2020-국가직-9급-네트워크보안-가형-해설-곽후근

문 1. 전송 과정에서 발생한 데이터 오류를 검출하고 검출된 오류를 정정할 수 있는 것은?
① BCD 코드
② 단일 패리티 비트
③ 해밍(Hamming) 코드
④ 체크섬
정답 체크
(3) 1950년에 해밍이 처음 고안한 것으로, 1비트의 오류를 정정할 수 있는 오류 정정 부호이다.
오답 체크
(1) 영숫자 코드로 6비트의 길이를 가지는 코드이다.
(2) 홀수 패리티(전송되는 데이터 중 1의 개수가 홀수 개)와 짝수 패리티(전송되는 데이터 중 1의 개수가 짝수 개)가 있다.
(4) 데이터와 1의 보수를 같이 보낸 후 수신지에서 데이터와 1의 보수를 더해서 결과 값이 0이면 수신하고 0이 아니면 폐기한다.

문 2. 방화벽과 침입탐지시스템의 장점을 결합한 네트워크 보안 장비로, 트래픽 모니터링과 유해 트래픽 차단을 목적으로 하는 것은?
① Honey Pot
② IPS
③ NAC
④ DMZ
정답 체크
(2) 수동적인 방어 개념의 침입 차단 시스템(Firewall)이나 침입 탐지 시스템(IDS)과 달리 침입 경고 이전에 공격을 중단시키는 데 초점을 둔, 침입 유도 기능과 자동 대처 기능이 합쳐진 개념의 솔루션이다.
오답 체크
(1) 크래커를 유인하는 함정을 꿀단지(곰을 유인)에 비유한 것에서 명칭이 유래한다. 마치 실제로 공격을 당하는 것처럼 보이게 하여 크래커를 추적하고 정보를 수집하는 역할을 한다. 침입자를 오래 머물게 하여 추적이 가능하므로 능동적으로 방어할 수 있고, 침입자의 공격을 차단할 수 있다. 직접적인 공격을 수행하지는 않는다.
(3) 접속 단말의 보안성을 검증해서 보안성을 강제화하고, 접속을 통제할 수 있는 보안 인프라이다. 내부 네트워크 접근하기 전에 보안 정책 준수했는지 여부를 검사해서 네트워크 접속을 통제한다.
(4) 기업의 내부 네트워크와 외부 네트워크 사이에 일종의 중립 지역이 설치되는 호스트 또는 네트워크이다. 외부 사용자가 기업의 정보를 담고 있는 내부 서버에 직접 접근하는 것을 방지하며, 외부 사용자가 DMZ 호스트의 보안을 뚫고 들어오더라도 기업 내부의 정보는 유출되지 않는다.

문 3. 다음에서 설명하는 SSL 프로토콜은?

메시지의 무결성과 기밀성을 제공하기 위하여, 클라이언트와 서버 간 약속된 절차에 따라 메시지에 대한 단편화, 압축, 메시지 인증 코드 생성 및 암호화 과정 등을 수행한다.

① Alert Protocol

② Record Protocol
③ Handshake Protocol
④ Change Cipher Spec Protocol
정답 체크
(2) 대칭 암호를 사용해서 메시지를 암호화하고 통신하는 부분이다. 대칭 암호와 메시지 인증 코드를 이용한다. 알고리즘과 공유 키는 핸드쉐이크 프로토콜을 사용해서 서버와 클라이언트가 상담하여 결정한다.
오답 체크
(1) 뭔가 에러가 발생했다는 것을 통신 상대에게 전달한다.
(3) 클라이언트와 서버가 암호 통신에 사용할 알고리즘과 공유 키를 결정한다. 인증서를 이용한 인증을 수행한다.
(4) 암호 방법을 변경하는 신호를 통신 상대에게 전달한다.

문 4. IPsec의 SA(Security Association)을 생성하기 위한 키 관리 방식은?
① EAPOL
② OSPF
③ DKIM
④ IKE
정답 체크
(4) 인터넷 표준 암호키 교환 프로토콜이다. 송신 측에서 수신 측이 생성한 암호키를 상대방에게 안전하게 송신하기 위한 방법이다.
오답 체크
(1) EAP Encapsulation over LAN의 약자로 LAN, WLAN을 통해 EAP 인증 메세지 패킷을 캡슐화하여 전달하는 프로토콜로써 802.1X에서 정의된다.
(2) 라우팅 프로토콜로써 AS(autonomous system) 내부(Intra-AS)에서 경로배정을 위해 사용된다.
(3) DomainKeys Identified Mail의 약자로 이메일 인증 방법 중 하나이다. 수신 서버에서 수신된 이메일이 위변조 되지 않았는지 디지털 서명을 이용해 검증하는 기술이다.

