Cyber Security
test-bed installation guide

What is test-bed?

A scenario based simulation system that used for cyber attacking (ethical hacking) and defending test

What is test-bed ?

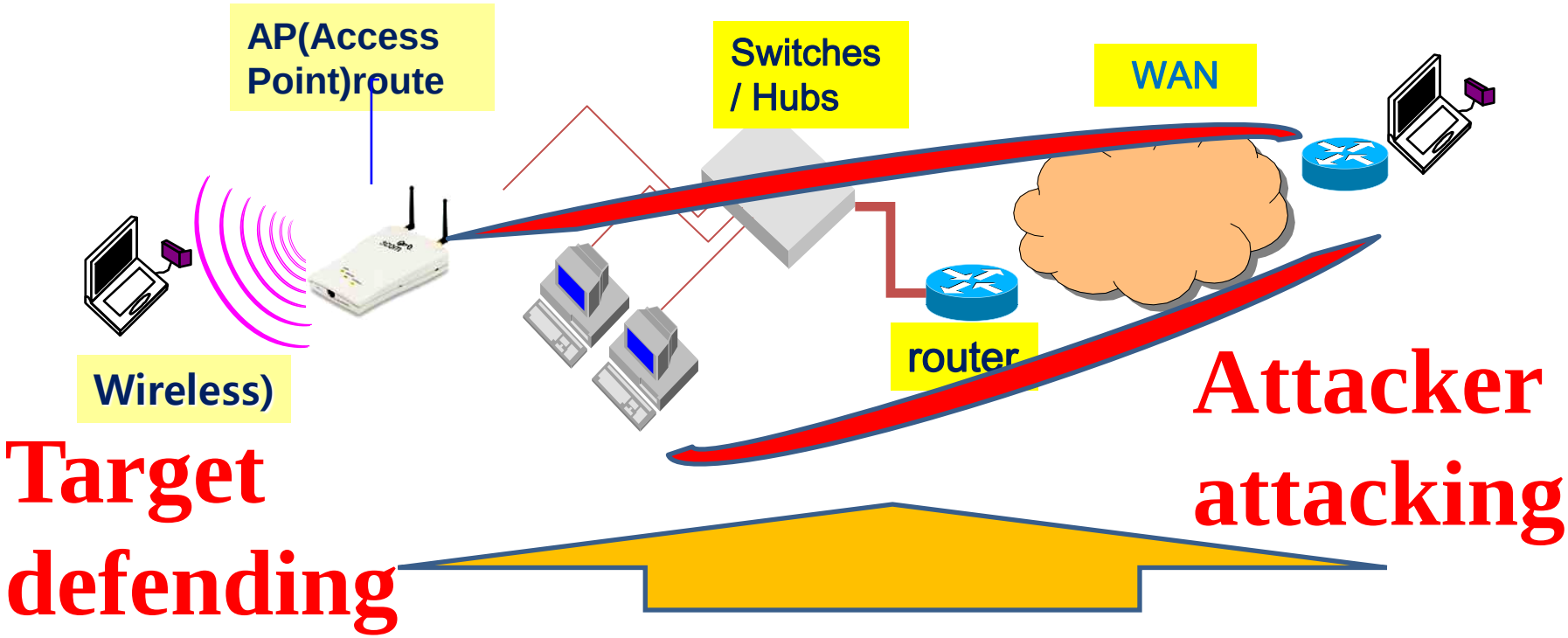
- **The test-bed is a real or virtual system for ethical hacking, pen-test and vulnerability checking.**

- **ethical hacking => attacking the target system for finding weak point in security side**

- **pen-test => programmed attacking on test-bed for finding weak point in security side**

