Research on flag-based network scanning technology

Guofang Zhang

Hainan College of software Technology, Qionghai, China

Keywords: encapsulation; network security; network vulnerability;

Abstract: In order to realize data transmission on the network, data needs to be encapsulated layer by layer. In the process of encapsulated data, different kinds of control information need to be added. This control information are necessary to realize network communication. Flag identity bits in data packets are the key part of establishing and closing communication session connections, and also the key to controlling the data transmission process. At the same time, flag identity bits become the vulnerabilities exploited by infiltrators. This paper studies the characteristic of data package encapsulation and the role of flag tag bit in the process of network connection and data transmission. Combining with the characteristics of network penetration, it puts forward the conclusion that flag tag bit has potential security risks, and points out a new direction for network security protection in this paper.

1. Introduction

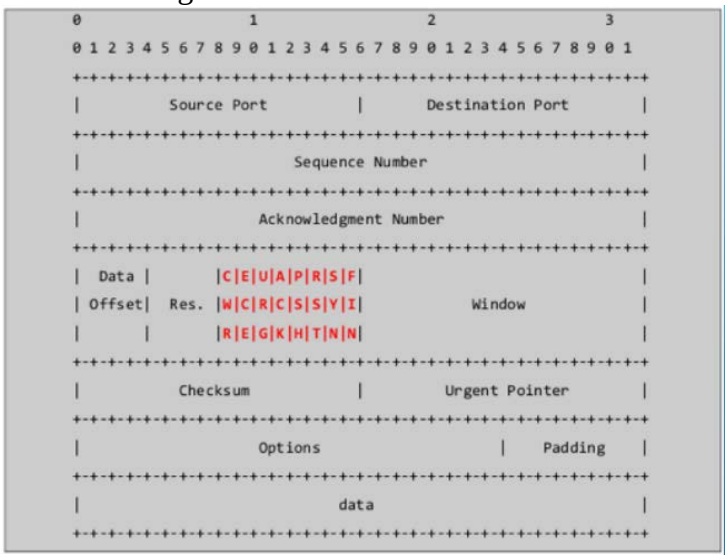
The popularity of the internet has penetrated into all walks of life and touched the depth of people's lives. It can be said that today's society is a cyberspace society, and all people's actions are based on internet communication. Various data of network communication shuttle through the whole network space. These data include tex, voice, picture, video and shared location information. Regardless of the form in which the information is displayed on the internet, they are transmitted on the internet in a common digital package format. This format has different encapsulation formats in different network layers. The data of these different network layers complies. The data of these different network layers complies with the requirements of each network layer, and the layers are independent and interconnected to realize data transmission. These data are of interest to people, at the same time they are of interest to network hackers. Hackers use various means to obtain user data is a network infiltration behavior. The data leakage incident caused by the internet penetration of the global internet has increased exponentially, and the losses caused to users are irreparable. If you want to prevent such an event, you must know how the network data is sniffed, and how the host in the network is infiltrated by the hacker. This paper analyzes the encapsulation format of network packet itself find out the vulnerabilities that can be used for network host discovery and network penetration, and proposes how to prevent this threat.

2. Packaging characteristics and differences of network data

The internet uses the TCP/IP model as a framework to divide the network into application layer,transport layer,network layer and date link layer from top to bottom. The order of data encapsulation in the internet is encapsulated sequentially from the application layer to the data link layer, and the layers are independent of each other. The transport layer data is encapsulated with information such as protocol port number, segment offset,sequence number,flag value,checksum and emergency pointer. The transport layer encapsulated data is called a data segment, and the main transport protocols are TCP, UDP, and ICMP. The data is encapsulated with header information from the transport layer to the network layer, including source IP address, destination IP address, IP protocol version,head length,TTL value,service type,protocol and other information. From the network layer to the data link layer, the IP packet is encapsulated with the header information, including the source MAC address, the destination MAC address,and a check value is added at the end of the data frame. The characteristics of network data encapsulation are low-level encapsulation

