# **LAB02 PoD simulation**

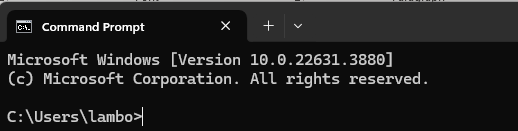
| Class | CT201H [M01-M04] |
| --- | --- |
| Student ID | B2111933 |
| Name | Truong Dang Truc Lam |
| Email address | [lamb2111933@student.ctu.edu.vn](mailto:lamb2111933@student.ctu.edu.vn) |
| Browser | Safari, Chrome, IE, Firefox |

1. **Fill in the test environment**

|  | **Attacker** | **Target** |
| --- | --- | --- |
| **OS** | **Windows 10** | **Ubuntu** |
| **IP address** | **192.168.1.55** | **192.168.1.11** |
| **Attacking type** | **DoS**  **Ping of Death** |  |
| **SW for Attacking** | **Window Powershell,**  **Window CMD** | **Linux CMD netstat**  **commands** |
| **SW for detecting** |  | **Linux CMD iptables** |
| **Command for monitoring** |  | **Linux monitoring**  **software Gnome**  **net-tools package  on Ubuntu** |

On attacker:

1. **Install Windows Powershell or use Windows CMD**

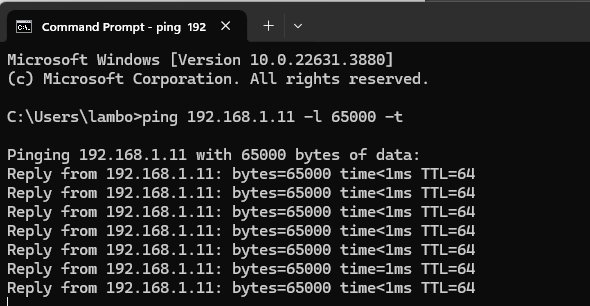
******

Windows CMD

1. **Send 65000-byte packets 5 times to Ubuntu server using CMD ping or, Powershell ping:**

Option: CMD

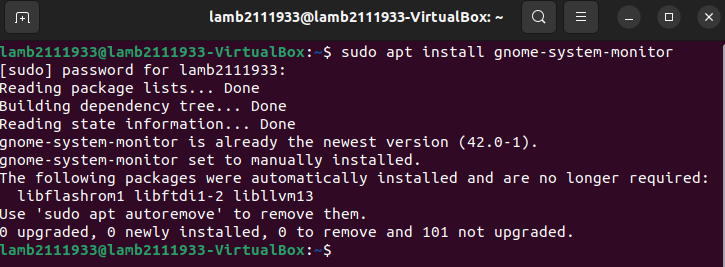
* 1. -t means the data packets should be sent until the program is stopped
  2. -l specifies the data load to be sent to the victim



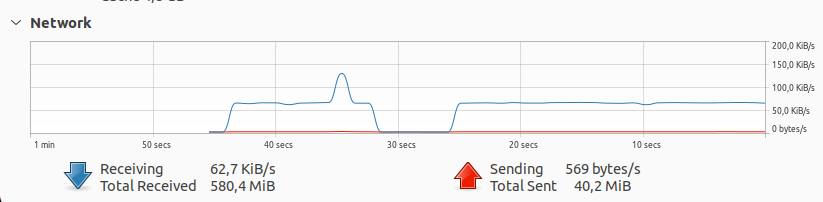
My network can respond normally because the data is not large enough.  
However, if there are thousands of instances that pinging like this,   
packet size will exceed and it cannot be processed

On target:

1. **Install Linux monitoring software Gnome on target and analyze target system**