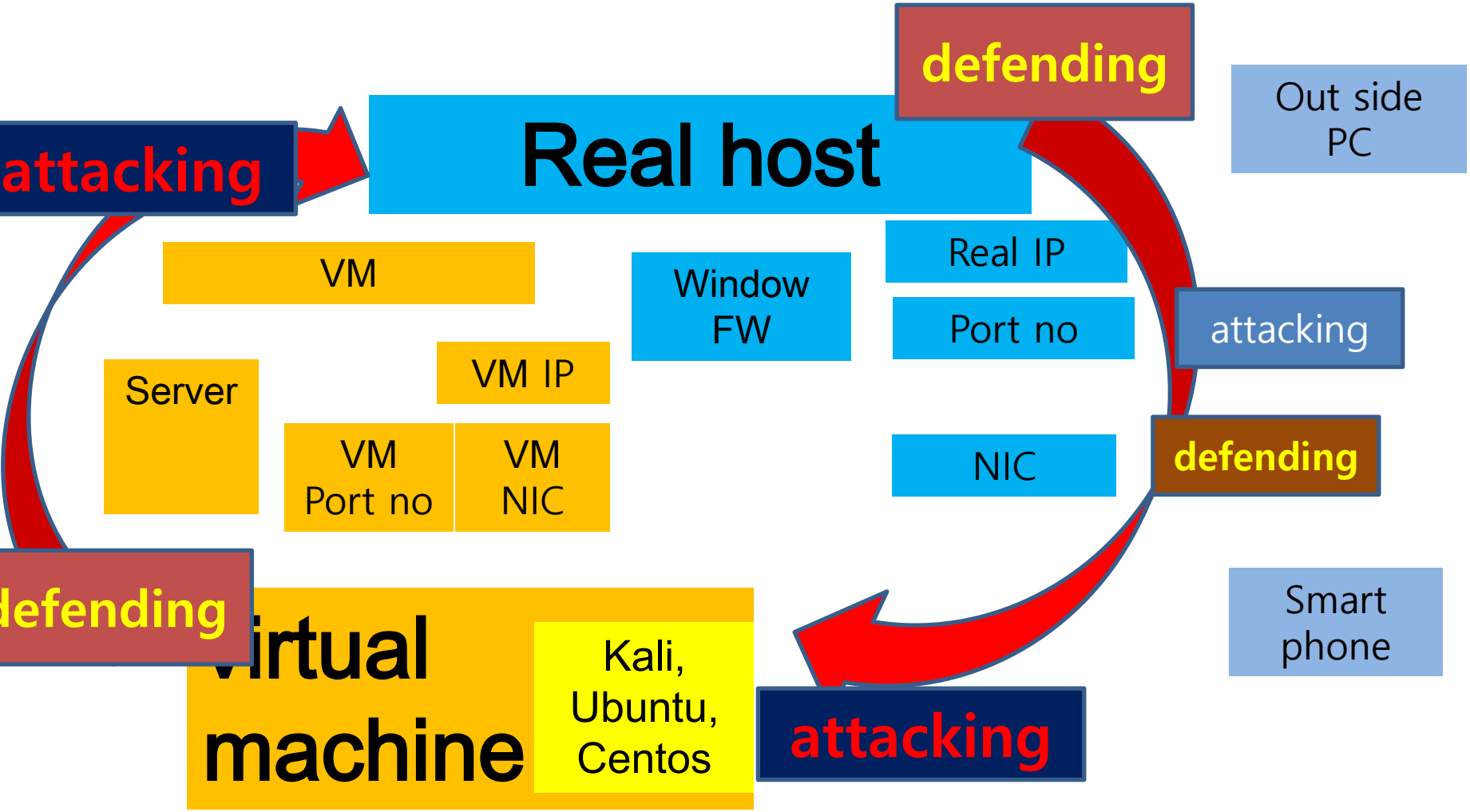
- **vulnerability checking => directly search weak point of target system using tools or application**

Test-bed on real system



Wired / wireless hybrid connection
connection internal, external network

Test-bed on virtual system



Through test-bed

- NW security test,
- Web security test,
- Secure coding test,
- Encryption and decryption test,
- Vulnerability analysis
- IoT test

