

내부 세미나 발표

ARP protocol



91613959 / 2학년 조재현

공부한거 목차 소개



1. ARP




2. RARP



3. ARP
Spoofing
&대응 방안

* 왜 ARP?

– 기초부터 쌓자!  (프로토콜 한개씩 꾸준히 공부)

– 지금도 많이 사용하고 있는 프로토콜이자
해킹으로부터 취약한 프로토콜



– 내가 면접때 틀림..



1. ARP란?

용어 설명 : ARP(Address Resoultion Protocol)는 IP를 가지고 MAC주소를 알아낼 수 있음.
그리고 가져온 정보는 ARP Table에 저장이 됨.

*** ARP Table:** 현재 알고 있는 목적지의 IP주소를 가지고 목적지의 MAC 주소를 찾아야할때 참조.
테이블에는 IP주소에 맞는 MAC주소가 맵핑되어 있음.

*** ARP가 사용되는 경우**

1. 호스트-호스트
2. 라우터-호스트
3. 라우터-라우터
4. 호스트-라우터

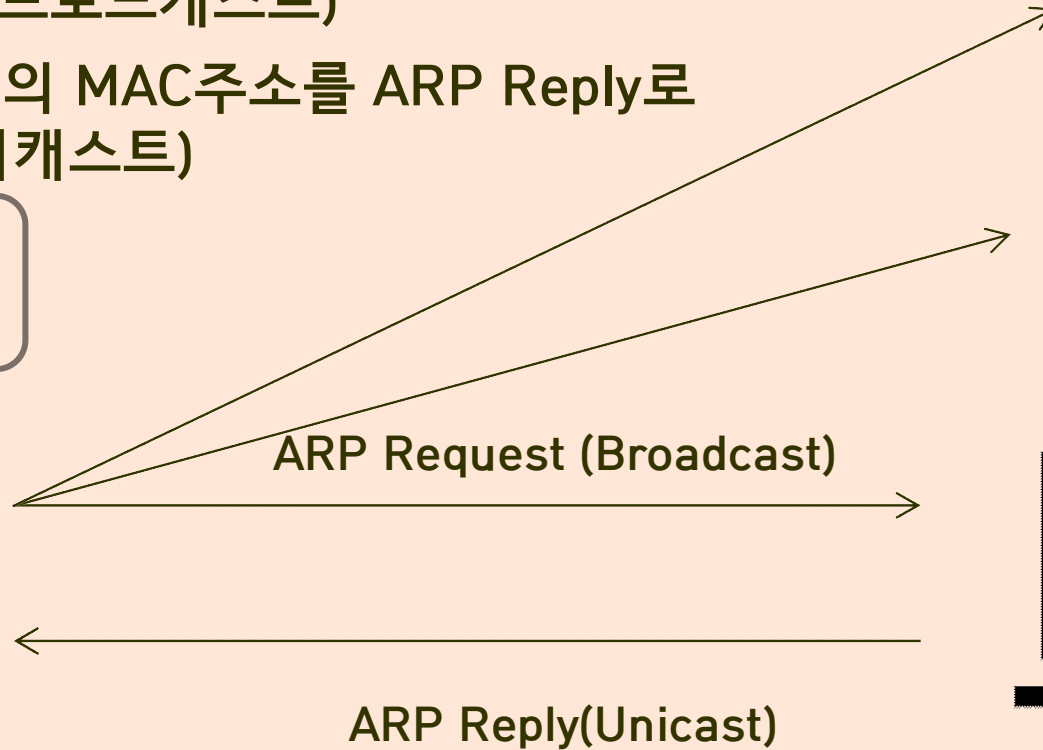
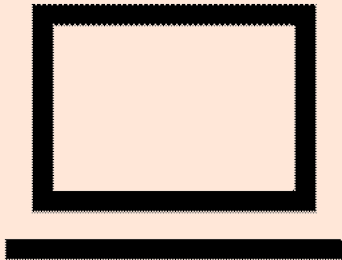


L7	응용 계층 (Application Layer)
L6	표현 계층 (Presentation Layer)
L5	세션 계층 (Session Layer)
L4	전송 계층 (Transport Layer)
L3	네트워크 계층 (Network Layer)
L2	데이터 링크 계층 (Data Link Layer)
L1	물리 계층 (Physical Layer)

1. ARP란?

1. 요청 HOST가 MAC주소가 필요한 IP를 ARP Request로 전체 호스트에게 전송 (브로드캐스트)
2. 해당 IP의 HOST가 자신의 MAC주소를 ARP Reply로 요청 HOST에게 전송 (유니캐스트)

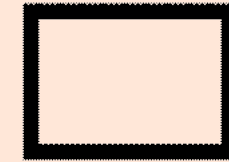
이 IP누구야? 이 IP인
사람은 MAC주소 알려줘~



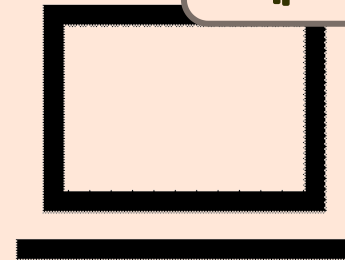
나 아님 ㅋ



나도 아님 ㅋ



나임. Reply 해줌.
내 MAC주소는!