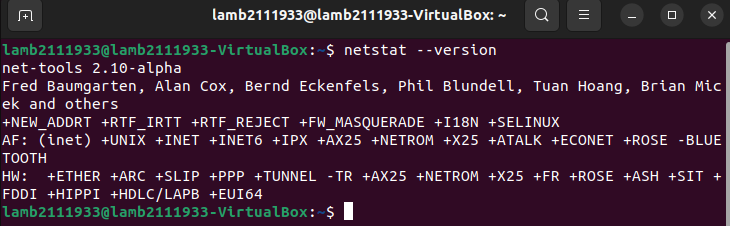
****

Install necessary packages for **Linux monitoring software Gnome**

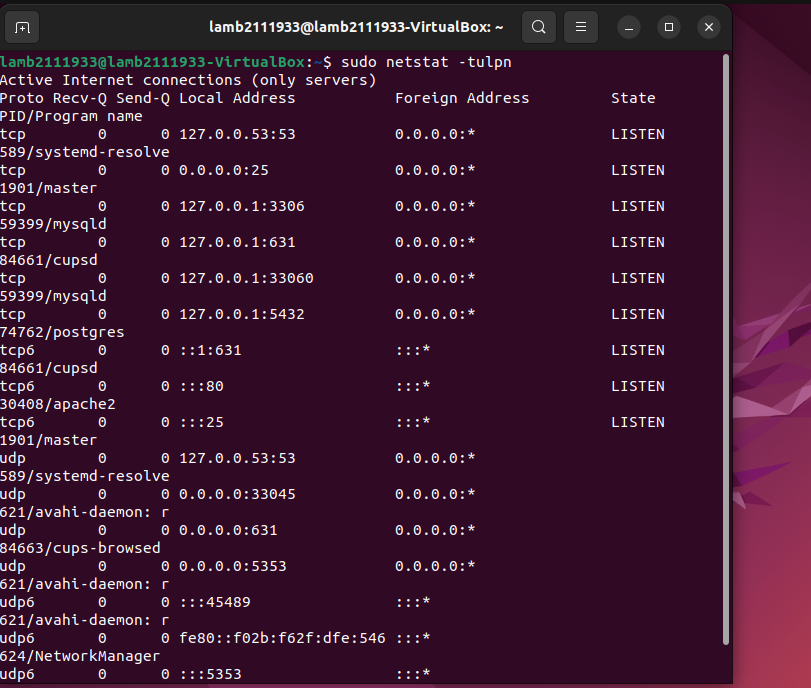
****

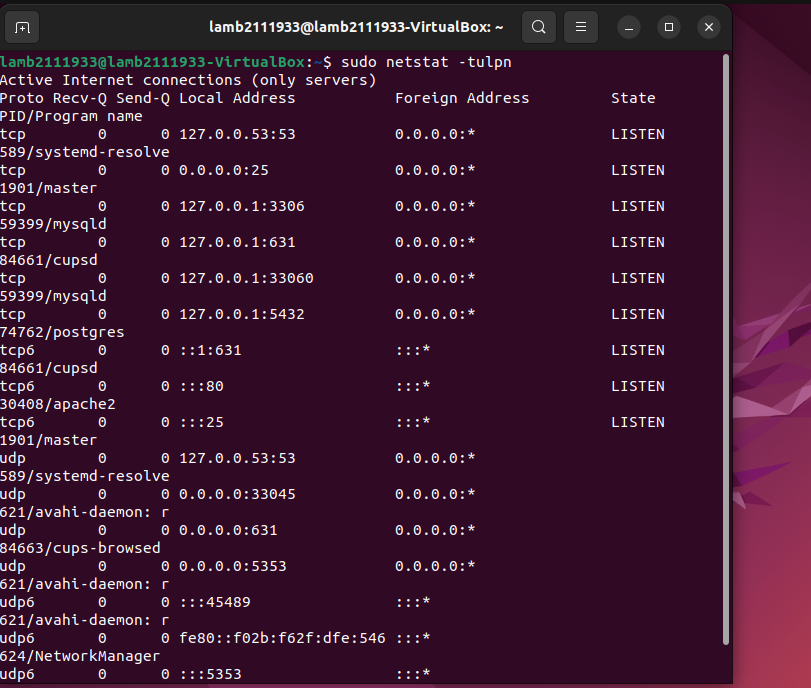
This is the network traffic (receiving 65000 bytes/s from host IP)

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



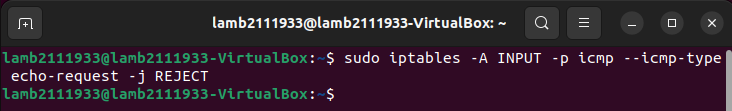
Checking **net-tools** version

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



**netstat** is a tool used to display network statistics and connection information.

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



This command is a Linux command used to configure the firewall (iptables) to block incoming ICMP echo requests (ping).

