LAB02 PoD simulation guide

Class	
Student ID	
Name	
Email address	
Class	cyber security
Browser	Safari, Chrome, IE, Firefox

1. Design test environment

	Attacker	Target
OS	**Windows 10**	**Ubuntu**
IP address	Test - bed IP	Test - bed IP
Attacking type	DoS Ping of Death	
SW for Attacking	**Window Powershell, Window CMD**	
SW for detecting		Linux **CMD netstat commands**
SW for blocking		Linux **CMD iptables**
Command for monitoring		Linux monitoring software Gnome **net-tools package on Ubuntu**

On attacker:

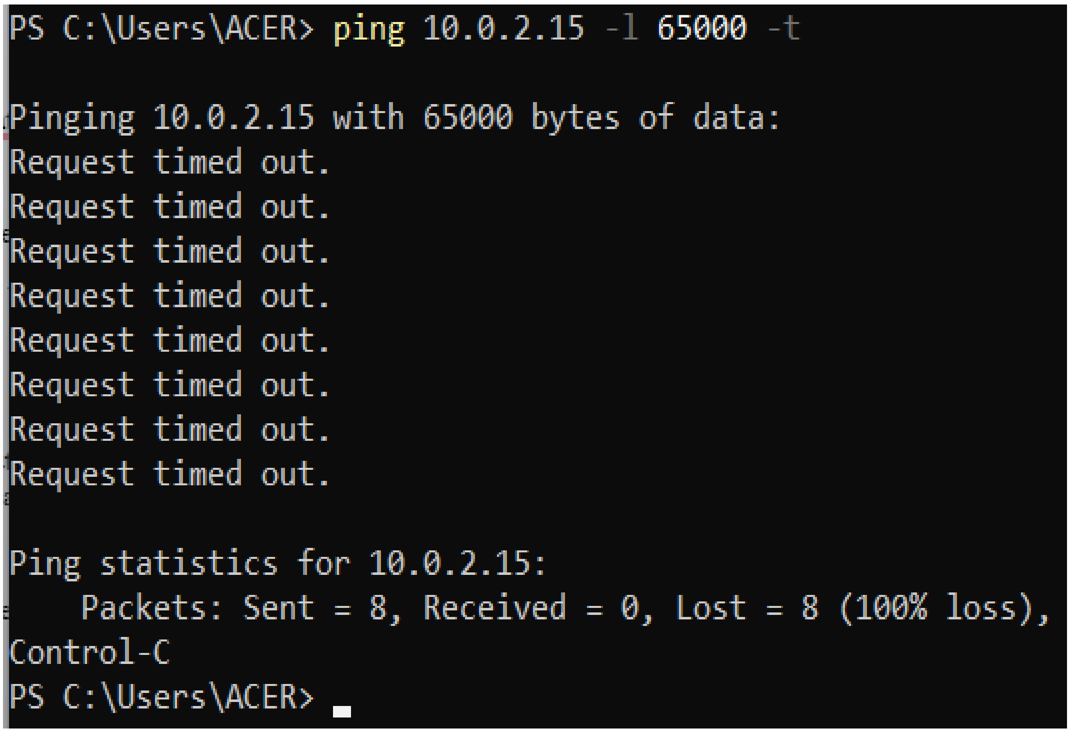
1. Install Powershell or call Window CMD

