네 트 워 크 보 안 (7 급)

(과목코드 : 142)

2022년 군무원 채용시험　　**응시번호 :**　　**성명 :**

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.

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.

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 127.0.0.1.0.255.255.255 any

① ingress 필터링 설정

② egress 필터링 설정

③ null routing을 활용한 필터링

④ Unicast RPF를 이용한 필터링

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

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

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.

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 만들어 졌다.
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.

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 특정페이지를 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.

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-up사용자가 공중망을 통해 터널링하여 사설망에 연결 될 수 있는 기능을 제공한다.
④ IPSec(IP Security) VPN의 적용계층은 OSI3계층이며, 어플리케이션 차원의 정교한 접근제어가 미흡하지만, 단대단 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 표현방식을 규정해서 각종 장비 간에 통신이 이루어질 수 있도록 한다.

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 재인증을 지속적으로 실시한다.
④ 취약점을 수정하는 패치 작업을 한다.

12. 다음 중 이더넷 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

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 곳에서는 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.

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 통합보안관제를 위해 구축된 다양한 보안 솔루션과 보안 장비에서 발생하는 로그와 보안 이벤트를 취합하고 이들 간에 상호 연관 분석을 함으로써 실시간 보안 위협을 파악하고 대응한다.

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 패킷조각은 이전에 이미 허용된 패킷조각의 ID를 가진 패킷조각이므로 역시 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 비연결성 및 비신뢰성 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.

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 파일 복사 프로토콜을 이용할 수 있다.

④ SSL(Secure Socket Layer)은 넷스케이프가 개발하였으며, 40bit와 128bit의 키를 가진 암호화 통신을 할 수 있게 해준다.

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.

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 스캔한다.

④ 스텔스 스캔은 로그를 남기지 않는 것만이 아니라 공격 대상을 속이고 자신의 위치를 숨기는 스캔 모두를 통칭한다.

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

① SPAN 포트 및 태핑

② ARP 스푸핑

③ ARP 리다이렉트

④ ICMP 리다이렉트

21. 다음 중 DNS(Domain Name System)기능과 DNS 보안위협에 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 매칭시킨다.
④ DNS 스푸핑 공격은 공격 대상 단말이 잘못된 IP 주소로 웹 접속을 하도록 유도한다.

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.

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.

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 사설망 등 다양한 종류의 보안 솔루션 로그 및 일반 시스템의 로그를 하나로 통합해 관리하는 솔루션이다.
③ 통합 보안 관리 시스템은 효과적인 침해사고 대응을 위해 보안 정책의 일관성을 유지해야 한다.
④ 통합 보안 관리 시스템은 일반적으로 관리 콘솔, 매니저, 에이전트로 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.