**-A INPUT:** This specifies that we're adding a new rule to the "INPUT" chain, which is used for incoming packets.

**-p icmp:** This indicates that we're dealing with the ICMP protocol.

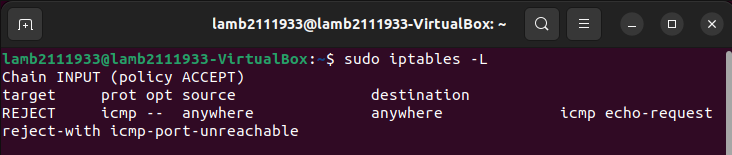
**--icmp-type echo-request:** This specifies that we're targeting ICMP echo requests (ping).

**-j REJECT:** This defines the action to be taken for matching packets: reject them.

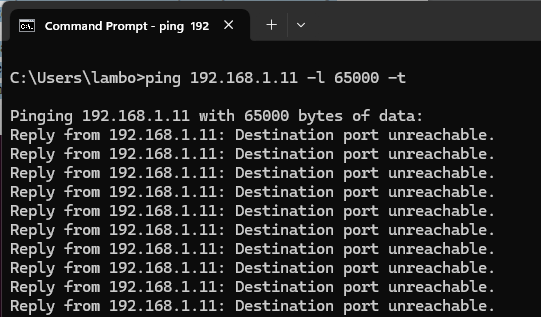
When you block a DoS (Denial of Service) attack IP using the iptables command on Ubuntu, the blocking result is that incoming traffic from the specified IP address will be dropped or denied.

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.



Command **iptables -L** shows a list of all the rules that the firewall is using to decide which network packets to allow or block. You can see that ICMP echo requests (ping) are blocked.

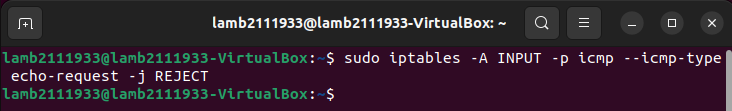


The result

1. **Explain how to Block/Allow ping from iptables?**

Block Ping

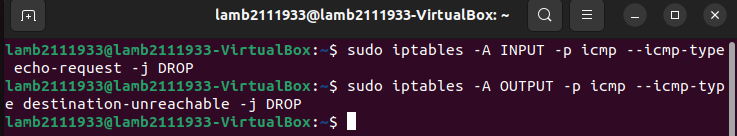
*$sudo iptables -A INPUT -p icmp --icmp-type echo-request -j REJECT*



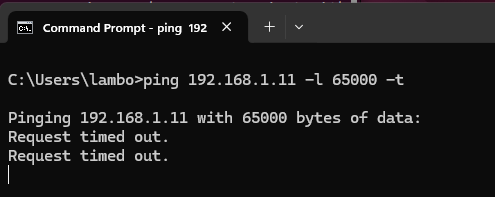
The command sudo iptables -A INPUT -p icmp --icmp-type echo-request -j REJECT blocks incoming ping (ICMP echo request) packets on your system by rejecting them with an ICMP "Destination Unreachable" message.

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*

My VM cannot completely prevent the sending of ICMP error messages after dropping a packet using standard iptables rules. So I add one more command:  *sudo iptables -A OUTPUT -p icmp --icmp-type destination-unreachable -j DROP*

