Analysis and Protection of Networks from Crossfire Attacks

V.Sahiti, Aditya Dhanekula, Achyuth Balanthrapu, Ramya Choppala

Abstract**:** ***Most part of examined assaults in Computer security or Network security are based on Crossfire Attacks and it is a critical concern for most of the Cyber Security experts. The attacker primarily focusses on the termination and degradation of the network connections for a selected target which is a server in this context. In crossfire attack, a set of bots starts damaging servers by flooding only few primary nodes in the network. These attacks are different from the DDOS attacks in quite few aspects otherwise it is common. The attacker here affects set of bots and he does not spoof the IP address unlike in the DDOS, and the flooding is done with very low intensity, rather than in a fast pace, DDOS packets can be filtered by packet filters. In this paper, we present a broad audit of Crossfire Attacks to arrange and dissect the Crossfire Attack assaults scope on topologies. We considered the TCP/IP reference model and Crossfire Attacks assaults are grouped depending on different parameters and different topologies, for example, the attack time and performance may be different for a Mesh topology and a Star topology based on the path between nodes, having same number of nodes. The current countermeasures are overviewed. The paper arranges Crossfire Attacks assaults into four modules i.e., topology, no. of bots, time taken to isolate a node, ideal topology. At last, we present counteractive action systems for every single such assault and furthermore distinguish couple of future research bearings.***

Index Terms**:** ***Crossfire Attack, Defensive Mechanisms, GNS3 tool, Penetration Testing, Vulnerabilities, Wireshark.***

I. INTRODUCTION

In the context of the Computer Security, Crossfire Attack is an assault where the aggressor affects the bots by malware and starts flooding the links and isolating node from server.

Crossfire Attack is similar to DDOS, where the attacking pattern is slightly different, here the packets which are not spoofed are sent. Attack is carried in low moderate intensity.

The aggressor must have the capacity to affect number of computers and allow them to send continuous requests to the particular server which may result in the overloading of the node and that particular node or router doesn't forward any packets, which may result in shutting down of the server.

As there are various techniques like authorization and authenticity, the attacks are going to increase with new methodologies. As an assault that goes for dodging common verification, the attack is carried out in a way it looks like a traffic congestion over the network and Traffic engineering can solve the congestion, but actually, it isn't enough.

II. RELATED WORK

Min Suk Kang *et al.* [1], in 2015 have constructed the Crossfire Attack as a powerful attack which can destroy large servers in companies and even of governments. The Crossfire attack is generally performed at very slow pace and the sources of the attack cannot be detected. They have also mentioned that the attack that they created is very different from the attack defined by Chou *et al.* [11] which also uses the term “crossfire”. The author and team have provided step by step procedure on how to perform a crossfire attack in their paper. First, they have constructed an attack network which they use to perform the attack on target server. They have also calculated almost every parameter that they can in the process like Flow-Density, Throughput, Latency and many more.

Himanshu Gupta *et al.* [2], in 2015 describes safety towards penetration assaults using Metasploit. In this paper the author tries to present a system to counter the attacks by using few frameworks, specifically Metasploit. It includes the belief of a system that’s able to block the Metasploit assaults in particular instances in any other case alert the administrator. Previous studies indicate that many Intrusion detection Systems and antiviruses are useless against Metasploit. The proposed machine makes use of an application which is monitored by the communities that is capable of displaying the connection tried to the host system and reply hence by using algorithm used inside the device.

Matthew Denis *et al.* [3], in 2016 have tried different tools. assault techniques and defense methodologies which are used for penetrating a system. In this paper the author carried out unique penetration technique by using private networks, different physical devices and some virtual softwares and tools. The author predominately used the equipment in Kali Linux environment. The attacks performed includes telephone penetration testing, hacking telephones via Bluetooth, sniffing the devices that came in our Wi-Fi range, hacking WPA protected Wi-Fi and hacking long distance computers through IP and open ports using advanced port scanner. This paper specified crucial penetration trying out assaults and discussed ability of different prevention tools.

Revised Manuscript Received on 30 March 2019.
***** Correspondence Author

V.Sahiti*, Department of ECE, mail:sahiti.v@kluniversity.in Koneru Lakshamaiah Education Foundation, Vaddeswaram, Guntur - 522502, AP, India.

Aditya Dhanekula, Department of ECE, Koneru Lakshamaiah Education Foundation, Vaddeswaram, Guntur - 522502, AP, India.

Achyuth Balanthrapu, Department of ECE, Koneru Lakshamaiah Education Foundation, Vaddeswaram, Guntur - 522502, AP, India.

Ramya Choppala, Department of ECE, Koneru Lakshamaiah Education Foundation, Vaddeswaram, Guntur - 522502, AP, India.

Yaroslav Stefinko *et al.* [4], in 2016 has provided that infiltration testing enables associations to survey vulnerabilities proactively, using genuine world exploits, allowing them to assess the potential for their frameworks in order not to undermine the potentiality through hacking and malware conspires in a similar way that attackers use special kind of frameworks on UNIX core, developed scripts, utilities and applications. Cyber strikes have ended up being a standout amongst the best perils to the universe of business and economics. Amount of damage has been building up every day and more associations or establishments have advanced toward getting to be setbacks of ambushes or data break performed by dim hats. Hence, companies are scanning for most perfect way to deal with guarantee their structures and essential information. Most surely understood course is to test their structures by methods for penetration tests by affirmed good teams, which can proactively watch computer systems.