Send 65000-byte packets 5 times to ubuntu server

Option: CMD

- -t means the data packets should be sent until the program is stopped

- -l specifies the data load to be sent to the victim

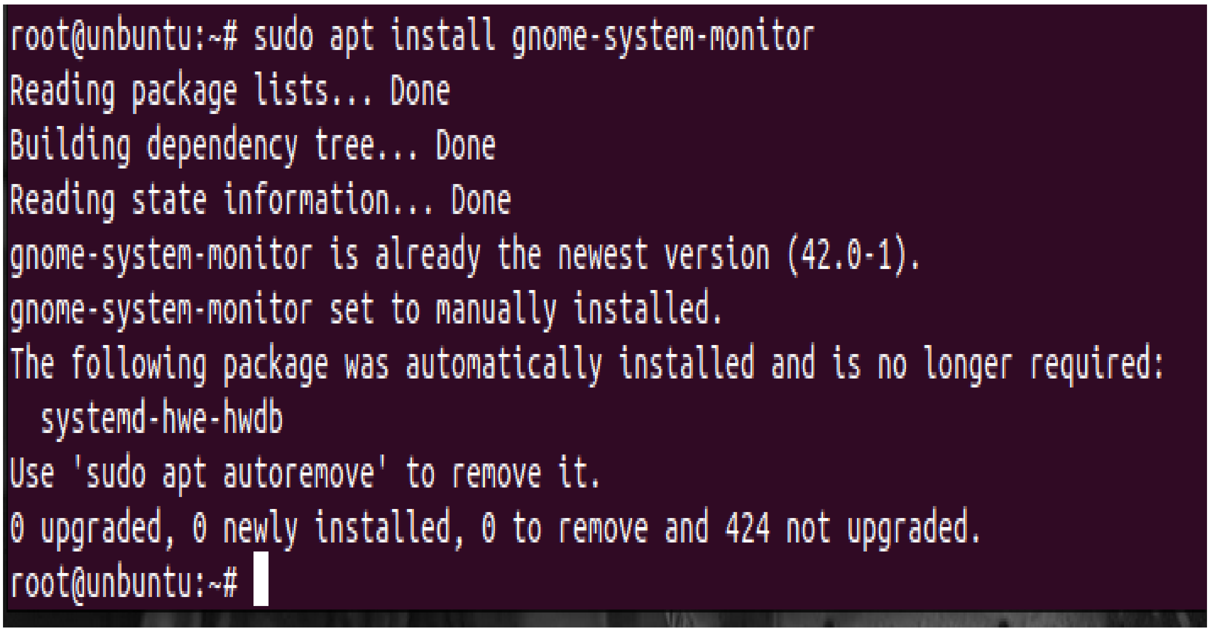


```
PS C:\Users\ACER> ping 10.0.2.15 -l 65000 -t

Pinging 10.0.2.15 with 65000 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.2.15:
    Packets: Sent = 8, Received = 0, Lost = 8 (100% loss),
Control-C
PS C:\Users\ACER>
```

<u>On target</u>:

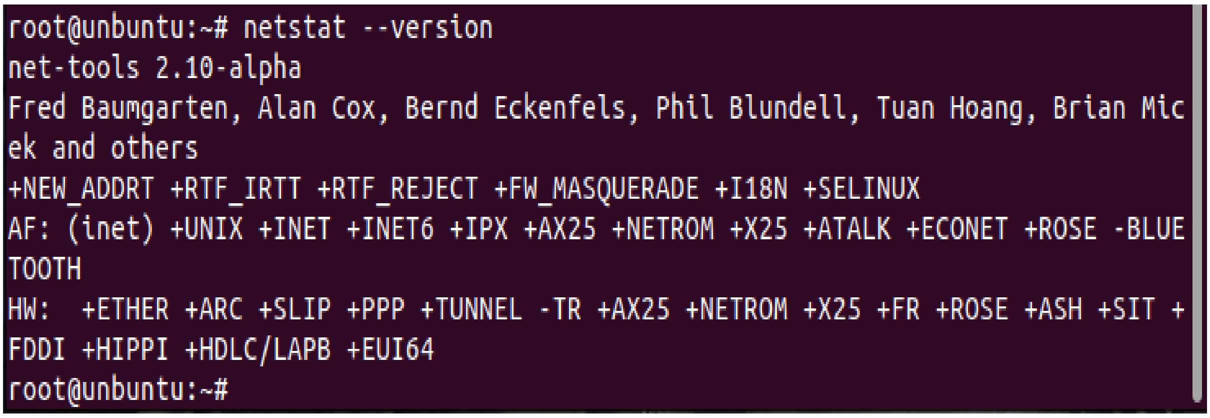
every few seconds this network receives about ~50kb, and it does not respond (sending – red line), because the packet size is exceeded, it cannot be processed

