2020-해경1차-네트워크보안-해설-곽후근

1. 다음 중 스니핑(Sniffing) 공격에 대처하는 방법으로 가장 올바른 것은?
① 전용 네트워크 망에서만 통신을 수행한다.
② SSL, SSH를 사용한다.
③ VLAN 기능을 활성화한다.
④ 데이터 전송시에 패킷마다 다른 경로를 사용한다.
정답 체크
(2) 암호화를 수행하면 스니핑 공격을 막을 수 있다.
오답 체크
(1) 전용 네트워크 망에서도 스니핑이 발생할 수 있다.
(3) 가상랜을 사용해도 스니핑을 막을 수 없다.
(4) 다른 경로를 사용해도 스니핑이 발생할 수 있다.

2. 다음 중 NAT(Network Address Translation)를 사용하는 가장 근본적인 이유로 올바른 것은?
① IP 주소 부족 문제를 해결
② 데이터 암호화
③ 네트워크 세그먼테이션
④ 네트워크 전송 속도 향상
정답 체크
(1) NAT를 사용하면 public IP 대신에 private IP를 사용할 수 있으므로 IP 주소 부족 문제를 해결할 수 있다.
오답 체크
(2) NAT에서는 데이터 암호화를 하지 않는다.
(3) NAT는 네트워크 세그멘테이션(네트워크 상에서 서브 네트워크를 만들어내어 공격자가 전체 네트워크가 아닌 일부 서브 네트워크에 접속할 수 있게함) 기술이 아니다.
(4) NAT 과정으로 인해 전송 속도가 오히려 늦어진다.

3. 다음 중 OSI 계층구조와 계층별로 사용되는 보안 프로토콜의 연결이 가장 옳지 않은 것은?
① 데이터링크 계층 - TLS
② 네트워크 계층 - IPSec
③ 전송계층 - SSL
④ 응용계층 - SSH
정답 체크
(1) TLS는 전송계층이고, 데이터링크 계층은 MACSec이다.
오답 체크
(2) VPN에서 사용한다.
(3) HTTPS에서 사용한다.
(4) telnet, ftp의 보안 버전으로 사용한다.

4. 다음 중 UTM(Unified Threat Management)에 대한 설명으로 가장 옳지 않은 것은?

① 방화벽, VPN, IPS 등의 보안 기능을 하나로 통합하여 제공한다.
② 각각 다른 보안 정책을 수립하여 적용한다.
③ 보안 기능이 하나로 통합되어 구축시 비용이 절감된다.
④ 다양하고 복잡한 보안 위협에 대응하고 편의성이 향상된다.
정답 체크
(2) 같은 보안 정책을 수립하여 적용한다.
오답 체크
(1) UTM의 Unified가 보안 기능이 하나로 통합되었음을 의미한다.
(3) 방화벽, VPN, IPS 등을 별도로 구축하는 것보다 비용이 절감된다.
(4) 방화벽, VPN, IPS 등의 기능을 이용하여 다양하고 복잡한 보안 위협에 대응할 수 있고 하나의 장비에 있으므로 편의성이 향상된다.

5. 다음 중 LAN(Local Area Network) 관련 IEEE 802 표준에 대한 설명으로 가장 옳은 것은?
① IEEE 802.2는 Token Bus에 관한 규정이다.
② IEEE 802.3은 CSMA/CD에 관한 규정이다.
③ IEEE 802.5는 LLC 서브계층에 관한 규정이다.
④ IEEE 802.6은 Token Ring에 관한 규정이다.
정답 체크
(2) Ethernet에 관한 규정이다.
오답 체크
(1) Token Bus는 802.4이다.
(3) 802.3은 LLC 서브계층에 관한 규정이다.
(4) Token Ring은 802.5이다.

6. 다음 중 TCP Well-Known Port 번호와 서비스의 연결이 잘못된 것은?
① TCP 21 - FTP
② TCP 22 - SSH
③ TCP 25 - SNMP
④ TCP 80 - HTTP
정답 체크
(3) SNMP는 UDP 161, 162이고, TCP 25는 SMTP이다.
오답 체크
(1), (2), (4) 주요 포트와 서비스는 다음과 같다.

