네트워크 보안 6

202246655 이봉민

실습 개요 :

이번 실습은 ARP 스푸핑, DNS 스푸핑, SSL 스니핑과 같은 중간자 공격(MITM) 기법을 직접 수행해 봄으로써, 네트워크 환경에서 발생할 수 있는 보안 위협을 체험하고 원리와 대응을 이해함

공격자는 피해자(Client)와 인터넷 사이의 중간에 위치한 게이트웨이를 공격 대상으로 하여, ARP 리다이렉션을 통해 네트워크 흐름을 가로채고, DNS 응답을 위조함으로써 피해자의 웹 요청을 공격자 자신에게 유도함

실습 환경

- 공격자 : 칼리(192.168.174.131)
- 피해자(클라) : Windows7 (192.168.174.130)
- 서버(게이트웨이) : 192.168.174.2

1. SSL 통신 확인

- 전북대학교 웹사이트 접속 테스트
- HTTPS 인증서 정보 확인

2. dnsspoof.hosts 파일 설정

- 위조 DNS 응답 설정
- 공격자 IP 로 리다이렉트 구성

3. SSL 위조 인증서 생성 및 webmitm 실행

- webmitm 을 통한 인증서 생성
- 공격자 SSL 서버 구동

4. ARP 리다이렉션 공격 및 패킷 릴레이

- arpspoof 를 통한 MITM 구성
- fragrouter 를 통한 패킷 전달

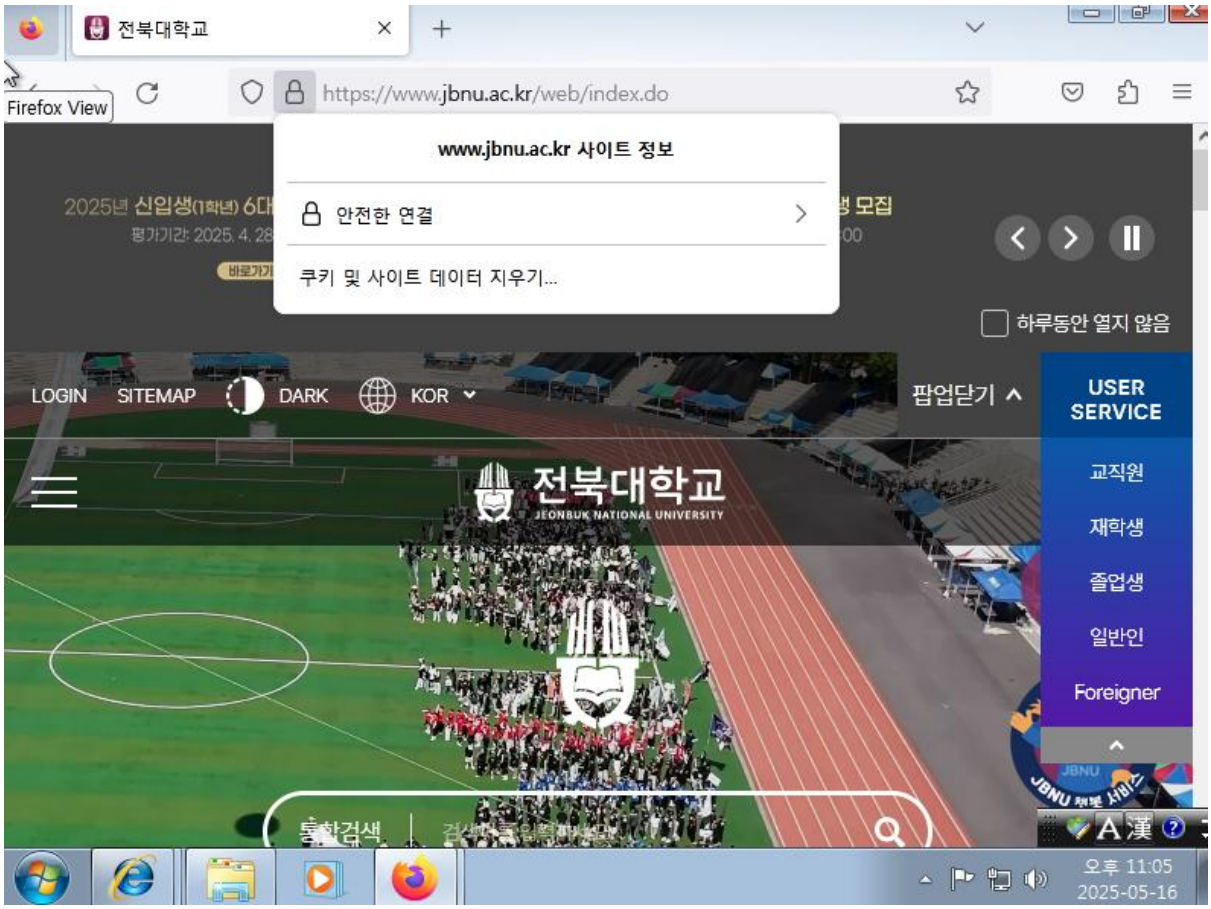
5. DNS 스푸핑 공격

- dnsspoof 실행
- 피해자 요청에 대해 위조된 DNS 응답 제공

6. 클라이언트에서 접속 시도

- 피해자가 공격자 SSL 서버로 접속
- 브라우저에서 인증서 경고 발생 확인

실습 과정



