네트워크 해킹 및 보안

국가 공무원 인재 개발원

2022.7.20-7.22

강사 소개

서울에서 출생해 인천 대학교(구 인천 전문 대학) 일어과와 경희 사이버 대학교 정보 통신 학과를 졸업하고 한국 외국어 대학교 교육 대학원에서 **전산 교육학 석사**를 취득했다.

약 9년 동안 한국 통신(KT) 등에서 근무하며 다양한 행정 처리와 정보 기술 환경 등을 경험했다. 사무 처리와 관련해 한자 능력 2급 등을 취득했고 정보 기술과 관련해 **정보 처리 산업 기사/정보 보안 산업 기사**와 CCNA/CCNP 등과 같은 자격증을 취득했다. 또한 **교원 2급 자격증과 직업 능력 개발 훈련 교사 3급 자격증** 등을 취득했다.

지난 2004년부터 현재까지 국가 공무원 인재 개발원과 서울시 인재 개발원 등에서 **정보 보안 기사 자격증과 모의 침투 분야 등을 강의 중**이다. 지난 2016년 경찰 인재 개발원(구 경찰 교육원)에서 우수 외래 강사로 감사장을 받았다. 사이버 보안 중 다양한 모의 침투 운영 체제와 사회 공학 등에 특히 관심이 많다.

강의가 없을 때에는 문학•사학•철학 등에 대한 책을 읽거나 국가 정보학 등과 같은 책을 읽는다. 페이스북에서 **모의 침투 연구회(www.facebook.com/groups/metasploits)**와 **사이버 안보 연구회(www.facebook.com/groups/koreancyberwar)** 등을 개설해 활동 중이다.

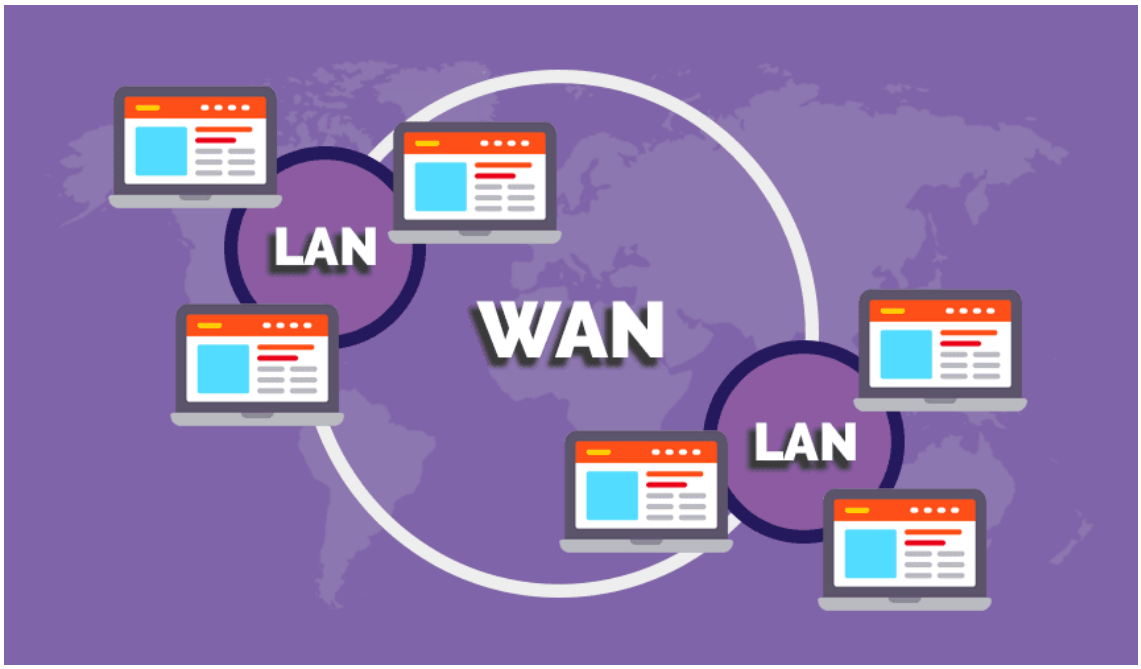
2015년부터 2019년까지 **에이콘 출판사**를 통한 저서로는 **<<해킹 입문자를 위한 TCP/IP 이론과 보안>>•<<칼리 리눅스 입문자를 위한 메타스플로잇 중심의 모의 침투>>•<<백박스 리눅스를 활용한 모의 침투>>•<<해커의 언어 파이썬 3 입문>>•<<소켓 개발 입문자를 위한 백박스 기반의 파이썬 2.7>>** 등이 있고, 공저로는 **<<데비안 리눅스 활용과 보안>>•<<우분투 리눅스 기반의 IDS/IPS 설치와 운영>>•<<모의 침투 입문자를 위한 파이썬 3 활용>>** 등이 있다.

雖不足藏之名山 庶無使墁之醬瓿[비록 명산에 비장할 바는 아니오나 간장 항아리 덮개로는 사용하지 말아 주시옵소서.]

김부식(金富軾)의 <<삼국사기(三國史記)>> 서문 편에서

제1장 TCP/IP 보안을 이해하기 위한 선수 내용

1. LAN 영역과 WAN 영역



(1) LAN 영역

1) MAC 주소에 기반해 내부에서 통신하기 위한 스위칭 공간

2) 이더넷•토큰 링•FDDI•ATM 등과 같은 프로토콜을 사용

(2) WAN 영역

1) IP 주소에 기반해 외부와 통신하기 위한 라우팅 공간

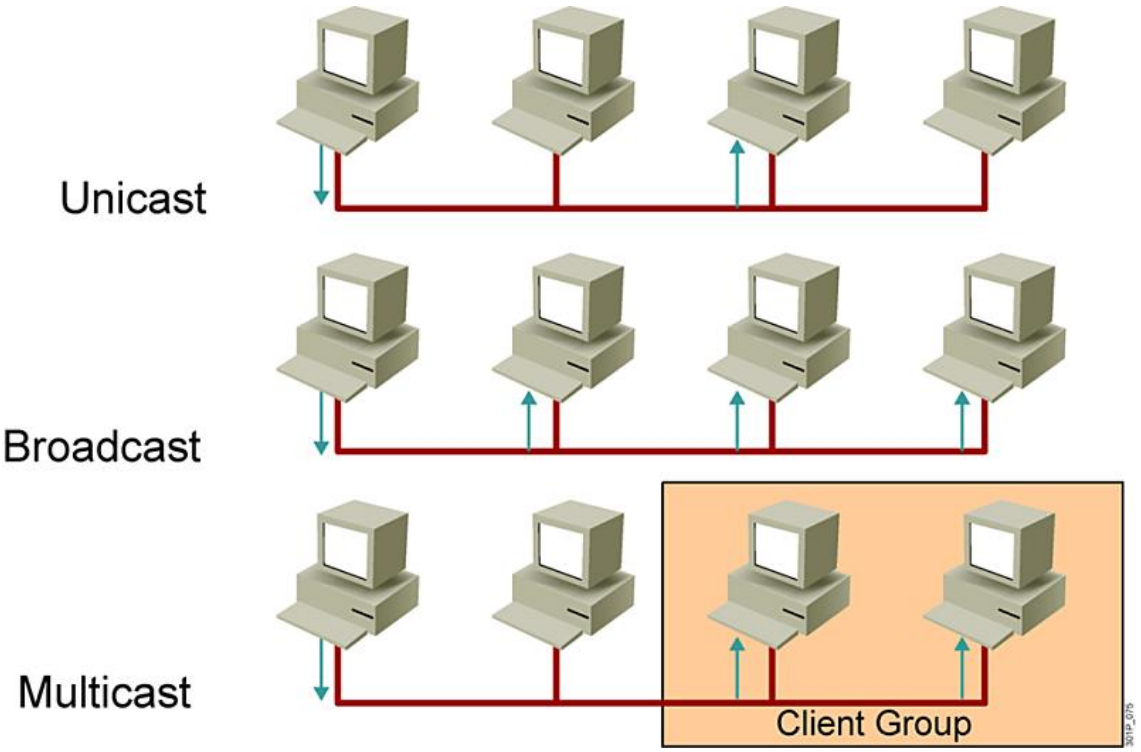
2) 다시 말해, 라우팅이란 IP 주소에 기반해 자신과 상이한 LAN 영역까지 도달할 수 있는 무수한 경로 중 최상의 경로를 구현하는 기능 또는 기법을 의미

3) RIP•OSPF•ISIS•EIGRP 등과 같이 자신의 기준에 따라 최상의 경로를 구하기 위한 라우팅 알고리즘이 필요

4) HDLC•PPP•X.25•프레임 릴레이•ATM 등과 같은 프로토콜을 사용

2. 통신의 개념

(1) 전송



1) 유니캐스트 전송

2) 브로드캐스트 전송

3) 멀티캐스트 전송

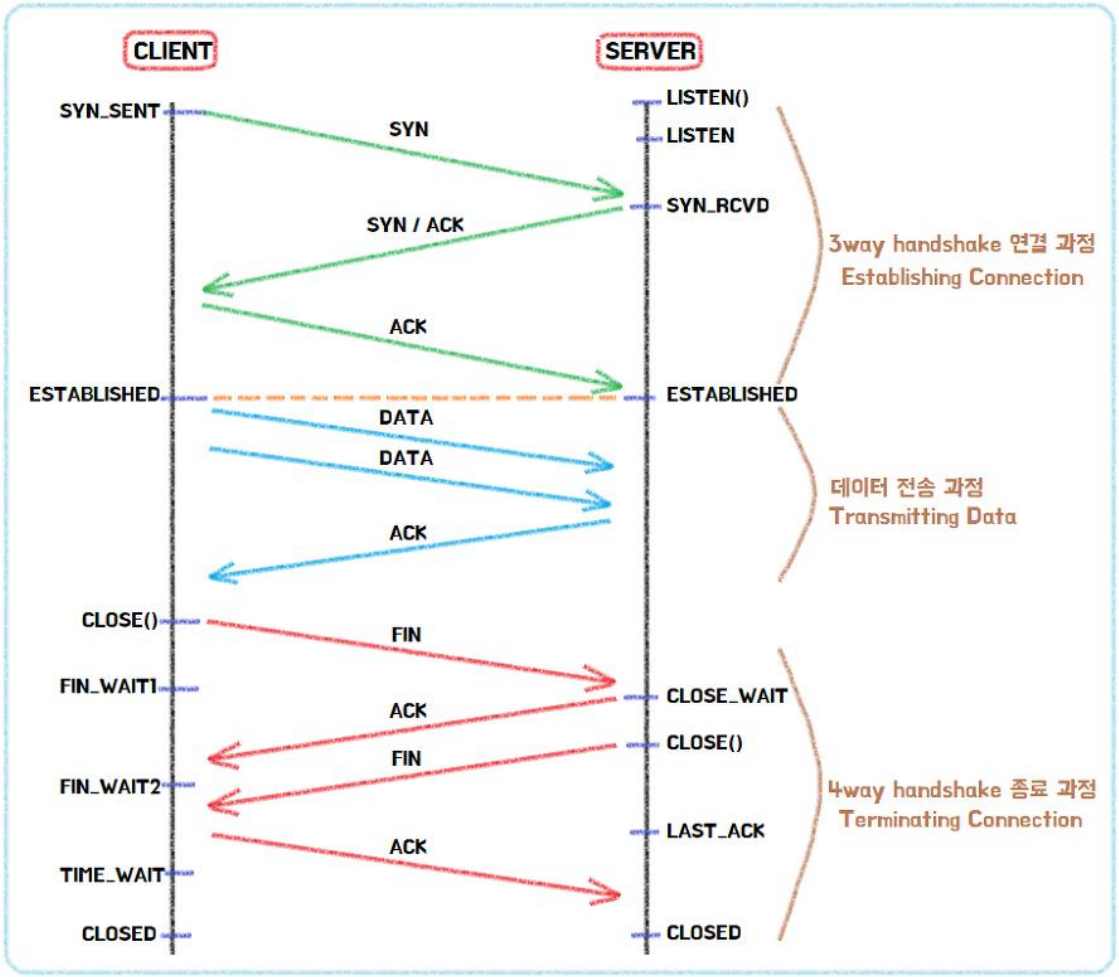
(2) 제어

일련의 흐름이기 때문에 기계적으로 분리는 불가능

1) 연결 제어

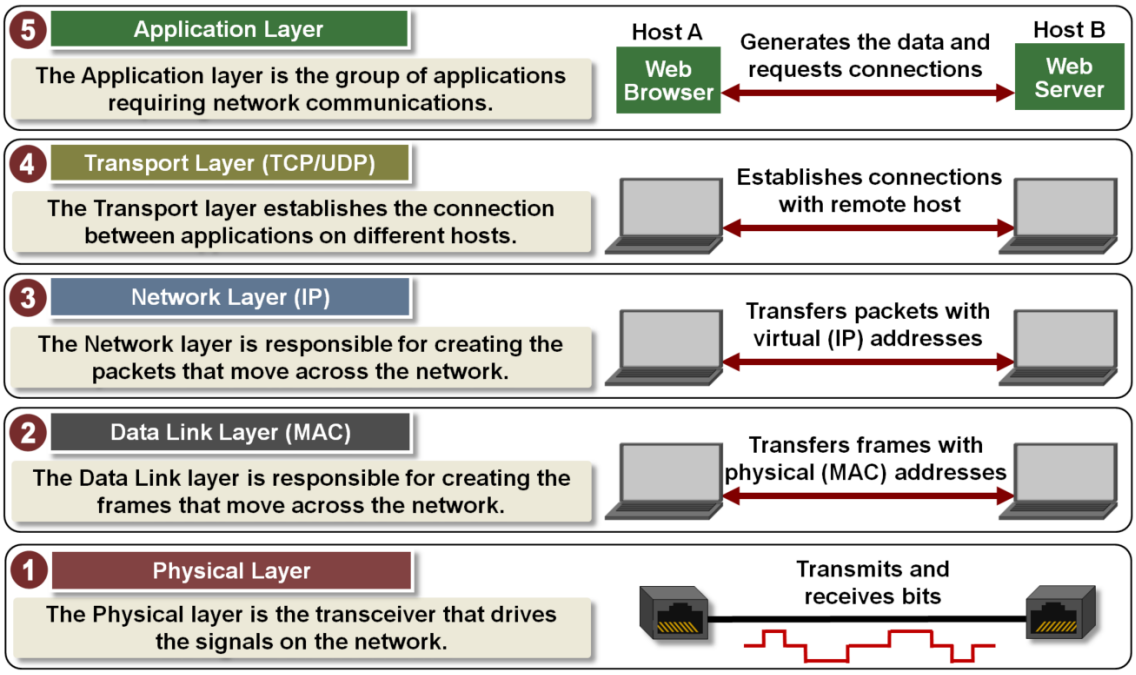
2) 전송 및 흐름 제어

3) 종료 제어


CLIENT
SERVER
SYN_SENT
SYN
LISTEN()
LISTEN
SYN_RCVD
SYN / ACK
ACK
3way handshake 연결 과정
Establishing Connection
ESTABLISHED
ESTABLISHED
DATA
DATA
ACK
데이터 전송 과정
Transmitting Data
CLOSE()
FIN
FIN_WAIT1
CLOSE_WAIT
ACK
CLOSE()
FIN
FIN_WAIT2
LAST_ACK
ACK
4way handshake 종료 과정
Terminating Connection
TIME_WAIT
CLOSED
CLOSED

