ISSN : 2350-0743

www.ijramr.com

International Journal of Recent Advances in Multidisciplinary Research
Vol. 07, Issue 10, pp. 6349-6354, October, 2020

RESEARCH ARTICLE

TRACING DISTRIBUTED DENIAL OF SERVICE ATTACKS FROM PRACTICAL PERSPECTIVES

* **May A Alotaibi, Emad Alsuwat**

Department of Computer Science, Taif University

ARTICLE INFO

Article History:
Received 30th July, 2020
Received in revised form
26th August, 2020
Accepted 24th September, 2020
Published online 30th October, 2020

Keywords:

DDoS, DDoS Attack Methods; Flood Simulation, SYN-flood.

ABSTRACT

Denial of service attack was a stretch of Distributed Denial of Service Attack (DDoS). DDoS comes the largest security risks and problems facing Internet users. This risk affecting obstruct with work of any system of targeted organizations, which leads to the harassment of system customer. This attack succeeds by exploiting several weaknesses to access resources in the target organizations. The attacker exhausts all capacity of resources in a period short time. The previous method leads to the denial of using any organization's resources from any authorized user. This paper illustrated DDoS attack and flooding concept have been proposed. This paper deals in general with describing structural approach of DoS attack in different levels of services. In addition, content explains the motivations of the attackers to use different attacks. In particular, the concept of DDoS attack has been clarified. Also describing types of different flooding attack with examines SYN-flood and flooding attack.

INTRODUCTION

Internet architecture focuses on performance rather than security. Beginners leave their systems more vulnerable by focusing on performance. Like using easy and usual passwords, using the default mode in design, ignore using firewalls. Each previous examples are weaknesses that exploit and facilitate access to information (1).Leaving the system without change the default mode cause vulnerability to the system. The default value in every system known to attacker that keep attacker begin attack from many points. The most important and dangerous attacks is DDOS attack. DDOS attack is follows the same technique that DoS attack follow but in distributed way. DDoS attack is threat experiment to flood on internet (2). Some organizations secure their facilities or service s by making plans to mitigate the effects of the attacks(1). In DDoS approach, the attacker before begin this attack must have number of computers zombies (3, 4).Then use these zombies to send a massive number of requests per seconds to target system. The attacker must have motive to harm and stopping the victim's resources. DDoS attacks depend on filling out all possibilities to receive requests from victim side. This way done by sending a number of packets at the same time instead of targeting specific vulnerabilities. The main responsibility became distinguish differential between the normal traffic and abnormal traffic (1). DDoS attack is organized by controlling a number of Zombies or Botnet. The attacker controls these Zombies or Botnet remotely and can distribute it very widely.

***Corresponding author: May A Alotaibi,**
Department of Computer Science, Taif University.

The attacker directing Zombies to send a batch of data during one time or you are sending continuously. This attack results in slow reaction, complete DoS, or total disruption of the system(5-7). Zombies of a botnet are usually recruited by usingworms, backdoors or Trojan horses (4, 8, 9).Even with the use of defense mechanisms, it is difficult to pinpoint the real attacker's address. The reason is due to the attacker uses a number of zombie impersonated and it is under his control (10). This research focuses DDOS attack. In several respects, in section 2 DOS attacks and type of DoS attack. Section 3DDoS attack. Section 4 attacker motivation in DDoS attack.Section 5flooding concept. Section 6 Types of DDOS. Section 7 conclusion.

DOSAttacks and Types of DoS Attack: This section defines the concept of denial of service. It also illustrates the levels of denial of service attack and weaknesses that may be exploitedat these different levels of denial of service attack. DoS attacks take advantage of flaw in internet to flood target critical Web services(11-16) .DoS attacks designed to make network or device unable to make services available for use. DOS attack occurs when a regular user cannot gain access to a service. The attacker aims to intentionally blocked or decadent to be unavailable. These attacks do not necessarily result in direct or permanent damage to the data, but are aimed at depriving the availability of resources (17)(18). Blind DOS attack is use approach of DoS attack. This type of attack works by mixed of the application DoS and the network. The attacker has to keep application to process a huge number of data then return response query to the attacker. The impact of this attack is on processing process with application server's resources and transmission process in application server's network(18). DOS attacks can be divided to groups as shown in fig1:

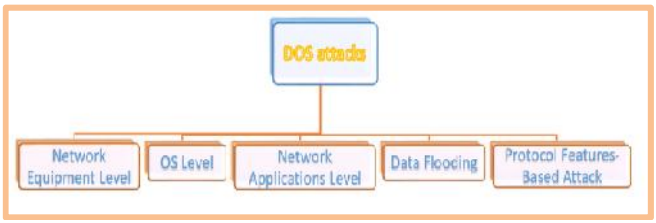

Fig 1. Levels of DoS attack (19)

Network Equipment Level: DOS attacks in this level contain attacks resulting from exploiting software errors or attempting to drain the network hardware resources (17).

OS Level: DOS attacks in this level gather and take advantage of method to implement protocols in operating systems (17).

Network Applications Level: Considerable many attacks attempt to straighten a device to make system out of service. Where can done by two different way. First by getting benefit of specific mistakes, which these mistakes are running in network applications of the target. the Second way is using this applications to know the resources of victim (17).

Data Flooding: At this level, the attacker uses the maximum available bandwidth for a network, host, or device. Then use it to send a large number of data that causing process very large amounts of data (17).

Protocol Features-Based Attack: DOS attack in this level need to take benefit from specific standard protocol features. For example benefit from spoofed IP by exploit in several attacks(17).

DDoS Attack

This section mentionsthe meaning of DDoS attack. The attacker in DDoS use numbers of computers to create a huge number of requests to flood victim server (20). These numbers of requests cause denial authorized user to access the system, network or server. In most cases, the owners of the attacked hosts do not know that attacker has used their recourse. In different case of example, opponent want to damage the utility rather than crash the system by flooding web server. Thus, now DDoS attacks are the considerable worry to get secure system in the cyberspace world. As shown in Fig 1 the DDoS attack depend on four main parts– an opponent, controller, zombies and target. They have places in numerous procedures. The opponent starting DDoS attack by compromises the multiple hosts to victim. The opponent uses one device to attack victim also, using remote authentication for all compromised machines. Then send many requests simultaneously for minimizing resources and bandwidth of the target machine (1).

Attacker Motivation in DDOS: In this section explains the motivations of the attackers to use this type of Attack. Motives for DDOS attackers are not limited to Specific reason. Thus, they are divided types based on their motivation. Where divide it into five main sections (21). Pecuniary/economic: These attacks are considered as the main worry of association. Attackers in this type have a high technical expertise. Based on their financial incentive, they are considered one of the most dangerous types of attackers. It is difficult to stop them.

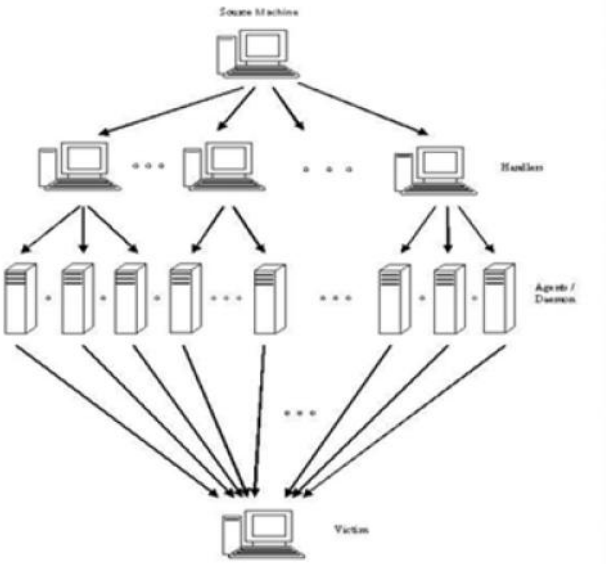

Fig 2. DDoS attack parts (17)

Reprisal: Attackers of this category are mostly suffering from depression. They have lower technical cleverness. Attackers of this kind are based on an injustice.

