

6. Replay Attack



Replay Attack은 정상적인 Packet을 중간에서 가로채 복사해 두었다가, 악의적인 목적으로 **Packet**을 반복해서 보내는 공격이다. 주로 인증을 통과하기 위해, 자신이 다른 사람인 것처럼 가장하여 Packet을 보내는 것이다.

6. Replay Attack

1. 실습 개요

다른 사람이 서버로 보내는 인증 정보 Password의 Hash 값을 중간에서 가로채어 복사해 두었다가, 나중에 가로챈 인증 정보를 서버로 보내어 인증을 통과한다.

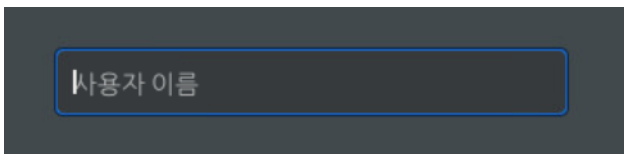
2. 시스템 정보

- * 공격자 Kali 계정 : root/root123
- * 웹 서버 CentOS7_GWJ 계정 : root/root123

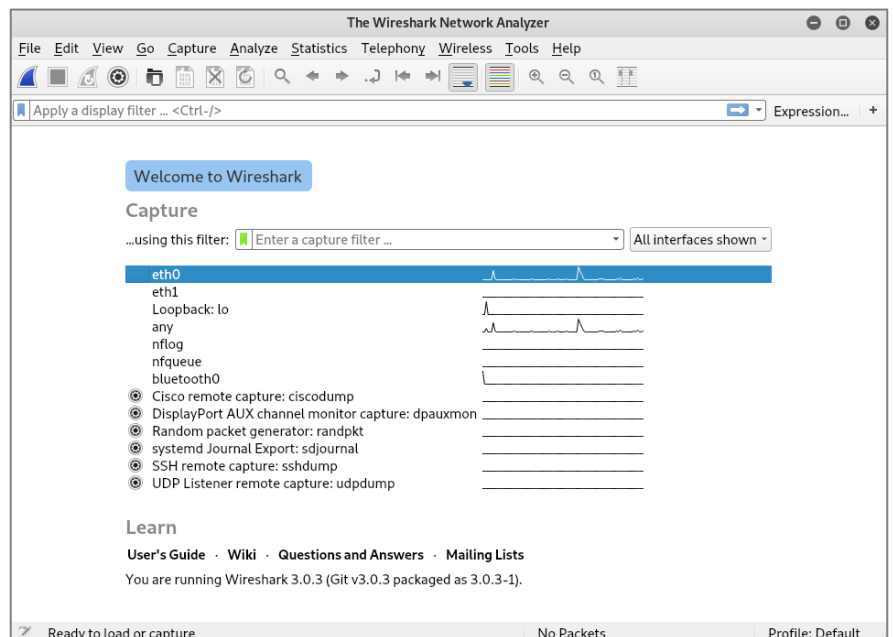
3. 문제풀이



1) (Kali) Kali 로그인 (root/root123)



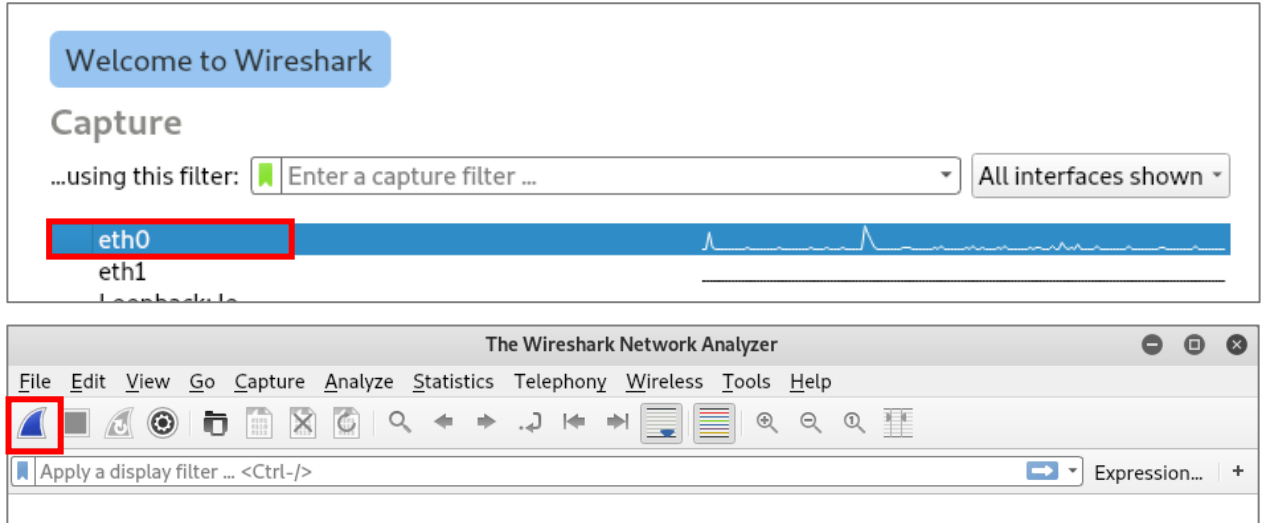
2) (Kali) WireShark 실행



6. Replay Attack

[공격]

