ISSN: 1813-4890

TCP protocol security and vulnerability analysis:A case study

Hai Tong [1, a], Guangqun Zhou[2, b] and Shihua Liu[3, 4, c, *]

1Ningbo branch of China Telecom Co., LTD, Ningbo 315000, China;

2China United Network Communications Group Co., LTD. Ningbo branch 315000, China;

3School of Artificial Intelligence, Wenzhou Polytechnic, Wenzhou 325000, China.

4Wenzhou Network Security Detection and Protection Engineering Technology Research Center, Wenzhou 325000, China.

[a]15306661027@189.cn, [b]zhouguangqun@chinaunicom.cn,
[c]Chaoshua@foxmail.com(corresponding author).

Abstract

TCP/IP protocol is the de facto industry standard of Internet, but security is not considered in the protocol. This paper mainly analyzes the working principle and security vulnerabilities of the triple handshake of the transport layer TCP protocol, and uses the network simulator to realize the attack process of TCP SYN Flooding, and uses the wireshark packet capture tool to capture and analyze the packets in the attack process to understand the working principle of the attack deeply. Finally, the corresponding preventive measures are put forward. It is an economical and applicable good method to analyze the vulnerabilities of network protocols by means of example analysis, which can realize the research of network security at a low cost and propose methods to solve security problems.

Keywords

TCP/IP protocol, three-way handshake protocol, SYN flooding attack, protocol analysis, security prevention.

1. Introduction

The third wave of the information revolution is slowly changing the way societies, businesses and individuals live. This information revolution is not only the hot topic of the Internet of things, in order to enable the Internet of things to achieve global secure interconnection and secure communication with others, which involves many network protocols. Transport layer is one of the key layers in the whole network architecture, which is mainly responsible for providing services for the communication between processes in two hosts. Transport layer is the core of the whole protocol hierarchy, which is located between the network layer and the application, providing transparent data transmission between the end users, and providing reliable data transmission services to the upper layer, as shown in the figure. Network layer is the highest layer of communication subnet, but it can not guarantee the reliability of connection-oriented services provided by communication subnet or router. Transport layer above the network layer can solve this problem and improve the transmission quality. Is the only layer responsible for overall data transmission and control. In the seven-layer OSI model, transport layer is the highest layer responsible for data communication, and it is the middle layer between the lower three layers oriented to network communication and the upper three layers oriented to information processing. Because the network layer does not guarantee the reliability of the service, and the user does not control the communication subnet directly, a transport layer is added on top of the network layer to improve the transmission quality.

ISSN: 1813-4890

The transport layer protocol includes TCP protocol and UDP protocol, which TCP(Transmission Control protocol) is a connection-oriented protocol[1], refers to the establishment of a connection between the two sides of the communication before the communication, such as the end of data transmission, the two sides then disconnect the connection. TCP is a connection-oriented, reliable process-to-process communication protocol. TCP provides full-duplex service, which means data can be transferred in both directions at the same time, and each TCP has a send cache and a receive cache to temporarily store data. UDP (User Datagram Protocol) is a connectionless network protocol. It means that the two sides of communication do not need to establish a communication line first, but send each packet with a destination address to the network line, and the system selects the route for transmission. UDP protocol is a connectionless and unreliable transport protocol. The sender does not care whether the sent data arrives at the target host, whether the data is wrong, etc. The receiving host does not tell the sender whether it has received the data, and its reliability is guaranteed by the upper protocol. Data transfer is faster and more efficient.

This paper focuses on the transport layer research, by telling the transport layer in the network architecture to play a role. Around the principle and reappearance of TCP protocol vulnerabilities, this paper describes TCP protocol vulnerabilities, introduces SYN flooding attacks, and starts to use kali virtual machine and ensp to set up experimental environment on the basis of understanding the principle. Commands are used to attack other virtual machines on kali virtual machine, and waireshark is used to capture and analyze packets. The experimental results are obtained. Through the way of example analysis, the working principle of the attack was deeply understood, and finally the corresponding preventive measures were put forward.

