

9/7 공부내용_공재호

Asignee	
Joined	@Sep 7, 2020 3:15 PM
Location	공재호
Title	

1. send_arp 수정

- 칼리 자체 오류 너무나서 다시 설치중.....

타겟 pc에서 아이디, 비번 로그인

게시판

52.78.238.225/login

[홈으로 돌아가기](#)

[회원가입 목록보기](#)

로그인 하기

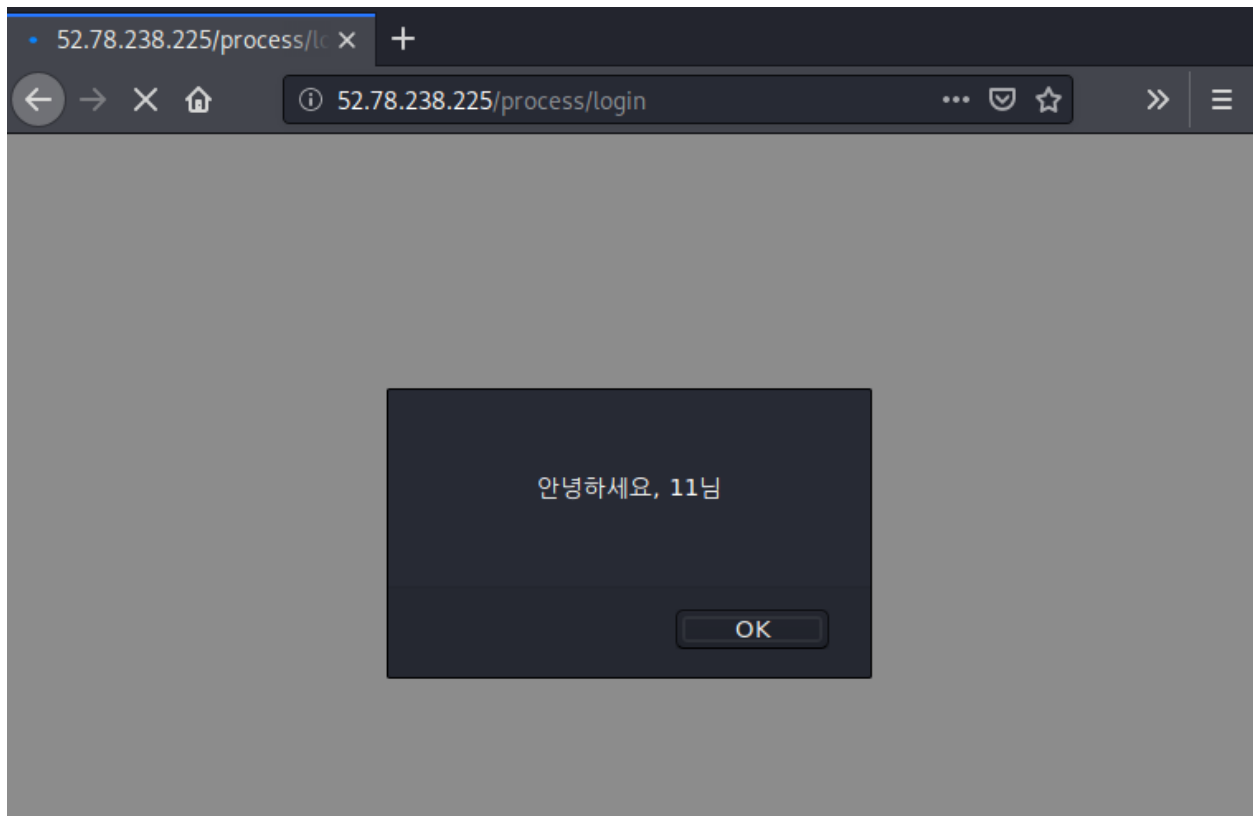
아이디

1

비밀번호

1

로그인



Capturing from eth1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
5	1.023684307	172.30.1.43	52.78.238.225	HTTP	470	GET /login HTTP/1.1
175	7.405193104	77.86.229.90	172.30.1.47	HTTP	10160	HTTP/1.1 206 Partial Content
189	7.670428694	172.30.1.47	77.86.229.90	HTTP	359	GET /online/qtsdkrepository/li
198	8.293336480	172.30.1.43	52.78.238.225	HTTP	470	GET /login HTTP/1.1
200	8.302228733	52.78.238.225	172.30.1.43	HTTP	1518	HTTP/1.1 200 OK (text/html)
212	8.714707629	52.78.238.225	172.30.1.43	HTTP	1518	HTTP/1.1 200 OK (text/html)
225	10.918416041	172.30.1.43	52.78.238.225	HTTP	553	POST /process/login HTTP/1.1
233	13.307583784	172.30.1.43	52.78.238.225	HTTP	553	POST /process/login HTTP/1.1
322	34.186143140	77.86.229.90	172.30.1.47	HTTP	398	HTTP/1.1 200 OK (text/plain)
330	34.445617070	172.30.1.47	77.86.229.90	HTTP	354	GET /online/qtsdkrepository/li

Frame 414: 553 bytes on wire (4424 bits), 553 bytes captured (4424 bits) on interface eth1, id 0

Ethernet II, Src: PcsCompu_e3:e4:f0 (08:00:27:e3:e4:f0), Dst: Mercury_4d:ed:1d (b4:a9:4f:4d:ed:1d)

Internet Protocol Version 4, Src: 172.30.1.43, Dst: 52.78.238.225

Transmission Control Protocol, Src Port: 36496, Dst Port: 80, Seq: 1, Ack: 1, Len: 487

Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "id" = "1"
- Form item: "pw" = "1"

```

0000  b4 a9 4f 4d ed 1d 08 00 27 e3 e4 f0 08 00 45 00  ..OM....'.....E-
0010  02 1b 1c 86 40 00 40 06 4b de ac 1e 01 2b 34 4e  ...@.@.K....+4N
0020  ee e1 8e 90 00 50 e9 4c db 02 ee 5f 73 7a 80 18  ....P.L...sz...
0030  01 f6 31 26 00 00 01 01 08 0a 37 4b 0f a7 24 0d  ..1&....~7K~$.
0040  be f6 50 4f 53 54 20 2f 70 72 6f 63 65 73 73 2f  ..POST / process/
0050  6c 6f 67 69 6e 20 48 54 54 50 2f 31 2e 31 0d 0a  login HT TP/1.1..
0060  48 6f 73 74 3a 20 35 32 2e 37 38 2e 32 33 38 2e  Host: 52 .78.238.
0070  32 32 35 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a  225..Use r-Agent:
0080  20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31  Mozilla /5.0 (X1
0090  31 3b 20 4c 69 6e 75 78 20 78 38 36 5f 36 34 3b  i; Linux x86_64;
00a0  20 72 76 3a 36 38 2e 30 29 20 47 65 63 6b 6f 2f  rv:68.0 ) Gecko/
00b0  32 30 31 30 30 31 30 31 20 46 69 72 65 66 6f 78  20100101 Firefox

```

eth1: <live capture in progress> Packets: 6030 · Displayed: 24 (0.4%) Profile: Default

→ 평문으로 보낸 아이디 비번 유출 가능