네트워크 보안(9급)

(과목코드 : 142)

2024년 군무원 채용시험 응시번호 : 성명 :

1. DDoS 공격의 형태로는 대역폭 공격, 자원 소진 공격, 웹/DB 부하 공격 등의 형태가 있다. 다음 중 네트워크 대역폭을 대상으로 하는 DDoS 공격의 특징으로 가장 적절한 것은?
① 대상 서버에 과부하 발생
② 높은 connection
③ 높은 pps(packet per second)
④ 높은 bps(bit per second)

2. 다음에서 설명하는 네트워크 보안 솔루션은?

- 네트워크에 접근하는 접속 단말의 보안성을 강제화할 수 있는 보안 인프라 - 허가되지 않거나 웜·바이러스 등 악성코드에 감염된 PC나 노트북, 모바일 단말기 등이 회사 네트워크에 접속되는 것을 원천적으로 차단해 시스템 전체를 보호하는 솔루션

① IPS(Intrusion Prevention System)
② SIEM(Security Information & Event Management)
③ NAC(Network Access Control)
④ SSL(Secure Sockets Layer)

3. 다음은 어떤 공격에 대한 대응방안인가?

- 비동기화 상태 탐지 - ACK Storm 탐지 - SSH와 같이 암호화된 연결 사용

① ARP 스푸핑
② TCP 세션 하이재킹
③ DRDoS 공격
④ SYN Flooding 공격

4. 다음 중 내부에 서버가 존재할 경우에 설정하여 사용하는 NAT는?
① Normal NAT
② Reverse NAT
③ Redirect NAT
④ Exclude NAT

5. 다음과 같은 특징을 갖는 네트워크 공격 기법으로 가장 적절한 것은?

- 주로 CGI를 기반으로 하는 웹서버(apache 등) 대상의 공격을 수행 - 리눅스 계열 OS에서 주로 사용하는 GNU Bash에서 공격자가 원격으로 악의적인 시스템 명령을 실행

① 쉘 쇼크
② 워터링 홀
③ 하트 블리드
④ DNS 포이즈닝

6. traceroute는 패킷이 목적지까지 도달하는 동안 거쳐가는 라우터의 IP를 확인하는 도구이다. traceroute를 실행하여 패킷이 목적지 시스템에 도달하였을 때 출발지에서 확인할 수 있는 정보는?
① ICMP Echo Reply
② ICMP Time Exceeded
③ ICMP Port Unreachable
④ ICMP Information Reply

7. 다음 중 FIN, NULL, XMAS 스캔의 공통점으로 가장 적절한 것은?
   ① TCP의 플래그 중 일부만 설정하여 패킷을 전송한다.
   ② 정상적인 3-Way Handshaking을 통한 세션이 수립되지 않으므로 시스템에 로그가 남지 않는다.
   ③ UDP 프로토콜을 이용하면 동일한 정보를 수신하여 닫힌 포트를 확인할 수 있다.
   ④ 포트가 열려있는 경우 ACK 패킷을 수신함으로써 열려있는 포트를 확인하는 방식으로 스캔을 수행한다.

8. DSniff는 한국계 미국인 송덕준 교수가 개발한 패키지이다. DSniff의 도구 중 하나인 macof를 이용하면 스위치의 MAC 테이블에서 오버플로우를 발생시킬 수 있다. 이 현상을 이용하여 수행할 수 있는 공격에 대한 설명으로 가장 적절한 것은?
   ① 스위치에서 임의의 코드를 수행하여 다양한 네트워크 공격을 수행할 수 있다.
   ② Fail safe가 적용되어 네트워크 패킷을 모두 차단함으로써 네트워크 통신을 마비시키는 서비스 거부 공격이 가능하다.
   ③ MAC 주소와 IP 주소를 정적으로 연결하는 static 설정이 불가능하여 arp 스푸핑이 가능하다.
   ④ 스위치가 허브처럼 동작하여 모든 패킷을 모든 포트에 전송하게 되므로 스니핑이 가능하다.

9. TLS는 취약한 SSL을 보강하여 암호화 통신을 지원한다. 이때 협상된 보안 파라미터를 이용하여 암·복호화 및 무결성 검증 등을 수행하는 과정을 Record라 한다. 다음 중 발신측에서 수행하는 Record 프로토콜의 절차를 올바른 순서로 나열한 것은?

㉠단편화	㉡암호화	㉢MAC 적용
㉣Record 헤더 추가	㉤압축	

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

10. SSL/TLS는 주로 RSA의 보안성을 다운그레이드 시키는 방식의 취약점들이 발견되었다. 이러한 SSL/TLS 대상의 공격 방식과 가장 거리가 먼 취약점은?
   ① 프리크(freak)
   ② 로그포제이(Log4j)
   ③ 로그잼(logjam)
   ④ 푸들(POODLE)

11. 악성코드는 기능과 목적에 따라 다양한 형태로 분류할 수 있다. 다음 중 지정된 외부 주소에 접속 후 추가로 악성코드를 다운로드하여 실행하지만, 다운로드 자체는 악의적인 것이 아니기 때문에 백신 우회용으로 활용할 수 있는 악성코드는?
   ① 루트킷(Rootkit)
   ② 다운로더(Downloader)
   ③ 트로이 목마(Trojan Horse)
   ④ 드롭퍼(Dropper)

12. 네트워크 기반의 침입탐지 시스템에 대한 설명 중 가장 적절한 것은?
   ① Snort, Suricata는 네트워크 기반의 침입탐지에 활용할 수 있다.
   ② 개별 시스템에 설치되어 공격의 결과를 상세하게 파악할 수 있다.
   ③ 공격을 탐지하면 즉시 차단이 가능하다.
   ④ 실행 중인 파일, 프로세스, 레지스트리 등을 모니터링한다.