문 5. 163.152.175.62/26이 클래스 없는 주소(classless address)로 주어졌다. 해당 IP 주소가 속한 네트워크에 대한 설명으로 옳은 것만을 모두 고르면?

ㄱ. /26에서의 26은 prefix의 길이를 의미한다.
ㄴ. 네트워크 내의 주소 개수는 128개이다.
ㄷ. 네트워크 마스크는 255.255.255.128이다.
ㄹ. 네트워크에는 주소 163.152.175.15/26이 포함된다.

① ㄱ, ㄴ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄷ, ㄹ
정답 체크
(2) ㄱ : AND 마스크를 하는 1의 개수를 의미한다.
ㄹ : /26은 00, 01, 10, 11의 서브넷을 가지는데 62는 00에 포함되므로 0부터 63까지의 주소를 포함한다.

오답 체크

(1), (3), (4) ㄴ : 네트워크 내의 주소 개수는 64개이다.

ㄷ : 네트워크 마스크는 255.255.255.192이다.

문 6. 다음은 SSL 프로토콜에서 쌍방이 응용 데이터를 전송하기 전에, 인증 및 키 합의를 위하여 교환한 메시지의 일부를 나타낸 것이다. 메시지가 발생하는 순서를 바르게 나열한 것은? (단, 순서 중간에 다른 메시지가 포함될 수 있음)

ㄱ. Client_Key_Exchange ㄴ. Certificate ㄷ. Change_Cipher_Spec

① ㄱ → ㄴ → ㄷ

② ㄱ → ㄷ → ㄴ

③ ㄴ → ㄱ → ㄷ

④ ㄴ → ㄷ → ㄱ

정답 체크

(3) SSL에서 메시지 발생 순서는 다음과 같다(3 or 7, 8, 10 or 12의 순서로 메시지가 전달).

(1) ClientHello	사용하는 버전 번호, 현재 시각, 클라이언트 랜덤값, 세션 ID, 사용하는 암호 스위트 목록, 사용하는 압축 방법 목록을 보낸다.
(2) ServerHello	사용하는 버전 번호, 현재 시각, 서버 랜덤값, 세션 ID, 사용하는 암호 스위트 목록, 사용하는 압축 방법 목록을 보낸다.
(3) Certificate	인증서 목록을 보낸다.
(4) ServerKeyExchange	키 교환을 위한 정보로서 (3)의 Certificate 메시지만으로는 정보가 부족할 때, 클라이언트에게 필요한 정보를 전달한다.
(5) CertificateRequest	서버가 클라이언트에게 인증서를 요구한다.
(6) ServerHelloDone	서버가 보낸 메시지의 끝을 나타낸다.
(7) Certificate	서버의 CertificateRequest 메시지에 대한 응답으로 클라이언트가 서버에게 자신의 인증서를 전송한다.
(8) ClientKeyExchange	(4)의 ServerKeyExchange 메시지에 대응하여 적합한 키 교환 알고리즘을 선정하여 필요한 정보를 전송한다.
(9) CertificateVerify	서버로부터 CertificateRequest를 받은 뒤 클라이언트는 자신의 인증서 속 공개키와 쌍이 되는 정당한 개인 키를 가지고 있다는 것을 서버에게 주장하는 것이다.
(10) ChangeChiperSpec	이 메시지를 이용해서 암호를 변경할 수 있다.
(11) Finished	핸드쉐이크 프로토콜 종료를 요청한다.
(12) ChangeChiperSpec	서버가 클라이언트에게 암호를 교환하자고 메시지를 전송한다.
(13) Finished	서버도 클라이언트에게 Finished 메시지를 전송한다.

문 7. IEEE 802.11i의 키 관리에 대한 다음 설명에서 (가) ~ (다)에 들어갈 용어를 바르게 연결한 것은?

