2022-군무원-9급-네트워크보안-해설-곽후근

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

정답 체크
(1) IPS의 기능이다.
오답 체크
(2), (3), (4) ESM은 기업과 기관의 보안 정책을 반영하는 중앙 통합관리, 침입 종합대응, 통합 모니터링 가능한 지능형 보안관리 시스템이다. 주요 기능은 통합로그관리, 이벤트 필터링, 실시간 통합 모니터링, 경보, 상황전파, 로그 분석 및 의사결정지원, 긴급대응, 리포팅 등이다.

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.

정답 체크
(2) 방화벽에 대한 설명이다.
오답 체크
(1) 탐지만 하면 IDS이고, 차단까지 수행하면 IPS이다.
(3) 침입차단 시스템과 침입탐지 시스템의 장점을 결합한 보안 시스템이다. 침입 탐지를 침입 방지로 잘못 표기하였으나 가장 틀린 답은 아니다.
(4) IDS는 수동형이고, IPS는 능동형이다.

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.

정답 체크
(1) 스노트(Snort)는 무료의 오픈 소스 네트워크 침입 차단 시스템(IPS)이자, 네트워크 침입 탐지 시스템(IDS)으로서, 마틴 로시가 1998년에 개발하였다. 실시간 트래픽 분석과 IP에서의 패킷 로깅을 수행하는 능력을 갖고, 프로토콜 분석, 내용 검색 그리고 매칭을 수행한다.

오답 체크
(2) Arachni에 대한 설명이다.
(3) Ipccrack에 대한 설명이다.
(4) 백트랙과 칼리 리눅스에 대한 설명이다.

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.

정답 체크
(1) 서버를 무력화하는 공격으로 루트권한을 획득하는 공격과 무관하다.
오답 체크
(2) DoS를 통해 하드디스크를 파괴하기도 한다.
(3) 출발지 IP를 위조한다.
(4) 취약점을 공격하거나 자원을 고갈한다.

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 ㉣, ㉤

정답 체크
(2) ㄴ : 1이면 확인 번호 필드가 유효함을 나타낸다.
ㄷ : 1이면 TCP 연결을 다시 설정한다.
ㄹ : 1이면 연결 요청과 설정을 하고 확인 응답에서 순서 번호를 동기화한다.
ㅁ : 1이면 TCP 연결을 종료한다.
오답 체크
(1) ㄱ : PSH에 대한 설명이다.
(3) ㄴ이 없다.
(4) ㄴ, ㄷ이 없다.

6. 다음 지문은 무엇에 대한 설명인가?

사용자 PC를 악성코드에 감염시켜 이용자가 인터넷 '즐겨찾기' 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)

정답 체크
(1) Phishing(개인 정보)과 farming(대규모 피해)의 합성어이다. DNS Spoofing과 같이 인터넷 주소창에 방문하고자 하는 사이트의 URL을 입력하였을 때 가짜 사이트(fake site)로 이동시키는 공격 기법이다.
오답 체크
(2) 특정 소프트웨어를 실행할 때 또는 설치 후 자동적으로 광고가 표시되는 프로그램을 말한다. 프리웨어인 경우 불가피하게 광고 수익으로 운영되는 경우가 많으므로, 애드웨어라고 반드시 악성 소프트웨어에 속하는 것은 아니다.
(3) 특정 목표에 피해를 주는 것을 목적으로 하고 있는 해킹을 뜻한다.
(4) 운영체제나 프로그램을 생성할 때 정상적인 인증 과정을 거치지 않고, 운영체제나 프로그램 등에 접근할 수 있도록 만든 일종의 통로로 트랩도어(Trapdoor) 혹은 Administrative hook이라고도 불린다.

7. 다음 중 표준 이더넷 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: 1,518 byte,
최대 데이터 길이: 1,500byte
④ 최소 프레임 길이: 56byte,
최소 데이터 길이: 48byte

정답 체크
(3) 최대 프레임 길이 = 최대 데이터 길이 + 18바이트
18바이트 = 목적지주소(6바이트) + 출발지주소(6바이트) + 길이/PDU(2바이트) + CRC(4바이트)

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 증가시킨 다.

