2022-군무원-7급-네트워크보안-해설-곽후근

1. 다음 중 메일서비스 공격 유형에 대한 설명으로 가장 옳지 않은 것은?
① Active Contents Attack은 메일 열람 시 HTML 기능이 있는 이메일 클라이언트나 웹 브라우저를 사용하는 이용자를 대상으로 하는 공격기법이다.
② Trojan Horse Attack은 일반 사용자가 Trojan 프로그램을 실행시켜 해당 시스템에 접근할 수 있는 백도어를 만들게 하거나 시스템에 피해를 주게 한다.
③ SendMail 버퍼오버플로 취약점 공격은 FTP 서버가 데이터를 전송할 때 목적지가 어디인지 검사하지 않는 설계상의 문제점을 이용한 공격이다.
④ Buffer Overflow Attack은 공격자가 조작된 외부입력을 삽입하여 피해자의 컴퓨터에서 임의의 명령을 실행하거나 트로이 목마와 같은 악성 프로그램을 심을 수 있도록 한다.

정답 체크
(3) FTP 바운스 공격이다.
오답 체크
(1) active contents는 클라이언트에서 동작하는 문서와 웹사이트에 숨겨진 코드를 의미한다.
(2) 사용자가 의도하지 않은 코드를 정상적인 프로그램에 삽입한 형태이다.
(4) 스택에는 복귀 주소(return address)가 저장되는데, 오버플로우가 발생하면 복귀 주소가 공격자가 원하는 주소로 바뀌어 공격자가 원하는 코드가 실행된다. 힙에 대한 공격도 가능하다.

2. 침입방지시스템(Intrusion Prevention System)에 대한 설명으로 가장 옳지 않은 것은?
① 네트워크 기반 IPS(NIPS)는 네트워크의 물리적 또는 논리적 경계지점에 인라인(in-line) 방식으로 설치되어 네트워크 접속 및 트래픽 분석을 통해 공격시도와 유해트래픽 차단 기능을 수행한다.
② 호스트 기반 IPS(HIPS)는 대규모 네트워크 환경에서 운영 및 관리 편의성이 떨어진다.
③ switch 기반 IPS는 대용량 트래픽 환경에서 제한된 성능을 제공한다.
④ firewall 기반 IPS는 패킷 기반 탐지 및 방어 기능을 제공한다.

정답 체크
(3) 성능을 제한하지 않는다.
오답 체크
(1) NIPS는 네트워크 중간에 설치한다.
(2) HIPS는 호스트에 설치한다.
(4) 방화벽을 기반으로 IPS를 구성한다.

3. 다음에서 설명하는 라우터 필터링(Router Filtering)은?

standard 또는 extended access-list를 활용하여 내부 네트워크로 유입되는 패킷의 소스 IP나 목적지 포트 등을 체크하여 허용하거나 거부하도록 필터링하는 것 • Router#configure terminal • Router(config)# access-list 102 deny

IP 27.0.0.1.0.255.255.255 any

① ingress 필터링 설정 ② egress 필터링 설정
③ null routing을 활용한 필터링 ④ Unicast RPF를 이용한 필터링

정답 체크
(1) 내부 네트워크로 유입되는 패킷을 필터링한다.
오답 체크
(2) 외부 네트워크로 나가는 패킷을 필터링한다.
(3) blackhole 필터링을 의미한다. 특정한 ip 대역에 대해서 Null 이라는 가상의 쓰레기 인터페이스로 보내도록 함으로써 패킷의 통신이 되지 않도록 하도록 하는 필터링한다.
(4) 인터페이스를 통해 들어오는 패킷의 소스 ip 에 대해 라우팅 테이블을 확인하여 들어온 인터페이스로 다시 나가는지 확인한다(악의적인 트래픽 공격을 막기 위해 사용).

4. 다음에서 설명하는 One-Time Password의 생성 및 인증방식은?

유닉스 계열 운영체제 인증에 사용되고 있으며 생성알고리즘은 다음과 같다. • Client에서 정한 임의의 비밀키를 Server로 전송한다. • Client로부터 받은 비밀키를 첫 값으로 사용하여 해시 체인 방식으로 이전 결과 값에 대한 해시값을 구하는 작업을 n번 반복한다. • 생성된 n개의 OTP를 Server에 저장한다.