Rina Elizabeth Lopez de Jimenez *et al.* [5], in 2016 have performed an analysis on different intrusion techniques that are used for penetrating a web application. As a Whole, the team has conducted a broad survey on different concepts, methodologies and tools that are used for intruding. They have provided that results that no web application in the internet is secured even though the owners of web application have implemented a lot of techniques for the prevention of intrusion. So, we can conclude that no web application is perfectly safe and secure. The team has arrived at a judgement that by using the tools which were utilized in Ethical Hacking we can cover most of the vulnerabilities. The entire work is done for the benefit of Multinational companies for whom the security of their web applications if the major concern.

Narmeen Zakaria Bawany *et al.* [6], in 2014 has performed a broad survey on the detection of attacks and they have classified based on different detection mechanisms so that we can understand it clearly and improve the ability of understanding in a better way. They have performed the survey in such a way that, they identified the advantages and disadvantages of every technique and illustrate the requirements necessary for the prevention of attacks. The authors also proposed a new kind of algorithm based on SDN of a proactive DDoS Framework. They have termed this as ProDefense which has distributed controllers so that it will be very easier for the management of data center which was established in the smart city in their country. Finally, they have given a case study on how the ProDefense mechanism can be used for securing applications used in that smart city.

Hsiu-Chuan Huang *et al.* [7], in 2017 has proposed a new algorithm to identify Cross-site Scripting attacks using VulScan tool. The main reason they have selected VulScan is that it can automatically generate detection algorithms for identifying and also establish new evasion techniques. The algorithm mainly uses the information such as target system and scan type to select the technique for performing evasion. An implantation strike happens when an enemy sends data to an improperly coded application that beguiles it into executing unintended headings or questions shown by the adversary. A principle driver of unapproved data gets to be SQL imbuement, which incorporates sending malevolent data to change SQL request executed by web application databases.

Mohd Azahari Mohd Yusof *et al.* [8], in 2016 This team has proposed a new methodology to detect DDoS Attacks and essentially block them so that the network will be safe. They have monitored the incoming traffic and analyzed it whether it is attack traffic or not. If the traffic belonged to attack traffic, then they will observe the behavior of the traffic to determine the type of attack. First, we have to check if the traffic is most of UDP packets then we will classify it a UDP flood. Next, we check for SYN packets if they were sent repetitively then we can classify it a TCP SYN flood. After that we check if the packets being sent are oversized so we can note it as Ping of Death attack. Finally, we determine whether the traffic comprises of spoofed ICMP packets and we can say it as a Smurf attack. In this way they will identify the type of attack being performed and notify us.

Sandhya S *et al.* [9], in 2017 developing innovation has made an unavoidable risk of uncover of information that is shared on the web. Wireshark apparatus empowers the moral programmer to uncover the blemishes in the framework security at the client validation level. This methodology of recognizing vulnerabilities is regarded fit as the technique engaged with this testing is fast and gives great achievement in recognizing vulnerabilities. The use of Wireshark additionally guarantees that the technique pursued is up to the required gauges. This paper talked about the need to use infiltration testing, the advantages of utilizing Wireshark for the equivalent and proceeds to delineate one technique for utilizing the apparatus to perform entrance testing. Most territories of a system are exceedingly helpless to security assaults by enemies. This paper centers around illuminating the previously mentioned issue by studying different devices accessible for infiltration testing. This additionally gives an example of fundamental entrance testing utilizing Wireshark.

Chung-Kuan Chen *et al.* [10], in 2018 Internet of Things (IoT) gadgets and administrations are presently basic to most every day exercises. In any case, the IoT brings included comfort as well as, by associating an ever-increasing number of items to the Web, new security threats. Many applications in IoT environments, from keen homes to altered medicinal services, contain delicate individual data that can turn into the objectives of system attacks. Unfortunately, guaranteeing the security of IoT objects isn't clear for three noteworthy reasons. In the first place, the IoT's heterogeneous nature makes it powerless against numerous sorts of assaults. Second, heavyweight security instruments are infeasible for asset compelled IoT devices. Third, numerous IoT objects are sent just once and from that point are once in a while kept up or refreshed. After conducting the research on various attacks that are most common in security field, we have got to know that Crossfire Attacks are the deadliest and stealthiest attacks of all. So, we decided to do our research work on it to analyze and devise some new plans in order to counter those attacks and keep the networks safe and secure.

III. THEORETICAL ANALYSIS

The assaults that are performed on the servers are for the most part sorted into Four kinds dependent on the Components. They are: Physical Assaults, System Based Assaults, Programming Assaults, Web Assaults. These assaults contrast from one another and utilize a particular piece of IoT gadgets and pcs to assault and upset them for their typical working and to take down the entire server and affecting much more gadgets.

