

네트워크보안

1. 네트워크 스위치는 기능에 따라 OSI 계층 모델에 따르는 수준이 다양하다. 다음 중 각 스위치의 최고 수준에서 제공할 수 있는 기능에 대한 설명으로 가장 옳지 않은 것은?
- ① L2스위치는 IP에 대하여 NAT로 주소 변환하여 패킷을 전송한다.

② L3스위치는 라우팅 경로에 따라 패킷을 전송한다.

③ L4스위치는 TCP/UDP 포트 정보에 따르는 서비스를 구분하여 패킷을 전송한다.

④ L7스위치는 패킷의 내용에 따르는 부가처리를 더하여 패킷을 전송한다.
2. 다음 <보기>는 어떤 형태의 공격에 대한 설명이다. 이와 관련된 내용으로 다음 중 가장 옳지 않은 것은?
- < 보 기 >

해커 A는 감염된 다수의 PC에 네트워크를 통해 특정 사이트에 대량의 패킷을 발송하는 프로그램을 다운로드 및 실행시켰으며, 이 프로그램은 특정 날짜, 시간에 어떤 사이트를 일제히 공격하였다. 사이트 관리자는 대량의 패킷 수신에 의한 사이트 마비를 감지하고, 즉시 한국인터넷진흥원에 연락하였고, DNS 싱크홀로 대처하였다.
- ① 싱크홀이 적용된 DNS 서버는 공격하려는 IP 요청에 대해, 싱크홀 IP 주소로 반환했다.

② 한국인터넷진흥원은 사이트에 대한 공격 접속을 회피시켰다.

③ 일반 사용자는 공격으로 인하여 사이트 접속이 느려졌으나, 접근이 가능했다.

④ 해커는 DDoS 공격을 위해 랜섬웨어를 대량 배포했다.
3. 다음 중 192.168.1.0과 같은 IPv4 C 클래스 네트워크를 8개의 서브넷으로 나누고, 각 서브넷에 30개의 호스트를 연결할 때 사용되는 서브넷 마스크는?
- ① 255.255.255.224

② 255.255.255.192

③ 255.255.255.252

④ 255.255.255.240

4. 다음 중 포트 스캔(Port Scan)에 관련된 내용으로 가장 옳지 않은 것은?
- ① FIN Scan, XMAS Scan, NULL Scan, ACK Scan은 로그를 남기지 않는다.

② UDP Scan에서 ICMP Port Unreachable 응답은 방화벽 탐지를 의미한다.

③ TCP 헤더를 조작하여 특수한 패킷을 만들어 열린 포트를 탐지한다.

④ 핸드셰이킹(Handshaking) 절차를 통해 열린 포트를 탐지한다.
5. 다음 중 네트워크 공격에 관련된 내용으로 가장 옳지 않은 것은?
- ① IP 스푸핑(Spoofing)은 공격대상과 신뢰관계에 있는 시스템 주소로 공격자 IP를 위장한다.

② ARP 스푸핑은 공격 대상자의 MAC 주소를 공격자의 MAC 주소로 갱신시킨다.

③ ARP 리다이렉트(Redirect)는 패킷 스니핑(Sniffing)은 불가능하나, 임의 IP로 패킷 전송이 가능해진다.

④ ICMP 리다이렉트는 스니핑 시스템을 네트워크상 추가 라우터(Router)로 등록하여 패킷 스니핑을 한다.
6. 다음 중 네트워크를 통한 침입에 대한 대처 방안으로 가장 옳지 않은 것은?
- ① 방화벽(Firewall), IDS, IPS는 모두 네트워크 액세스에 대한 보안 대책이다.

② 트로이목마에 의해 방화벽 안쪽 PC가 해킹되었을 때, 방화벽은 공격에 매우 취약하다.

③ 방화벽은 패킷 내부의 전송 데이터에 대한 분석을 수행하지 않는다.

④ 가장 적극적인 차단을 실시하여 예방적 방어를 수행하는 것은 IDS이다.
7. 다음 중 무선랜에 관련된 설명으로 가장 옳지 않은 것은?
- ① WPA2-PSK는 인증서버를 두고 사용자 계정과 패스워드에 기반한 암호화이다.