AAAK라고도 불리는 MSK는 IEEE 802.1X 프로토콜에 의해 인증 단계에서 생성된다. 인증의 마지막 과정이 끝나고 나면 AP(Access Point)와 STA(클라이언트 스테이션)는 (가)를 공유하게 된다. (가)로부터 AP와 STA 간의 통신에 사용할 (나)가 만들어지는데, (나)의 일부인 (다)가 사용자의 무선 데이터 패킷의 암호화에 사용된다.

	(가)	(나)	(다)
①	PMK	PTK	TK
②	PMK	TK	PTK
③	PTK	PMK	TK
④	PTK	TK	PMK

정답 체크

(1) PMK : MSK(IEEE 802.1x에 의해 만들어진다(RADIUS 패킷을 통해 AP에게 전달됨))로부터 만들어지는 키로, 무선단말과 AP 간에 공유되는 키이다.

PTK : PMK로부터 만들어지는 키이다.

TK : PTK로부터 만들어지는 키이다.

문 8. 방화벽 유형의 하나인 응용 레벨 게이트웨이에 대한 설명으로 옳은 것은?

① 외부 네트워크와 내부 네트워크 간의 직접적인 패킷 교환을 허용한다.

② OSI 참조 모델의 응용 계층에서 동작하며 여러 응용 서비스에 대하여 하나의 프록시로 구현된다.

③ 단순 패킷 필터링 방식에 패킷들의 상태 정보를 관리하는 기능이 추가된 것이다.

④ 응용 프로그램 수준의 트래픽을 기록하고 감시하기가 용이하며, 추가로 사용자 인증과 같은 부가 서비스를 지원할 수 있다.

정답 체크

(4) 응용 계층(layer 7)에서 동작한다.

오답 체크

(1) 패킷 필터링 방식(layer 4)과는 달리 외부와 내부 네트워크 간의 직접적인 패킷 교환을 허용하지 않는다.

(2) 여러 응용 서비스에 대하여 개별 프록시로 구현된다.

(3) stateful 방화벽에 대한 설명이다.

문 9. TCP RFC 793을 준수하는 시스템의 닫혀 있는 포트에 대하여 TCP FIN, NULL, Xmas 스캔을 한 경우 시스템의 반응으로 옳은 것은?

① ICMP 도달 불가능 오류 메시지

② 아무 응답 없음

③ RST

④ RST + ACK

정답 체크

(3) 닫힌 경우 RST 패킷을 전송한다.

오답 체크

(1) UDP 스캔을 하여 닫힌 상태를 의미한다.

(2) 열린 상태를 의미한다.

(3) TCP open 또는 half open에서 닫힌 상태를 의미한다.

문 10. SNMP(Simple Network Management Protocol)에 대한 설명으로 옳지 않은 것은?
① 관리자는 GetRequest와 같은 메시지를 에이전트에 보내서 에이전트의 정보를 요구한다.
② 에이전트는 비정상적인 상황을 관리자에게 경고하기 위하여 Trap 메시지를 관리자에 보냄으로써 관리 과정에 기여할 수 있다.
③ TCP/IP 프로토콜을 사용하는 인터넷에서 장치를 관리하기 위한 것으로, UDP 포트 161번과 162번을 사용한다.
④ MIB는 객체의 이름을 붙이고 객체의 유형을 정의하며, 객체와 값을 부호화하는 등의 일반적인 규칙을 정의한다.
정답 체크
(4) SMI를 의미하고, MIB는 관리자가 조회하거나 설정할 수 있는 개체들의 데이터베이스이다.
오답 체크
(1) Get Request, Get Next Request, Set Request, Get Response 등을 이용한다.
(2) Trap 메시지에는 Cold Start, Warm Start, Link Down, Link Up 등이 존재한다.
(3) Get Request를 위해 161번 포트를 사용하고, Trap을 위해 162번 포트를 사용한다.

문 11. IPv4 헤더의 필드 중, IP 패킷이 방문할 수 있는 최대 라우터 수를 제한하기 위한 것은?
① Time To Live
② Fragment Offset
③ Header Checksum
④ Flags
정답 체크
(1) 라우팅 과정에서 라우터를 몇 개 이상 통과하면 해당 패킷을 버릴지를 입력한다. 라우터 하나를 지날 때마다 값이 1씩 줄어들고 0이 되면 해당 패킷은 버려진다.
오답 체크
(2) 기존 데이터그램 안에서 단편의 상대적 위치를 의미한다.
(3) 패킷 전달 중 발생할 수 있는 오류 검사를 위해 사용하는 것으로, 송신측에서 체크섬을 계산하여 전송한다.
(4) 단편화 여부와 단편화된 조각이 첫 번째 조각인지, 중간 혹은 마지막 조각인지를 알려준다.