A. Physical Assaults

These assaults are performed on the equipment utilized. Inclusion of gadgets like flash drives and different gadgets can infuse malware into the gadgets and influence their usefulness. As the IoT gadgets are associated with one another the aggressors can likewise make botnets utilizing the associated gadgets and can play out a Crossfire Attacks assault on the objective gadget. The gadgets which are utilized for the most part utilized in the outside situations are powerless for physical assaults.

B. System Based Assaults

These assaults are finished by invading into the system and this does not require physical access to the gadget. These assaults are finished by accessing the gadgets present in the system. One of such assaults is Man in The Middle (MITM) attacks. Amid this assault the aggressor places himself between the two gadgets which are conveying in the system and captures the information that is transmitted between those gadgets. These are used within the organizations to steal the security keys related to the network or access the server from within a particular organization. These assaults are fundamentally done my phishing and furthermore diverting the clients to different site that ask individual data and they take over their gadget.

C. Programming Assaults

Programming assaults alludes to the assault on the product utilized in the IoT gadgets by infusing malware, infections into the product and interfering with its typical capacity. This malware can take the gadget or pc and can operate remotely with the instructions given from the assaulter and these become Zombie computers.

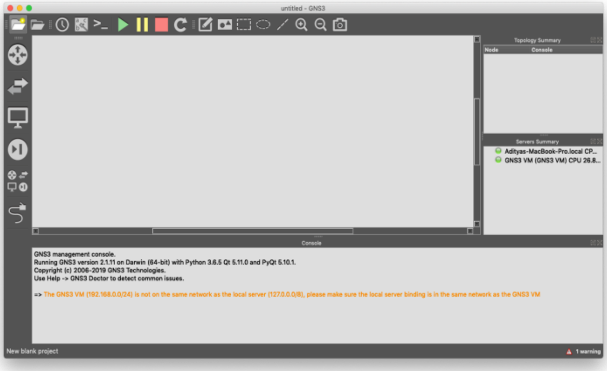
D. Web Assaults

These are the assaults that the attackers attach a file to the web server in java script whenever we try to access our web, these files automatically get downloaded without our concern and they perform certain tasks without user authentication. This questions our privacy.

So, Crossfire Attack not only brings down an entire server down, it also affects our gadgets and puts our privacy in risk. A lot of personal data will be stolen from the user.

IV. EXPERIMENTAL ANALYSIS

A. GNS3



```
GNS3 management console.
Running GNS3 version 2.1.11 on Darwin (64-bit) with Python 3.6.5 Qt 5.11.0 and PyQt 5.10.1.
Copyright (c) 2006-2019 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=> The GNS3 VM (192.168.0.0/24) is not on the same network as the local server (127.0.0.0/8), please make sure the local server binding is in the same network as the GNS3 VM
```

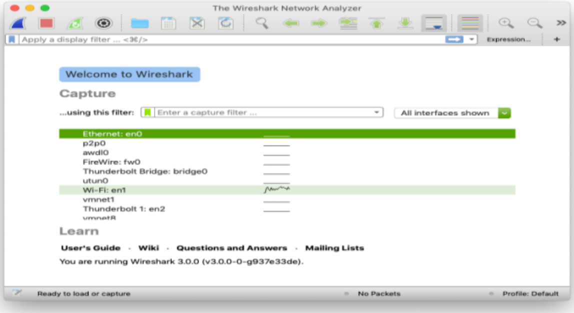
Fig. 1 GNS3 tool layout

GNS3 is a Graphical Network Simulator used for construction of complex networks, it allows the combination of virtual and real devices. Using GNS3 we get an actual virtual working network.

GNS3 tool is more of an emulator rather than simulator because all the devices which we use work similar to those of real-world devices. We can also buy more devices if we wish from the respective vendors of devices.

Here, we have different panels and menus in the main layout. The central part of our window is the main Workspace area where we create all the virtual networks using the devices. The left side panel is where all the network devices and other devices are stored, and we can simply drag and drop any device on to the workspace area and finally we can connect those devices using wiring option which is also available in the left side panel. To the right side we have Topology summary where all the devices which we use in our emulation are listed and detailed. Just below that we have Servers summary where all the servers we use to perform the emulation are present. The default server is the localhost and we can even use GNS3 VM as another server which is more efficient than that of localhost. Then we have a console display to the bottom of the window where all the information about the software is displayed and it also shows all th errors and warnings.

B. Wireshark



You are running Wireshark 3.0.0 (v3.0.0-0-g937e33de).

Fig. 2 Wireshark tool layout

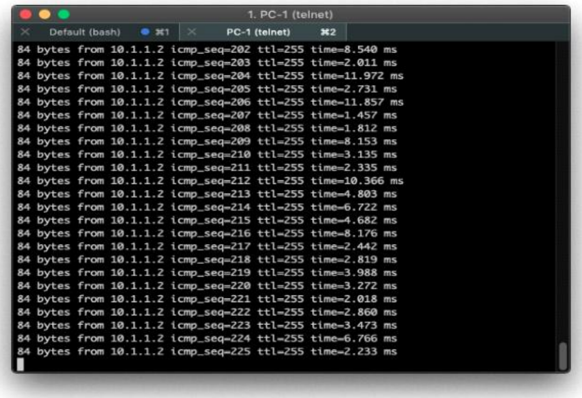
Wireshark is a ground-breaking instrument used to Analyze, Filter and Capture the packets in a system. It is exceptionally valuable in sniffing packets from the system. We can painlessly dissect the system and analyze it by using this tool.