제2장 TCP/IP 방식의 총론

1. TCP/IP 방식의 개요



(1) 인터넷 표준 프로토콜로서 TCP/IP 방식

1) 빈튼 서프와 밥 칸과 로버트 칸 등이 1973년부터 개발

2) TCP/IP 방식은 다양한 프로토콜의 집합체를 의미

(2) 전송 단위의 계층별 종류

편지지	편지 봉투

1) 응용 계층

UDP 페이로드

메시지 단위

2) 전송 계층

UDP 페이로드	UDP 헤더

데이터그램 또는 세그먼트로 단위

3) 네트워크 계층

UDP 페이로드	UDP 헤더	IP 헤더

패킷 단위

4) 데이터 링크 계층

UDP 페이로드	UDP 헤더	IP 헤더	이더넷 헤더

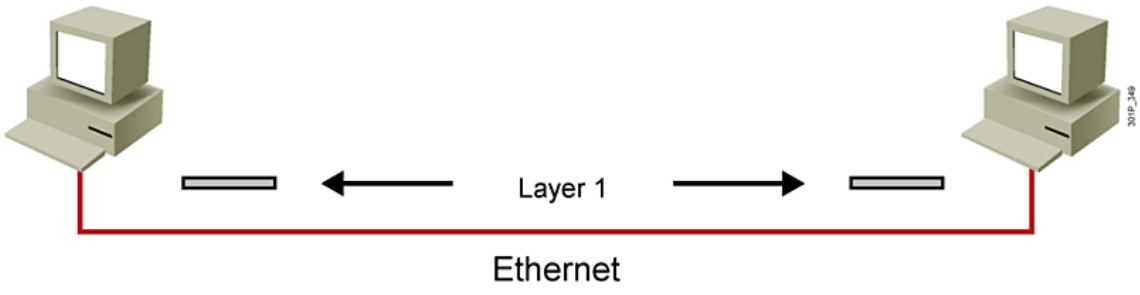
프레임 단위 또는 셀 단위

5) 물리 계층

비트 단위

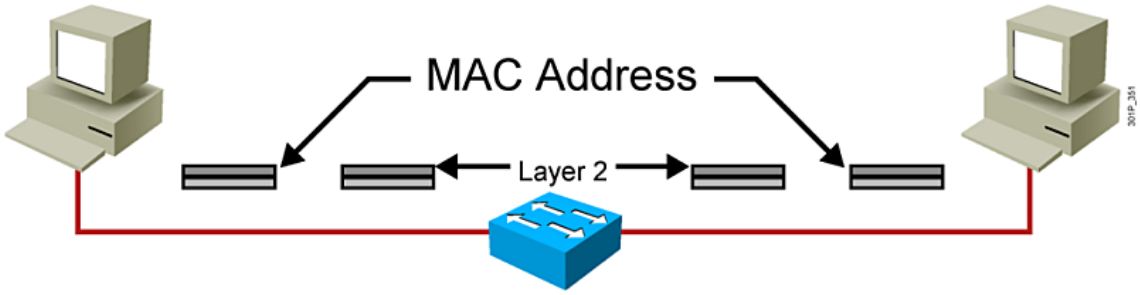
2. TCP/IP 방식에 따른 장비 분류 및 동작 방식

(1) 1계층 장비



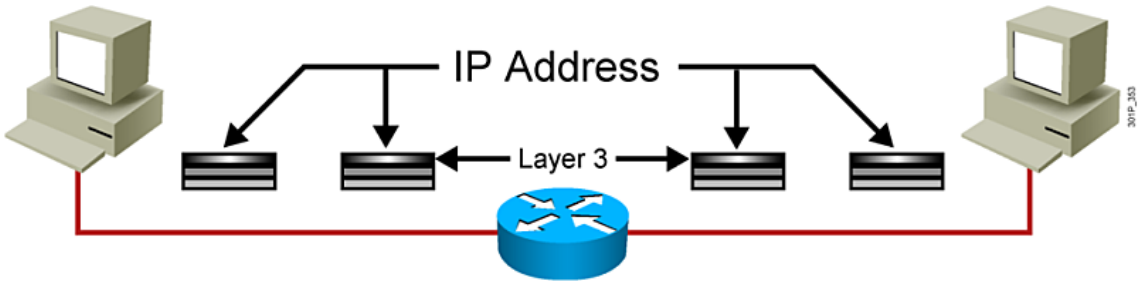
허브 장비와 같이 비트 단위를 처리하는 장치

(2) 2계층 장비



스위치 장비 또는 무선 AP 장비와 같이 프레임 단위를 처리하는 장치

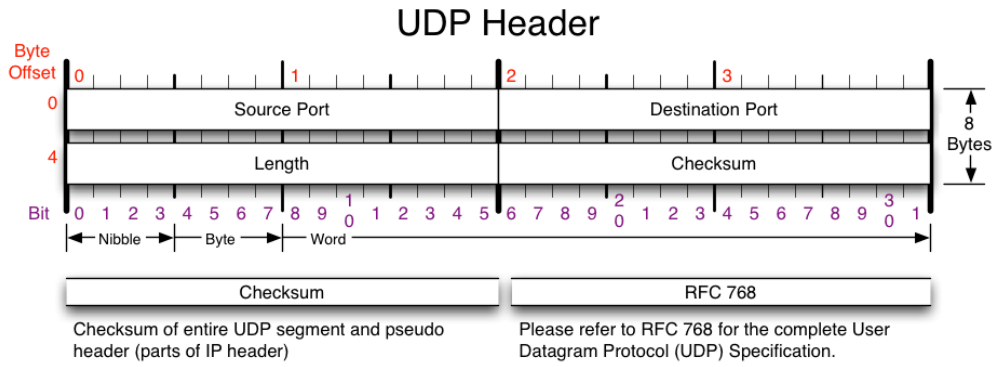
(3) 3계층 장비



라우터 장비와 같이 패킷 단위를 처리하는 장치

제3장 TCP/IP 전송 계층의 헤더

1. UDP 방식의 특징



(1) 버퍼링 기능이 없는 개념

(2) 단편화가 없는 데이터그램 단위로 전송

(3) 일반적으로 512 바이트 미만의 데이터를 전송

2. TCP 방식의 특징

(1) 버퍼링 기능이 있는 개념

(2) 단편화가 있는 세그먼트 단위로 전송

(3) 일련의 제어 과정

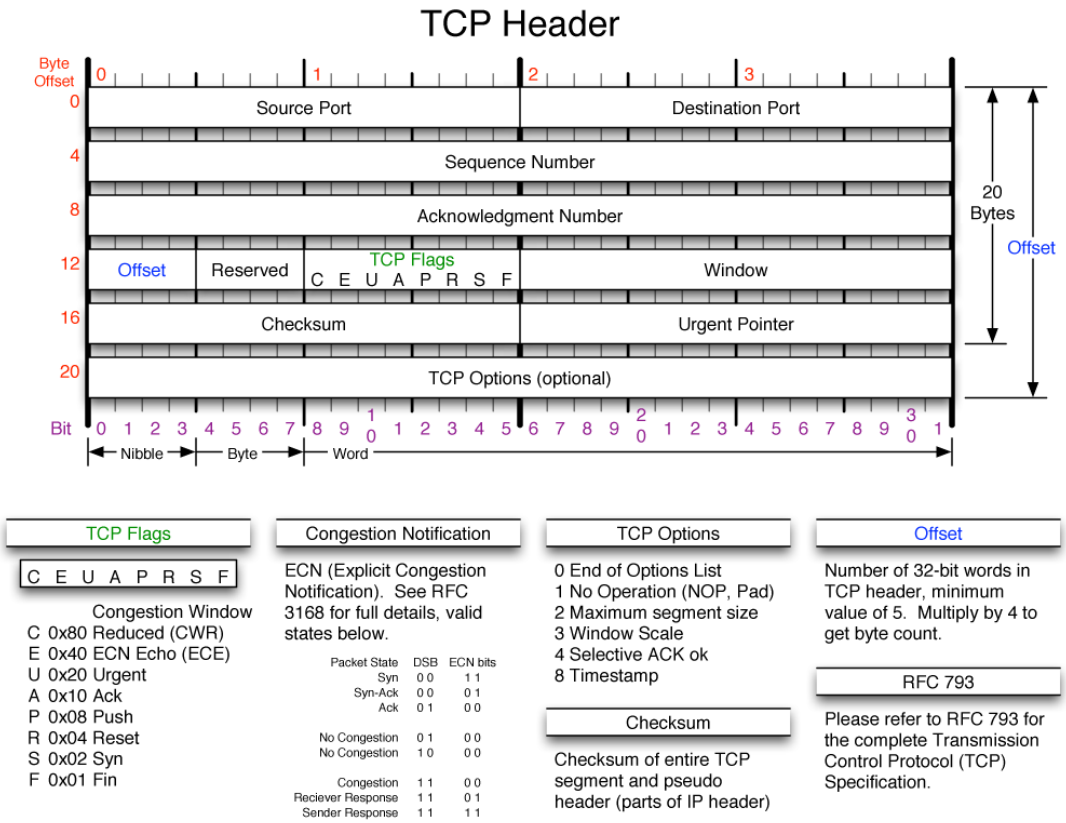
1) 전송 전 3단계 연결 설정 과정

2) 전송 중 오류 발생

송신자는 수신자로부터 ACK 신호를 받아야만 다음 정보를 전송하는데 이를 네글 알고리즘이고 함

3) 흐름 제어

송신자는 수신자의 확인 응답에 따라 전송할 정보의 양을 조절하는데 이를 혼잡 윈도우라고 하며 송신자가 전송할 수 있는 동적인 정보의 양을 슬라이딩 윈도우라고 함



