

네트워크 보안(7급)

(과목코드 : 142)

2023년 군무원 채용시험

응시번호 :

성명 :

1. 네트워크에서 해커의 IP 추적은 매우 중요하다. 다음 중 IP 추적 방법으로 가장 적절하지 않은 것은?

- ① 해커의 메일 헤더(Header) 분석 기법
- ② 해커가 웹 게시판에 접근했을 때, 웹서버 로그 분석 기법
- ③ OS에서 제공하는 traceroute 도구를 이용한 기법
- ④ NAT 분석 기법

2. DDoS(Distributed Denial of Service) 공격의 목표로 가장 적절하지 않은 것은?

- ① 디스크, 데이터, 시스템 등의 파괴
- ② CPU, 메모리, 디스크 등의 시스템 자원을 고갈시켜 시스템 마비
- ③ 시스템 및 네트워크에 전송되는 데이터 등의 위변조를 통해 정보시스템 무력화
- ④ 네트워크 대역폭과 같은 네트워크 자원을 고갈시켜 네트워크 마비

3. 네트워크 트래픽을 암호화하여 스니핑(Sniffing)을 방어하는 기술이 아닌 것은?

- ① SSL(Secure Socket Layer) / TLS(Transport Layer Security)
- ② SSH(Secure Shell)
- ③ VPN(Virtual Private Network)
- ④ HTTP(Hyper Text Transfer Protocol)

4. TCP Session Hijacking 공격에 대한 설명으로 가장 적절하지 않은 것은?

- ① 정상적인 TCP 동작 과정에 내재된 고유의 취약점을 이용한 공격이다.
- ② 공격 과정에서 ARP Spoofing이 동반된다.
- ③ 사회공학적(Social Engineering) 해킹이다.
- ④ 기본적인 보안대책은 SSH(Secure Shell)와 같은 보안채널을 사용한다.

5. 다음 설명에 해당하는 악성 웹사이트 공격으로 가장 적절한 것은?

공격자는 웹사이트에 접속한 사용자가 스스로 원하지 않는 악의적 요청을 웹사이트로 보내게 유도하고, 이를 통해 사용자의 권한 획득을 시도한다. 이 공격이 성공하면, 공격자는 사용자의 권한으로 사용자와 해당 웹사이트를 공격하게 된다.

- ① SQL Injection
- ② 취약한 인증 및 세션 공격
- ③ CSRF
- ④ XSS

6. SSL(Secure Socket Layer) 혹은 TLS(Transport Layer Security)에서 서버와 클라이언트를 인증하기 위해 사용되는 기술로 가장 적절한 것은?

- ① 공개키 인증서 기술
- ② ID/Password 인증기술
- ③ OTP(One Time Password) 인증기술
- ④ FIDO(Fast IDentity Online) 인증기술

7. UNIX 계열 운영체제에서 해커가 특정 랜카드(LAN Card)로 들어오는 모든 패킷을 모아서 분석할 필요가 있을 때, 그 랜카드를 어떤 모드로 설정해야 하는가?

- ① Public 모드 ② Promiscuous 모드
- ③ Open 모드 ④ Personnel 모드

8. 해커는 DNS(Domain Name System) 서버를 공격하여 정상적인 도메인 이름에 대응하는 IP 주소를 자신이 만든 IP 주소로 변경한다. 이후 정상적인 도메인 이름으로 방문한 사용자를 해커가 만든 사이트로 유도한 뒤, 중요 개인정보 등을 입력하도록 하여 이를 갈취하는 공격으로 옳은 것은?

- ① 피싱(Phishing) 공격
- ② 스미싱(Smishing) 공격
- ③ 파밍(Pharming) 공격
- ④ 스니핑(Sniffing) 공격

9. 다음 중 아래 설명에 해당하는 것은?

네트워크에서 보안을 위협하는 악성 트래픽을 실시간으로 탐지 및 차단하는 능동형 보안기술이다. 주요기능으로는 외부망으로부터 들어오는 패킷의 실시간 분석, 침입 및 바이러스에 대한 상황별 실시간 대응, Zero-day 공격 탐지, 패킷 및 세션 행위기반 탐지 등을 들 수 있다.

- ① FW(Firewall)
- ② IPS(Intrusion Prevention System)
- ③ DDoS(Distributed Denial of Service)
- ④ IDS(Intrusion Detection System)

10. 다음 중 아래 설명에 해당하는 것은?

- (1) 네트워크에 접속하는 사용자나 장치가 정당한지를 검증한다. 이때, 사용자명/비밀번호 혹은 경우에 따라 MAC 주소가 검증 수단으로 사용된다.
- (2) 검증된 사용자나 장치가 네트워크 자원에 어떻게 접근할 수 있는지 결정한다. 경우에 따라 접근할 수 있는 네트워크, 서비스, 시간대를 제한할 수 있다.
- (3) 사용자나 장치가 네트워크를 접근한 기록을 남긴다. 이를 통해 어떤 장치를 누가, 언제, 어디서, 어떻게 사용했는지 알 수 있다.

- ① SAC(System Access Control)
- ② AAC(Account Access Control)
- ③ NAC(Network Access Control)
- ④ MAC(Mandatory Access Control)

11. 다음 중 SSL에 대한 설명 중 가장 적절하지 않은 것은?