① S/KEY 방식 ② 시간 동기화 방식
③ 챌린지/응답 방식 ④ 이벤트 동기화 방식

정답 체크
(1) 클라이언트에서 정한 임의의 비밀키를 서버로 전송한다. 클라이언트로부터 받은 비밀키를 첫 값으로 사용하여, 해시 체인 방식으로, 이전 결과 값에 대한 해시 값을 구하는 작업을 n번 반복한다. 그렇게 생성된 n개의 OTP를 서버에 저장한다. 클라이언트에서 정한 OTP에 해시 함수를 n-i번 중첩 적용하여 서버로 전송한다. 서버에서는 클라이언트로부터 받은 값에 해시 함수를 한 번 적용하여, 그 결과가 서버에 저장된 n-i+1번째 OTP와 일치하는지 검사한다. 일치하면 인증에 성공한 것으로, 카운트를 1 증가시킨다.
오답 체크
(2) 클라이언트는 현재 시각을 입력값으로 OTP를 생성해 서버로 전송하고, 서버 역시 같은 방식으로 OTP를 생성하여 클라이언트가 전송한 값의 유효성을 검사한다. 하지만 클라이언트와 서버의 시간 동기화가 정확하지 않으면 인증에 실패하게 된다는 단점이 있으며, 이를 보완하기 위해 일반적으로 1~2 분 정도를 OTP 생성 간격으로 둔다.
(3) 서버에서 난수 생성 등을 통해 임의의 수를 생성하고 클라이언트에 그 값을 전송하면, 클라이언트가 그 값으로 OTP를 생성해 응답한 값으로 인증하는 방식이다.
(4) 서버와 클라이언트가 카운트 값을 동일하게 증가시켜 가며, 해당 카운트 값을 입력값으로 OTP를 생성해 인증하는 방식이다.

5. 다음에서 설명하는 방화벽(Firewall)의 가장 적절한 구축형태는?

- 필터링 속도가 빠르고, 비용이 적게 든다.
- 네트워크 계층에서 동작하므로 클라이언트와 서버에 변화가 없다.
- 네트워크 계층과 트랜스포트 계층에 입각한 트래픽만을 방어할 수 있다.
- 패킷 필터링 규칙을 구성하여 검증하기 어렵다.
- 패킷 내의 데이터에 대한 공격을 차단하지 못한다.

① Application Proxy ② Dual Homed Gateway
③ Screening Router ④ Single Homed Gateway

정답 체크
(3) IP와 Port 정보를 이용하여 필터링한다.
오답 체크
(1) 7계층에서 필터링한다.
(2) 2개의 NIC을 가진 베스천 호스트이다(감사, 인증 등을 수행).
(4) 1개의 NIC을 가진 베스천 호스트이다(감사, 인증 등을 수행).

6. 다음 중 IPSec에 대한 설명으로 가장 옳지 않은 것은?
① 응용, 전송, 네트워크 계층에서 동작하는 다양한 서비스에 보안을 제공한다.
② 전송 모드(transport mode), 터널 모드(tunnel mode) 또는 두 모드의 조합 형태로 운용될 수 있다.
③ AH 프로토콜은 기밀성을 지원하는 프로토콜이다.
④ ESP 프로토콜은 암호화를 지원하는 인증 및 암호화 프로토콜이다.

정답 체크
(3) AH는 인증, 무결성, 재전송 방지를 지원한다.
오답 체크
(1) 전송 모드는 전송, 응용을 보호하고, 터널 모드는 네트워크, 전송, 응용을 보호한다.
(2) 전송 모드는 기존 패킷을 보호하고, 터널 모드는 새로운 패킷을 보호한다.
(4) ESP는 인증, 무결성, 기밀성, 재전송 방지를 지원한다.