- Deological persuasion: opponent who indicates to this set are driven by his ideological beliefs to attack based on their goals (22). Currently they consider this group one of the main incentives for the attackers to start DDoS attacks.
- Challenge of Intellectual: opponent of this group attacks the specific system to test and know how to start different types if attacks. Most of them are young hackers who wish to boast their ability. In these days, many useable attack programs enable amateurs to launch an attack.
- Cyber warfare: This group of attackers belong to the organizations of military or terrorist.

Flooding Concept: This section shows to you the meaning of flooding by using VM. Flooding helps attacker to begin DDoS attack. Itmeans full all available resources on targeted system. This method prevents the use of resources from any authorized user on the server. VM help you to understanding the flooding method by using kali machine and windows machine. Kali represent attacker machine where windows represent server or the targeted system. Send flood requests using hping3 to IP address of windows machine as the following command in Fig 3 sent 11113414 packets per short time. Go back to windows and open the wireshark tool to see if sent flood packets are received at victim side as shown in Fig 4 ,5 and 6.

Fig 3: Flooding command.

DDoS Attack Process: This section mentions the process of DDoS attack. In addition, the types of food require.

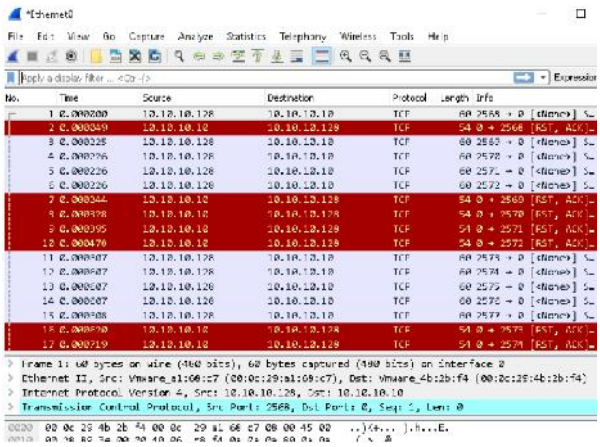

Fig 4. Wireshark displays flood packets received in victim side

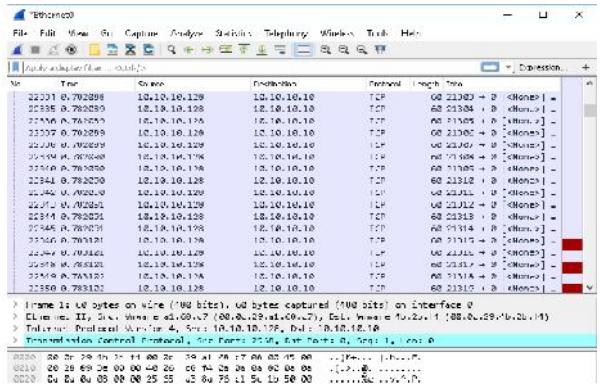

Fig 5: wire shark displays flood packets received in victim side.

