INFORMATION SECURITY AND MANAGEMENT-BCSE354E

LAB ASSESSMENT - 4

NISHANT AGRAWAL – 21BCB0067

SLOT – L27+L28

TOPIC – DdoS ATTACK USING LOIC(LOW ORBIT ION CANNON)

DDoS Attack:

A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic. This attack is executed using multiple compromised computer systems or devices, often referred to as botnets, to generate the large volume of traffic needed to overwhelm the target. Unlike a traditional Denial of Service (DoS) attack, which is launched from a single source, DDoS attacks involve multiple sources distributed across the internet, often in the form of a botnet. This distributed nature makes DDoS attacks more difficult to mitigate.

There are several types of DDoS attacks, including:

1. **Volumetric Attacks**: These flood the target with a high volume of traffic, consuming all available bandwidth and preventing legitimate users from accessing the service.

SUBMITTED TO – CHANDRA MOHAN B

2. **Protocol Attacks**: These exploit weaknesses in network protocols, such as TCP, UDP, or ICMP, to overwhelm the target's resources or disrupt its communication.
3. **Application Layer Attacks**: Also known as Layer 7 attacks, these target specific applications or services (e.g., HTTP, DNS) by exploiting vulnerabilities in the application layer.

DDoS attacks can have severe consequences, including downtime, financial losses, and damage to reputation.

1.TOOL-

LOIC (Low Orbit Ion Cannon):

LOIC is a popular open-source network stress testing and DoS tool that is often used for DDoS attacks. It was originally developed as a legitimate tool for network administrators to test the resilience of their systems to high traffic loads, but it has been repurposed by malicious actors for conducting DDoS attacks.

LOIC allows users to launch DDoS attacks by sending a large volume of TCP, UDP, or HTTP requests to a target server. It is relatively simple to use and does not require advanced technical skills, which has contributed to its widespread use in DDoS attacks.

There are several versions of LOIC available, including a web-based version called "JS LOIC" that runs directly in a web browser. This makes it even easier for individuals to participate in DDoS attacks without needing to download or install any software.

2. Download Link:

https://sourceforge.net/projects/loic/
It should be noted that this tool should not be downloaded on windows as it contains some malware files and it can cause damage to windows OS leading to crash of system so, it is advisable to download it on KALI Linux OS as it is used for cyber security attacks and has encryptions on OS which prevents its crash.