② TKIP과 CCMP 중 CCMP가 더 강화된 보안 프로토콜이다.

③ WEP에서 WPA, WPA2로 발전하면서, 암호 알고리즘이 점차 강화되었다.

④ CCMP는 AES 블록 암호에 기반한 프로토콜로 WPA2에 적용된다.

8. 다음 <보기>는 어떤 웹서버 공격에 관련된 내용을 말한 것이다. 다음 중 내용으로 알 수 있는 것으로 가장 옳지 않은 것은?

< 보 기 >

“우리 원의 웹사이트 외주 제작자가 큰 실수를 했습니다. 게시물 업로드 폼에 GET이 쓰였고, 해커가 이를 이용해 웹서버에서 악성 스크립트를 실행시켰습니다. 그리고 그 스크립트로 웹 DB의 사용자 게시물에 다른 해킹 서버로 액세스하도록 또 다른 스크립트를 덧붙였습니다.

결국 그 해킹된 웹서버에 접속해 게시글을 읽은 민원인 PC에 랜섬웨어가 다운로드 되어서 큰 문제가 터졌습니다. 현재 웹서버 로그에 남은 해커 IP 기록을 찾았고, 추적 중입니다.”

- ① 해커는 CSRF, XSS, 랜섬웨어를 모두 사용했다.
- ② 해커는 서버와 게시물을 읽은 사용자 PC에 모두 악성 스크립트를 실행시켰다.
- ③ 폼의 입력란에 대한 필터링과 GET대신 POST를 이용하면 보완이 가능하다.
- ④ 해커는 일반 사용자 PC를 우선 해킹하고 이를 경유하여 원의 웹서버를 해킹했다.

9. DNS는 도메인에 대한 IP 주소 변환을 수행하는 역할을 한다. 다음 중 이에 관련된 내용으로 가장 옳지 않은 것은?

- ① DNS 스푸핑(Spoofing)은 특정 도메인에 대해 가짜 IP 주소를 반환하는 기법이다.
- ② DNS 싱크홀(Sinkhole)은 방어할 도메인에 대해 공격 트래픽을 처리할 대치된 IP주소를 반환하는 방법이다.
- ③ DNS Cache Poisoning은 공격대상 DNS 서버에 대량의 패킷을 전송하여 동작을 정지시키고, 해킹서버를 가짜 DNS 서버로 등록시킨다.
- ④ DNSSEC은 전자서명을 이용해, 서명된 응답만이 등록되도록 검증 처리한다.

10. 다음 중 NAC(Network Access Control) 시스템의 기능 설명으로 가장 옳지 않은 것은?

- ① 접근 제어 및 접근 인증
- ② 백신 관리 및 패치 관리
- ③ 방화벽 및 IPS 통합 로그 관리
- ④ 유해 트래픽 탐지 및 차단

11. 다음 중 VPN에 의해 제공되는 보안 기능으로 가장 옳지 않은 것은?

- ① 전송 데이터에 대해 암호화 보안 전송이 이루어진다.
- ② LAN에 대한 연결 허가를 통제할 수 있는 접근 제어가 제공된다.
- ③ 패킷을 데이터 내용에 따라 필터링하여 바이러스를 차단한다.
- ④ 터널링(Tunneling)을 통하여 원격지 PC를 내부망으로 연결해준다.

12. 다음 중 FDS(Fraud Detection System)에 관련된 내용으로 가장 옳지 않은 것은?

- ① 금융전산망 및 서버에 대한 해킹 침입을 탐지한다.
- ② 전자상거래에서 이상 거래를 탐지하기 위한 방법으로 사용한다.
- ③ 거래 발생 시 거래자 위치, 업종, 물품, 금액 등의 위험성을 평가한다.
- ④ 동일한 공간이 아니고, 시간적으로도 이동할 수 없는 위치에서의 거래 발생을 탐지한다.

13. 다음 중 OSI 계층과 전송단위의 연결로 가장 옳은 것은?

OSI 계층	전송단위
① 데이터링크(Data Link)	세그먼트(Segment)
② 응용(Application)	메시지(Message)
③ 전송(Transport)	프레임(Frame)
④ 네트워크(Network)	비트 스트림(Bit Stream)

14. 다음 중 TCP/UDP 설명으로 가장 옳지 않은 것은?

- ① UDP는 순서번호를 사용하지 않는다.
- ② TCP는 상당한 양의 자원을 사용하지만 UDP보다 느리다.
- ③ TCP는 흐름 제어와 윈도우 매커니즘이 없다.
- ④ UDP는 ACK를 보내지 않으며 신뢰성이 없는 프로토콜이다.

15. 다음 중 송신측에 데이터가 손실되고 있음을 알려서 전송을 잠시 중단하거나 전송률을 줄이도록 하는 ICMP(Internet Control Message Protocol) 메시지로 가장 옳은 것은?

- ① Destination Unreachable(Type 3)
- ② Source Quench(Type 4)
- ③ Redirection(Type 5)
- ④ Time Exceeded(Type 11)

16. 다음 <보기>에서 설명하는 라우팅 프로토콜로 가장 옳은 것은?

- < 보 기 >
- 인트라 도메인 라우팅 프로토콜이다.
 - 링크 상태 라우팅 프로토콜을 기반으로 한다.
 - 논리적 백본(Backbone)을 사용하며 영역(Area)과 연결한다.

- ① RIP(Routing Information Protocol)
- ② IGRP(Interior Gateway Routing Protocol)
- ③ BGP(Border Gateway Protocol)
- ④ OSPF(Open Shortest Path First)

17. 라우터 텔넷 관리 접근통제를 위해 <보기>와 같이 access-list를 설정하였다. 다음 중 적용하는 방법으로 가장 옳은 것은?

- < 보 기 >
- ```
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#access-list 1 deny any
-생략-
```

- ① Router(config-if)#ip access-group 1 in
- ② Router(config)#ip access-group 1 in
- ③ Router(config-con)#access-class 1 in
- ④ Router(config-line)#access-class 1 in

18. 다음 중 VPN 프로토콜에 대한 설명으로 가장 옳지 않은 것은?

- ① IPSec의 ESP는 암호화, AH는 인증기능을 제공한다.
- ② IPSec의 전송모드는 원래의 IP 헤더에 새로운 IP 헤더를 추가한다.
- ③ PPP를 기반으로 마이크로소프트가 제안한 프로토콜은 PPTP이다.
- ④ PPTP, L2TP, L2F는 2계층 프로토콜이다.

19. 다음 중 윈도우 또는 리눅스 네트워크 기반 프로그램 설명으로 가장 옳지 않은 것은?

- ① ipconfig /all 명령으로 컴퓨터의 IP주소, 서브넷 마스크, 기본 게이트웨이 정보를 출력하지만 물리적 주소는 확인할 수 없다.
- ② ping 명령은 원격 호스트가 정상적으로 운영하고 있는지를 확인하며 ICMP Echo Reply와 ICMP Echo Request를 사용한다.
- ③ traceroute 명령 실행결과에서 응답시간이 ‘\*’로 표시 되는 경우는 보안상의 이유로 차단되었거나 실제 해당 구간에 문제가 발생한 경우로 볼 수 있다.
- ④ netstat 명령은 TCP/IP 프로토콜 진단 시 다양하게 사용하며 프로토콜, 로컬 주소, 외부 주소, 상태 정보를 출력한다.

20. 다음 중 네트워크 기반 보안위협에 대한 설명으로 가장 옳지 않은 것은?

- ① SYN Flooding 공격은 TCP의 3-way Handshake 취약점을 이용한 공격이다.
- ② Smurf 공격은 출발지와 목적지의 IP 주소를 공격대상의 IP 주소로 변조하여 전송하며, 자신에게 응답하는 과정을 반복하게 하여 과부하를 유발하는 공격이다.
- ③ Teardrop 공격을 받을 경우 네트워크 연결이 끊어지거나 블루 스크린 오류화면을 출력하고 시스템이 정지된다.
- ④ Ping of Death 공격은 아주 작은 조각(Fragment)의 ICMP Ping 패킷을 처리하게 하여 공격 대상 시스템의 성능저하 및 마비를 일으키는 공격이다.