3) (Kali) 인터페이스 선택 > 패킷캡처 시작

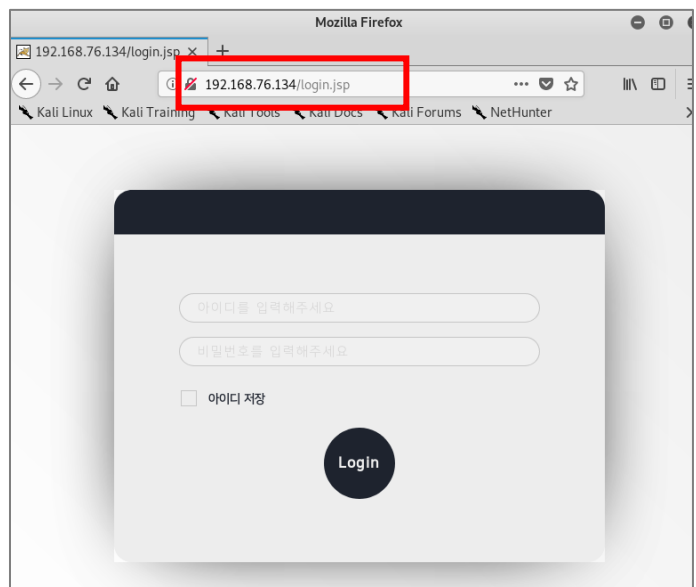
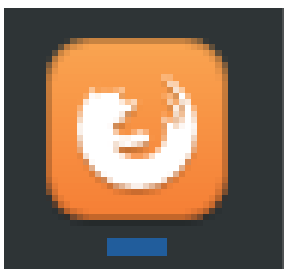


※ WireShark란?

와이어샤크는 네트워크 패킷을 캡처하고 분석하는 오픈소스 도구이다. 강력하고 쉬운 사용법 때문에 해킹 뿐만 아니라 보안 취약점 분석, 보안 컨설팅, 개인정보 영향평가 등 여러 분야에서 폭 넓게 사용된다.

Wireshark는 자체 프로그램으로 네트워크 트래픽을 캡처하는 것이 아니고, 운영체제에서 지원하는 캡처 라이브러리를 이용하여 수집한다.

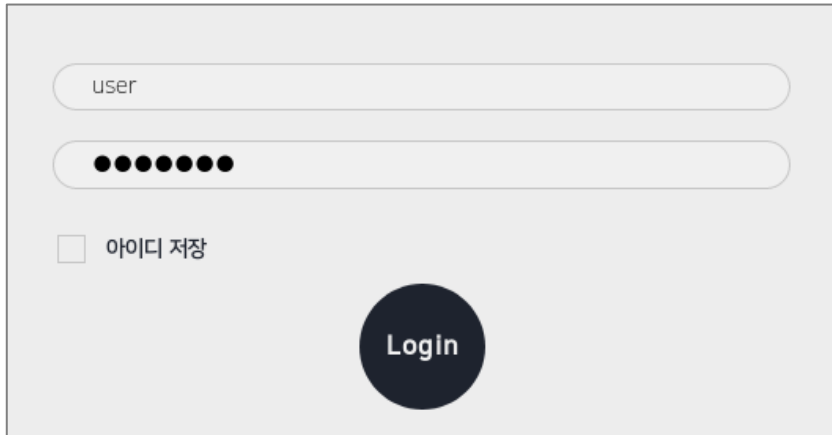
4) (Kali) Firefox 실행 > Web서버 로그인 페이지접속([웹 서버 IP]/login.jsp)
ex)192.168.76.134/login.jsp