2. TCP three-way Handshake Protocol and SYN Flooding Attack

2.1. TCP Protocol

TCP protocol is a reliable, connection-oriented transport protocol, it provides connection-oriented reliable transport services, supports a variety of network applications, can be used in a variety of reliable or unreliable networks. Connection-oriented means that two applications using TCP must establish a TCP connection before they can exchange data with each other. Therefore, TCP is mainly designed to achieve reliable packet exchange transmission between hosts.

The TCP header format is shown in Figure 1.

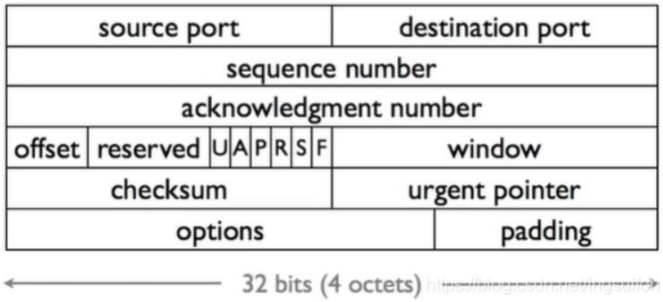

Fig. 1 The TCP header format.

TCP protocol provides connection-oriented and highly reliable communication services. Before TCP can be used for communication, the two communicating parties need to establish a TCP connection, and TCP uses SYN(Synchronization segment) packets to describe the messages used in the three-way handshake to create a connection [2].

2.2. TCP three-way Handshake Protocol

As shown in Figure2, the process of TCP three-way Handshake Protocol is as follow:

ISSN: 1813-4890

First handshake: When the connection is established, the client sends a request packet SYN(SEQ= k) to the server. The client enters the Syn-send state and waits for the server to acknowledge the request flag syn=1.

Second handshake: when the server receives the request packet, it must acknowledge the client's request packet (ACK= k+ 1). At the same time, the server also sends a reply packet (SEQ=q), i.e., SYN+ ACK packet.

Third handshake: The client receives the SYN+ ACK packet from the server, and sends an acknowledgment packet ACK(SEQ= q+ 1) to the server. After sending the packet, both the client and the server enter the ESTABLISHED state, thus completing the TCP three-way handshake.

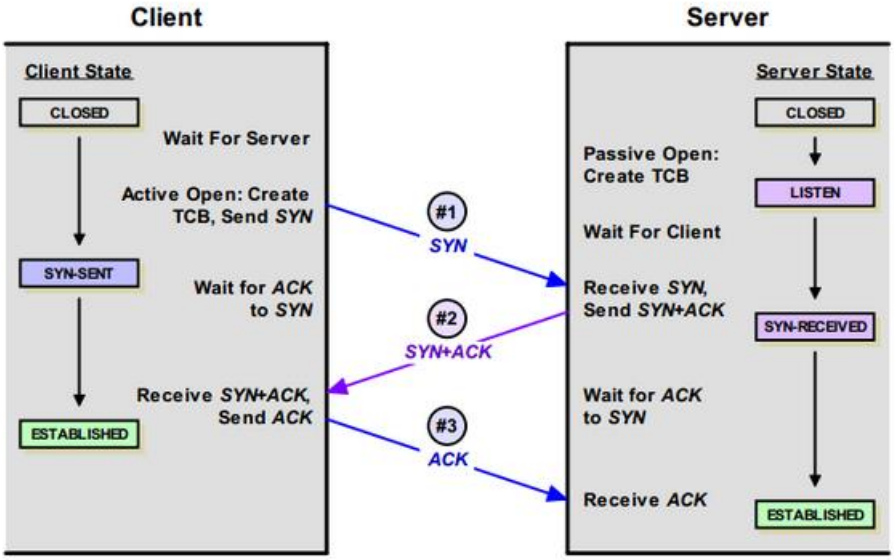

Fig. 2 TCP three-way Handshake Protocol.

The three-way handshake to create a TCP connection requires both the client and the server to generate a random 32-bit initial sequence number. If an application tries to establish a new TCP connection after the computer is restarted,TCP must choose a new random number to ensure that the new connection is not affected by the original connection.

2.3. DoS Attacks in TCP

Since TCP protocol is a connection-oriented transmission control protocol, the main purpose of DoS attacks is to make the user host or network unable to receive or process external requests. For example, by creating a large amount of useless data, resulting in network congestion, so that the host can not communicate with the outside world; It used the repeated connection defect to send repeated service requests repeatedly, so that it could not handle other requests normally. Or use protocol defects, repeatedly send attack data, occupy host or system resources, cause crash and so on.

In simple terms, Denial of Service (DoS) attacks usually use packets to flood the local system in order to disturb or seriously prevent services that are willing to help the local system from responding to legitimate requests from outside, causing the local system to crash. SYN flood attack is the most common type of DoS attack.

The attacker disguises his IP address and sends TCP connection request to the local system. The local system replies SYN-ACK to the masquerading address, so that the local system cannot receive RST message and ACK response, and will remain in the semi-connected state until the resource is exhausted.

Attackers send connection requests faster than TCP timeouts to release resources, and use repeated connection requests to make the local service unable to accept other connections.

ISSN: 1813-4890

3. A Case Study of SYN Flooding

Preparation work: Experimental tool ensp, kali virtual machine, experimental topology construction Figure 3 TCP flooding experimental topology.

The kali virtual machine was connected to the cloud to attack the server. Router AR1 was used as the client and AR2 was used as the server, and they were connected by a switch.

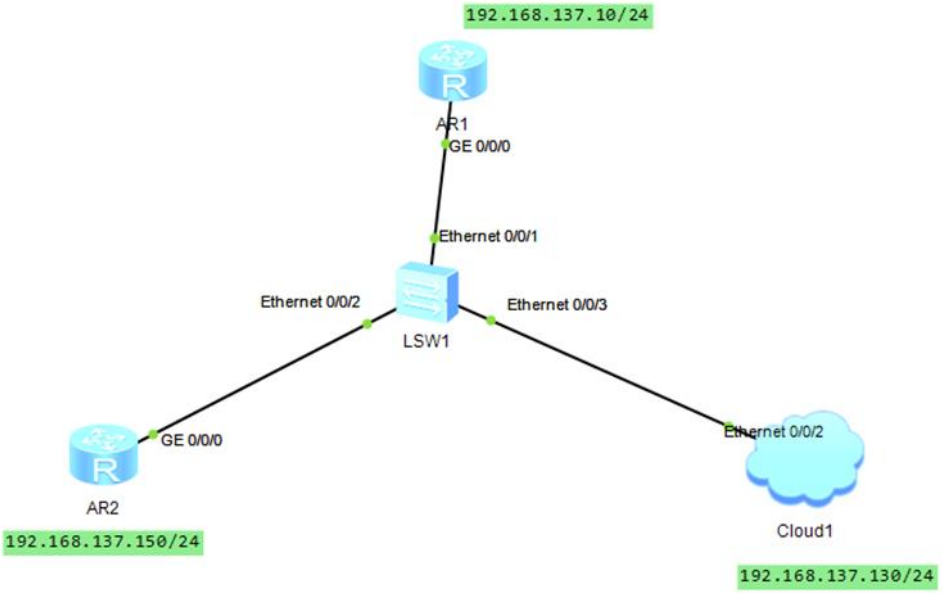

Fig. 3 Topology of the TCP flooding experiment.

3.1. Configuration of Kali VM

(1) After the ip configuration of the two routers in the topology graph is completed, open VMware to enable kali and modify kali's network to "host only mode" :

Locate the kali virtual machine, right click and click Settings;

Set to host only mode in the network adapter.

(2) In the command line, enter vi /etc/network/interfaces to enter the network configuration file, press i to modify the network IP address, and add it to the end of the file.

auto eth0 # auto *means boot the network card device*

iface eth0 inet static *# Use static addresses*

address 192.168.1.2/24 # Static IP address/subnet mask

gateway 192.168.1.1 # Gateway address

Once the modification is complete, enter systemctl restart networking to reset the network card information and use the ifconfig/ip addr command to view the network segment of kali network.

```
kali@kali:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 10
00
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group defau
lt qlen 1000
    link/ether 00:0c:29:d1:0c:68 brd ff:ff:ff:ff:ff:ff
    inet 192.168.137.130/24 brd 192.168.137.255 scope global dynamic noprefixroute eth0
       valid_lft 973sec preferred_lft 973sec
    inet6 fe80::20c:29ff:fed1:c68/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Fig. 4 IP Address of Kali VM.

ISSN: 1813-4890

3.2. Configuration of Cloud Module

Open the cloud device configuration interface, the network card selects the network card connected to the kali virtual machine for the first time, and directly click Add. The second time, select UDP, and also directly click Add. The port mapping is set as the inbound port number is 1, and the outbound port number is 2. As shown in Figure 5.

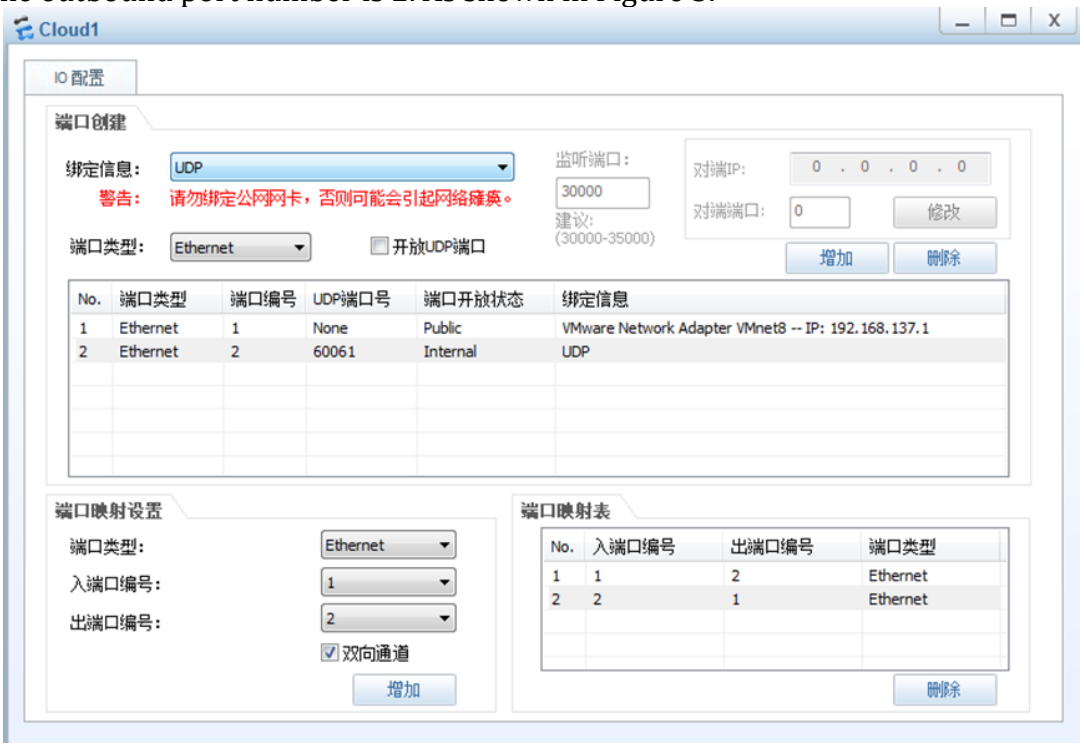

Fig. 5 Configuration of Cloud.

3.3. TCP SYN Flooding and Analysis

Enter the command hping3 -S --flood -p 23 192.168.137.150 in the kali virtual machine to carry out the attack, as shown in Figure 6 TCP attack. -S: This means that the TCP SYN field is set to 1 and -p is the destination port.

```
kali@kali:~$ sudo hping3 -S --flood -p 23 192.168.137.150
```

Fig. 6 Attack Command.

At the same time, ensp is opened and packets are captured on the g0/0/1 interface of the switch, and it is found that R2 receives a large number of SYN packets, as shown in Figure 7 TCP packet capture.

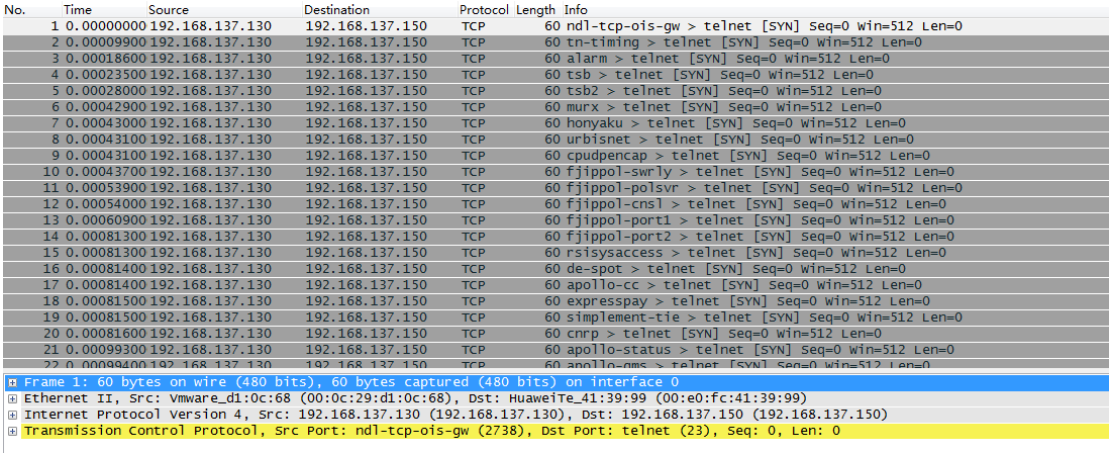

Fig. 7 Attack Command.

ISSN: 1813-4890

When you open the R2 command box, you can't do anything with the R1 device.The kali virtual machine stops the attack and opens R2 to input display anti-attack statistics tcp-syn to view the statistics of the flooding attack, as shown in Figure 8 flooding attack.

```
[R2]display anti-attack statistics tcp-syn
Packets Statistic Information:
-------------------------------------------------------------------------------
AntiAtkType  TotalPacketNum        DropPacketNum         PassPacketNum
             (H)        (L)        (H)        (L)        (H)        (L)
-------------------------------------------------------------------------------
Tcp-syn       0          22415      0          18105      0          4310
-------------------------------------------------------------------------------
```

Fig. 8 Attack Result.

It can be found from the figure that there are a total of 22415 attack packets, the number of dropped packets is 18105, and the number of passed packets is 4310.

So far, the attack has been completed. Due to the DDOS attack, the system resources and bandwidth have been occupied in large quantities, resulting in the inability to provide normal network services, resulting in denial of service.

3.4. Prevention of TCP SYN Flooding Attacks

The best way to solve SYN flood is to do a good job of prevention strategy, through network performance management tools, automatic screening of suspicious data packets, shorten the SYN Timeout time, set SYN Cookie, set Cookie for each request, if a certain IP received repeated SYN packets in a short period of time, Consider it an attack and discard the IP address.

Taking the above instance reproduction environment as an example, it can be configured accordingly in devices such as routers.

(1) Configure R2 to prevent TCP SYN flood attacks

[R2]anti-attack tcp-syn enable Note: There will be an error if it is enabled, and no error if it is not

[R2]anti-attack TCP-SYN car cir 8000 Limits the rate at which TCP SYN packets can be received Note: By default, TCP SYN packets are received at a rate of 155000000bit/s. Here the acceptance rate is modified to 8000.

```
[R2]anti
[R2]anti-attack tcp
[R2]anti-attack tcp-syn en
[R2]anti-attack tcp-syn enable
Error: Anti-attack tcp-syn has been enabled.
[R2]anti-
[R2]anti-attack tcp
[R2]anti-attack tcp-syn car cir 8000
```

Fig. 9 R2 Protection Configuration.

(2)See the statistics of fragmented packet attacks

To see our configuration command in action, let's first clear R2's packet attack data:

[R1]reset anti-attack statistics tcp-syn (Reset Anti-attack statistics)

Using kali to attack R2 again, we can see the attack data:

[R1]display anti-attack statistics tcp-syn

ISSN: 1813-4890

```
[R2]reset anti
[R2]reset anti-attack statistics tcp-syn
[R2]dis
[R2]display anti
[R2]display anti-attack stat
[R2]display anti-attack statistics tcp-
[R2]display anti-attack statistics tcp-syn
Packets Statistic Information:
------------------------------------------------------------------------------
AntiAtkType  TotalPacketNum        DropPacketNum         PassPacketNum
             (H)        (L)        (H)        (L)        (H)        (L)
------------------------------------------------------------------------------
Tcp-syn       0          3706       0          3014       0          692
------------------------------------------------------------------------------
```

Fig. 10 the Result of R2 Protection

At this time, we can see that the total attacked packets are 3706, the dropped packets are 3014, and the passed packets are 692, which proves that the TCP SYN FLOOD attack is successfully prevented.

4. Conclusion

This paper analyzes the transport layer protocol from the perspective of theoretical knowledge, this paper takes the transport layer vulnerability as an example (such as TCPFlood), analyzes the transport layer TCP protocol, and takes the vulnerability implementation as the research center, and carries out research. The purpose of this research is to understand the vulnerabilities of TCP protocol, know its prevention methods, and the application mechanism of TCP protocol in the transmission of data, and effectively improve people's understanding of the transport layer. This paper uses the vulnerability reproduction experiment to analyze the problem of transport layer protocol vulnerability rationally, which is conducive to the in-depth expansion of transport layer protocol vulnerability research. Through the analysis of typical cases, the advantages and disadvantages of transport layer protocol are pointed out and the machine causes are analyzed, so that people can better understand and grasp the theory in specific scenes.

Acknowledgements

This research was supported by Wenzhou Network Security Detection and Protection Engineering Technology Research Center.

References

[1] Xu Shuang, Su Yu. Network Protocol Analysis [M]. China Water Resources and Hydropower Press,2016.9.

[2] LI Chao, Analysis of Transport Layer Protocol in TCP_IP Architecture [J]. Information Communication,2008, 4th Issue, 30-32.

[3] LI Long, Research and application of attack and defense technology based on TCP_IP protocol vulnerability [J]. Northeast: Northeastern University, 2013-05-01, Master Degree

[4] Huang Yi-wang, WAN Liang, LI Xiang, SYN flooding attack based on IP spoofing [J]. Computer Technology and Development,2008, 12 (159-161,165).

[5] Tang Huan-rong, ZenG Yi-jing, SYN flooding attack detection based on semi-connected list [J]. Computer Engineering, 19,2011, 135-137,144.

[6] Zhang Huanming, Song Zhenfeng. Analysis of SSH protocol. Journal of Jinan University, 2003.6

[7] Chen Peng, Fu Fengnian. Security Analysis of TCP/IP Protocol. Electronic Science and Technology, 2005, No.7.

ISSN: 1813-4890

[8] LIANG L. Comparison of TCP/IP transport layer protocols. Journal of Chengdu Teachers College, 2003.12.

[9] LI Chao. Analysis of Transport Layer Protocol in TCP/IP architecture. Information and Communication, No.4, 2008, 30-03.

[10] ZHAO Y. Analysis of TCP and UDP protocols. Journal of Anshun University, 2008.8.