How to set test-bed

Cyber security test-bed resource

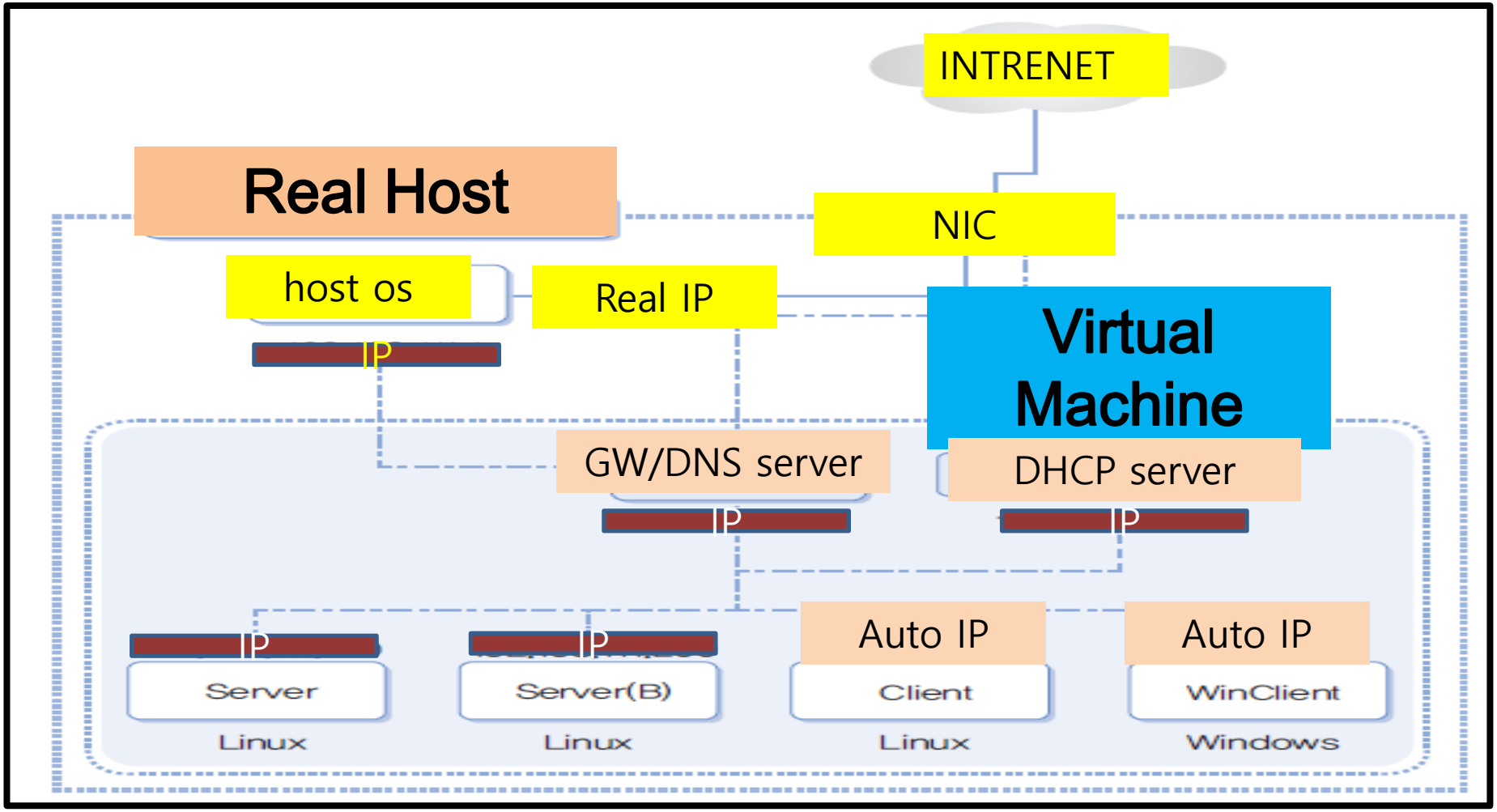
	ATTACKER	TARGET
role	hacker	victim
Host & target address	Student's real IP Student's VM IP	Real system :CTU,CICT IP VM : stident's VM IP
HW	Class terminal	Class terminal
NW	Hub, router, GW	
VM OS	Real host(window) VM(Kali,Ubuntu,Centos)	VM host(window) VM(Kali,Ubuntu,Centos)
Web	VM Web	VM Web
Cloud Web	VM Cloud Web	VM Cloud Web
IoT	VM Cloud IoT	VM Cloud IoT

Resource for test-bed installation

- **Network : AP,line, switch, router, G/W**
- **HW: terminal(PC, notebook), servers**
- **SW: virtual machine,**
- **OS: Window, Kali, Ubuntu, Centos, Mac**
- **SW : Web,**
- **Language : C, Java, Python3, Scapy**

CICT`s environment

Virtual machine configuration



Virtual machine configuration

Name	Server	Server	Client	WinClient
Guest OS	Fedora64bits	Fedora64bits	Fedora64bits	Window10^2
IP types	static IP	static IP	auto IP by DHCP	auto IP by DHCP
Subnet mask	manualy setting	manualy setting	auto IP by DHCP	auto IP by DHCP
gateway	manualy setting	manualy setting	auto IP by DHCP	auto IP by DHCP
DNS server	manualy setting	manualy setting	auto IP by DHCP	auto IP by DHCP

Test-bed type

Test-bed type

Type	Attacker	Defender	System type
Type A (one PC)	guest OS Linux	host OS window10	VMware or Virtual box one PC
Type B (one PC)	guest OS Linux	guest OS Linux	VMware or Virtual box one PC
Type C (one PC)	host OS Window10	guest OS Linux	VMware or Virtual box one PC
Type D (two PCs)	host OS Window10	host OS Window10	different two PC neighbor PC in class