In Wireshark, we can intercept any network device that is in our system to monitor and analyze all the traffic that goes through that particular network module. When we open Wireshark tool it displays all the available network devices in our system, and we can select any module to monitor. When we click on any device it opens a new window where all the traffic in the form of packets that flows through the device will be displayed, we can also select any particular packet and know all the details about it like headers, source and destination IP. In the main menu we also have tutorials about the Wireshark tool and along with the wiki forums.

C. ICMP FLOOD

ICMP flood also called as Ping Attack, is generally a Denial of Service Attack in which we send a lot of ICMP packets to the target. This ICMP protocol is used because it sends packets as fast as possible and also it does not wait for the acknowledgement from the destination.

In GNS3 tools, when we add any new devices or even computers, we will have access to the terminal of that particular device which we can use just like how we are using for a real device. We can configure the IP address of the device and also mention the DNS servers for it. We have to connect that device to internet module in or der to access it even from outside world.



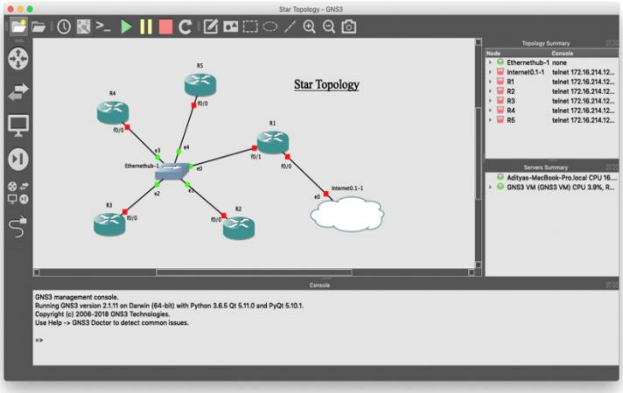
```
84 bytes from 10.1.1.2 icmp_seq=202 ttl=255 time=8.540 ms
84 bytes from 10.1.1.2 icmp_seq=203 ttl=255 time=2.011 ms
84 bytes from 10.1.1.2 icmp_seq=204 ttl=255 time=11.972 ms
84 bytes from 10.1.1.2 icmp_seq=205 ttl=255 time=2.731 ms
84 bytes from 10.1.1.2 icmp_seq=206 ttl=255 time=11.857 ms
84 bytes from 10.1.1.2 icmp_seq=207 ttl=255 time=1.457 ms
84 bytes from 10.1.1.2 icmp_seq=208 ttl=255 time=1.812 ms
84 bytes from 10.1.1.2 icmp_seq=209 ttl=255 time=8.153 ms
84 bytes from 10.1.1.2 icmp_seq=210 ttl=255 time=3.135 ms
84 bytes from 10.1.1.2 icmp_seq=211 ttl=255 time=2.335 ms
84 bytes from 10.1.1.2 icmp_seq=212 ttl=255 time=10.366 ms
84 bytes from 10.1.1.2 icmp_seq=213 ttl=255 time=4.803 ms
84 bytes from 10.1.1.2 icmp_seq=214 ttl=255 time=6.722 ms
84 bytes from 10.1.1.2 icmp_seq=215 ttl=255 time=4.682 ms
84 bytes from 10.1.1.2 icmp_seq=216 ttl=255 time=8.176 ms
84 bytes from 10.1.1.2 icmp_seq=217 ttl=255 time=2.442 ms
84 bytes from 10.1.1.2 icmp_seq=218 ttl=255 time=2.819 ms
84 bytes from 10.1.1.2 icmp_seq=219 ttl=255 time=3.988 ms
84 bytes from 10.1.1.2 icmp_seq=220 ttl=255 time=3.272 ms
84 bytes from 10.1.1.2 icmp_seq=221 ttl=255 time=2.018 ms
84 bytes from 10.1.1.2 icmp_seq=222 ttl=255 time=2.860 ms
84 bytes from 10.1.1.2 icmp_seq=223 ttl=255 time=3.473 ms
84 bytes from 10.1.1.2 icmp_seq=224 ttl=255 time=6.766 ms
84 bytes from 10.1.1.2 icmp_seq=225 ttl=255 time=2.233 ms
```

Fig. 3 ICMP flood simulation

For performing the ICMP flood, we have to open the terminals for a lot of virtual computers, and we have to perform ping operation from every computer on our target server. On doing this, the load on the server will increase gradually and at some point, if we use a lot of computers then server may also get shutdown.

D. STAR TOPOLOGY

The Star Topology is the most common because maximum of the server client architectures is based on this topology. In this topology, the central hub controls and inspects all the traffic that flows through the network. The main advantage of this topology is that any new device can be added or removed without disturbing other nodes in the network.