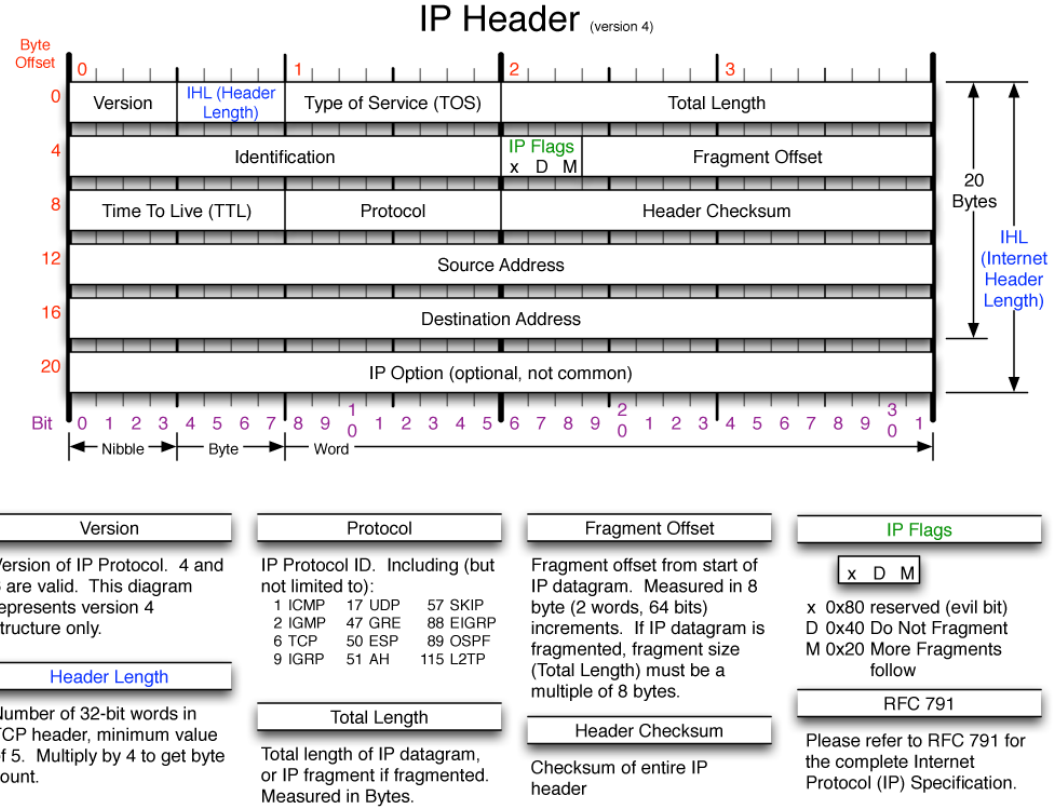
4) 전송 후 3/4단계 연결 종료 과정

(4) 전송 전 3단계 연결 설정 과정과 전송 후 3/4단계 연결 종료 과정은 연속적인 동작

(5) RTO 타이머란 전송 실패한 데이터를 재전송하기 위한 타임아웃

제4장 TCP/IP 네트워크 계층의 헤더

1. IP 헤더



(1) MTU 개념 및 종류

이더넷 방식은 1500 바이트이고 PPP 방식은 약 300 바이트

(2) IP 플래그 항목의 구성

1) D 비트가 0이면 분할이고 1이면 미분할을 의미

2) M 비트가 1이면 분할의 연속이고 0이면 분할의 종료를 의미

(3) 패킷 분할의 예

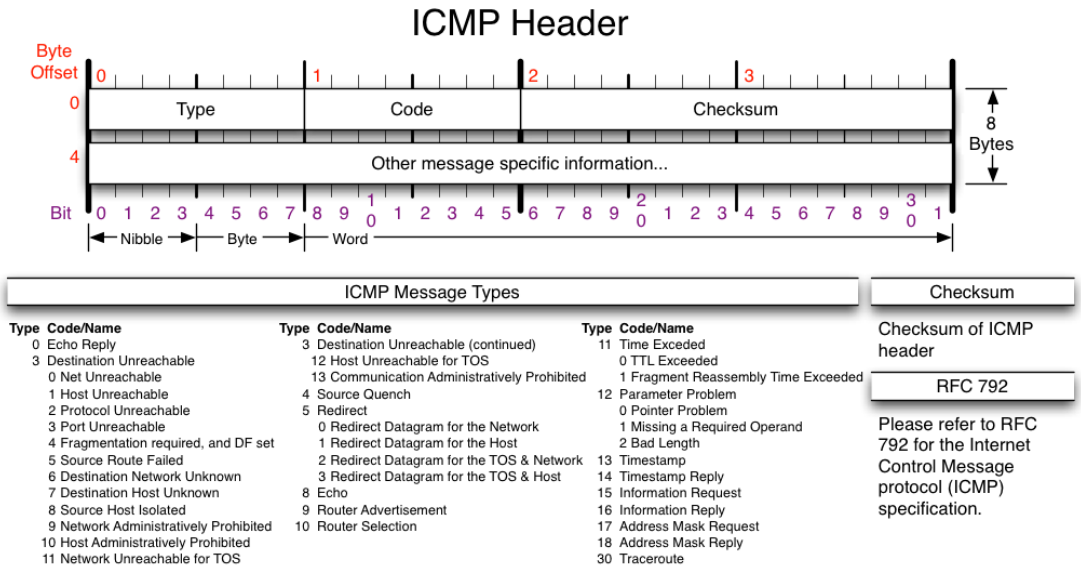
1) 1,500 바이트 패킷의 경우

ID 항목	플래그 항목(D 비트)	플래그 항목(M 비트)	플래그먼트 오프셋
Null	1	Null	Null

2) 6,000 바이트 패킷의 경우

ID 항목	플래그 항목(D 비트)	플래그 항목(M 비트)	플래그먼트 오프셋
1234	0	1	0
1234	0	1	1500
1234	0	1	3000
1234	0	0	4500

2. ICMP 헤더



(1) 오류 통보 기능

(2) 질의와 응답 기능

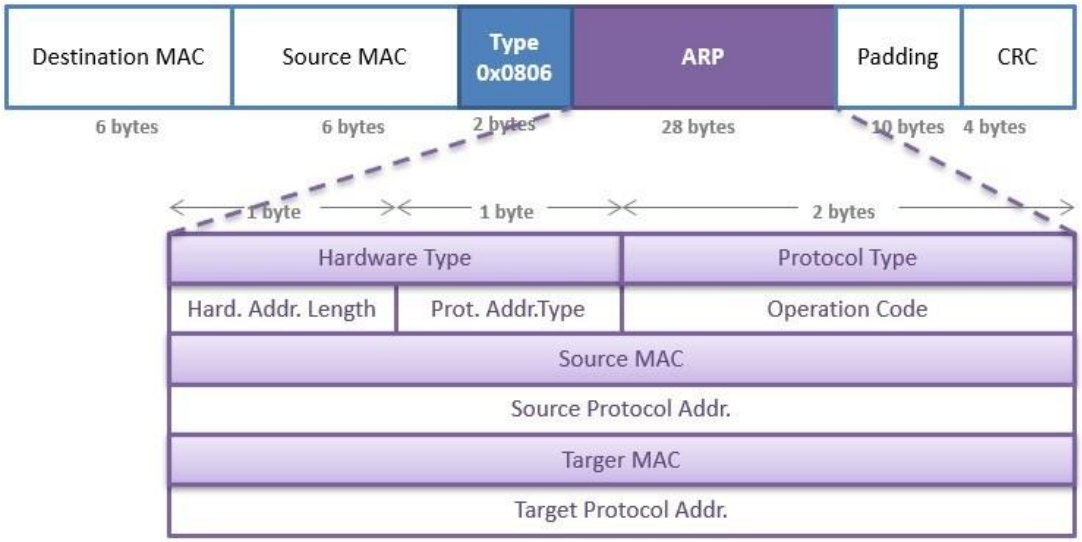
제4장 TCP/IP 데이터 링크 계층의 헤더

1. ARP 방식의 기능과 구조

(1) ARP 방식의 기능

상대방 IP 주소에 기반해 자기가 속한 LAN 영역에서 상대방 MAC 주소를 구하는 기능을 수행

(2) ARP 헤더의 구조



1) 하드웨어 유형

해당 LAN 영역에서 사용하는 프로토콜의 유형을 정의

2) 프로토콜 유형

TCP/IP 네트워크 계층에서 사용하는 프로토콜의 유형을 정의

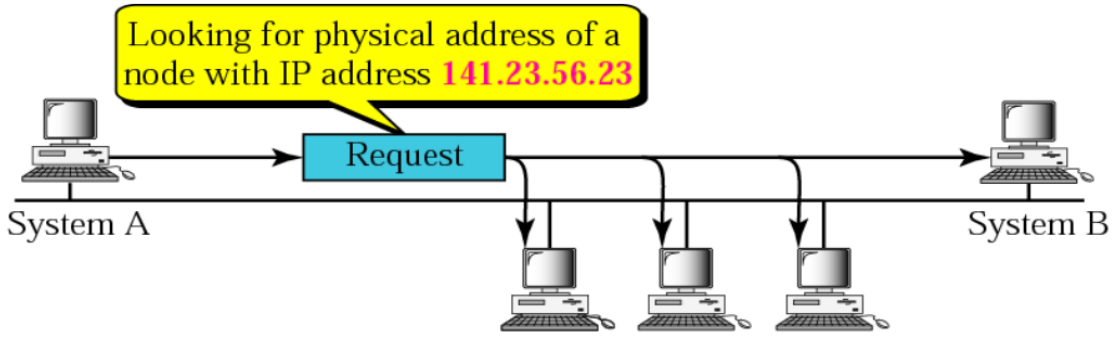
3) 하드웨어 주소 길이

4) 프로토콜 주소 길이

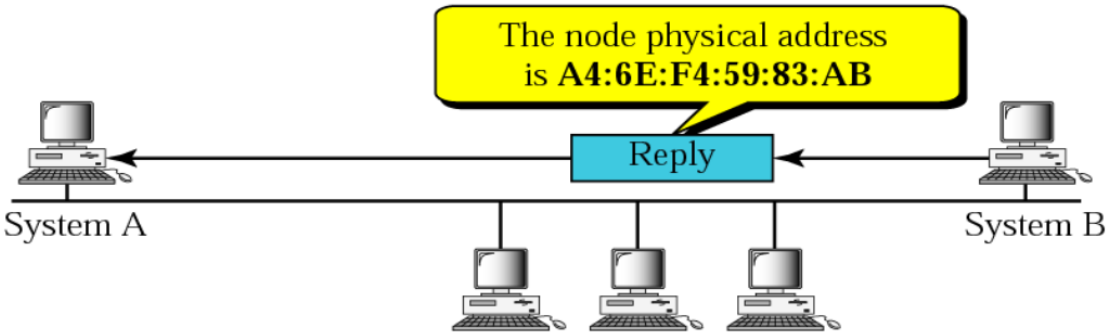
5) 동작 코드

1은 요청이고 2는 응답

2. ARP 방식의 동작 순서



a. ARP request is broadcast



b. ARP reply is unicast

(1) 송신자는 목적지 IP 주소에 대응하는 목적지 MAC 주소를 구하기 위해 라우터를 포함한 동일한 LAN 영역에 속한 모든 호스트를 대상으로 브로드캐스트 방식에 따라 ARP 요청

(2) 수신자는 자신의 MAC 주소를 유니캐스트 방식으로 ARP 응답

(3) 송신자는 ARP 캐시 테이블에 해당 목적지 MAC 주소를 등록시킨 뒤 유니캐스트 방식으로 실제 정보를 수신자에게 전송

```
# cat /proc/net/arp
IP address       HW type     Flags       HW address            Mask     Device
```

```
192.168.10.1      0x1         0x2         00:50:56:c0:00:08     *        eth0
192.168.10.220    0x1         0x2         00:0c:29:c8:66:0d     *        eth0
192.168.10.2      0x1         0x2         00:50:56:ec:c3:ba     *        eth0
```

제5장 TCP/IP 네트워크 공격 유형

1. 프린팅 또는 배너 그래빙 공격

```
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-116-generic i686)

Last login: Mon May 21 14:48:12 2018 from 192.168.10.1
root@debian:~#
```

2. 포트 스캔 공격

해당 포트가 닫힌 경우에는 ACK + RST(RST + ACK) 플래그로 응답

(1) TCP Full Open 스캔 방식

```
root@debian:~# nmap 127.0.0.1 -p 22 --reason -sT

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 10:37 KST
Nmap scan report for localhost (127.0.0.1)
Host is up, received localhost-response (0.00095s latency).

PORT    STATE SERVICE REASON
22/tcp open  ssh     syn-ack
```

(2) TCP Half Open 스캔 방식

```
root@debian:~# nmap 127.0.0.1 -p 22 --reason -sS

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 10:38 KST
Nmap scan report for localhost (127.0.0.1)
Host is up, received localhost-response (0.000057s latency).

PORT    STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
```

(3) FIN 스캔 방식

```
root@debian:~# nmap 127.0.0.1 -p 22 --reason -sF

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 10:39 KST
Nmap scan report for localhost (127.0.0.1)
Host is up, received localhost-response.

PORT    STATE         SERVICE REASON
22/tcp open|filtered ssh     no-response
```

SYN 플래그를 차단한 방화벽 등을 통과하기 위한 기법

(4) X-mas 스캔 방식

```
root@debian:~# nmap 127.0.0.1 -p 22 --reason -sX

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 10:39 KST
Nmap scan report for localhost (127.0.0.1)
Host is up, received localhost-response.

PORT    STATE         SERVICE REASON
22/tcp open|filtered ssh     no-response
```

SYN 플래그를 차단한 방화벽 등을 통과하기 위한 기법

(5) Null 스캔 방식

```
root@debian:~# nmap 127.0.0.1 -p 22 --reason -sN

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 10:40 KST
Nmap scan report for localhost (127.0.0.1)
Host is up, received localhost-response.

PORT    STATE         SERVICE REASON
22/tcp open|filtered ssh     no-response
```

SYN 플래그를 차단한 방화벽 등을 통과하기 위한 기법

3. 스푸핑 공격

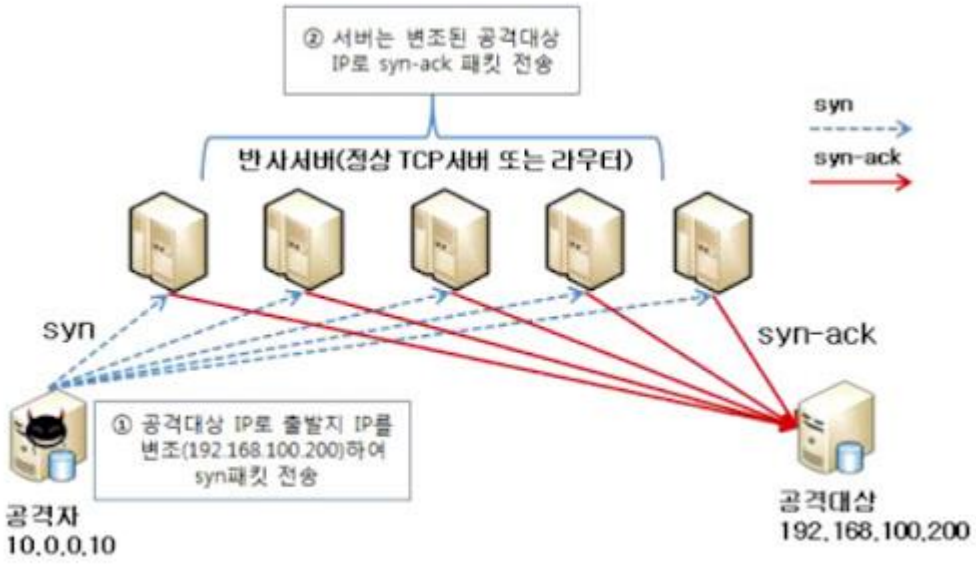
(1) ARP 스푸핑 공격

(2) IP 스푸핑 공격

(3) DNS 스푸핑 공격

4. 플러딩 공격

좀비 시스템 종류에 따라 Syn DDoS 공격과 Syn DRDoS 공격으로 구분



▲DRDoS 공격방식(출처: 한국인터넷진흥원)