Test-bed setting[sering] process

① Select VM type & configuration
② Select test-bed type
③ Download & Install VM
④ Download & Install OS on VM
⑤ Define host & target address list
⑥ Check connection route internal, external network
⑦ Packet sending test

Test-bed setting[sering] process

Define attacker, target

To scan or attack other system is illegal

We define our system for security test

	Attacker system	Target system
	Hacker	victim
Host & target address	**Student's real IP** **Student's VM IP**	**Real system:CTU,CICT IP** **VM : stident's VM IP**

Search test-bed IP in class

- Host => ipconfig/all =>Vmware Virtual Ethernet Adapter for Vmnet8
- Host => arp –a => dynamic address
- Guest => ifconfig => ether 0 => inet addr

Check real host Window address

CMD ipconfig/all

```
   링크-로컬 IPv6 주소 . . . . . : fe80::31fa:b31a:7514:fe39%10(기본 설정)
   IPv4 주소 . . . . . . . . . . : 192.168.148.1(기본 설정)
   서브넷 마스크 . . . . . . . . : 255.255.255.0
   기본 게이트웨이 . . . . . . . :
   DHCPv6 IAID . . . . . . . . . : 167792726
   DHCPv6 클라이언트 DUID. . . . : 00-01-00-01-22-C1-13-06-98-83-89-48-A1-83
   DNS 서버. . . . . . . . . . . : fec0:0:0:ffff::1%1
                                   fec0:0:0:ffff::2%1
                                   fec0:0:0:ffff::3%1
   Tcpip를 통한 NetBIOS. . . . . : 사용

이더넷 어댑터 VMware Network Adapter VMnet8:

   연결별 DNS 접미사. . . . . :
   설명. . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet8
   물리적 주소 . . . . . . . . . : 00-50-56-C0-00-08
   DHCP 사용 . . . . . . . . . . : 아니요
   자동 구성 사용. . . . . . . . : 예
   링크-로컬 IPv6 주소 . . . . . : fe80::5c38:e742:aa29:aa%24(기본 설정)
   IPv4 주소 . . . . . . . . . . : 192.168.159.1(기본 설정)
   서브넷 마스크 . . . . . . . . : 255.255.255.0
   기본 게이트웨이 . . . . . . . :
   DHCPv6 IAID . . . . . . . . . : 402673750
   DHCPv6 클라이언트 DUID. . . . : 00-01-00-01-22-C1-13-06-98-83-89-48-A1-83
   DNS 서버. . . . . . . . . . . : fec0:0:0:ffff::1%1
                                   fec0:0:0:ffff::2%1
                                   fec0:0:0:ffff::3%1
   Tcpip를 통한 NetBIOS. . . . . : 사용
```

Search guest OS Ubuntu

$ ifconfig

Ubuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

student@clc: ~

```
student@clc:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:ee:4d:a0
          inet addr:172.30.117.121  Bcast:172.30.117.255  Mask:255.255.255.0
          inet6 addr: fe80::3283:b387:90d5:23b2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19141 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5785 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13961254 (13.9 MB)  TX bytes:518204 (518.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:305 errors:0 dropped:0 overruns:0 frame:0
          TX packets:305 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:23362 (23.3 KB)  TX bytes:23362 (23.3 KB)

student@clc:~$
```

Check guest OS name: GNU/Linux

$ uname -o

```
student@clc:~$ uname -o
GNU/Linux
```

Check Virtual Machine name: VirtualBox

$ uname -a

```
student@clc:~$ uname -a
Linux clc 4.15.0-29-generic #31~16.04.1-Ubuntu SMP Wed Jul 18 08:54:04 UTC 2018
x86_64 x86_64 x86_64 GNU/Linux
```

NW Test process

What kind of test on NW ?