1-1 ARP header

ARP 헤더 정보(28 Byte)

H/W Type (2 byte)	Protocol Type (2 byte)	H/W Length (1 byte)	Protocol Length (1 byte)	OP (2 byte)	
SA (Sender ethernet address) (6 byte)					Sender IP address (4 byte)
DA (Target ethernet address) (6 byte)					Target IP address (4 byte)

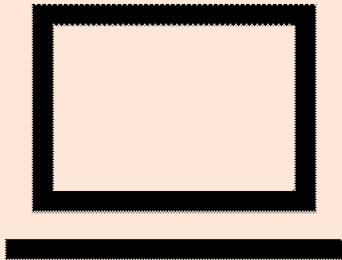
1-1 ARP header

H/W Type (2byte)	하드웨어 타입
Protocol Type(2byte)	네트워크 계층의 프로토콜의 타입을 알려줌
Sender MAC address(6byte) — 보내는 MAC 주소 (00:26:66:c6:0d:3c) —	
Address Resolution Protocol (request)	
Hardware type: Ethernet (1)	
Protocol type: IP (0x0800)	
Hardware size: 6	
Protocol size: 4	
Opcode: request (1)	
[Is gratuitous: False]	
Sender MAC address: EfmNetwo_c6:0d:3c (00:26:66:c6:0d:3c)	
Sender IP address: 192.168.0.1 (192.168.0.1)	
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)	
Target IP address: 192.168.0.2 (192.168.0.2)	
Target IP address(4byte) — 받는 IP 주소	
Target ethernet address(6byte) — 받는 MAC 주소	

2. RARP란?

용어 설명 : ARP와 반대되는(Reverse) 개념으로 서버에 요청하여 MAC주소를 통해 IP를 획득할 수 있음.

내 MAC주소는 이거거든?
내 IP뭐냐? 나 바보라서ㅋ



RARP Request (Broadcast)

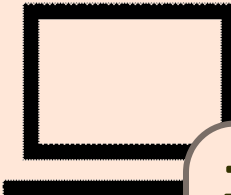
RARP Reply(Unicast)

RARP Reply(Unicast)