(1) 랜드 공격

(2) 티얼드롭 공격

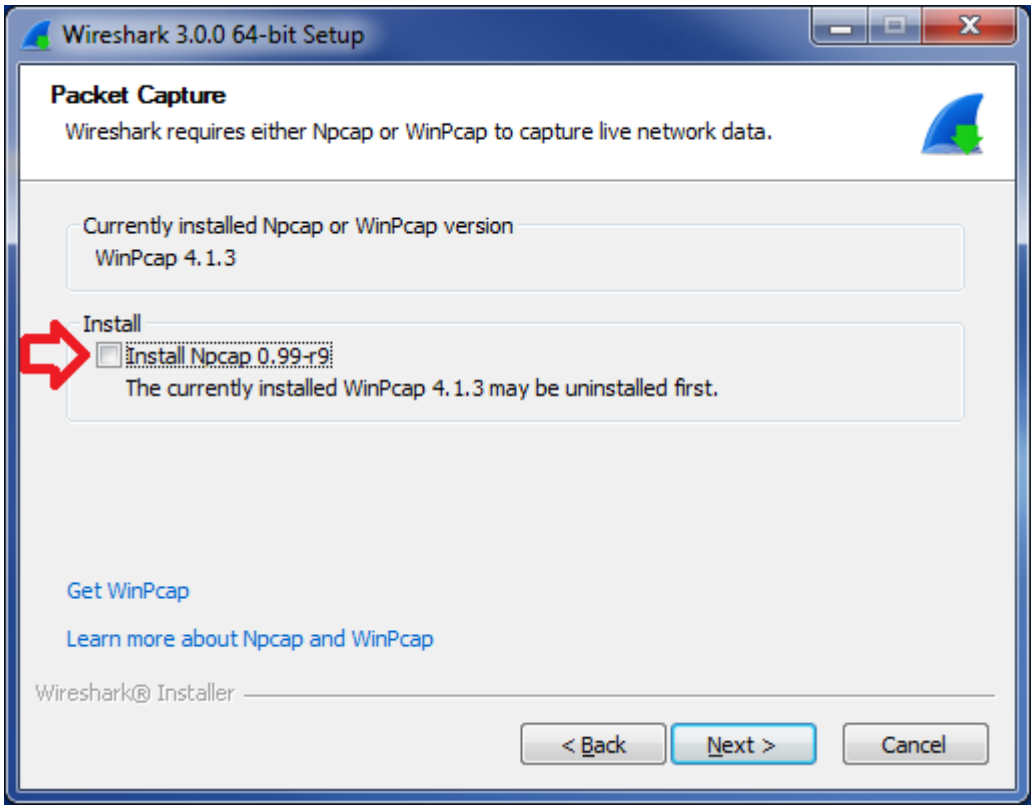
(3) ICMP 플러딩 공격

(4) ICMP 스머프 또는 ICMP 증폭 공격

(5) TCP SYN 플러딩 공격

(6) TCP 본크•보잉크 공격

5. 스니핑 공격



무작위(promiscous) 모드란 프레임 헤더의 목적지 MAC 주소와 LAN 카드의 MAC 주소를 비교한 뒤 두 개의 주소가 상이하더라도 LAN 카드가 해당 프레임을 수신하는 동작

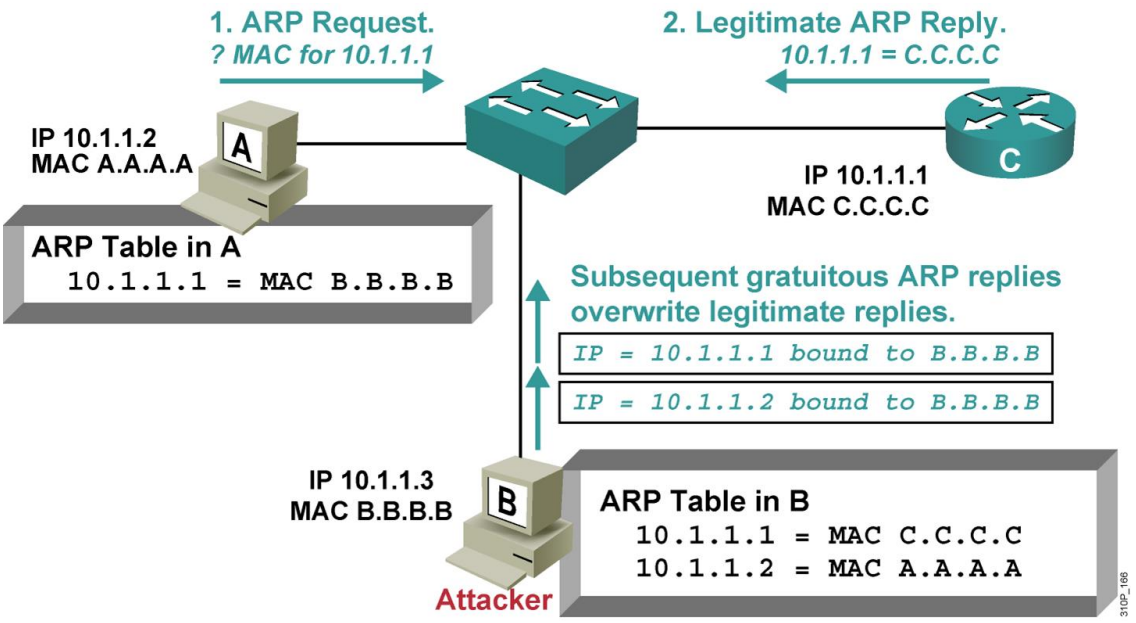
```
root@debian:~# ifconfig eth0 promisc
root@debian:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:91:39:80
          inet addr:192.168.10.215  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe91:3980/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:1578 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1593 errors:0 dropped:0 overruns:0 carrier:0
```

```
          collisions:0 txqueuelen:1000
          RX bytes:317233 (317.2 KB)  TX bytes:184616 (184.6 KB)
          Interrupt:18 Base address:0x2000

root@debian:~# ifconfig eth0 -promisc
root@debian:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:91:39:80
          inet addr:192.168.10.215  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe91:3980/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1603 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1623 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:320009 (320.0 KB)  TX bytes:190124 (190.1 KB)
          Interrupt:18 Base address:0x2000
```

제6장 TCP/IP 방식의 계층별 취약점에 기반한 공격 유형

1. 데이터 링크 계층에서 ARP 스푸핑 공격

(1) 동일한 LAN 영역에서 라우터 MAC 주소 등을 조작하는 기법으로 각종 스니핑 공격을 위한 전제로 수행하는 대표적인 중간자 개입(MITM) 공격




```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# arpspoof -t 10.1.1.2 -r 10.1.1.1
```

(2) IP 주소와 MAC 주소를 고정하는 방식으로 방어

```
C:₩>arp -s 10.1.1.1 C.C.C.C
```

2. 네트워크 계층에서 공격 유형

(1) IP 스푸핑 공격

1) TCP 연결 하이재킹 공격 과정에서 등장

2) 출발지의 IP 주소를 제거하거나 조작하여 상대방으로 하여금 자신을 은폐하는 기법으로 일종의 NAT 기법

3) 방화벽 설정을 통해 방어

(2) 랜드 공격

1) IP 스푸핑 공격의 변형으로 출발지 IP 주소와 목적지 IP 주소를 동일하게 설정하는 일종의 플러딩 공격

2) 들어오는 패킷 헤더에서 출발지 IP 주소와 목적지 IP 주소가 동일하면 차단

(3) 티얼드롭 공격

1) 패킷 분할이 발생할 때 IP 헤더의 오프셋 항목을 조작해 수신자로 하여금 정상적인 재조립 과정을 방해하는 일종의 플러딩 공격

ID 항목	플래그 항목(D 비트)	플래그 항목(M 비트)	플래그먼트 오프셋
1234	0	1	0
1234	0	1	1500
1234	0	1	1500
1234	0	0	4500

2) 운영 체제 차원에서 시간에 기반한 임계치 방식으로 차단

(4) ICMP 플러딩 공격 또는 죽음의 핑 공격

1) 65,535 바이트 크기 이상의 ICMP 요청을 연속적으로 전송하는 플러딩 공격

```
root@kali:~# hping3 192.168.10.215 -a 192.168.10.215 --icmp --flood -d 65000 &
root@kali:~# tcpdump -e icmp[icmptype] == 8
```

2) 운영 체제의 ICMP 기능 중지 등으로 방어

```
root@debian:~# echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all
root@debian:~# tcpdump -e icmp[icmptype] == 0
```

3) 방화벽 설정을 통해 방어

(5) ICMP 스머프 또는 ICMP 증폭 공격

```
root@debian:~# echo 0 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
root@debian:~# ping 192.168.10.255 -b
```

1) IP 스푸핑 공격의 변형으로서 DRDoS 공격의 시조

2) 출발지 IP 주소 항목에 공격 대상자의 IP 주소를 설정하고, 목적지 IP 주소 항목에 다이렉티드 브로드캐스트 IP 주소 255를 포함하도록 설정해 ICMP 요청을 전송하는 일종의 플러딩 공격

```
root@kali:~# hping3 192.168.10.255 -a 192.168.10.215 --icmp --flood -d 65000 &
root@kali:~# tcpdump -e icmp[icmptype] == 8
```

3) 방화벽 설정을 통해 방어

3. 전송 계층에서 공격 유형

(1) TCP SYN 플러딩 공격

```
root@kali:~# hping3 192.168.10.215 -a 192.168.10.219 -p 22 -S --flood &
root@kali:~# tcpdump "tcp[tcpflags] & (tcp-syn) != 0"
```

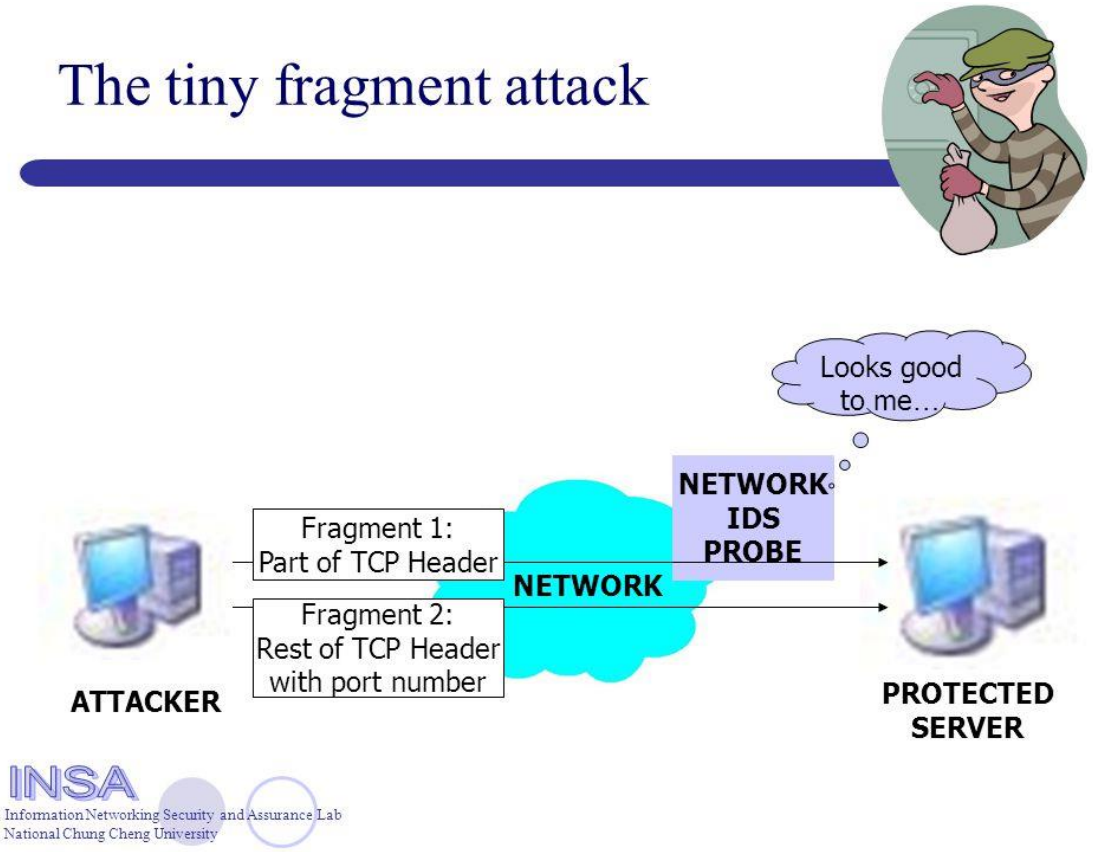
1) 연결 요청에 대한 임계치 설정[재시작 시 설정 해제]

```
root@debian:~# sysctl -a | egrep "tcp_max_syn_backlog"
net.ipv4.tcp_max_syn_backlog = 128

root@debian:~# sysctl -w net.ipv4.tcp_max_syn_backlog=1024
net.ipv4.tcp_max_syn_backlog = 1024

root@debian:~# sysctl -a | egrep "net.ipv4.tcp_max_syn_backlog"
net.ipv4.tcp_max_syn_backlog = 1024
```