① Teardrop ② Land Attack
③ Syn Flooding ④ Smurf Attack

정답 체크
(4) 희생자의 스푸핑된 원본 IP를 가진 수많은 인터넷 제어 메시지 프로토콜(ICMP) 패킷들이 IP 브로드캐스트 주소를 사용하여 컴퓨터 네트워크로 브로드캐스트하는 분산 서비스 거부 공격이다. 네트워크의 대부분의 장치들은 기본적으로 원본 IP 주소에 응답을 보냄으로써 이에 응답한다. 원본 IP 주소를 컴퓨터는 대량의 ICMP 패킷을 받게 되므로 서비스 거부 상태에 빠지게 된다.
오답 체크
(1) 데이터의 송수신과정에서 데이터의 송신한계를 넘으면 MTU(1500byte) 조각으로 나누어 fragment number를 붙여 송신하고, 수신측에는 fragment 넘버로 재조합하여 분석한다. fragment 내의 나누어진 byte 정보인 fragmentation offset을 위조하여 offset을 중복되게 하거나 공간을 두면 수신측에서 재조합이 안 되어 다운이 되게 하는 공격이다. TCP에서는 순서 번호가 겹치고, UDP에서는 IP fragment offset이 겹치는 공격이다.
(2) 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소를 똑같이 만들어서 공격 대상에게 보내는 공격이다.
(3) 존재하지 않는 클라이언트가 서버별로 한정되어 있는 접속 가능한 공간에 접속한 것처럼 속여 다른 사용자가 서버의 서비스를 제공받지 못하게 하는 공격이다.

9. 다음 중 분산 서비스 거부 공격(DDoS, Distributed Denial of Service)의 공격 도구에 해당하지 않는 것은?
① Trinoo Attack ② TFN Attack ③ Targa Attack ④ Stacheldraht

정답 체크
(3) 여러 종류의 서비스 DoS 공격을 실행할 수 있도록 만든 '공격 도구'로 이미 나와 있는 여러 DoS 공격 소스들을 사용해 통합된 '공격 도구'를 만든 것이다. Targa에는 bonk, joit, land, nestea, newtear, syndrop, teardrop, winnuke 등이 있다.
오답 체크
(1) 1999년 6월 말부터 7월 사이에 퍼지기 시작한 것으로, 미네소타 대학 사고의 주범이다(원래 이름은 Trin00). 솔라리스 2.x(유닉스) 시스템에서 처음 발견되었으며, 최소 227개 시스템이 공격에 쓰인 것으로 알려져 있다. UDP를 기본으로 공격을 시행하며 ‘statd, cmsd, ttdbserverd’ 데몬이 주된 공격 대상으로 한다.
(2) 믹스터(Mixter)가 개발한 Trinoo가 약간 발전된 형태이다. Teletubby Flood Network라고 부르기도 한다. Trinoo처럼 statd, cmsd, ttdb 데몬의 취약점을 공격한다. 클라이언트(마스터)와 데몬 간에 ICMP Echo Request 패킷을 사용하고, TCP, UDP도 연결도 이루어지지 않아 모니터링이 쉽지 않다.
(4) 독일어로 ‘철조망’이라는 뜻이다. 1999년 10월에 처음 출현한 것으로 알려져 있으며, TFN을 발전시킨 형태이다. 공격자와 마스터, 에이전트, 데몬과의 통신에 암호화 기능이 추가되었다. Stacheldraht의 각 마스터가 제어할 수 있는 데몬의 개수는 기본적으로 1,000개이다. 마스터에 에이전트가 자동으로 갱신된다.

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

정답 체크
(3) 내외부 경계가 사라짐으로써 제로 트러스트 보안이 출현하였다.
오답 체크
(1) 데이터 및 리소스를 보호하기 위해 네트워크 경계에 기능적 장치 또는 기술을 설정한다.
(2) 엣지는 응답 시간을 개선하고 대역폭을 절약하기 위해 필요한 곳에 연산과 데이터 스토리지를 도입하는 하는 것으로 이에 대한 보안을 다룬다.
(4) 공용 인터넷에 연결되는 웹 애플리케이션, 웹 서버 및 기타 리소스는 내재적으로 공격에 취약하고, 이에 대한 보안을 다룬다.