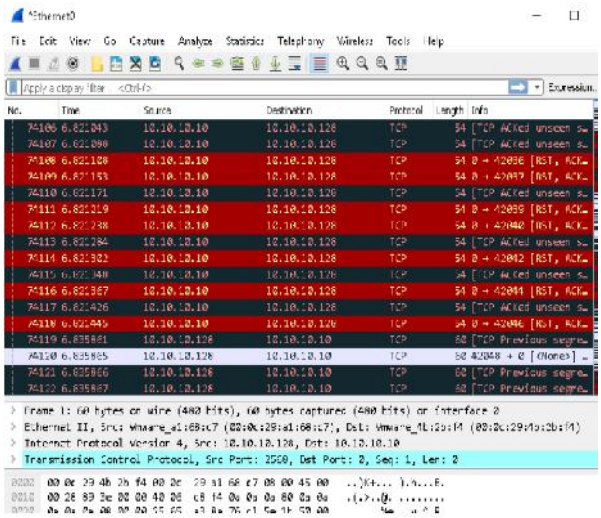

Fig 6. Wireshark displays flood packets received in victim side

DDoS attack target the misuse of security vulnerabilities in the software running at the victim side. The attacker exploits these vulnerabilities for deplete resources or (Flooding Attacks).Flooding attacks depends on sending massive number of traffic that running in victim side (23). When attacker want to perform exploit vulnerability attacks like TCP SYN attack, normally must include packets of a specific kind or signification. Some few packets cause to frequently exploit vulnerabilities. Vulnerability attacks are low-volume. Low volume features and specific kind of packets are works to simplify the handling of vulnerabilities. The target system can correct these vulnerability or discover the specific kind of packets and Treat it separately (23). Flooding attacks considered as the most difficult strategy. It hard to handle any type or content of malicious packets and the massive handicap detailed traffic analysis. The reason is overcome the target resource by sending massive volume of packets (23). The most widespread methods in DDOS attacks are Smurf,ICMP, TCP SYN, UDP, TCP floods and set of them(23).

Smurf Floods: This type of flood is known as a reverse attack. An opponent sending ICMP ECHO requests to flood the network and take reply with IP address of victim. It changes the source address to the target system address, so it can respond to a number of pings that flood the network. We can control the attack by publishing filter packet enter at source network or filtering at intermediate network for ICMP ECHO requests (23).

ICMP Floods: The opponent is sending a batch of ICMP ECHO requests to the victim machine. The victim addresses these requests with a response that consumes the victim's resources. This attack is easy to spread and defend. Defense against this flood attack by determined a high bandwidth frequency that come from any requests. This type of defense need to drop bandwidth higher than specified which cause some real requests are dropped(23, 24).

UDP Floods: UDP floods means sending a huge number of UDP packets to the victim side. The attacker needs to connect to available space to effectively utilize in all network bandwidth at target system. Generally, the attack can perpetrate in simple way. Packets are sent over this attack has large size. Here are many targeted sites that do not accept receiving large volume regularly from UDP traffic coming from any user. as they can deal with the attack in a successful way and they ignore the packets that are high bandwidth by using easy filtering commands (3, 23, 24).

TCP Floods: In TCP floodis using TCP protocol rather than UDP floods. They are similar in implement but different in type of packet (23).

TCP SYN Floods: A TCP SYN attack done by using specific weaknesses in the TCP protocol many times to exploited. This attack works by exploiting the usual method of servers with setting up a TCP connection (triple handshake).In each server has to provide number of messages with Clint to connect and get service. When client and server established session over network, a small buffer space for exchange packets "hand-shaking". TCP SYN attack succeeds if this resource is well exploited by the attacker (23). In each connection over TCP need to exchange Three Way Handshake between client and server. Client send SYN with sequence number in the message exchange. When the server receives this package, it temporarily stores information about the client in a temporary buffer record. Then server reply to client with a SYN / ACK to tell the client your request will be granted sends initial sequence number about the server's. When client receive SYN/ACK packet has to allocate a record of the connection buffer. Then client reply to server with ACK response. which that mean ready to exchange message (open connection) (23, 24).

SYN flooding attack: Here is an example of SYN-flood by using Virtual machine (VM) in Linux to perform SYN Flooding. For preforming this attack, I need three vm's. First machine, for the attacker, target machine and server machine.

The IP address of each machines can be defined by using ifconfig command. Hereis the IP address of three machine Victim, server, and attacker:

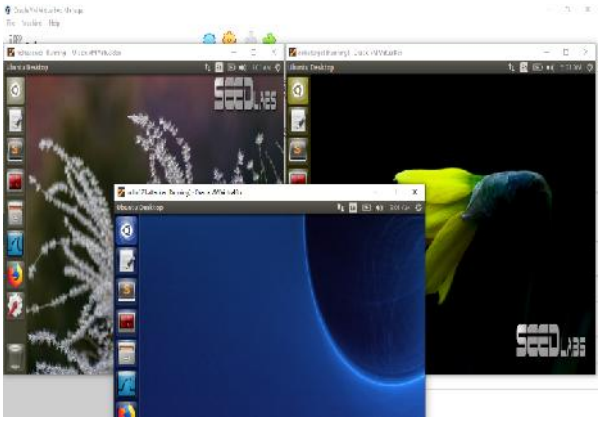

Fig 7. Three machines in VM.