6. Replay Attack

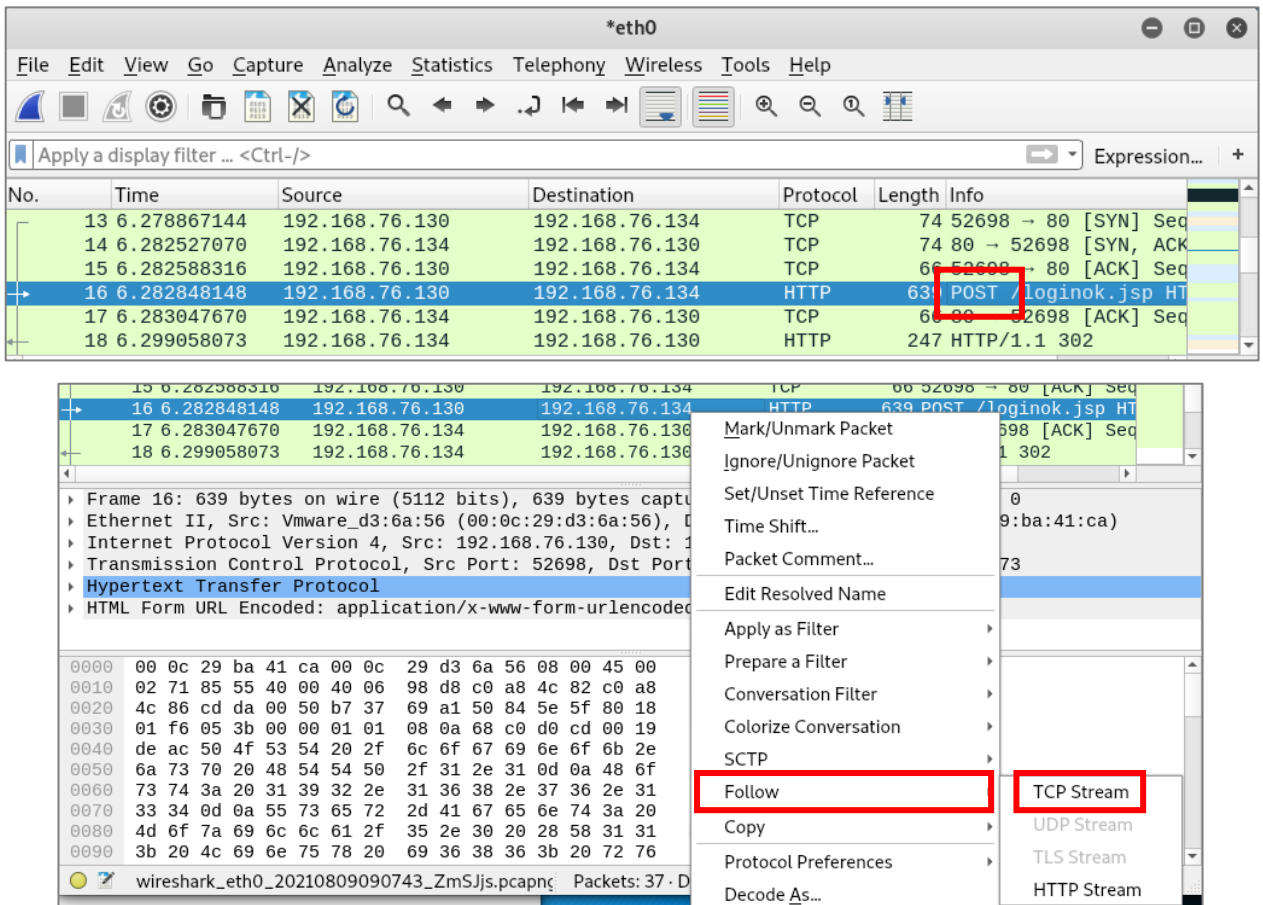
[공격]

- 5) (Kali) 웹페이지 로그인 페이지에서 사용자가 본인의 계정으로 정상 로그인(user/user!23) 했다고 가정



A login form with a text input field containing 'user', a password input field with 8 dots, a checkbox labeled '아이디 저장' (Save ID), and a large circular 'Login' button.

- 6) (Kali) WireShark로 ID/PW 스니핑
POST방식으로 보내지는 패킷 선택 > 해당 패킷 찾아서 마우스 오른쪽 클릭 > Follow > TCP Stream



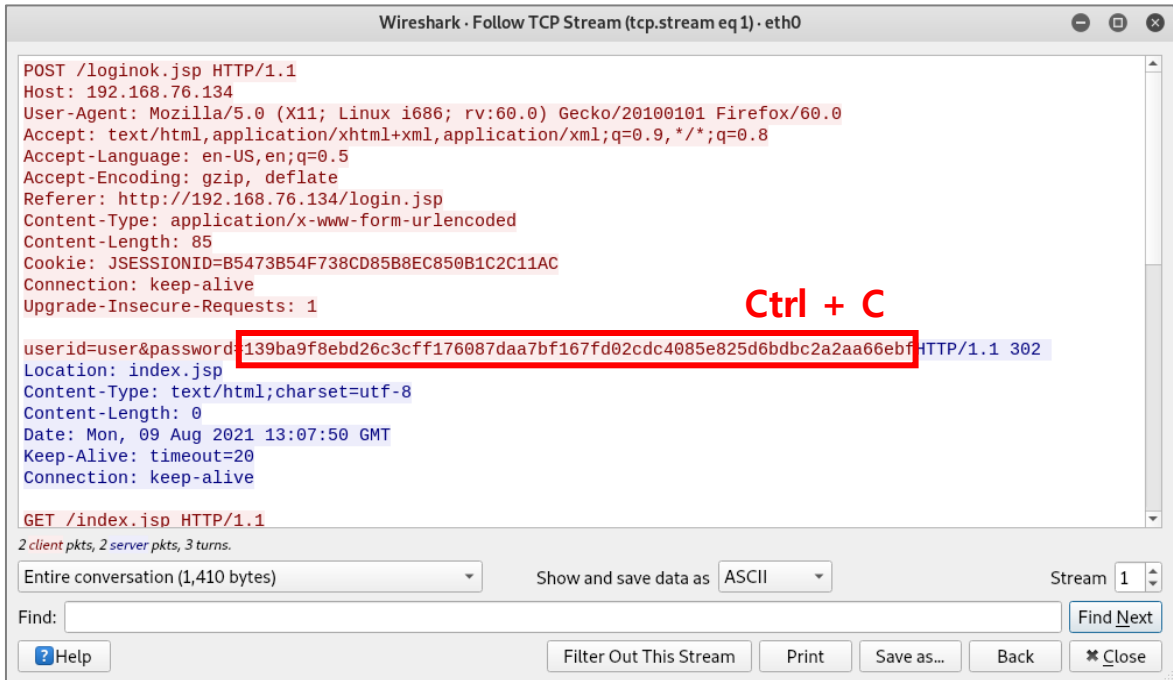
The image shows a Wireshark packet capture window for interface *eth0. The packet list shows several packets, with packet 16 (HTTP POST) selected. A right-click context menu is open over packet 16, and the 'Follow' option is highlighted. A secondary menu is open from 'Follow', showing 'TCP Stream' as the selected option. The packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
13	6.278867144	192.168.76.130	192.168.76.134	TCP	74	52698 → 80 [SYN] Seq...
14	6.282527070	192.168.76.134	192.168.76.130	TCP	74	80 → 52698 [SYN, ACK] Seq...
15	6.282588316	192.168.76.130	192.168.76.134	TCP	60	52698 → 80 [ACK] Seq...
16	6.282848148	192.168.76.130	192.168.76.134	HTTP	639	POST /loginok.jsp HT...
17	6.283047670	192.168.76.134	192.168.76.130	TCP	60	80 → 52698 [ACK] Seq...
18	6.299058073	192.168.76.134	192.168.76.130	HTTP	247	HTTP/1.1 302

