A Review of Security Vulnerabilities of Networking Protocol Associated with DoS Attacks

Ankur Kumar Bajaj[1], Dr. Vineet Richhariya[2]

[1]M.Tech Scholar, [2]Professor

Abstract - Numerous attacks builds clog block in path of consistent and innocuous communication. Denial-of-Services (DoS) attacks included in these clogs which usually wants to unavailing the services empowered by any service provider. Availability becomes necessity once consumers utilize metered policy services facilitate by numerous organization. This paper evaluates the evolution of DoS attacks centered to academic models and its realistic consequence. Several patterns of DoS attacks exploits the networking protocols typically to TCP/IP suite through disrupting its fundamental functionality. Vulnerabilities presents in networking protocols continuously embedded by attacker in attacks techniques for survival from being blocked. Resolution to these attacks against protocol weakness done by fusion of various procedures of mitigation.

Keywords - DoS Attack, Security, Vulnerabilities, Network protocols.

1. INTRODUCTION

Today our business are growing progressively for the reason of the consumption of Computer Technologies in our regular work. And technologies are more usable by the facility of Distributed system are inter-connected but working individually to facilitate the services from one end to other. Nowadays these Computer Networks also become a major security issue in the list of our traditional business issue. But, in today's discipline, security issues are commonly seeing in three category: Confidential, Integrity and Availability. In this survey, we are focusing more on the Availability security issue. In term of Availability security issue of IT resources, a crucial task is playing to disrupting the resources by DoS Attacks. DoS Attacks refers as unavailing the resources to legal users by attackers through building congestion in network resources and exhausting the servers. This paper objectives is to introduce the overview of security vulnerabilities related to DoS Attacks in the Private or Internal Network which are subjected to many applications. Denial-of-Service overview is described under Section 2, with defining others thoughts on conducting attacks. Section 3 illustrated all attacks, focusing on SYN flag misuse attack. Section 4 represented TCP/IP Header inspection for identification related to Flags. And next section which is 5, associated effort is shown towards DoS attack and resistances with TCP/IP Header identification for attack, finally concluding with Section 6.

2. DOS OVERVIEW

DoS attacks, in general, to shutdown a server or machine which spreading service to their legal user by mean of legal packet containing illegal data that cause the server itself in busy state or shutdown situation [2][3][4]. DoS attacks are now turn into very complicated threat. Almost every web-servers and great quantity of ISP suffers this fatigueness. These classes of attacks are famous for a long phase, however gained quality with recent events linked with the unidentified hacking activities combined. DoS attack feature is that, for the most scenario, definite arrangement of genuine packet are used to produce a terrific, disrupting effect. As DoS scheme have progressed with years, fewer resources are requisite to accomplish malicious attacks, so in certain situation a solo attacker is sufficient to bring down a complete network, by approach of disparate to preliminary techniques which impose huge networked attack resources compulsory to refuse service to a single target.

3. TYPES OF DOS ATTACKS

DoS Attacks come to be a prospect communally between hackers, they thought through this, they acquired route to celebrity in accumulation to respect in the hidden troop of Internet. DoS attacks fundamentally means repudiating valid internet and system clients from consuming the facilities of the target network or server. [2]It mainly described to initiation an attack that will provisionally create the services reachable by network unfeasible by genuine clients.

Denial of Services attacks are ultimately of three different natures:

- Those that exploit weaknesses founded in TCP/IP format.
- Those that exploit exposures of IPv4 operation.
- There are as well nearly brute force spasms which attempt to consume all resources of the target system and create the facilities impracticable.

Formerly a heading to all attacks type, here we recognize one mechanism that all these are vulnerabilities of the

TCP/IP format. Around collective susceptibilities are Ping-of-Death attack [2], Teardrop Attack [2], SYN Attacks [2] and Land Attacks [3].

But several kind of attacks are popular, so we include all in paper and which are:

A) Ping of Death Attack: In this attacks a ping tool is typically used to influence the target station to collapse, restart or crash. [1]PING is the utility does the ECHO messages of ICMP IP protocol and is regularly used to identify whether the target node is active. [2]Attacker initiate a packet using above tool with setting total length crosses the boundary of protocol, which is 65535 bytes, as prescribed by Fig. 1. Controlling of a giant in size packet disturbs the target's device alongside the nodes which routes this packet. Providentially, around completely all the Network nodes and OS, these generations are not in danger to this attack since they facilitate the neglecting technique to any IP packet containing total length above 65535 bytes.