3.Username/Password

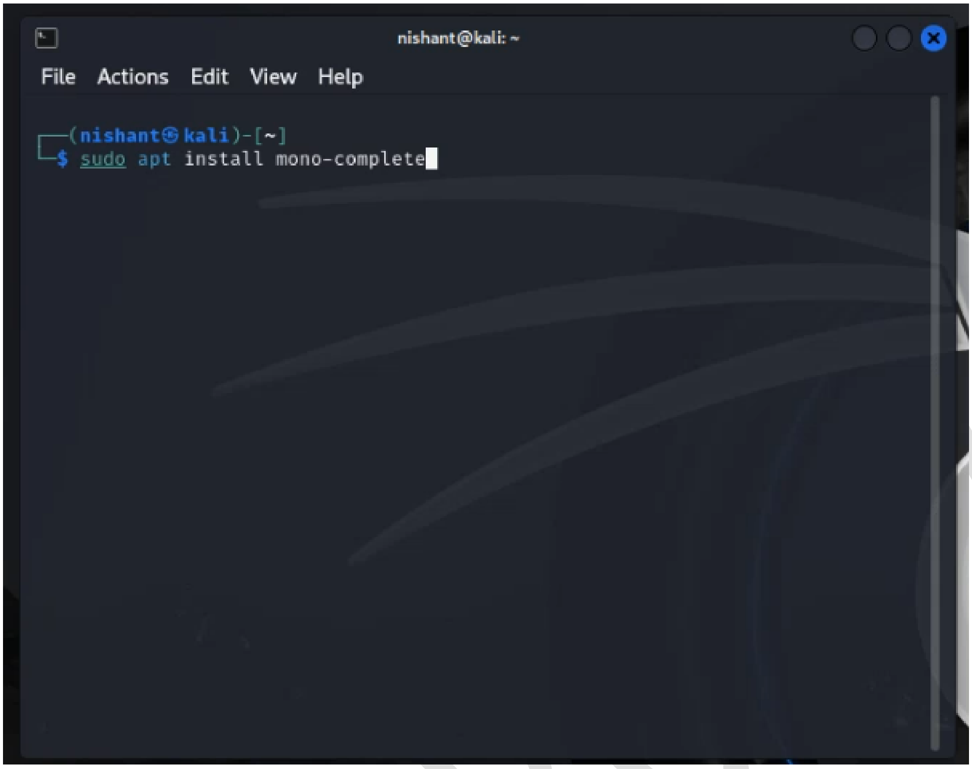
Kali Linux Os Username: nishant

Password: root

SUBMITTED TO – CHANDRA MOHAN B

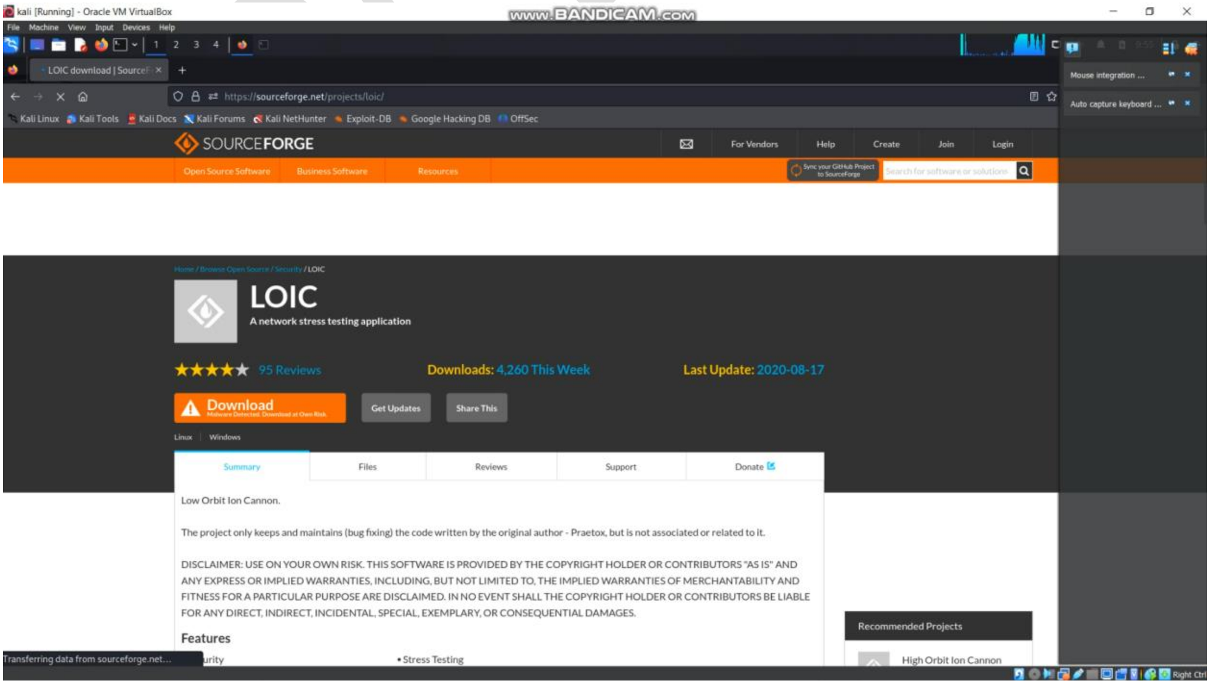
4. Installation Method:

First install mono-complete on kali terminal



```
┌──(nishant㉿kali)-[~]
└─$ sudo apt install mono-complete
```

Second, install LOIC from the link



https://sourceforge.net/projects/loic/

Home / Browse Open Source / Security / LOIC

LOIC

A network stress testing application

★★★★★ 95 Reviews   Downloads: 4,260 This Week   Last Update: 2020-08-17

Low Orbit Ion Cannon.

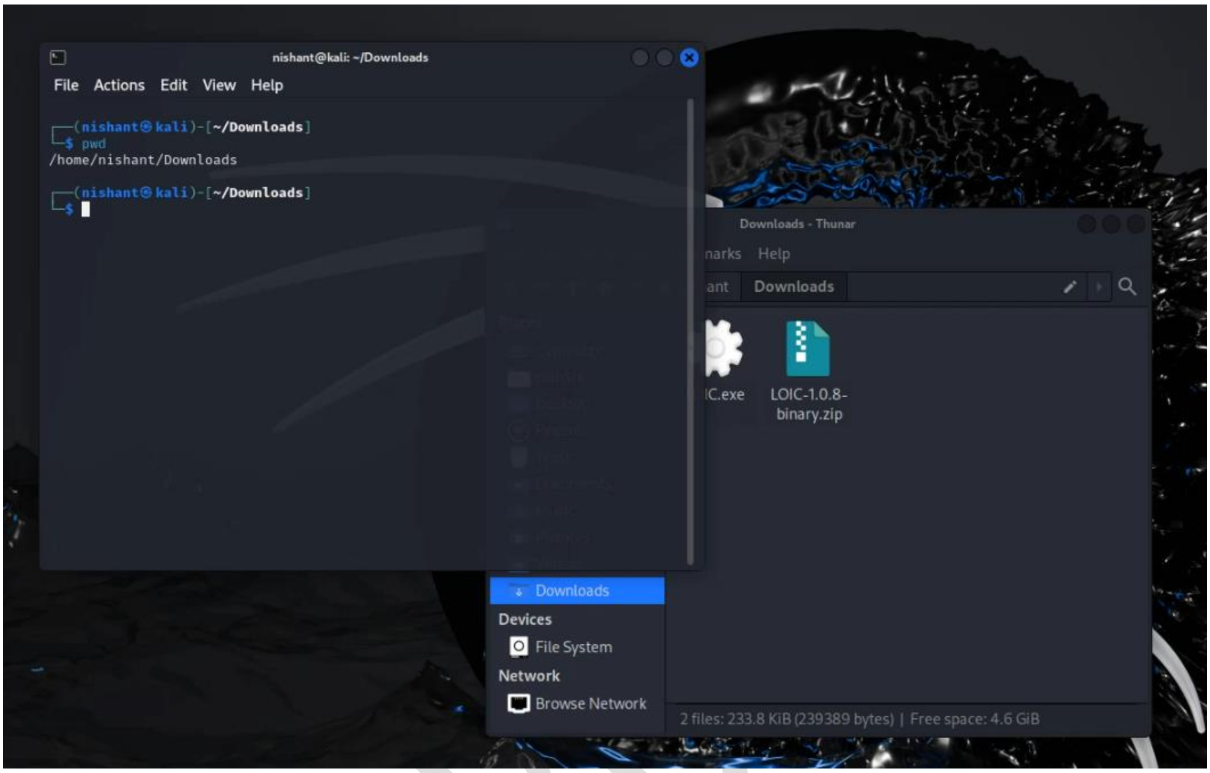
The project only keeps and maintains (bug fixing) the code written by the original author - Praetox, but is not associated or related to it.

DISCLAIMER: USE ON YOUR OWN RISK. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER OR CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES.

Features

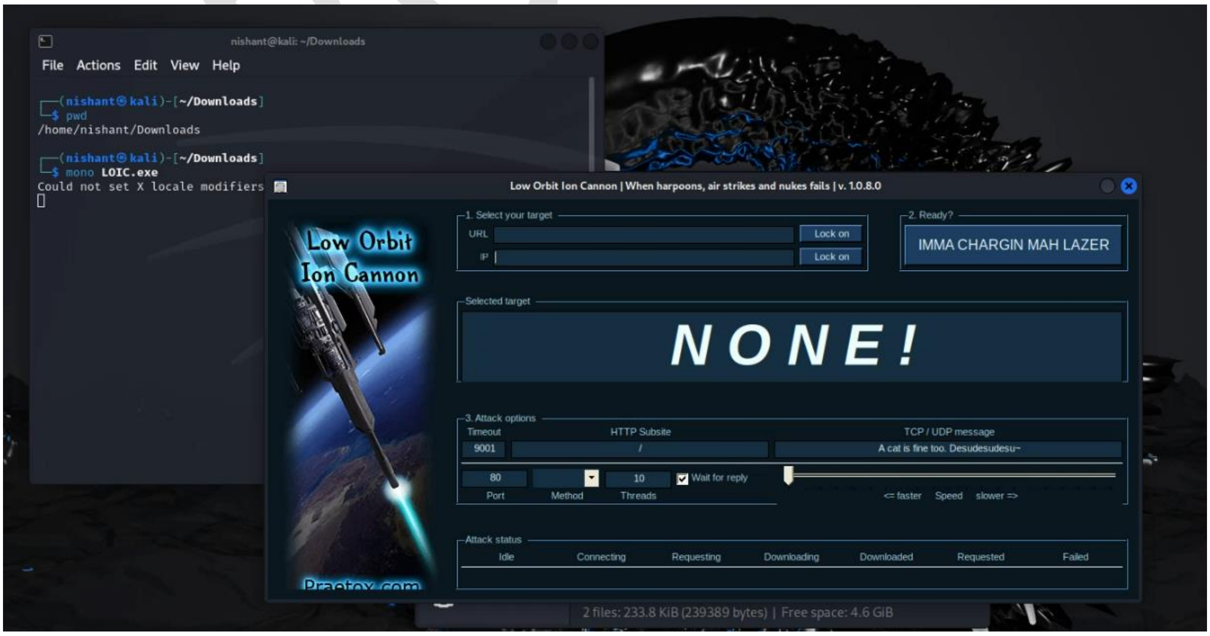
Transferring data from sourceforge.net...

Third, open extract the downloaded zip file in download folder and open terminal in download folder and enter pwd command



```
┌──(nishant㉿kali)-[~/Downloads]
└─$ pwd
/home/nishant/Downloads

┌──(nishant㉿kali)-[~/Downloads]
└─$ ▮
```

Fourth, enter mono LOIC.exe command it will open the tool and now you are all set to go



```
┌──(nishant㉿kali)-[~/Downloads]
└─$ pwd
/home/nishant/Downloads

┌──(nishant㉿kali)-[~/Downloads]
└─$ mono LOIC.exe
Could not set X locale modifiers
▯
```

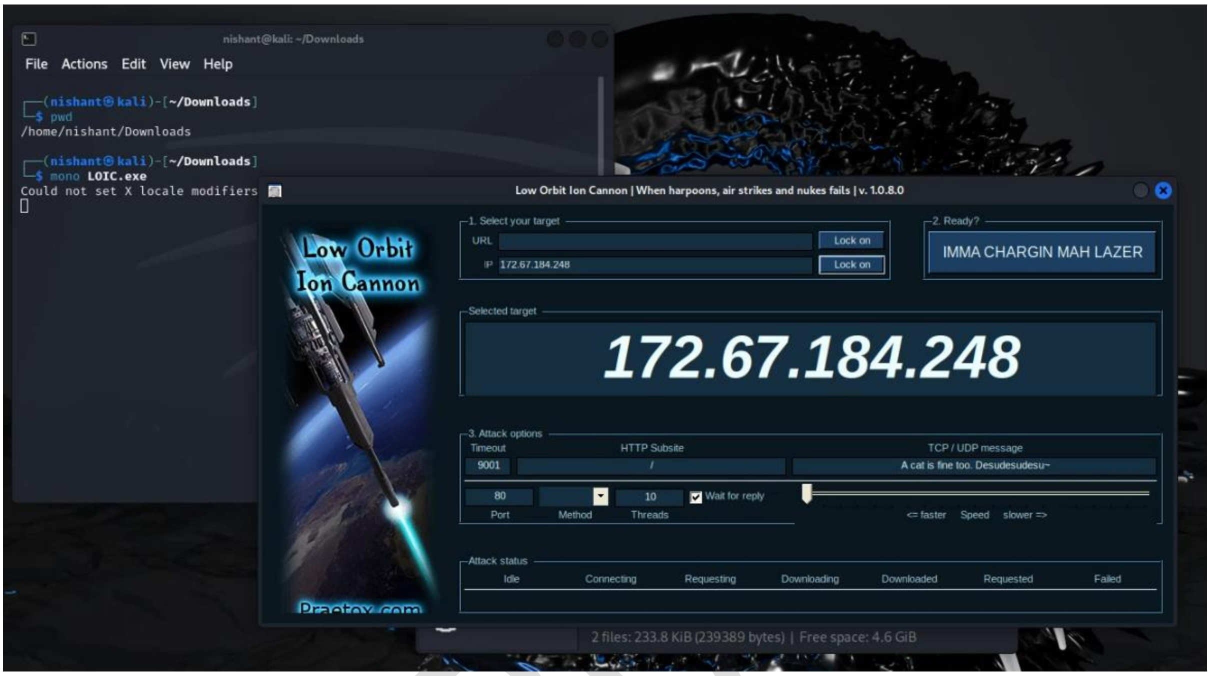
Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0

Selected target: NONE!

Timeout: 9001
HTTP Subsite: /
TCP / UDP message: A cat is fine too. Desudesudesu~
Port: 80
Threads: 10
☑ Wait for reply

5.Process of Attack and Prevention:

First, choose a website/server/device you want to attack and then enter its IP in LOIC tool



```
nishant@kali: ~/Downloads

┌──(nishant㉿kali)-[~/Downloads]
└─$ pwd
/home/nishant/Downloads

┌──(nishant㉿kali)-[~/Downloads]
└─$ mono LOIC.exe
Could not set X locale modifiers
```

Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0

1. Select your target

URL

IP 172.67.184.248

Selected target

172.67.184.248

3. Attack options

Timeout 9001

HTTP Subsite /

TCP / UDP message A cat is fine too. Desudesudesu~

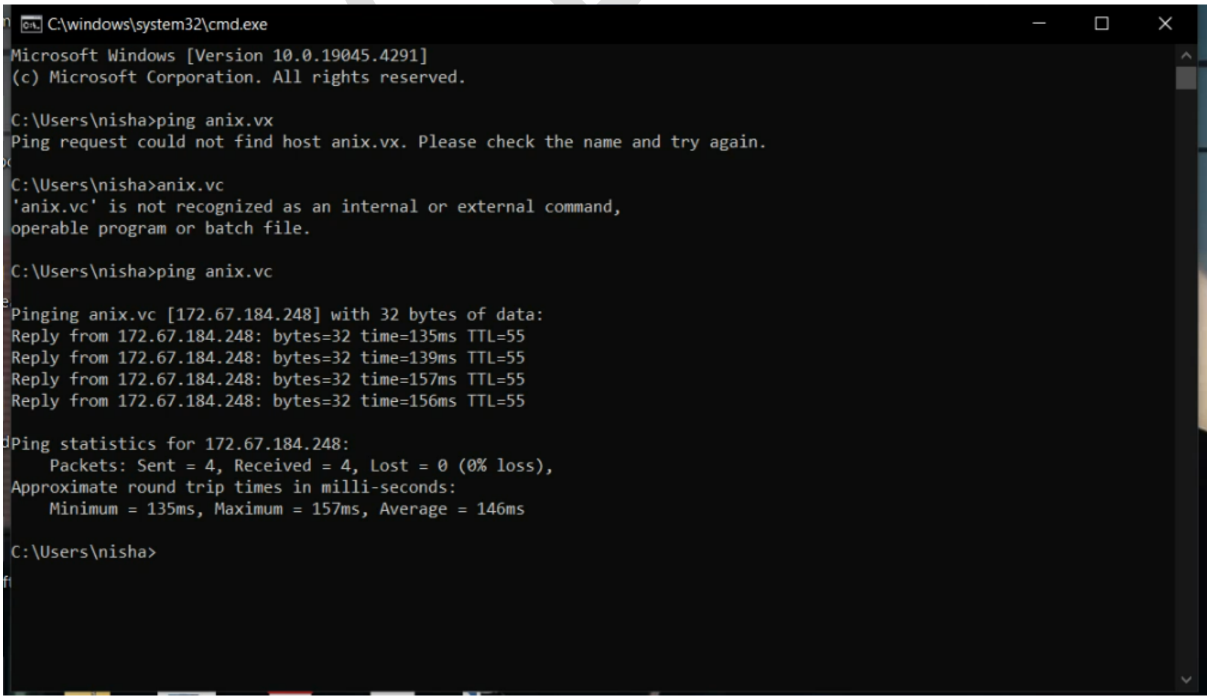
Port 80

Threads 10

☑ Wait for reply

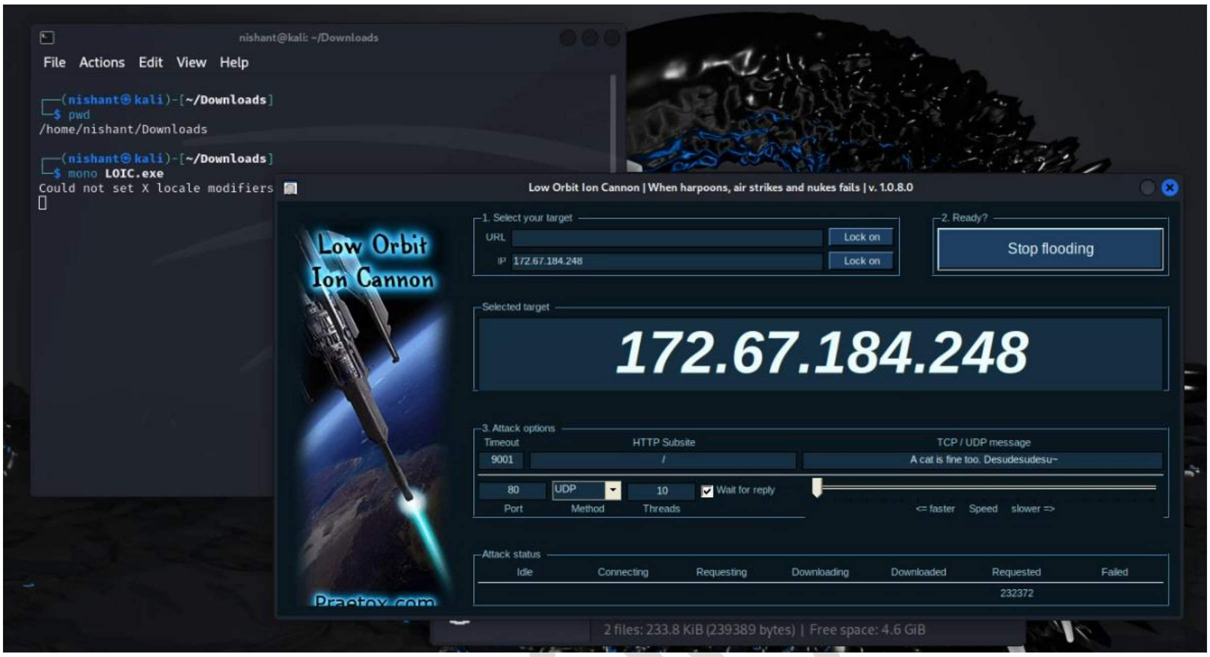
Attack status

Second, I have chosen anix.vc website it is working currently in cmd by pinging



```
C:\windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nisha>ping anix.vx
Ping request could not find host anix.vx. Please check the name and try again.

C:\Users\nisha>anix.vc
'anix.vc' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\nisha>ping anix.vc

Pinging anix.vc [172.67.184.248] with 32 bytes of data:
Reply from 172.67.184.248: bytes=32 time=135ms TTL=55
Reply from 172.67.184.248: bytes=32 time=139ms TTL=55
Reply from 172.67.184.248: bytes=32 time=157ms TTL=55
Reply from 172.67.184.248: bytes=32 time=156ms TTL=55

Ping statistics for 172.67.184.248:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 135ms, Maximum = 157ms, Average = 146ms

C:\Users\nisha>
```

Third, now enter the protocol I have entered UDP as it is for educational purpose and start attack



```
┌──(nishant㉿kali)-[~/Downloads]
└─$ pwd
/home/nishant/Downloads

┌──(nishant㉿kali)-[~/Downloads]
└─$ mono LOIC.exe
Could not set X locale modifiers
```

Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0

1. Select your target

URL:

IP: 172.67.184.248

2. Ready?

Selected target

172.67.184.248

3. Attack options

Timeout: 9001

HTTP Subsite: /

TCP / UDP message: A cat is fine too. Desudesudesu~

Port: 80

Method: UDP

Threads: 10

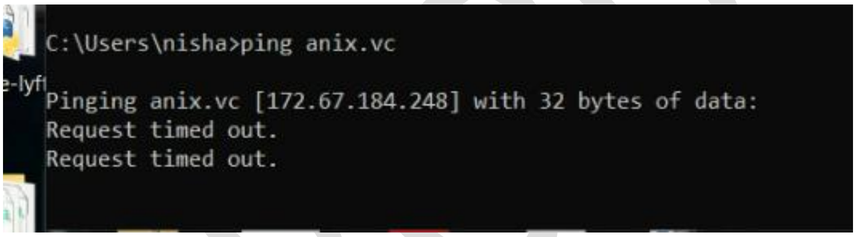
☑ Wait for reply

Attack status

Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
					232372	

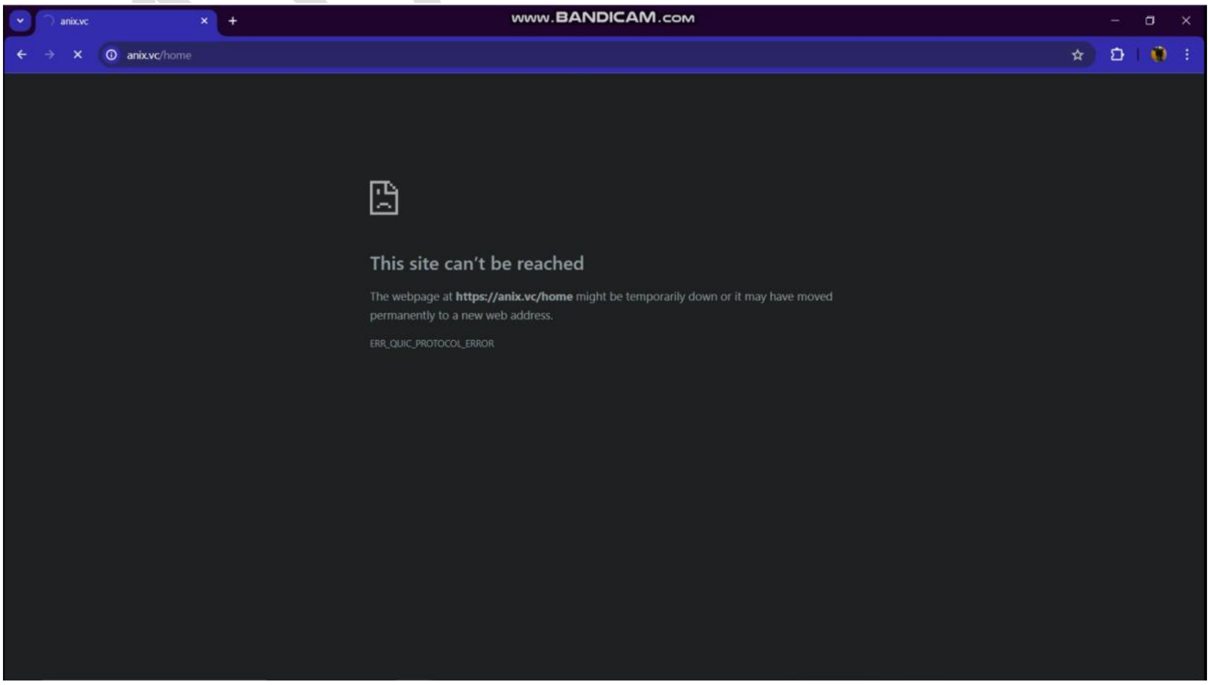
2 files: 233.8 KiB (239389 bytes) | Free space: 4.6 GiB

Fourth, ping the website again and check if attacked work



```
C:\Users\nisha>ping anix.vc

Pinging anix.vc [172.67.184.248] with 32 bytes of data:
Request timed out.
Request timed out.
```

Fifth, open website also check if working



This site can't be reached

The webpage at **https://anix.vc/home** might be temporarily down or it may have moved permanently to a new web address.

