Research on the Dynamic Network Defense Technology Based on the DHCP Protocol

Tao sun*, Hai wang, Yang gao and Bingbing luo

ZhangJiaKou Electric Power CO., LTD. 075000, China
*Corresponding author's e-mail: 254576969@qq.com

Abstract. The article proposes a network dynamic defense model based on the DHCP protocol for enterprise internal network security protection needs, which not only implements network terminal access verification, but also it realizes the periodic dynamic adjustment of the IP address, and increases the difficulty of network detection and attack. So, the security of the enterprise intranet is improved.

1. Introduction

With the popularization and development of computer technology, the development of network has a profound impact on people's production, life and work. As enterprises undertake the task of technological innovation and production, they are faced with more and more network security problems. The main safety risks it faces mainly include[1]:

(1) Risk of internal malicious or non-conforming terminal access

It mainly includes that the internal personnel can access any position and interface of the internal network by using the office terminal, or access non-conforming terminals such as personal computers to the enterprise internal network, or malicious personnel can access the enterprise internal network at will. This kind of risk may lead to the overflow of Intranet virus, the leakage of internal information or the malicious introduction of backdoor loopholes.

(2) Risks from external attacks

It mainly includes all kinds of network attacks from the outside of the intranet. Because the information system always has security risks, such as new vulnerabilities of the operating system are found, business software or protocol vulnerabilities, and all kinds of security policy are not configured, the enterprise intranet may be attacked, which may bring serious security consequences.

The application of firewall, intrusion detection, anti-virus and other traditional protection technologies can solve the security problems of Intranet to a certain extent. However, the integrated use of a variety of security technology products, on the one hand, has a high cost and complexity of configuration management; on the other hand, most of the traditional protection technologies are based on prior knowledge, which can achieve effective protection against all kinds of known network attacks, but in the face of more and more new and unknown threats, they are unable to cope effectively.

Dynamic defense is different from the previous network security research ideas. It aims to deploy and run uncertain, random and dynamic networks and systems, making it difficult for attackers to find targets. Dynamic defense can also take the initiative to deceive the attacker, disturb the attacker's sight, lead him to a dead end, and set a fake target / decoy to lure the attacker to attack him, thus triggering an attack alarm. Dynamic defense changes the passive situation of network defense, changes the "rules of the game" of both sides, and truly realizes "active" defense. Based on the DHCP protocol, this paper
proposes a network dynamic defense model, which can not only support network access authentication, prevent non-conforming or malicious terminals from accessing the network, but also dynamically and periodically change the IP address of the internal network host, change the fingerprint information of the internal network host, increase the difficulty of detection and attack from the external network attacker, and improve the effectiveness of the internal network security protection.

2. Theory of 802.1x and DHCP

2.1. 802.1X protocol

802.1x protocol can be divided into authentication mode with client access device and authentication mode without client access device (MAC bypass authentication mode) according to the actual intranet situation and in order to meet the different types of access devices in the intranet[2].

(1) With client access device authentication
When the access device can install the authentication client, the user name and password are used to authenticate the legitimacy of the access device, which is suitable for computers, servers, etc.

(2) No client access device authentication
When the access device cannot install the authentication client, the legitimacy of the access device can be verified by confirming the MAC address, which is applicable to all devices, including computers, servers, printers, etc.

2.2. DHCP protocol

Dynamic Host Configuration Protocol (DHCP) is a LAN network protocol, which uses UDP protocol to work. Its main purpose is to automatically assign IP address to hosts in LAN[3].

DHCP uses UDP protocol and port: 67 (server) and 68 (client). The process of DHCP client computer acquiring TCP/IP protocol is four line call back, such as:

(1) Discovery stage. The client computer sends the dhcpdiscover message, broadcasts to the network, and searches for the DHCP server in the network;

(2) Provision stage. After receiving the dhcpdiscover message, the server selects an unassigned IP address from its own address pool to distribute to the client computer, and then sends DHCP including rental IP address and other configurations to the client _ Offer message;

(3) Selection stage. That is, the DHCP client selects the IP address. If there are multiple DHCP servers sending DHCP to the client computer _ Offer message, client computer only accepts the first received DHCP_ Offer message, and then respond to DHCP server by broadcasting_ Request message, which contains the content of requesting IP address from the selected DHCP server.

(4) Confirmation stage. When the DHCP server receives the DHCP response from the client computer _ After the request message, it sends the DHCP containing the IP address and other configuration provided by it to the client computer_ ACK confirmation message. Then the client computer binds its TCP/IP protocol components to the network card.

DHCP message format is based on BOOTP message format, in which Option field is the optional field of its expandable function[4,5]. All DHCPOption are in [type] [length] [value] format. The type (field) is the 1-byte identification number, which represents the DHCPOption information type; the length (length) is 1-byte, which represents the length of the information content after; the value (meaning) is the length specified by the length field, which represents the information content.