윈도우 7 환경에서 크롬이 다운로드 되지 않아 파이어 폭스 esr 115 버전으로 다운로드 하여 SSL 확인

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat dnsspoof.hosts
192.168.174.130  *.jbnu.ac.kr
```

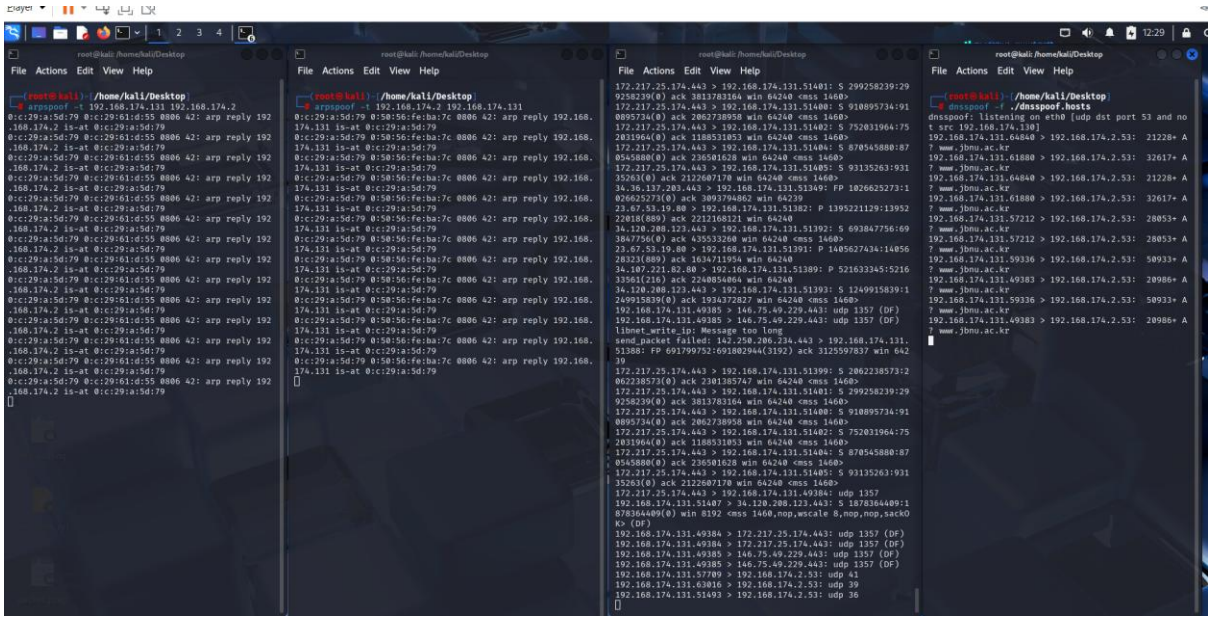
DNS 스푸핑을 위해 파일을 설정 dnsspoof.hosts 파일은 피해자가 *.jbnu.ac.kr 에 접속하려고 하면 192.168.174.130 인 공격자(kali)의 IP 로 리다이렉트 되도록 설정하였음

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# webmitm
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:KR
State or Province Name (full name) [Some-State]:JEONJU
Locality Name (eg, city) []:JEONJU
Organization Name (eg, company) [Internet Widgits Pty Ltd]:JBNU
Organizational Unit Name (eg, section) []:CSAI
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Certificate request self-signature ok
subject=C=KR, ST=JEONJU, L=JEONJU, O=JBNU, OU=CSAI
webmitm: certificate generated
webmitm: relaying transparently
^C
```

