



**slington college**  
(इस्लिङ्टन कलेज)

**Module Code & Module Title**  
**CC5004NI Security in Computing**

**Assessment Weightage & Type**  
**30% Individual Coursework**

**Year and Semester**  
**2018-19 Autumn**

**Student Name: Abiral Joshi Shrestha**

**London Met ID: 17030696**

**College ID: NP01NT4A170008**

**Assignment Due Date: 2<sup>nd</sup> May, 2019**

**Assignment Submission Date: 2<sup>nd</sup> May, 2019**

**Word Count (Where Required):**

*I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a marks of zero will be awarded.*

## Contents

<i>Abstract</i> .....	3
<b>1. Introduction</b> .....	4
<i>Aims and Objectives</i> .....	5
<b>2. Background</b> .....	6
<b>3. Demonstration</b> .....	8
<b>4. Mitigation</b> .....	10
<i>*Solution for our particular scenario</i> .....	13
<b>5. Evaluation</b> .....	14
<b>6. Conclusion</b> .....	15
Bibliography .....	16

## Table of Figures

Figure 1 Demonstration of ICMP attack .....	5
Figure 2 Network Topology .....	8
Figure 3 Ping command .....	9
Figure 4 Ping results before attack.....	9
Figure 5 ICMP flood attack command .....	9
Figure 6 Ping results after the attack.....	10
Figure 7 Configuration of ACL.....	13
Figure 8 Ping results of Kali Linux & Router .....	13
Figure 9 Ping results of Windows 7 & Router .....	14