Node	Console
Ethernethub-1	none
Internet0.1-1	telnet 172.16.214.12...
R1	telnet 172.16.214.12...
R2	telnet 172.16.214.12...
R3	telnet 172.16.214.12...
R4	telnet 172.16.214.12...
R5	telnet 172.16.214.12...

Adityas-MacBook-Pro.local CPU 16...
GNS3 VM (GNS3 VM) CPU 3.9%, R...

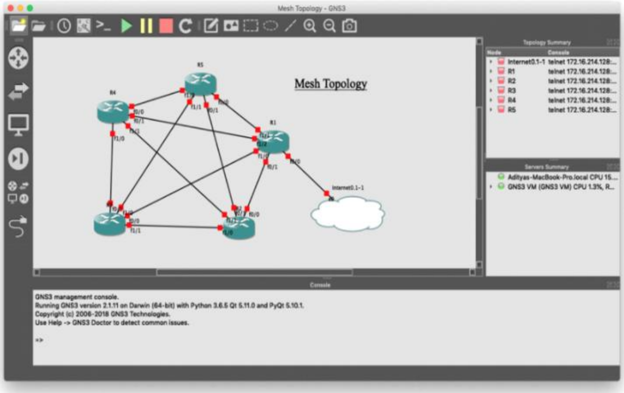
```
GNS3 management console.
Running GNS3 version 2.1.11 on Darwin (64-bit) with Python 3.6.5 Qt 5.11.0 and PyQt 5.10.1.
Copyright (c) 2006-2018 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

Fig. 4 Layout of Star Topology in GNS3 tool

In Fig. 4, we have constructed the star topology network in GNS3 tool. We have used an ethernet hub at the center. We have used Cisco c3745 Routers as nodes in the topology. The network is also connected to the internet using an internet module which is in the shape of cloud in Fig. 4. The links between the nodes will be in green color in they are running, and they will switch to red color if the nodes are stopped. We have implemented the entire virtual network on GNS3 VM instead of the local server so that network works efficiently.

E. MESH TOPOLOGY

In the Mesh Topology, all the nodes were connected to all the other nodes in the network using direct links. All the nodes manage the connections dynamically and cooperate with one another to form efficient route for the traffic flow. The main advantage is that the latency will be very low. Each node is connected to maximum other nodes possible.



Node	Console
Internet0.1-1	telnet 172.16.214.128:...
R1	telnet 172.16.214.128:...
R2	telnet 172.16.214.128:...
R3	telnet 172.16.214.128:...
R4	telnet 172.16.214.128:...
R5	telnet 172.16.214.128:...

Adityas-MacBook-Pro.local CPU 15...
GNS3 VM (GNS3 VM) CPU 1.3%, R...

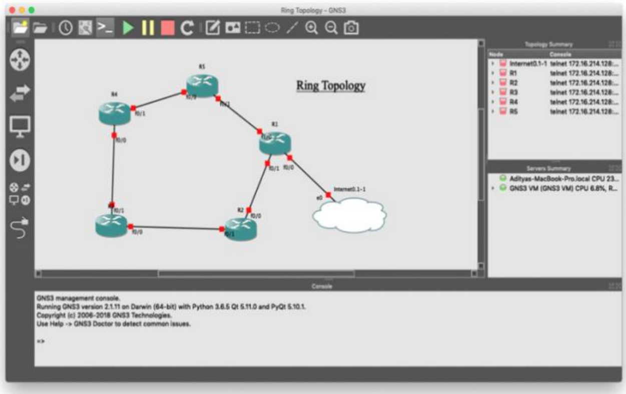
```
GNS3 management console.
Running GNS3 version 2.1.11 on Darwin (64-bit) with Python 3.6.5 Qt 5.11.0 and PyQt 5.10.1.
Copyright (c) 2006-2018 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

Fig. 5 Layout of Mesh Topology in GNS3 tool

Just like Star Topology, we have constructed the Mesh Topology using Cisco c3745 Routers, connecting all the nodes with all the other nodes in the network. We have connected the network to the internet using the internet module which is in the shape of cloud in Fig. 5. The entire Mesh Network is in a Subnet with IP range of 10.8.1.0/24. The links between the nodes will be in green color in they are running, and they will switch to red color if the nodes are stopped. We have implemented the entire virtual network on GNS3 VM instead of the local server so that network works efficiently.

F. RING TOPOLOGY

In the Ring Topology, all the nodes in the network are connected to only 2 other nodes of the same network forming a ring like structure. In this ring network, the traffic flow is unidirectional which can be classified as simplex structure. The main advantage is that the network is built in an orderly fashion which will help us to easily identify any faulty nodes.