2) L4 스위치 장비 등을 이용한 부하 분산 처리

(2) Tiny Fragment 공격

IP 주소/포트 번호 기반의 보안 장비 우회 목적

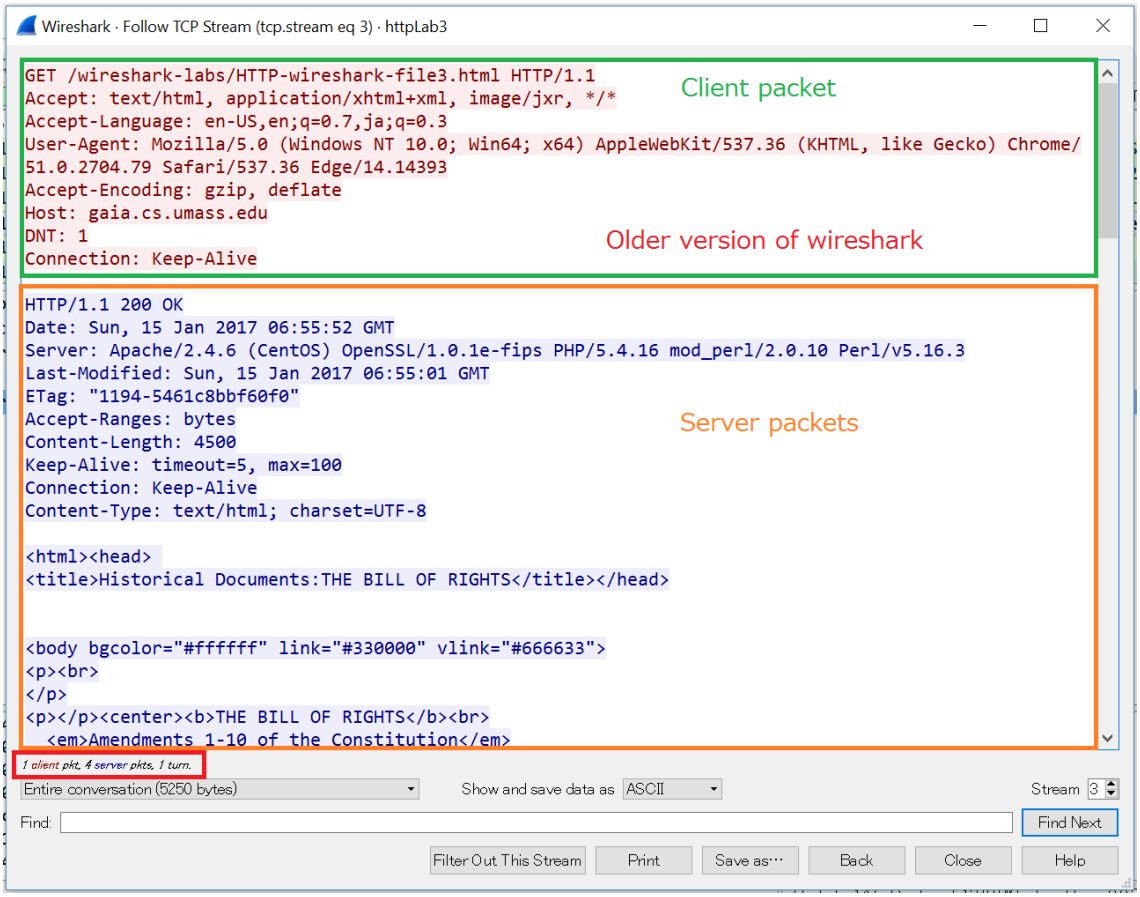


(3) TCP 본크•보잉크 공격

1) TCP 헤더의 일련 번호 항목을 조작하여 수신측에서 재조립할 때 과부하를 유발시키는 기법으로 일종의 플러딩 공격

2) 운영 체제 차원에서 시간에 기반한 임계치 방식으로 차단

3. 응용 계층에서 공격 유형

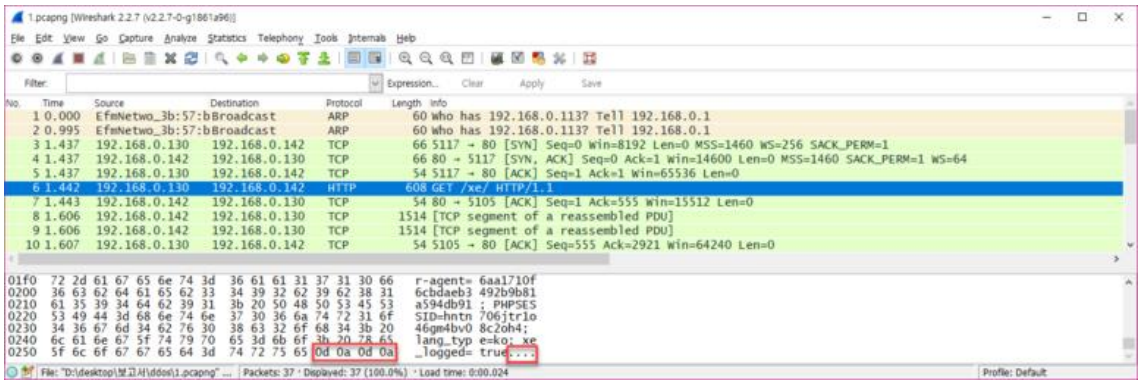


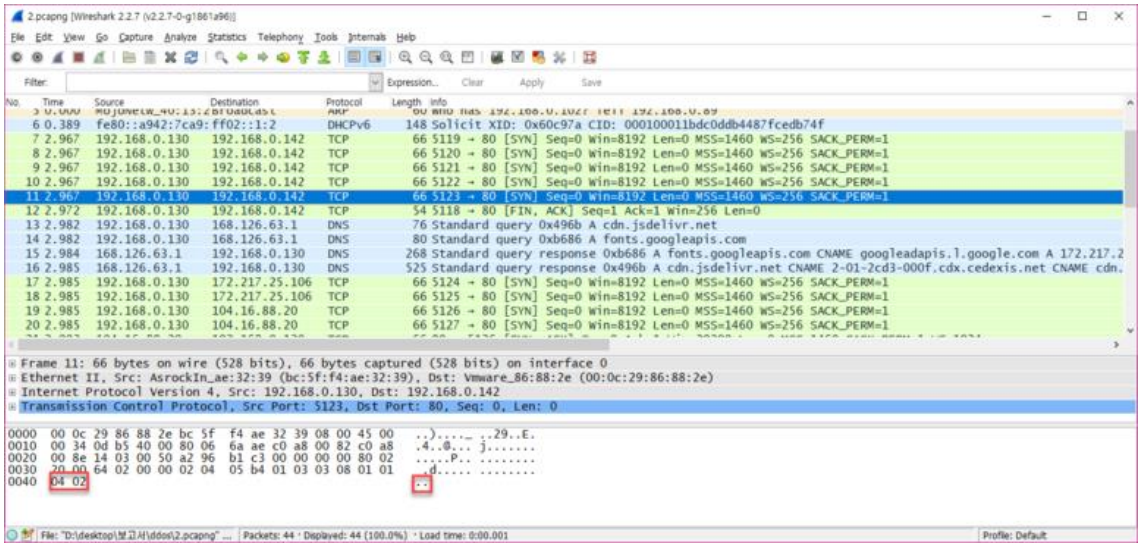
(1) HTTP GET 플러딩 공격

1) 서버에게 반복적으로 기본 페이지를 요청

2) 타임아웃에 기반한 임계치 설정을 통해 방어

(2) 슬로우 로리스(Slow Loris) 공격

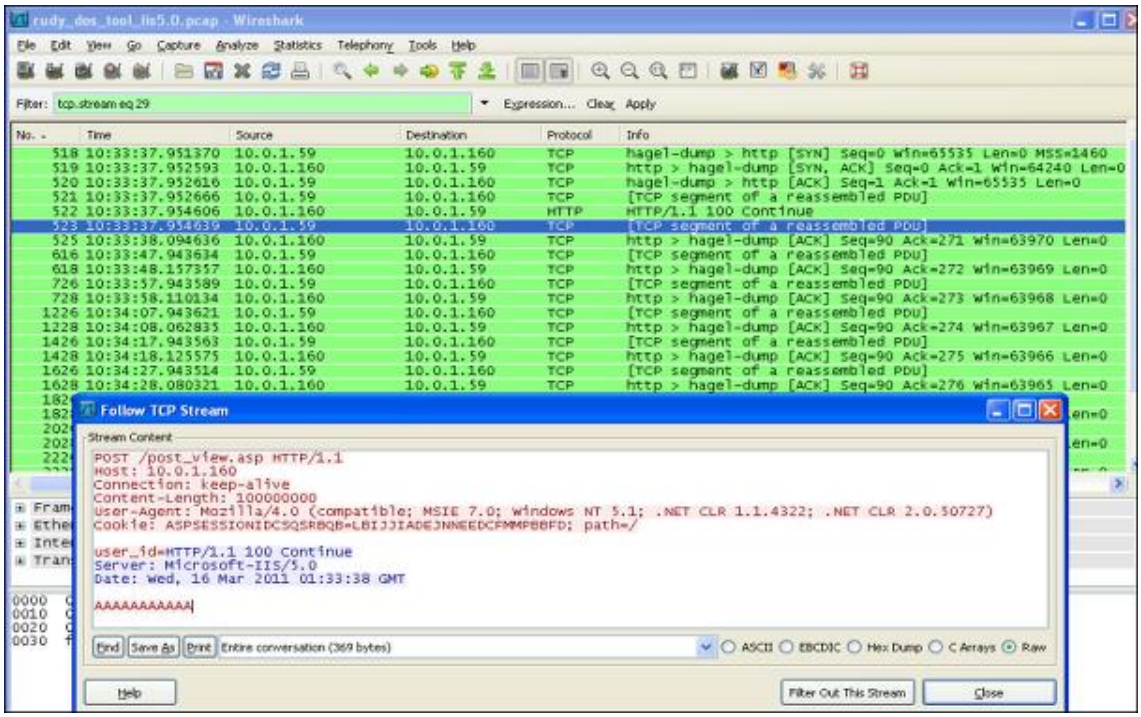




1) HTTP 헤더와 HTTP 바디 사이의 경계를 ₩r₩n(0d0a) 등과 같이 애매하게 설정해 반복적으로 전송하면 서버가 헤더 정보를 완전히 수신할 때까지 연결을 유지

2) 타임아웃에 기반한 임계치 설정을 통해 방어

(3) 러디(Rudy) 공격



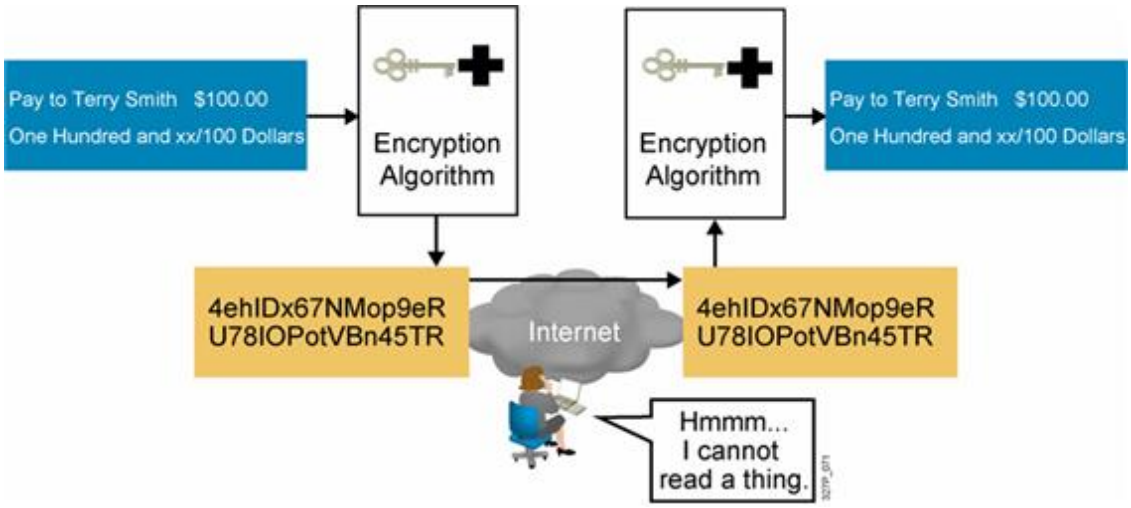
1) content-length 항목에 기반해 서버로 대량의 데이터를 전송할 때 장시간 동안 분할 전송

2) 타임아웃에 기반한 임계치 설정을 통해 방어

제7장 사이버 보안의 구성 요소

가상 공간에서는 송신자와 수신자의 대면이 없다는 가정이 필요

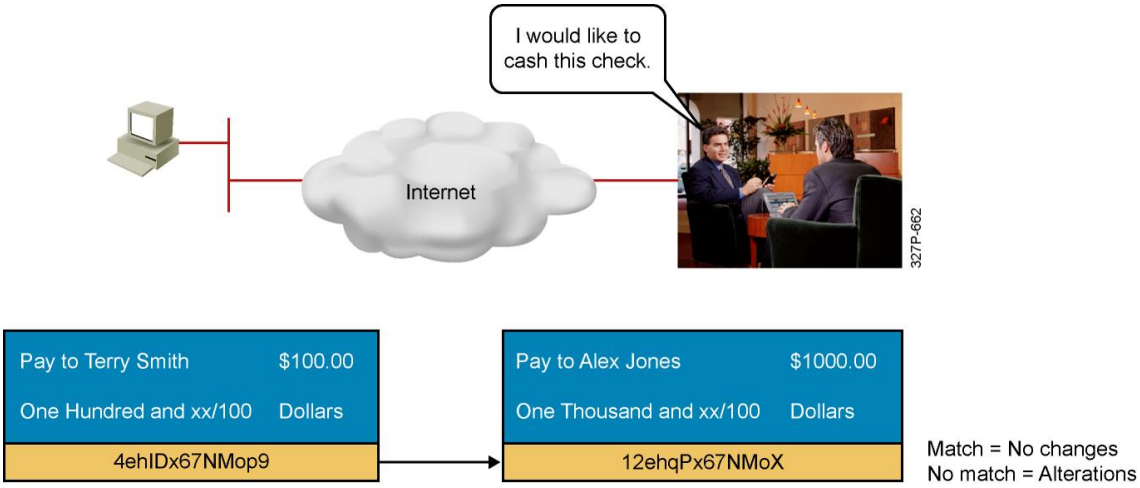
1. 기밀성(Confidentiality)



(1) 쌍방간에 주고받는 실제 정보의 비밀성을 보장하는 개념

(2) 각종 VPN 기법 등을 통해 기밀성을 유지

2. 무결성(Integrity)



