Analysis and Protection of Networks from Crossfire Attacks

A. Venkata Lakshmi
Dept of CSE
Besant Theosophical College.

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 focuses 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, Wire shark.

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.

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. 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 system

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, and 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.

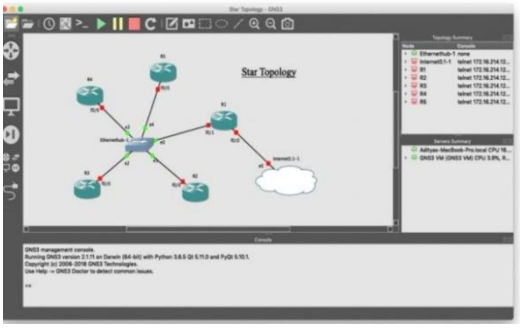
C. PROGRAMMING ASSAULTS:
Programming assaults alludes to the assault on the product utilized in the IoT gadgets by infusing malware, infections into the product and interfering with its typical capacity. This malware can take the gadget or pc and can operate remotely with the instructions given from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

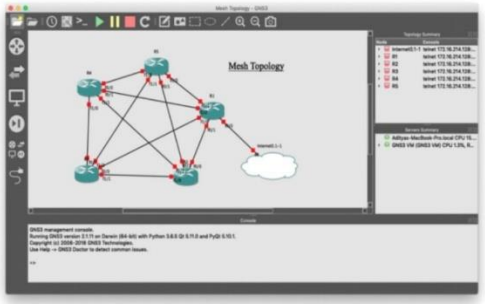
EXPERIMENTAL INVESTIGATION:

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.



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 Attack.



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.

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.

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.
[5] Bawany, N.Z., Shamsi, J.A. & Salah, K. Arab J Sci Eng (2017) 42: 425.
[6] 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.
[7] 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.
[8] 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.
[9] 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.
[10] 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, 200