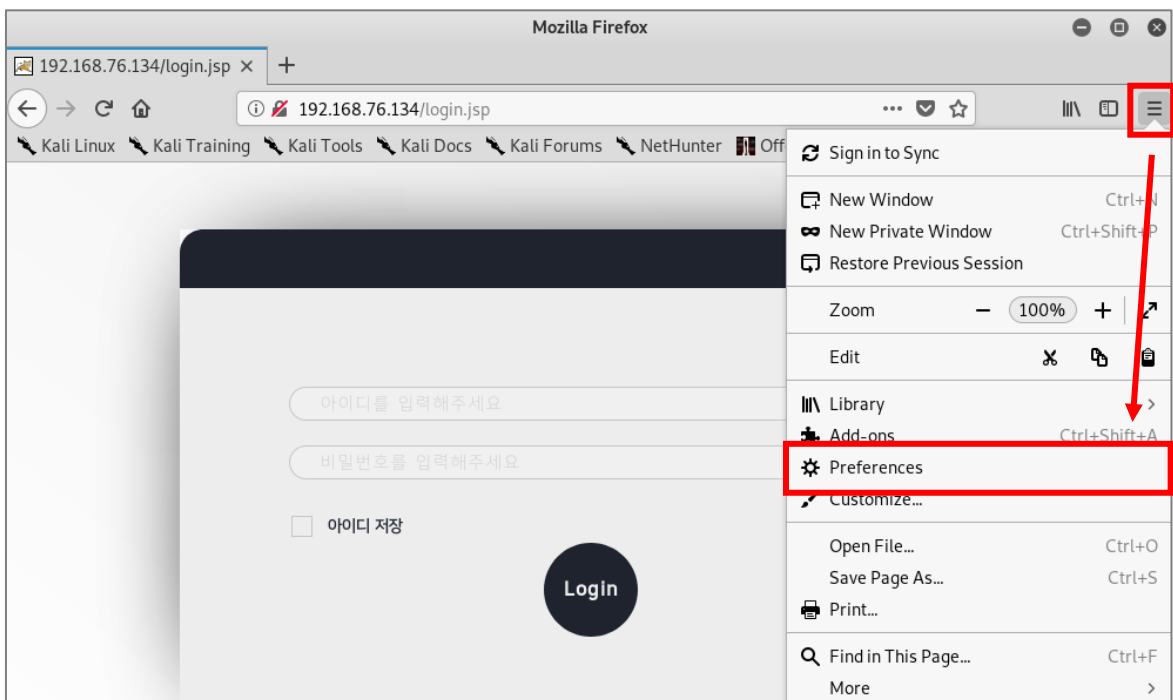
6. Replay Attack

[공격]