7. 다음 중 WPA(Wi-fi Protected Access)에 대한 설명으로 가장 옳지 않은 것은?
① 802.11i 보안 표준의 일부분으로 WEP(Wired Equivalent Privacy)방식 보안의 문제점을 해결하기 위해 만들어졌다.
② WPA-1은 CCMP(CCM mode Protocol) 암호화 방식을 사용하는 것으로 정의되어 있다.
③ WPA-개인은 무선랜 인증방식으로, PSK(Pre-Shared Key)모드를 사용하는 경우이다.
④ WPA-엔터프라이즈는 무선랜 인증방식으로 RADIUS(Remote Authentication Dial-In User Service)인증 서버를 사용하는 경우이다.

정답 체크
(2) TKIP를 사용한다.
오답 체크
(1) WEP는 키 길이 작고 암호화키가 고정되었다는 문제점을 가진다.

(3) 10,000개의 패킷마다 키를 교체한다.
(4) 802.1x 프로토콜을 사용한다.

8. 다음 중 웹 어플리케이션 DoS 공격에 대한 설명으로 가장 옳지 않은 것은?
① HTTP GET Flooding 공격은 TCP 3-way 핸드셰이킹 과정을 통해 공격 대상 시스템에 정상적으로 접속한 뒤 HTTP의 GET Method로 특정 페이지를 무한 실행한다.
② HTTP CC 공격은 HTTP 1.1 버전의 Cache-Control 헤더 옵션에서 자주 변경되는 데이터에 HTTP 요청 및 응답을 새롭게 요구하기 위한 캐시 기능을 사용하지 않게 하여 웹서비스의 부하를 증가시킨다.
③ 동적 HTTP Request Flooding 공격은 요청 페이지를 변경하여 웹 페이지를 지속적으로 요청한다.
④ Slow HTTP Header DoS 공격은 HTTP POST 메시지에 헤더의 Content-Length 필드의 임의의 큰 값을 설정하여 전송한다. 공격자는 소량의 데이터를 느린 속도로 전송하여 웹 서버와의 커넥션을 장시간 동안 유지하게 만들어 서버의 자원을 잠식한다.

정답 체크
(4) Slow HTTP Post DoS 공격이다.
오답 체크
(1) 서버에 TCP 3-웨이 핸드셰이킹 과정을 통해 정상적인 접속을 한 뒤, 특정한 페이지를 HTTP의 GET Method를 통해 무한대로 실행하는 것이다.
(2) HTTP 1.1 버전의 CC(Cache-Control) 헤더 옵션은 자주 변경되는 데이터에 대해 새롭게 HTTP 요청 및 응답을 요구하기 위하여 캐시(Cache) 기능을 사용하지 않게 할 수 있다. 서비스 거부 공격 기법에 이를 응용하기 위해 'Cache-Control: no-store, mustrevalidate' 옵션을 사용하면 웹 서버는 캐시를 사용하지 않고 응답해야 하므로 웹 서비스의 부하가 증가하게 된다.
(3) 방화벽을 통해 특징적인 HTTP 요청 패턴 차단 기법을 우회하기 위해 지속적으로 요청 페이지를 변경하여 웹 페이지를 요청하는 기법이다.

9. 다음 중 가상사설망(Virtual Private Network)에 대한 설명으로 가장 옳지 않은 것은?
① SSL(Secure Sockets Layer) VPN의 적용계층은 OSI 5계층이며, 어플리케이션 차원의 정교한 접근제어가 미흡하지만, Client Server 모드 인증이 가능하다.
② Point to Point Tunneling Protocol은 이동 중인 사용자가 기업의 Home Server에 dial-up 접속하고자 할 때 사용하는 방식이다.
③ Layer2 Tunneling Protocol은 remote dial-up 사용자가 공중망을 통해 터널링하여 사설 망에 연결될 수 있는 기능을 제공한다.
④ IPSec(IP Security) VPN의 적용계층은 OSI 3계층이며, 어플리케이션 차원의 정교한 접근제어가 미흡하지만, 단대단 보안이 가능하다.

정답 체크
(1) OSI 4계층이다.
오답 체크
(2) MS에서 만들었다.

(3) PPTP와 L2F(CISCO에서 개발)의 장점을 결합하였다.
(4) 3계층인 IP를 보호하기 위해 만들어졌으며, E2E 보안이 가능하다.