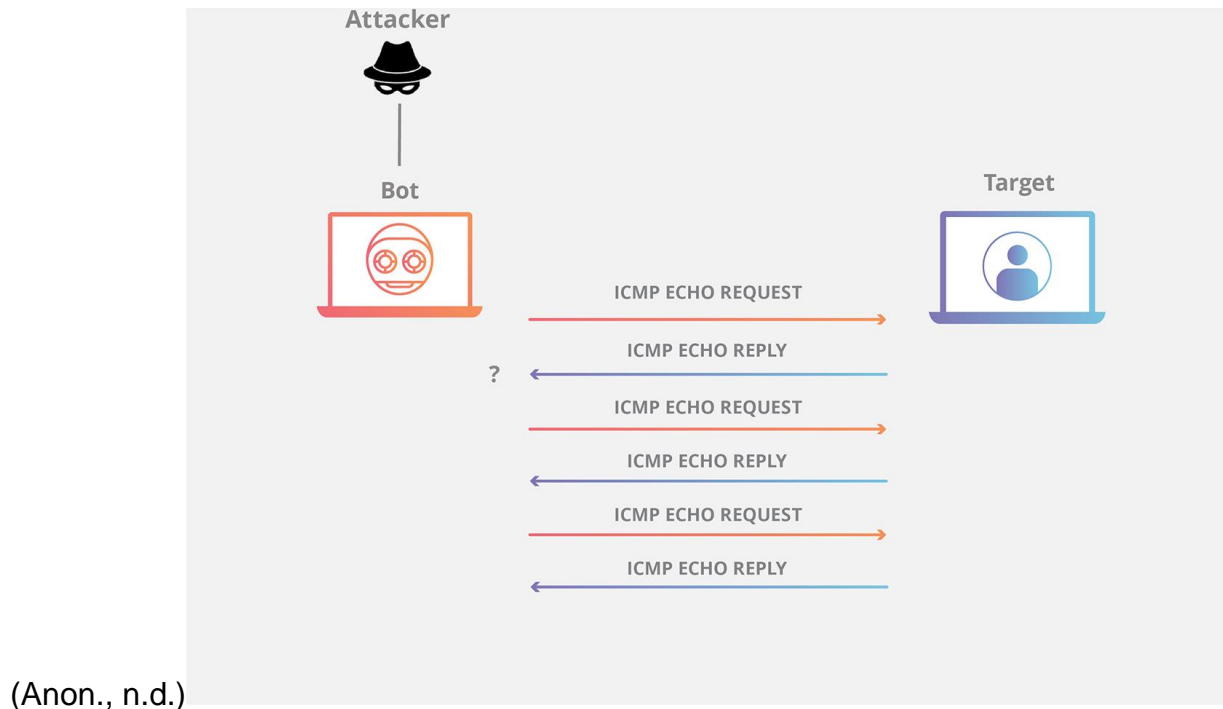
## ***Abstract***

The following project is a report of a demonstration of an ICMP (Internet Control Message Protocol) flood attack developed in the network software emulator, GNS3. It also provides the counter measures against such attacks. The ICMP flood attack was done in a virtual environment and no real harm was caused. It helped us analyse the effects of flood attacks on network security. Network security is the process of adopting suitable designs in order to protect the usability and integrity of the network and data.

## **1. Introduction**

Internet Control Message Protocol (abbreviated for ICMP) flood attack also known as a ping flood, is a type of Denial of Service (DOS) attack where the attacker takes down a victim's computer by overwhelming it with ICMP echo requests (pings). The ICMP flood attack involves the victim's network with request packets with the knowledge that the network will respond with an equal number of packets to reply (Anon., n.d.).

The Internet Control Message Protocol (ICMP), an internet layer protocol used by network devices to communicate is utilized in an ICMP flood or Ping flood attack. Traceroute and ping (network diagnostics tools) both operate using the ICMP. For the purpose of diagnosing the health and the connectivity of the device and the connection between the sender and the receiver. ICMP echo request and echo reply messages are used to ping a network device. Some server resources are required to process each ICMP request and to send a response. Some amount of bandwidth is also used on both the echo request (incoming message) and outgoing request (echo reply). In the ICMP flood attack, the attacker aims to overwhelm the targeted network device's ability to respond to a high number of requests and overload the network connection with unnecessary traffic. Having many devices in the targeted network, the attack traffic is increased considerably resulting in the disruption of normal network activity. The scale of damage caused by an ICMP flood attack is directly proportional to the number of requests made to the targeted server (Anon., n.d.).



*Figure 1 Demonstration of ICMP attack*

### ***Aims and Objectives***

The aims of this report are:

- i) To stimulate ICMP flood attack.
- ii) To learn about the preventive and counter measures against such attacks.
- iii) To understand the effects of ICMP flood attacks.

The objectives of this report are:

- i) The topic of ICMP flood attack is discussed along with a brief introduction.
- ii) ICMP flood attack and its consequences are explained.
- iii) Preventive and counter measures are explained.
- iv) Proper testing is carried out.

## **2. Background**

Network Security is a broad topic which covers a multitude of technologies, devices and processes. In simple words, network security is a set of rules and configurations designed to protect the confidentiality, integrity and accessibility (C.I.A) of computer networks and critical information using both hardware and software technologies. In today's day and age, attackers are continuously trying to find and exploit vulnerabilities, which can exist in a broad number of areas such as – devices, data, applications, users, locations, etc. So, it has become necessary to use network security management tools and applications in order to address individual threats and exploits. Network security should be designed in such a manner that it addresses the attacks that can occur in any layer of the network security layers model. Generally, network security consists of three types of controls: physical, technical and administrative (Anon., 2019).

Denial of Service (DOS) is a security incident which occurs when an attacker prevents legitimate users from accessing particular computer systems, devices, services and other IT resources (Rouse, 2018). Distributed Denial of Service (DDoS) is an attack in which multiple compromised computer systems attack a target, such as a server, website and/or other network resources, and cause a denial of services for the users of the targeted resource (Rouse, 2019). The primary reasons to carry out DOS and DDoS attacks are to effect the: consumption of computational resources, like bandwidth, processing time, disk space, etc., disruption of configuration information like – routing information, disruption of state information like unsolicited resetting of TCP sessions and to disrupt the physical network components (Monika Malik, 2015).