NW security test => starting of test

- Environmental check
- Packet exchanging test
- Packet routing route check test
- DoS, DDoS attack & defence simulation

NW Test process

① Search target IP
② Send attacking packet to target
③ Check connection route
④ Scan open port in target IP
⑤ Enter into target system through open port
⑥ Exploit target system
⑦ Analyze the test result

Search guest OS Centos

$ ifconfig

```
File  Edit  View  Search  Terminal  Help
[noat@localhost ~]$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:E1:98:AD
          inet addr:172.30.117.52  Bcast:172.30.117.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fee1:98ad/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:12503 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4728 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13722705 (13.0 MiB)  TX bytes:292932 (286.0 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:94 errors:0 dropped:0 overruns:0 frame:0
          TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:8920 (8.7 KiB)  TX bytes:8920 (8.7 KiB)
```

Target address list for testing

- **C:₩Users₩pc>nslookup cit.ctu.edu.vn**
- 서버: vip.cnmnoc.co.kr
- **Address: 182.172.255.180**

- 권한 없는 응답:
- 이름: cit.ctu.edu.vn
- **Address: 123.30.143.202**

Target address list for testing

- **CTU domain name ctu.edu.vn**
- **CTU IPv4 123.30.143.225**

- **CICT domain name cit.ctu.edu.vn**
- **CICT IPv4 123.30.143.202**
-
- **Neighbor student's address in class IPv4**

To scan or attack other system is illegal

Just ping or tracert test

- **Google domain name google.com**
- **Google IPv4 142.250.207.14**

Target address list for testing

- **Loopback address127.0.0.1**

- The most commonly used IP address on the loopback network is **127.0. 0.1 for IPv4 and ::1 for IPv6**.

- **The standard domain name for the address is localhost**.

What is 127.0 0.1 address used for?

- the IP address of the local computer.
- This IP address allows the machine to connect to and communicate with itself.
- Therefore, localhost (127.0. 0.1) is used **to establish an IP connection to the same device used by the end-user**.

Loopback
cmd ping 127.0.0.1

- C:₩Users₩pc>ping 127.0.0.1

- Ping 127.0.0.1 32바이트 데이터 사용:
- 127.0.0.1의 응답: 바이트=32 시간<1ms TTL=128
- 127.0.0.1의 응답: 바이트=32 시간<1ms TTL=128
- 127.0.0.1의 응답: 바이트=32 시간<1ms TTL=128
- 127.0.0.1의 응답: 바이트=32 시간<1ms TTL=128

- 127.0.0.1에 대한 Ping 통계:
- 패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
- 왕복 시간(밀리초):
- 최소 = 0ms, 최대 = 0ms, 평균 = 0ms

Environmental check

Check connection route internal, external network

CMD tracert outside network

C:\Windows\system32\cmd.exe

```
C:\Users\student>tracert 172.30.117.51

Tracing route to 172.30.117.51 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  172.30.117.51

Trace complete.

C:\Users\student>
```

Window cmd tracert 127.0.0.1

- C:₩Users₩pc>tracert 127.0.0.1

- 최대 30홉 이상의
- DESKTOP-C27V8J7 [127.0.0.1](으)로 가는 경로 추적:

- 1 <1 ms <1 ms <1 ms DESKTOP-C27V8J7 [127.0.0.1]

- 추적을 완료했습니다.

Search MAC address

CMD arp -a

Select C:\Windows\system32\cmd.exe

```
C:\Users\student>arp -a

Interface: 172.30.117.11 --- 0x3
  Internet Address      Physical Address      Type
  172.30.117.1          20-67-7c-7b-30-80     dynamic
  172.30.117.31         00-25-ab-a9-f8-2b     dynamic
  172.30.117.40         00-25-ab-a9-f8-6c     dynamic
  172.30.117.51         08-00-27-dd-52-b0     dynamic
  172.30.117.118        00-25-ab-a9-c8-d3     dynamic
  172.30.117.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  225.16.8.68           01-00-5e-10-08-44     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.56.1 --- 0x6
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.182.1 --- 0xd
  Internet Address      Physical Address      Type
  192.168.182.254       00-50-56-fc-04-1e     dynamic
  192.168.182.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
```

CMD ->_ping from host OS(windows10) to guest OS

C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 10.0.16299.726]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\student>ping 172.30.117.51

Pinging 172.30.117.51 with 32 bytes of data:
Reply from 172.30.117.51: bytes=32 time<1ms TTL=64
Reply from 172.30.117.51: bytes=32 time<1ms TTL=64
Reply from 172.30.117.51: bytes=32 time<1ms TTL=64
Reply from 172.30.117.51: bytes=32 time<1ms TTL=64