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat webmitm.crt
-----BEGIN PRIVATE KEY-----
MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGBAMtgVWBSmfZ71LIC
sI43sa4V36MnPz+RdJC1llrBExGlnOyKJbOx8N39BIlmwpyakbMDjQsb2QvW0mpt
xtB8f3oLYfcLQvjdcDPOpxsQsRJwegl/t58Pig3Ws85tmhh3LPIM17AaZ1uxWGWd
KVKTwo2+ggTdui3H9N1KAB81K8xfAgMBAAECgYAWQaCWPfPjaYHJSUoRBj9HkdU7
gZwGVOCwxW6C2AZCNCGMMUIW/C4j3QCWGMzLXo77TDQvNwj1pri4NPNA9Z7thfXx
ULq07dORA4BPx0++iHjl3HHZmeRh/VaySMrx754fvlx3kS1xrATKeIjYbbUDEd4L
/Gfv5OnGvGqRWEnHAQJBAP+Zs60IYMfffP+O9C1rGBkddfpO4+cooJDOrXg0ViAx
+aM2YjORTHxs923yoCcR+NpzFqadH7IVa32/gy7wvyECQQDLsbrrk+ngbzPqUUnh
uEbcvHB+I0SpYW5aksJ1SD/keH6bKpZfu4s6ZmpsxnCDVwhLiDmoMizlIEcsAnA7
hJt/AkEA1gt+/e5ALeEoKlMqhEZk3dNgEwexrsjE/b82Ya1iWn+/UECgqBKLfL87
zWUbXNyeC0HJvClke5uYcqvITazqQQJAHJAxq/Mz6prtZsA7YgGbPjzWcXm0mSPm
e6D0z8lv3DPhXRTdvVLpNSlDZzl0cZZ0vVK+8w0GKqMaF9vHrTDtNQJBAObQMu51
LpQ9g5SRZecNuo7HBb8aFIAZigcp5B9v6Cxt3bI/ZOItXx+S+d8BuG+NDVTxB+Ql
YDuevxLhp6j4WfU=
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIICRDCCAa2gAwIBAgIUbhoOc4EYCdXSxyiL1eyUslt1GvQwDQYJKoZIhvcNAQEL
BQAwTTELMAkGA1UEBhMCS1IxDzANBgNVBAgMBkpFT05KVTEPMA0GA1UEBwwGSkVP
TkpVMQ0wCwYDVQQKDARKQk5VMQ0wCwYDVQQLDARDU0FJMB4XDTI1MDUxNjE0MjQ1
NVoXDTI2MDUxNjE0MjQ1NVowTTELMAkGA1UEBhMCS1IxDzANBgNVBAgMBkpFT05K
VTEPMA0GA1UEBwwGSkVPTkpVMQ0wCwYDVQQKDARKQk5VMQ0wCwYDVQQLDARDU0FJ
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDLYFVgUpn2e9SyArCON7GuFd+j
Jz8/kXSQtZZawRMRpZzsiiWzsfDd/QSJZsKcmpGzA40LG9kL1tJqbcbQfH96C2H3
C0L43XAzzqcbELEScHoJf7efD4oN1rPObZoYdyzyDNewGmdbsVhlnSlSk8KNvoIE
3botx/TdSgAfNSvMXwIDAQABoyEwHzAdBgNVHQ4EFgQUHW6pmcSkcV1WmV0U4KlA
VByrE9MwDQYJKoZIhvcNAQELBQADgYEAPFh4CcmiEsnBnFAcwxRXQ8l3h3uD10JV
QosQ4L9anyrmAsNXsTQEz8yUryRhfWmLXS0cRwlNrfS3KfI9PKNlHqY8hyfSn4T2
Dgj6r3mGpiIDNXgFSHjOIdq3zTP8BG5X4ldnNlyMm9jl4cMP8H4tRWHI1mYS7Bt0
MDDz3d40eyc=
-----END CERTIFICATE-----
```

피해자에게 가짜 HTTPS 인증서를 제공하고, 공격자가 중간에서 TLS 연결을 중계함으로써 SSL 스니핑을 가능하게 한다. 피해자의 브라우저에서는 "안전하지 않은 연결" 경고가 나오게 됨

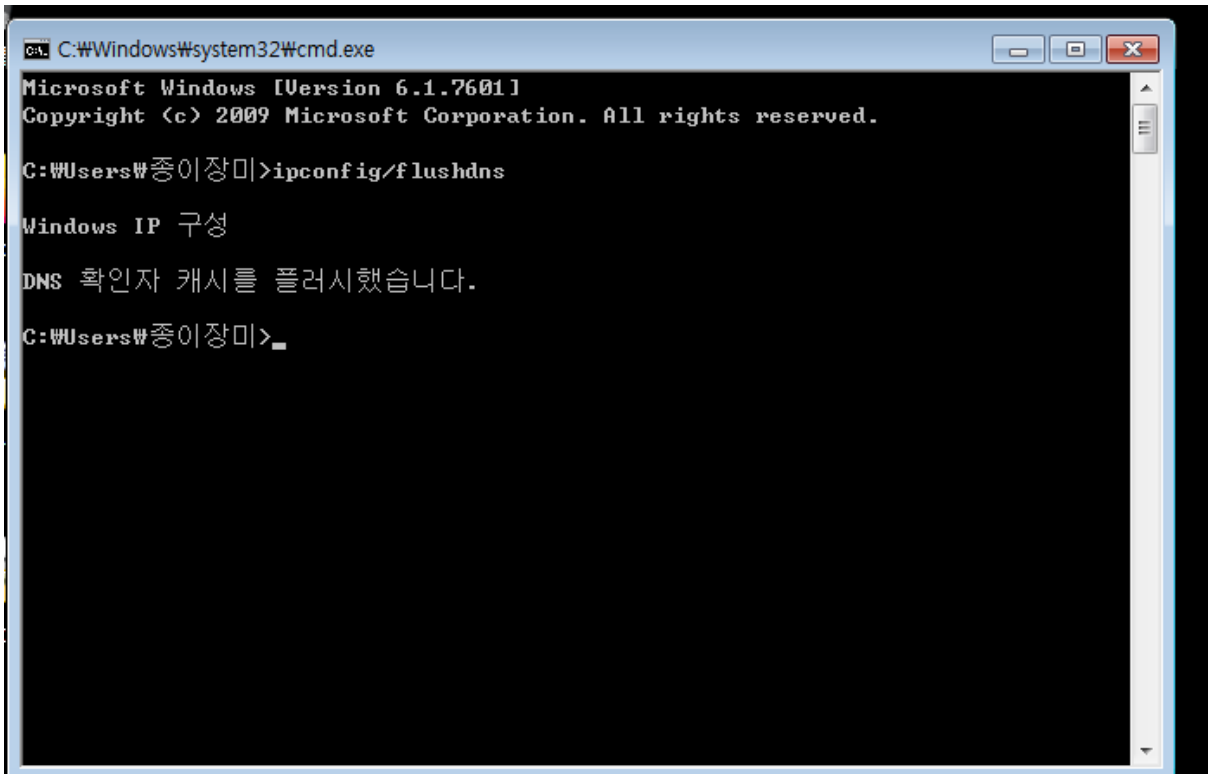


첫 번째 터미널 : 피해자에게 칼리가 게이트웨이라고 속이는 ARP 스푸핑

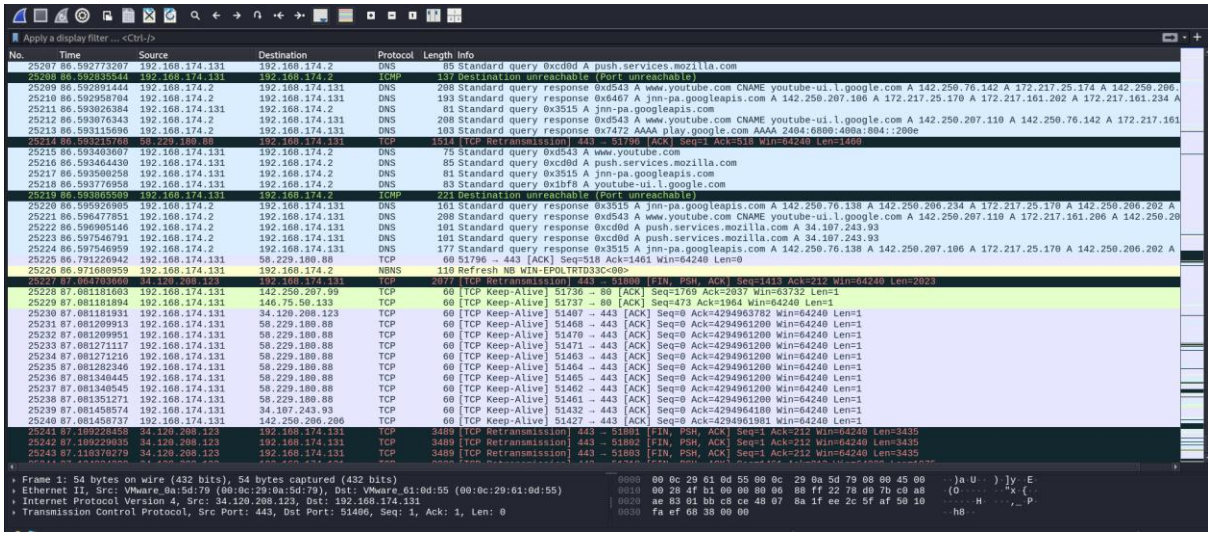
두 번째 터미널: 게이트웨이에게 칼리가 클라이언트(피해자)라고 속이는 ARP 스푸핑

세 번째 터미널 : 중간자 위치에서 릴레이

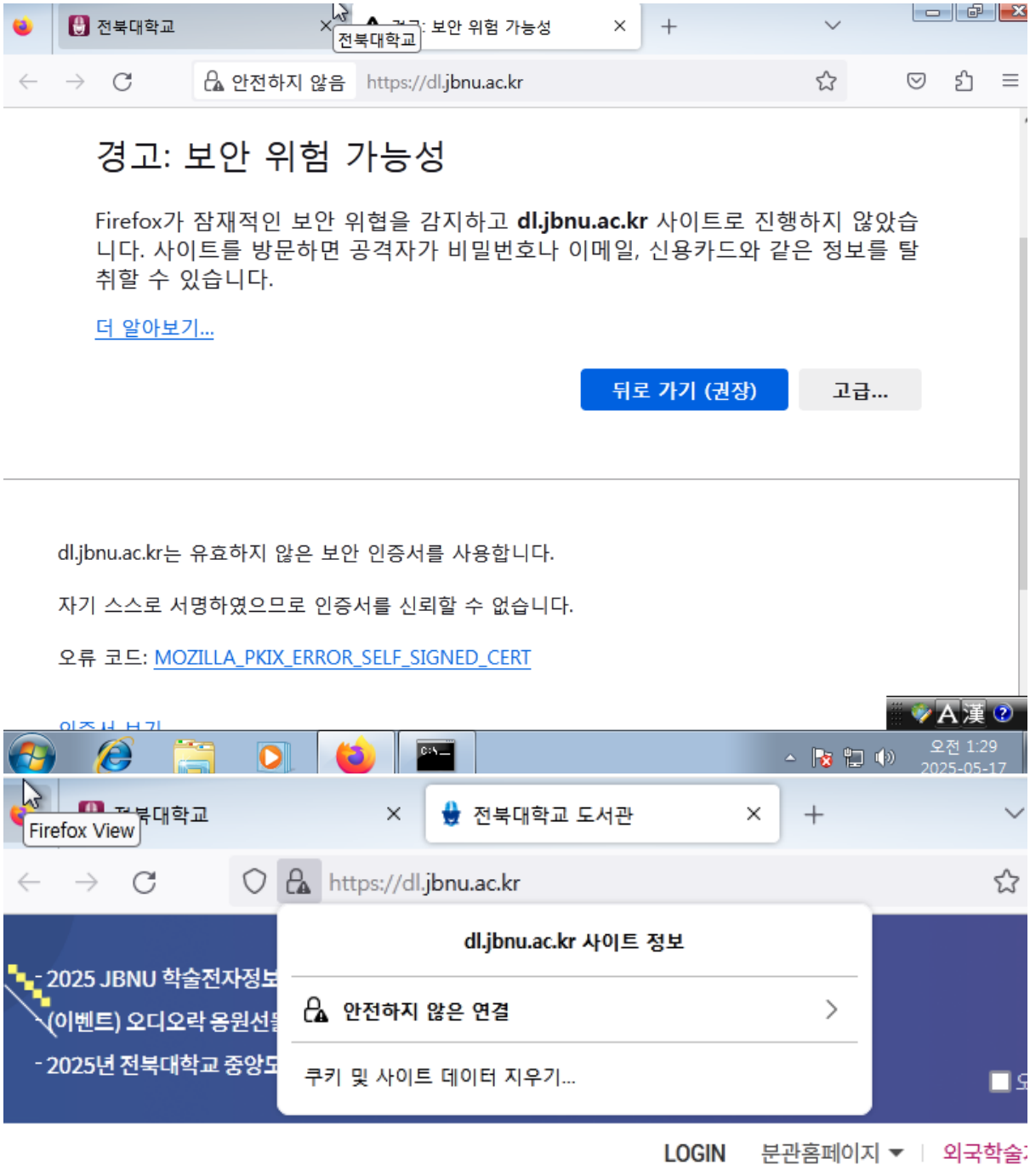
네 번째 터미널 : 피해자의 DNS 요청에 가짜 IP 응답을 반환하는 DNS 스푸핑



공격자(칼리)가 DNS 스푸핑을 통해 피해자의 요청을 가로채기 위해 클라(피해자)에서 DNS 캐시를 초기화 하여 공격이 이루어지도록 하였음



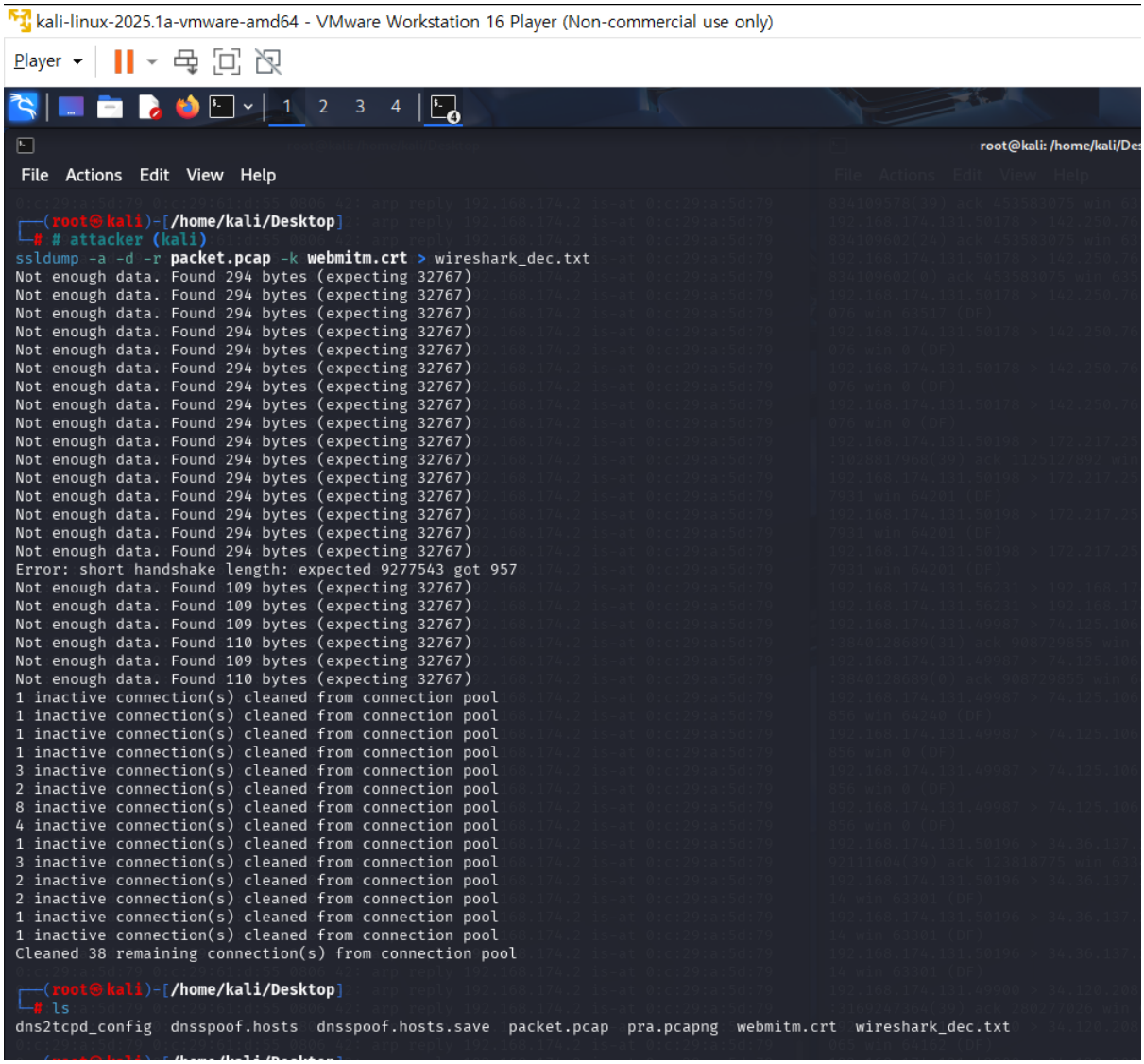
와이어 샤크로 ARP 스푸핑, DNS 스푸핑 이후 클라(피해자)가 공격자에게 리다이렉트 되어 트래픽이 오가는걸 캡처



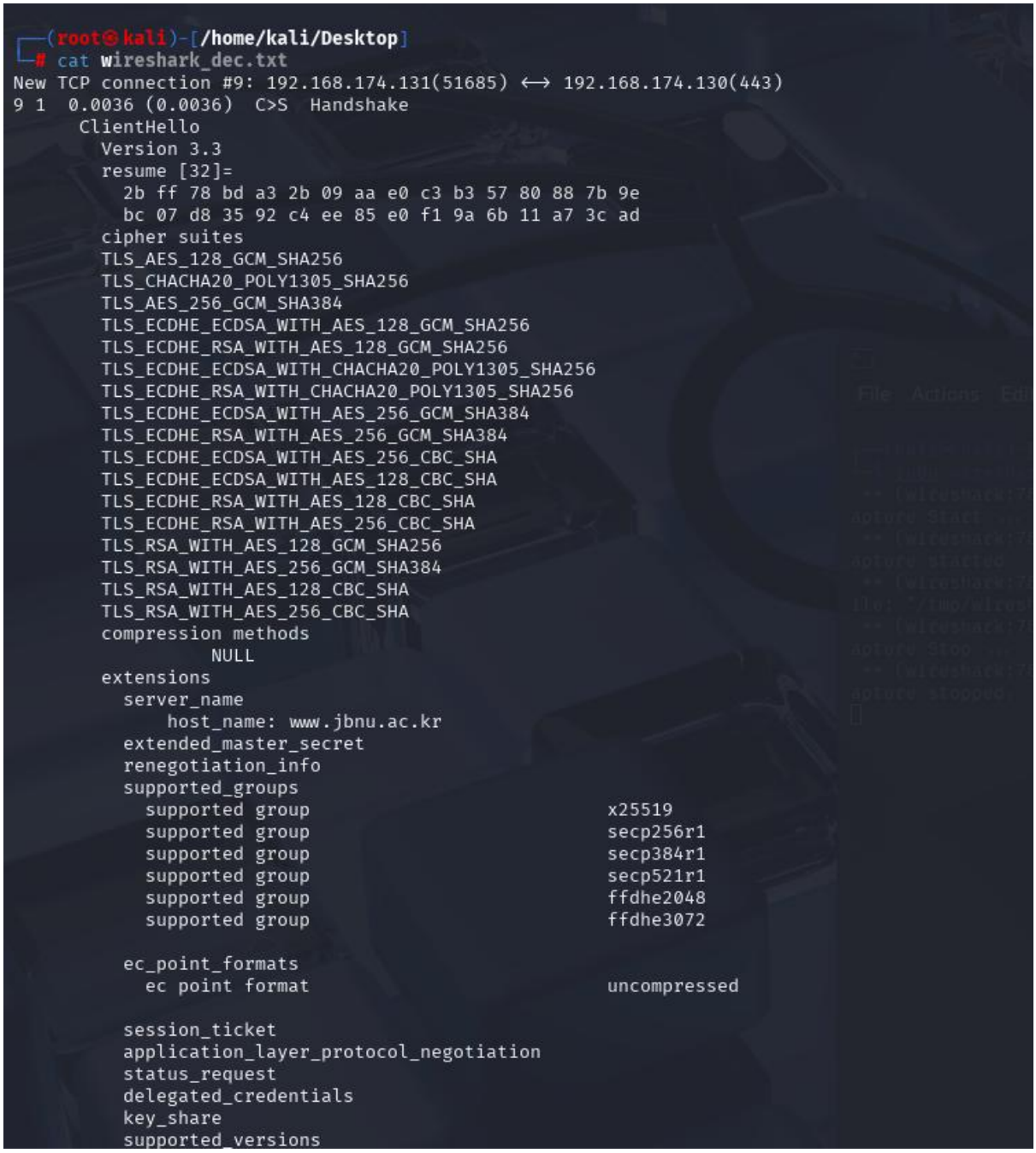
공격자가 자체 생성한 SSL 인증서를 통해 피해자의 HTTPS 접속 요청을 가로챘고 이로 인해 브라우저에서 인증서 경고창이 띄워진걸 볼 수 있고 인증서가 신뢰되지 않음을 알 수 있음