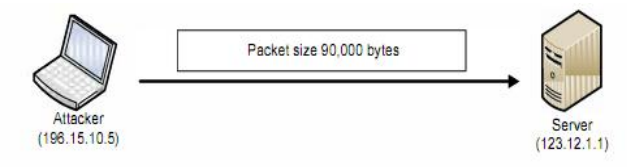

Fig. 1. Ping of Death Attack

B) SYN Flood Attack: To achieve trusty and reliable connection in internet, TCP facilitates tremendous procedure through which virtually direct connection is established. In a classic TCP connection presented by figure 2(a), first a user sends SYN (synchronizing) request to server for forming a connection. Second, after receives the request, the server reply with SYN/ACK (synchronizing/acknowledgment) to user for informing that it accepts the SYN request and wait for his ACK.

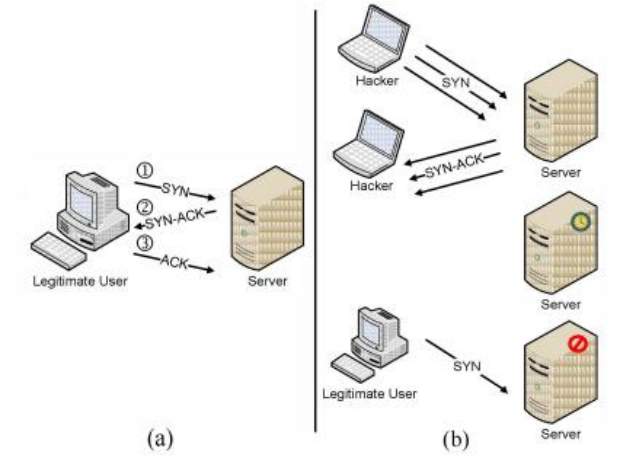

Fig. 2. SYN Flooding Attack

Third, the connection established when user complete the procedure through sending of ACK to server. This mechanism referred as three-way handshaking. To commit attack, attacker initiates a great quantity of synchronizing segments to server for exploits the queue limit of handling the request then SYN flooding attack occurs [2][3][4]. Illustration in Fig. 2(b), when queue of handling requests overflowed then server puts all genuine requests in waiting condition as server unable to process them. Handshaking procedure is essential to build connection but its vulnerabilities also abandoned the global performance.

C) TearDrop Attack: This attack abuses the weakness exists in the re-assembling of data packets. Data before directed through Internet divided into short datagrams (packets). These packets have an Offset field in their TCP header part. This OFFSET value states that particular data packet carries the Original readable data. But, to pursue the attack, a chain of fragmented data being directed towards target machine with intersecting OFFSET field values. Afterwards, the target system doesn't have capability to reconvene the fragmented data and being crash, hang down or restart. Illustrate a scenario, assume we requisite to send data around 5000 bytes among two clients. Relatively, transfer whole information in a solo packet, the information is split into static-size of packets, respectively packet containing a definite array of information like so:

- Packet 1 will carry bytes 1-1400
- Packet 2 will carry bytes 1401-2500
- Packet 3 will carry bytes 2501-4200
- Packet 4 will carry bytes 4201-5000

Normally, this packet are sent in order and Offset field was set to normal arrangement. In teardrop attack packets are send in normal order but setting the Offset wrong like in fig. 3:

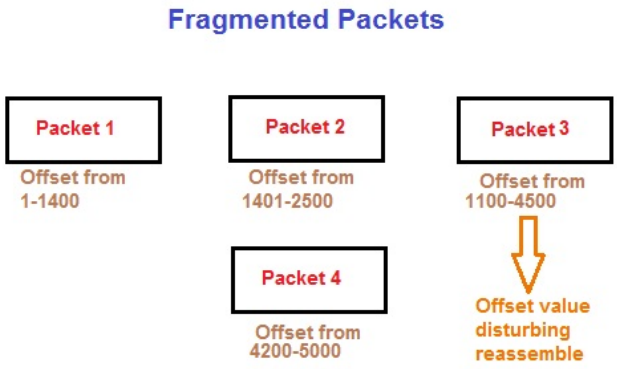

Fig. 3. Teardrop Attack

When the object machine take delivery of this, it merely can't rearrange it and crashed. Recent Network nodes and OS are eligible to handle this attack so further it will not harm us.