Ring Topology - GNS3
Ring Topology
R1
R2
R4
R5
f0/0
f0/1
e0
Internet0.1-1
Topology Summary
Node
Console
Internet0.1-1 telnet 172.16.214.128:...
R1 telnet 172.16.214.128:...
R2 telnet 172.16.214.128:...
R3 telnet 172.16.214.128:...
R4 telnet 172.16.214.128:...
R5 telnet 172.16.214.128:...
Servers Summary
Adityas-MacBook-Pro.local CPU 23...
GNS3 VM (GNS3 VM) CPU 6.8%, R...
Console

```
GNS3 management console.
Running GNS3 version 2.1.11 on Darwin (64-bit) with Python 3.6.5 Qt 5.11.0 and PyQt 5.10.1.
Copyright (c) 2006-2018 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

Fig. 6 Layout of Ring Topology in GNS3 tool

In a similar fashion, we have constructed the Ring Topology using Cisco c3745 Routers, connecting the nodes with only the two adjacent nodes. We have connected the network to the internet using the internet module which is in the shape of cloud in Fig. 5. Just like the other 2 networks, the entire Ring Topology is in a Subnet with IP range of 10.8.1.0/24. The links between the nodes will be in green color in they are running, and they will switch to red color if the nodes are stopped. We have implemented the entire virtual network on GNS3 VM instead of the local server so that network works efficiently.

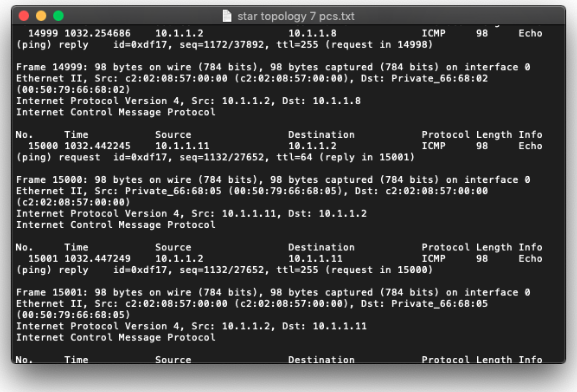
Finally, we have performed the ICMP flood on one of the nodes of the networks constructed separately.

V. EXPERIMENTAL INVESTIGATION

We have performed a simulation of crossfire attack using 7 computers on a single virtual computer in the GNS3 tool. We have analyzed all the traffic during this attack and the results are taken out in the form of a text file. We have kept a screenshot of the results at the 15000th packet to compare the time factor in the 3 different topological networks. All the source and destination computers lie in the same network in our simulation.

A. STAR TOPOLOGY

During the process of attack on Star Topology the 15000th packet occurred after 1032.44 seconds which means that due to the network structure it took 1032.44 seconds for the 15000th packet to reach the destination node from the source computer. This time factor lies between the time of mesh and ring topologies even though we used the same number of computers and same type of nodes.

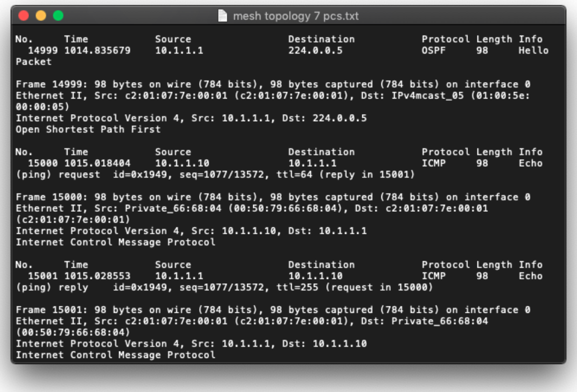


```
  14999 1032.254686    10.1.1.2              10.1.1.8              ICMP     98     Echo
(ping) reply    id=0xdf17, seq=1172/37892, ttl=255 (request in 14998)

Frame 14999: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: c2:02:08:57:00:00 (c2:02:08:57:00:00), Dst: Private_66:68:02
(00:50:79:66:68:02)
Internet Protocol Version 4, Src: 10.1.1.2, Dst: 10.1.1.8
Internet Control Message Protocol

No.     Time           Source                Destination           Protocol Length Info
  15000 1032.442245    10.1.1.11             10.1.1.2              ICMP     98     Echo
(ping) request  id=0xdf17, seq=1132/27652, ttl=64 (reply in 15001)

Frame 15000: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Private_66:68:05 (00:50:79:66:68:05), Dst: c2:02:08:57:00:00
(c2:02:08:57:00:00)
Internet Protocol Version 4, Src: 10.1.1.11, Dst: 10.1.1.2
Internet Control Message Protocol

No.     Time           Source                Destination           Protocol Length Info
  15001 1032.447249    10.1.1.2              10.1.1.11             ICMP     98     Echo
(ping) reply    id=0xdf17, seq=1132/27652, ttl=255 (request in 15000)

Frame 15001: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: c2:02:08:57:00:00 (c2:02:08:57:00:00), Dst: Private_66:68:05
(00:50:79:66:68:05)
Internet Protocol Version 4, Src: 10.1.1.2, Dst: 10.1.1.11
Internet Control Message Protocol

No.     Time           Source                Destination           Protocol Length Info
```

Fig 7. Performing ICMP Attack on Star Topology

B. MESH TOPOLOGY

While performing the same attack using the same type of nodes and computers, we have observed that the 15000th packet reached the destination after 1015.01 seconds. This time is the lowest of the other topological networks. This means Mesh Topology is very vulnerable to the Crossfire Attacks.

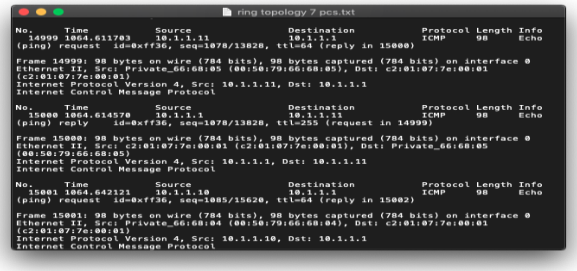