포트 번호	서비스	설명
20	FTP	• File Transfer Protocol (Data) • FTP 연결 시 실제로 데이터를 전송한다.
21	FTP	• File Transfer Protocol (Control) • FTP 연결 시 인증과 제어를 한다.
23, 22	Telnet, SSH	• 텔넷 서비스로, 원격지 서버의 실행창을 얻어낸다.
25	SMTP	• Simple Message Transfer Protocol • 메일을 보낼 때 사용한다.
53	DNS/UDP	• Domain Name Service • 이름을 해석하는 데 사용한다.
69	TFTP/UDP	• Trivial File Transfer Protocol • 인증이 존재하지 않는 단순한 파일 전송에 사용한다.
80	HTTP	• Hyper Text Transfer Protocol • 웹서비스를 제공한다.
110	POP3	• Post Office Protocol • 메일 서버로 전송된 메일을 읽을 때 사용한다.
111	RPC	• Sun의 Remote Procedure Call • 원격에서 서버의 프로세스를 실행할 수 있게 한다.
138	NetBIOS	• Network Basic Input Output Service • 윈도우에서 파일을 공유할 수 있게 한다.
143	IMAP	• Internet Message Access Protocol • POP3와 기본적으로 같으나, 메일이 확인된 후에도 서버에 남는다는 것이 다르다.
161, 162	SNMP/UDP	• Simple Network Management Protocol • 네트워크 관리와 모니터링을 위해 사용한다.

7. 다음 중 IPv6의 주소 유형으로 옳지 않는 것은?
① Unicast
② Anycast
③ Broadcast
④ Multicast
정답 체크
(3) 멀티캐스트로 브로드캐스트를 대체한다.
오답 체크
(1) 유니캐스트 주소는 유니캐스트 주소 종류의 범위 내에서 단일 인터페이스를 식별한다. 유니캐스트 주소로 지정된 패킷은 적절한 유니캐스트 라우팅 토폴로지를 통해 단일 인터페이스로 배달된다.
(2) 애니캐스트 주소는 여러 인터페이스를 식별한다. 애니캐스트 주소로 지정된 패킷은 적절한 멀티캐스트 라우팅 토폴로지를 통해 주소로 식별되는 가장 가까운 인터페이스인 단일 인터페이스로 배달된다.

(4) 멀티캐스트 주소는 여러 인터페이스를 식별한다. 멀티캐스트 주소로 지정된 패킷은 적절한 멀티캐스트 라우팅 토폴로지를 통해 주소로 식별되는 모든 인터페이스에 배달된다.

8. 다음 중 네트워크로 연결된 단말을 확인하는 것으로 무결성 검사, IP 주소와 MAC 주소로 접근제어를 하는 보안솔루션으로 가장 올바른 것은?
① IPS(Intrusion Prevention System)
② NAT(Network Address Translation)
③ NAC(Network Access Control)
④ DRM(Digital Rights Management)
정답 체크
(3) 사용자 기기가 기업 내부 네트워크 접근 전 보안 정책을 준수했는지 여부를 검사하여 비정상 접근 여부에 따라 네트워크 접속을 통제하는 기술이다.
오답 체크
(1) 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.
(2) 대부분의 가정에서 설치된 유무선 공유기나 방화벽에서 동작한다. 유무선 공유기 내부인 가정에서는 사설 IP를 사용하고 해당 패킷이 외부로 나갈 때는 공유기를 통해 NAT 과정을 거쳐 공인 IP로 변환되어 나간다. 외부에서 패킷이 들어올 때는 공인 IP가 NAT에 의해 사설 IP로 바뀐다.
(4) 콘텐츠 제공자의 권리와 이익을 안전하게 보호하며 불법복제를 막고 사용료 부과와 결제대행 등 콘텐츠의 생성에서 유통·관리까지를 일괄적으로 지원하는 기술이다.

9. netstat -s 명령으로 프로토콜별 통계정보를 확인할 수 있다. 다음 중 이에 해당되지 않는 프로토콜은 무엇인가?
① MAC ② ICMP ③ TCP ④ UDP
정답 체크
(1) MAC 정보는 확인할 수 없다.
오답 체크
(2), (3), (4) IP, ICMP, TCP, UDP 통계 정보를 확인할 수 있다.

