RESEARCH INVESTIGATIONS ON DDOS ATTACK

[1] Dr.A.Thomas Paul Roy, Dr.N.Dhanalakshmi[2], Dr.D.Suresh [3]

[1] Professor, PSNA College of Engineering and Technology, Dindigul, India
[2] Professor, PSNA College of Engineering and Technology, Dindigul, India
[3] Professor, PSNA College of Engineering and Technology, Dindigul, India
pauli.dgl@gmail.com

Abstract — The DDoS attack is the most well-known network security attack for network and internet improvement. This paper mentions the DDoS Attack Precept and analyzes some methods of DDoS Attack. Applied sciences consisting of network visitor detection and packet content detection are presented in the DoS attack detection. It adds DDoS, which is mainly based on DoS, and describes certain DDoS tools and discusses the vital TCP flood DoS assault concept. The DoS Attack software and the DoS Assault Detection software are primarily scanned based on Winpcap and the community package and take-over technology are implemented. The test showed the key development of DoS attack and element detection.

Keywords- Network security; Denial of Service; Detection and Detection Software.

I. INTRODUCTION

With fast improvements of network tools and application, network security is becoming increasingly more serious. The DoS attack is the famous strategies of intrusion, with regular financial losses and consequences. Studies on the precept and detection of DoS attacks have become very essential and the science of DoS must now be up-to-date because of the progressive improvement of the hackers' assault equipment and science. There is no absolute network protection environment and the network attack coexist. The DoS development has many motives. The vulnerability of the software and software gadget is posted and rogue software is often used on the internet. Software and system are often ruined by the pc virus and Trojan. It can lead to the DoS attack being launched. Since some attacks can make money using the DoS, they become the tool to make money. The DoS attack is subject to many strategies. In this paper we present the DoS attack standard and certain attack techniques and design and application of attack and detection software.

Copyright © Author

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

II. ATTACK PRINCIPLE

The DoS [1] is described as a result of the hacker taking on some special assault strategies to harm the device and the community, and to also take on the laptop property such as CPU, ram, buffer and community bandwidth, the ordinary person cannot get the carrier. The DoS attack has many effects. Perhaps the device is very slow and the person might not be able to join the community server. The normal development of DoS assaults involves certain interrelated steps. The attacker first of all sends a wide range of carrier applications with false addresses. The server transmits a response message to the transmitter and waits for the client's responses. Due to the forged addresses, the server cannot get facts and have to wait a long time and the connection with overtime will be reduced. You cannot release the useful resource assigned to this request. If the request is very large, the useful resource of the server will be used. SO the new consumer cannot get the provider and the attack is positively carried out. Service denial [2] is now a risky Internet intrusion. The packet measurement can be labeled as two groups according to the assault. One is to use a wide variety of meaningless packages in the useful resource of the sufferer, which can be called resource ingestion. It is the main type and can make the person affected by the disease in a very short time exhaustive. The other way is to make the patient not be able to grant the software provider the vulnerability to the victim, which has been named the most DoS. In recent years, even a single packet has emerged as an essential phase of DoS as the key function of smaller packet flows. What we need to do is try our best to protect the severe cyber attack. This machine presents a whole security mechanism for DDoS attacks to achieve the highest level of safety.

The attack can also paralyze the firewall and the network target routes and lead to the congestion of the community. The packet sent to the target host may be ordinary or unusual facts about the community that can collapse the target machine. There are numerous practical do-strategies like SYN Flood, ICMP Flood, Smurf and the method of assault on the Utility Layer. Due to the 3 TCP protocol palms, the target host will devour TCP connection resources when the attacker makes an error IP tackle packet using a SYN note. Any other SYN Flood approach sends a long-byte packet of SYN. The assault may misplace certain firewalls. In addition, the TCP packet can make the gadget error with disordered flags such as SYN+RST. Because UDP protocol does not have drift handling and error control, it lets the attacker run the risk of making

Copyright © Author
SSN (Print): 2204-0595
ISSN (Online): 2203-1731

a very good UDP packet version to the server and the consumer cannot receive the service. ICMP is used for displaying the country of community and is commonly used to notify the host about a larger route to reach the holiday destination and to identify packet course problems and disasters in the community. ICMP can also cause the attack because it is often used to file Community failures. The Ping command for example can be upgraded to attacks from Flood. The ICMP that is redirected and unattainable during the vacation can also be used to create floods due to the fact that the message is useful and the attacker ships with false regular users the protocol or port to create an unaccessible ICMP packet. The DNS is used to unwind the IP tackle area heading and is a database system that has been dispensed. DNS includes forward mapping and reverse mapping that could lead to error and be used by the attacker. Some other DoS attack is a multiple connection to the web server. The net server cannot process the request because there is a lot of connections to the server at the same time. The attacker sometimes sends a unique GET request that pays a large amount of CPU database time or internet sites.

The DDoS [2] is primarily based on the DoS and is the best-known DoS assault technology because it can easily and quickly have greater severe consequences. The structure of DDoS is separated into three layers: the attacker layer, the major controller host and the host host layer. All hosts that send the assault code to the dealer host are controlled. The controller host is also available to any host in the web. The dealer host may take the actual attack from the controller host and receive the command. The attacker cannot be determined without any problems because the attack develops and the attacker data are hidden. There are many facilities for DoS attacks and they can be utilized with the help of someone who may have knowledge of litter PC. Trinoo[4] is a DoS assault device that uses the UDP inundation to cause the DoS disbursed. In three phases, the present EHIDS[5] will operate. Authentication & authorisation, verification of signature and integrity records. Each node is assigned with a special identification and special identification is used throughout communication, road discovery and transmission.

III. DETECTION

The machine administer ought to locate the DoS assault initial in order to defend the community aid for the everyday users. Detection approach for the DoS assault is vital and many researchers furnished some applied sciences to scan the community country and make measures

Copyright © Author
SSN (Print): 2204-0595
ISSN (Online): 2203-1731

to forestall DoS attack. When a massive range of statistics packets show up unexpectedly and the community visitors grows quickly, the server run with overload and the overall presentation reduced, these may additionally be symptoms of the attack. If the packet content material is now not steady with the ordinary provider connection and response via checking the content material of packet, it may also be the height of community carrier and the overall performance and ability of the server need to be improved[9-10].

If the TCP facts or UDP date comprise first-rate range of contents which size is greater than the regular average, the assault perhaps show up and must analyze these packets carefully. When some packets are no longer the section of community provider connections and the vacation spot port is no longer the regular carrier port, the server perhaps intruded by means of the attacker. To discover the machine vulnerabilities early and installation the device patches well timed is quintessential to keep away from the DoS attack. On the different hand, the necessary data need to backup and the password of the privileges account need to be blanketed carefully. These measurements may also limit the probability of DoS attack. The gadget bodily surroundings have to regularly be checked and the needless community provider ought to be no longer open. The network safety log have to be checked each and every day and discover the odd information. The community protection units such as firewall have to be configured to filter the feasible falsification community packets.

IV. EXPERIMENTAL ANALYSIS

The DoS attack uses a protocol defect regularly to generate a large number of packets to the target machine. The TCP/IP is used for the Internet and with the help of the intruder, TCP's defect can be used. The fundamental instance is the SYN flood attack using the three TCP connection handshakes. If a significant range of SYN packets is dispatched to the target host, the target host generates additional buffers to establish the sender. When the connection is not complete by sending one hand packet, it measures greater CPU time and ram sources. Building upon three handshakes [6], the TCP is using the response packet to ensure the sender is legitimate. The buyer send the SYN flag packet to the server and it enters the country of SYN SEND and awaits the server response. The server receives packets from the consumer and

Copyright © Author
SSN (Print): 2204-0595
ISSN (Online): 2203-1731

transmits the ACK and SYN flag packets and the server enters SYN RECV and waits for the client's response.

The patron will finally send the server an ACK flag packet and send it to the server that the buyer receive the packet. This enables you to connect the client to the server and to change the date. The consumer and the server enter the state of ESTABLISHED. The SYN Flood [7] uses three handshake mechanisms to send a huge amount of the SYN flag packet and the IP address to provide failure.

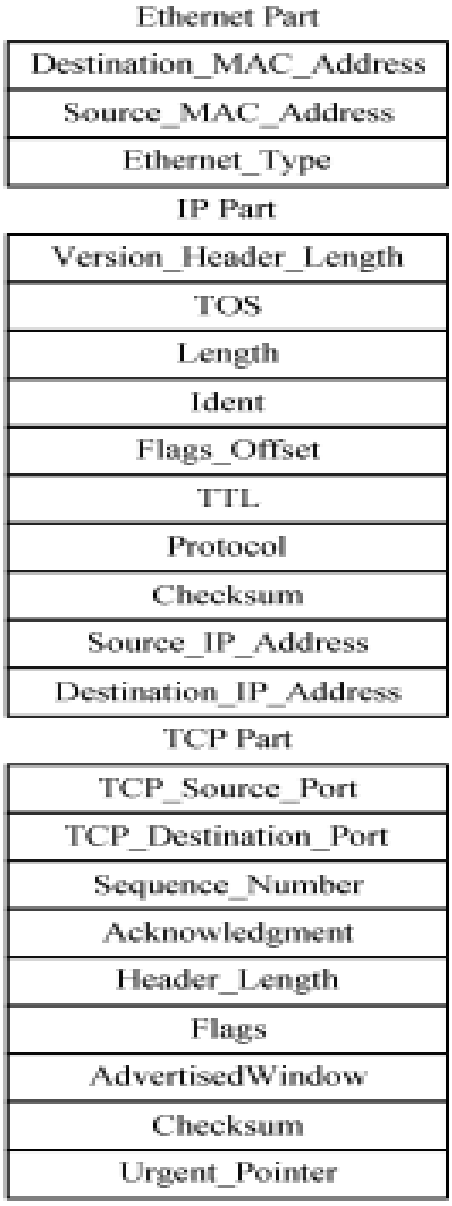

Figure 1. The TCP SYN packet structure

Copyright © Author
SSN (Print): 2204-0595
ISSN (Online): 2203-1731

```
memset(&ethernet,0,sizeof(Ethernet));
BYTE mac1[8]={0};
memcpy(ethernet.Destination_MAC_Address,mac1,6);
BYTE mac2[8]={0};
memcpy(ethernet.Source_MAC_Address,mac2,6);
ethernet.Ethernet_Type=htons(0x0800);
memcpy(&TCP_SYN_Packet,&ethernet,sizeof(struct
Ethernet_Part));
ip.Version_Header_Length = 0x45;
ip.TOS = 0;
ip.Length = htons(size of(struct IP_Part)
+size of(struct TCP_Part)
+strlen(TCP_Protocol_Payload));
ip.Ident = htons(1);
ip.Flags_Offset = 0;
ip.TTL = 128;
ip.Protocol = 6;
ip.Checksum = 0;
ip.Source_IP_Address =inet_addr("192.168.26.28");
ip.Destination_IP_Address=
inet_addr("192.168.17.12");
memcpy(&TCP_SYN_Packet[size of(struct
Ethernet_Part)],&ip,20);
tcp.TCP_Destination_Port = htons(21);
208  208tcp.TCP_Source_Port = htons(3421);
tcp.Sequence_Number = htonl(678);
tcp.Acknowledgment = 0;
tcp.Header_Length = 0x50;
tcp.Flags = 0x02;
tcp.AdvertisedWindow = htons(512);
tcp.Urgent_Pointer = 0;
tcp.Checksum = 0;
memcpy(&TCP_SYN_Packet
[size of(struct Ethernet_Part)+20],&tcp,20);
```

The packet is the first packet to progress with the three handshakes. The server receives the SYN packet and assigns the ram to the queue. When the server receives large packets in fast time, the semi-connection is overflowed and removed via the running gadget and the connection becomes

Copyright © Author
SSN (Print): 2204-0595
ISSN (Online): 2203-1731

invalid. If the packet size of the SYN is more than the maximum of the SYN semiconnection, the SYN packet will be requested from everyday consumers by the SYN packet. The cost of each semi-connection is a small and limited memory of the kernel. The SYN Flood core code is set out below. As shown in figure 1, the structure of the SYN packet.

Three parts of the SYN packet are: Ethernet, IP and TCP. The packet is handmade and can be adjusted arbitrarily with exceptional parameter fields. The WinPcap [8] is used to send the SYN packet, which is a useful way to flexibly seize and ship the community package. First, Ethernet records the decrease layer protocol, and then the IP layer information, the TCP segment, is produced. The picap sendpacket feature, which is the key feature of sending the community packet in the Winpcap element, will then use the protocol packet that contains a certain kind of facts that include the SYN flag. The core software code above is the way for the DoS-attack to be sent by one packet and a huge variety of such packets. It can be achieved using multi-threading and dispensed system software. In Winpcap it is necessary to build the packet content material by using the byte array that shops the protocol headers and loads the data exclusively. The key characteristic of the ship is the pcap send packet with three parameters: the handle for the Winpcap, the packet material pointer and the size of the packet. All facts are positioned with the pointer, and the start and end can be calculated by the size.

The SYN Flood application's core code is as follows. The Winpcap uses the packet filter instructions to seize single packets for the exceptional package. You can access the Community machine listing on your laptop using the pcap findalldevs. The consumer can use the right interface to seize the packet. Open the machine and set the key associated parameters by pcap open live. The filter policies are managed using the pcap compile and pcap setfilter characteristics. The packet is captured using the pcap loop feature and the person can analyze packet contents in the callback described in the feature.

Copyright © Author
SSN (Print): 2204-0595
ISSN (Online): 2203-1731

```
tatic int SYN_Packet_Number=-1;
static int SYN_Flood_Warning_Number=0;
IP_Part *ip;
ip =(IP_Part *)(packetdata
+sizeof(Ethernet_Part));
int IP_Header_Length = sizeof(unsigned long)*
(ip ->Version_Header_Length &0x0f);
if (ip ->Protocol == IPPROTO_TCP)
{TCP_Part *pTcpHeader;
  pTcpHeader = (TCP_Part*)(packetdata
+sizeof(Ethernet_Part)
+ IP_Header_Length);
if((pTcpHeader->Flags&0x02))
SYN_Packet_Number++;}
QueryPerformanceFrequency(&Frequency);
if(SYN_Packet_Number==0)
{QueryPerformanceCounter(&SYN_Start);}
if(SYN_Packet_Number==300)
{QueryPerformanceCounter(&SYN_End);
 double End_Start = SYN_End.QuadPart
- SYN_Start.QuadPart;
  double SYN_Interval=End_Start *1000.0 /
(double)Frequency.QuadPart;
 printf("SYN_Interval Time:%f  ms\n",
 SYN_Interval);
  if(SYN_Interval<=1000.0
&& SYN_Interval>0.0)
  {SYN_Flood_Warning_Number++;
  print("%d: Maybe SYN Flood Attack.\n",
  SYN_Flood_Warning_Number);}
  SYN_Packet_Number=0;
  if(SYN_Packet_Number==0)
  {QueryPerformanceCounter(&SYN_Start);}}
```

This method of detecting SYN Flood DoS attacks can cause the SYN Flood if the overall interval of 300 SYN packets is less than a second. Some detection outcomes are as follows for the SYN Flood DoS attack.

Copyright © Author

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

```
SYN_Interval Time:732.922760  ms
1: Maybe SYN Flood Attack.
SYN_Interval Time:730.184144  ms
2: Maybe SYN Flood Attack.
SYN_Interval Time:747.814038  ms
3: Maybe SYN Flood Attack.
SYN_Interval Time:730.332766  ms
4: Maybe SYN Flood Attack.
SYN_Interval Time:747.531041  ms
5: Maybe SYN Flood Attack.
SYN_Interval Time:729.798061  ms
6: Maybe SYN Flood Attack.
SYN_Interval Time:749.962914  ms
7: Maybe SYN Flood Attack.
SYN_Interval Time:731.543814  ms
8: Maybe SYN Flood Attack.
SYN_Interval Time:743.023205  ms
9: Maybe SYN Flood Attack.
```

The SYN Packet shows the seize packet range. The result of the test is an interval of approximately 725 to 750 milliseconds of all 300 packets. The detection software runs first and maintains monitoring and analysis of the contents of the incoming packet over the entire community. Run the DOS assault program and in a couple of minutes it ships many packets. The detection software can notice the attack and deliver the correct results.

V. CONCLUSION

The DDoS attack uses the scheme, protocol, and server vulnerabilities to interfere with the objective and will lead to the server failing to make the carrier easier for regular users. The DDoS attack can reduce the overall performance of gadgets and ingest the bandwidth of the

Copyright © Author
SSN (Print): 2204-0595
ISSN (Online): 2203-1731

community. This paper discusses, analyzes and adds DDoS mechanism into the element and presents some detection-applied science for the DDoS attack. The DDoS assault application is designed with the aid of the WinPcap toolkit and DoS detection is also applied.

REFERENCES

[1]. S. Ramesh, C. Yaashuwanth, K. Prathibanandhi, Adam Raja Basha, T. Jayasankar, "An optimized deep neural network based DoS attack detection in wireless video sensor network", *Journal of Ambient Intelligence and Humanized Computing (2020),* https://doi.org/10.1007/s12652-020-02763-9

[2]. Thomas Paul Roy, "DAD: A Secured Routing Protocol for Detecting and Preventing Denial-of-Service in Wireless Networks", Wireless Personal Communications, ISSN 0929-6212, Sep 2015

[3]. Bennett Todd ,"Distributed Denial of Service Attacks", http://www.linuxsecurity.com/resource_files/intrusion_detection/ddos-whitepaper.html, 18 February 2000

[4]. David Dittrich, "The DoS Project's 'trinoo' distributed denial of service attack tool", http://packetstormsecurity.org/distributed/trinoo.analysis.txt, October 21, 1999

[5]. R.ArunPrakash, W. R. Salem Jeyaseelan, T.Jayasankar, "Detection, Prevention and Mitigation of Wormhole Attack in Wireless Ad Hoc Network by Coordinator", Appl. Math. Inf. Sci. Vol.12, No.1, Jan 2018, pp.233–237.
DOI: http://dx.doi.org/10.18576/amis/120123

[6]. W Richard Stevens. TCP/IP Illustrated, Volume l : The Protocols. Addison Wesley, 1994

[7]. CERT, TCP SYN Flooding and IP Spoofing Attacks, http://www.cert.org/advisories/CA-1996-21.html, November 29, 2000

[8]. The WinPcap Team ,The WinPcap manual and tutorial for WinPcap 4.0.2,

[9]. G.Mani, V.Nivedhitha, N.S.Pradeep, T.Jayasankar and K.Vinothkumar , *"Reliable Wormhole Detection System (RWDS) Based Secure Routing and Authentication for Environmental Monitoring",* Journal of Green Engineering (JGE), Vol.10, No.3, pp.734-749,March 2020

[10]. *R. Kiruba Buri* and T. Jayasankar**,** *"Intelligence Intrusion Detection Using PSO with Decision Tree Algorithm for Adhoc Network"*, Bioscience Biotechnology Research Communications, Special Issue Recent Trends in Computing and Communication Technology**,** Vol. 12, No.2, March (2019),pp.27-34.

Copyright © Author

SSN (Print): 2204-0595
ISSN (Online): 2203-1731