네트워크 보안(7급)

(과목코드 : 142)

2024년 군무원 채용시험 응시번호 : 성명 :

1. 다음 설명 중 가장 적절하지 않은 것은?
   ① 프로토콜 데이터 단위인 PDU는 SDU(Service Data Unit)와 PCI(Protocol Control Information)로 구성되어 있다.
   ② 다중화란 여러 통신선로를 통해 여러 시스템이 동시에 통신할 수 있는 기법이다.
   ③ 프로토콜의 3요소는 구문, 의미, 순서이다.
   ④ 흐름제어는 송신측 개체에서 오는 데이터 양이나 속도를 조절하는 기능으로 송신측과 수신측의 속도차이 등으로 인한 정보유실을 방지한다.

2. OSI 7계층에 대한 설명으로 가장 적절하지 않은 것은?
   ① 7계층은 사용자 시스템에서 데이터 구조를 하나의 통일된 형식으로 표현해 데이터의 압축과 암호화를 수행하며 메일프로그램, 디렉토리 서비스 등을 제공한다.
   ② 5계층은 양끝단의 응용 프로세스가 통신을 관리하는 방법을 제공한다.
   ③ 2계층은 두 포인트 간의 신뢰성 있는 전송을 보장하기 위한 계층으로 CRC 기반의 오류제어 및 흐름제어가 필요하다.
   ④ 3계층은 다양한 길이의 데이터를 네트워크를 통해 전달하면서 그 과정을 통해 라우팅, 흐름제어, 오류제어를 수행한다.

3. 다음 중 응용계층에서 활용되는 프로토콜에 대한 설명으로 가장 적절하지 않은 것은?
   ① FTP는 서버와 클라이언트가 대화형으로 통신이 가능하며 20, 21번 포트를 사용한다.
   ② DNS는 도메인 이름 주소를 통해 IP 주소를 확인할 수 있으며 53번 포트를 사용한다.
   ③ SMTP는 메일 전송을 위한 프로토콜로 25번 포트를 사용한다.
   ④ SNMP는 네트워크 관리와 모니터링을 위한 프로토콜로 138번 포트를 사용한다.

4. 데이터 링크 계층의 설명으로 가장 적절하지 않은 것은?
   ① 스위칭은 패킷 전송 방식에 따라 컷스루 방식, 저장 후 전송 방식, 인텔리전트 스위칭 방식으로 구분한다.
   ② 프레임 릴레이란 전송오류제어나 흐름제어 등 복잡한 기능을 최소화하고 망 종단장치에서 처리하도록 해 고속 전송을 실현한 기술이다.
   ③ 이더넷 패킷 중 FCS(Frame Check Sequence)는 크기가 4Byte이며, 전송되는 패킷의 오류를 확인하기 위해 사용되는 필드이다.
   ④ 컷스루 방식은 완전한 프레임을 수신해 버퍼에 보관했다가 전체 프레임을 수신하면 CRC 등의 오류를 확인해 정상 프레임을 목적지 포트로 전송하는 방식이다.

5. SNMP(Simple Network Management Protocol)에 대한 설명으로 가장 적절하지 않은 것은?
   ① SNMP는 관리시스템과 관리대상(에이전트)으로 구분한다.
   ② SNMP는 TCP를 사용하며 Get Request, Get Next Request, Set Request는 관리시스템이 에이전트 정보를 얻거나 변경할 때 사용한다.
   ③ 관리시스템과 에이전트가 통신하려면 버전, 커뮤니티, PDU가 일치해야 한다.
   ④ Trap은 에이전트가 관리시스템이 미리 설정한 특정한 상황이 일어났음을 관리시스템에 알리는 메시지 송출 함수다.

6. 다음의 네트워크 장비 기능관리에 대한 설정으로 가장 적절하지 않은 것은?
   ① Finger 서비스 차단
   ② TCP keepalive 차단
   ③ Bootp 서비스 차단
   ④ source routing 차단

7. 스푸핑에 대한 설명 중 가장 적절하지 않은 것은?
   ① DNS 스푸핑은 실제 DNS 서버보다 빨리 공격 대상에게 DNS Response 패킷을 보내 공격 대상이 잘못된 IP 주소로 웹 접속하도록 유도하는 공격이다.
   ② ARP 스푸핑을 막는 방법으로는 MAC 테이블을 static으로 설정하는 방법이 있다.
   ③ DNS 스푸핑 공격을 피하는 방법으로 hosts 파일에 중요 사이트의 IP 주소를 적어두는 방법이 있다.
   ④ IP 스푸핑 공격의 대책으로 신뢰 대상의 MAC 주소를 동적으로 설정한다.

8. TCP세션 하이재킹에 대한 보안 대책으로 가장 적절하지 않은 것은?
   ① 전송 데이터를 암호화해서 전송한다.
   ② 서버와 시퀀스 넘버를 주기적으로 체크해 동기화 상태가 되는지 탐지해 대응한다.
   ③ 공격자가 중간에 끼어서 동작하므로 패킷의 유실과 재전송 증가를 탐지해 대응한다.
   ④ SSH와 같이 암호화된 연결을 사용한다.