문 12. TCP 포트 번호 143을 사용하는 메일 접속 프로토콜로, 사용자가 폴더를 생성하고 폴더에 메시지를 할당하는 기능을 제공하는 것은?
① HTTP
② SMTP
③ POP3
④ IMAP
정답 체크
(4) POP3와 기본적으로 같으나, 메일이 확인된 후에도 서버에 남는다는 것이 다르다.
오답 체크
(1) 80번 포트를 사용하고, 웹서비스를 제공한다.
(2) 25번 포트를 사용하고, 메일을 보낼 때 사용한다.
(3) 110번 포트를 사용하고, 메일 서버로 전송된 메일을 읽을 때 사용한다.

문 13. ICMP Echo Request 패킷을 브로드캐스트 주소로 전송하여 많은 양의 응답 패킷이 공격 대상으로 전송되게 하는 서비스 거부 공격은?
① Ping of Death
② SYN Flooding
③ Smurf
④ Land
정답 체크
(3) 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) 네트워크에서는 패킷을 전송하기 적당한 크기(1,500바이트)로 잘라서 보내는데, Ping of Death는 네트워크의 이런 특성을 이용한 것이다. 네트워크의 연결 상태를 점검하기 위한 ping 명령을 보낼 때, 패킷을 최대한 길게 하여(최대 65,500바이트) 공격 대상에게 보내면 패킷은 네트워크에서 수백 개의 패킷으로 잘게 쪼개져 보내진다(DoS 공격).
(2) 클라이언트가 SYN 패킷을 보내고 서버는 이에 응답해서 SYN+ACK 패킷을 보낸다. 서버는 클라이언트가 ACK 패킷을 보내올 때까지 SYN Received 상태로 일정 시간을 기다려야 하고, 그동안 공격자는 가상의 클라이언트로 위조한 SYN 패킷을 수없이 만들어 서버에 보냄으로써 서버의 가용 동시 접속자 수를 모두 SYN Received 상태로 만들 수 있다.
(4) Land는 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소를 똑같이 만들어서 공격 대상에게 보내는 공격이다. (포트 번호도 같을 수 있다)

문 14. IPsec 터널 모드를 사용하는 VPN(Virtual Private Network)에 대한 설명으로 옳지 않은 것은?
① 인터넷과 같은 공중망을 이용하여 사설망의 효과를 얻기 위한 기술이다.
② 내부 네트워크의 호스트는 보안 게이트웨이를 거쳐서 통신함으로써 자신의 본래 IP 주소를 외부 네트워크에 노출하지 않는다.
③ 내부 IPv4 패킷의 전체를 암호화하고 선택적으로 인증할 수 있다.
④ IPv6의 경우에는 New IP Header를 사용하지 않고, 본래 헤더를 그대로 사용한다.
정답 체크
(4) 터널 모드는 IP 헤더를 포함한 전체 IP 패킷에 대한 보호하므로 New IP Header를 사용한다.
오답 체크
(1) 비용을 절감하고 보안을 유지한다.
(2) 내부 IPv4 패킷의 전체를 암호화하므로 자신의 본래 IP 주소를 노출하지 않는다.
(3) 암호화 따로, 인증 따로 수행할 수 있다.

문 15. 커버로스 버전 4의 메시지 교환 중, 클라이언트(C)가 서버(V)의 서비스를 얻기 위해 티켓발행서버(TGS)에게 보내는 메시지에 포함되지 않는 것은?
① C가 인증서버(AS)로부터 받은 티켓
② V의 식별자
③ C와 V가 사용할 공유비밀키

④ C와 TGS의 세션키로 암호화된 타임스탬프
정답 체크
(3) TGS가 클라이언트에게 보내는 메시지에 포함된다.
오답 체크
(1) TGT에 해당된다.
(2) IDv에 해당된다.
(4) Authenticator(클라이언트 ID, 클라이언트 IP, 타임스탬프가 C와 TGS의 세션키로 암호화됨)에 해당된다.

