

네트워크 보안

문 1. 네트워크 관리자가 원격으로 네트워크 장비를 모니터링하고 환경 설정을 수행하고자 할 때, 네트워크 구성 요소에 의해 유지되는 변수값을 조회하거나 변경할 수 있도록 고안된 프로토콜은?

- ① FTP
- ② NFS
- ③ SNMP
- ④ SMTP

문 2. 근거리 통신망에서 공격대상의 MAC 주소를 공격자의 컴퓨터 MAC 주소로 변경하여 공격대상이 전송하는 모든 데이터를 가로챌 수 있는 공격 기법은?

- ① 스위치 재밍
- ② IP 스푸핑
- ③ DNS 스푸핑
- ④ ARP 스푸핑

문 3. 라우터 외부로 나가는 패킷의 소스 IP만을 검사하여 필터링하는 것으로, 라우터 내부의 네트워크에서 소스 IP를 위조하여 다른 네트워크를 공격하는 형태의 공격을 차단하는 필터링 기법은?

- ① ingress 필터링
- ② egress 필터링
- ③ black hole 필터링
- ④ null routing을 이용한 필터링

문 4. 전자금융거래상에서 사용되는 접속정보 및 거래정보, 단말기 정보 등을 종합적으로 분석하여 의심되는 거래를 탐지하고 이상 금융거래를 차단하는 시스템으로, 일반적인 보안 프로그램에서 방지하지 못하는 전자금융사기의 이상거래를 탐지하고 조치할 수 있는 기법은?

- ① STP
- ② ARIA
- ③ SARA
- ④ FDS

문 5. 사설 네트워크 용도로 사용되는 사설 IPv4 주소에 해당하는 것은?

- ① 10.10.20.300
- ② 168.10.40.11
- ③ 172.16.10.20
- ④ 192.10.20.30

문 6. URL(Uniform Resource Locator)이 웹페이지를 정의하는 데 사용하는 식별자가 아닌 것은?

- ① Protocol
- ② Sequence Number
- ③ Host
- ④ Path

문 7. OSI(Open Systems Interconnection) 참조 모델과 TCP/IP 프로토콜에 대한 설명으로 옳지 않은 것은?

- ① OSI 참조 모델은 국제 표준 기구인 ISO가 만든 모델이며, 서로 다른 컴퓨터 간의 기능을 여러 계층으로 구분하여 계층마다 표준화된 서비스와 프로토콜을 규정하였다.
- ② OSI 참조 모델은 Layer 1인 최상위의 응용 계층부터 Layer 7인 최하위의 물리 계층까지 7개 계층으로 구성된다.
- ③ 데이터 링크 계층은 물리 계층에서 발생할 수 있는 오류를 발견하는 역할을 한다.
- ④ 네트워크 계층에서는 출발지부터 목적지까지 여러 링크를 경유하여 패킷을 포워드 할 수 있으며, 이때 IP 주소와 같은 논리 주소가 이용된다.

문 8. 다음 중 HTTPS가 사용될 때 통신 간에 암호화되는 요소에 해당하는 것은?

- ① 요청되는 문서의 URL
- ② IP 헤더의 TTL 필드
- ③ TCP 헤더의 플래그 비트들
- ④ 탐색엔진

문 9. HTTP 메시지의 header 정보를 조작하여 서버가 header 정보를 완전히 수신할 때까지 연결을 유지하도록 하여 서버의 가용량을 소비시킴으로써 다른 사용자의 정상적인 서비스를 방해하는 공격은?

- ① Slowloris 공격
- ② HTTP CC 공격
- ③ HTTP GET Flooding 공격
- ④ Slow HTTP POST 공격

문 10. 다음 ㉠ ~ ㉤에 들어갈 용어를 바르게 연결한 것은?

가상 사설망이라 불리는 (㉠) 기법은 접근 제어를 위해 보안서비스와 터널링 기술이 요구된다. 터널링 프로토콜로 MS에서 개발한 (㉡) 기법과 시스코에서 개발한 (㉢) 기법이 있으며, 이 둘을 결합한 형태로 (㉣) 기법이 있다.

- | | | | | |
|---|------|------|------|------|
| | ㉠ | ㉡ | ㉢ | ㉣ |
| ① | VPN | PPTP | L2TP | L2F |
| ② | VPN | PPTP | L2F | L2TP |
| ③ | PPTP | VPN | L2TP | L2F |
| ④ | PPTP | VPN | L2F | L2TP |

문 11. 데이터링크의 효율성을 위해서 다수의 디바이스가 단일 링크를 공유하여 전송해 주는 기술은?

- ① 변조
- ② 부호화
- ③ 암호화
- ④ 다중화

문 12. 부인 봉쇄(non-repudiation) 기능을 제공하는 기법은?

- ① 디지털 서명
- ② 트래픽 패딩
- ③ 접근 제어
- ④ CRC

문 13. 공중 무선랜의 공격에 대한 대응 기법이 아닌 것은?

- ① 폐쇄 시스템 운영
- ② MAC 주소 인증
- ③ SSID 설정을 통한 접속 제한
- ④ WEP/WPA 키 크래킹

문 14. 방화벽 내에서 내부 사설 IP 주소를 가진 클라이언트가 외부로 접속하는 단계를 순서대로 바르게 나열한 것은?