  DOI: 10.25236/isrme.2019.076

high-level, and data is more and more convenient for network device identification from the upper layer to the lower layer. The port number encapsulated in the transport layer is an identifier of the computer service type that can be identified by the service process inside the computer. IP packets at the network layers are identified and forwarded by routers working at the network layer, and data frames at the data link layer are identified and forwarded by switchers which are operating at the data link layer. The advantage of the method of encapsulating data from the top layer to the bottom layer of the network is that the division of labor is clear, and it is convenient for each layer to implement independent functions. The layers are independent of each other. they are a black box relationship each other. The common feature of each layer of packaged data is that the header information of each layer is encapsulated, and the header information filled with data. The difference in the package data of each layer is that the data added to the header is different, and the amount of added data information is different. The transport layer adds two ports numbers to the header, including source port and target port, service types, fill bits, flag tags, etc.t.each data port occupies 2 bytes, a total of 32 bits, port number is the identification of application service process and the interface between application layer and network layer. Transport layer packet header encapsulation format as shown in figure 1.



The network layer adds two IP addresses to the header, including source IP address and destination IP address, TTL value, encapsulated high-level protocol, flag value, segment offset, check value, fill bits, etc. Each IP address occupies 4 bytes, a total of 64 bits. The link layer adds two MAC address to the header, including source and target MAC addresses, data frame checksum, LLC, control bits and other information. Each MAC address takes up 6 bytes, a totla of 48 bits. In addition, other information added by each layer is different secondly, the role of information added at each level is different. The check value of data link layer is to veritfy the data frame at the destination. The segment offset and flag value of network layer are the measures to recover data after the data reaches the target node in the network layer. The port number of transmission layer is the interface between network layer and application layer, and the flag value is the communication mechanism between the two sides. TTL value and TOS are used to route data packets between communication nodes and provide quality of service in the network layer. In a word, data encapsulation in each layer serves the communication between communication nodes.

3. The role of flag in packet and its reverse utilization

Flag is encapsulated in the header information of TCP-type data packets in the transport layer, which takes up one byte and total eight bits. From low to high, the order is fin, syn, rst, psh, ack, urg, ECE and CMR, which are not yet used. Tcp is a connection-oriented protocol. At the beginning of communication, both sides of communication transmit syn location “1” to the target, the other flag identification bits are “y” packets. After receiving the target, the syn location “1” and ack location “1” is returned to the initiator, and the other identification bits are “0” response packet, after

receiving the target response packet, the initiator sends the answer packet which ACK location "y+1" to the target, and other flags identification locations "0" to the initiator. This is the famous handshakes. When the connection is established between the two sides, data transmission can be carried out between the two sides. During the established of three handshakes, when the target first receives the data packet from the sender requesting synchronous connection, the target often allocates some resource to establish connection with the sender, including the new process, memory space, port number created, and sends the reply package to the sender. DOS attack is to attack the target by using the characteristic of three handshakes to establish connections. Firstly, attacker use tools to forge a large number of false source IP address requests for synchronization of packets, in a short period of time at a massive speed to send to the target host. The target host cannot recognize that the IP addresses of these request packets are forged. The target host allocates memory resources, including process, port number and other physical resource, to these connection request packets according to normal connection requests. Because the source IP address of these requests are false, the response signals sent by the target host can never be answered, and the resources allocated by the target host can not be released and recycled in a certain response time, which is wasted in vain. Because the physical resources are limited, and the attacking host sends a large number of requests to the target host in a short time, the physical resources will be quickly exhausted because of the response to these requests, which results in the subsequent normal connection requests will not be responded. DOS attacks can also be used to penetrate other networks by identifying flag values when TCP is used to establish connections. When a network host finds a scan attack, the attacker sends a broadcast packet of syn location "1" in the flag tag. The host online in the scanned network will respond to such a packet and respond differently according to the different configuration of the host.

(1) when the host sends reply packages with syn and ACK packages, the attacker's host does not send replay packages anymore, but it has been determined that the host is online and the IP of the host is displayed.

(2) When the host sends the replay packages of RST and ACK placement, it tell the attacker that the host can judge that the host is online based on this information, but it is not allowed to establish a connection.

(3) When the host sends the PSH and ACK bits, the attacker's host identifies the data contained in the response package and accepts the data.