D) Smurf Attack: This is belongs to brute-force DoS attack[2], where attacker sends the massive extent of ICMP packets containing only echo request to the target

machine[3][4]. But here the main target machine states to the router of the target machine's network or say the gateway of the network. This attack initiate with ICMP echo packets containing spoofed IP in source IP part by using IP address of victim machine and destination IP as broadcast address (typically denotes to Flood) of the target machine's network range. As fig. 4 illustrated the scenario of this mechanism and shows the gateway or router works in simple manner but help to raising the attack. As router receive the ICMP request and it will flood to the network. After receiving the request from target machine' IP address, all machine will reply to target machine and then machine will flooded. The ultimate terrible situation reaches when great quantity of machine replying the request. This attack is difficult to prevent but mitigates to a great scope by configuring the router to don't direct the IP broadcast address packets.

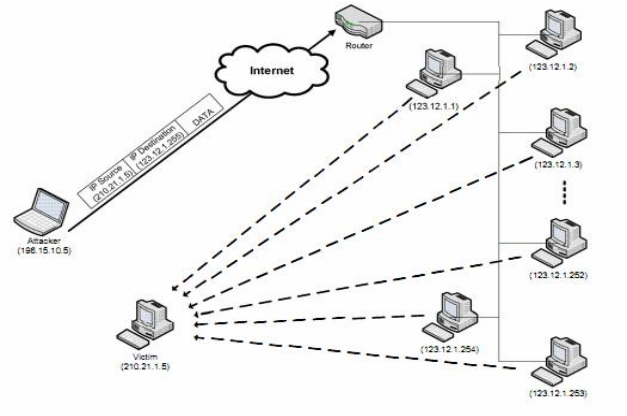

Fig. 4. Smurf Attack

E) Land Attack: This attack is typically related to the SYN attack as it uses SYN flag to implement the attack [2][4]. Unlike, SYN attack uses Random IP as source address in TCP handshaking mechanism, here Target machine IP is used as source and also as destination. Here one thing is remarkable that attacker uses identical port no. as source field and destination field so an unbounded loop created and machine will crash or reboot. Fig. 5 clarified the situation. Alike, smurf attack mitigation, this is also moderate by checking these form of TCP request at networking resources in network.

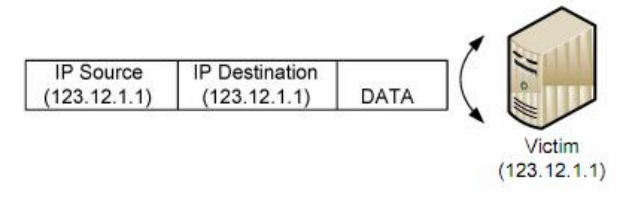

Fig. 5. Land Attack

F) UDP Attack: This is also states as the Fraggle Attack, which usually done in UNIX types OS includes switches and routers [2]. In this mechanism formally 2 ports are prerequisite to implement as port #7 for ECHO and port # 19 for CHARGEN. Referring to RFC864, IP Suite facilitates a service called Character Generator Protocol [5] shortly referred CHARGEN proposed for debugging the situation of machine. To build an unbounded loop the CHARGEN port of secondary target is utilize by attacker to initiate UDP ECHO packet including target's echo service port and spoofed address of target machine. The characters produced by CHARGEN port receives by victim machine at ECHO port indefinitely. So victim machine reply back to secondary target machine at CHARGEN service port which causes a loop, resulting both systems are crashed as picturized in Fig. 6.