4 Install Linux monitoring software Gnome on target and analyze target system



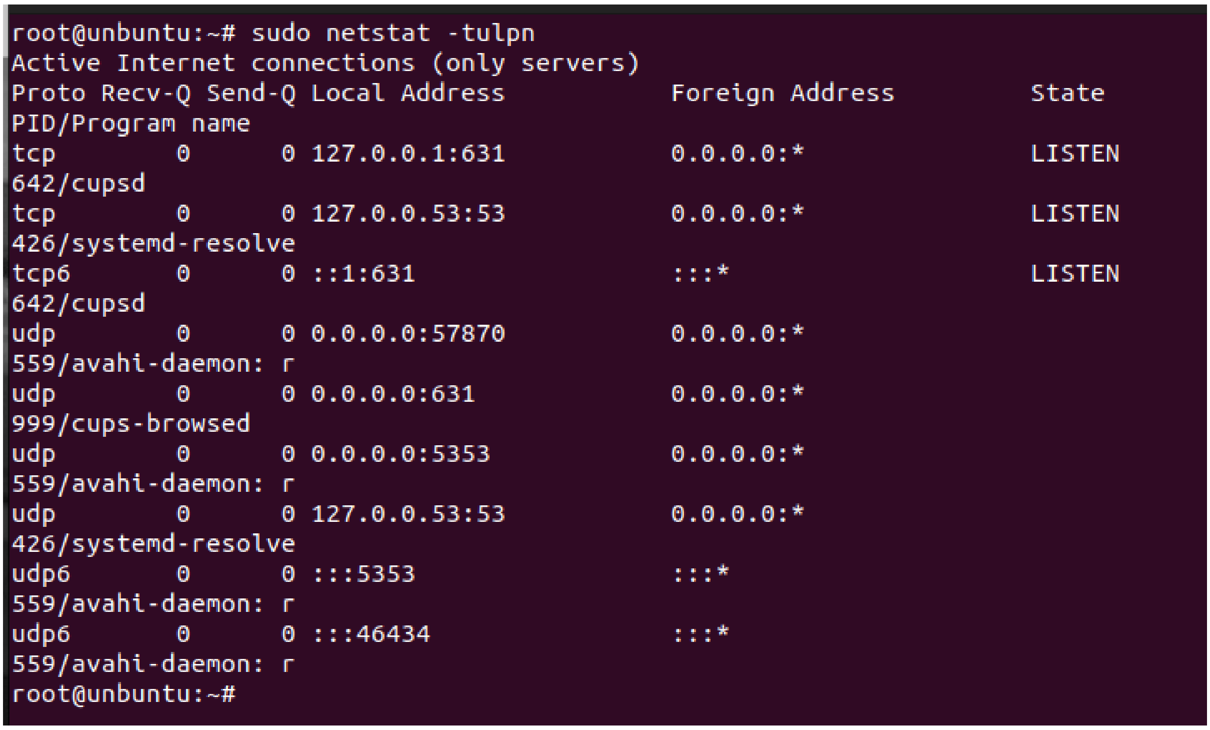
```
root@unbuntu:~# sudo apt install gnome-system-monitor
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gnome-system-monitor is already the newest version (42.0-1).
gnome-system-monitor set to manually installed.
The following package was automatically installed and is no longer required:
  systemd-hwe-hwdb
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 424 not upgraded.
root@unbuntu:~#
```

5 **Install CMD net-tools package on Ubuntu and explain attacking result**



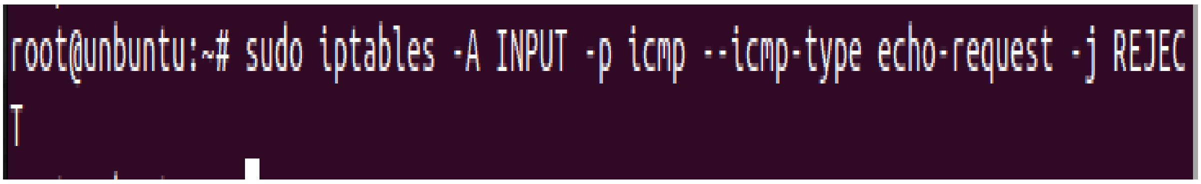
```
root@unbuntu:~# netstat --version
net-tools 2.10-alpha
Fred Baumgarten, Alan Cox, Bernd Eckenfels, Phil Blundell, Tuan Hoang, Brian Mic
ek and others
+NEW_ADDRT +RTF_IRTT +RTF_REJECT +FW_MASQUERADE +I18N +SELINUX
AF: (inet) +UNIX +INET +INET6 +IPX +AX25 +NETROM +X25 +ATALK +ECONET +ROSE -BLUE
TOOTH
HW:  +ETHER +ARC +SLIP +PPP +TUNNEL -TR +AX25 +NETROM +X25 +FR +ROSE +ASH +SIT +
FDDI +HIPPI +HDLC/LAPB +EUI64
root@unbuntu:~#
```

