2009 Third International Symposium on Intelligent Information Technology Application

Research on DoS Attack and Detection Programming

Wentao Liu
Department of Computer and Information Engineering,
Wuhan Polytechnic University
Wuhan Hubei Province 430023, China
idssoap@gmail.com

Abstract—**The DoS attack is the most popular attack in the network security with the development of network and internet. In this paper, the DoS attack principle is discussed and some DoS attack methods are deeply analyzed. The DoS attack detection technologies which include network traffic detection and packet content detection are presented. The DDoS based on DoS is introduced and some DDoS tools are described and the important TCP flood DoS attack theory is discussed. The DoS attack program and a DoS attack detection program based on Winpcap for experiment are designed and the network packet generation and capture are implemented. The experiment expressed the key progress of DoS attack and detection in detail.**

Keywords- Denial of Service; network security; detection

I. Introduction

The network security becomes more and more serious with the rapid development of network technology and application. The DoS attack is one of the most popular intrusion methods which often make great economic losses and impact. The study on DoS attack principle and detection method become very imperative and the new technology for DoS must be updated because the attack tools and technology of the hackers are enhanced gradually. The network attack and network security coexist and there is no absolute network security environment. There are many reasons for the DoS development. The vulnerability for the system software and application program is published and the rogue software often occurs in the internet. The computer virus and Trojan often destroy program and system. They can lead to the emergence of the DoS attack. Because some attacks can use the DoS to make money, it becomes the tool of making money. There are many methods to implement the DoS attack. In this paper, the DoS attack principle and some attack methods are introduced and the program for attack and detection are designed and implemented.

II. Attack Principle

The DoS [1] is defined that the normal user can’t get the service because the hacker seized the service using some different attack methods which can destroy the system and network and it also can occupy the computer resources such as CPU, ram, buffer, and network bandwidth. There are many results due to the DoS attack. The system maybe very slow and the user maybe cannot connect the network server. The typical DoS attack progress contains some steps which are interrelated. First of all, an attacker sends a large number of service requests with false address. The server sends a response message back to the sender and waits for response information from the client. Because the addresses are forged, the server can't get any information and must wait for a long time and the connection will be cut with overtime. The resource allocated for this request cannot be released. If the request number is very large, the server resource will be used up finally. SO the new user can’t get the service and the attack is produced successfully.

The attack also can make firewall and routes of the target network be paralyzed and lead to the network congestion. The packet sent to the target host may be normal or abnormal network data which can make the target system collapsed. There are many concrete DoS attack methods such as SYN Flood, UDP Flood, ICMP Flood, Smurf attack and application layer attack method. Because of the three hands of TCP protocol, when the attacker makes false IP address packet with SYN note, the target host will consume the TCP connection resources. There is another SYN Flood method which sends the SYN packet with long bytes.

The attack can make some firewall lost function. The TCP packet with disordered flags such as SYN+RST can also make the system error. Because UDP protocol has no flow control and error checking mechanism, it let the attacker have chance to make the great number of UDP packet to the server and the user can’t get the service. ICMP protocol is used to monitor the state of network and usually used to notify the host of a better route to reach the destination and report problems of the packet path and detect network failures occur. Because ICMP is often used to report network failures, it also can produce the attack. For example, The Ping command can be evolved to the Flood attacks. The redirected and destination unreachable ICMP also can be used to create Flood because the message is easy to counterfeit and the attacker send the protocol or port unreachable ICMP packet to the target with false normal user. DNS is used to resolve the domain name to the IP address and it is a distributed database system.

DNS contains the forward mapping style and reverse mapping which can lead to error and used by the attacker. Using multi-connection with Web server is another DoS attack. Because there are amount of connects with the server at the same time, the web server cannot process the request. Sometimes the attacker sends special GET request which

978-0-7695-3859-4/09 $26.00 © 2009 IEEE
DOI 10.1109/IITA.2009.165

cost a large number of CPU time of database or some web pages.

The DDoS (Distributed DoS) [2] based on the DoS becomes the most popular method of DoS attack because it can lead more serious effects easily and quickly. The DDoS architecture is divided into three layers: attacker layer, main controller host layer and broker host layer. The attacker controls all the hosts which send the attack code to the broker host. The controller host may be any one host in the internet and its number is very large.

The broker host can make the real attack through receiving the command from the controller host. The attacker cannot be found readily because the progress of attack contains more steps and the information of attacker is hided. There are many tools to make DoS attack and they can be used by some person who maybe has litter computer knowledge. Trinoo [3] is a DoS attack tool which uses the UDP flood to produce the distributed denial of service. The TFN (Tribe Flood Network) [4] use the ICMP, SYN Flood, UDP flood and Smurf attacks to create the DDoS attack and it contains the client and daemon. The TFN client send the command to the daemon and the attacker control the client by use of many different connection technologies.

III. Detection

The system administer should find the DoS attack early in order to protect the network resource for the normal users. Detection method for the DoS attack is important and many researchers provided some technologies to scan the network state and make measures to prevent DoS attack. When a large number of data packets appear suddenly and the network traffic grows rapidly, the server run with overload and the performance decreased, these may be signs of the attack. If the packet content is not consistent with the normal service connection and response through checking the content of packet, it may be the peak of network service and the performance and capacity of the server should be improved.

If the TCP data or UDP date contain great number of contents which length is more than the usual average, the attack maybe appear and should analyze these packets carefully. When some packets are not the part of network service connections and the destination port is not the normal service port, the server maybe intruded by the attacker. To find the system vulnerabilities early and install the system patches timely is necessary to avoid the DoS attack.

On the other hand, the important information should backup and the password of the privileges account should be protected carefully. These measurements may decrease the opportunity of DoS attack. The system physical environment should often be checked and the unnecessary network service should be not open. The network security log should be checked every day and find the abnormal information. The network security devices such as firewall should be configured to filter the possible falsification network packets.

IV. Programming experiment

The DoS attack often uses the protocol flaw to produce a large number of packets to the target machine. The TCP/IP is used for the Internet and the defect of TCP can be used by the intruder. The classic example is the SYN Flood attack which uses the three handshake of TCP connection. When great number of SYN packet is sent to the target host, target host produce more buffer to make establishment with the sender. It cost more CPU time and ram resources when it make incomplete connection through sending one hand packet. Because the TCP use the response packet to make sure that the sender is legitimate, it uses the three handshake mechanism [5]. The client sends a packet with SYN flag to the server and it come into the SYN_SEND state and wait the response of the server. The server receives the packets from the client and it sends the packet with ACK flag and SYN flag and the server enters the SYN_RECV state and waits for the response of the client.

Finally, the client sends a packet with ACK flag to the server and express that the client receives the packet from the server. So the connection between the client and the server is established and the date can be transformed. The client and server come into the ESTABLISHED state. The SYN Flood [6] use the mechanism of three handshake to send great number of packet with SYN flag and failure source IP address. The packet is the first packet of the three handshake progress. The server receives the SYN packet and allocate ram and put it the queue of semi-connection.

If the server receives more packets within a short time, the semi-connection will be overflow and it will be discarded by the operating system and the connection becomes invalid. When the SYN packet number exceeds the maxim of the semi-connection, the normal user send the SYN packet to request the service and it will be discarded by the server. The every semi-connection will cost the kernel memory which is scarce resource and limited. The core code of SYN Flood program is as follows. The structure of the SYN packet is as shown in Figure 1.

```
    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(sizeof(struct IP_Part)
    +sizeof(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[sizeof(struct
Ethernet_Part)],&ip,20);
    tcp.TCP_Destination_Port = htons(21);
tcp.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
[sizeof(struct Ethernet_Part)+20],&tcp,20);
Pseudo_TCP_Part.Source_IP_Address =
        ip.Source_IP_Address;
Pseudo_TCP_Part.Destination_IP_Address =
        ip.Destination_IP_Address;
Pseudo_TCP_Part.Zero = 0;
Pseudo_TCP_Part.Protcol = 6;
Pseudo_TCP_Part.TCP_Length = htons
(sizeof(struct TCP_Part)+
strlen(TCP_Protocol_Payload));
char Buffer_For_Checksum[65535];
memcpy(Buffer_For_Checksum,
&Pseudo_TCP_Part,
sizeof(struct PsdTCP_Part));
memcpy(Buffer_For_Checksum
+ sizeof(struct PsdTCP_Part),
 &tcp, sizeof(struct TCP_Part));
memcpy(Buffer_For_Checksum
+sizeof(struct PsdTCP_Part)
+sizeof(struct TCP_Part),
TCP_Protocol_Payload,
strlen(TCP_Protocol_Payload));
tcp.Checksum = checksum((USHORT*)
(Buffer_For_Checksum),
sizeof(struct PsdTCP_Part)
+ sizeof(struct TCP_Part)
+strlen(TCP_Protocol_Payload));
memcpy(TCP_SYN_Packet
+sizeof(struct Ethernet_Part)
+sizeof(struct IP_Part),
&tcp, sizeof(struct TCP_Part));
memcpy(TCP_SYN_Packet
+sizeof(struct Ethernet_Part)
+sizeof(struct IP_Part)
+sizeof(struct TCP_Part),
TCP_Protocol_Payload,
strlen(TCP_Protocol_Payload));
memset(Buffer_For_Checksum,0,
sizeof(Buffer_For_Checksum));
memcpy(Buffer_For_Checksum, &ip,
 sizeof(struct IP_Part));
ip.Checksum = checksum((USHORT*)
(Buffer_For_Checksum), sizeof(struct IP_Part));
memcpy(TCP_SYN_Packet+sizeof
(struct Ethernet_Part),&ip, sizeof(struct IP_Part));
Result=pcap_sendpacket(Winpcap_Handle,
TCP_SYN_Packet,sizeof(struct Ethernet_Part)
+sizeof(struct IP_Part)+sizeof(struct TCP_Part)
+strlen(TCP_Protocol_Payload));
```

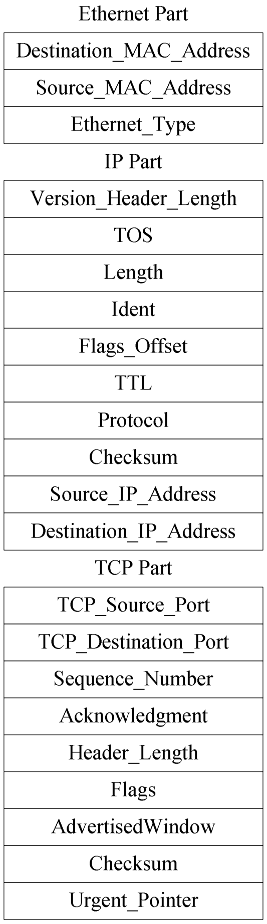

Figure 1. The structure of the TCP SYN packet

The SYN packet contains three parts: Ethernet, IP and TCP. The packet is created with different parameter fields by hand and it can be adjusted arbitrarily. The SYN packet is sent by use of WinPcap [7] which is a useful tool to capture and send the network packet flexibly with more functions. Firstly, the lower layer protocol data Ethernet is made and the next is IP layer data, TCP segment. Then, the protocol packet with the special data which contain the SYN flag is made using the function pcap_sendpacket which is the key function of sending the network packet in the Winpcap component. The above core program code is the process of one packet and a large number of such packets must be sent in order to produce the DoS attack. It can be got by use of multithread program and distributed system. In Winpcap, the packet content must be constructed by manual using the byte array which stores the every head of protocol and the payload of the special data. The key send function is the pcap_sendpacket and it includes three parameters: Winpcap handle, the packet content pointer and the length of sending packet. The all information is located by the pointer and the length can calculate the beginning and the end.

The core code of SYN Flood detection program is as follows. In order to get the special packet, the Winpcap use the packet filter rules to capture the specific packets. It use the pcap_findalldevs to get the network device list in the computer and the user can get the correct interface to capture the packet. Open the device is to use the pcap_open_live and set the key related parameters. The filter rules are operated by the function pcap_compile and pcap_setfilter. The packet is captured by the function pcap_loop and the user can analyze the packet content in the callback defined in the function.

```
static 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++;
  printf("%d: Maybe SYN Flood Attack.\n",
  SYN_Flood_Warning_Number);}
  SYN_Packet_Number=0;
  if(SYN_Packet_Number==0)
  {QueryPerformanceCounter(&SYN_Start);}}
```

In this SYN Flood DoS attack detection method, the SYN Flood may be occurs if the total interval time of 300 SYN packets is less than one second. Some results of detection for SYN Flood DoS attack are as follows.

```
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_Number expresses the number of capture packet. In the experiment result, the interval time of each 300 packets is about between 725 and 750 milliseconds. The detection program run firstly and it keep watch over the whole network and analyze the content of the incoming packet. Then run the DOS attack program and it send many packets in a few minutes. The detection program can detect the attack and provide the correct results.

V. CONCLUSION

The DoS attack makes use of the vulnerabilities of system, protocol and server to intrude the target and lead to the result that the server cannot provide the service for the normal users. The DoS attack can decrease the performance of system and consume the network bandwidth. In this paper, some concrete DoS attack methods are analyzed and the mechanism of DoS is introduced in detail and some detection technologies for the DoS attack are presented. The program of DoS attack is designed by use of the WinPcap toolkit and the program of DoS detection is also implemented. In the program, the processes of sending packet and analyzing packet are illustrated and it shows the implementation mechanism of DoS attack and detection method.

REFERENCES

[1] CERT, Denial of Service Attacks, http://www.cert.org/tech_tips/denial_of_service.html, June 4, 2001

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

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

[4] David Dittrich, The "Tribe Flood Network" distributed denial of service attack tool, http://staff.washington.edu/dittrich/misc/tfn.analysis.txt, October 21, 1999

[5] W Richard Stevens. TCP/IP Illustrated, Volume 1 : The Protocols . Addison Wesley, 1994

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

[7] The WinPcap Team ,The WinPcap manual and tutorial for WinPcap 4.0.2, http://www.winpcap.org/docs/docs_40_2/html/main.html