Target VM IP : 10.0.2.6
Server VM IP : 10.0.2.8
Attacker VM IP : 10.0.2.9

- At the first, I opened 3 VM then, change all of them to be in the same LAN as shown in Fig 7.
- At server side, in Fig 8shows to you commandtoturn off the SYN cookies, otherwise the SYN cookies will prevent the SYN attack.

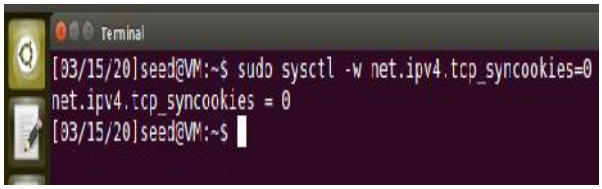

Fig 8. Closing the SYN cookies at the server side

- After that, use *netstate –tna*command in Fig 9to check if ports are listening.

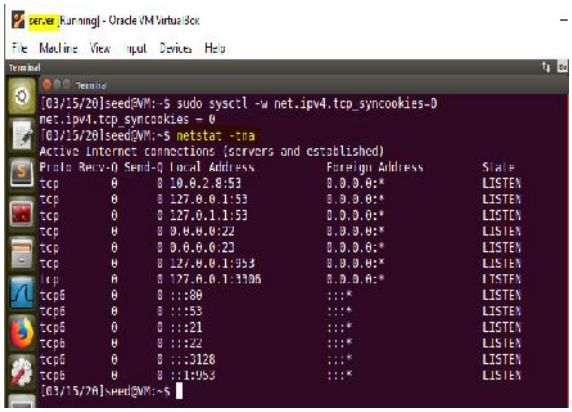

Fig 9. Display network state

- You can see target side in Fig 10, whichmadetelnet connection to server IP address.
- At server sidein Fig 11, type the same previous command, *netstat-tna*. You canfind the connection that made between the target and the server has been established.

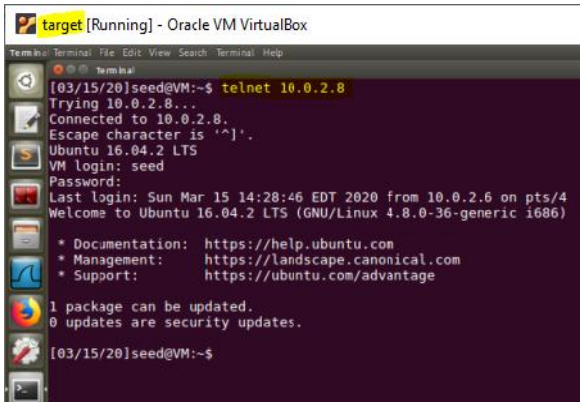

Fig 10: Telnet connection to the server

- At attacker side, send multiple SYN packets toward server VM by using *netwox 76* command as shown in Fig 12.

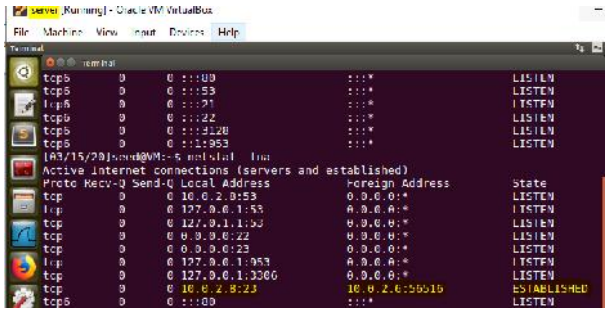

Fig 11: Connection state between target and server

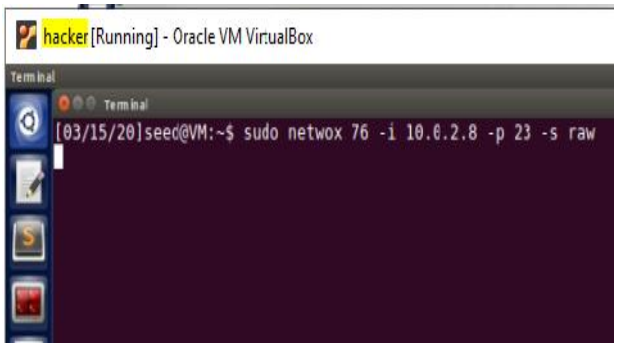

Fig 12. Send multiple SYN packets to the server

- As seen in Fig 13all these packets are half-open and making the server unable to except more packets.
- From target machine In Fig 14you can see the server VM are stoked with half open requests and making new connection impossible.