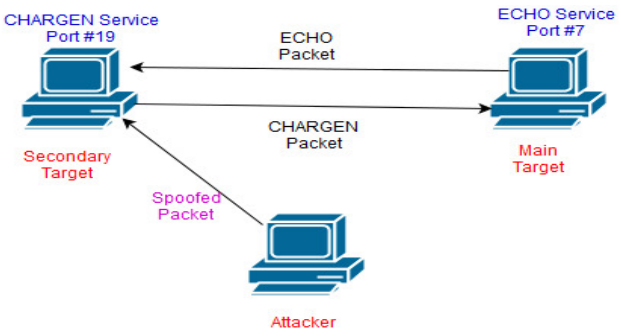

Fig. 6. UDP Flood Attack

G) Distributed DoS Attack: This attack is not the kind of DoS attack, merely the advance scenario of DoS attack. Most of the hackers teasing that DoS attacks are "Accient" attack, as numerous countermeasure were developed [2]. Analogous to DoS, DDoS has potential to unavailing the services of any machine but the impact of arrangement is so excessive than DoS and takes reduced time to execute. In DoS several shortcoming are introduced due to evolution of technology and resources, hackers move to drastic stroke to realize their existence. In DoS, formally hackers prerequisites his system or a spoofed address to execute the entire crucial attack. This states that in DoS, the quantity of system in entire arrangement is in the ratio of 1:1 as attacker and target is one. From the attacker prospective, this ratio might be hopeless as it has great possibility of failure in attack. Misery of failure in attack, announced the Distributed DoS as this procedure prerequisite many systems to implement the attack. In typically DDoS, 3 zones evolved in whole scenario: Attacker, Bots and Target [3], as illustrated in Fig. 7. Attacker, the main person, the one who supposed entire idea. Bots refers to the machines of least protected network which are manipulate by attacker easily. And Target is the machine depending upon its server or individual. The steps of evolution of 3 zones from attacker to target are as below manner:

- First attacker notorious the most vulnerable network, instead to execute the attack directly.

- Second attacker abuses the whole machines of that network and refers them as Bots, the whole network become BOTNET.
- Third mount the DDoS tool on all bots to accomplish the attack.
- Fourth attacker instruct all to execute the attack on target machine.

In case expect the bots in botnet are 500 then the ratio becomes for entire arrangement is 500:1 where attackers are 500 to solo target. Resulting, the attacker list turns into enormous measure which disturbs the target tremendously than the antique DoS attack. This procedure has minor chance of failure as if some system are defeated then vast quantity still exist in encounter. So from attacker's perspective, numerous benefit of executing distributed DoS attack in place of regular DoS are observed which are resulting:

- Detecting personality of organizer is very challenging for target in Distributed DoS. Since there are huge machines are attacking so the target confused and defeated in tracking practice. This indicates that Distributed DoS facilitate to hide attacker.
- Compared to traditional DoS attack it is disturbing, perilous and more rapidly to accomplish.
- Since the mastermind has complete control on BOTS which facilitate him to obliterate entire data regarding attack like logs files, so chief offender never ever spotted by anybody.

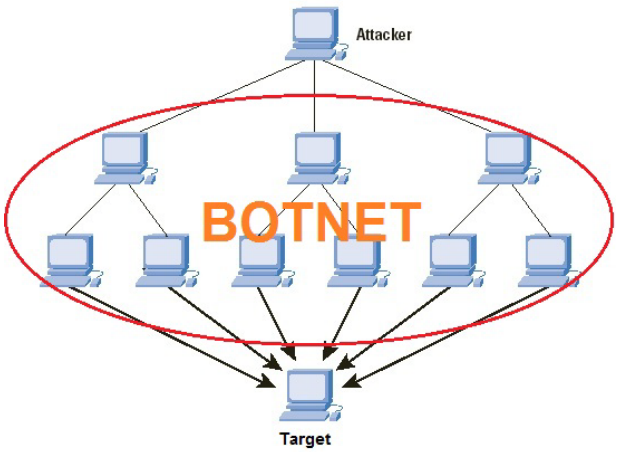

Fig. 7. DDoS Attack

4. TCP/IP HEADER

TCP/IP header feature revealed in Fig. 8, the TCP/IP header built with two header which are TCP and IP header. Here the grouping of two protocol exchange the data over Internet using process to process communications. As TCP protocol is providing that how the applications can connected while from different nodes. Whereas, IP protocol gives facility to route the packet from network to network. So here IP is bounded with TCP to facilitate the reliable and guaranteed service to devices. TCP header enclose many of 1-bit flags but in our study, the Flag bits used in TCP header are vulnerable to great extent. According to Handshaking protocol, two flag bit (SYN and ACK) are used to complete the process for making connection between communication devices. But in the handshaking scenario, one flag bit will turn into a cause of dead point to any server. We analyzed the weaknesses linked with TCP/IP suite in next segment through all attack that we discussed above and also evaluate the mechanism to overwhelm them.