문 16. 사설 주소를 이용하는 내부 네트워크를 인터넷에 연결하는 NAT(Network Address Translation) 라우터에 대한 설명으로 옳지 않은 것은?
① 여러 개의 사설 주소는 내부 통신을 위하여 사용하고, 한 개 이상의 전역 인터넷 주소는 외부 통신을 위하여 사용하도록 해 준다.
② 변환 테이블을 이용하여 내부에서 외부로 전송하고자 하는 모든 패킷의 발신지 주소를 전역 주소로 변환해 준다.
③ 외부 인터넷에서 라우터뿐만 아니라 사설 주소를 사용하는 호스트를 식별할 수 있다.
④ 내부 네트워크 호스트와 외부 서버 프로그램들이 다대다 관계를 가질 수 있도록, 변환 테이블에는 IP 주소 외에 전송 계층의 포트 번호와 같은 추가적인 정보가 포함될 수 있다.
정답 체크
(3) 외부 인터넷에서 라우터(공인 주소)만 식별할 수 있고 호스트(사설 주소)를 식별할 수 없다.
오답 체크
(1), (2) 사설 주소를 전역 인터넷 주소로 바꿔주는 테이블을 의미한다.
(4) 내부에서 외부로 갈 때는 IP 주소를 이용하고, 외부에서 내부로 올 때는 포트를 이용한다(port forwarding).

문 17. ARP에 대한 설명으로 옳지 않은 것은?
① 호스트와 라우터는 IP 주소와 MAC 주소의 매핑 정보를 캐시 테이블에 가지고 있다.
② 캐시 테이블 정보를 공격자 호스트의 MAC 주소로 업데이트하게 하는 ARP 스푸핑 공격을 통해 스니핑이 발생할 수 있다.
③ 한 호스트의 캐시 테이블은 서브넷상의 모든 호스트와 라우터에 대한 엔트리를 가지고 있어야 한다.
④ ARP의 요청은 브로드캐스트되고, 응답은 유니캐스트된다.
정답 체크
(3) 모든 호스트와 라우터가 아닌 자신과 통신을 수행하는 상대에 대한 엔트리만 가지면 된다.
오답 체크
(1) 캐시 테이블을 가지면 매번 ARP 요청을 할 필요가 없다.
(2) 공격자가 가짜 MAC 주소를 주면 ARP spoofing 공격을 당하게 된다.
(4) MAC 브로드캐스트와 유니캐스트를 이용한다.

문 18. TCP의 3-Way Handshaking을 통한 서버와의 연결 설정 과정에서, 연결에 성공한 클라이언트 측의 연결 상태 천이 다이어그램상의 상태 변화의 순서를 바르게 나열한 것은?
① CLOSED → SYN_RCVD → ESTABLISHED
② CLOSED → SYN_SENT → ESTABLISHED
③ LISTEN → SYN_RCVD → ESTABLISHED
④ LISTEN → SYN_SENT → ESTABLISHED

정답 체크
(2) 클라이언트 측의 연결 상태 천이이다(연결이 닫힌 상태에서 SYN을 보내서 연결을 맺음).
오답 체크
(1), (4) 해당 연결 상태 천이는 발생하지 않는다.
(3) 서버 측의 연결 상태 천이이다.

문 19. IDS의 오용 탐지(misuse detection) 기법에 대한 설명으로 옳은 것은?
① 이미 발견되어 알려진 공격 패턴과 일치하는지를 검사하여 침입을 탐지한다.
② 오탐률이 높지만 새로운 공격 기법을 포함한 광범위한 공격을 탐지할 수 있다.
③ 정상적이고 평균적인 상태의 범주를 벗어나 상대적으로 급격한 변화를 일으키거나 확률이 낮은 일이 발생할 경우에 침입 탐지를 알린다.
④ 데이터 마이닝 등을 활용하여 수집한 다양한 정보를 분석하므로 많은 학습 시간이 소요된다.
정답 체크
(1) 시그너처 또는 knowledge를 이용한다.
오답 체크
(2), (3), (4) 이상 탐지(anomaly detection) 기법에 대한 설명이다.

문 20. IPsec의 ESP에서 재전송 공격(replay attack)을 방지하기 위해 사용하는 것은?
① Sequence Number
② SPI(Security Parameters Index)
③ ICV(Integrity Check Value)
④ Next Header
정답 체크
(1) 순서 번호를 이용하여 재전송 공격을 방지한다.
오답 체크
(2) SA를 나타내기 위한 인덱스이다.
(3) HMAC 등을 이용하여 인증과 무결성을 수행한다.
(4) 이후에 오는 패킷을 나타낸다.