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)

정답 체크
(4) 2017년의 Broken Authentication이다.
오답 체크
(1) 소프트웨어 업데이트 등에서 문제가 발생함을 의미한다.
(2) 디자인 패턴 등에서 보안 상의 결함을 의미한다.
(3) 서버의 요청이 위조되어 신뢰 관계의 서버에게 해당 요청을 수행함을 의미한다.

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)

정답 체크
(2) 라우터 탐색 프로토콜(IRDP, ICMP 라우터 탐색 프로토콜)를 갖는 장비가 네트워크에 진입시, 그 장비는 RS(Router Solicitation) 라는 ICMP 질의메세지를 방송한다. 라우터는 RA(Router Advertisement)로써 이에 응답하거나 또는 주기적으로 방송하며, 사용 가능한 라우터에 대한 정보

를 알려준다.
오답 체크
(1) 터널링은 IPv6/IPv4 호스트와 라우터에서 IPv6 데이터그램을 IPv4 패킷에 캡슐화하여 IPv4 라우팅 토폴로지 영역을 통해 전송하는 방법이다.
(3) IPv6와 IPv4 간의 주소 전환 장비를 이용하여, 기존의 IPv4에서 사용되던 NAT 기술과 마찬가지로 IPv6와 IPv4 간의 Address Table을 생성하여 양단간의 통신이 가능하도록 한다.
(4) IPv4/IPv6 듀얼스택은 IPv6 노드가 IPv4 전용 노드와 호환성을 유지하는 가장 쉬운 방법이다. IPv6/IPv4 듀얼스택 노드는 IPv4와 IPv6 패킷을 모두 주고받을 수 있는 능력이 있어, IPv4 패킷을 사용하여 IPv4 노드와 직접 호환된다.

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 루프 백(loopback)과 같은 특수주소를 가지는 데이터그램에 대해서는 ICMP 오류메시지가 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.

정답 체크
(4) 멀티캐스트 주소에 해당한다.
오답 체크
(1) 127.0.0.0 이나 0.0.0.0 과 같은 특별한 주소를 가진 데이터그램에 대해서는 오류 메시지가 생성되지 않는다.
(2) 처음 단편이 아닌 단편화된 데이터그램에 대해서는 ICMP 오류 메시지가 생성되지 않는다.
(3) ICMP 오류 메시지를 전달하는 데이터그램에 대해 ICMP 오류 메시지가 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 IP 헤더를 추가한다.
④ 전송층에서 온 정보에 IP 헤더만 추가하고 IPSec 헤더를 나중에 추가한다.

정답 체크
(2) 전송모드는 기존패킷을 보호한다.
오답 체크
(1), (2), (4) 터널모드에 해당한다.

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 코드로 된 메시지만 전송할 수 있다.
③ MIME에 기밀성과 무결성 같은 보안서비스를 위해 암호 메시지 구문(CMS, Cryptography Message Syntax)을 정의한다.
④ 암호 알고리즘으로는 대칭암호와 비대칭암호를 모두 사용할 수 있다.

정답 체크
(2) 이미지, 동영상 등도 전송할 수 있다.
오답 체크
(1) 안전한 전자메일 전송을 위한 산업체 표준 규약으로 기존 MIME 형식의 전자메일 서비스에 암호 및 보안 서비스가 추가된 구조이다.
(3) CMS object (Cryptographic Message Syntax)는 서명과 암호화 관련 데이터 필드를 포함한다.
(4) 하이브리도 암호를 사용한다.

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

정답 체크
(4) Record, Handshake(Handshake, ChangeCipherSpec, Alert, Application Data) 프로토콜을 사용한다.
오답 체크
(1), (2), (3) Authentication Header는 IPSec에서 사용하고, Peer Certificate는 SSL에서 사용된다. 그리고 SessionID는 HTTP에서 사용한다.