(1) 쌍방간에 주고받는 실제 정보의 정확성을 보장하는 개념

(2) 다시 말해, 상호간에 사용하는 열쇠의 유출 유무를 검증해 정보의 훼손•변조•유출 등을 방지하는 개념

(3) 요약 함수 또는 전자 서명 등을 통해 무결성을 유지

3. 인증(Authentication)

(1) 송신자와 수신자 사이의 확신성을 보장하는 개념

(2) 인증 정보 또는 생체 인식 등에 기반하며 접근 통제의 적용 대상

(3) HMAC 기법 또는 전자 서명 등을 통해 인증을 유지

4. 가용성(Availability)

(1) 정당한 사용자가 필요할 때마다 즉각적으로 정보에 접근해 사용하는 개념

(2) DDoS 공격 또는 자연 재해 등이 위협 요소

(3) 사업 연속성 계획(BCP)•재난 복구 계획(DRP) 등을 통해 가용성을 유지

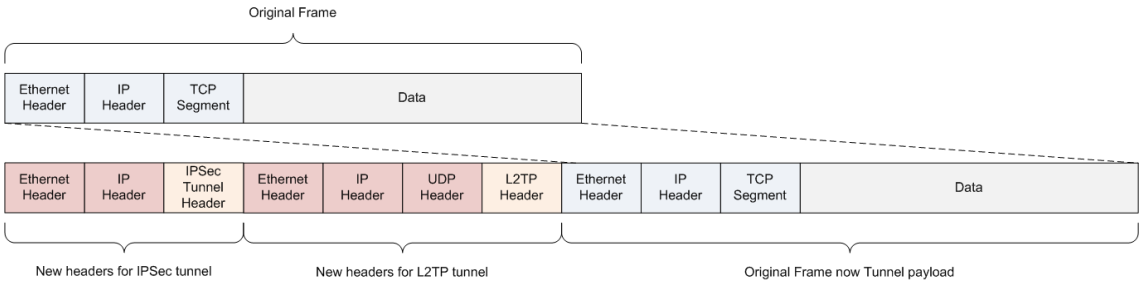
5. 부인 방지(Non-Repudiation)

(1) 송신자가 정보를 전송했는데 수신자가 이를 부인하는 일 등을 방지하는 개념

(2) 다시 말해, 특정 행위나 사건 등을 증명해 나중에 그러한 부분을 부인할 수 없게 하는 일종의 공증과 같은 개념

(3) 전자 서명 등을 통해 부인 방지를 유지

제8-1장 VPN 개념과 종류



1. 응용 계층 기반의 VPN

SSH VPN 방식

2. 전송 계층 기반의 VPN

SSL/TLS VPN 방식

3. 네트워크 계층 기반의 VPN

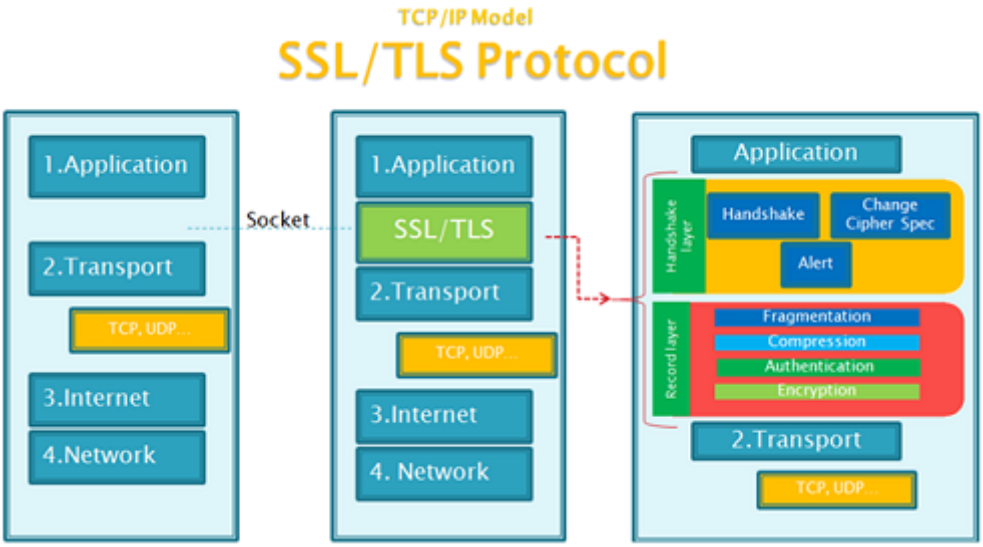
IPSec VPN 방식

4. 데이터 링크 계층 기반의 VPN

L2F VPN(시스코)•PPTP VPN(마이크로소프트)•L2TP VPN(시스코와 마이크로소프트) 방식

제8-2장 SSL/TLS VPN 구성과 동작

1. SSL/TLS 방식의 계층적 구조



(1) SSL 핸드쉐이크 프로토콜

1) DES 또는 RC4 방식 등에 기반해 임시 비밀 열쇠를 생성

2) 서버와 클라이언트 상호 간의 인증 기능을 수행

(2) SSL 암호 변경 사양 프로토콜

일련의 보안 매개 변수를 주고받으면서 보안 협상을 수행

(3) SSL 경고 프로토콜

상대방에게 오류 통보 기능을 수행

(4) SSL 레코드 계층 프로토콜

단편화 > 압축화 > 해쉬 첨부 > 암호화 > SSL 레코드 헤더 추가

2. SSL/TLS 방식의 동작

전자 봉투 생성 과정

(1) 초기 협상 단계

클라이언트와 서버 사이에서 클라이언트 헬로•서버 헬로 신호 교환

(2) 서버 인증 단계

서버가 클라이언트에게 공개 열쇠를 전송

(3) 클라이언트 인증 단계

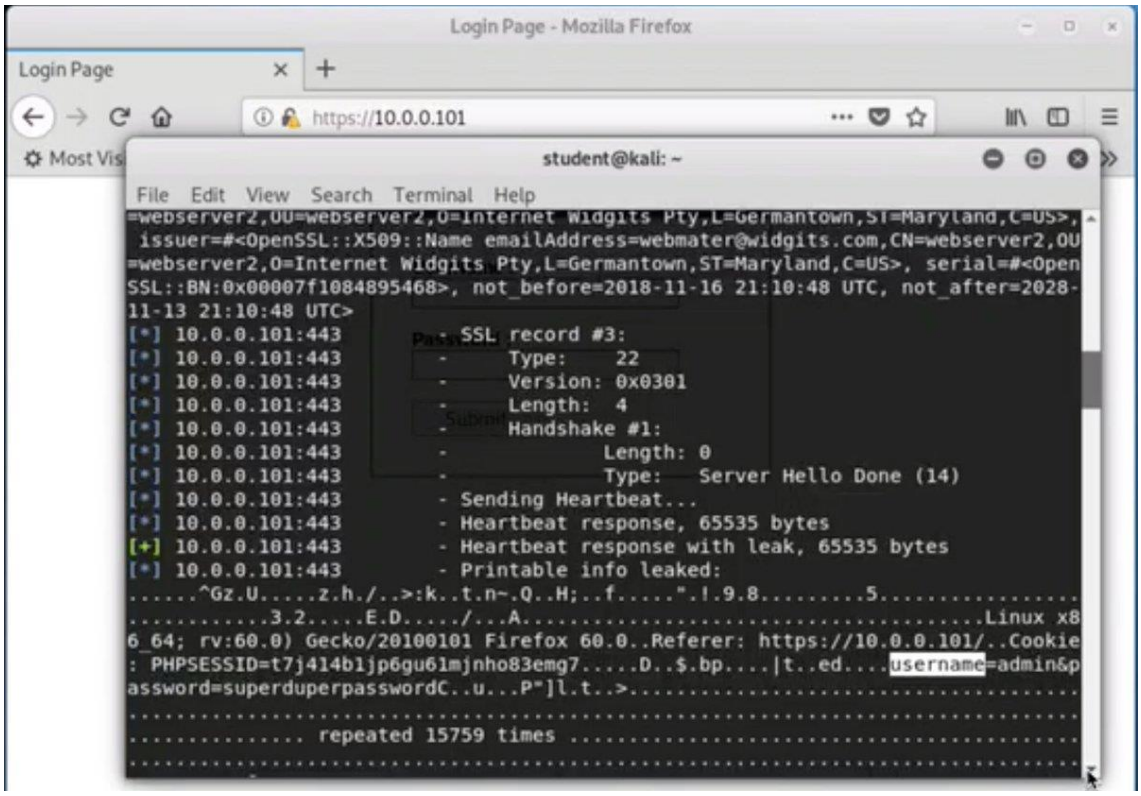
핸드쉐이크 프로토콜에서 생성한 임시 비밀 열쇠를 공인 인증서에 담긴 공개 열쇠로 암호화해 전송하고 암호 변경 사양 프로토콜에서 다음 단계에서 사용할 일련의 보안 매개 변수를 서버에게 전송

(4) 종료 단계

일련의 SSL/TLS 통신을 진행한 뒤 TCP 방식에 따라 순차적으로 연결 종료

3. SSL/TLS 방식의 취약점

(1) OpenSSL 하트블리드(HeartBleed) 공격

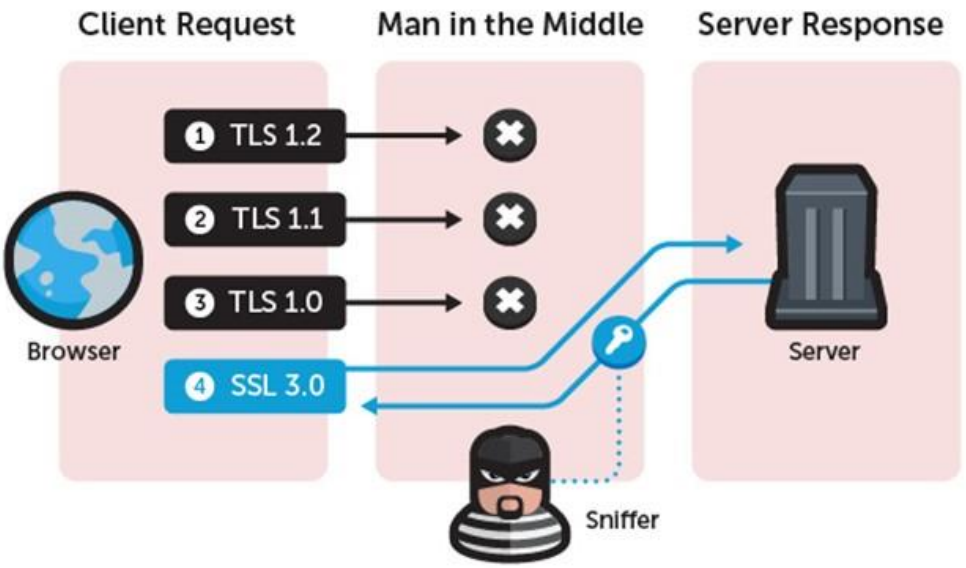


1) 2014년 OpenSSL 1.0.1-1.0.1f 버전과 1.0.2-beta 버전 등에서 발견한 일종의 버퍼 오버플로우 기법으로서 인증 정보가 노출되는 취약점

2) 침투 발견 시 비밀 번호 재설정•해당 버전 업데이트•공인 인증서 재발급

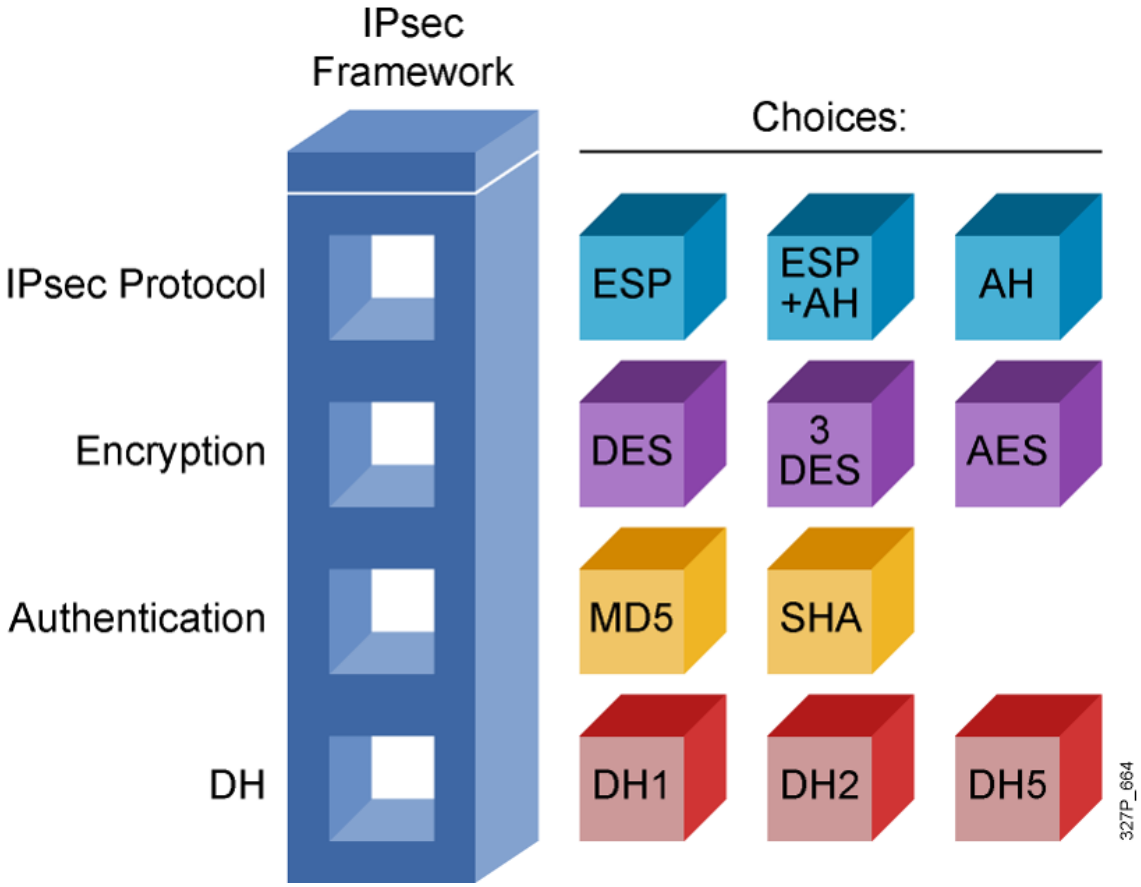
(2) SSLv3 POODLE 공격

1) 구형인 SSLv3 방식은 CBC 모드로 동작하기 때문에 웹 브라우저에서 SSLv3 방식을 사용하는 공격 대상자를 대상으로 ARP 스푸핑 공격을 가한 뒤 공격 대상자와 서버 사이에 SSLv3 방식으로 강제 연결되도록 유도