사용자가 경고를 무시하고 접속하면 공격자는 HTTPS 내용을 가로챌 수 있음

오류 메시지인 **MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT** 이 메시지는 webmitm 에서 생성된 인증서임을 알 수 있음



패킷 복호화를 위해 ssldump 를 사용하였으나 대부분 세션에서 Not enough data 가 출력되었음
여러가지 시도를 해보았지만 계속 동일하게 나와 그대로 실습을 진행하였음



복호화된 패킷은 클라가 공격자의 443 포트로 HTTPS 연결을 시도하며 전송한 ClientHello 메시지는 TLS 핸드셰이크 과정에서 전송하는 메시지로 클라와 서버가 암호화 통신을 시작하기 위한 메시지임

TCP 연결정보

Source IP : 192.168.174.131:51685(피해자)

Destination IP : 192.168.174.130:443(공격자)

TLS 버전 : 1.2 (version 3.3)

Resume : 클라는 이전 서버와 TLS 통신을 했던 세션 ID 를 재전송하여 해당 세션을 재사용함

Cipher Suites : 클라가 지원하는 암호화 방식들을 나열한 것임
Compression Method : 사용하지 않았음으로 NULL
Extensions
SNI : www.jbnu.ac.kr 도메인의 접근할 것을 지정하였음
Extended Master Secret : 세션 키 유도 시 보안을 강화하는 확장
Supported Groups : x25519, secp256r1, secp384r1, ffdhe2048 등 클라가 지원하는 키 교환 알고리즘

실습 후기

이번 실습을 통해 ARP 및 DNS 스푸핑 기반으로한 SSL 중간자 공격의 구체적인 수행을 할 수 있었다.

칼리를 이용해 클라와 서버 사이의 트래픽을 가로채고 가짜 인증서를 생성하여 SSL 통신을 복호화 해보는 과정은 상당히 흥미로웠다. 실습중 ssldump 복호화가 제대로 되지 않아 애를 먹고 여러가지를 찾아보고 원인을 분석해봤다. 이러한 결과로 SSL 프로토콜 구조와 패킷 복호화 과정에 대한 이해도가 깊어졌다.

이번 실습을 통하여 공격 방법을 익히는 것을 넘어 보안이 왜 중요하고 왜 HTTPS 와 인증서 검증이 필수적인지 실질적으로 느낄 수 있었다. 요즘같이 해킹이 난무한 시대에 보안은 정말로 필수적으로 알고 있어야 하는 것 같다. 보안은 뚫는 법을 알아야 막을 수 있다는 말이 있는 것처럼 다음엔 방어 하는 실습도 해보고 싶다.