10. 다음 중 SNMP(Simple Network Management Protocol)에 대한 설명으로 가장 옳지 않은 것은?
① 관리 작업을 수행하기 위해 SMI(Structure of Management Information)와 MIB(Management Information Base)를 사용한다.
② 네트워크 관리자가 원격으로 네트워크 장비를 모니터링하고 환경 설정을 수행하고자 할 때, 네트워크 구성 요소에 의해 유지되는 변수값을 조회하거나 변경할 수 있도록 고안된 프로토콜이다.
③ MIB는 객체에 이름을 붙이고 객체 유형을 정의하며, 객체와 값을 부호화하는 방법을 나타내기 위한 일반적 규칙을 정의한다.
④ SMI는 공통된 정보 표현 방식을 규정해서 각종 장비 간에 통신이 이루어질 수 있도록 한다.

정답 체크
(3) SMI에 대한 설명이다.
오답 체크
(1) SMI, MIB, OID 등으로 구성된다.
(2) 네트워크 장비를 설정 및 모니터링할 때 사용한다.
(4) SMI는 표준에 적합한 MIB를 생성하고 관리하는 기준이다(관리 정보 구조).

11. 다음 중 세션 하이재킹(Session Hijacking) 방어 대책에 대한 설명으로 가장 옳지 않은 것은?
① 전송되는 데이터를 암호화하는 것이 최선의 방어이다.
② ACK 패킷의 비율을 증가시킨다.
③ 처음 로그인 후 일정 시간 내에 재 인증을 지속적으로 실시한다.
④ 취약점을 수정하는 패치 작업을 한다.

정답 체크
(2) 세션 하이재킹이 발생하면 ACK storm(ACK 비율이 증가)이 발생한다.
오답 체크
(1) 암호화를 하면 패킷을 도청할 수 없다.
(3) 하이재킹을 했더라도 재 인증을 하면 공격자를 파악할 수 있다.
(4) 서버가 가지는 취약점을 해결하기 위해 주기적으로 패치를 해야 한다.

12. 다음 중 이 더넷 물리 주소(MAC)가 될 수 있는 것은?
① 00:0C:29:97:13:8C:48:A0
② 00:0C:29:97:13:8C:48
③ 00:0C:29:97:13:8C
④ 00:0C:29:97:13

정답 체크
(3) 48비트(=4x12)이다.

13. 다음 중 IDS(Intrusion Detection System)에 대한 설명으로 가장 옳지 않은 것은?
① HIDS(Host-based IDS)는 호스트 시스템으로부터 생성되고 수집된 감사 자료를 침입 탐지에 사용하며, 시스템 이벤트 감시를 통해 정확한 침입 탐지가 가능하다.
② IDS의 성능을 향상시키려면 합법적 사용자를 침입자로 판단하는 부정오류(false negative)와 침입자를 합법적 사용자로 판단하는 긍정오류(false positive)를 최적화해야 한다.
③ HIDS와 NIDS는 각각 장단점이 있어서 보안을 중요하게 생각하는 곳 에서는 HIDS와 NIDS를 상호 보완적으로 사용한다.
④ NIDS(Network-based IDS)는 네트워크에서 패킷 헤더, 데이터 및 트래픽 양, 응용프로그램 로그 등을 분석하여 침입 여부를 판단한다.

정답 체크
(2) 부정오류와 긍정오류가 반대로 설명되었다.
오답 체크
(1) HIDS는 호스트(일반 PC)에 설치된다.
(3) 비용과 관리 포인트는 늘어나지만 보안은 더 안전하다.
(4) NIDS는 네트워크 중간에 설치된다.

14. 다음 중 UTM(Unified Threat Management)과 ESM(Enterprise Security Management)에 대한 설명으로 가장 옳지 않은 것은?
① UTM은 단일장비로 다양한 보안 기능을 하나의 장비로 통합하여 제공할 수 있다.
② UTM은 특정 보안 기능에 장애가 발생 시, 다른 보안 기능에 영향을 주지 않는다.
③ ESM은 기업과 기관의 보안 정책을 반영하고 다양한 보안 시스템을 관제, 운영, 관리함으로써 조직의 보안 목적을 효율적으로 실현하는 시스템이다.
④ ESM은 통합 보안 관제를 위해 구축된 다양한 보안 솔루션과 보안 장비에서 발생하는 로그와 보안 이벤트를 취합하고 이들 간에 상호 연관 분석을 함으로써 실시간 보안 위협을 파악하고 대응한다.