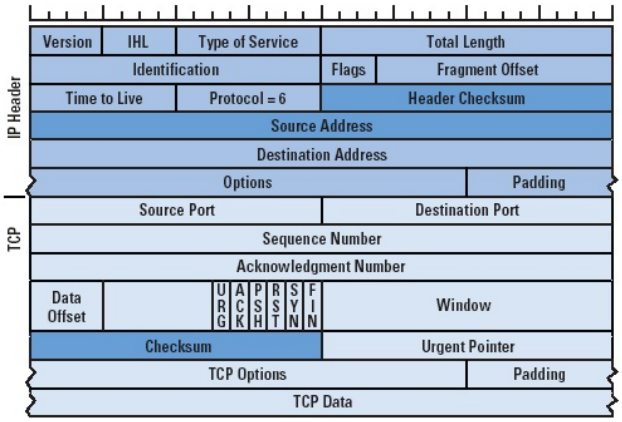

Fig. 8. TCP/IP Header

5. RELATED WORK

Various researchers proposed several mechanism to defend the entire network and servers from DoS and Distributed DoS attacks. These mechanism broadly categorized by landscape of volume and protocol centric attacks [6]. In Volume centered attacks, UDP and ICMP floods attacks plays great role as attacker aims to drench the bandwidth of target's network. In protocol concentrated attacks, Smurf , PoD, Teardrop and SYN Flood attacks contributed major part as attacker wants to use the vulnerabilities associated to network protocols which never be changed. But researcher works to defeat these attacks to a great extent.

Recognize the area of source through IP Traceback [7] and Pushback [8] were used to encounter the attacker which states as source of attack. [8] DoS attack situations must be controlled by the routers as pushback functionality is configured on every single router to classify and specially drop the packets that possibly appropriate to an attack. Pushback term stats that routers should also notified upside routers to deny such traffic.

Limwiwatkul et al. [16] suggested for defense from DoS attack that to monitoring the traffic on the basis of networking protocols such that TCP and IP field value

which contain detailed statistics concerning the attack. But this resulted inefficient and overheaded. Similarly, Mohamed et al. [17] recommended to securing TCP/IP format in contradiction of SYN attack through implemented some configuration on every OS platform to handle huge SYN request which were OSs set to low by default.

Chen et al. [10] suggested a new combined technique worked on core networks which employed by ISPs. Across several network domains, detecting rapid traffic variations proposed distributed (DCD) design used change aggregation trees (CAT) worked in earliest time but overhead of communication made it suffer. Xuan et al. [11] also proposed group testing methodology to detect attacks which implemented at back-end servers but undergo ambiguous at malicious requests.

Francois et al. [9] proposed a new collaborative mechanism "Fire Col" to protect network with detecting the flood attacks. Fire Col acts as IDS implemented at ISP premises which sensed on all movements. The IPSs created effective shield around the hosts to secure and collaborates to exchanged traffic information to stop the attack.

[12] IHoneycol introduced through combination of FireCol and Honeypot mechanism formally used the filtering procedure of blackhole and sinkhole to mitigate Ping related attack. When attacker send vast volume of data, honeypot server recorded that client as black listed then attacker can't authorized to attack. Here FireCol fragmented vast volume of ICMP data and broadcasted to honeypot server, so honeypot disowned that user connections.

To protect from Smurf attack, Zargar et al. [13] proposed PCA based mechanism which performed on training and learning approach. Whereas, Kumar [14] proposed the structure to understand the association amongst original smurf and amplified smurf attack in smurf typed DDoS attack.

Wei [15] introduced scrutiny mechanism to defeat UDP flooding in SDN technology by done minor changes to SDN controller, afterwards using of ARP packets and associated TCP packets.

6. LITERATURE SURVEY

Limwiwatkul et al. [16] suggested very good mechanism as to mitigate DoS attack through monitoring the load based on TCP and IP header values under protocol defined but such methodology produce more effort on the resources and have no dynamically reactions.

Similarly, Mohamed et al. [17] indorsed a way to secure TCP/IP format regarding SYN attack through employing particular alteration on OS configuration for huge SYN request are consumed but this also goes to wrong if the updates will come for that OSs and all previous configuration removed.