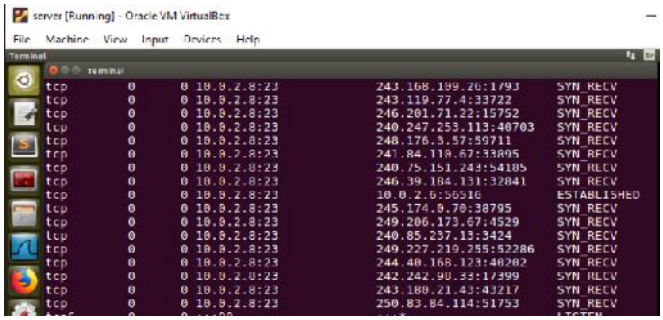

Fig 13. Send multiple SYN packets to the server

Table 1. Types of DoS and DDoS Attack

	Type of attacks	Causes of this type of attack	Example
DoS Attack By using single machine to send many requests	Network Equipment Level	1. Software errors. 2. Draining network hardware resources [17].	Flood ng with any type can be exploited [17].
	OS Level	Take advantage of implement protocols methods in OS [17].	Like TCP protocol [17].
	Network Applications Level	1. By exploiting specific mistakes in network applications. 2. Using applications to know the victim's resources [17].	Exploit any type of protocol can be known from victim resources to cause flooding [17].
	Data Flooding	Send a large number of data those causing process very large amounts of data [17].	Flood ng with any type can be exploited [17].
	Protocol Features-Based Attack	By taking advantage of specific standard protocol features [17].	E.g. using spoofed IP by exploit in severe attacks [17].
DDoS Attack By using many zombies machine to flood the target system	Smurf Floods	It changes the source address to the target system address, so it can respond to a number of pings that flood the network [23]	Flood ng by ICMP ECHO requests with spoofed IP of the victim [23].
	ICMP Floods	The opponent is sending a batch of ICMP ECHO requests to the victim Then victim response these requests that consumes the victim's resources [23, 24].	Flood ng victim side with ICMP ECHO requests [23, 24].
	UDP Floods	Sending a huger number of UDP packets to the victim side [3, 23, 24].	Flood ng victim side with UDP [3, 23, and 24].
	TCP Floods	Similar to UDP flood in implement but different in type of packet [23].	Flood ng victim side with TCP [23].
	TCP SYN Floods	1. Client send SYN 2. Then server reply with SYN / ACK 3. When client receive SYN/ACK. Then client doesn't reply to server with ACK response.(half open connection)[23]	TCP protocol [23].

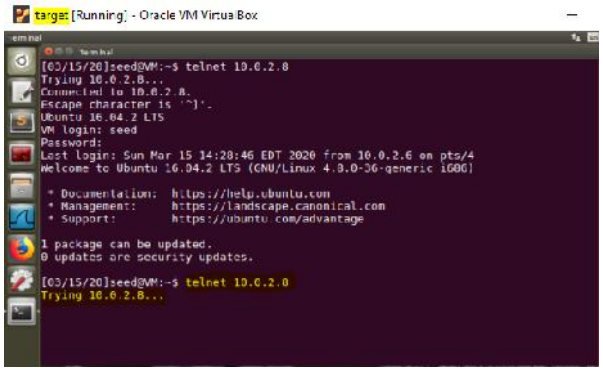

Fig 14. Failed connect to the server

Conclusion

In recent years, there has been no significant change in the Internet. In addition, network resources are still vulnerable to consumption attacks because it need more flexibility. Obviously, DDoS attacks consider as a big problem for each system, where this research described the meaning of flooding in DDoS attack against IP address. In addition, have been present many topics begins with concept of DoS attack and DoS level because DDoS attack follows the same way of DoS but with many devices. Then explains the motivations of the attackers to use different type of Attack. In attack process show to you SYN-flood and flooding concept in a practical way.