6 **Detect dos attack Symptom on the target system with CMD netstat commands**



```
root@unbuntu:~# sudo netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
642/cupsd
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
426/systemd-resolve
tcp6       0      0 ::1:631                 :::*                    LISTEN
642/cupsd
udp        0      0 0.0.0.0:57870           0.0.0.0:*
559/avahi-daemon: r
udp        0      0 0.0.0.0:631             0.0.0.0:*
999/cups-browsed
udp        0      0 0.0.0.0:5353            0.0.0.0:*
559/avahi-daemon: r
udp        0      0 127.0.0.53:53           0.0.0.0:*
426/systemd-resolve
udp6       0      0 :::5353                 :::*
559/avahi-daemon: r
udp6       0      0 :::46434                :::*
559/avahi-daemon: r
root@unbuntu:~#
```

7 **Block dos attack IP on Ubuntu using commands iptables (snap shot) and explain blocking result**



```
root@unbuntu:~# sudo iptables -A INPUT -p icmp --icmp-type echo-request -j REJEC
T
```

When you block a DoS (Denial of Service) attack IP using the iptables command on Ubuntu, the blocking result is that incoming traffic from the specified IP address will be dropped or denied.

This means that any network packets or connections initiated by the blocked IP address will not reach your Ubuntu system.

Here's what happens when you block an IP address using iptables:

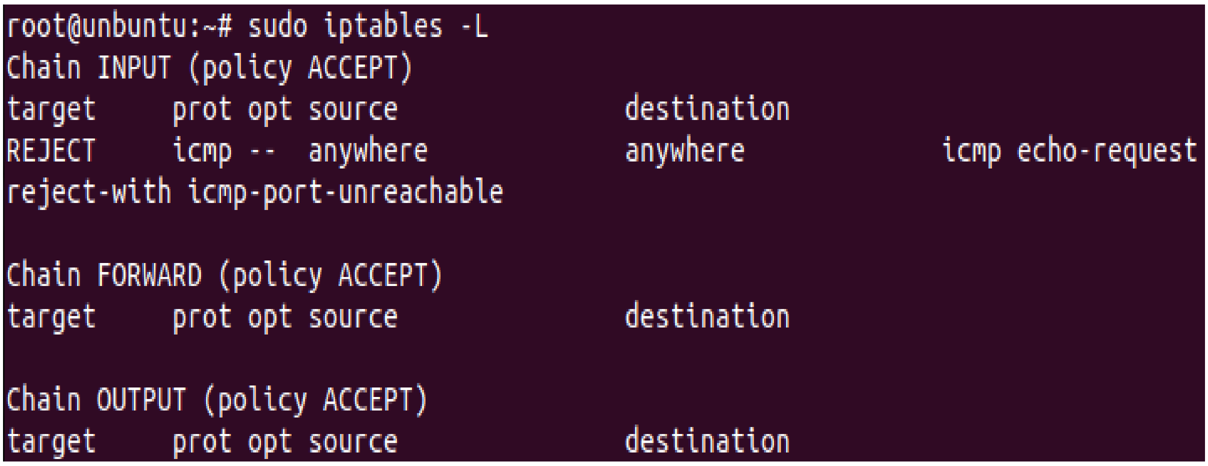
Traffic Rejection: Any incoming network packets from the blocked IP address will be stopped at the firewall level, and no further processing will occur. These packets are essentially discarded, which means they don't reach the target application or service running on your Ubuntu system.

No Response: When the blocked IP address attempts to establish a connection, your Ubuntu system will not respond. This can result in the attacker's requests being met with silence, leading them to believe that their attacks are not having any effect.

Protection: By blocking the attacking IP address, you are providing protection to your Ubuntu system against the DoS attack. This helps in mitigating the impact of the attack because the malicious traffic is not allowed to overwhelm your resources.

Temporary or Permanent: You have the flexibility to choose whether the block is temporary or permanent, depending on your needs. If you want to remove the blocking rule after a certain period, you can do so. The ability to adjust the blocking duration allows you to apply countermeasures as needed.

Monitoring: After blocking the IP address, you should monitor your system's logs and network traffic to ensure that the blocking rule is effective. Continued monitoring helps you assess the impact of the block on the DoS attack and ensures that your system remains protected.



