혀있는 경우 PSH 플래그가 세팅된 패킷이 수신된다.
- ④ 플래그 하위 비트 6개를 모두 1로 전송하면 대상 포트가 닫혀있는 경우 RST 플래그가 세팅된 패킷이 수신된다.