REFERENCES

Nagpal, B., *et al*. DDoS tools: Classification, analysis and comparison. in 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom). 2015. IEEE.

Kotenko, I. and A. Ulanov, Agent-based simulation of DDOS attacks and defense mechanisms. International Journal of Computing, 2014. 4(2): p. 113-123.

Criscuolo, P.J., Distributed denial of service: Trin00, tribe flood network, tribe flood network 2000, and stacheldraht ciac-2319. 2000, California Univ Livermore Radiation Lab.

Lau, F., *et al*. Distributed denial of service attacks. in Smc 2000 conference proceedings. 2000 ieee international conference on systems, man and cybernetics.'cybernetics evolving to systems, humans, organizations, and their complex interactions'(cat. no. 0. 2000. IEEE.

Mirkovic, J. and P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 2004. 34(2): p. 39-53.

Ranjan, S., *et al*. DDoS-Resilient Scheduling to Counter Application Layer Attacks Under Imperfect Detection. in INFOCOM. 2006. Citeseer.

Chang, R.K., Defending against flooding-based distributed denial-of-service attacks: a tutorial. IEEE communications magazine, 2002. 40(10): p. 42-51.

Puri, R., Bots & botnet: An overview. SANS Institute, 2003. 3: p. 58.

Center, C.C., Denial of service attacks.http://www.cert.org/tech_tips/denial_of_service. html, 2001.

Liu, J., *et al*., Botnet: classification, attacks, detection, tracing, and preventive measures. EURASIP journal on wireless communications and networking, 2009. 2009(1): p. 692654.

Peng, T., C. Leckie, and K. Ramamohanarao, Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys (CSUR), 2007. 39(1): p. 3-es.

Chandola, V., A. Banerjee, and V. Kumar, Anomaly detection: A survey. ACM computing surveys (CSUR), 2009. 41(3): p. 1-58.

Loukas, G. and G. Öke, Protection against denial of service attacks: A survey. The Computer Journal, 2010. 53(7): p. 1020-1037.

Bhuyan, M.H., D.K. Bhattacharyya, and J.K. Kalita, Surveying port scans and their detection methodologies. The Computer Journal, 2011. 54(10): p. 1565-1581.

Kashyap, H.J. and D. Bhattacharyya. A DDoS attack detection mechanism based on protocol specific traffic features. in Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology. 2012.

Lin, S. and T.-c. Chiueh, A survey on solutions to distributed denial of service attacks. 2006.

Douligeris, C. and A. Mitrokotsa. DDoS attacks and defense mechanisms: a classification. in Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No. 03EX795). 2003. IEEE.

Soliman, M. and M.A. Azer. Web Application API Blind Denial of Service Attacks. in 2018 14th International Computer Engineering Conference (ICENCO). 2018. IEEE.

Douligeris, C. and A. Mitrokotsa, DDoS attacks and defense mechanisms: classification and state-of-the-art. Computer Networks, 2004. 44(5): p. 643-666.

Alomari, E., *et al*., Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art. arXiv preprint arXiv:1208.0403, 2012.

Zargar, S.T., J. Joshi, and D. Tipper, A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE communications surveys & tutorials, 2013. 15(4): p. 2046-2069.

Fultz, N. and J. Grossklags. Blue versus red: Towards a model of distributed security attacks. in International Conference onFinancial Cryptography and Data Security. 2009. Springer.

Poongothai, M. and M. Sathyakala. Simulation and analysis of DDoS attacks. in 2012 International Conference on Emerging Trends in Science, Engineering and Technology (INCOSET). 2012. IEEE.

Specht, S. and R. Lee, Taxonomies of distributed denial of service networks, attacks, tools and countermeasures. CEL2003-03, Princeton University, Princeton, NJ, USA, 2003.

****