Generally speaking, DOS and DDoS attacks can be classified as three types:

i) Volume based attacks

The aim of this type of attack is to saturate the bandwidth of the attacked site. The magnitude of such attacks is measured in bits per

second (bps). UDP floods, ICMP floods, and other spoofed packet floods are some of the examples of volume based attacks (Anon., 2019).

ii) Protocol attacks

The purpose of this type of attack is that it consumes the actual server resources, or the resources of intermediate communication equipment such as firewall and load balancers. The magnitude is measures in terms of packets per second (pps). SYN floods, fragmented packet attacks, ping of death, Smurf DDoS, are some of the examples of protocol attacks (Anon., 2019).

iii) Application Layer attacks

The aim of this type of attack is to crash the web server. Its magnitude is measures in requests per second (rps). Low and slow attacks, GET/POST floods, attacks targeting Apache, Windows or OpenBSD vulnerabilities are some of the examples of Application Layer attacks (Anon., 2019).

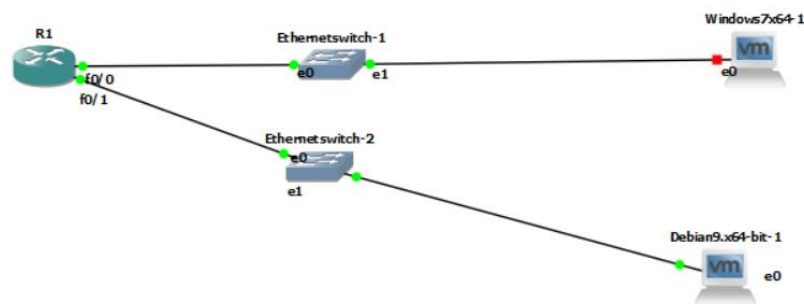
ICMP is a flooding attack. In the ICMP flood attack, the attacker overwhelms the target resource with ICMP echo request (ping) packets, large ICMP packets and other ICMP types to considerably slow down the victim's network infrastructure. ICMP stands for Internet Control Message Protocol. It is a connectionless protocol. It is used mainly to report errors and for diagnostics. But attackers use the ICMP to send payloads. In the ICMP flood attack, the attacker sends an abnormally large number of requests packets in order to overwhelm the target server, which has to deal with every incoming ICMP request. An ICMP flood attack contains a stream of ICMP echo packets generated by the attacker and aimed at the victim. The victim system then attempts to reply each and every ICMP request, consuming its CPU and network resources as the packets request for a reply which results in the saturation of the bandwidth of the victim's network. Even the source IP address might be spoofed. IP

spoofing is often used by attackers in order to hide their true identity which makes it even more difficult to trace back DDoS attacks (Harshita, 2017).

### 3. Demonstration

To simulate the ICMP flood attack, GNS3 (Graphical Network Simulator 3), VMWare Workstation and Hping3 were utilized. GNS3 is a network stimulation tool used to emulate, configure, test and troubleshoot virtual and real networks (Anon., n.d.). VMWare Workstation is a virtual machine software for running multiple operating systems as virtual machines on a single PC (Anon., n.d.). Hping3 is a network tool which is used to send custom TCP/IP packets and to display target replies (Anon., n.d.).

#### 3.1) Creating the topology



*Figure 2 Network Topology*

The topology contains a router (R1), switch (Ethernetswitch1), another switch (Ethernetswitch2) and two virtual machine (VMs): Windows 7 and Kali Linux. Switch 1 is connected to the interface fa0/0 of the router R1, having an IP address 192.168.0.1 and subnet mask of 255.255.255.0. The Windows 7 VM is connected to the Ethernet port e1. Windows 7 has an IP address of 192.168.0.2 and subnet mask of 255.255.255.0. Ethernetswitch2 is connected to interface fa0/1 of the router R1, having an IP address 192.168.1.1 and subnet mask 255.255.255.0. In this scenario, the router, R1, is the victim, Kali Linux is the attacker and Windows 7 is used for ping testing.