정답 체크
(2) 다양한 보안 기능이 서로 연계되어 있으므로, 특정 보안 기능에 장애 발생 시 다른 보안 기능에 영향을 준다.
오답 체크
(1) 방화벽, 가상 전용 네트워크, 침입 차단 시스템, 웹 컨텐츠 필터링, 안티스팸 소프트웨어 등을 포함하는 여러 개의 보안 도구를 이용한 관리 시스템이다.
(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.

15. 다음 중 Fragment Overlap Attack에 대한 설명으로 가장 옳지 않은 것은?
① 공격자는 공격용 IP 패킷을 위해 두 개의 패킷조각을 생성한다.
② 일반적으로 공격자들은 첫 번째 패킷조각의 포트번호가 있는 부분까지 덮어씌운다.
③ 공격을 구성하는 클라이언트 모듈은 서버 모듈을 제어하는 모듈로서, 서버에게 언제 어떤 공격을

누구에게 할 것인지를 지시한다.
④ 침입탐지 시스템(IDS)에서 첫 번째 패킷조작은 허용된 포트번호이므로 통과시키고, 두 번째 패킷 조각은 이전에 이미 허용된 패킷조각의 ID를 가진 패킷조각이므로 역시 통과시킨다.

정답 체크
(3) DDoS 공격을 의미한다.
오답 체크
(1) Fragment는 일반적으로 발생하고, 공격자를 이를 이용한다.
(2) 두 번째 fragment가 첫 번째 fragment를 덮어씌우도록 한다.
(4) IP header 중에 Identification이 동일한 패킷은 통과시킨다.

16. 다음 중 네트워크 기반 공격에 대한 설명으로 가장 옳지 않은 것은?
① SYN Flooding은 TCP의 3-way Handshake가 갖는 약점을 이용하는 공격이다.
② UDP Flooding은 UDP의 비 연결성 및 비 신뢰성 때문에 공격이 용이한 방법이다.
③ Land Attack은 패킷을 전송할 때 소스(source) IP 주소와 목적지(destination) 주소 값을 똑같이 만들어서 공격 대상에게 보내는 것이다.
④ Targa/New Tear/Nestea Attack은 서버의 포트를 반개방(half open) 상태로 만들어 제3의 사람들이 서버에 접근하지 못하게 한다.

정답 체크
(4) syn flooding에 대한 설명이다.
오답 체크
(1) 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.
(2) 대량의 UDP 패킷을 위조된 소스 주소와 함께 공격 대상 호스트의 임의의 포트로 전송한다. 호스트는 이러한 데이터그램과 연계된 애플리케이션을 점검하고 아무 것도 발견하지 못하곤 "도달할 수 없는 목적지(Destination Unreachable)" 패킷으로 응답한다. 공격자는 호스트가 압도당해 더 이상 합법적인 사용자에게 응답할 수 없을 때까지 더 많은 패킷을 보낸다.
(3) 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소를 똑같이 만들어서 공격 대상에게 보내는 공격이다.

17. 다음 중 응용 계층의 보안프로토콜에 대한 설명으로 가장 옳지 않은 것은?
① S/MIME(Security Services for Multipurpose Internet Mail Extension)는 인증서를 통해 암호화한 이메일 서비스를 제공한다.
② PGP(Pretty Good Privacy)는 암호알고리즘을 이용하여 기밀성, 인증, 무결성, 부인방지 등의 기능을 지원한다.
③ SSH(Secure Shell) VPN은 원격 단말기에서 접속하는 경우에 주로 이용되며 SSH를 이용한 파일전송 및 파일복사 프로토콜을 이용할 수 있다.
④ SSL(Secure Socket Layer)은 넷스케이프가 개발하였으며, 40bit와 128bit의 키를 가진 암호

화 통신을 할 수 있게 해준다.