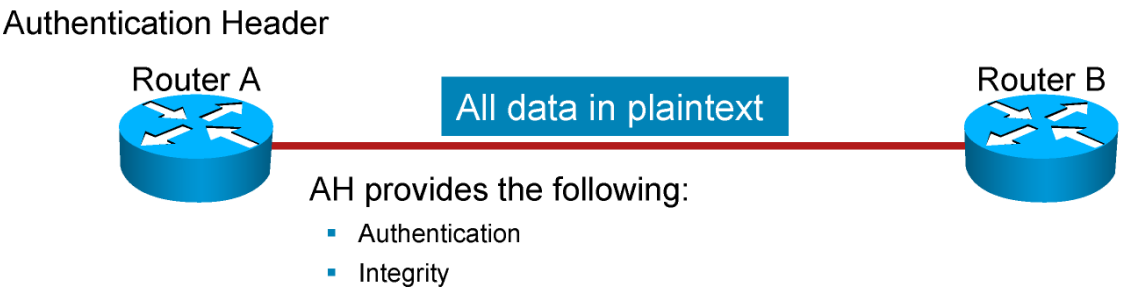


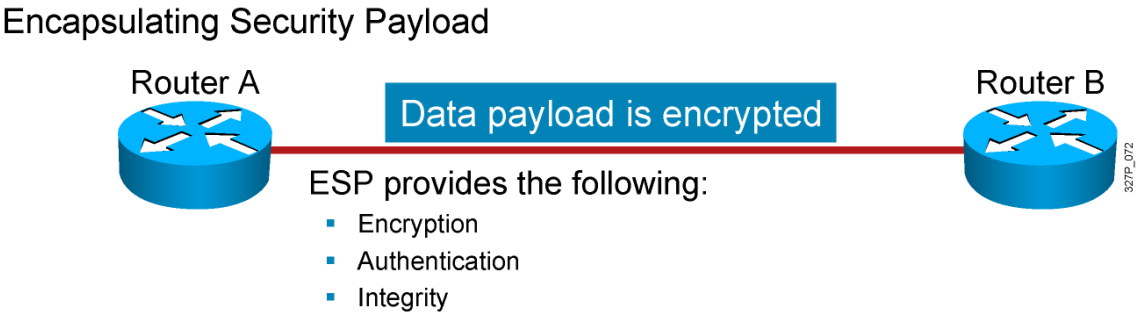
2) SSLv3 방식의 동작 중지

제8-3장 IPSec VPN 구성과 동작



1. IPSec 방식의 종류[터널 모드의 경우]





(1) AH 방식은 무결성•인증 기능만을 지원

(2) ESP 방식은 무결성•인증 기능은 물론 기밀성을 선택적으로 지원

2. ESP 방식에 기반한 보안 협상 절차

(1) IKE 1단계 절차

1) 6단계의 메인 모드로 동작하거나 3단계의 축약 모드로 동작

2) VPN 장비 상호간 인증 절차로서 선택적 기능(생략 시 no crypto isakmp enable 명령어 이용)

```
crypto isakmp policy 10 #(선택적) IKE 1단계 절차 설정
encryption des
group 2
hash md5
authentication pre-share
lifetime 60
```

```
exit
crypto isakmp key 4321 address 192.168.34.4 #메인 모드 설정
exit
crypto ipsec transform-set KNHI esp-3des esp-md5-hmac #(필수적) IKE 2단계 절차 설정
exit
```

```
crypto isakmp policy 10 #(선택적) IKE 1단계 절차 설정
encryption des
group 2
hash md5
authentication pre-share
lifetime 60
exit
crypto isakmp peer address 192.168.34.4 #축약 모드 설정
set aggressive-mode password 4321
set aggressive-mode client-endpoint ipv4-address 192.168.23.2
exit
crypto ipsec transform-set KNHI ah-md5-hmac #(필수적) IKE 2단계 절차 설정
exit
```

(2) IKE 2단계 절차

3단계의 퀵 모드로 동작

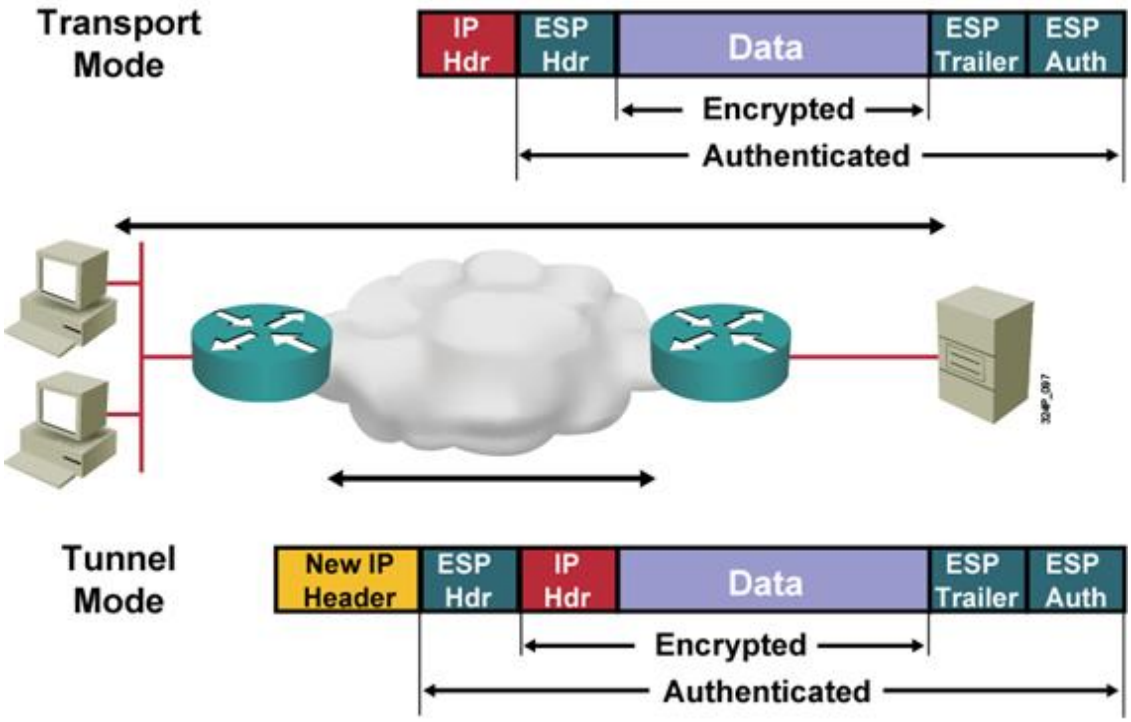
3. IKE•ISAKMP 개념

(1) 보안 협상이 가능하도록 지원하는 프로토콜

(2) IKE 방식은 구체적인 절차를 명시한 프로토콜이고 ISAKMP 방식은 전체적인 절차를 명시한 프로토콜

(3) 2010년 현재 IKE 2.0 방식에서 ISAKMP 방식을 흡수•통합

4. ESP 방식에 기반한 IPSec VPN 전송 유형



터널 구간의 차이와 ESP 헤더의 삽입 위치의 차이에 따라 전송 모드와 터널 모드로 구분

(1) 전송 모드

1) 일종의 종단간 VPN 기법으로 암호화•복호화의 주체가 각각 송신자와 수신자

2) 동일한 LAN 영역에서도 암호문으로 송신•수신하기 때문에 높은 보안성을 유지

3) 사용자가 직접 IPSec VPN 작업을 수행

(2) 터널 모드

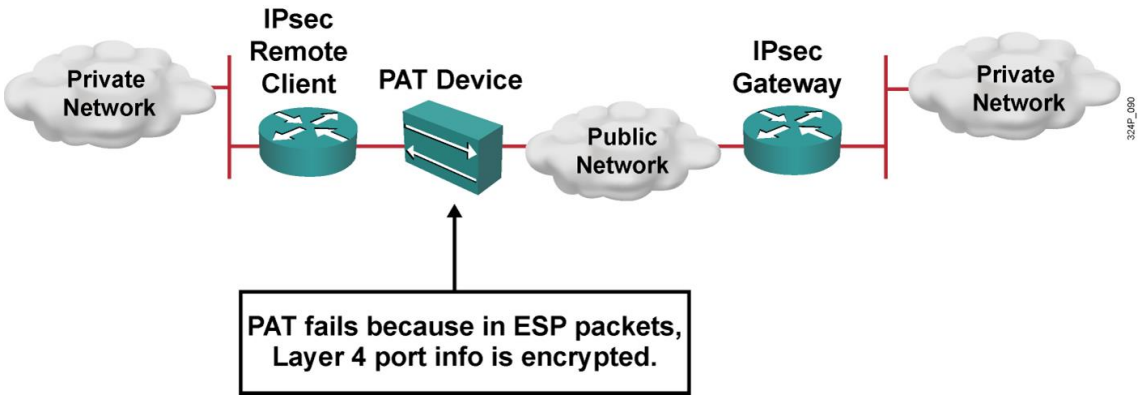
1) 일종의 링크 VPN 기법으로 암호화•복호화의 주체가 라우터 또는 VPN 장비

2) 사용자에게 IPSec VPN 투명성을 제공

3) 송신자•수신자와 해당 장비 사이에서 평문으로 송신•수신

5. IPSec VPN 환경에서 PAT 방식의 처리 문제

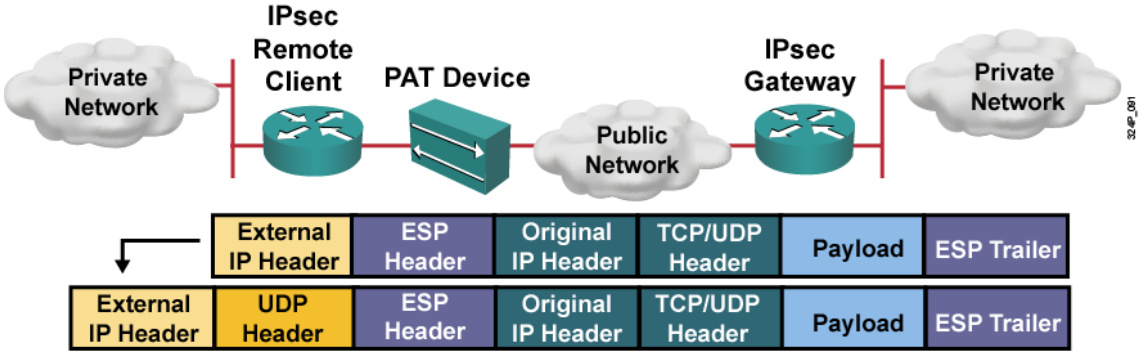
(1) 문제점



1) IPSec VPN 환경에서는 PAT 동작 불능

2) 전송 계층 헤더에 접근이 불가능

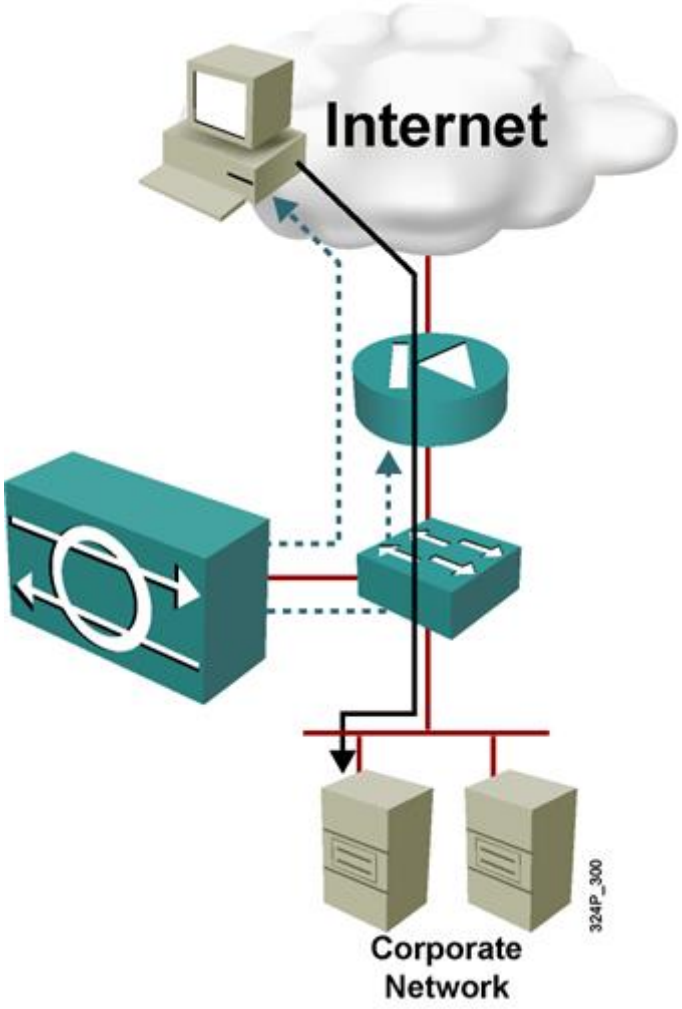
(2) 해결책



ESP 헤더 앞에 새로운 UDP 헤더를 추가

제9-1장 침입 탐지 장비와 침입 차단 장비의 이해

1. IDS의 기능



일정한 탐지 규칙에 기반해 모니터링 또는 미러링 방식에 따라 기존의 공격 유형을 탐지

2. IDS의 동작 순서

정보 수집 > 정보 가공•축약 > 분석•침입 탐지 단계 > 보고•대응

3. IDS의 탐지 오류

(1) 오탐(False Positive)