```
No.     Time           Source                Destination           Protocol Length Info
  14999 1014.835679    10.1.1.1              224.0.0.5             OSPF     98     Hello
Packet

Frame 14999: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: c2:01:07:7e:00:01 (c2:01:07:7e:00:01), Dst: IPv4mcast_05 (01:00:5e:
00:00:05)
Internet Protocol Version 4, Src: 10.1.1.1, Dst: 224.0.0.5
Open Shortest Path First

No.     Time           Source                Destination           Protocol Length Info
  15000 1015.018404    10.1.1.10             10.1.1.1              ICMP     98     Echo
(ping) request  id=0x1949, seq=1077/13572, ttl=64 (reply in 15001)

Frame 15000: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Private_66:68:04 (00:50:79:66:68:04), Dst: c2:01:07:7e:00:01
(c2:01:07:7e:00:01)
Internet Protocol Version 4, Src: 10.1.1.10, Dst: 10.1.1.1
Internet Control Message Protocol

No.     Time           Source                Destination           Protocol Length Info
  15001 1015.028553    10.1.1.1              10.1.1.10             ICMP     98     Echo
(ping) reply    id=0x1949, seq=1077/13572, ttl=255 (request in 15000)

Frame 15001: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: c2:01:07:7e:00:01 (c2:01:07:7e:00:01), Dst: Private_66:68:04
(00:50:79:66:68:04)
Internet Protocol Version 4, Src: 10.1.1.1, Dst: 10.1.1.10
Internet Control Message Protocol
```

Fig 8. Performing ICMP Attack on Mesh Topology

C. RING TOPOLOGY

Finally, when we performed the attack on the node which is in a ring topology the time taken for the 15000th packet to reach the target node is 1064.61 seconds which is the largest of all the other topologies. This means that the Ring Topology is the least prone to Crossfire Attack and anyone who wants to build their network which is resistant to crossfire attack can select this topology preferably.



```
No.     Time           Source                Destination           Protocol Length Info
  14999 1064.611703    10.1.1.11             10.1.1.1              ICMP     98     Echo
(ping) request  id=0xff36, seq=1078/13828, ttl=64 (reply in 15000)

Frame 14999: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Private_66:68:05 (00:50:79:66:68:05), Dst: c2:01:07:7e:00:01
(c2:01:07:7e:00:01)
Internet Protocol Version 4, Src: 10.1.1.11, Dst: 10.1.1.1
Internet Control Message Protocol

No.     Time           Source                Destination           Protocol Length Info
  15000 1064.614570    10.1.1.1              10.1.1.11             ICMP     98     Echo
(ping) reply    id=0xff36, seq=1078/13828, ttl=255 (request in 14999)

Frame 15000: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: c2:01:07:7e:00:01 (c2:01:07:7e:00:01), Dst: Private_66:68:05
(00:50:79:66:68:05)
Internet Protocol Version 4, Src: 10.1.1.1, Dst: 10.1.1.11
Internet Control Message Protocol

No.     Time           Source                Destination           Protocol Length Info
  15001 1064.642121    10.1.1.10             10.1.1.1              ICMP     98     Echo
(ping) request  id=0xff36, seq=1085/15620, ttl=64 (reply in 15002)

