2021-국가직-9급-네트워크보안-나형-해설-곽후근

문 1. IPv6의 특성으로 옳지 않은 것은?
① 32Bit에서 128Bit로 확장된 주소 공간
② IP 주소의 동적 할당
③ 인증 및 보안 기능 지원
④ 헤더를 고정길이에서 가변길이로 변경
정답 체크
(4) 가변길이(20바이트-60바이트)에서 고정길이(40바이트)로 변경하였다.
오답 체크
(1) 주소가 4배 확장되었다.
(2) IPv6 호스트는 IPv6 네트워크에 접속하는 순간, 자동적으로 호스트 주소를 부여받는다.
(3) 패킷 출처 인증과 데이터 무결성 및 비밀 보장 기능을 IP 프로토콜 체계에 반영하였다. IPv4에서는 IPSec이 선택이었으나, IPv6에서는 필수이다.

문 2. 다음에서 설명하는 통신규약은?

○ IETF에서 만든 공개키암호화 표준을 따름 ○ PGP에 비해 보안성이 높지만 사용이 어려움 ○ 전자우편 사용 시 전송하기 전에 자동으로 암호화하여 전송 도중 유출되어도 편지의 내용을 알 수 없음

① PPTP
② DNS
③ SNMP
④ PEM
정답 체크
(4) 인터넷상에서 안전한 전자우편을 제공하기 위해 제안된 인터넷 표준안을 만드는 기술위원회(IETF: Internet Engineering Task Force) 표준안이다.
오답 체크
(1) Microsoft사에서 제안한 프로토콜로 OSI 2계층에서 동작한다. 처음에는 1:1 연결을 지원하고 암호화를 지원한다.
(2) 도메인 혹은 호스트 이름을 IP 주소로 변환해 준다. Inverse(Reverse) DNS는 IP 주소를 도메인 혹은 호스트 이름으로 변환한다.
(3) SNMP는 네트워크 장비 관리와 모니터링을 위해 사용된다.

문 3. 무선 LAN에서 사용하는 인증 프로토콜은?
① RIP
② EAP
③ BGP
④ SIP
정답 체크

(2) EAP는 EAP 방식들이 만들어내는 키 요소와 매개변수의 전송 및 이용을 제공하기 위한 인증 프레임워크이다. RFC가 정의하는 방식들의 수는 많으며 수많은 업체에 특화된 방식들과 새로운 제안들이 존재한다. EAP는 유선 프로토콜이 아니며 단지 메시지 포맷을 정의하기만 할 뿐이다. EAP를 사용하는 개별 프로토콜은 프로토콜의 메시지 내의 EAP 메시지들을 캡슐화하는 방법을 정의한다. 예를 들면, EAP-TLS, EAP-MD5, EAP-PSK 등이 있다.
오답 체크
(1) AS(autonomous system) 내부(Intra-AS)에서 경로배정을 위해 사용되는 라우팅 프로토콜이다.
(3) AS 경계(Inter-AS)에서 경로배정을 위해 사용되는 라우팅 프로토콜이다.
(4) 인터넷 기반 회의, 전화, 음성 메일, 이벤트 통지, 인스턴트 메시징 등 멀티미디어 서비스 세션의 생성, 수정, 종료를 제어하는 요구/응답 구조로서 TCP와 UDP에 모두 사용한다.

문 4. Land 공격의 출발지 주소와 목적지 주소로 옳은 것은?

	출발지 주소	목적지 주소
①	192.168.0.1	192.168.0.1
②	192.168.0.1	192.168.0.200
③	192.168.0.5	192.168.0.1
④	192.168.0.5	192.168.0.200

정답 체크
(1) 2가지 조건을 만족해야 한다. 첫 번째는 출발지 주소와 목적지 주소가 일치해야 한다는 것이고, 두 번째는 해당 주소가 목적지 주소의 내부 IP여야 한다는 것이다.
오답 체크
(2), (3), (4) 출발지 주소와 목적지 주소가 일치하지 않는다.

문 5. 다음에서 설명하는 보안 기술은?

> ○ 외부 네트워크로부터의 공격 탐지에 중점을 두는 전사적 보안 관리(ESM) 기능에 내부의 정보 유출 탐지 영역까지 담당
> ○ ESM와 상호보완적인 관계로 다양한 정보시스템에 대한 로그 관리 및 분석이 강화되고 빅데이터 기술이 접목되어 정보시스템 전반에 대한 신속한 위협 탐지가 가능한 지능형 로그 관리 플랫폼

① DLP
② NAC
③ SIEM
④ DRM
정답 체크
(3) 로그 분석해서 이상 징후 파악한 후 결과를 경영진에게 보고할 수 있도록 해주는 시스템이다. 이벤트 로그 데이터를 실시간 수집/분석한다. 침해 공격 로그에 대한 포렌식(디지털 증거)과 컴플라이언스(보안에 대한 방향성 제시) 또는 법적 조사를 위해 해당 데이터의 신속한 검색, 리포팅한다. 원본 이벤트 정보 분석하기보다, 정규화 과정을 통해 데이터 표준화해서 분석한다.
오답 체크
(1) 기업 내에서 이용하는 다양한 주요 정보인 기술 정보, 프로젝트 계획, 사업 내용, 영업 비밀, 고객 정보 등을 보호하고 외부 유출을 방지하기 위해서 사용된다.

(2) 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) 콘텐츠 제공자의 권리와 이익을 안전하게 보호하며 불법복제를 막고 사용료 부과와 결제대행 등 콘텐츠의 생성에서 유통·관리까지를 일괄적으로 지원하는 기술이다.

문 6. 포트 스캔에 대한 설명으로 옳지 않은 것은?
① TCP stealth 스캔은 정상적인 3-way handshake를 완성하지 않아 로그를 남기지 않는다.
② XMAS 스캔은 NULL 스캔과 반대로 모든 플래그를 설정하여 패킷을 전송한다.
③ NULL 스캔은 어떠한 플래그도 설정하지 않고 NULL 상태로 패킷을 전송한다.
④ UDP 포트 스캔은 3-way handshake 절차를 거쳐 수행한다.
정답 체크
(4) UDP 포트 스캔은 TCP와 같이 연결을 맺지 않는다.
오답 체크
(1) TCP open 스캔은 로그를 남기지만, TCP half open은 로그를 남기지 않는다.
(2) XMAS는 TCP의 모든 플래그를 설정한다.
(3) NULL은 TCP의 어떤 플래그도 설정하지 않는다.

문 7. Brute Force Attack에 대한 설명으로 옳지 않은 것은?
① 특정 단어 또는 문자 조합으로 성공할 때까지 대입을 시도해 원하는 계정 정보를 얻는다.
② 공격이 가능한 서비스는 Telnet, FTP 등이 있다.
③ 공격을 막는 방법에는 포트 변경, 패스워드 변경, 필터링 툴 사용 등이 있다.
④ 악성 스크립트가 삽입되어 있는 페이지를 읽는 순간 방문자의 브라우저를 공격한다.
정답 체크
(4) XSS 공격에 해당한다.
오답 체크
(1) 다양한 길이와 다양한 조합에 대해 대입을 시도해 본다.
(2) ID/PW에 전사 공격을 수행한다.
(3) 포트를 변경하여 서비스를 노출시키지 않고, 패스워드를 주기적으로 변경하여 전사 공격을 막는다. 또한 전사 공격이 수행되는 것을 필터링하는 툴을 사용한다.

문 8. HMAC(Hashed MAC)에 대한 설명으로 옳지 않은 것은?
① RFC2004에서 정의된 HMAC은 수정 없이 이용 가능한 해시함수를 사용하면 소프트웨어 구현이 어렵다.
② IP 보안을 위한 필수 구현 MAC으로 선택되어 TLS나 SET에서 사용된다.
③ 더 빠르고 안전 해시함수가 있거나 필요하다면 기존의 해시함수를 쉽게 바꿀 수 있다.
④ 심각하게 기능 저하를 유발하지 않고 해시함수의 원래 성능을 유지하도록 한다.
정답 체크
(1) 소프트웨어에서 잘 돌아가고 코드를 무료로 제공하고 널리 쓸 수 있도록 한다.
오답 체크
(2) 해시 기반의 MAC(메시지 인증 코드, 상호 인증과 무결성 수행)으로 TLS, IPSec, SSH, SET 등에 사용된다.
(3) 해시함수는 고정된 것이 아니라 더 좋은 것으로 언제든지 교체가 가능하다.
(4) 성능을 유지하기 위해 기능 저하가 발생하면 안된다.