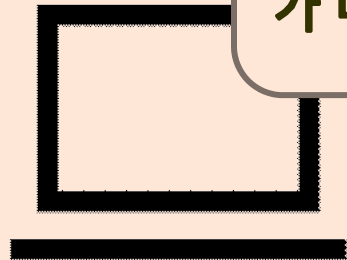
난 몰라



나도 몰라ㅋ

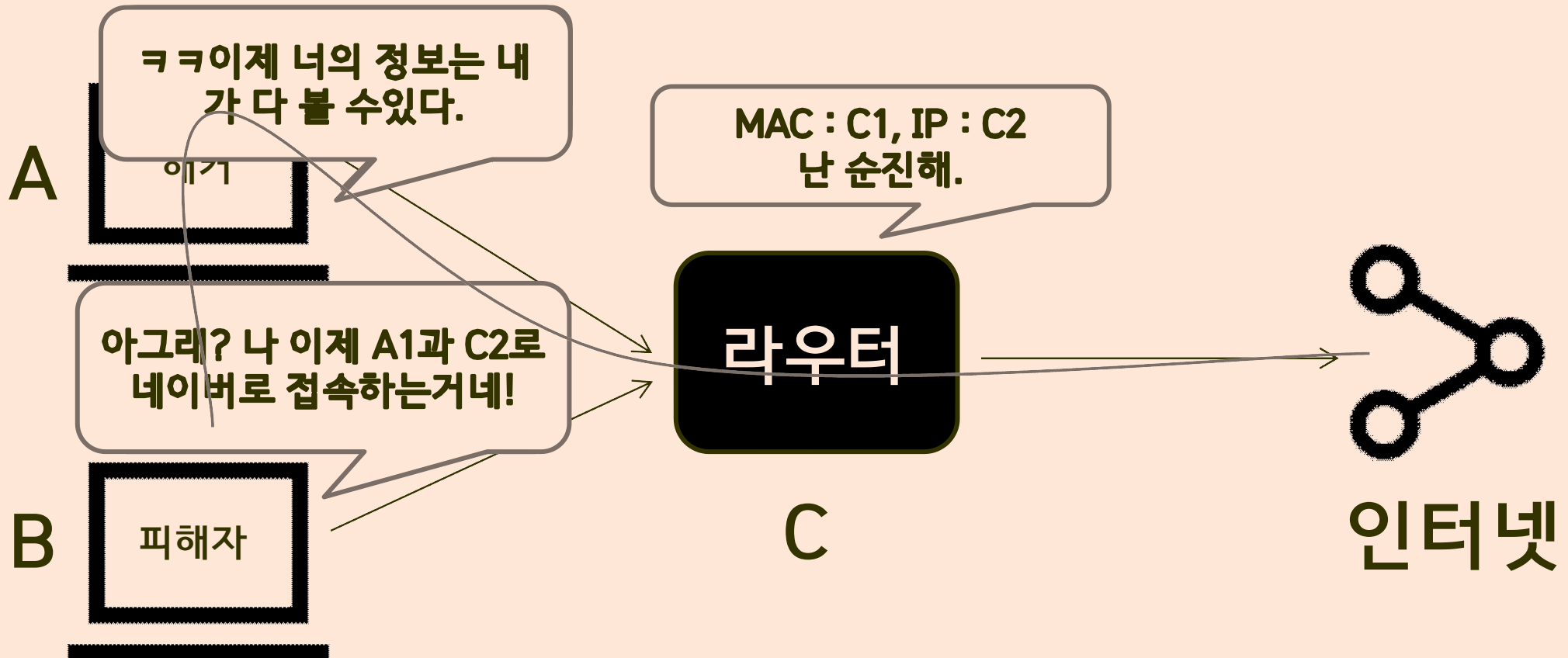


으휴 바보. 나한테 RARP기능이 있는 서버가 있어서 내가 대답해줄게. 니 IP는!



3. ARP Spoofing?

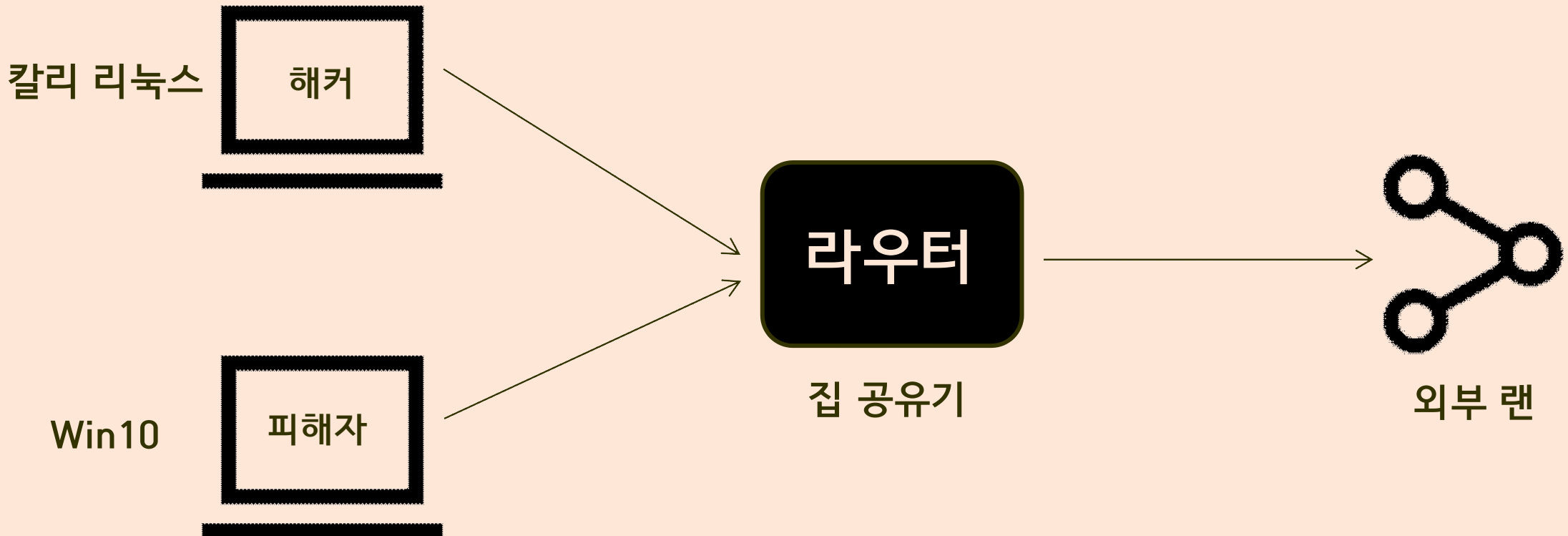
용어 설명 : ARP Spoofing은 ARP와 Spoofing의 합성어로 ARP를 속이는 중간자(MITM) 해킹기법이다.