An attacker can scan the port of the target host using flag to find out which ports the target host has opened. According to the open port number, the attacker can analyze the type of service opened by the target host and further judge the operating system running by the target host. The attacker uses the attack tool to send the target host a constantly changing detection packet of the destination port, and then judges the open state of the port of the target host according to the response package received from the target.

(1) When flag is marked as ACK and SYN at the same time in the response report of the target host, it indicates that the target host opens the corresponding port, and the port number opened by the target host will be displayed on the attacker's host. According to the port's number, the service function opened by the target host can be judged and the operating system running by the target host can be judged further. On the basis of obtaining the operating system running on the target host, we search which vulnerabilities have appeared in the operating system. According to the vulnerabilities, we use tools to penetrate the target host to achieve the purpose of penetrating the target host.

(2) When flag tag "ack" is not positioned or RST is positioned in the response message of the target host, it means that the target host has not opened the corresponding port, but it does not necessarily meant that the target host has closed the corresponding port. In the actual network environment, for the sake of security, most enterprise networks have deployed firewalls. Firewall are usually configured to restrict external request connections and only open 53 port, 80 port and 443 port to provide services to the network. These ports are used to provide network services to the network. These ports are used to provide network services to the network and allow eternal connection requests. In this case, an attacker may consider initiating connection requests to these

ports, penetrating through web pages after connecting to the target host, or letting the target host initiate requests to connect to the attacker's host on its own initiative. Because the firewall does not restrict the active connection request from the target host to the outside, it can realize the connection between the attacker host and the target host, and achieve the goal of bypassing the firewall to penetrate the target host.

4. Flag markup vulnerabilities

In order to validate the flag tagging function, this paper uses network penetration tools to penetrate the selected target machine, which is a certain vulnerability of the CentOS 6.5 system and Windows 2003 system. The penetration tool used is also the key to the experiment. According to the type of operating system, the commonly used tools for network penetration based on flag value can be divided into two categories, tools based on Windows platform and tools based on Linux platform. Because Windows platform is not open source, a large part of all kinds of penetration tools based on different versions of Windows are platform-dependent and can not be used across platforms, which brings restrictions to use. Kali Linux is an open source attack platform with more than 600 penetration tools. It is secure and sTable and widely used. In this paper, NMAP and NC are used as scanning tools to penetrate target aircraft, Wireshark and TCPDUMP are used to capture data packets, and the flag values of data packets are decomposed and analyzed. Based on the analysis of the data packets sent and received and the comparison with the results obtained by using the tool, it is proved that flag tag bit is the vulnerability used for network penetration.

5. Conclusion

This paper studies the characteristic of data package encapsulation and the role of flag tag bit in the process of network connection and data transmission. As an important parameter of network communication, FLAG flag bit is the key to establish TCP session connection and carries the status information of TCP session connection establishment. Like the two sides of a coin, on the one hand, normal network communication can use it to establish session connections, on the other hand, it can also become a vulnerability in the network. Using flag flag information, network penetrators can develop various tools for network attacks, which also provides a research direction for network security defense. Network security maintainers can intercept intruders who exploit flag vulnerabilities outside the protected network.

References

[1] Guofang Zhang, Weitao Li. A security reinforcement scheme for the server. WOP in education social sciences and psychology. 2018.7

[2] Guofang Zhang, Dengpan Yang. Research on SQL Injection based on web pages. Network security technology and application. 2019.3

[3] Alboba, B., & Dixon, W.(2004). IPsec-network address translation(NAT) compatibility requirements. RFC3715.

[4] Guo-Fang Zhang. A rapid switching technology of IP data packet based on Multi-Protocol. International Journal of Technology Management 2014.8.

[5] Windows 2003 server safty reinforcement scheme.

[6] GUO-FANG ZHANG. The solution and management of VPN based IPSec technology. International Journal of Technology Management 2014.7.

[7] Peifei Wu. Network security management and technical protection. 2017.3

[8] Heping Ye. Cloud computing security protection technology. 2018.8

[9] Mingyi Ding. The way of linux operations and maintenance.2016.8

[10] Yongming Cai. The foundation of python programming. 2019.1