Frame 15001: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Private_66:68:04 (00:50:79:66:68:04), Dst: c2:01:07:7e:00:01
(c2:01:07:7e:00:01)
Internet Protocol Version 4, Src: 10.1.1.10, Dst: 10.1.1.1
Internet Control Message Protocol
```

Fig 9. Performing ICMP Attack on Ring Topology

VI. DEFENSIVE MECHANISMS

A. IP TRACEBACK

IP traceback is mainly used to identify the born place of any packet in the internet.

1) The IP protocol does not provide for the source authentication of source IP address of an IP packet.
2) Router based approach, router is charged with the packets that pass through it.
3) The ICMP traceback sends the ICMP packet to the destination of host IP address.

B. BOT HUNTERS

BotHunter is mainly is used for detecting Botnets in the internet or even in the traffic that our network is experiencing. They are not any kind of firewalls, blockers and spam blockers, they just detect the systems that are being used as bots or zombies. They identify the botnets in the internet when the communication is going on between the nodes.

In our work, BotHunters are used because the crossfire attack can only be done used a large group of systems which is termed as a Botnet.

C. PHANTOM NETS

Phantom Nets lures an attacker into a replica of our network topologies and traps them. White-Holes trick the attacker by portraying the actual network nodes as honeypots, thus failing the botnets miserably.

D. PACKET INSPECTORS

Packet inspectors inspect the packets during transmissions, they check how many numbers of packets are transmitted, if there are a greater number of packets are transmitted within a certain time than the actual amount it discards the packets and transmission. Similarly, it attaches all the fragments at the destination and checks the size of the packet, if any size overflow occurs it discards those packets too.

E. USER INSTRUCTIONS

1) Up to now there is no specified mechanism is invented for it.
2) Whenever we browse any website, we have to check for SSL certificate which can be easily identified by verifying the URL of that website.
3) Always confirm the particulars of the sender of any email before clicking on links in it.
4) Admin should have HSTS (HTTP Strict Transport Security).
5) Never download pirate software.
6) Always have a strong firewall.
7) Maintain logs for every action.
8) Regularly perform security checks and updates.
9) Secure your home network if it is connected to your commercial network.
10) Update your system accordingly.
11) Never click on malicious links or emails.
12) Have proper security tools installed on your system.

VII. CONCLUSION

Crossfire attack is considered a serious threat for man IT companies. Many companies are vulnerable to these attacks, they must be thorough with their security updates. The defense mechanism for this is attack not ready till now. It has become a great research area for providing defense mechanism for this threat. Crossfire may bring an empire down.

From the experimental investigations, when we perform ICMP flood attack on a node which is in Star Topology, it generally takes 1032.44 seconds for sending 15000 packets. In the same way, if we perform the same attack using same number of bots and for sending 15000 packets the time taken is 1015.01 seconds in Mesh Topology. Finally, for the Ring Topology, the time taken for sending 15000 packets is 1064.61 seconds.

Even though the time difference for sending same number of packets to different topology networks is minute which is in milli-seconds, in practical this small difference in time costs huge amounts for the companies.

Finally, we can conclude that the Ring Topological network is hard to penetrate because the time taken for sending packets is relatively more when compared to other topologies. So, whenever any company wants to design a topology for their network it is better, they opt for Ring Topology if the security is their primary concern.

REFERENCES

1. M. S. Kang, S. B. Lee and V. D. Gligor, "The Crossfire Attack," *2013 IEEE Symposium on Security and Privacy*, Berkeley, CA, 2013, pp. 127-141.
2. H. Gupta and R. Kumar, "Protection against penetration attacks using Metasploit," 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), Noida, 2015, pp. 1-4.
3. M. Denis, C. Zena and T. Hayajneh, "Penetration testing: Concepts, attack methods, and defense strategies," *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, Farmingdale, NY, 2016, pp. 1-6.
4. Y. Stefinko, A. Piskozub and R. Banakh, "Manual and automated penetration testing. Benefits and drawbacks. Modern tendency," *2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*, Lviv, 2016, pp. 488-491.
5. R. E. L. de Jiménez, "Pentesting on web applications using ethical - hacking," *2016 IEEE 36th Central American and Panama Convention (CONCAPAN XXXVI)*, San Jose, 2016, pp. 1-6.
6. Bawany, N.Z., Shamsi, J.A. & Salah, K. Arab J Sci Eng (2017) 42: 425. https://doi.org/10.1007/s13369-017-2414-5.
7. H. Huang, Z. Zhang, H. Cheng and S. Shieh, "Web Application Security: Threats, Countermeasures, and Pitfalls" in *Computer*, vol. 50, no. 06, pp. 81-85, 2017.
8. Yusof M.A.M., Ali F.H.M., Darus M.Y. (2018) Detection and Defense Algorithms of Different Types of DDoS Attacks Using Machine Learning. In: Alfred R., Iida H., Ag. Ibrahim A., Lim Y. (eds) Computational Science and Technology. ICCST 2017. Lecture Notes in Electrical Engineering, vol 488. Springer, Singapore.
9. S. Sandhya, S. Purkayastha, E. Joshua and A. Deep, "Assessment of website security by penetration testing using Wireshark," *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, 2017, pp. 1-4.
10. C. Chen, Z. Zhang, S. Lee and S. Shieh, "Penetration Testing in the IoT Age," in *Computer*, vol. 51, no. 4, pp. 82-85, April 2018.
11. J. C.-Y. Chou, B. Lin, S. Sen, and O. Spatscheck, “Proactive Surge Protection: a defense mechanism for bandwidth-based attacks,” *IEEE/ACM Transactions on Networking (TON)*, vol. 17, no. 6, pp. 1711–1723, 2009.

AUTHORS PROFILE

Sahiti Vankayalapati is an assistant professore currently working in the Department of Electronics and Communication Engineering in Koneru Lakshamaiah Education Foundation. Her work domain majorly covers Wireless Communications and Antennas.

Aditya Dhankeula is currently pursuing his bachelor's degree in Technology in the Department of Electronics and Communication Engineering at Koneru Lakshamaiah Education Foundation. His major field of interest is Networks and Cyber Security.

Achyuth Balanthrapu is currently pursuing his bachelor's degree in Technology in the Department of Electronics and Communication Engineering at Koneru Lakshamaiah Education Foundation. His major field of interest is Networks and Cyber Security.

Ramya Choppala is currently pursuing his bachelor's degree in Technology in the Department of Electronics and Communication Engineering at Koneru Lakshamaiah Education Foundation. His major field of interest is Networks and Cyber Security.