7) (Kali) TCP Stream > 내용 확인 > 사용자 계정 ID와 PW해시 값 탈취 > PW해시 값 복사

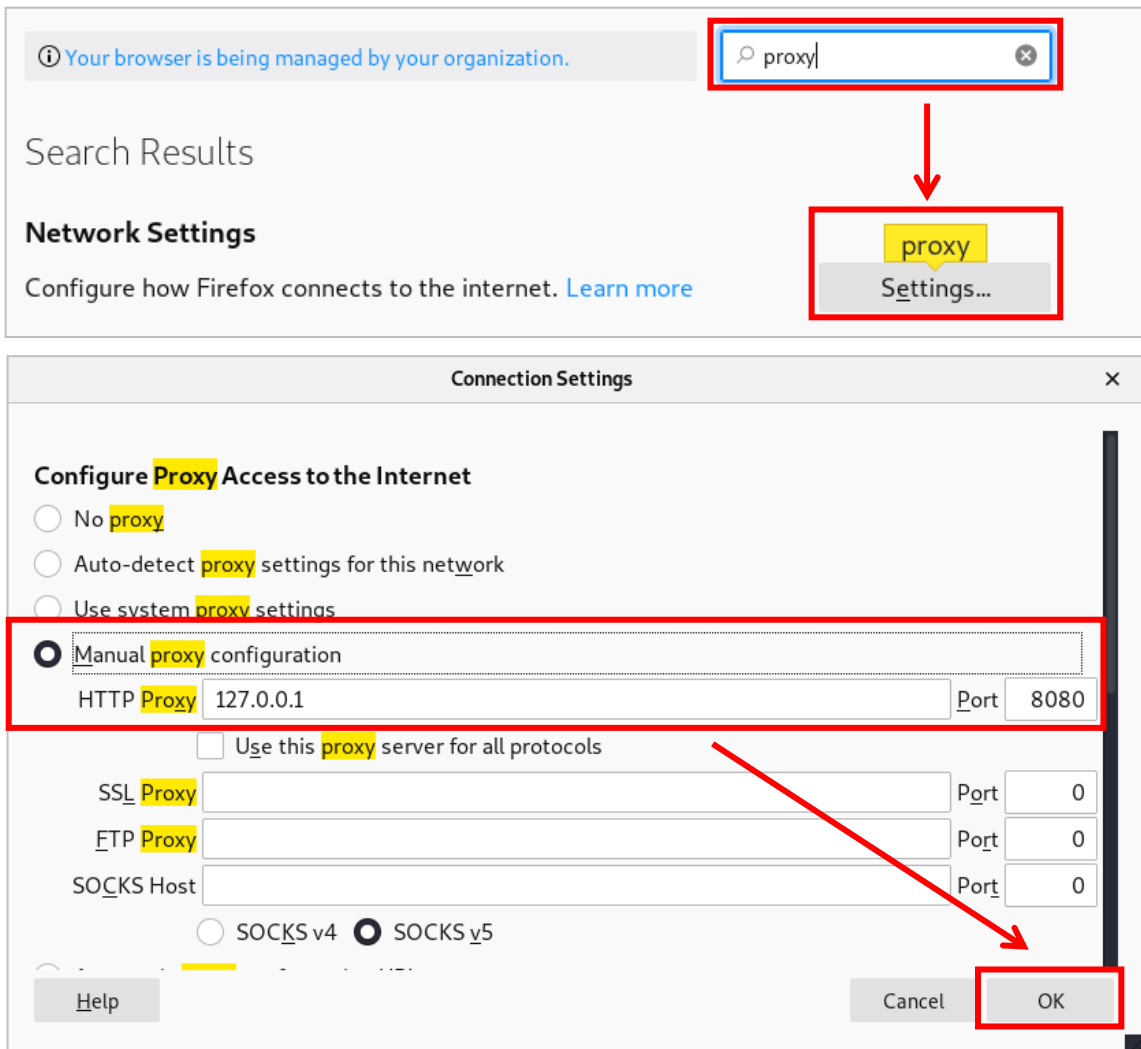


8) (Kali) 로그인창 재접속 > Preferences > 'Proxy' 검색 > Settings > Manual proxy configuration > 'OK' 클릭

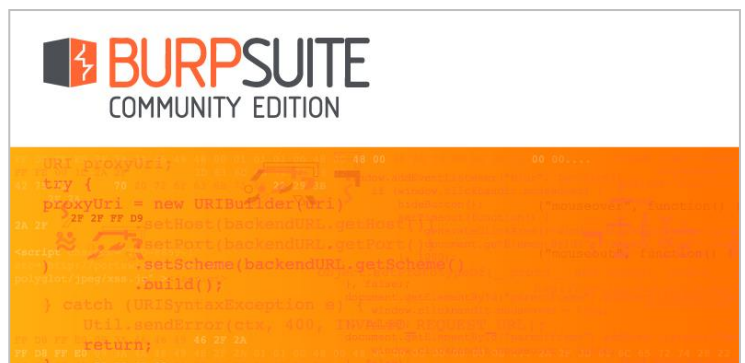
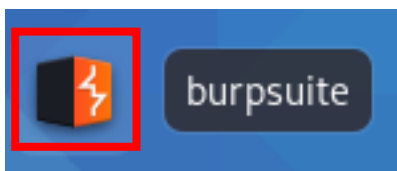


6. Replay Attack

[공격]



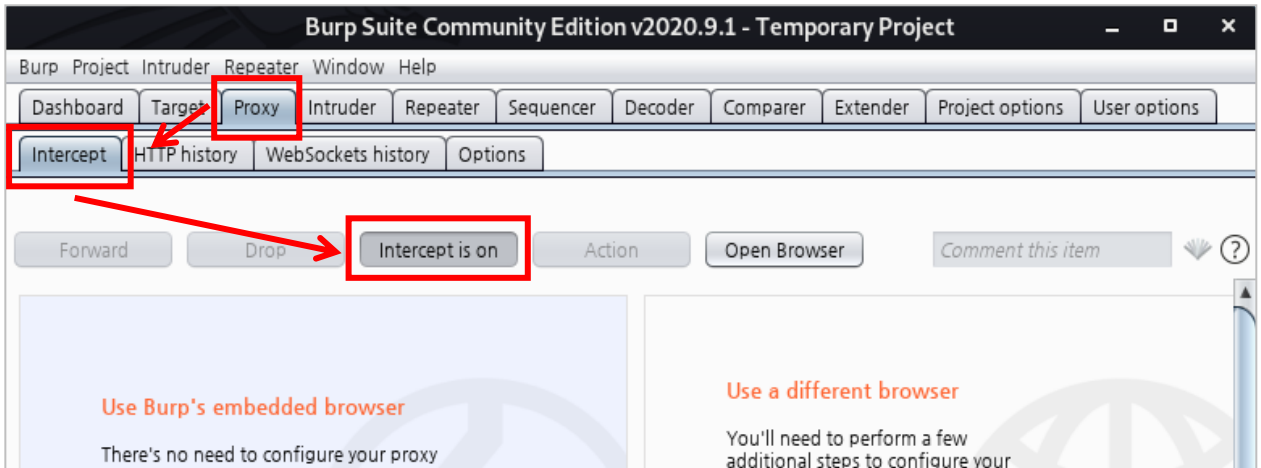
9) (Kali) Burp Suite 실행 > Next > Start Burp > Proxy > Intercept is on



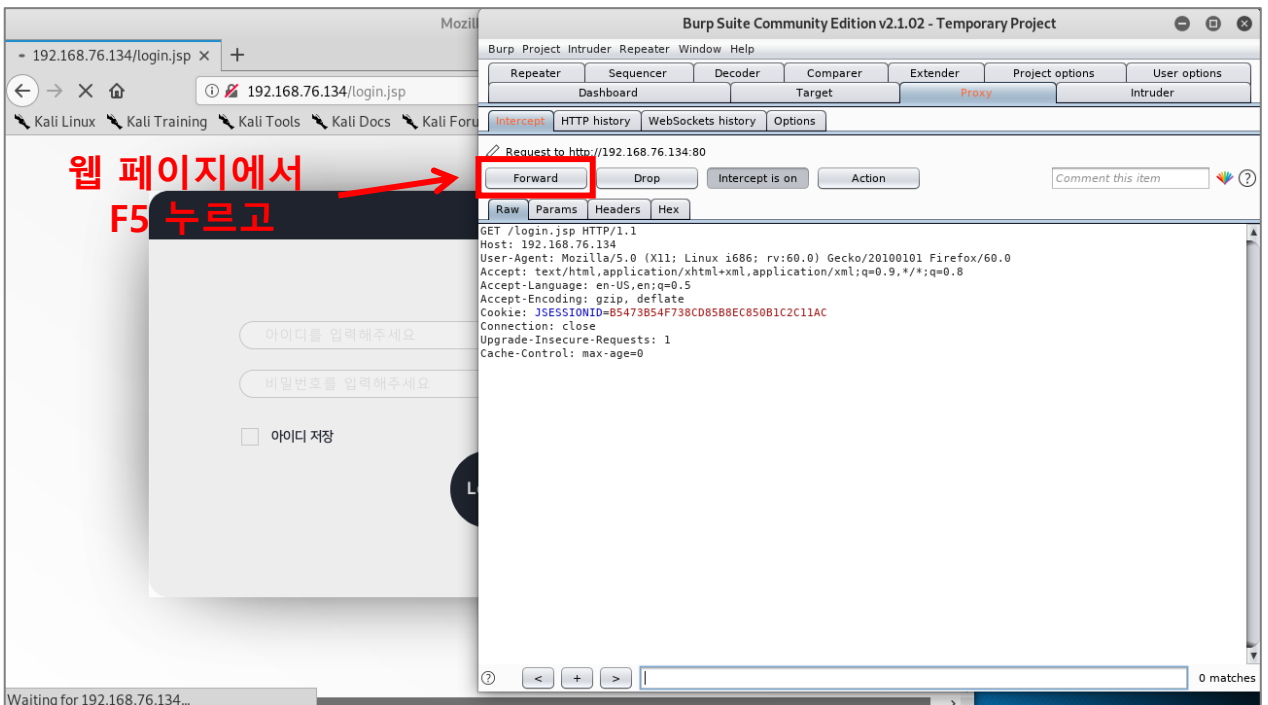
6. Replay Attack

[공격]

10) (Kali) Next > Start Burp > Proxy탭 > Intercept탭 > Intercept is on 상태가 되도록 설정



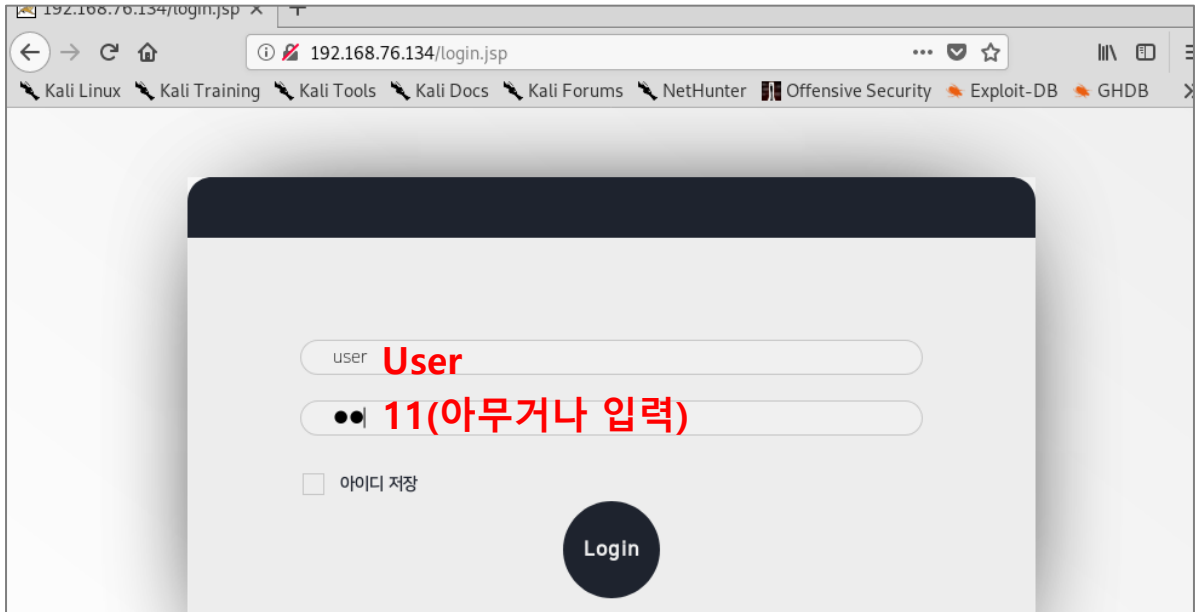
11) (Kali) 접속해있던 웹페이지 새로고침 (F5) 누르면 Burp Suite의 Proxy 서버에서 'Forward'를 계속 누르면서 패킷이 지나가는 흐름 확인