### 3.2) Normal Ping

The interface fa0/0 of R1 pinged from Kali Linux before the attack.

```
>ping 192.168.0.1
```

Figure 3 Ping command

```
Pinging 192.168.0.1 with 32 bytes of data:  
Reply from 192.168.0.1: bytes=32 time=2ms TTL=255  
Reply from 192.168.0.1: bytes=32 time=7ms TTL=255  
Reply from 192.168.0.1: bytes=32 time=8ms TTL=255  
Reply from 192.168.0.1: bytes=32 time=10ms TTL=255  
  
Ping statistics for 192.168.0.1:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 2ms, Maximum = 10ms, Average = 6ms
```

Figure 4 Ping results before attack

As you can see, the ping results before the flood attack is normal and there is no delay or packet loss.

### 3.3) ICMP Flood attack

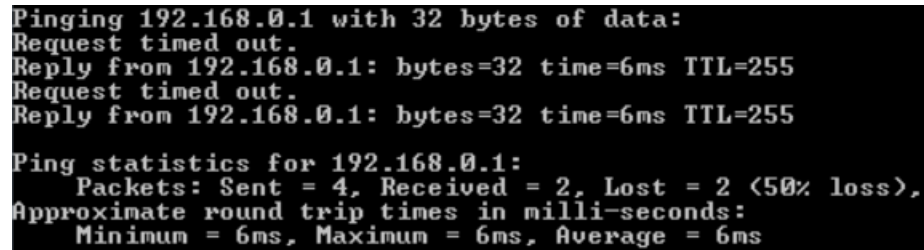
```
root@kali:~# hping3 -1 --flood -a 192.168.0.1 192.168.0.255  
HPING 192.168.0.255 (eth0 192.168.0.255): icmp mode set, 28 headers + 0 data bytes  
hping in flood mode, no replies will be shown
```

Figure 5 ICMP flood attack command

ICMP flood attack was carried out as seen in the figure above. Kali Linux is used to carry out the flood attack through the use of hping3.

### 3.4) Post attack ping

After the attack, I tried to use Windows 7 to ping to the router.



```
Pinging 192.168.0.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.0.1: bytes=32 time=6ms TTL=255
Request timed out.
Reply from 192.168.0.1: bytes=32 time=6ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 6ms, Average = 6ms
```

*Figure 6 Ping results after the attack*

As you can observe, even when pinging from a trustworthy client, Windows 7, there is loss of packets and a slight delay as well.

So, we can conclude that the ICMP flood attack was successful.

## 4. Mitigation

Although DOS attacks such as- ICMP flood attack, can be quite harmful and unrecognisable. There are a few techniques which can be applied to lessen the effects and the occurrence of such DOS attacks. Some of the mitigation techniques are:

### i) Attack Detection

The first step of any mitigation strategy is understanding when you are targeted for a DOS attack. The first step in keeping your service responsive and available is analysing incoming traffic and determining whether or not it's legitimate. Another great method to mitigate DOS attacks is to use scalable cloud service providers but they are not affordable due to bandwidth and resource overuse. To avoid this, you have to make sure that your cloud provider makes scaling decisions based only on the legitimate traffic. In short, every detection of attacks increases the overall efficiency of any mitigation strategy drastically (Anon., 2017).

ii) IP Whitelisting/Blacklisting

One of the simplest defence against a DOS attack is to either block (blacklisting) known attackers' IP or to whitelist only the legitimate IP addresses. It is much simpler to blacklist or whitelist from a specific IP range. This can issues where only the citizens of a given nation at are use a provided network resources, but it can prevent legitimate traffic from other countries from accessing the network resources. Blacklisting is also miserable in the case that you blacklist all users sharing an IP address, even if some of those users are legitimate. Also, this technique is not that reliable against those DDoS attacks and DOS attacks which use spoofed IP addresses. In the distributed scenario, there may be zombie computers with IP addresses everywhere but it may become complicated and untenable to create a rule to filter the out (Anon., 2017).

iii) Rate Limiting

The practice of limiting the amount of traffic available to a specific Network Interface Controller (NIC) is known as rate limiting. It can be carried out in both hardware and software level to mitigate the chances of falling victim to DOS attacks. Switches and routers have some degree of rate limiting capabilities at the hardware level while it's essential to establish a limit on the number of concurrent calls available to a given customer. Establishing the limit for user to make concurrent or total requests over a duration of time can be a great way of avoiding traffic and maintaining service stability. But relying on a router's rate limiting features means that the requests still reach the router and as we know, even the best routers can be DOSed and overwhelmed. This means that your service can still be overwhelmed, even though it is only returning error status code (Anon., 2017).