13. TCP는 연결지향 프로토콜로 가상의 연결 통로를 설정하여 물리적인 전용회선과 같이 동작한다. 다음 중 TCP에서 신뢰성을 확보하기 위하여 적용하는 제어 기법으로 볼 수 없는 것은?
   ① 흐름 제어　　② 오류 제어
   ③ 혼잡 제어　　④ 경로 제어

14. 다음 네트워크 프로토콜 중 가장 상위 계층에서 동작하는 것은?
① PPTP(Point-to-Point Tunneling Protocol)
② L2TP(Layer 2 Tunneling Protocol)
③ IPsec(Internet Protocol Security)
④ TLS(Transport Layer Security)

15. 다음 중 DDoS 공격을 방어하기 위한 기본적인 방법으로 가장 적절하지 않은 것은?
① 공격 트래픽의 소스 IP 주소 차단
② 방화벽 및 IDS/IPS 시스템을 이용한 필터링
③ 트래픽 분석을 통한 비정상적인 패턴 탐지
④ 유입되는 모든 트래픽을 허용하여 네트워크 자원을 최대한 활용

16. 제로트러스트 보안 모델에서 최소 권한 원칙에 대한 설명으로 가장 적절한 것은?
① 사용자에게 네트워크에 접근할 최소한의 권한만 부여해야 한다.
② 관리자만이 네트워크 자원에 접근할 수 있도록 해야 한다.
③ 사용자는 네트워크에 접근할 때마다 새로운 권한을 요청해야 한다.
④ 모든 네트워크 트래픽을 검증해야 한다.

17. TCP 연결설정을 위한 3-Way Handshaking 과정에서 Half-Open 연결 시도가 가능하다는 취약점을 이용한 공격 방식을 나타낸 것으로 가장 적절한 것은?
① 스머프 공격
② ARP 스푸핑
③ SYN Flooding 공격
④ 핑 오브 데스

18. OSI 참조 모델에서 라우터가 동작하는 계층은?
① 응용 계층
② 데이터링크 계층
③ 세션 계층
④ 네트워크 계층

19. 쿠키와 세션의 차이점을 가장 잘 설명한 것은?
① 쿠키는 파일로 저장되는 경우 탈취, 변조, 스니핑 등의 공격에 취약하다.
② 세션은 서버에서 데이터를 참조하므로 속도가 빠르다.
③ 쿠키는 브라우저를 종료하면 삭제된다.
④ 쿠키는 서버의 메모리에 저장된다.

20. SSL/TLS를 구성하는 프로토콜이 아닌 것은?
① Handshake Protocol
② Change Cipher Spec Protocol
③ Authorization Protocol
④ Record Protocol

21. 다음 중 ㉠, ㉡에 들어갈 도구 이름으로 가장 적절한 것은?

> (㉠)은(는) 네트워크 검색 및 보안 점검을 위해 제작된 오픈소스 도구로서 여러 가지 네트워크 스캐닝 관련 스크립트를 포함하고 있다.
>
> (㉡)은(는) 네트워크 연결을 통해 TCP연결, UDP 패킷 전송, 임의 TCP 및 UDP 포트청취 등을 수행할 수 있어 포트 포워딩, 데이터전송, 네트워크 디버깅 등에 활용할 수 있다.

① ㉠: netcat ㉡: nmap
② ㉠: netcat ㉡: Hydra
③ ㉠: Burp Suite ㉡: netcat
④ ㉠: Burp Suite ㉡: Hydra

22. TCP 연결설정을 위한 3-Way Handshaking 과정에서 주고받는 메시지의 종류와 순서가 올바른 것은?

① FIN → SYN → SYN ACK
② SYN ACK → ACK → SYN
③ SYN → SYN ACK → FIN
④ SYN → SYN ACK → ACK

23. 진짜처럼 꾸며진 가짜 와이파이로 접근을 유도한 뒤 사용자 신상정보를 훔치는 공격기법을 나타내는 용어는?

① 사회공학공격기법
② 딥페이크(Deep Fake)
③ 이블 트윈(Evil twin)
④ APT 공격

24. 다음 중 SSL Handshake를 하는데 주고받는 메시지의 순서가 올바른 것은?

㉠: Client Hello ㉡: Change Cipher Spec Finished ㉢: Server Key Exchange ㉣: Client Key Exchange ㉤: Server Hello ㉥: Certificate

① ㉠ → ㉢ → ㉣ → ㉡ → ㉤ → ㉥
② ㉥ → ㉠ → ㉤ → ㉢ → ㉣ → ㉡
③ ㉠ → ㉤ → ㉥ → ㉢ → ㉣ → ㉡
④ ㉤ → ㉠ → ㉢ → ㉥ → ㉣ → ㉡

25. ㉠, ㉡에 들어갈 단어로 가장 적절한 것은?

(㉠)은(는) 방화벽 정책 설정 시 (㉡) 패킷에 대해서는 차단 정책을 두지 않은 허점을 이용하는 공격 방식으로 서버에서 공격자의 컴퓨터로 접속하도록 하여 시스템의 보안정책을 우회한다.

① ㉠: 리버스 텔넷
㉡: 아웃바운드
② ㉠: 원격 데스크톱 프로토콜 공격
㉡: 아웃바운드
③ ㉠: 리버스 텔넷
㉡: 인바운드
④ ㉠: 원격 데스크톱 프로토콜 공격
㉡: 인바운드