정답 체크
(4) 전송 계층 보안이다.
오답 체크
(1), (2) 응용 프로그램 계층(application layer)으로 이메일 보안 프로토콜이다.
(3) 응용 프로그램 계층(application layer)이고, Telnet 혹은 FTP의 보안 버전이다.

18. 다음 중 스니핑 탐지 방법에 대한 설명으로 가장 옳지 않은 것은?
① 대부분의 스니퍼는 일반 TCP/IP 프로토콜로 동작하기 때문에 Ping을 보냈을 때 ICMP Echo Reply를 받으면 응답한 호스트가 스니핑을 한다는 의미이다.
② 가짜 계정과 패스워드를 네트워크에 뿌린 후 가짜 계정과 패스워드로 접속을 시도하는 공격자를 스니퍼로 탐지한다.
③ 원격에서 테스트 대상 네트워크로 Ping Sweep을 보내고 들어오는 Inverse-DNS lookup을 감시하여 스니퍼를 탐지한다.
④ IP 주소와 장치 이름의 매칭 값을 저장하고, 트래픽을 모니터링하여 매칭 값이 변한 패킷을 전송한 장치를 공격자로 탐지한다.

정답 체크
(4) IP 주소와 MAC을 저장한다.
오답 체크
(1) ARP에 의한 방법이다.
(2) Decoy에 의한 방법이다.
(3) Ping에 의한 방법이다.

19. 다음 중 네트워크 스캔 기법에 대한 설명으로 가장 옳지 않은 것은?
① NULL 스캔은 플래그 값을 설정하지 않고 보내는 방법으로 스캔한다.
② FIN 스캔은 포트가 열린 경우에는 응답하고, 닫힌 경우에는 응답하지 않는다.
③ XMAS 스캔은 ACK, RST, FIN, URG, SYN, PSH 플래그 모드를 설정하여 보내는 방법으로 스캔 한다.
④ 스텔스 스캔은 로그를 남기지 않는 것만이 아니라 공격 대상을 속이고 자신의 위치를 숨기는 스캔 모두를 통칭한다.

정답 체크
(2) 열린 경우에 응답하지 않고, 닫힌 경우에 RST로 응답한다.
오답 체크
(1) 열린 경우에 응답하지 않고, 닫힌 경우에 RST로 응답한다.
(3) 열린 경우에 응답하지 않고, 닫힌 경우에 RST로 응답한다.
(4) TCP half open, NULL, FIN, XMAS가 해당된다.

20. 다음 중 패킷의 흐름을 바꾸기 위한 공격으로 가장 적절 하지 않은 것은 ?

① SPAN 포트 및 태핑 ② ARP 스푸핑
③ ARP 리다이렉트 ④ ICMP 리다이렉트

정답 체크
(1) 스니핑을 위해 사용한다.
오답 체크
(2) 자신이 서버 또는 클라이언트라고 속인다.
(3) 자신이 라우터라고 속인다.
(4) 자신이 원하는 목적지 호스트를 가지고 있다고 속인다.

21. 다음 중 DNS(Domain Name System)기능과 DNS 보안 위협에 대한 설명으로 가장 옳지 않은 것은?
① DNSSEC(DNS Security Extensions)는 기존의 DNS를 대체하여 DNS 메시지에 대한 기밀성과 서비스 거부 공격에 대한 방지책을 제공한다.
② ARP 스푸핑 대응 방법이 DNS 스푸핑 공격에 대한 예방 방법이 된다.
③ DNS는 네트워크 주소인 IP 주소를 도메인 이름으로 상호 매칭 시킨다.
④ DNS 스푸핑 공격은 공격 대상 단말이 잘못된 IP 주소로 웹 접속을 하도록 유도한다.

정답 체크
(1) 서명을 통해 서명자 인증, 무결성, 부인방지 만을 제공한다.
오답 체크
(2) MAC을 고정하면 ARP 스푸핑을 막을 수 있다.
(3) 도메인 이름과 IP 주소 간 변환 서비스를 제공한다.
(4) 가짜 DNS 서버가 잘못된 IP 주소를 알려준다.