10. 다음 중 허니팟(Honeypot)에 대한 설명으로 가장 옳지 않은 것은?
① 컴퓨터 시스템에 침입한 스팸, 바이러스, 크래커를 탐지하기 위하여 의도적으로 설치한 시스템이다.
② 실제 공격을 당한 것처럼 보이도록 만든 함정이다.
③ 공격자가 허니팟으로 접근할 수 없도록 차단해야 한다.
④ 침입자가 오래도록 머물게 해야 한다.
정답 체크
(3) 공격자가 허니팟에 접근할 수 있도록 유인해야 한다.
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.
(2) 실제 공격을 당하지 않으면 공격자가 의심한다.
(4) 오래 머물러야 공격 패턴을 파악할 수 있다.

11. 다음 중 지능형 지속 공격(Advanced Persistent Threat, APT)에 대한 설명 중 가장 옳지 않은 것은?
① 사회 공학적 방법을 사용한다.
② 공격 대상이 명확하다.
③ 불분명한 목적과 동기를 가진 해커 집단이 주로 사용한다.
④ 가능한 방법을 총동원한다.
정답 체크
(3) 분명한 목적과 동기를 가진다.
오답 체크
(1) 사장님에 보낸 메일로 위장한다.
(2) 특정 공격 대상을 지정한다.
(4) 사회공학과 제로데이 공격 등을 감행한다.

12. 다음 중 공공기관의 보안성 강화를 위한 망분리 기술에 대한 설명으로 가장 옳은 것은?
① 망분리 기술로 USB와 같은 저장매체를 통한 악성코드 침입이 불가능하다.
② 물리적 망분리 기법에는 SBC 및 CBC 기반의 망분리 기법이 존재한다.
③ 애플리케이션 가상화 및 데스크톱 가상화를 통해 물리적 망분리 실현이 가능하다.
④ 논리적 망분리는 VDI(Virtual Desktop Infrastructure)와 OS 커널 분리로 분류 될 수 있다.
정답 체크
(4) VDI는 SBC이고, OS 커널 분리는 CBC이다.
오답 체크
(1) 저장매체를 통한 악성코드 침입이 가능하다.
(2) SBC와 CBC는 논리적 망분리 기법이다.
(3) 애플리케이션 가상화와 데스크톱 가상화는 논리적 망분리 기법이다.

13. 다음 중 DMZ(dimilitarized zone)에 대한 설명으로 가장 옳은 것은?
① 외부 네트워크에서는 DMZ에 접근할 수 없다.
② DMZ내에는 외부 인터넷에 서비스를 제공하기 위해 매우 높은 보안 수준을 요구하므로 주로 내부 접속용 데이터베이스 서버가 위치하고 있다.
③ 내부 사용자가 DMZ에 접속하기 위해서는 외부 방화벽을 거쳐야 한다.
④ DMZ는 보안 조치가 취해진 네트워크 영역으로 내부 방화벽과 외부 방화벽 사이에 위치할 수 있다.
정답 체크
(4) 방화벽 유형 중 스크린드 서브넷 게이트웨이가 이에 해당한다.
오답 체크
(1) 외부 네트워크에서 DMZ에 접근할 수 있다.

(2) 내주 접속용 데이터베이스 서버는 내부 네트워크에 설치하고, DMZ에는 외부에 공개해도 되는 웹서버, FTP 서버, SMTP 서버 등이 위치한다.
(3) 내부 방화벽을 거쳐야 한다.

14. 다음에서 설명하고 있는 공격은?

이 공격은 할당된 메모리 경계에 대한 검사를 하지 않은 프로그램의 취약점을 이용해서 공격자가 원하는 데이터를 덮어 쓰는 방식이다. 만약 실행 코드가 덮어 써진다면 공격자가 원하는 방향으로 프로그램이 동작하게 할 수 있다.