- ㄱ. 원격지 서버가 방화벽이 보낸 패킷에 대한 응답 패킷을 보낸다.
- ㄴ. 클라이언트는 내부 IP 주소를 출발지 주소로, 접속하고자 하는 외부 IP 주소를 목적지 주소로 하는 패킷을 생성하여 방화벽으로 보낸다.
- ㄷ. 방화벽은 Normal NAT 규칙에 따라 패킷의 출발지 주소를 미리 설정되어 있는 방화벽 IP 주소로 바꾸어 원격지 서버에 전송한다.
- ㄹ. 방화벽은 Normal NAT 규칙에 따라 목적지 주소를 처음 접속을 시도한 클라이언트의 내부 IP 주소로 바꾼 후, 클라이언트로 전송한다.

- ① ㄴ → ㄷ → ㄱ → ㄹ
- ② ㄴ → ㄹ → ㄱ → ㄷ
- ③ ㄷ → ㄱ → ㄴ → ㄹ
- ④ ㄷ → ㄹ → ㄴ → ㄱ

문 15. 스니핑을 수행하는 스니퍼(sniffer)를 탐지하는 방법에 대한 설명으로 옳지 않은 것은?

- ① 로컬 네트워크에 존재하지 않는 주소로 위장하여 ping(ICMP Echo Request)을 보냈을 때, ICMP Echo Reply를 받으면 해당 호스트는 스니퍼임을 추측할 수 있다.
- ② FIN 패킷을 보냈을 때, RST 패킷을 받으면 해당 호스트는 스니퍼임을 추측할 수 있다.
- ③ 특정 호스트에서 promiscuous mode의 설정 여부를 확인하면 스니퍼임을 추측할 수 있다.
- ④ ARP 트래픽을 모니터링하는 ARP watch를 이용하여 스니퍼임을 추측할 수 있다.

문 16. IPSec에 대한 설명으로 옳지 않은 것은?

- ① IPSec을 침입차단시스템이나 라우터에서 구현할 경우 경계를 통과하는 모든 트래픽에 적용할 수 있는 강한 보안성을 제공하기 때문에 회사나 작업그룹 사이의 트래픽 보안을 위해 특별한 처리를 할 필요가 없다.
- ② IPSec은 전송계층(TCP와 UDP)의 아래에 있으며 응용 프로그램에는 투명하다. 침입차단시스템이나 라우터에서 IPSec이 작동되고 있을 때는 서버 시스템과 사용자 시스템의 소프트웨어를 바꿀 필요가 없다.
- ③ 만약 외부로부터의 모든 트래픽이 IP를 사용해야만 한다면 침입차단시스템에서의 IPSec은 우회하는 트래픽을 차단할 수 없으며, 개별적인 사용자가 보안이 필요하다면 IPSec은 그 사용자에게 보안을 제공할 수 없다.
- ④ IPSec은 중단 사용자에게 투명하게 할 수 있다. 따라서 번거롭게 사용자에게 보안 메커니즘을 훈련시키거나, 개별 기반으로 키를 발급하거나, 사용자가 근무를 그만두고 떠날 때 키를 취소할 필요가 없다.

문 17. 전송계층에 적용되는 SSL(또는 TLS) 보안 프로토콜에 대한 설명으로 옳은 것은?

- ① Authentication Header 프로토콜은 발신지 호스트를 인증하고 페이로드의 무결성을 보장하기 위하여 설계되었다.
- ② Alert 프로토콜은 암호화 또는 암호화/인증의 결합을 제공하기 위해 사용되는 캡슐화 헤드와 트레일러로 구성된다.
- ③ Change Cipher Spec 프로토콜은 연결에서 사용될 암호화 그룹을 갱신하는 프로토콜이다.
- ④ Handshake 프로토콜은 응용데이터가 전송된 후에 사용되며, 서버와 클라이언트 간의 상호인증, 그리고 암호와 MAC 알고리즘을 협상하지만, 보안 프로토콜로 송신되는 데이터를 보호하기 위한 암호화 키들은 협상하지 않는다.

문 18. TCP session hijacking 공격에 대한 설명으로 옳지 않은 것은?

- ① 이 공격 기법에 대한 대응 방안으로 데이터를 암호화하여 전송하는 방식을 사용한다.
- ② 이 공격은 클라이언트와 서버가 통신할 때 사용되는 TCP의 sequence number를 이용한 공격이다.
- ③ 이 공격을 성공적으로 수행하기 위해서는 ARP 스푸핑과 같은 추가적인 공격 기술이 필요하다.
- ④ 세션 성립은 일반적으로 인증 성립을 의미하며, 인증이 성립된 후에는 이 공격을 막을 수 있다.

문 19. 네트워크 공격 기법에 대한 설명으로 옳지 않은 것은?

- ① 서비스 거부 공격은 대상 시스템의 서비스를 중단시키기 위해 공격하는 기법이다.
- ② 중간자 공격(man-in-the middle attack)은 두 컴퓨터의 통신 중간에 위치하는 공격 기법이다.
- ③ DDoS 공격은 일반적으로 공격을 증폭시키는 중간자가 사용되는 공격 기법이다.
- ④ CSRF 공격은 메일 서버를 요청하지 않은 이메일로 공격하는 기법이다.

문 20. 203.230.15.0과 같은 IPv4의 C 클래스 네트워크를 30개의 서브넷으로 나누고, 각각의 서브넷에는 5개의 호스트를 연결하려고 한다. 30개의 서브넷 대부분에서 사용되는 서브넷 마스크는?

- ① 255.255.255.224
- ② 255.255.255.240
- ③ 255.255.255.248
- ④ 255.255.255.252