문 9. 매체 접근 기법 중에서 유선망에서 사용되며, 호스트가 채널의 상태를 감지하여 충돌을 피하는 데이터 전송 방안은?
① Token Bus
② Carrier Sense Multiple Access with Collision Detection
③ Token Ring
④ Carrier Sense Multiple Access with Collision Avoidance
정답 체크
(2) MA는 네트워크가 비어있으면 누구나 사용 가능함을 의미하고, CS는 네트워크가 사용 중인지 확인함을 의미한다. 그리고 CD는 데이터를 전송하며 충돌여부 감지함을 의미한다.
오답 체크
(1) 버스 구조에서 토큰이 있어야 데이터를 전송할 수 있는 LAN을 의미한다.
(3) 링 구조에서 토큰이 있어야 데이터를 전송할 수 있는 LAN을 의미한다.
(4) 무선망에 사용되고, 무선을 특성을 고려하여 충돌을 회피한다.

문 10. VLAN에 대한 설명으로 옳지 않은 것은?
① 물리적 장치의 이동이나 분리 없이 소프트웨어로 하나의 LAN으로 구현된다.
② 물리적인 세그먼트가 아닌 논리적인 세그먼트로 분할한다.
③ VLAN 멤버십 구성 정보로는 포트 번호, MAC주소, IP주소 등이 있다.
④ VLAN 표준으로 IEEE 802.3 부위원회에서 IP 태깅을 위한 IP 형식을 정의하는 802.3Q표준을 제정하였다.
정답 체크
(4) 802.3Q가 아닌 802.1Q이다.
오답 체크
(1), (2) 물리적인 세그먼트(하드웨어 분리)가 아닌 논리적인 세그먼트(소프트웨어 분리)이다.
(3) 포트, MAC, IP 주소 등이 포함되지만 Payload는 포함되지 않는다.

문 11. OSI 7계층의 응용 계층 프로토콜로 옳지 않은 것은?
① FTP
② TCP
③ HTTP
④ SMTP
정답 체크
(2) 전송 계층 프로토콜이다.
오답 체크
(1) 파일 전송 관련 응용 계층 프로토콜이다.
(3) HTML 전송 관련 응용 계층 프로토콜이다.
(4) 이메일 관련 응용 계층 프로토콜이다.

문 12. L2 스위치에 대한 설명으로 옳은 것은?
① OSI 2계층에서 기능을 수행하며, 고유 MAC 정보를 사용하여 통신한다.
② 패킷의 정보를 확인하여 가장 빠른 네트워크 IP 주소 경로를 찾아내 패킷을 전달한다.

③ 서로 다른 프로토콜 통신망 간에도 프로토콜을 변환하여 정보를 주고받을 수 있다.
④ 응용 계층까지 분석해서 높은 수준의 로드밸런싱을 수행한다.
정답 체크
(1) 스위칭 허브나 브리지가 존재한다.
오답 체크
(2) L3 스위치인 라우터를 의미한다.
(3) 전계층 정보를 이용하는 게이트웨이를 의미한다.
(4) L7 스위치인 어플리케이션 스위치를 의미한다.

문 13. 다음에서 설명하는 네트워크 기반 유틸리티는?

○ 네트워크 모니터링 및 패킷 분석을 위해 많이 사용
○ 패킷 수집을 위해 libpcap 라이브러리를 사용
○ 유닉스 및 윈도우즈 등에서 사용

① ping
② netstat
③ tcpdump
④ traceroute
정답 체크
(3) 네트워크 모니터링 및 패킷 분석을 위해 가장 많이 사용되며 모든 모니터링 및 패킷 분석 툴의 모태가 된다(현재는 wireshark를 많이 사용).
오답 체크
(1) IP 네트워크를 통해 특정한 호스트가 도달할 수 있는지의 여부를 테스트하는 데 쓰이는 컴퓨터 네트워크 도구의 하나이다.
(2) 컴퓨터 내에서 사용 중인 포트를 확인할 때 사용한다.
(4) 최종 목적지 컴퓨터(서버)까지 중간에 거치는 여러 개의 라우터에 대한 경로 및 응답속도를 표시해 준다(리눅스/유닉스). 윈도우에서는 tracert를 사용한다.

문 14. 취약점을 악용해 공격을 수행하는 프로그램뿐만 아니라 공격 수행 절차, 스크립트 등을 의미하는 것은?
① Exploit
② Bell-LaPadula
③ Biba
④ IPSec
정답 체크
(1) 컴퓨터 소프트웨어와 하드웨어의 버그나 취약점 등을 이용하여 공격자가 원하는 악의적 동작을 하도록 하는 공격 방법이다.
오답 체크
(2) 미 국방부 지원 보안 모델로 보안 요소 중 기밀성 강조한다. 최초의 수학적 모델로 강제적 정책에 의해 접근 통제하는 모델이다. 보안 정책은 정보가 높은 레벨에서 낮은 레벨로 흐르는 것을 방지한다. BLP의 속성은 No Read Up(보안 수준이 낮은 주체는 보안 수준이 높은 객체를 읽어서는 안되는 정책), No Write Down(보안 수준이 높은 주체는 보안 수준이 낮은 객체에 기록해서는 안됨)이다.

(3) BLP의 단점을 보완한 무결성을 보장하는 최초의 모델이다. 비바의 속성은 BLP의 반대 개념인 No Read Down (높은 등급의 주체는 낮은 등급의 객체를 읽을 수 없음), No Write Up(낮은 등급의 주체는 상위 등급의 객체를 수정할 수 없음)이다.
(4) IP 망에서 안전하게 정보를 전송하는 표준화된 OSI 3계층 프로토콜이다.

문 15. SSH에 대한 설명으로 옳은 것은?
① SSH는 TCP 및 UDP 기반의 보안 프로토콜이다.
② SSH 전송계층 프로토콜, SSH 인증 프로토콜, SSH 연결 프로토콜을 포함한다.
③ SSH는 SSH 터널링을 지원하지 않는다.
④ SSH 전송계층 프로토콜은 다수의 기본 SSH 연결을 사용하여 통신채널을 다중화한다.
정답 체크
(2) TCP 위에 전송계층, 사용자인증, 연결 프로토콜을 포함한다.
오답 체크
(1) TCP 기반의 프로토콜이다.
(3) VPN 등에서 사용되는 터널링을 지원한다.
(4) 다중화는 전송계층이 아닌 연결 프로토콜에서 제공한다.

문 16. DDoS 공격기법에 해당하지 않는 것은?
① Trin00
② TFN
③ MITM
④ Stacheldraht
정답 체크
(3) DDoS가 아닌 중간자 공격 기법이다.
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.
(2) 믹스터(Mixter)가 개발한 Trinoo가 약간 발전된 형태이다. Teletubby Flood Network라고 부르기도 한다. Trinoo처럼 statd, cmsd, ttdb 데몬의 취약점을 공격한다.
(4) 독일어로 '철조망'이라는 뜻이다. 1999년 10월에 처음 출현한 것으로 알려져 있으며, TFN을 발전시킨 형태이다. 공격자와 마스터, 에이전트, 데몬과의 통신에 암호화 기능이 추가되었다.

문 17. 다음에서 설명하는 스위치 환경에서의 스니핑은?