- ① SSL은 안전한 서비스를 제공하기 위해 TCP를 사용하도록 설계되었다.
- ② SSL은 메시지에 대한 부인방지 기능을 제공한다.
- ③ SSL 레코드 프로토콜은 다양한 상위 계층 프로토콜에 기본적인 보안 서비스를 제공한다.
- ④ 웹/서버 상호교환을 위해 전송 서비스를 제공하는 HTTP는 SSL 위에서 작동할 수 있다.

12. 스위치(Switch) 네트워크 장비 환경에서 MAC(Media Access Control) 테이블의 저장용량을 초과하도록 공격하여 스위치 장비를 더미 허브(Dummy Hub) 장비처럼 작동시켜 모든 패킷을 스니핑하는 공격으로 옳은 것은?

- ① ARP Redirect 공격
- ② ICMP Redirect 공격
- ③ Switch Jamming 공격
- ④ SPAN Port Tapping 공격

13. 다음 중 ICMP를 활용하여 공격 대상 시스템의 활성화 여부를 알아보는 방법으로 가장 적절하지 않은 것은?

- ① ICMP Domain Name Request와 ICMP Domain Name Reply를 이용한다.
- ② ICMP Address Mask Request와 ICMP Address Mask Reply를 이용한다.
- ③ Information Request와 Information Reply를 이용한다.
- ④ Timestamp Request와 Timestamp Reply를 이용한다.

14. 다음 중 Sniffing 공격에 대한 대응방법으로 가장 적절하지 않은 것은?

- ① SSL을 사용한다.
- ② 가상시설망(VPN)을 사용한다.
- ③ 방화벽을 설치한다.
- ④ PGP를 사용한다.

15. 다음 중 이미 알려진 공격에 대한 침입패턴과 비교를 통해 침입을 탐지하는 IDS(Intrusion Detection System)의 탐지모델로 가장 적절한 것은?

- ① Misuse detection
- ② Anomaly detection
- ③ Behavior detection
- ④ Statistical detection

16. 다음 중 아래 설명에 해당하는 것은?

제품의 생산, 유통, 유지 등 모든 하드웨어 및 소프트웨어의 제조·유통 과정에서 악성코드를 배포하는 공격으로, SW 빌드 및 배포 과정에 악성코드를 삽입하여 선의의 소프트웨어를 통해 이용자들을 공격한다.

- ① Malware
- ② Ransomware
- ③ Blockchain Attack
- ④ Supply Chain Attack

17. 해커가 해킹할 시스템을 스캔(Scan)하여 시스템을 살피는 것은 중요하다. 다음 중 스캔을 통해 확인할 수 있는 내용이 가장 다른 하나는?

- ① TCP Open 스캔
- ② ICMP Echo Request와 Echo Reply 스캔
- ③ ICMP Timestamp Request와 Timestamp Reply 스캔
- ④ Ping 스캔

18. 다음 중 패킷 필터링 라우터에 대한 공격과 대응 방법이 잘못 짝지어진 것은?

- ① IP address spoofing - 패킷의 내부 발신지 IP 주소를 확인하여 차단
- ② Source routing attack - 발신지 경로 배정 옵션을 이용하는 패킷 모두 차단
- ③ Tiny fragment attack - TCP 패킷 중 IP fragment offset이 1인 패킷 모두 차단
- ④ ARP spoofing - 패킷의 외부 발신지 IP 주소를 확인하여 차단

19. 다음 중 네트워크 방화벽(Firewall)의 한계로 가장 적절하지 않은 것은?

- ① 바이러스 차단 불가
- ② 내부 공격자 차단 불가
- ③ 방화벽을 우회하는 공격 차단 불가
- ④ 패킷의 IP 주소와 이에 대응하는 포트번호 차단 불가

20. 다음 중 OSI 7계층의 2계층(Data Link)에 해당하는 공격으로 옳은 것은?

- ① DNS Spoofing ② ARP Spoofing
- ③ IP Spoofing ④ ICMP Spoofing

21. 본사와 지사 간에 임대 전용망을 사용하여 고가의 임대료를 지불하며 이들 간에 통신하였다. 고가의 임대료 문제를 해결하기 위해 전용망을 사용하지 않고 공용인터넷 사용을 고려하였다. 이를 위해 본사와 지사 간에 VPN(Virtual Private Network) 장비를 각각 설치하였다. 이를 통해서 본사와 지사 간에 터널링 기술로 Secure 채널이 만들어져 공용인터넷을 전용망처럼 사용하였다. 이와 같은 환경에서 가장 적절한 VPN 프로토콜은?

- ① IPsec(IP security)
- ② TLS(Transport Layer Security)
- ③ SSL(Secure Socket Layer)
- ④ SSH(Secure Shell)

22. 다음 중 오픈소스 라이브러리의 취약점을 이용한 공격으로 가장 적절하지 않은 것은?

- ① Lockbit 2.0 ② Apache Log4j
- ③ Spring4shell ④ HeartBleed

23. 다음 중 가상사설망(VPN)에서 사용하는 암호화 프로토콜에 해당하는 것은?

- ① L2TF ② PGP
- ③ S/MIME ④ WTLS

24. 사설 IP 주소가 할당된 클라이언트가 외부 공인 IP 주소를 가진 사이트에 접속할 때 사용하는 NAT(Network Address Translation)는?

- ① Exclude NAT ② Normal NAT
- ③ Redirect NAT ④ Reverse NAT

25. 다음 중 패킷 필터링 방화벽(Firewall)의 패킷에 포함된 정보로 가장 적절하지 않은 것은?

- ① IP Protocol Field
- ② Packet 생성 시간
- ③ Interface
- ④ Destination Transport-Level Address