정상적인 유형을 악의적인 유형으로 오판

(2) 미탐(False Negative)

악의적인 유형을 정상적인 유형으로 오판

4. IDS의 탐지 방법

(1) 오용 탐지

1) 지식 기반 탐지•패턴 기반 탐지•서명 기반 탐지라고도 함

2) 전문가 시스템(Expert System)을 이용하고 침입 유형 등을 사전에 등록해 탐지

3) 미탐 비율이 높은 편

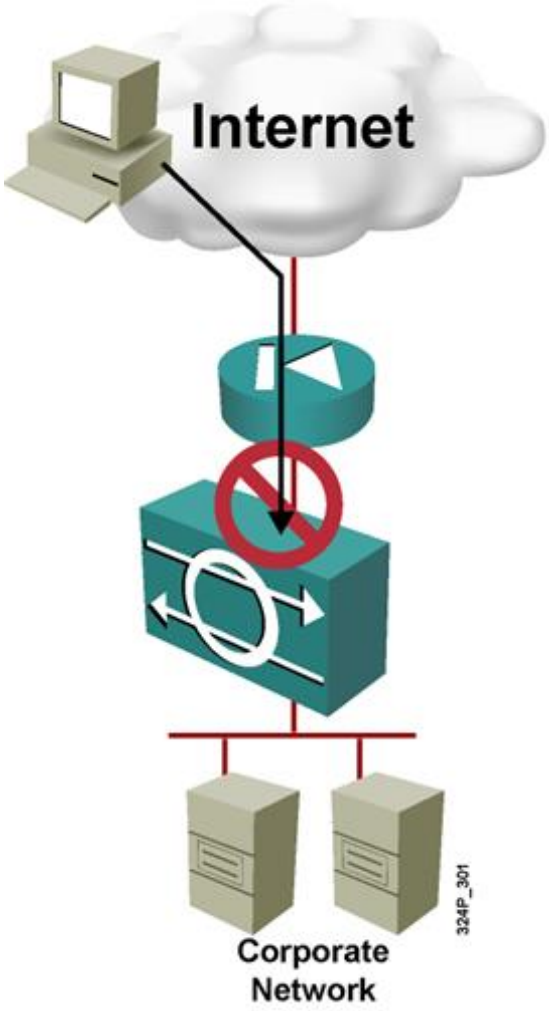
(2) 이상 탐지

1) 행위 기반 탐지라고도 함

2) 정량적•통계적 분석에 기반해 일정한 시간 동안 발생한 트래픽 유형을 관찰하면서 임계치를 초과하면 경보를 발생

3) 오탐 비율이 높은 편

5. IPS의 기능



IDS가 탐지하면 게이트웨이 방식 또는 인라인 방식에 따라 침입을 방지

6. IDS/IPS의 종류

(1) 네트워크 기반의 IDS/IPS

1) LAN 영역 전체를 탐지하는데 유리

2) 자신에게 향하는 패킷이나 암호화 패킷 등은 탐지 곤란

(2) 호스트 기반의 IDS/IPS

1) 내부 공격을 탐지하는데 유리

2) 호스트 단위만 탐지

제9-2장 스노트 사용 일례

1. ICMP 요청 탐지 설정

```
cat > /etc/snort/rules/local.rules

alert icmp any any -> any any (sid:1000001;)
```

(1) 동작(action) 설정 종류

1) alert 동작

경고를 발생시키고 로그를 기록

2) log 동작

단순히 로그만을 기록

3) pass 동작

무시

4) drop 동작

차단하고 로그를 기록

5) sdrop 동작

차단하고 로그를 미기록

6) reject 동작

차단하고 로그를 기록하고 차단 사실을 상대방에게 통보

7) activate 동작

경고를 발생시키고 dynamic 동작을 활성화

8) dynamic 동작

activate 동작과 연동해 단순히 로그만을 기록

(2) 탐지 가능한 프로토콜의 종류

IP•ICMP•UDP•TCP

(3) sid 의미

1) 99 이하

시스템 내부에서 사용

2) 100부터 1,000,000 이하

스노트 사이트에서 배포하는 탐지 규칙에서 사용

3) 1,000,001 이상

사용자가 local.rules에서 임의로 사용

2. 죽음의 핑 공격 탐지 설정

```
alert icmp any any -> any any (msg:"PingOfDeath";threshold:type both,track by_src,count 10,seconds 2;sid:1000001;)
alert icmp any any -> any any (msg:"PingOfDeath";threshold:type both,track by_src,count 10,seconds 2;dsize:>5000;sid:1000002;)
```

(1) msg 의미

이벤트 발생 시 설정한 문자열을 제목으로 출력

(2) threshold:type 의미

1) threshold:type threshold 경우

패킷의 갯수에 기반해 매 2초 간격으로 10개의 패킷을 단위로 경고창을 출력[패킷이 20개라면 두 번 출력]

2) threshold:type both 경우

시간 간격에 기반해 매 2초 간격으로 10개의 패킷까지만 경고창을 출력[패킷이 20개라도 한 번 출력]

3) threshold:type limit 경우

패킷의 갯수와 시간 간격에 기반해 매 2초 간격으로 경고창을 10번 출력

(3) track 의미

1) track by_src 경우

출발지 IP 주소에 기반해 추적

2) track by_dst 경우

목적지 IP 주소에 기반해 추적

(4) dsize 의미

패킷의 크기 설정

3. IP 스푸핑 공격 탐지 설정

```
alert icmp 10.0.0.0/8 any -> any any (sid:1000001;)
alert icmp 172.16.0.0/16 any -> any any (sid:1000002;)
```

4. 랜드 공격 탐지 설정

```
alert icmp 192.168.10.215 any -> 192.168.10.215 any (sid:1000001;)
alert icmp any any -> any any (sameip;sid:1000002;)
```

5. 각종 포트 스캔 탐지 설정

```
alert tcp any any -> 192.168.10.215 22 (flags:S;sid:1000001;)
alert tcp any any -> 192.168.10.215 22 (flags:F;sid:1000002;)
alert tcp any any -> 192.168.10.215 22 (flags:UPF;sid:1000003;)
alert tcp any any -> 192.168.10.215 22 (flags:!UAPRSF;sid:1000004;)
```

6. SYN 플러딩 공격 탐지 설정

```
alert tcp any any -> any any (flags:S;threshold:type both,track by_src,count 10,seconds 2;sid:1000001;)
```

7. 무차별 대입 공격 탐지 설정

```
alert tcp any any -> any 21 (threshold:type both,track by_src,count 10,seconds 2;sid:1000001;)
```

8. FTP 계정별 접속 탐지 설정

```
alert tcp any any -> any 21 (content:"user root";nocase;sid:1000001;)
```

(1) content 의미

페이로드에서 검색할 문자열 또는 헥사 코드 설정

(2) nocase 의미

대•소문자 구분 무시

9. SSH 접속 탐지 설정

```
alert tcp any any -> any 22 (content:"SSH";nocase;offset:3;depth:5;sid:1000001;)
```

(1) 검색 시간을 줄이기 위한 좌표 지정

(2) 응용 계층의 페이로드에 12345ABCDE라는 내용이 있는 경우

1) content:"45";offset:2;depth:5;

2 번째 위치(시작 문자 3)에서 5 바이트 검색한 뒤(345AB) 해당 문자열을 추출(45)

2) content:"123";depth:5;content:"BC";nocase;distance:2;within:3;

0 번째 위치(시작 문자 1)에서 5 바이트 검색하고(12345) 해당 문자열을 추출(123)한 뒤 해당 문자열(123) 이후부터 2 바이트 통과하고(45) 해당 문자(A)에서 3 바이트 검색해(ABC) 해당 문자열을 추출(BC)

10. HTTP GET 플러딩 공격 탐지 설정

```
alert tcp any any -> any 80 (content:"GET / HTTP/1.";nocase;threshold:type both,track by_src,count 10,seconds 2;sid:1000001;)
```

11. 슬로우 로리스 공격 탐지 설정

```
alert tcp any any -> any 80 (flow:to_server,established;pcre:"/[^₩x0d₩x0a]₩x0d₩x0a$/";threshold: type both ,track by_src,count 10,seconds 2;sid:1000001;)
```

(1) flow 의미

1) 서버와 클라이언트의 흐름을 제어하는 용도로 사용

2) flow:to_server,established

스노트 서버로 향하는 패킷을 대상으로 3단계 연결 설정 이후의 패킷만을 제어하겠다는 의미

(2) pcre 의미

펄 호환 정규 표현식(Perl Compatible Regular Expressions)을 의미

제10-1장 방화벽의 이해

1. 방화벽의 기능

외부망과 내부망 사이에서 일정한 차단 규칙에 따라 특정 패킷을 차단•허용하는 소프트웨어 설정 또는 하드웨어 장비

2. 방화벽의 접근 제어 기법

(1) ACL 방식

TCP/IP 네트워크 계층•전송 계층에 기반해 필터링 기능을 수행

(2) ALG 방식

프록시 방화벽이라고도 부르며, TCP/IP 응용 계층에 기반해 필터링 기능을 수행하기 때문에 웹 방화벽(Web Application Firewall)처럼 특정 응용 계층의 프로토콜만을 지원해 과부하 해소

(3) 상태 추적(SPF) 방식

1) 상태 추적 테이블을 통해 리턴 패킷 여부를 검사

2) UDP 방식 등은 TCP 플래그와 같은 기능이 없어서 추적이 불가능하기 때문에 타임아웃을 설정해 사용

제10-2장 IPTables 사용 일례

1. ICMP 요청 차단 설정

```
iptables --append INPUT --protocol icmp --icmp-type echo-request -j LOG
iptables --append INPUT --protocol icmp --icmp-type echo-request -j REJECT
```

(1) --append INPUT 명령어는 들어오는 패킷을 대상으로 적용하겠다는 의미

(2) --protocol icmp 명령어는 ICMP 방식을 대상으로 적용하겠다는 의미

(3) --icmp-type echo-request 명령어는 ICMP 요청을 대상으로 적용하겠다는 의미

(4) -j LOG 명령어는 조건에 부합하면 로그를 기록하겠다는 의미

(5) -j REJECT 명령어는 조건에 부합하면 ICMP 오류 응답을 통해 차단하겠다는 의미

2. ICMP 요청 차단 추가 설정

```
iptables --append INPUT --source 192.168.10.219 --protocol icmp --icmp-type echo-request -j DROP
```

(1) --source 192.168.10.220 명령어는 출발지 IP 주소가 192.168.10.220번인 경우 적용하겠다는 의미

(2) -j DROP 명령어는 조건에 부합하면 단지 차단하겠다는 의미

3. ICMP 요청 차단 추가 설정

```
iptables --append INPUT --protocol icmp --icmp-type echo-request --match length --length 1024: -j REJECT
iptables --append INPUT --protocol icmp --icmp-type echo-request -j ACCEPT
```

--match length --length 1024: 명령어는 패킷의 길이가 1024 바이트 이상을 대상으로 정책을 적용하겠다는 의미

4. TCP 오픈 스캔과 TCP 할프 오픈 스캔 차단 설정

```
iptables --append INPUT --protocol tcp --tcp-flag ALL SYN -j REJECT
```

--tcp-flag ALL SYN 명령어는 SYN 플래그를 설정한 세그먼트를 대상으로 적용하겠다는 의미

5. 기타 스캔 차단 설정

```
iptables --append INPUT --protocol tcp --tcp-flag ALL FIN -j REJECT
iptables --append INPUT --protocol tcp --tcp-flag ALL URG,PSH,FIN -j REJECT
iptables --append INPUT --protocol tcp --tcp-flag ALL NONE -j REJECT
```

(1) --tcp-flag ALL FIN 명령어는 모든 플래그 중에서 FIN 플래그를 설정한 세그먼트를 대상으로 적용하겠다는 의미

(2) --tcp-flag ALL URG,PSH,FIN 명령어는 모든 플래그 중에서 URG•PSH•FIN 플래그를 동시에 설정한 세그먼트를 대상으로 적용하겠다는 의미

(3) --tcp-flag ALL NONE 명령어는 어떤 플래그도 없는 세그먼트를 대상으로 적용하겠다는 의미

6. SSH 접속 차단 설정

```
iptables --append INPUT --source 192.168.10.219 --protocol tcp --destination-port 22 -j REJECT
```

--destination-port 22 명령어는 목적지 포트 번호가 22번인 경우 적용하겠다는 의미

7. SSH 무차별 대입 공격 차단 설정

```
iptables --append INPUT --source 192.168.10.219 --protocol tcp --destination-port 22 --match state --state NEW --match recent --set
iptables --append INPUT --source 192.168.10.219 --protocol tcp --destination-port 22 --match state --state NEW --match recent --update --seconds 1 --hitcount 2 -j REJECT
```

(1) --match state --state NEW 명령어는 TCP 3단계 연결 수립부터 정책을 적용하겠다는 의미

(2) --match recent --set 명령어는 출발지 IP 주소 등을 동적으로 반영해 정책을 적용하겠다는 의미

(3) --match recent --update 명령어는 새로운 출발지 IP 주소 등을 동적으로 추가해 정책을 적용하겠다는 의미