9. 방화벽 구조에 대한 설명으로 가장 적절하지 않은 것은?
   ① 스크린된 호스트 게이트웨이 - 스크리닝 라우터보다 좀 더 발전된 형태의 방화벽으로 이 구조를 배스천 호스트라 한다.
   ② 이중 홈 게이트웨이 - 외부 네트워크와 내부 네트워크에 대한 네트워크 카드를 두 개 이상 갖추어 구분해 운영한다.
   ③ 스크리닝 라우터 - 일반 라우터에 패킷 필터링 규칙을 적용한 방화벽이다.
   ④ 스크린된 서브넷 게이트웨이 - 외부 네트워크와 내부 네트워크 사이에 서브넷을 두는 방화벽으로 서브넷에 DMZ가 위치한다.

10. Land Attack을 탐지하기 위한 snort 룰(rule) 중 가장 적절한 것은?
   ① log ip any any -> any 110 (session:printable;msg:“land attack”; sid:1000001;)
   ② alert ip any any -> any any (itype:0;msg:“land attack”;sid:1000001;)
   ③ alert ip any any -> 210.210.210.210/24 any (msg:”land attack”;sameip;sid:1000001;)
   ④ alert ip any any -> any any (flags:SF;msg:“land attack”;sid:1000001;)

11. VLAN(Virtual LAN)에 대한 설명으로 가장 적절하지 않은 것은?
   ① VLAN을 통해 논리적이고 유연한 망 구성이 가능하며 네트워크 분할 기능을 제공해 보안 수준을 높일 수 있다.
   ② VLAN은 스위치에서 설정하며 포트별로 수동 할당되는 형태를 정적 VLAN이라 한다.
   ③ VLAN 통신 시 두 개 이상의 스위치에서 여러 개의 VLAN 프레임을 전송할 때 트렁크 포트를 이용한다.
   ④ VLAN은 작은 네트워크로 나눈 후 각각의 작은 네트워크에 ARP Request, NetBIOS Name Query와 같은 멀티캐스트 패킷 제한 기능을 부여한다.

12. 다음 중 ARP(Address Resolution Protocol) 캐시 감염(Cache Poisoning) 공격의 발생 원인에 대한 설명으로 가장 적절한 것은?
   ① ARP 테이블이 모두 정적(static)으로 설정되어 있기 때문이다.
   ② ARP 요청(Request)의 목적지 IP에 해당하는 시스템만 응답(Reply) 메시지를 보낼 수 있기 때문이다.
   ③ 트러스트 인증 방법을 사용하고 있기 때문이다.
   ④ ARP가 상태 없는(Stateless) 프로토콜이기 때문이다.

13. IP 관리시스템과 유사하며, 2005년 가트너 그룹에서 새로운 네트워크 보안 모델을 제시하였다. 제시된 모델의 기능으로 접근제어 및 인증, PC 및 네트워크 장치 통제 그리고 해킹, 웜, 유해 트래픽 탐지 및 차단의 기능을 가진 것에 대한 설명으로 가장 적절한 것은?
① NAC(Network Access Control)
② SSH(Secure Shell)
③ VPN(Virtual Private Network)
④ SSL(Secure Socket Layer)

14. TCP 패킷 헤더의 Control Bit 설명으로 가장 적절하지 않은 것은?
① URG - 1이면 헤더의 마지막 필드인 긴급 포인터의 내용을 확인
② RST - 1이면 송신자에게 높은 처리율을 요구
③ SYN - 1이면 연결 요청과 설정, 확인 응답에서 순서번호를 동기화
④ FIN - 1이면 TCP 연결을 종료

15. 다음 중 침입탐지 시스템에 대한 설명으로 가장 적절하지 않은 것은?
① 데이터 수집을 위한 방식으로 호스트 기반, 네트워크 기반으로 구분 설치 운용할 수 있다.
② 침입탐지 기법의 오용탐지는 이미 발견되고 정립된 공격 패턴을 미리 입력해 두었다가 여기에 해당하는 패턴이 탐지되면 알려주는 방식이다.
③ 네트워크 기반 방식은 운영체제에 설정된 사용자 계정에 따라 어떤 사용자가 어떤 접근을 시도하고 작업했는지에 대한 기록을 남기고 추적하는 방식이다.
④ 목적에 따라 방화벽과 같이 외부와 내부의 경계선에 존재하지 않고 네트워크의 어느 부분에나 설치할 수 있다.

16. 다음 중 방화벽에 기능에 대한 설명으로 가장 적절하지 않은 것은?
① 방화벽은 접근제어 기능을 가지고 있다.
② 방화벽은 바이러스 차단 및 내부 공격 차단을 수행한다.
③ 방화벽 인증에는 메시지 인증, 사용자 인증, 클라이언트 인증과 같은 방법을 사용한다.
④ 로깅을 통해 방화벽을 통과하는 패킷과 연결에 대한 정보나 관리자의 설정 변경 정보를 저장한다.