① Buffer Overflow 공격
② SQL Injection 공격
③ IP Spoofing 공격
④ Format String 공격
정답 체크
(1) 스택에는 복귀 주소(return address)가 저장되는데, 오버플로우가 발생하면 복귀 주소가 공격자가 원하는 주소로 바뀌어 공격자가 원하는 코드가 실행된다. 힙 버퍼 오버플로우 공격도 가능하다.
오답 체크
(2) 웹 주소창에 SQL 구문에 사용되는 문자 기호의 입력을 적절히 필터링하지 않아, 조작된 SQL 구문을 통해 DB에 무단 접근하여 자료를 유출/변조할 수 있는 취약점이다. 예를 들어 패스워드에 '1' or '1'='1'를 입력하면 or의 첫 번째 문장은 패스워드와 '1'을 비교해서 false가 되고 두 번째 문장은 true가 되기 때문에 전체적인 문장은 true(or는 두 문장 중 하나라도 true면 true가 됨)가 되어 패스워드 없이 로그인에 성공하게 된다.
(3) 트러스트(Trust)로 접속하고 있는 클라이언트에 DoS 공격을 수행해 클라이언트가 사용하는 IP가 네트워크에 출현하지 못하도록 한 뒤, 공격자 자신이 해당 IP로 설정을 변경한 후 서버에 접속하는 형태로 이루어진다.
(4) printf() 사용된 %s와 같은 문자열을 가리켜 포맷 스트링이라 한다. 포맷 스트링을 조작하면 (%n을 사용) 임의의 메모리 주소의 쓰기 혹은 복귀 주소를 변경할 수 있다.

15. 다음은 네트워크 서비스 거부 공격으로 인한 접속 마비에 대한 현상 및 대응요령을 설명한 것이다. 다음 중 가장 옳지 않은 것은?
① 리눅스 시스템의 경우 iptables를 이용한 패킷 필터링을 설정한다.
② 이상 트래픽에 의한 네트워크 속도 저하시 서비스 거부 공격을 의심하고, 트래픽을 분석한다.
③ 서비스 거부 공격시 라우터의 패킷 필터링 기능을 설정하여 대응한다.
④ 외부에서 들어오는 패킷의 발신자를 확인하여 공격자에게 역공격을 감행한다.
정답 체크
(4) 접속 마비가 발생하면 해결을 하기 위한 노력을 수행해야 한다(역공격을 할 시간이 없음).
오답 체크
(1) iptables를 이용하여 패킷의 허용과 거부를 결정한다.
(2) 속도가 저하되거나 이상 트래픽이 너무 많이 유입되면 서비스 거부 공격을 의심한다.
(3) 라우터의 패킷 필터링을 이용하여 의심 트래픽을 차단한다.

16. 다음 중 웹 보안을 제공하는 방법인 SSL의 설명으로 가장 옳지 않은 것은?

① TCP/IP 프로토콜의 네트워크 계층에서 보안기능을 수행하며 전송 계층이 있는 프로토콜의 안정성을 제공한다.
② 웹사이트 접속시 http:// 대신 https:// 를 사용하며, 서버와 클라이언트의 상호 인증 기능이 있다.
③ 넷스케이프에서 개발된 프로토콜로써 네트워크 통신 및 인터넷 사용자에게 안전한 정보를 교환하기 위한 보안 프로토콜이다.
④ 기밀성 제공을 위한 비밀키는 핸드쉐이크 프로토콜에 의해 생성된다.
정답 체크
(1) 네트워크 계층이 아닌 전송 계층에서 보안기능을 수행한다.
오답 체크
(2) 상호 인증을 위해 인증서를 사용한다.
(3) 초기의 GUI 웹 브라우저를 개발한 넷스케이프에서 개발하였다(지금은 없음).
(4) 핸드쉐이크 프로토콜은 공유키를 생성하고 인증서를 교환한다.

17. 다음 중 ㉠~㉢에 들어갈 용어를 바르게 연결한 것은?

· (㉠) 기법은 정상적인 활동 데이터베이스와 비교하여 침입을 구분한다. · (㉡) 기법은 공격패턴, 시그니처 데이터베이스와 비교하여 침입을 구분한다. · (㉢) IDS(Intrusion Detection System)는 네트워크 상의 모든 패킷을 캡처한 후 이를 분석하여 침입을 탐지하는 시스템이다. ※ 이상탐지 : Anomaly Detection, 오용탐지 : Misuse Detection

	㉠	㉡	㉢
①	이상탐지	오용탐지	네트워크 기반
②	이상탐지	오용탐지	호스트 기반
③	오용탐지	이상탐지	네트워크 기반
④	오용탐지	이상탐지	호스트 기반