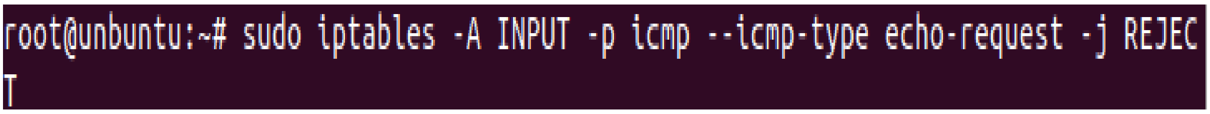
```
root@unbuntu:~# sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     icmp --  anywhere             anywhere             icmp echo-request
reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

8 Explain how to Block/Allow ping from iptables?

Block Ping

$sudo iptables -A INPUT -p icmp --icmp-type echo-request -j REJECT

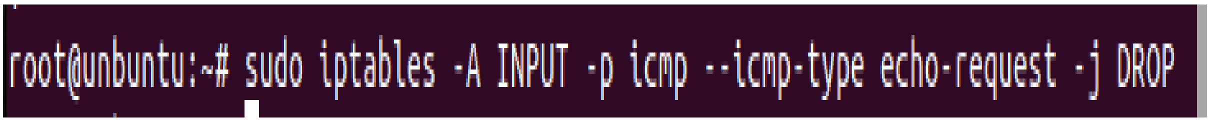
The command sudo iptables -A INPUT -p icmp --icmp-type echo-request -j REJECT blocks incoming ping (ICMP echo request) packets on your system by rejecting them with an ICMP "Destination Unreachable" message.



```
root@unbuntu:~# sudo iptables -A INPUT -p icmp --icmp-type echo-request -j REJEC
T
```

Or else, you can add the following rules in order to block ping without printing an error message:

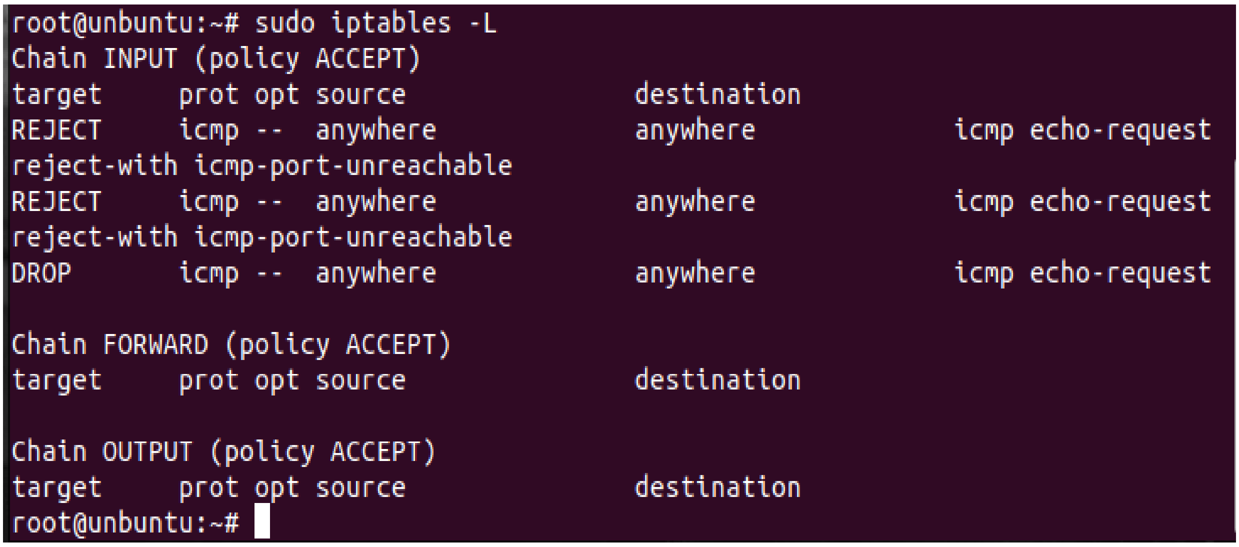
$sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP



```
root@unbuntu:~# sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
```

Allow Ping

$ sudo iptables -L



```
root@unbuntu:~# sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     icmp --  anywhere             anywhere             icmp echo-request
reject-with icmp-port-unreachable
REJECT     icmp --  anywhere             anywhere             icmp echo-request
reject-with icmp-port-unreachable
DROP       icmp --  anywhere             anywhere             icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@unbuntu:~# 
```