Ping statistics for 172.30.117.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\student>
```

Ping from real host to local host

C:₩Users₩pc>ping localhost

Ping DESKTOP-C27V8J7 [::1] 32바이트 데이터 사용:
::1의 응답: 시간<1ms

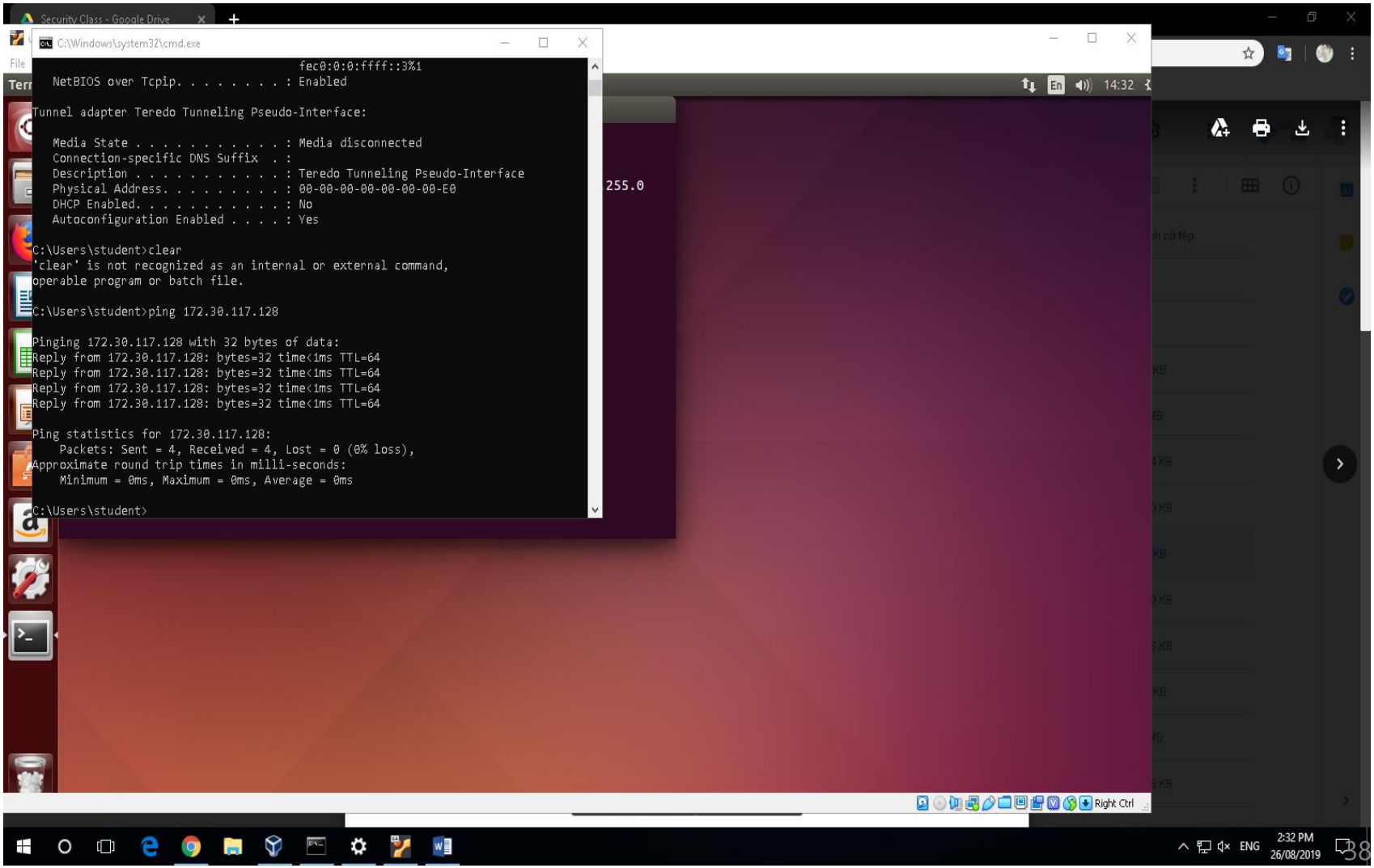
::1에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 0ms, 최대 = 0ms, 평균 = 0ms

C:₩Users₩pc>ping 127.0.0.1

Ping 127.0.0.1 32바이트 데이터 사용:
127.0.0.1의 응답: 바이트=32 시간<1ms TTL=128

127.0.0.1에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 0ms, 최대 = 0ms, 평균 = 0ms

CMD ->_ping from host windows10 to guest OS



CMD ->_ping from guest OS to host OS

$ ping host IP