iv) Upstream Filtering and DDS

In the process, the requests are filtered upstream before it reaches the target network. Even done correctly, the API never notices this traffic, so the rate limiting policies are not triggered. Passing DOS mitigation to

upstream providers is a great way to reduce risk and liability as mitigation can be very complex and ever-changing for both the service providers and attackers. Such companies offer support even if your service is currently under attack, in order to minimize damages. It is then the duty of such companies to keep abreast of new DDoS attack vendors and strategies. This allows the client to focus on building your service (Anon., 2017).

v) Programming for Scale

In some cases, the team pays more attention to the shipping features and less attention to the performance. As service becomes more and more popular, it becomes harder to go back and to fix the performance issues before they create a widened surface area for attackers. So, it is a good idea to make performance testing a part of the development cycle and continuous integration process. The Apache Bench command can be used to get basic performance information about your service. This command can also be used to write automated tests that stimulates users and checks if the service responds to the requests within a specified time. To ensure the application code performs according to the satisfaction of the organization, performance tests should be run during the continuous integration process (Anon., 2017).

### ***\*Solution for our particular scenario***

Due to the ICMP flood attack by Kali Linux, even the genuine user windows 7 is not able to access the network resources efficiently. To remove this issue, an ACL (Access Control List) was created in the router R1 as shown below:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list standard QWE
R1(config-std-nacl)#permit hosy 192.168.0.2
Translating "hosy"
                                     ^
% Invalid input detected at '^' marker.

R1(config-std-nacl)#permit host 192.168.0.2
R1(config-std-nacl)#deny any
R1(config-std-nacl)#exit
R1(config)#int fa0/0
R1(config-if)#ip access-group QWE out
```

*Figure 7 Configuration of ACL*

You can observe that it states to permit access to 192.168.0.2 (Windows 7).

Then, we trying to ping the router R1 from Kali Linux, the results of the ping were as shown below:

```
root@kali:~# ping -s 10 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 10(38) bytes of data.
From 192.168.1.2 icmp_seq=1 Destination Host Unreachable
From 192.168.1.2 icmp_seq=2 Destination Host Unreachable
From 192.168.1.2 icmp_seq=3 Destination Host Unreachable
From 192.168.1.2 icmp_seq=4 Destination Host Unreachable
From 192.168.1.2 icmp_seq=5 Destination Host Unreachable
From 192.168.1.2 icmp_seq=6 Destination Host Unreachable
From 192.168.1.2 icmp_seq=7 Destination Host Unreachable
From 192.168.1.2 icmp_seq=8 Destination Host Unreachable
From 192.168.1.2 icmp_seq=9 Destination Host Unreachable
^C
--- 192.168.0.1 ping statistics ---
10 packets transmitted, 0 received, +9 errors, 100% packet loss, time 9175ms
pipe 4
```

*Figure 8 Ping results of Kali Linux & Router*

As we can observe, the ping from Kali Linux to router, R1, is unsuccessful due to the ACL configuration.

To check whether the mitigation was fully successful, I again tried to ping the router, R1, from Windows 7. The ping results were as shown below:

```
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Reply from 192.168.0.1: bytes=32 time=5ms TTL=255
Reply from 192.168.0.1: bytes=32 time=6ms TTL=255
Reply from 192.168.0.1: bytes=32 time=7ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 7ms, Average = 5ms
```

*Figure 9 Ping results of Windows 7 & Router*

As we can observe, the ping from a genuine user, Windows 7 to the router, R1 is successful without any packet loss or delay. So, the effects of the ICMP flood attack were mitigated.

## **5. Evaluation**

There are many advantages and disadvantages of using DOS attacks such as ICMP flood attack. Some of the advantages of using DOS attacks are:

- i) DOS attacks require only one or a small number of launch systems in order to instigate the attack (Anon., 2010).
- ii) DOS attacks are pretty simple to launch and the resources required to launch a DOS attack can be within the reach of even the general public (Anon., 2010).
- iii) DOS attacks can be extremely as simple as flooding, as DOS attacks rely on large numbers of launch systems in order to overwhelm the defences of the target (Anon., 2010).
- iv) Through spoofing, the identity and the IP of the attacker can be kept private.

Along with these advantages, there are a few drawbacks to DOS attacks. Some of the disadvantages of DOS attacks are:

- i) Although DOS attacks require only one or a small number of launch systems to initiate the attack, we need to have knowledge of what kinds of small, low volume activities will take out the target (Anon., 2010).
- ii) In many types of DOS attacks, for example – flooding, we are relying on brute force (or volume), so there can be a problem in gathering a large number of systems to make this types of attacks successful (Anon., 2010).
- iii) If used by the wrong individuals, it can be very difficult or nearly impossible to trace back DOS attacks.

## **6. Conclusion**

In the above project, an individual report was created through research, analysis and use of appropriate software tools, covering the topic of DOS and DDoS attacks. From the above report, we can conclude that DOS and DDoS attacks are simple and yet complex to implement as the process to carry out such attacks is simple but it can be difficult to collect the necessary tools.

For the purpose of completing the task, we carried out an ICMP flood attack, where an attacker overwhelms the target resource with ICMP echo request, large ICMP requests and other types of ICMPs to effect the victim's network infrastructure negatively. We analysed and evaluated the effects of the attack on the network. This was later also demonstrated. Additionally, the mitigation techniques against such DOS and DDoS attacks were also discussed. Finally, the use of DOS (ICMP flooding) and DDoS was evaluated to explore some advantages and disadvantages of using such attacks.

## Bibliography

Anon., 2010. *DOS Review*. [Online]

Available at: <https://ezinearticles.com/?DosProtect-Review---The-Advantages-And-Disadvantages&id=5563632>

Anon., 2017. *How to Mitigate DoS Attacks*. [Online]

Available at: <https://developer.okta.com/books/api-security/dos/how/#dos-how>

Anon., 2019. *DDoS Attacks*. [Online]

Available at: <https://www.imperva.com/learn/application-security/ddos-attacks/>

Anon., 2019. *What is Network Security?*. [Online]

Available at: <https://www.forcepoint.com/cyber-edu/network-security>

Anon., n.d. [Online]

Available at: <https://www.cloudflare.com/img/learning/ddos/ping-icmp-flood-ddos-attack/ping-icmp-flood-ddos-attack-diagram.png>

Anon., n.d. *Getting Started with GNS3*. [Online]

Available at:

[https://docs.gns3.com/1PvtRW5eAb8RJZ11maEYD9\\_aLY8kkdhgaMB0wPCz8a38/index.html](https://docs.gns3.com/1PvtRW5eAb8RJZ11maEYD9_aLY8kkdhgaMB0wPCz8a38/index.html)

Anon., n.d. *hping3*. [Online]

Available at: <https://linux.die.net/man/8/hping3>

Anon., n.d. *Ping Flood*. [Online]

Available at: <https://www.imperva.com/learn/application-security/ping-icmp-flood/>

Anon., n.d. *Ping Flood DOS attack*. [Online]

Available at: <https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/>

Anon., n.d. *VMWare*. [Online]

Available at: <https://www.vmware.com/products/workstation-pro.html>

Harshita, 2017. Detection and Prevention of ICMP Flood DDoS Attack. *International Journal of New Technology and Research*, 3(3), pp. 63-69.

Monika Malik, D. Y. S., 2015. A review: DOS and DDoS Attacks. *International Journal of Computer Science and Mobile Computing*, 4(6), pp. 260-265.

Rouse, M., 2018. *DOS attack*. [Online]

Available at: <https://searchsecurity.techtarget.com/definition/denial-of-service>

Rouse, M., 2019. *DDoS attack*. [Online]

Available at: <https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack>