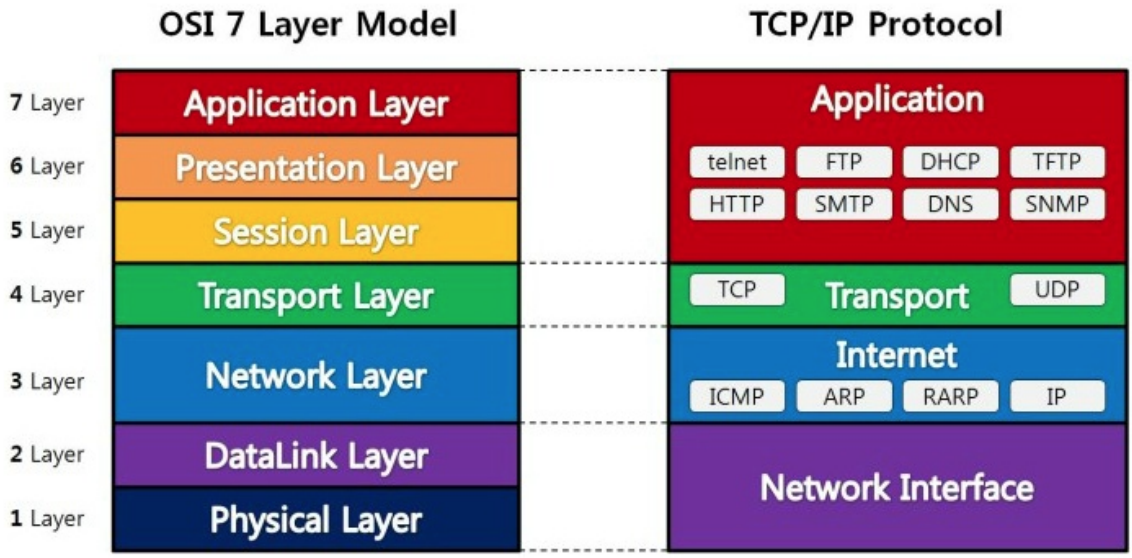
Part 5. 네트워크 보안

Section 20. 네트워크 개요

1. 개요

2. OSI 모델과 TCP/IP 프로토콜



- L1 : 물리 계층
  - 특징 : 물리적 연결 성정
  - 데이터 종류 : bit stream
  - 프로토콜/서비스 : RS-232, X25, X21
- L2 : 데이터 링크 계층
  - 특징 : 종단-대-종단, 오류제어, 흐름제어, 혼잡 제어, LLC/MAC
  - 데이터 종류 : frame
  - 프로토콜/서비스 : Ethernet, Token Ring, PPP, HDLC
- L3 : 네트워크 계층
  - 특징 : 라우팅
  - 데이터 종류 : packet
  - 프로토콜/서비스 : IP, ICMP, **ARP**, RARP, BGP, OSPF, RIP, IPSec, Q930

- L4 : 전송 계층(transport)
  - 특징 : 데이터 전송 보장, 흐름제어, 종단간(End-to-End) 제어
  - 데이터 종류 : segment
  - 프로토콜/서비스 : **TCP, UDP**, RTP, SCTP
- L5 : 세션 계층
  - 특징 : 동기화, 세션 연결,관리,종료
  - 데이터 종류 : message
  - 프로토콜/서비스 : 전송모드 결정(반이중, 전이중), NFS, SQL, RPC
- L6 : 표현 계층
  - 특징 : 압축, 암호화
  - 데이터 종류 : message
  - 프로토콜/서비스 : ASCII, Mpeg, jpg
- L7 : 응용 계층
  - 특징 : 각종 응용서비스 제공
  - 데이터 종류 : message
  - 프로토콜/서비스 : FTP, SNMP, SMTP, 텔넷, HTTP, SSH

통합보안시스템(UTM : Unified Threat Management)

> 방화벽, 침입탐지/방지시스템(IDS/IPS), VPN, 안티 바이러스, 웹/이메일 필터링 등 다양한 보안 기능을 **하나의 장비로 통합**하여 제공하는 보안 솔루션이다.

> 단일 장비로 다양한 보안 기능을 수행하므로 경제성과 보안 관리 및 운영을 편리하게 할 수 있는 장점이 있지만 장애 발생 시 모든 보안기능에 영향을 미치는 단점이 있다.

Section 21. TCP/IP

1. 물리 계층
2. 데이터링크 계층
   - 노드-대-노드 통신
   - 서비스 : framing, 흐름 제어, 오류 제어, 혼잡제어
3. 네트워크 계층 (IP, IGMP, **ARP**, RARP, BGP, OSPF, RIP, IPSec)

   [IP, Internet Protocol]

   - IPv4
     - Subnet Mask
       - CIDR(클래스 없는 주소지정 방식, Classless Inter-network Domain Routing)

        - VLSM(Variable Inter-network Domain Routing)
    - Supernetting : 여러 개의 네트워크를 하나의 네트워크 주소로 묶는 것
- IPv6
    - 128비트 주소체계, **8개**의 필드로 구성된 헤더, 보안과 **인증** 확장헤더

[IGMP, Internet Group Management Protocol]

- IP 멀티캐스트 그룹에서 호스트 멤버를 관리하는 프로토콜

[ICMP, Internet Control Message Protocol]

- IP 프로토콜은 호스트와의 관리 질의를 위한 메커니즘이 없는데, **비신뢰성**과 **비연결성**을 보완하기 위한 프로토콜 (즉, 라우터나 다른 호스트가 동작하고 있는지, 네트워크 관리자의 다른 호스트나 라우터 정보 획득 등)
    - 오류보고 메시지
    - 질의 메시지

      Type 8 : Echo Request

      Type 0 : Echo Reply

      Type 5 : Redirect 더 나은 경로가 있음을 알리기 위해 라우터가 보내는 메시지

      Type 3 : Destination Unreachable 타임아웃 발생하여 IP 패킷이 폐기됨 (Code=0은 TTL=0)

      Type 4 : Soure Quench 데이터를 보낸 호스트에게 IP 데이터그램이 라우터의 집중 현상에 의해 손실되고 있음을 알리는 메시지

      Type 11 : Time Exceeded

[ARP, Address Resoultion Protocol] ←→ RARP

- IP주소를 이용해 해당 MAC 주소를 요청하는 프로토콜
    - ARP 요청(request) 메시지 : 특정 IP에 대한 MAC 주소 요구, **Broadcast**
    - ARP 응답(reply) 메시지 : MAC 주소 정보를 **Unicast**로 전송

4. 전송 계층 (TCP, UDP)

서비스	TCP	UDP
신뢰성	신뢰성 프로토콜	비신뢰성 프로토콜
연결	연결지향적(3-handshaking)	비연결지향적
패킷 순서	패킷 내에 순서번호를 사용	X
혼잡제어	혼잡해질 경우 이를 통보	X
속도, 오버헤드	많은 자원 사용, UDP보다 느림	적은 자원 사용, TCP보다 빠름

[UDP, User Datagram Protocol]

- 비연결형, 비신뢰성
- 프로세스-대프로세스 통신 (소켓 주소 이용)
- 흐름제어(X), 혼잡 제어(X), 오류 제어(△, Checksum을 제외하고는 없음),

[TCP, Transmission Control Protocol]

- 프로세스-대-프로세스 통신
- 스트림 전송 서비스(stream delivery service)
- 전이중 통신(full-duplex service)
- 연결 지향 서비스 : 논리적인 연결통로를 통해 데이터를 주고받음으로써 전송순서 보장

[TCP Header Flag]

- SYN : 연결 시작
- FIN : 연결 종료
- RST : 연결 리셋 지시
- ACK : Ack Number가 유효함 (요청 응답)
- PSH : 수신자에게 빨리 응용프로그램으로 전달할 것으로 지시

[TCP 프로토콜 타이머]

- RTT(Round Trip Time) : 패킷이 송신 측에서 수신 측에 전달된 후, 그 응답신호가 다시 송신 측에 도달하기까지에 시간
- RTO(Retransmission Timeout) : 재전송을 위한 타임아웃. TCP 통신시 전송이 정확히 이루어졌다는 확인을 받지 못한 경우 일정시간을 정해놓고 이 시간동안 확인을 받지 못한 경우 재전송을 하게 된다.
- Fast retransmission : 특정 데이터 segment에 대해 Timeout이 되기 전에 그 세그먼트를 재전송해달라는 ACK가 3개 연속 수신되면 timeout되기를 기다리지 않고 즉시 재전송(fast retransmission) 한다.

[문제]

1. RTO 값은 해당 시간까지 Acknowledge가 전송되어 오지 않는 경우 재선송하기 위한 설정값이다.
2. TCP 세그먼트가 유실되어, 해당 세그먼트를 요구하는 Acknowledge가 연속 도착하더라도, RTO 시간이 Time-out되어야 재전송이 가능하다.
3. RTO 시간이 너무 클 경우 수신자측의 중복 ACK에 대한 손실 세그먼트를 재전송하는 Fast retransmission 현상이 발생
4. RTO 값은 초기 RTT 값을 기준으로 고정되어 있다.

→ 정답 4번, RTO 값은 동적으로 변한다.

5. 응용 계층

Section 22. 라우팅 (출제빈도 0.9%)

1. 라우팅 개요

- 주어진 IP Packet을 전송하기 위해 송신측에서 목적지까지의 경로를 정하고, 정해진 경로를 따라 패킷을 전달하는 일련의 과정
- Default Routing

  [라우터 모드]

  - User Mode : 테스트를 목적(ping, trace)으로 사용되며, 현재 상태만 확인 가능
  - Priviledge Mode : 유저 모드에서 enable 명령어를 통해 전환 가능, 운영자 모드로서 라우터의 모든 명령어 가능(라우터의 구성확인 및 변경 가능)
  - Global Configure Mode : Priviledge Mode에서 config terminal 명령어를 통해 전환되는 모드. 라우터 구성 파일을 변경하는 경우 사용
  - Setup Mode

2. 유니캐스트 라우팅

- 라우팅 알고리즘
  - 거리 벡터(distance vector) : 목적지까지의 최소비용
    - 일정 시간마다 이웃에 위치한 라우터와 경로정보를 교환해서 최적경로를 설정한다.
  - 링크 상태 라우팅(Link-state) : 다익스트라 알고리즘
  - 경로 벡터 알고리즘(path-vector) : 스패닝 트리를 이용한 가장 최선의 규칙
- 라우팅 프로토콜
  - RIP(Routing Information Protocol) (**거리 벡터 알고리즘)**
    - 가장 오래되고 널리 사용되는 내부 라우팅 알고리즘, 문제점(느린 수렴, 라우팅 루프, 무한 세기, 작은 무한값)
    - 라우팅 루프가 발생할 수 있다 (O)
    - 홉수 15이상 네트워크에서 사용 불가 → 네트워크 규모에 제한을 받음
    - 라우팅 정보가 30초마다 교환되므로 장애 시 복구에 많은 시간이 소요된다. (O)
    - RIP은 요청과 응답 2가지 종류의 메시지로 단순한 구조를 갖는다. (O)
    - 작은 규모의 네트워크에 적용되므로 네트워크 변화를 즉시 라우팅 경로에 반영할 수 있다. (X)

- RIPv2 : RIP 확장 프로토콜, CIDR과 VLSM 지원, 서브넷마스크 식별, 경로정보 인증, AS 구별
- IGRP(Interior Gateway Routing Protocol) : RIP 문제점을 해결하기 위한 거리 벡터 알고리즘
- EIGRP(Enhanced IGRP) : IGRP 확장 프로토콜. 링크 상태 라우팅 프로토콜에 가까움
- OSPF(Open Shortest Path First) : 링크 상태 라우팅 프로토콜 **(링크 상태 알고리즘 → Dijkstra 알고리즘)**
  - 모든 라우터가 동일한 네트워크 토폴로지 DB를 기반으로 경로를 계산하기 때문에 라우팅 루프가 발생하지 않는다.
- BGP4(Border Gateway Protocol v4) : 현재 인터넷에서 사용하고 있는 유일한 인터 도메인 라우팅 프로토콜. **(경로 벡터 알고리즘)**

3. 라우터 보안

- Null Routing **(blackhole routing)**
  - access-list와 함께 유용하게 사용할 수 있는 필터링 기법
  - 특정 ip 또는 ip 대역에 Null이라는 가상의 쓰레기 인터페이스로 보내 패킷이 텅신이 되지 않도록 하는 것
- unicast filtering
  - access-list나 blackhole 필터링을 이용하여 IP나 IP대역을 지정하지 않고도 비정상 트래픽을 효율적으로 필터링할 수 있다.

Section 23. 네트워크 장비의 이해

1. 네트워크 장비의 이해

- NIC (Network Interface Card)
  1. PC 혹은 네트워크에서 전달되어 오는 정보를 상호 교환할 수 있도록 만들어 주는 역할을 담당한다.
  2. PC에서 전송 요구가 발생하면 이 정보를 일단 버퍼에 저장한다.
  3. 빠른 전송을 위해 데이터를 코딩하고 압축한다.
  4. 네트워크로 정보를 전송하기 위해 병렬구조로 데이터를 바꾼다. (X)

     → 직렬로 전환한다.
- 허브(HUB) **1계층 (물리)**

    - **물리 계층**에서 동작하는 장비
    - **리피터**(repeater) : 약해진 신호를 원래 형태로 재생 및 증폭하는 장치
- 브릿지(bridge) **2계층 (데이터링크)**
    - **데이터링크 계층인 MAC(Media Access Control)**에서 동작하는 장비
    - 충돌 도메인(collision domain)을 나누어준다.
    - 스위치와 달리 S/W로 구현됨
- 라우터(router) **3계층 (네트워크)**
    - 물리, 데이터 링크, 네트워크 계층에서 동작한다.
        - 이기종 LAN간 연결, LAN을 WAN에 연결, 효율적 경로를 선택하는 라우팅 기능, 에러 패킷에 대한 폐기 수행
    - 라우터는 각 인터페이스를 위한 IP주소와 MAC주소를 갖는다.
    - 인터넷에서 IP네트워크들 간 연결 또는 IP네트워크와 인터넷을 연결
    - 브릿지와 달리 라우터는 브로드캐스팅과 멀티캐스팅 패킷을 모두 차단 (= 회선의 효율적인 사용)

- 스위치(switch) **2계층, 4계층, 7계층**
    - L2 : Mac Address 기반
    - L4 : TCP/UDP 포트 정보를 분석해 해당 패킷이 현재 사용하는 서비스 종류별(HTTP, FTP 등)로 패킷 처리
    - L7 : 트래픽의 내용 패턴 등을 분석해 패킷을 처리

    [스위칭 방식]

        - Store-and-Forward : 스위치나 브리지가 일단 들어오는 프레임을 모두 받아들인 다음 처리 시작 (에러 발견시 프레임을 버리고 재전송 요구함→ 에러 복구능력 ↑)
        - Cut-Through : 앞에 들어오는 목적지 주소만 보고 처음 48비트만 전송 (에러 복구능력 ↓)
        - Fragment-Free : 위 두 방식 결합. 512비트를 보게 됨.

2. VLAN의 구성 및 관리

- VLAN(Virtual Local Area Network) **2계층 (데이터링크)**
    - 소프트웨어에 의해 구성한 근거리 네트워크
    - 데이터링크 계층에서 브로드캐스트 도메인을 나누기 위해 사용하는 기술
    - VLAN이란 브로드캐스팅 트래픽을 제한하여 불 필요한 트래픽을 차단하기 위한 논리적인 LAN이다.

Section 24. 무선통신 보완 (1.6%)

1. 무선통신

[무선네트워크 유형]

- WPAN : 단거리 Ad hoc 또는 Peer to Peer 방식
- WLAN : 유선랜의 확장 개념 또는 유선랜 설치가 어려운 지역으로 네트워크 제공
- WMAN : 대도시, 대학 캠퍼스처럼 넓은 지역

[무선랜 표준 기술]

- IEEE 802.11b
  - 공공장소에서 많이 사용하는 무선랜 (2.4GHz, 최대 11Mbps)
- IEEE 802.11a
  - 주파수 5GHz, 최대 54MBps
- IEEE 802.11g
- IEEE 802.11i
  - WPA-1, WPA-2 규격이 포함
- IEEE 802.11n

2. 무선랜 보안

[무선랜 인증 기술]

- SSID(Service Set IDentifier) : AP를 구분하는 ID로 무선랜을 통해 전송되는 패킷 헤더에 덧붙이는 32바이트의 고유 식별자
- MAC 주소 인증
- WEP(Wired Equivalent Privacy) 인증
  - 공유키인 WEP를 이용해 사용자를 인증하는 방식
  - (장점) 데이터 암호와 함께 적용하고, 무선랜 장비에서 WEP의 구현이 간단하고 인증 절차 또한 간결하다는 장점이 있음
  - (단점) 고정된 공유키를 사용하여 키값이 외부로 유출될 경우 보안 문제에 취약하여 현재는 권장되지 않음
  - (단점) 단방향 인증으로 인해 악의적 목적으로 운영되는 복제 AP를 이용해 정상 사용자의 정상 AP 접속을 방해하거나 복제 AP로 접속하게끔 유도 가능
- EAP(Extensible Authentication Protocol) 인증

[무선랜 암호화 기술]

- WEP(Wired Equivalent Privacy) : 보안적으로 취약하여 현재는 권장되지 않음
  -

[무선랜 인증 및 암호화 복합 기술]

- WPA(Wi-Fi Protected Access)
  - 802.11i 보안 규격 일부 기능을 수용
- WPA2(Wi-Fi Protected Access 2) = **RSN(Robust Security Network)**
  - 2세대 WPA로서, CCMP(Counter Mode with Cipher Block Chaining Messgae Authentication Code Protocol) 암호화 방식을 사용
  - TKIP를 대체하기 위해 AES에 기반을 둔 CCMP 암호화 방식을 사용
  - RC4 알고리즘 대신 AES 암호화 알고리즘을 사용하여 좀 더 강력한 보안을 제공한다.
- 802.1x/EAP(Extensible Authentication Protocol)
  - WPA/WPA2-PSK가 기존 WEP를 보완항 방식이라면, WPA-EAP는 사용자 인증 영역까지 보완한 방식이다.
  - IEEE 802.11의 WPA와 WPA2 표준은 공식 인증 메커니즘으로 이 프로토콜을 채택함.

3. WAP(Wireless Application Protocol)

- WAP는 모든 기존 무선 네트워크 기술(GSM, CDMA, TDMA) 및 IP, XML, HTML, HTTP 등의 인터넷 기술과 가능한 한 호환해서 설계

  [규격]

  - WWW 프로그래밍 모델에 기반
  - XML과 무선 마크업 언어(WML)
  - 모바일 무선 단말기에 적합한 소영 브라우저의 규격
  - 경량 통신

4. 디바이스 인증기술(기기 인증)

- 아이디/패스워드 기반 인증
  1. 아이디/패스워드 기반 : 서버의 DB와 비교하여 인증
  2. 무선 네트워크 아이디(SSID) : AP와 무선랜 클라이언트 간에 SSID를 공유
  3. 무선단말과 AP간 WEP 사용
  4. 서버 간 접근제어 아이디/패스워드 사용
- MAC 주소값 인증
- 암호 프로토콜을 활용한 인증

- Challenge/Response 인증

5. RFID

- RFID 공격 유형
  - 도청
  - 트래픽분석
  - 위조
  - 서비스 거부(DoS, Denial of Service)
- RFID 보안 기술
  - 암호 기술을 사용하지 않는 정보보호 정책
    - 킬(kill) 명령어, Sleep 명령과 Wake 명령어, 블로커(Blocker) 태그 기법, Faraday Cage, Jamming
  - 암호 기술을 이용한 정보보호 대책
    - 해시 락(Hash Lock) 기법, XOR(Exclusive OR) 기반 원타임 패드 기법

6. 모바일 보안

[1] 모바일 운영체제의 보안과 취약점

- iOS 보안 체계
- iOS 취약점
- 안드로이드의 보안 체계
- 안드로이드의 취약점

[2] BYOD 보안 기술

- MDM(Mobile Device Manangement)
- 컨테이너화(Containerization)
- 모바일 가상화(Hypervisors)
- MAM(Mobile Application Management)
- NAC(Network Access Control)

Section 25. 네트워크 관리

1. 네트워크 관리

2. SNMP (Simple Network Management Protocol)

- 관리자와 에이전트 간의 간단한 상호작용으로 관리 작업 수행하는 **응용 계층** 프로토콜

  [관리 구성 요소]

  - SMI (Structure of Management Information) : 객체에 이름을 붙이고, 객체 유형을 정의하며, 객체와 값을 부호화하는 방법의 규칙
  - MIB (Management Information Base) : 관리 정보 집합
    - 네트워크를 관리하는 데 필요한 모든 관리정보를 보관하는 저장소
    - 모든 네트워크 관리 자원들은 객체로 표현되며, 이러한 객체들의 구조적인 모임이 바로 MIB이다.
    - 네트워크 피관리요소에 관한 정보를 규정한 DB이다.

3. 원격 접속 서비스

   [Telnet]

   - 가상 터미널 서비스에 대한 표준 TCP/IP 프로토콜

   [Rlogin]

   - remote login의 약자, 패스워드 입력이 필요 없다.
   - BSD(유닉스 계열 O/S)간의 원격접속

   [SSH]

   - Telenet, Rlogin을 대체하기 위해 설계. 강력한 인증 방법, 안전한 통신 기능을 제공
   - 포트 전달(Port Forwarding) 제공
   - RSA 암호화

Section 26. 네트워크 기반 프로그램 활용

1. 네트워크 기반 프로그램 활용

   - 연결테스트 : ping
     - (ICMP) Ehco Request, (ICMP) Echo Reply
   - 경로추적 : traceroute

```
traceroute -m 5 hostname : 최대 TTL을 지정한다. 디폴트는 30
traceroute -p port : UDP 포트를 지정한다. 디폴트는 33434번이다.
```

   - 네트워크 인터페이스 진단 : netstat

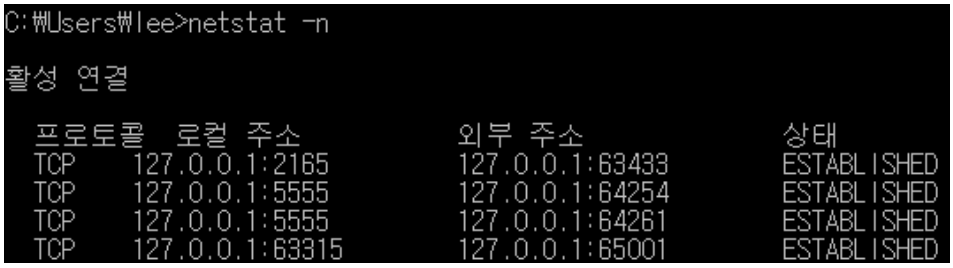
```
-a : 모든 연결과 수신 대기 포트 표시 (all)

-e : 이더넷 통계(ethernet)
```

```
-n : 주소와 포트 번호를 숫자 형식으로 표시

-an : 네트워크 주소를 숫자로 나타낸다.
```

▲ netstat -e



▲ netstat- n

- 네트워크 인터페이스 설정 : ifconfig

```
ifconfig [device] [ip_address] [netmask IP] [broadcast IP] [up|down]

  - device : IP 주소를 부여할 장치 (ex : eth0)
  - up|down : 장치 활성화 or 비활성화

EX) ifconfig eth0 16.64.1.86 netmask 255.255.255.0 broadcast 16.64.1.255 up
```

- 네트워크 패킷/로그 분석 : tcpdump

```
  tcp dump [-option]

  - [-A} : 패킷 내용을 ASCII로 출력
  - [-c] : 주어진 수의 패킷을 받은 후 종료
  - [-i] : 인터페이스 지정 (default : 가장 낮은 숫자의 인터페이스)

  tcpdump host 16.64.10.15 and port 80

  - 출발지나 목적지가 16.64.10.65이고, 포트가 80인 트래픽을 모니터링
```

Seciton 27. 네트워크 기반 공격의 이해 ★★★ (매회 5-7문제 출제)

1. 서비스 거부공격(DoS, Denial of Service)

TCP SYN Flooding Attack, SMURF Attack, Flooding Attack, Land Attack, Ping of Death, Teardrop Attack, Inconsistent Fragmentation

- 가용성 침해

[SYN Flooding Attack]

- 공격자가 임의의 자신의 IP를 속인 뒤, 서버로 대량의 SYN 패킷을 보내 서벌르 대기 상태(syn+ack sent)로 만드는 공격'
- 3-way handshaking 과정에서 Half-Open 연결 시도가 가능하다는 취약점

[공격방법]

- 공격자 : 시작 주소가 조작된 SYN 메시지를 목적지에 상당히 많이 보냄
- 서버 : 이 패킷 각각에 대해 서버에 정보를 저장하고, SYN/ACK 패킷을 조작된 주소에 보냄
- 이 주소에 시스템이 존재하면 RST 패킷이 전송되어 요청된 연결이 끊어지고 정보도 삭제되지만, 존재하지 않는다면 해당 주소에서 응답이 오지 않음
- 서버 : 서버는 멍청하게 연결이 실패했다고 생각할 때까지 SYN/ACK 패킷을 보내어 연결 설정 시도를 반복
    - 이 기다리는 시간과 정보가 TCP 연결 테이블에 저장되어 이후 정상적인 연결 요청이 거부됨

[조치방법]

- 보안 패치, IDS/IPS 설치, 접속 타임아웃 시간 단추 등
- Connect Queue Size를 증가시킴 (=Backlog Queue)
- SYN Cookie Size를 늘림
- Router단에서 서브넷 외의 주소를 가지는 소스IP를 가지는 패킷 차단 (tcp intercept)
- 리눅스 계열의 경우 syncookies 기능을 사용하고, Windows의 경우 레지스트리를 변조

[문제]

1. TCP SYN Flooding 공격과 관련이 없는 것은?

1. Half Open Conneciton 공격
2. 분산 DoS 공격
3. Reflector 공격
4. Teardrop 공격

> 💡 정답 : 4번
> 오버플로우 공격을 일으키는 DoS 공격기법이 Teardrop이다.

[Smurf Attack]

- IP 위장과 ICMP의 특징을 이용한 광범위한 DoS 공격
- Boradcasting Network를 이용한다.

```
hping3 192.168.0.255 -a 10.10.10.5 -icmp -flood

  - hping은 사용자가 커스텀 패킷을 전송한 후 타깃으로부터 응답을 출력하는 툴
```

[Land Attack]

- 패킷 전송 시 출발지 IP 주소와 목적지 IP 주소 값을 똑같이 한다.

  = 패킷의 출발지와 도착지와 같은 패킷이 다수 유입된다.
- IP Spoofing을 이용한 SYN 공격

[Ping of Death]

- 한 개의 ICMP 패킷으로 많은 부하를 일으켜 정상적인 서비스를 방해하는 공격법(65,535 bytes 이상)

```
sysctl -w net.ipv4.icmp_echo_ignore_all = 1

 - sysctl 명령은 커널 변수의 값을 제어하여 시스템을 최적화할 수 있는 명령이다.
 - 외부의 모든 ping of death 공격을 방어하기 위한 명령어

 -w variable=value : 변수에 값을 설정한다
 -n : 특정 키에 대한 값을 보여준다.
```

[Teardrop Attack]

- IP가 정상적으로 패킷을 전송할 때 **IP 단편화(fragmentation)**가 발생한다. 수신자는 재조립을 통해 데이터를 복구하게 되는데, 정확한 조립을 위해 Offset값을 더하게 된다. 이 오프셋 값보다 더 큰 값을 더해 오버플로우를 일으켜 시스템의 기능을 마비시키는 DoS 공격기법이다.
- Teardrop 기법은 이 **Offset값을 고의적으로 수정**하거나, 더 큰 값을 더해 오버플로우(overflow)를 일으킨다.

2. 분산 서비스 거부공격(DDoS, Distributed Denial of Service)

DDoS 공격 사례 : 트리누(Trinoo), TFN, Stacheldraht, TFN2K
최신 DDoS 공격유형 : UDP/ICMP Flooding, TCP Traffic Flloding, IP Flooding, HTTP Traffic Flooding, HTTP Header/Option Spoofing Flooding

- DDoS : 공격 시스템을 분산배치하여 동시에 대량 트래픽을 발생시키는 공격(Zombie PC)

  [종류]

  1. Trinoo Attack
  2. Stacheldraht
     - 트리누와 TFN을 참고하여 제작된 도구로서, 마스터 시스템 및 에이전트 데몬 사이에 통신을 할 때 암호화하는 기능이 추가됨.
     - ICMP Flood, SYN Flood, UDP Flood와 Smurf 등의 DDoS 공격을 할 수 있는 기능을 갖고 있음
  3. TFN2K
     - TFN의 발전된 형태
     - 통신에 특정 포트가 사용되지 않고 암호화되어 있음.
  4. Targa
     - 여러 종류의 서비스 거부 공격을 실행할 수 있도록 만든 공격 도구로 Mixter에 의해 만들어짐
     - 즉, 이미 나와 있는 여러 DoS 공격 소스를 사용하여 통합된 공격도구를 만듦.
     - 공격 기법 : bonk, jolt, land, nestea, newlear, syndrop, teardrp, winnuke 등
- ※ UDP Flooding Attack은 DoS 공격

  [공격 방법]

  1. **UDP/ICMP Traffic Flooding 공격**
  2. **TCP Traffic Flooding 공격**

3. **IP Flooding 공격**
4. **HTTP Traffic Flooding 공격**

   1) GET Flooding

   - 동일한 URL을 반복 요청
   - TCP 3-Way 핸드셰이킹 과정을 통해 정상적인 접속 후 → HTTP Get Method를 통해 무한대로 실행하는 것

   2) Cache Control Attack (CC Attack)

   - HTTP 메시지의 캐시 옵션을 조작하여 캐싱서버가 아닌 웹서버가 메시지를 처리하도록 하여 웹서버의 자원을 소모시킨다.

5. **HTTP Header/Option Spoofing Flooding 공격**

   1) Slow HTTP Post DoS

   2) Slow HTTP Header DoS(slowris)

   - HTTP Get 헤더 수신시 발생하는 취약점을 이용한 공격이다.
   - 공격자는 HTTP Header 정보를 비정상적으로 조작하여 웹서버가 온전한 Header 정보가 올때까지 기다리도록 한다.

   [동작]

   - HTTP에서 헤더의 끝을 /r/n 이라는 개행문자로 구분하는데, 공격자는 개행문자를 보내지 않고 지속적으로 의미없는 변수를 추가한다.
   - 서버는 헤더 정보가 아직 전송 중이라고 인식하고 연결을 유지한다.

   [대응]

   - 방화벽 등을 통해 세션 임계치 제한을 설정
   - 연결 타임아웃 시간을 짧게 두어 연결이 종료된록 한다.

   3) Slow HTTP Read Dos

6. **HULK(HTTP Unreadable Load King) DoS**
   - 웹서버의 가용량(최대 접속 가능 클라이언트 수)을 모두 사용하도록 하여 정상적인 서비스가 불가능하도록 유도

7. **SIP (Session Initiation Protocol) Flood**
   - INVITE request를 위조된 시작주소에 넣어 전송하는 공격 기법

[공격 사례]

(1) 트리누(Trinoo) 공격

- 1999.06~07 / 미네소타 대학 / 솔라리스 2.x 시스템

- UDP Flood 서비스 거부 공격에 사용되는 툴

[대응 방안]

1. 라우터(Router)
   - 대응공격 : Direct Flooding, Broadcast Flooding, DNS UDP Flooding, DNS Query Flooding, DNS Reply Flooding등
   - 대응공격의 특징 : 회선의 대역폭 증가 및 동일 네트워크를 사용하는 모든 서비스에 장애 발생
2. 경계 라우터
   - 대응공격 : 단순 논리공격 (Tear Drop, Bonk, Land Attack) 등의 공격을 방어
   - 대응공격의 특징 : 논리적 오류를 이용한 공격으로 피해 서버의 오작동을 유발한다.
   - AC에 비해 구성이 쉽고 부하가 적어 사용이 용이
3. QoS
   - 차단중심의 대응이 아닌 가용성(Guranteed Capacaity) 중심의 선택적 대역폭 조정방식 사용

[방어 사례]

- URL Redirect 우회 공격 방어 : 좀비 PC에서 특정 URL 요청시 다른 URL 리다이렉트 신호를 전송해 공격을 차단한 방어 기법

[VoIP 서비스 공격]

- SIP Flood
- RTP(Real-time Transport Protocol) 공격
- INVITE 플러딩 공격
- Register 플러딩 공격

[한국 DDoS 사례]

- 2013.01.25 인터넷 대란 : MS SQL 서버의 허점을 이용한 슬래머웜이 KT 혜화전화국에 있는 DNS 서버에 인터넷 트래픽을 집중 (디스크 파괴 및 파일 삭제 X)
- 2009.07.07 DDoS 공격 : URL Redirect 우회 공격 방어를 통해 컴퓨터 하드디스크 파괴 코드 발견
- 2011.03.04 DDoS 공격 : 정부기관, 은행, 포털이 DDoS를 통해 일시적으로 두 차례 마비
- 2013.03.20 사이버테러 : KBS, MBC, YN과 농협, 신한은행 등 방송 및 금융 6개사 전산망 마비 사태. 북한 정찰총국 소행 (3만 2천여대 마비)

- DRDoS (Distributed Reflection DoS)

- 출발지의 IP를 위조(IP Spoof)하여 정상 요청(request)하면 공격 대상에 대량의 응답 값이 전달되는 것을 이용한 공격방법
- 별도의 에이전트 설치 없이 TCP 프로토콜 및 라우팅 테이블 운영상의 취약성을 이용한 공격이다.
  - TCP 3way-handshake을 이용하는 DDoS 공격으로 공격자는 출발지 IP를 공격대상의 IP로 위조하여 syn 패킷을 다수의 반사서버로 전송하여 공격대상이 이 장비들을 응답하는 syn-ack 패킷을 받아 서비스 거부 상태가 된다.
- 정상적으로 서비스를 제공 중인 서버를 Agent로 활용하는 공격기법
- 클라이언트의 특성상 외부 인터넷 서버 접속이 잦음으로 인하여 클라이언트의 보호는 사실상 불가능하다.

[DDoS와의 차이점]

- IP Spoofing(IP 위조)의 사용 : DDoS는 선택 DRDoS에는 필수
- 반사체(Reflector)의 활용 : 반사 서버 사용

[DRDos의 장점]

- 패킷이 전송되는 경로가 무수히 많다.
- 반사 서버의 단계적 사용 및 확산 : 다수의 반사 서버 목록을 보유하고 있으면 공격 경로를 끊임없이 변경할 수 있음
- 위조된 SYN 패킷 출발지 IP를 랜덤하게 생성하는 DDoS 공격과 다르게 공격대상 IP를 출발지 IP로 위조하여 전송하기 때문에 추적이 힘듦.

[DRDos의 단점]

- DDoS는 Layer 7을 공격하거나 단순 Flood가 아닌 특수 공격에도 활용이 가능하지만 DRDoS는 반사체를 원하는 대로 제어할 수 없어 오로지 **Flood 타입 공격만 가능**

- Slowloris 공격

3. 네트워크 스캐닝

[1] 포트 스캔 종류

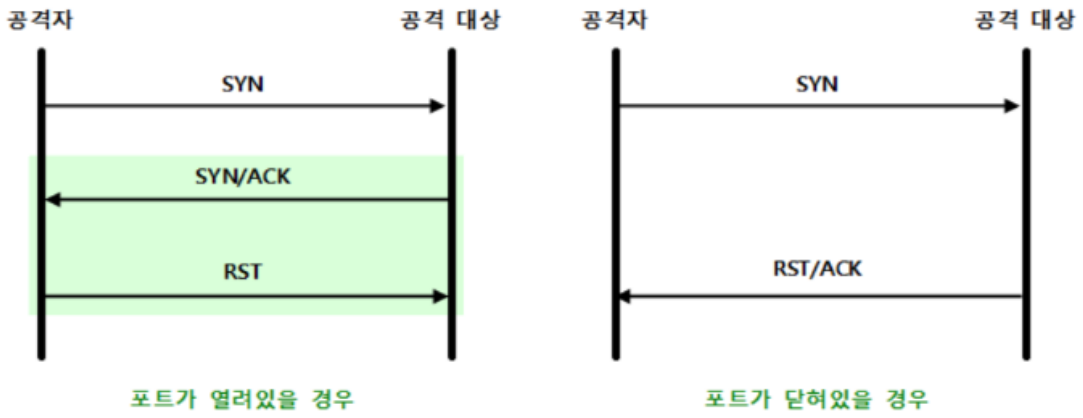
[1] Sweep : 특정 네트워크에 대해 해당 네트워크에 속해 있는 시스템의 유무 판단을 할 수 있고, 목표 네트워크에서 사용하거나 소유하고 있는 IP 주소와 네트워크 범위를 알아내는 기법

- ICMP Sweep
- TCP Sweep
- UDP Sweep

[2] Open Scan : 시스템 활성화 여부, 스캔하는 포트에 해당되는 서비스와 활성화 여부를 조사할 수 있는 방법

1) TCP Full Open Scan (= TCP SYN/ACK Scan)

2) TCP Half Open Scan (= TCP SYN Scan)

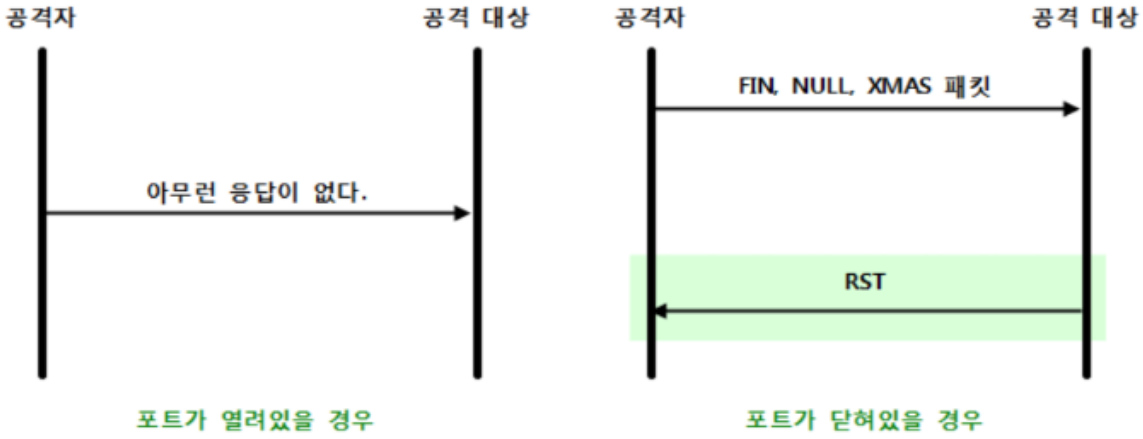


- 세션을 완전히 연결하지 않고, 포트의 활성화 여부만 판단

  (포트 열린 경우) 공격자 SYN 패킷 → 서버 SYN/ACK 패킷 → 공격자 SYN 패킷 (세션에 대한 로그를 남기지 않음)

  (포트 닫힌 경우) 공격자 SYN 패킷 → 서버 RST/ACK 패킷

[3] Stealth Scan



- TCP 헤더를 조작하여 **특수한 패킷**을 만들어 보낸 후 그 응답으로부터 포트 활성화 여부를 파악하며 세션을 완전히 연결하지 않아 로그가 남지 않음
- 포트가 열려있는 경우 응답이 없고, 포트가 닫혀 있는 경우 RST 패킷이 돌아온다.

  1) TCP FIN Scan : 헤더 내에 FIN 플래그 설정

  2) TCP NULL Scan : 헤더 내에 플래그 값 설정않고 전송

  3) TCP XMAS Scan : ACK, FIN, RST, SYN URG 플래그 전송

  4) ACK Scan

  5) TCP Fragment Scan

[2] 대표적인 스캔종류

1. NMap

   [Scan Type]

   -sS : TCP SYN(Half-open) Scan, 다른 스캔 기법보다 더 비밀스러우며 타깃 호스트에 log가 남지 않는 방법

   -sP : Ping Scan, 네트워크의 어느 호스트가 살아있는지 알고 싶을 때

   [Port Option]

   [Output Option]

   -v : 자세하게 출력

   -oX <file> : XML 파일 형식으로 출력

   [기타]

   -O : 대상 호스트의 운영체제 정보 출력

   -f : 스캔 시 방화벽을 통과할 수 있도록 패킷을 분할

   -T0 ~ T5 : T0 아주 느리게 ~ T5 아주 빠르게

[3] Sniffing

> ! (1) 스니핑의 종류 (2) 네트워크 스니퍼

- 허브 환경에서의 스니핑
  - 시스템 NIC를 promiscuous 모드로 동작하게 하면 버려지는 패킷을 저장하고 분석이 가능
- 스위치 환경에서의 스니핑
  - Switch Jamming : 스위치의 MAC Address Table을 버퍼 오버플로우시켜서 스위치가 허브처럼 동작하게 강제적으로 만드는 기법
  - ARP Redirect : 공격자가 자신이 라우터인 것처럼 MAC 주소를 위조하여 ARP Reply 패킷을 해당 네트워크에 boradcast한다.
  - ARP spoofing : 공격자가 특정 호스트의 MAC 주소를 자신의 MAC 주소로 위장한 ARP Reply 패킷을 맏늘어 희생자에게 지속적으로 전송하면, 희생자의 ARP Cache에 특정 호스트의 MAC 정보가 공격자의 MAC 정보로 변경이 된다.
  - ICMP Redirect :
  - 스위치의 span/monitor port를 이용한 스니핑

  [대처방법]

1) 능동적인 방법

- 주요 데이터 전송구간에 **VPN** 운용
- 네트워크 스니퍼

[공격형식]

- UP BROADCAST RUNNING PROMISC : 무차별모드로 장비가 실행됨

[4] Spoofing

- ARP Spoofing
- IP Spoofing
- DNS Spoofing

[5] Session Hijacking

- 서버와 클라이언트가 TCP 통신을 할 때, RST 패킷을 보내 일시적으로 TCP 세션을 끊어 시퀀스 넘버를 새로 생성하여 세션을 빼앗아 인증을 회피하는 것
- HTTP Session Hijacking : 웹브라우징시 세션 관리를 위해 사용되는 Session ID를 스니핑이나 무작위 추측 공격(brute force guessing)을 통해서 도용하는 기법
- Slow HTTP Read DoS : 공격자는 웹서버와 TCP 연결 시, TCP 윈도우 크기 및 데이터 처리율을 감소시킨 후 HTTP 데이터를 송신하여 웹서버가 정상적으로 응답하지 못하도록 DoS 상태를 유발한다.
- 공격도구 : hunt

[Remote Finger Printing]

[IP Scanning, Port Scanning]

[Sniffing, 암호화 프로토콜]

- 원리
  - NIC 모드를 Promiscuous로 바꾸고 네트워크 상의 모든 트래픽을 다 받아들임으로써 스니핑 가능
- 대응
  - ARP Cache Table을 정적으로 운영
  - 데이터 암호화 : SSL(전자상거래) / PGP, S/MIME(메일) / SSH(원격 접속) / VPN / IPSec

Section 28. IDS/IPS (출제빈도 2.9% / 매회 출제)

1. 침입탐지시스템(IDS, Intrusion Detection System)

- IDS의 동작 순서 : 데이터 수집 - 데이터 가공 및 축적 - 분석 및 침입탐지 단계 - 보고 및 대응

[3] 분류

[탐지 방법에 따른 분류]

1. 지식기반 침임탐지(knowledge-based detection) = 규칙-기반 침입 탐지(Rule-based Detection) = 오용 침입탐지(misuse detection)
    - 전문가 시스템 = knowledge based detection
    - 상태전이 모델(State Transition Detection)
    - 패턴 매칭(Pattern Matching)
    - 시그니처 분석
    - 키 모니터링(Keystroke Monitoring)
    - 페트리넷(Petri-net) : 정보 흐름의 표현을 극도로 간소화한 병렬 가동 시스템 표현. 완전 탐색을 해야하기 때문에 비효율적이며, 시간적 비용과 저장용량이 많이 필요하다는 단점이 있다.
    - 규칙 기반 침입 탐지
        - 변형 탐지 (Anomaly detection) : 이전 사용패턴과 달라진 걸 탐지
        - 침투 식별 (Penetration identification) : 의심스런 행동을 찾아내는 전문가 시스템
2. 행위기반 침임탐지(behavior-based detection) = 통계적 변형 탐지 = 비정상 행위 탐지 (anomaly detection, anomaly-based detection)
    - 통계적 분석 방법(Stastistical Detection)
    - 예측 가능 패턴 생성(Predictive Pattern Generation)
    - 신경망 (Neural Netoworks)
    - 통계적 변형 탐지
        - 임계값 탐지(Threshold detection) : 사용자와는 무관하게 다양한 사건들의 발생빈도에 대한 임계값 정의
        - 프로파일 기반(Profile based) : 각 사용자의 동작에 대한 프로파일을 구성하고 개인별 행동의 변화를 감지

[데이터 수집원에 따른 분류]

NIDS (Network-based IDS)	분류	HIDS((Host-based IDS)
네트워크를 통해 전송되는 패킷 정보를 수집·분석하여 침입을 방지	탐지방법	호스트 시스템으로부터 생성되고 수집된 감사 자료로 침입을 방지
· 초기 구축비용이 저렴 · OS에게 독립적이어서 구현·관리 쉬움 · 공격자가 흔적을 제거하기 어려움	장점	· 정확한 탐지가 가능 · 암호화 및 스위칭 환경에 적합 · 추가적인 H/W가 필요하지 않다.
· 암호화된 패킷 분석 X · 스위칭 환경에서 구축비용↑ · 고속 네트워크 환경에서 패킷 손실이 많아 탐지율이 떨어짐 · 호스트 상에서 수행되는 세부 행위 탐지 X	단점	· 각각의 시스템에 설치해야 하므로 다양한 OS를 지원해야 한다. · 시스템에 추가적인 부하가 걸림 · 구현이 용이하지 않음 · 로그 변조, 공격에 의한 무력화

- **NIDS (Network-based IDS)**
  - 네트워크 트래픽을 분석하고 모니터링
  - **정상행위 프로파일**과 현재 수집된 트래픽 정보의 특징을 비교하여 침입여부를 판정

  [장점]
  - HIDS보다 설치되는 시스템 수가 적다

  [단점]
  - 암호화되는 트래픽에 대한 침입 탐지를 하지 못한다.
- **HIDS (Host-based IDS)**

  [장점]
  - 정확한 탐지 가능
  - 암호화 및 스위칭 환경에 적합
  - 추가 하드웨어 필요하지 않음
  - 트로이목마, 백도어, 내부자에 의한 공격탐지/차 가능

  [단점]
  - 각각의 시스템마다 설치해야 하므로 다양한 O/S를 지원해야 함
  - 침입 탐지 시스템으로 인해 시스템 부하 발생

  [문제]
  - 비정상행위기반 침입탐지 방법은 사전에 구축된 비정상행위 프로파일과 현재 수집된 트래픽 정보의 특징을 비교하여 침입여부를 판단한다.
    → (X) 사전에 구축된 '정상적인' 프로파일과 비교

[IDS의 응용]

- Snort

- 일종의 IDS, 실시간 트래픽 분석, 프로토콜 분석, 내용검색/매칭, 침입탐지 Rule에 의거하여 오버플로우, 포트스캔, CGI 공격, OS 확인 시도 등의 다양한 공격과 스캔을 탐지할 수 있다.
- snort 룰(시그니처 형식)

```
alert tcp 192.168.159.0/24 any -> 192.168.159.131 80
 (1)  (2)       (3)        (4) (5)    (6)         (7)
(msg : "DOS SMBdie attack" : flow: established: content: "|57724c65648314849a | ":)


(1) Action
  - alert : alert를 발생하고 로그에 남김
  - dynamic : activate action에 의해 활성화가 되면 log action과 동일한 액션을 취한다.

(2) Protocol
  - tcp, udp, icmp, ip 중 택1

(3) IP
  - 복수개 IP : 10.10.10.0/24, 11.11.11.11
  - 부정 연산자 사용 : !10.10.10.0.24

(4) PORT
  - 1:1024 - 1부터 1024번 포트
  - :1024 - 1024이하 포트
  - 1024  - 1024이상 포트
```

2. 침입방지시스템(IPS)

Section 29. 침입차단시스템(Firewall) (2~3문제 / 20문제 中)

1. 침입차단 시스템(방화벽, Firewall) 개요

- 개요 : 내/외부 네트워크 사이에서 접근제어 정책을 구현하는 시스템
- 기능
  - 접근 통제, 사용자 인증, 감사 및 로그 기능, 프라이버시 보호, 서비스 통제, 데이터 암호화
  - 패킷 분석 및 공격 탐지 (X) → IDS의 기능
- 분류
  - 서비스 제어 : 안에서 밖으로 혹은 밖에서 안으로 접근할 수 있는 인터넷 서비스 유형을 결정
  - 목적지 제어 : 특정 서비스를 요청들을 시작하거나 침입차단시스템 통과를 허용할 때 목적지를 결정
  - 행동 제어 : 특정 서비스를 어떻게 사용(how)할지 제어
  - 사용자 제어 : 어느 사용자가 접근을 시도하는지에 따라서 서비스 접근을 제어한다.

2. 침입차단시스템의 유형에 따른 분류

[1] 패킷 필터링 시스템

- ACL을 이용하며, 속도가 빠르고 비용이 적게 든다. (O)
- 패킷 내의 데이터에 대한 공격을 차단하지 못한다. (O) = 상대적으로 낮은 보안이다. (O)
- 응용 프로그램 사용에 따른 기록 및 감사 추적이 가능하다 (X)

  → OSI 7의 3계층과 4계층에서 관리자가 필터링을 위해 정의한 IP와 Port 목록을 기반으로 필터링 수행하며, 프로그램 사용에 따른 기록 및 감사추적 불가능
- 일반적인 패킷 라우터에 패킷 필터링 기능을 구현한 것을 `스크리닝 라우터(=패킷 필터링 라우터)` 라고 한다.

[2] NAT(Network Address Translation)

- 라우터에 의해 적은 숫자의 유효 IP 주소만으로도 많은 시스템들이 인터넷에 접속할 수 있게 해주는 네트워크 서비스 (O)
- 외부에서 내부 네트워크로 직접적인 접근이 불가능하게 되므로 네트워크 보안효과를 가져올 수 있다. (O)
- NAT은 Layer 4 프로토콜이다. (X)

[3] Stateful 패킷 검사 침입차단 시스템

- 패킷 피터링처럼 패킷 정보를 검토하지만, TCP 연결에 관한 정보를 기록한다.
- `세션 하이재킹` 같은 공격을 방어

[4] Proxy (801번 문제)

- 침입차단 시스템 호스트에서 실행되는 전문화된 application 서버나 서버 프로그램으로서 침입차단 시스템에서 사용되는 베스천 호스트에 설치되어 운영됨

> 💡 Bastion Host : 침입차단 S/W가 설치되어 내/외부 네트워크 사이에서 게이트웨이 역할을 수행하여 철저한 보안 방어 기능이 구축되어 있는 시스템
> - Application 계층에서 동작

[5] 응용 계층 게이트웨이(application level proxy)

- `내부 서버` 보호 목적
- 사용자 응용계층에서 침입차단 시스템 기능 제공

[6] 회선 레벨 게이트웨이(circut-level gateway)

- 응용 계층 게이트웨이는 `내부 서버` 보호 목적이지만, 서킷 레벨(circut level) 게이트웨이는 `내부 네트워크의 호스트` 보호 목적

3. 침입차단시스템의 구축에 따른 분류

(1) 스크리닝 라우터 구조(Screening Router Architecture)

(2) 이중 네트워크 호스트 구조 (Dual-Home HHost Architecture)

(3) 스크린드 호스트 게이트웨이 구조 (Screened Host Gateway)

- 장점
  - `2단계(네트워크, 응용)`로 방어하기 때문에 안전
  - 가장 많이 사용하는 방화벽 시스템이며, 융통성이 좋다. (Dual-Homed 게이트웨이 장점을 그대로 가진다)

- 단점
  - 해커에 의해 screening router의 routing table이 변경되면 방어할 수 없다.
  - 방화벽 시스템 구축 비용 ↑
  - 로그인 정보가 유출되면 내부 네트워크를 보호할 수 없다.

(4) 스크린드 서브넷 구조 (Screened Subnet Architecture)

- 스크리닝 라우터들 사이에 `dual-homed` 게이트웨이가 위치하면서, 인터넷과 내부 네트워크 사이에 **DMZ(Demilitarized Zone)**라는 네트워크 완충지역 열할을 하는 서브넷을 운영

4. iptables

Section 30. VPN

1. VPN(Virtual Private Network)

- 공중 네트워크를 이용하여 사설 네트워크가 요구하는 서비스를 제공할 수 있도록 네트워크를 구성한 것.

[프로토콜 종류]

[2계층 터널링 프로토콜]

- PPTP(Point-to-Point Tunneling Protocol) : MS개발, 일대일 통신만 지원, 사용자 인증, TCP 사용 - PPP인증
- L2F (Layer 2 Fowarding Protocol) : CISCO 개발, 다자간 통신 지원, UDP 사용
- L2TP (Layer 2 Tunneling Protocol) : MS+CISCO (호환성O)

[3계층 터널링 프로토콜]

- IPSec

[개요]

- IP 계층(3계층)의 보안 프로토콜이다. (O) = VPN의 3계층 프로토콜이다. (O)
- 보안 서비스 제공을 위하여 AH와 ESP 기능을 이용한다 (O)

  [AH, Authentication header]

  - 데이터의 **무결성** 보장과 IP 패킷 **데이터 원본 인증**에 사용
  - 인증은 제공하지만, 암호화 기능은 없음
  - AH 헤더에는 전송모드와 터널모드로 나뉘어진다. (O)

  [ESP, Encapsulating Security Payload]

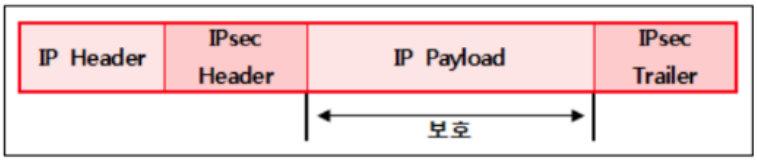
  - 메시지 출처 인증 + 메시지 무결성 + 메시지 기밀성
  - 재전송 공격 방지, 제한된 트래픽 흐름 기밀성
    - 터널모드 : 라우터와 라우터 사이만 암호화

> 💡 IPSec 보안 프로토콜에서 메시지 출처 인증, 메시지 무결성, 메시지 기밀성 서비스를 지원하는 프로토콜과 새로운 IP 헤더가 추가되는 동작모드가 잘 묶여진 것은?
>
> ① ESP 프로토콜, Transport 동작모드
>
> ② ESP 프로토콜, Tunnel 동작모드
>
> ③ AH 프로토콜, Transport 동작모드
>
> ④ AH 프로토콜, Tunnel 동작모드
>
> 정답 : 2번

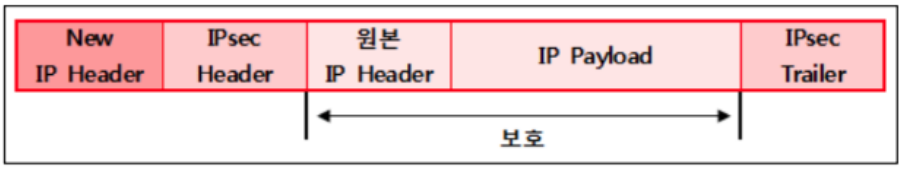
[전송모드, 터널모드]

• 동작 모드 종류

- 전송 모드(Transfer Mode) : 호스트와 호스트간의 메시지(Payload) 무결성을 제공



- 터널 모드(Tunnel Mode) : IP 패킷 전체를 보호하는 모드



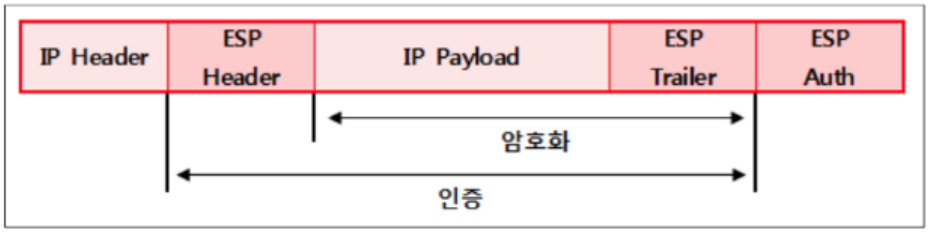
- **전송모드** : 단말과 단말 간에 설정되는 것이 일반적이며 **IP 패킷의 페이로드를 암호화**하여 IP헤더로 캡슐화
- **터널모드**
  - 라우터와 라우터 간에 설정되는 것이 일반적이며 inbound **IP 패킷을 모두 암호화**하여 IPSec AH 또는 ESP 프로토콜을 적용
  - IP 패킷 인증의 범위는 출발지 IP 패킷의 헤더 부분을 포함한다
  - 터널모드는 주로 VPN 기능을 수행하는 게이트웨이 간에 보안 기능을 제공한다. (O)

- 전송모드는 데이터그룹 전체를 AH로 캡슐화하고 새로운 IP헤더를 추가한다. (X)

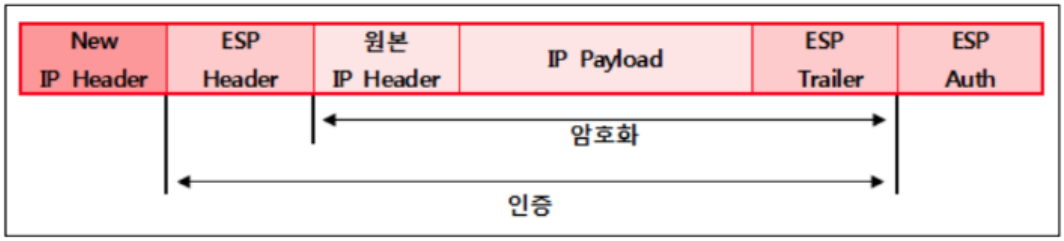
  → AH와 ESP 전송모드 순서 : IP헤더 - AH/ESP 헤더 - IP Payload (IP헤더를 보호하지 않음)

- IETF에 의해 IP 계층 보안을 위해 개방형 구조로 설계된 VPN 기술이다. (O)

- 전송 모드



- 터널 모드



[SSL VPN]

- PPTP(Point-to-Point Tunneling Protocol) : MS개발, 일대일 통신만 지원, 사용자 인증, TCP 사용 - PPP인증
- L2F (Layer 2 Fowarding Protocol) : CISCO 개발, 다자간 통신 지원, UDP 사용
- L2TP (Layer 2 Tunneling Protocol) : MS+CISCO (호환성O)

- 사용하는 프로토콜

  [IKE, Internet Key Exchange]

  - 키 관리 프토토콜, ISAKMP + OAKLEY

Section 31. 최신 네트워크 동향 (1-2문제)

- 각종 네트워크 보안제품의 인터페이스를 표준화하여 중앙 통합 관리
  - EX) 통합 로그 관리, 이벤트 필터링, 시릿간 통합 모니터링/경보/상황전파, 로그 분석 및 의사결정 지원

1. 최신 보안 기술과 솔루션

- ESM(Enterprise Security Management)
- NAC(Network Access Control)
  - 일련의 프로토콜을 사용해 '엔드포인트(Endpoint)'가 처음 내부망 네트워크에 접속시도를 할 때 기존 내부망에 피해를 끼치지 않도록 접속하는 엔드포인트에 일련의 보안정책을 적용할 수 있도록 하는 컴퓨터 네트워킹 솔루션이다.
- APT(Advanced Persistent Threat, 지능형 지속 위협)
  - 특정 대상을 겨냥해 다양한 공격 기법을 이용하여 장기간 지속적으로 공격하는 것
- SIEM(Security Information Event Management)
  - 보안 시스템에서 발생하는 로그를 분석하여 이상 징후 파악하고, 그 결과를 경영진에게 보고할 수 있도록 해주는 시스템
  - QRader, Arcsight, SPLUNK, enVision 와 같은 프로그램 사용

2. 최신 보안 주제

다음은 TCP 프로토콜의 타이머에 대한 설명이다. 옳지 않은 것은?

- ① TCP 타이머에서 재전송 타이머(RTO, Retransmission Time Out)값으로 설정하고 타이머가 끝나기 전에 확인응답이 수신되면 타이머는 소멸한다.

- ② 왕복시간(RTT, Round Trip Time)은 재전송 초과 값을 계산하기 위해서 왕복시간을 계산한다.
- ③ 영속 타이머는 교착상태가 발생한다.
- ④ RTO 값은 최기 RTT 값을 기준으로 항상 고정되어 있다.

정답 : 4, 손실 하면 RTO값을 2배로 늘림

17. 다음의 보기에서 빈칸에 알맞은 용어는 무엇인가?

( )는 /etc/hosts.deny와 /etc/hosts.allow 파일을 통하여 접근 통제를 구현한다.

① TCP Wrapper
② Tripwire
③ SARA
④ NESSUS

정답 : 1

10. 서버 보안을 강화하기 위한 방법으로 서버에 들어오고 나가는 IP 트래픽을 제어할 수 있는 방법은?

① ipchain/iptable
② IP Control/mod_security
③ mod_security/nmap
④ IP Manager/IP Filtering

정답 : 1

6. 다음의 보안 도구 중 무결성 검증용으로 사용하는 것과 가장 거리가 먼 것은?

① tripwire
② fcheck
③ md5
④ nessus

정답 : 4번

nesus : 전 세계적으로 가장 널리 사용하는 취약점 스캔 도구

워너크라이 랜섬웨어와 페트야 랜섬웨어의 차이점을 바르게 설명한 것은?

- ① 워너크라이 랜섬웨어에 네트워크 웜 기능이 추가되었다.
- ② MFT(Master File Table) 영역 암호화가 추가되었다.
- ③ 워너크라이 랜섬웨어와 달리 SMB 취약점을 기반으로 한다.
- ④ MBR(Master Boot Record) 영역을 감염시켜서 부팅을 불가능하게 만든다.

정답 : 4번

페트야 랜섬웨어(Petya Ransomware)

- 2016년 최초 발견
- MFT(Master File Table) 영역 암호화 + MBR(Master Boot Roader) 영역 감염

다음 중 가장 옳지 않은 것은?

- ① wtmp : 사용자들이 로그인, 로그아웃한 정보를 가지고 있다.
- ② pacct : 사용자가 로그인한 후부터 로그아웃할 때까지 입력한 명령과 시간, 작동된 tty 등에 대한 정보를 가지고 있다.
- ③ utmp : 시스템에 현재 로그인한 사용자들에 대한 상태정보를 가지고 있다.
- ④ btmp : 사용자별로 가장 마지막에 로그인한 시간과 접속 IP, tty 등에 대한 정보를 가지고 있다.

정답 : 4번

- 5번 이상 로그인에 실패했을 경우에 로그인 실패정보를 기록, lastb 명령어로 확인가능

다음 보기에서 설명하는 공격은?

```
ㅇ 여러 호스트가 특정 대상에게 다량의 ICMP Echo Request 를 보내게 하여 서비스거부(DoS)를 유발시킨다.
ㅇ 소스 주소를 공격 대상 호스트로 위조한 ICMP 패킷을 브로드캐스트하면 근처의 호스트가 다량의 Echo Reply를 발생시킨다.
```

- ① 세션 하이젝킹 공격
- ② 브로드캐스팅 공격
- ③ Tear Drop 공격
- ④ Smurf 공격

정답 : 4번

- 여러 호스트가 특정 대상에게 다량의 ICMP Echo Request를 보내게 하여 서비스 거부(DoS)를 유발시킨다.
- 소스 주소를 공격 대상 호스트로 위조한 ICMP 패킷을 브로드캐스트하면 근처의 호스트가 다량의 Echo Reply를 발생시킨다.
- 공격 대상 호스트는 다량으로 유입되는 패킷으로 인해 서비스 불능 상태에 빠진다.

다음 중 베스천 호스트에 대한 설명으로 올바른 것은?

- ① 두 개의 스크린 호스트를 이용한다.
- ② 라우터 기능 외에 패킷 통과 여부를 결정할수 있는 스크린 기능을 가지고 있다.
- ③ 두 개의 랜 카드를 가진 호스트를 말한다.
- ④ 보호된 네트워크에 유일하게 외부에 노출되는 내외부 네트워크 연결점으로 사용되는 호스트이다.

40. 다음의 공격 방법을 방어하기 위한 침입차단시스템의 유형으로 가장 적절한 것은?

```
침입차단시스템을 우회하기 위하여 침입차단시스템 내부망에 있는 시스템의 서비스 요청을 받은 것으로 가장하여 패킷을 전송한다.
```

- ① 응용레벨 게이트웨이

- ② 회로레벨 게이트웨이
- ③ 패킷 필터링 라우터
- ④ 상태검사 패킷 필터

다음 중 CIDR 기법을 사용하지 않는 라우팅 프로토콜은?

- ① RIP v1
- ② RIP v2
- ③ EIGRP
- ④ OSPF

정답 : 1

원격지 OS를 탐지하는 방법으로 옳지 않은 것은?

1. telnet ip port 명령을 사용하여 배너 정보를 검토한다.
2. nmap -oX 명령어 이용
3. TCP 초기 시퀀스 넘버를 확인한다.
4. HTTP GET 명령어와 SERVER 키워드를 grep하여 OS를 확인한다.

정답 : 2,

- nmap -oX <파일명> : 스캔결과를 XML로 출력

1. 애니캐스트는 다중 송신자와 그룹 내에서 가장 가까운 곳에 있는 일부 수신자들 사이의 통신을 말한다. (X)

   → 단일 송신자와 그룹 내에서 가장 가까운 곳에 있는 수신자 사이의 통신을 말함.

정리 못한 부분

봇넷(bot-net) 감염된 시스템인 봇이 네트워크로 연결된 형태.

[AH, Authentication header]

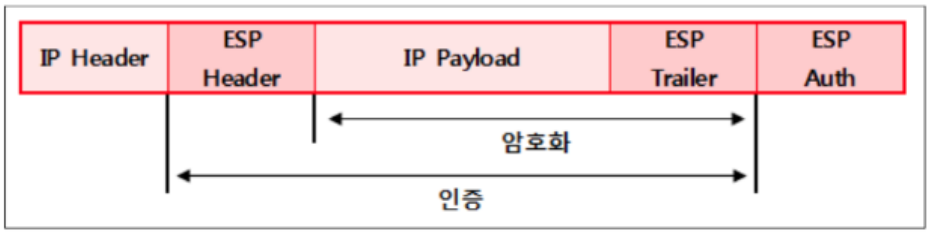
- 데이터의 무결성 보장과 IP 패킷 인증에 사용

[ESP, Encapsulating Security Payload]

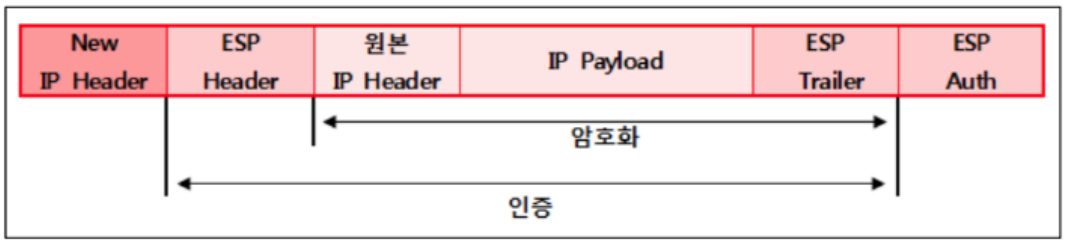
- AH와 동일한 인증 + 기밀성 보장

- 재전송 공격 방지, 제한된 트래픽 흐름 기밀성

- 전송 모드



- 터널 모드



  - 터널모드 : 라우터와 라투어 사이만 암호화