```
File  Edit  View  Search  Terminal  Help
[noat@localhost ~]$ ping 172.30.117.12
PING 172.30.117.12 (172.30.117.12) 56(84) bytes of data.
64 bytes from 172.30.117.12: icmp_seq=1 ttl=128 time=0.211 ms
64 bytes from 172.30.117.12: icmp_seq=2 ttl=128 time=0.255 ms
64 bytes from 172.30.117.12: icmp_seq=3 ttl=128 time=0.257 ms
64 bytes from 172.30.117.12: icmp_seq=4 ttl=128 time=0.254 ms
64 bytes from 172.30.117.12: icmp_seq=5 ttl=128 time=0.271 ms
64 bytes from 172.30.117.12: icmp_seq=6 ttl=128 time=0.297 ms
^C
--- 172.30.117.12 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5336ms
rtt min/avg/max/mdev = 0.211/0.257/0.297/0.030 ms
[noat@localhost ~]$
```

$ping from guest OS(Centos) to host

- https://monovm.com/post/33/how-to-ping-in-centos
- https://m.wikihow.com/Ping-in-Linux

```
[centoslive@livecd ~]$ ping 172.30.117.11
PING 172.30.117.11 (172.30.117.11) 56(84) bytes of data.
64 bytes from 172.30.117.11: icmp_seq=1 ttl=128 time=0.576 ms
64 bytes from 172.30.117.11: icmp_seq=2 ttl=128 time=0.245 ms
64 bytes from 172.30.117.11: icmp_seq=3 ttl=128 time=0.571 ms
64 bytes from 172.30.117.11: icmp_seq=4 ttl=128 time=0.566 ms
64 bytes from 172.30.117.11: icmp_seq=5 ttl=128 time=0.587 ms
^Z
[1]+  Stopped                 ping 172.30.117.11
[centoslive@livecd ~]$
```

CMD ->nslookup cit. ctu.edu. vn

CMD ->nslookup ctu.edu.vn

To Query DNS Records

These records contain information like the domain name's IP addresses

C:\Windows\system32\cmd.exe

```
C:\Users\student>nslookup ctu.edu.vn
Server:  CTUAD2.ctu.edu.vn
Address:  172.18.27.2

Name:    ctu.edu.vn
Addresses:  172.18.27.6
          172.18.45.6
          10.18.36.54
          172.18.45.2
          172.18.27.2


C:\Users\student>
```

nslookup ctu.edu.vn

- C:₩Users₩pc>nslookup ctu.edu.vn
- 서버: vip.cnmnoc.co.kr
- Address: 182.172.255.180

- 권한 없는 응답:
- 이름: ctu.edu.vn
- **Address: 123.30.143.225**

Ping and Traceroute with WinMTR

WinMTR v0.92 64 bit by Appnor MSP - www.winmtr.net

Host: google.com | Stop | Options

Copy Text to clipboard | Copy HTML to clipboard

Hostname	Nr	Loss %	Sent	Recv	Best	Avrg	Worst	Last
192.168.200.254	1	1	2930	2926	1	4	114	8
No response from host	2	100	595	0	0	0	0	0
172.21.14.125	3	1	2930	2926	9	14	125	13
172.20.0.37	4	1	2934	2931	9	14	135	11
172.20.1.49	5	1	2934	2931	9	20	204	19
172.20.0.134	6	89	656	76	0	14	31	23
192.145.251.168	7	1	2941	2940	40	45	186	59
108.170.242.193	8	1	2941	2940	45	52	313	49
216.239.43.53	9	1	2937	2935	40	45	221	42
nrt13s54-in-f14.1e100.net	10	1	2941	2940	45	50	169	48

https://support.8x8.com/support-services/support/download-winmtr-ping-traceroute-tool

Ping and Traceroute with WinMTR

1. Go to https://winmtr.en.uptodown.com/windows.
2. Follow instructions to download the compressed file.
3. After downloading has completed, extract the folder to the desktop (or other desired location).
4. Open the folder and run the program (WinMTR.exe or WinMTR64.exe).
5. For **Host** use the correct 8x8 media server based on the phone location. The full list of IP Addresses is available in the X Series Technical Requireme
6. Press **Start**.
7. Run test for a minimum of 2 minutes and a maximum of 5 minutes. Click **S**

CMD -> netstat

LISTENING: currently waiting for service

ESTABLISHED: Connected to another computer

CLOSED: Connection is completely closed

TIME WAIT: Connection is terminated, but the socket is open for the time being

C:\Windows\system32\cmd.exe