Francois et al. [9] methodology named as "Fire Col" was also best at ISP premises employed through IDS for investigating flood based attack but these analysis ultimately goes wrong when prime period of internet usage arrives and it will not reflect dynamic result.

[12] IHoneyCol was introduced as fusion of Fire Col with honeypot mechanism to record all the unwanted behavior through honeypot server and take action similar to FireCol methodology but the behavior of honeypot server lacks under heavy load and also dynamically ineffective.

As above researchers introduced their methodology for controlling or mitigating the DoS based attacks but all of them lacks under dynamicity of mechanism to work immediately when attacks detected and also should take actions.

7. CONCLUSION

Today network security applied as the most recommended compliances in establishment of network. Services like web, mail, file and several are available through service providers are presently affected by DoS attack to an abundant scope. Security and access are two aspects of scales states that defensible and consistent communication happen only by perfect configuration prerequisite in certain situation. This paper evaluated different scenario of attacks with associated mechanisms to overwhelm them. But evolution of attacks appears with equal proportion as its defense mechanism developed. Finally, we concluded that to overwhelm these attacks only through fusion of related mechanisms, so the attacks defeats at certain level. TCP/IP suite possesses several layers and assorted regulation to control attacks as entire thing starts from it, so it has power to end.

REFERENCES

[1] Ping (networking utility)," https://en.wikipedia.org/wiki/Ping_ (networking_utility). [Online; Accessed: 28-Apr-2018].

[2] A. Fadia, The unofficial guide to ethical hacking. Boston (Mass.): Thomson Course Technology, 2006.

[3] W. Ali, J. Sang, H. Naeem, R. Naeem, and A. Raza, "Wireshark window authentication based packet captureing scheme to pervent DDoS related security issues in cloud network nodes," 2015 6th IEEE ICSESS, 2015.

[4] M. Darwish, A. Ouda, and L. F. Capretz, "Cloud-based DDoS attacks and defenses," in International Conference (i-Society 2013), 2013.

[5] "Character Generator Protocol," https://en.wikipedia.org/wiki/ Character_Generator_Protocol. [Online; Accessed: 29-Apr-2018].

[6] "Denial of Service Attack Definition," https://www.incapsula.com/ ddos/ddos-attacks/. [Online; Accessed: 01-May-2018].

[7] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, “Practical network support for IP traceback,” ACM SIGCOMM Computer Communication Review, vol. 30, no. 4, pp. 295–306, Jan. 2000.

[8] J. Ioannidis and S. M. Bellovin, “Implementing Pushback: Router-Based Defense against DDoS Attacks,” in NDSS Symposium 2002.

[9] J. Francois, I. Aib, and R. Boutaba, “FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks,” IEEE/ACM Transactions on Networking, vol. 20, no. 6, pp. 1828–1841, 2012.

[10] Y. Chen, K. Hwang, and W.-S. Ku, “Collaborative Detection of DDoS Attacks over Multiple Network Domains,” IEEE Transactions on Parallel and Distributed Systems, vol. 18, no. 12, pp. 1649–1662, 2007

[11] Y. Xuan, I. Shin, M. T. Thai, and T. Znati, “Detecting Application Denial-of-Service Attacks: A Group-Testing-Based Approach,” IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 8, pp. 1203–1216, 2010.

[12] M. Buvaneswari and T. Subha, “IHoneycol: A distributed collaborative approach for mitigation of DDoS attack,” 2013-ICICES, 2013.

[13] G. R. Zargar and P. Kabiri, “Identification of effective network features to detect Smurf attacks,” 2009 IEEE (SCOReD), 2009.

[14] S. Kumar, “Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet,” Second (ICIMP), 2007.

[15] H.-C. Wei, Y.-H. Tung, and C.-M. Yu, “Counteracting UDP flooding attacks in SDN,” 2016 IEEE NetSoft Conference and Workshops (NetSoft), 2016.

[16] L. Limwiwatkul and A. Rungsawang, “Distributed denial of service detection using TCP/IP header and traffic measurement analysis,” IEEE ISCIT, 2004.

[17] A. B. Mohamed and A. Kandil, “Strengthening and securing the TCP/IP stack against SYN attacks,” Proceedings of the ITI 2009 31st International Conference, 2009.