22. 다음 중 라우터에 정의한 ACL(Access Control List) 적용 규칙으로 가장 옳지 않은 것은?
① ACL은 먼저 입력한 순서로 수행된다.
② named ACL은 순서대로 입력되므로 중간에 삽입하거나 삭제할 수 없다.
③ numbered ACL은 순서대로 입력되므로 중간에 삽입하거나 삭제할 수 없다.
④ ACL의 마지막은 deny any가 생략되어 있다.

정답 체크
(2) 임의대로 입력되고 중간에 삽입하거나 삭제할 수 있다.
오답 체크
(1) 번호를 가지고 입력한 순서대로 수행된다(어떤 규칙을 앞에 두느냐가 아주 중요).
(3) 순서대로 입력된다.
(4) 조건에 안맞으면 해당 패킷은 폐기된다.

23. 다음 중 SNMP(Simple Network Management Protocol)에 대한 설명으로 가장 옳지 않은 것은?
① 누구나 SNMP의 MIB정보를 볼 수 있고, 대부분이 커뮤니티를 기본 설정인 public으로 사용한다.

② 패킷이 UDP로 전송되어 연결의 신뢰도가 낮다.
③ SNMP 버전 1은 데이터가 암호화되지 않은 평문으로 전송되어 스니핑이 가능하다.
④ SNMP 버전 2는 인증 기능을 추가해서 보안성을 향상시켰다.

정답 체크
(4) SNMP 버전 3에 대한 설명이다.
오답 체크
(1) 다른 사람의 접속을 막으려면 커뮤니티를 바꾸면 된다.
(2) 연결의 신뢰가 낮고 도청이 가능하다.
(3) 1988년 IAB에서 표준화 작업을 거친 후 SGMP(Simple Gateway Monitoring Protocol)를 발전시켜 만든 것이고, 보안 기능이 없어 해당 네트워크 장비의 모든 정보를 얻어낼 수 있다.

24. 다음 중 통합 보안 관리 시스템(ESM)에 대한 설명으로 가장 옳지 않은 것은?
① 통합 보안 관리 시스템은 공격을 사전에 탐지하는 목적으로 사용된다.
② 통합 보안 관리 시스템은 방화벽, 침입 차단/탐지 시스템, 가상 사설 망 등 다양한 종류의 보안 솔루션 로그 및 일반 시스템의 로그를 하나로 통합해 관리하는 솔루션이다.
③ 통합 보안 관리 시스템은 효과적인 침해 사고 대응을 위해 보안 정책의 일관성을 유지해야 한다.
④ 통합 보안 관리 시스템은 일반적으로 관리 콘솔, 매니저, 에이전트로 구성된다.

정답 체크
(1) IPS에 대한 설명이다.
오답 체크
(2) 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.
(3) 보안 정책이 일관적이지 않으면 효과적인 침해 사고 대응이 어렵다(신속한 대응 처리가 가능).
(4) 관리 콘솔(모니터링), 매니저(로그 분석), 에이전트(로그 수집)로 구성된다.

25. 다음 중 침입탐지시스템(Intrusion Detection System)의 오용탐지(Misuse Detection) 방법에 대한 설명으로 가장 옳지 않은 것은?
① 조건부 확률(conditional probability)은 이벤트 패턴 중에서 특정 이벤트가 발생할 확률로 공식에 의하여 계산한다.
② 키 모니터링(keystroke monitoring)은 공격패턴을 나타내는 특정키 입력 순서를 패턴화 한다.
③ 상태전이 분석(state transition analysis)은 공격패턴을 특정시스템의 상태전이의 순서로 표현한다.
④ 패턴매칭(pattern matching)은 알려지지 않은 보안 취약점에 근거한 공격만을 발견한다.

정답 체크
(4) 알려진 보안 취약점에 근거한 공격만을 발견한다.
오답 체크
(1) 특정 데이터가 침입일 확률을 공식에 의해 계산 후 탐지한다.

(2) 키 눌림을 모니터링한다.
(3) 공격 상황에 대한 시나리오를 작성해두고 각각의 상태에 따른 공격을 분석하는 것이다. 결과가 매우 직관적이지만 세밀한 시나리오를 만들기가 어렵고 추론 엔진이 포함되어 시스템에 부하를 준다.