17. 데이터베이스 서버 등 중요 시스템이 외부와의 연결을 필요로 하지 않은 경우 사설 IP로 할당하여 외부에서 직접 접근이 불가능하도록 설정하여야 한다. 다음 중 국제표준에 따른 사설 IP 주소 대역으로 옳은 것은?
① C Class: 192.0.0.1 ~ 192.255.255.255
② C Class: 192.16.0.1 ~ 192.31.255.255
③ C Class: 192.168.0.1 ~ 192.168.255.255
④ C Class: 192.200.0.1 ~ 192.200.255.255

18. 다음 중 아래 설명에 해당하는 것으로 가장 적절한 것은?

> 블루투스 장비 간의 취약한 연결 관리를 악용한 공격이다. 공격 장치와 공격 대상 장치를 연결하여 공격 대상 장치에서 임의의 동작을 실행하는 공격이다.

① 블루프린팅(Blueprinting)
② 블루스나핑(Bluesnarfing)
③ 블루버깅(Bluebugging)
④ 블루재킹(Bluejacking)

19. 다음 중 아래 설명에 해당하는 것으로 가장 적절한 것은?

> 특정 네트워크에 대하여 해당 네트워크에 속해 있는 시스템의 작동 유무를 판단할 수 있는 기법으로 이를 통해 목표(Target) 대상 기관에서 사용하거나 소유하고 있는 IP 주소와 네트워크 범위를 알아낼 수 있다.

① Sweep 스캔
② Open 스캔
③ Stealth 스캔
④ FTP 바운스(bounce) 스캔

20. NAC(Network Access Control) 구축 방식에 대한 설명 중 가장 적절하지 않은 것은?

① 인라인 방식 - 방화벽과 같이 물리적으로 접근을 차단하는 방식으로 일부 물리적 네트워크에 NAC를 추가하므로 기존 네트워크의 변경을 최소화할 수 있다.

② VLAN 방식 - 인가받지 않은 클라이언트가 인가된 클라이언트와는 다른 VLAN으로 격리되기 때문에 보안에 뛰어나다.

③ 소프트웨어 에이전트 설치 방식 - 네트워크 접속을 관리하는 서버에 에이전트를 설치하는 방식으로 각 클라이언트에 차단 정책을 설정해 관리한다.

④ ARP 방식 - 모든 스위치에서 ARP를 사용할 수 있기 때문에 장비의 제약이 없으며 구조가 단순해 빠르게 적용이 가능하다.

21. 다음 중 스머프(Smurf) 공격에 대한 대응책으로 가장 적절한 것은?

① ARP watch를 이용한 스니퍼(Sniffer) 탐지

② SSL(Secure Socket Layer)/TLS(Transport Layer Security) 적용

③ /etc/hosts 파일에 URL과 IP 정보 등록

④ 라우터의 다이렉트 브로드캐스트(Direct Broadcast) 기능 정지

22. 다음 중 windows 환경에서 ipconfig /displaydns에 표시되는 항목에 해당하지 않는 것은?

① 응답시간

② 데이터 유형

③ 데이터 길이

④ TTL(Time To Live)

23. SOAR(Security Orchestration, Automation and Response)에 대한 설명으로 가장 적절하지 않은 것은?

① SIRP(Security Incident Response Platform)

② SOA(Security Orchestration and Automation)

③ SPD(Security Policy Database)

④ TIP(Threat Intelligence Platform)

24. 다음 중 아래 설명에 해당하는 것으로 가장 적절한 것은?

> - 2023년 상반기에는 불특정 다수를 대상으로 하는 피싱 공격이 지속되었다.
> - 탈취된 계정정보는 해커의 다음 공격을 위한 비밀번호 사전(dictionary)으로 축적되거나 다크웹에서 팔리게 된다.
> - 특히 여러 사이트에서 동일한 비밀번호를 사용하고 있는 사용자라면 이 공격으로 추가 피해가 발생할 수 있다.
> - 공격자가 여러 방법으로 기존에 획득한 계정정보를 이용하여 다른 사이트에 로그인을 시도하는 공격이다.

① 크리덴셜 스터핑(Credential Stuffing)

② 피싱(Phishing) 공격

③ N-Day 취약점

④ 익스플로잇(Exploit) 공격

25. 다음 중 아래 설명에 해당하는 것으로 가장 적절한 것은?

> - 2023년 3월과 6월에 발표된 공격에 활용된 방법으로 공격자는 피해기관을 타겟팅해 언론사를 통한 이 기법으로 국가·공공기관 및 방산, 기업 등 국내외 주요기관 수십여 곳의 PC를 해킹한 것으로 알려졌다.
> - 공격 대상이 방문할 것으로 추정되는 특정 웹사이트를 해킹 후 취약점 공격 코드를 삽입하고 피해자의 접속을 기다리는 기법이다.
> - 취약한 버전의 프로그램이 설치된 사용자가 접속 시 악성코드에 감염된다.

① 워터링홀 공격(Watering Hole Attack)

② 제로데이 공격(Zero-day Attack)

③ 샤오치잉

④ 랜섬웨어(Ransomware)