17. 데이터를 전용선(leased line)으로 전송하면 보안적 측면이나 속도면에서 좋지만 회선 사용료가 고가이며, 미사용 시간이 길어 대역폭 낭비가 발생 할 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)

정답 체크
(3) 공용망과 사설망의 장점을 결합한 네트워크이다.
오답 체크
(1) AS 내부(Intra-AS)의 라우팅 프로토콜이다.
(2) 시스코사가 만든 원래의 IGRP를 기반으로 한 개방형 라우팅 프로토콜이다.
(4) 논리적으로 분리한 랜이다.

18. 다음 중 HTTPS를 활성화하면 데이터는 대칭암호시스템으로 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.

정답 체크
(4) 공개키를 확보한다.
오답 체크
(1) 하이브리드 암호 방식이다.
(2) 서버는 개인키로 대칭키를 복호화한다.
(3) 대칭키로 암호화하면 속도를 향상시킬 수 있다.

19. 다음 중 커버로스(Kerberos)에 대한 설명으로 가장 옳은 것은?
① 네트워크 그룹을 이동시켜야할 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.

정답 체크
(3) AS, TGS를 이용한다.
오답 체크
(1) 가상랜을 의미한다.
(2) 스위치를 의미한다.
(4) 커버로스는 해시함수가 아니다.

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 요청 자에 대한 보안 요구 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 확장 인증프로토콜로 인증 절차를 수행한다.

정답 체크
(1) 해당 방식은 존재하지 않는다.
오답 체크

(2) 공격자를 분리된 VLAN에 할당한다(일반 PC가 있는 LAN에 접근할 수 없음).
(3) Port 또는 IP를 대상으로 차단한다.
(4) Radius 서버를 이용한다.

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 시간 초과 메시지 및 TCP 포트 도달 불가 오류 메시지를 이용해 구현한다.
④ Windows 명령어는 tracert이고, Linux 명령어는 traceroute이다.

정답 체크
(3) ICMP TTL Time Exceeded를 이용해 구현한다.
오답 체크
(1) ICMP를 이용하여 경로를 조사한다.
(2) ICMP를 이용하여 문제가 발생한 라우터를 찾는다.
(4) 운영체제에 따라 명령어 이름이 다름에 유의해야 한다.

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

정답 체크
(1) 통신 전 연결 단계에서 주고 받는 정보로 암호화되지 않는다.
오답 체크
(2), (3), (4) 연결 후에 해당 정보들이 암호화된다.

23. 다음 중 침입탐지시스템에 활용하는 기법으로 임계값 탐지와 프로파일 기반 변형 탐지를 활용하는 탐지 방법을 가장 적절하게 설명한 것은?
① 규칙 기반 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)

정답 체크
(2) 이상탐지에 해당한다.
오답 체크
(1) 오용탐지에 해당한다.
(3) 감사 기록을 이용하여 이상 또는 오용 탐지를 수행한다.
(4) 큰 네트워크에 여러 개의 IDS로 구성하여 탐지를 수행한다.

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)

정답 체크
(4) 해당 방화벽은 존재하지 않는다.
오답 체크
(1) 4계층 보안장비이다.
(2) 들어오는 패킷에 대한 정보를 기록하고 나갈 때 이와 비교하여 패킷을 필터링한다(동일 패킷은 허용).
(3) 5, 6, 7계층 보안장비이다.

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 닫혀 있는 경우 RST 플래그가 세팅된 패킷이 수신된다.
③ 플래그 하위 비트 6개를 모두 0으로 전송하면 대상 포트가 닫혀 있는 경우 PSH 플래그가 세팅된 패킷이 수신된다.
④ 플래그 하위 비트 6개를 모두 1로 전송하면 대상 포트가 닫혀 있는 경우 RST 플래그가 세팅된 패킷이 수신된다.

정답 체크
(3) RST을 수신한다.
오답 체크
(1) TCP open 또는 TCP half open에서 사용한다.
(2) Fin 스캔이다.
(4) Xmas 스캔이다.