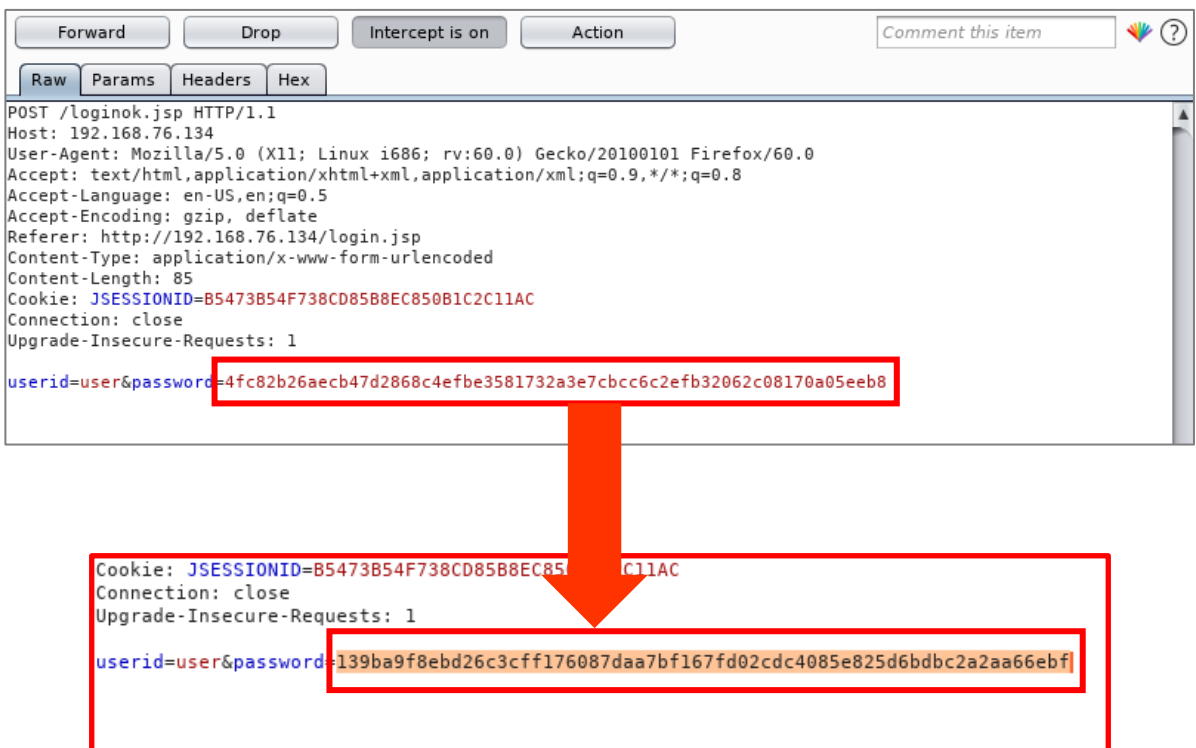
6. Replay Attack

[공격]