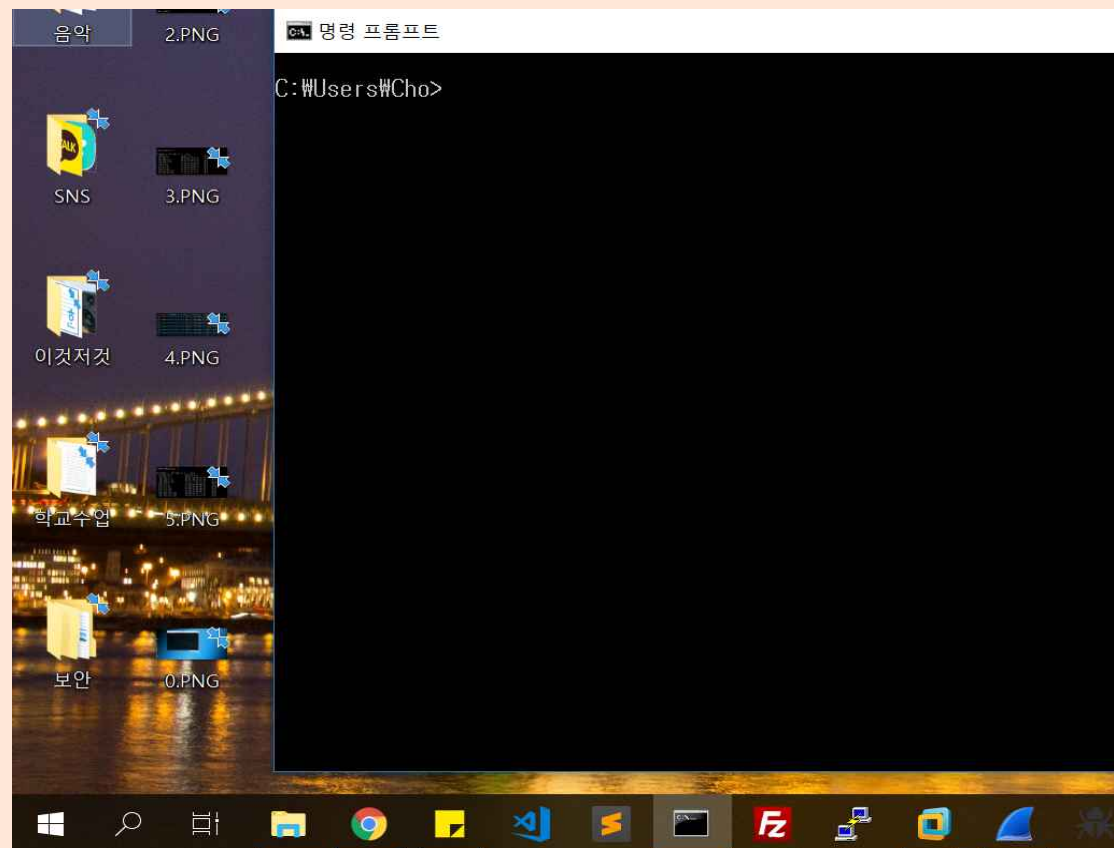


3. ARP Spoofing 실습

실습 목적 : 칼리리눅스(해커)로 윈도우10(피해자)의 패킷을 훔쳐본다.