ERR_QUIC_PROTOCOL_ERROR

Prevention:

Preventing DDoS attacks requires a multi-layered approach. Here are some preventive measures:

1. **DDoS Protection Services**: Utilize DDoS protection services offered by various providers. These services often include traffic filtering, rate limiting, and specialized hardware to mitigate DDoS attacks.
2. **Network Monitoring**: Implement network monitoring tools to detect unusual traffic patterns that may indicate a DDoS attack in progress. Early detection allows for quicker response and mitigation.
3. **Firewalls and Intrusion Prevention Systems (IPS)**: Deploy firewalls and IPS to filter out malicious traffic and prevent it from reaching the target network.
4. **Load Balancers**: Distribute incoming traffic across multiple servers using load balancers. This helps prevent a single server from being overwhelmed by the traffic.
5. **Scalability**: Design your infrastructure to be scalable so that it can handle sudden increases in traffic. This can involve utilizing cloud-based services that can dynamically allocate resources as needed.
6. **Rate Limiting**: Implement rate-limiting mechanisms to prevent excessive requests from a single source. This can help mitigate the impact of DDoS attacks by limiting the amount of traffic that reaches the target.
7. **CAPTCHA**: Integrate CAPTCHA challenges into your web applications to differentiate between human users and bots. This can help reduce the effectiveness of automated DDoS attacks.

6.Result:

The result of conducting a DDoS attack simulation using tools like LOIC in a controlled environment for demonstration purposes can vary depending on several factors, including the intensity of the attack, the resources available to the target server, and the network infrastructure.

Here are some potential outcomes that you might observe:

1. **Service Disruption**: The targeted server may become unresponsive or slow to respond to legitimate requests due to the overwhelming volume of traffic generated by the DDoS attack. This could result in temporary downtime or degraded performance of the service hosted on the server.

2. **Network Congestion**: The network infrastructure surrounding the target server may experience congestion as it tries to handle the large volume of incoming traffic. This could affect other services or users on the same network.
3. **Resource Exhaustion**: The target server's resources, such as CPU, memory, and network bandwidth, may become fully utilized or exhausted due to the excessive load imposed by the DDoS attack. This could lead to crashes, freezes, or instability of the server.
4. **Mitigation Efforts**: If the target server has DDoS mitigation measures in place, such as traffic filtering or rate limiting, you may observe these measures in action as they attempt to mitigate the impact of the attack. This could include dropping or throttling incoming traffic from suspicious sources.
5. **Learning Experience**: From an educational perspective, conducting the demonstration can provide valuable insights into the mechanics of DDoS attacks, their impact on target systems, and the challenges involved in defending against them. It can also raise awareness about the importance of cybersecurity and the need for proactive measures to protect against such threats.

7.Knowledge Gained from Result:

From the results of the DDoS attack simulation demonstration, several key insights and knowledge can be gained:

1. **Understanding of DDoS Attack Impact**: Participants will gain a firsthand understanding of the impact of a DDoS attack on a target server or network. They will see how even a relatively simple attack tool like LOIC can effectively disrupt services and cause downtime or degraded performance.
2. **Awareness of Vulnerabilities**: The demonstration highlights the vulnerabilities that exist in network infrastructure and services, particularly in terms of their susceptibility to being overwhelmed by large volumes of traffic. Participants will learn that even well-designed systems can be vulnerable to DDoS attacks if adequate protections are not in place.
3. **Importance of DDoS Mitigation**: Participants will recognize the importance of implementing DDoS mitigation measures to protect against such attacks. They will learn about various mitigation techniques, such as traffic filtering, rate limiting, and use of content delivery networks (CDNs), to minimize the impact of DDoS attacks and ensure service availability.

4. **Ethical Considerations**: The demonstration underscores the ethical considerations involved in conducting security-related experiments or simulations. Participants will gain an appreciation for the potential legal and ethical implications of using tools like LOIC to perform DDoS attacks, even in a controlled environment.
5. **Education on Cybersecurity**: The demonstration serves as an educational opportunity to raise awareness about cybersecurity threats, such as DDoS attacks, and the importance of proactive security measures. Participants will be encouraged to take steps to protect their own systems and networks against such threats.

Overall, the knowledge gained from the demonstration can empower participants to make informed decisions about cybersecurity practices and measures, both in their personal and professional contexts. It reinforces the need for vigilance, preparedness, and collaboration in defending against cyber threats.