**

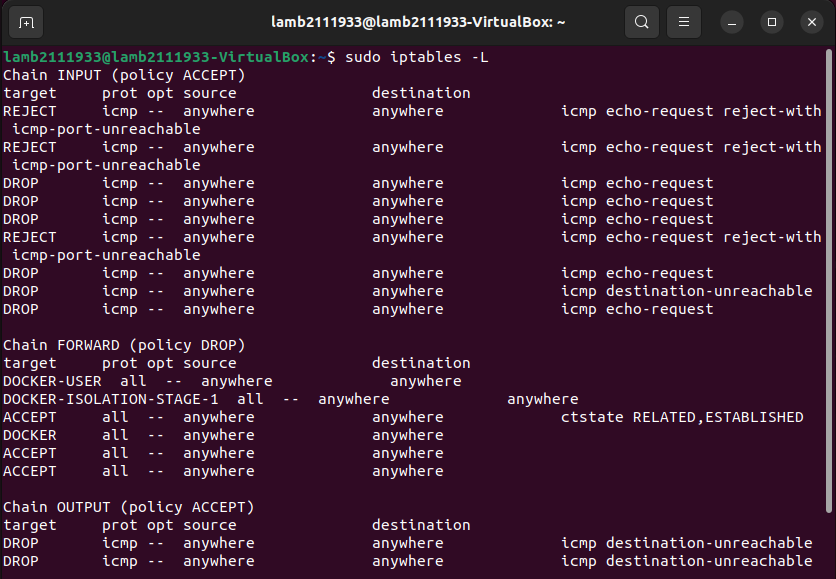
Set those rules to drop the packets in silence

**

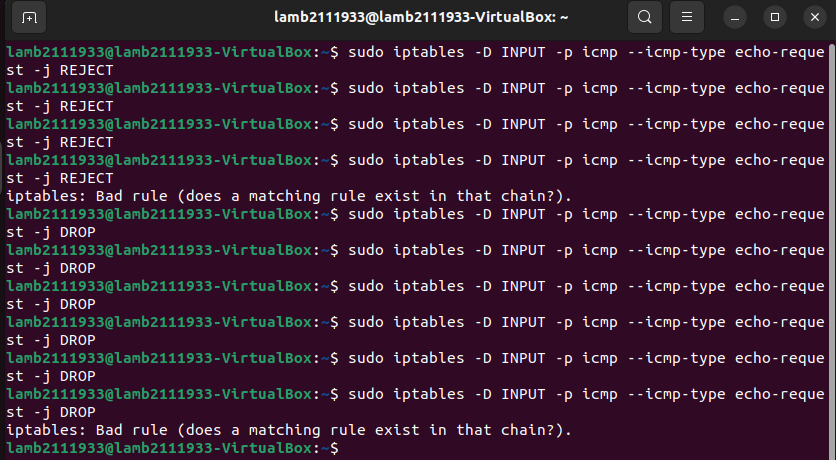
The result

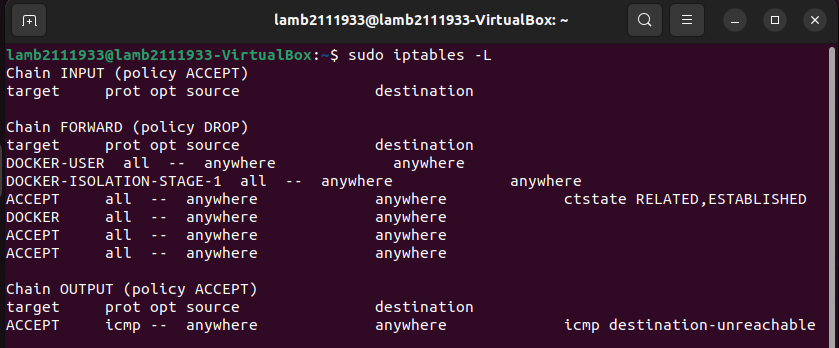
Allow Ping

*$ sudo iptables –L*

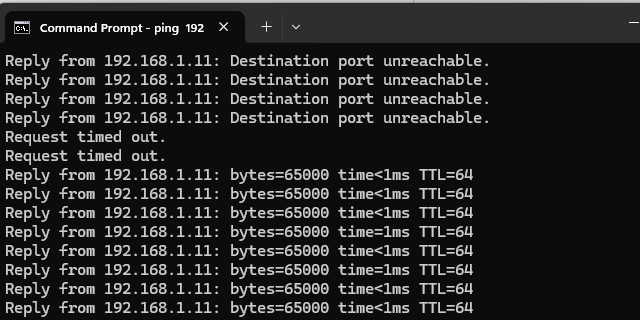
**

Delete those rules for allowing pinging  
*$ sudo iptables -D INPUT -p icmp --icmp-type echo-request -j DROP*  
*$ sudo iptables -D INPUT -p icmp --icmp-type echo-request -j REJECT*





The rules of the firewall now



From now on, we can pinging again