정답 체크

오답 체크
(1) 이상탐지 : 알려지지 않은 공격 기법에 대비하여, 각종 비정상적인 침입 행동을 통계(Statistics) 기반으로 판단한다(예 너무 많은 syn 패킷이 온다면?).
오용탐지 : 과거의 부정행위 패턴을 기반으로 현재 알려진 패턴과 일치하는지 검사하여 부정행위를 탐지하는 것으로, 시그니처(Signature) 기반 탐지 혹은 지식(Knowledge) 기반 탐지로 부른다.
네트워크 기반 : IDS의 위치가 어디냐에 따라서 기능도 달라지게 되고 탐지할 수 있는 영역 또한 변할 수 있다(in-line).
오답 체크
(2), (4) 호스트 기반 : OS의 감사 자료(Audit Trail)나 시스템/응용 프로그램의 로그(Log)를 이용하여 공격을 판단한다(개별 호스트에 설치).
(3) 오용탐지와 이상탐지의 순서가 바뀌었다.

18. 컴퓨터의 네트워크 연결 상태를 점검하기 위해 netstat 명령을 사용하였다. 다음 설명 중 가장 옳지 않은 것은?

① LISTENING : 연결을 위해 접속을 대기하고 있는 상태
② CLOSE_WAIT : 연결 종료 메시지를 수신하고 그에 대한 확인메시지를 보낸 상태
③ ESTABLISHED : 완전히 종료된 상태
④ TIME_WAIT : 연결이 종료되었거나 다음 연결을 위해 대기하고 있는 상태
정답 체크
(3) 연결을 맺고 있는 상태이다.
오답 체크
(1) 연결 설정 과정에서 사용한다.
(2) 연결 해제 과정에서 사용한다.
(4) 연결은 종료되었으나 원격의 수신 보장을 위해 기다리고 있는 상태이다.

19. 다음 중 ESM(Enterprise Security Management) 기능으로 가장 옳지 않은 것은?
① 트래픽 조절 : 네트워크상의 트래픽 조절을 통한 연구생산성과 안정적인 성능을 지원 및 중요 트래픽의 대역폭 우선순위를 조절하여 안정적 이고 신뢰성 있는 통신을 제공
② 통합관리 : 다양한 시스템에서 발생되는 이벤트를 로그화하여 관리자가 필요로 하는 모든 정보(Error, Warning, Notice, Account)를 손쉽게 검색
③ 종합관제 : 통합 관리 기능을 수행하기 위한 인터페이스를 제공하여, 다양한 보안시스템(방화벽, IDS, Scanner)에서 보내온 데이터에 의한 공격 유형, 공격자 정보, 발생 일시, 적용 필터 등을 실시간 모니터링하여 종합적으로 관리
④ 운영관리 : 관리자 관리, 권한별 접근 관리, 실시간 연결 데이터 관리 등을 통해, 관리자가 시스템을 보다 더 체계적으로 운영할 수 있도록 지원
정답 체크
(1) 부하 분산기(L4 스위치) 또는 어플리케이션 스위치(L7 스위치) 등의 장비에서 제공하는 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.

20. 다음 중 무선랜의 보안을 강화하기 위한 대책으로 가장 안전하지 않은 것은?
① 무선랜 AP(Access Point) 접속시 데이터 암호화와 사용자 인증 기능을 제공하도록 한다.
② 무선랜 AP에 MAC(Media Access Control) 주소를 필터링하여 등록된 MAC 주소만 허용 하는 정책을 설정한다.
③ 무선랜 AP에 보안을 위해 무지향성 안테나를 사용한다.
④ 무선랜 SSID(Service Set ID)를 숨김으로 설정하여 폐쇄시스템을 운영하면 SSID를 모르는 사용자의 접속시도가 현저하게 줄어든다.
정답 체크
(3) 무지향성 안테나를 사용하면 데이터가 사방팔방으로 전송되므로 도청에 당할 확률이 높다. 보안을 위해 지향성 안테나를 사용한다.
오답 체크
(1) 데이터를 암호화하고, ID/PW를 사용한다.

(2) MAC filtering 기능인데, MAC 주소를 공격자가 변경할 가능성이 존재한다.
(4) SSID를 알고 있는 사람만 접속할 수 있다(직접 타이핑을 하고 연결을 해야 함).