○ 스위치에 저장 용량 이상의 MAC 주소를 보내 스위치 기능을 잃고 더미 허브처럼 동작하게 만드는 방식
○ 일부 고가 스위치는 MAC 테이블의 캐시와 연산 장치가 쓰는 캐시가 독립적으로 나뉘어 스니핑 공격이 통하지 않는 경우도 있음

① ICMP 리다이렉트
② SPAN 포트 태핑
③ 스위치 재밍

④ ARP 리다이렉트
정답 체크
(3) 스위치의 주소 테이블의 기능을 마비시키는 공격이다. MACOF(MAC Flooding) 공격이라고도 한다. 스위치에 랜덤한 형태로 생성한 MAC을 가진 패킷을 무한대로 보내면, 스위치의 MAC 테이블은 자연스레 저장 용량을 넘게 되고, 스위치의 원래 기능을 잃고 더미 허브(패킷을 받으면 브로드캐스팅 한다)처럼 작동하게 된다. 공격자가 자연스럽게 브로드캐스팅된 패킷을 스니핑(sniffing)할 수 있다.
오답 체크
(1) 3계층에서 스니핑(sniffing) 시스템을 ICMP Redirect 메시지를 통해 네트워크에 존재하는 또 다른 라우터라고 알림으로써 패킷의 흐름을 바꾸는 공격이다.
(2) 스니핑을 위해 포트 미러링(Port Mirroring)을 이용한 것이다. 포트 미러링이란 각 포트에 전송되는 데이터를 미러링하고 있는 포트에도 똑같이 보내주는 것이다.
(4) 공격 대상에게 자신의 MAC 주소가 라우터인 것처럼 속이는 것을 의미한다(자신이 라우터라고 arp reply를 보냄).

문 18. IDS(Intrusion Detection System)에 대한 설명으로 옳지 않은 것은?
① IDS는 네트워크기반 및 호스트기반의 침입탐지시스템으로 분류할 수 있다.
② 침입탐지 기법 중 오용탐지기법은 시그니처기반 탐지 또는 지식기반 탐지로 불린다.
③ 네트워크기반 침입탐지시스템은 네트워크 전반에 대한 감시를 할 수 있다.
④ 호스트기반 침입탐지시스템은 시스템의 로그에 대한 탐지보다는 네트워크 패킷을 수집하여 공격을 판단한다.
정답 체크
(4) 네트워크 패킷을 수집하여 공격을 판단하는 것보다 시스템의 로그에 대한 탐지를 수행한다.
오답 체크
(1) 네트워크기반은 네트워크 중간에 설치되고, 호스트기반은 개별 호스트에 설치된다.
(2) 오용탐지는 패킷을 시그너처(웜이나 바이러스가 가지는 특정 문자열)와 비교한다.
(4) 네트워크 중간에 설치되므로 네트워크 전반에 대한 감시를 수행한다.

문 19. Wireshark에 대한 설명으로 옳지 않은 것은?
① 윈도우즈 운영체제만을 지원한다.
② www.wireshark.org에서 구할 수 있는 프로그램이다.
③ 네트워크 분석도구이다.
④ 트래픽 수집을 위해 WinPcap을 사용한다.
정답 체크
(1) 리눅스를 포함한 다양한 유닉스 계열 운영 체제와 윈도우에서 동작한다.
오답 체크
(2) 해당 사이트를 통해 공개 배포한다.
(3) 네트워크를 분석하거나 통신 프로토콜 개발에 사용된다.
(4) WinPcap이라는 패킷 캡처 라이브러리를 사용한다.

문 20. 네트워크 관리기능에 대한 설명으로 옳은 것은?
① 장애 관리 – 네트워크의 동작 및 효율성을 평가하는 기능
② 구성 관리 – 상호 연결 및 네트워크의 정보를 제공하는 기능

③ 성능 관리 – 비정상적인 동작을 발견하고 대처하는 기능
④ 보안 관리 – 자원 사용량과 관련이 있는 네트워크 데이터를 수집하는 기능
정답 체크
(2) 네트워크와 사용되는 모든 장치 및 연결된 장치를 구성하여 특정 작업을 수행하는 것이다.
오답 체크
(1) 성능 관리에 해당하고, 장애 관리는 문제를 감지한 후 격리하고 해결하고 해결 과정을 기록한다.
(3) 장애 관리에 해당하고, 성능 관리는 데이터 수집과 분석을 통해 이루어지며 운영의 임계값을 설정한다.
(4) 성능 관리에 해당하고, 보안 관리는 방화벽, 프록시, 바이러스 백신 소프트웨어 및 침입 시도를 탐지하는 시스템 구현을 통해 네트워크 구조를 보호한다.