실습 환경





해커

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
304...	5.206164	23.67.53.9	192.168.0.11	TCP	1514	80 → 56293 [ACK] Seq=33360996 Ack=1 Win=913 Len=1460
305...	5.206165	23.67.53.9	192.168.0.11	TCP	1514	80 → 56293 [ACK] Seq=33362456 Ack=1 Win=913 Len=1460
305...	5.206271	192.168.0.11	23.67.53.9	TCP	54	56293 → 80 [ACK] Seq=1 Ack=33363916 Win=8520 Len=0
305...	5.206274	192.168.0.11	23.67.53.9	TCP	54	[TCP Dup ACK 30501#1] 56293 → 80 [ACK] Seq=1 Ack=33363916 Win=8520 Len=0
305...	5.206991	23.67.53.9	192.168.0.11	TCP	1514	80 → 56293 [ACK] Seq=33363916 Ack=1 Win=913 Len=1460
305...	5.206991	23.67.53.9	192.168.0.11	TCP	1514	80 → 56293 [ACK] Seq=33365376 Ack=1 Win=913 Len=1460
305...	5.206992	23.67.53.9	192.168.0.11	TCP	1514	80 → 56293 [ACK] Seq=33366836 Ack=1 Win=913 Len=1460
305...	5.206993	23.67.53.9	192.168.0.11	TCP	1514	80 → 56293 [ACK] Seq=33368296 Ack=1 Win=913 Len=1460
305...	5.206994	23.67.53.9	192.168.0.11	TCP	1514	80 → 56293 [ACK] Seq=33369756 Ack=1 Win=913 Len=1460
305...	5.206994	23.67.53.9	192.168.0.11	TCP	1514	80 → 56293 [ACK] Seq=33371216 Ack=1 Win=913 Len=1460
305...	5.206995	23.67.53.9	192.168.0.11	TCP	1514	80 → 56293 [ACK] Seq=33372676 Ack=1 Win=913 Len=1460
305...	5.207111	192.168.0.11	23.67.53.9	TCP	54	56293 → 80 [ACK] Seq=1 Ack=33374136 Win=8520 Len=0
305...	5.207115	192.168.0.11	23.67.53.9	TCP	54	[TCP Dup ACK 30510#1] 56293 → 80 [ACK] Seq=1 Ack=33374136 Win=8520 Len=0
305...	5.208715	23.67.53.9	192.168.0.11	TCP	1514	80 → 56293 [ACK] Seq=33374136 Ack=1 Win=913 Len=1460

> Frame 9211: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

> Ethernet II, Src: EfmNetwo_7c:23:9c (88:36:6c:7c:23:9c), Dst: LiteonTe_25:17:a1 (c8:ff:28:25:17:a1)

> Internet Protocol Version 4, Src: 23.67.53.9, Dst: 192.168.0.11

> Transmission Control Protocol, Src Port: 80, Dst Port: 56293, Seq: 10211659, Ack: 1, Len: 1460

0000	c8 ff 28 25 17 a1 88 36 6c 7c 23 9c 08 00 45 00	..(%...6 l #...E.
0010	05 dc aa 93 40 00 38 06 85 89 17 43 35 09 c0 a8@.8. ...C5...
0020	00 0b 00 50 db e5 27 7a 6a 0b c7 8e 54 f8 50 10	...P...'z j...T.P.
0030	03 91 f3 8a 00 00 db 92 a8 f6 15 7a 95 49 45 b6z..IE.
0040	5d 98 da 93 9d 64 5f 08 cf be fc 23 26 13 b6 99]....d_...#&...
0050	7b 0b ac ab 4d b1 34 11 97 7d 57 49 5b 25 ba 8e	{...M.4. .}WI[%...
0060	ef 0f 9a 39 51 a9 09 0a 74 a1 a2 c2 61 f6 d9 9b	...9Q... t...a...
0070	38 44 64 1c 0d b9 2e 5d ef 15 8d 0c 12 6b 94 70	8Dd....]k.p
0080	60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

피해자

3. 대응방안 & 목표

- 대책 방안 : ARP Table을 정적할당해 고정시키면 ARP Spoofing을 방지 가능!

(Ex: 앞에서 C1,C2가 아예 라우터라고 피해자 컴퓨터에서 애초에 ARP Table을 고정시킴)

* BUT!

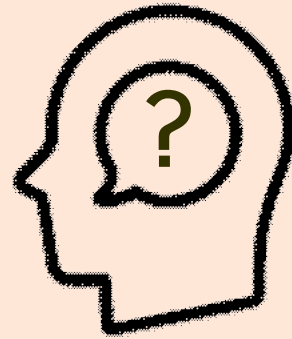
회사같은곳에서 모든 컴퓨터의 ARP테이블을 정적할당하기엔 현실적인 어려움

->

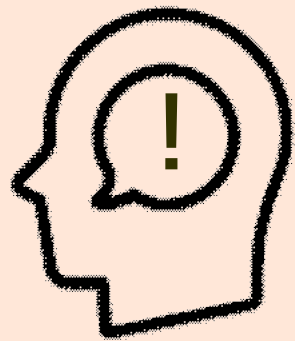
아직도 많이 악용되는 공격

* 목표!

현재 소켓공부중인데 더 공부해서 ARP Spoofing 직접 구현, 보안 구현



Q&A



들어주셔서 감사합니다.