12) (Kali) 로그인 창에 탈취한 ID와 PW 아무거나 입력하고 로그인 버튼 클릭



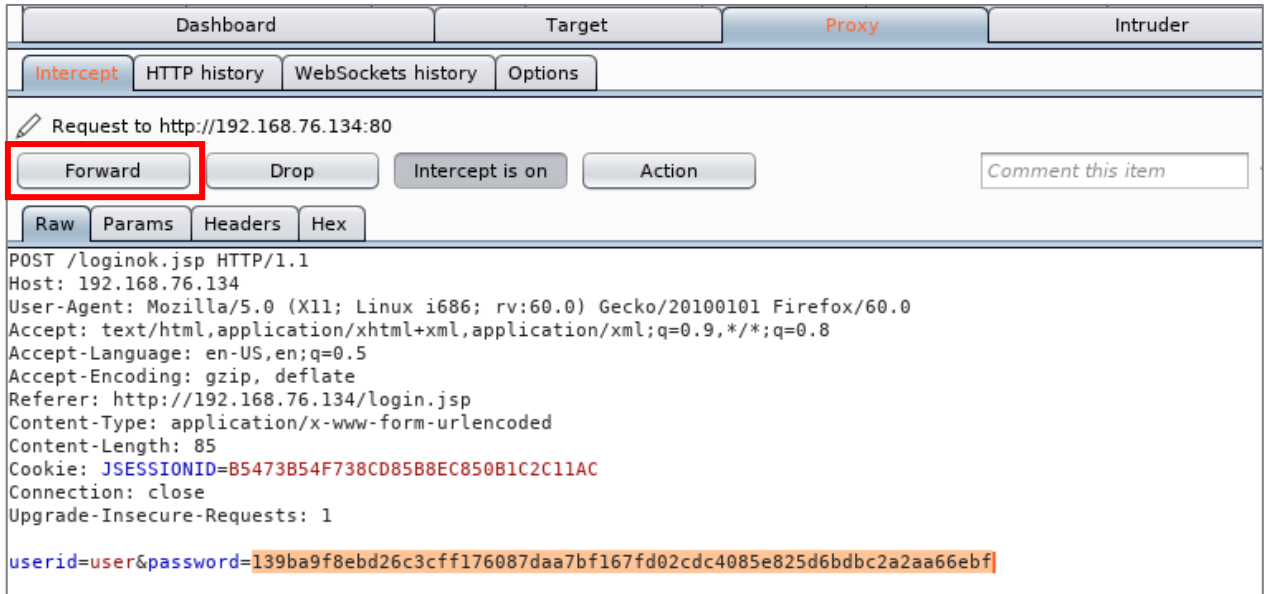
13) (Kali) BurfSuite에서 'Forward'버튼 계속 누르다 보면 입력한 값에 대한 ID와 PW 해시 값이 나타나는데 이때 복사해 났던 해시 값으로 수정



6. Replay Attack

[공격]

14) (Kali) 'Forward' 버튼 계속 누르면 로그인 되는 것 확인, Replay Attack 성공



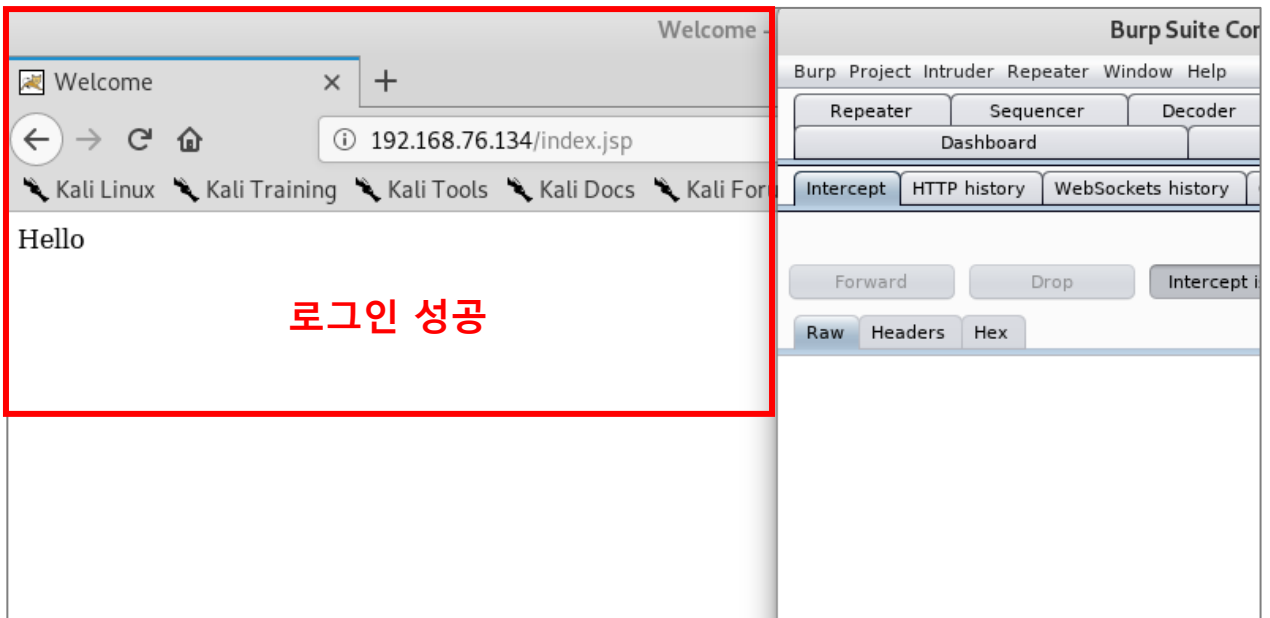
Request to http://192.168.76.134:80

Forward Drop Intercept is on Action [Comment this item](#)

Raw Params Headers Hex

```
POST /loginok.jsp HTTP/1.1
Host: 192.168.76.134
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.76.134/login.jsp
Content-Type: application/x-www-form-urlencoded
Content-Length: 85
Cookie: JSESSIONID=B5473B54F738CD85B8EC850B1C2C11AC
Connection: close
Upgrade-Insecure-Requests: 1

userid=user&password=139ba9f8ebd26c3cff176087daa7bf167fd02cdc4085e825d6bdbc2a2aa66ebf
```



Welcome

192.168.76.134/index.jsp

Kali Linux Kali Training Kali Tools Kali Docs Kali For

Hello

로그인 성공

Burp Suite Cor

Burp Project Intruder Repeater Window Help

Repeater Sequencer Decoder

Dashboard

Intercept HTTP history WebSockets history

Forward Drop Intercept i

Raw Headers Hex