```
C:\Users\student>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    172.30.117.24:52705    cache-st:3128          CLOSE_WAIT
  TCP    172.30.117.24:53455    cache-st:3128          CLOSE_WAIT
  TCP    172.30.117.24:53456    cache-st:3128          CLOSE_WAIT
  TCP    172.30.117.24:53457    cache-st:3128          CLOSE_WAIT
  TCP    172.30.117.24:54726    proxy:3128             ESTABLISHED
  TCP    172.30.117.24:55242    proxy:3128             ESTABLISHED
  TCP    172.30.117.24:55361    proxy:3128             TIME_WAIT
  TCP    172.30.117.24:55391    proxy:3128             ESTABLISHED
  TCP    172.30.117.24:55420    proxy:3128             ESTABLISHED
  TCP    172.30.117.24:55423    proxy:3128             ESTABLISHED
  TCP    172.30.117.24:55424    proxy:3128             ESTABLISHED
  TCP    172.30.117.24:55511    proxy:3128             ESTABLISHED
  TCP    172.30.117.24:55549    proxy:3128             ESTABLISHED
  TCP    172.30.117.24:55850    cache-st:3128          ESTABLISHED
  TCP    172.30.117.24:55962    cache-st:3128          ESTABLISHED
  TCP    172.30.117.24:55963    cache-st:3128          ESTABLISHED
  TCP    172.30.117.24:56084    40.90.23.247:https     SYN_SENT
  TCP    [::1]:56091            P22M14:9229            SYN_SENT
  TCP    [::1]:56092            P22M14:9229            SYN_SENT

C:\Users\student>
```

CMD -> netstat -na

LISTENING: currently waiting for service

ESTABLISHED: Connected to another computer

CLOSED: Connection is completely closed

TIME WAIT: Connection is terminated, but the socket is open for the time being

C:\Windows\system32\cmd.exe

```
C:\Users\student>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    172.30.117.24:52705    cache-st:3128          CLOSE_WAIT
  TCP    172.30.117.24:53455    cache-st:3128          CLOSE_WAIT
  TCP    172.30.117.24:53456    cache-st:3128          CLOSE_WAIT
  TCP    172.30.117.24:53457    cache-st:3128          CLOSE_WAIT
  TCP    172.30.117.24:54726    proxy:3128             ESTABLISHED
  TCP    172.30.117.24:55242    proxy:3128             ESTABLISHED
  TCP    172.30.117.24:55361    proxy:3128             TIME_WAIT
  TCP    172.30.117.24:55391    proxy:3128             ESTABLISHED
  TCP    172.30.117.24:55420    proxy:3128             ESTABLISHED
  TCP    172.30.117.24:55423    proxy:3128             ESTABLISHED
  TCP    172.30.117.24:55424    proxy:3128             ESTABLISHED
  TCP    172.30.117.24:55511    proxy:3128             ESTABLISHED
  TCP    172.30.117.24:55549    proxy:3128             ESTABLISHED
  TCP    172.30.117.24:55850    cache-st:3128          ESTABLISHED
  TCP    172.30.117.24:55962    cache-st:3128          ESTABLISHED
  TCP    172.30.117.24:55963    cache-st:3128          ESTABLISHED
  TCP    172.30.117.24:56084    40.90.23.247:https     SYN_SENT
  TCP    [::1]:56091            P22M14:9229            SYN_SENT
  TCP    [::1]:56092            P22M14:9229            SYN_SENT

C:\Users\student>
```

CMD -> nbtstat –a to neighbor computer

- A Displays the name table of the remote computer using the specified computer name.
- A Displays the name table of the remote computer using the specified IP address.
- C Displays the contents of the NetBIOS name cache including IP addresses.
- N Display a list of local NetBOIS names (own)

C:\Windows\system32\cmd.exe

```
C:\Users\student>nbtstat -a 172.30.117.23

VirtualBox Host-Only Network:
Node IpAddress: [192.168.56.1] Scope Id: []

    Host not found.

VMware Network Adapter VMnet1:
Node IpAddress: [192.168.36.1] Scope Id: []

    Host not found.

VMware Network Adapter VMnet8:
Node IpAddress: [192.168.72.1] Scope Id: []

    Host not found.

Ethernet:
Node IpAddress: [172.30.117.24] Scope Id: []

            NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    P22M13         <00>  UNIQUE      Registered
    CLC4           <00>  GROUP       Registered
    P22M13         <20>  UNIQUE      Registered

    MAC Address = 00-25-AB-A9-D8-56
```

CMD -> finger

Check local account information for Linux

- Check remote server account information
- Linux command to check user information

C:\Windows\system32\cmd.exe

```
C:\Users\student>finger @172.30.117.23

[172.30.117.23:79]
> Finger: connect::Connection refused

C:\Users\student>finger 172.30.117.23

[P22M14]
> Finger: connect::Host is unreachable

C:\Users\student>
```