The [type] and [value] fields of DHCPOption are unique identifiers, so different terminal devices can be distinguished by checking DHCPOption information in DHCPDiscover and Request messages sent by DHCP clients.

The data part of the message with ID 12 is the host name of the client; the data part of the message with ID 55 is the parameter option representing different operating systems; the data part of the message with ID 60 identifies the type and configuration of the DHCP client.
3. Network dynamic defense model based on DHCP protocol

This paper proposes a dynamic network defense model based on DHCP protocol. The model uses the MAC address authentication method based on 802.1x protocol to authenticate the network access devices. After the authentication is passed, the dynamic random IP address is assigned to the network access devices periodically based on DHCP protocol. The model is shown in the figure.

Figure 1. Network dynamic defense graph based on DHCP protocol

(1) Collecting MAC addresses of all legitimate intranet devices, as well as options (12), options (60), and options (55) in DHCPOption, we can bind them together as MAC fingerprint information of legitimate intranet devices and store them in the database. Where: option (12) is the host name of the device, option (55) represents the set request parameter list option, and option (60) is a custom field of each operating system manufacturer.

(2) When the device accesses the network, based on no client access device authentication mode (MAC bypass authentication mode), we can obtain the MAC address of the device and compare it with the data in the database. If it exists and is correct, it is allowed to access, otherwise it is not allowed to access.

(3) The device sends dhcpdiscover message. The DHCP server collects Mac, option12, 55, 60 and other information of the access terminal device, and compares it with the MAC fingerprint information of the device stored in the database. If the comparison is successful, it sends dhcpoffers message to the device, randomly and dynamically assigns IP to the device. If the comparison is not successful, it assigns isolation IP to the device. Then the device sends dhcprequest to the DHCP server Finally, the DHCP server replies dhcpack message to the device to confirm the service cycle of the assigned IP.

(4) When the device IP lease expires, it is handled as follows:

- When the equipment is in the communication state and the communication object is the external network equipment, IP is released directly and new random IP is applied again;
- When the equipment is in the communication state and the communication object is the intranet equipment, it is allowed to apply for the renewal of IP from the DHCP service, release the IP directly after the communication, and then apply for a new random IP again;
- When the device is not in the communication state, release the IP address; apply to the DHCP server again, and the DHCP server dynamically generates random IP for it.
3.1. VLAN division of Intranet
According to the needs, the Intranet can be divided into several subnets, one of which is regarded as the isolated subnet and does not interwork with other subnets, and other subnets can interwork. Several situations are as follows:

- Devices without MAC address authentication are not allowed to enter the network;
- The network access devices that pass MAC address authentication and MAC fingerprint information authentication can randomly assign an IP address within the IP range of the allowed interconnection subnet;
- The network access devices that pass MAC address authentication but fail to pass MAC fingerprint information authentication are randomly assigned an IP address within the IP range of the isolated subnet.

3.2. Dynamic IP address allocation method based on DHCP protocol
The IP address pool is built by all idle IP addresses that allow interconnection. If the intranet IP address subnet is between 192.168.1.X-192.168.255.X, the maximum number of idle IP addresses in the IP address pool can be 216.

When there is a new application or periodic IP update for a network access device that has passed MAC address authentication and MAC fingerprint information authentication, the MAC of the device and the current time t are taken to hash together, and then the number of idle IPS in the IP address pool of the value module is taken and the remainder is taken, then the idle IP corresponding to the remainder is selected to assign to the device.

4. Design of network dynamic defense system based on DHCP protocol

![Diagram of network dynamic defense system based on DHCP protocol](image)

The network dynamic defense system based on DHCP protocol is shown in Figure 2, including device authentication module, option check module, address pool module, address random assignment module, address recovery module and data flow table management module. Several situations are as follows:

- Equipment authentication module: complete the identity check of the network access equipment, only the equipment with legal MAC address is allowed to enter the network, otherwise it is not allowed to enter the network.
- Address pool module: manage the IP address in the address pool, make real-time statistics on the number of active IP and idle IP, and sort the idle IP randomly.
• Option check module: after the network access equipment passes the authentication check, check whether the Mac, option12, 55 and 60 information matches the legal MAC fingerprint information existing in the database.
• Random address assignment module: when the option check is passed, the module assigns IP to the device according to the algorithm and sets the lease period; when the option check is not passed, it isolates IP for assignment and sets the lease period.
• Address recovery module: when the device IP lease expires, release the IP to the address pool.
• Data flow table management module: it is responsible for maintaining the flow table entries of devices with communication behavior. The composition of flow table entries: <source MAC, source IP, source port, lease, destination MAC, destination IP, destination MAC, lease). When the device has communication behavior, the flow table item is built, when there is IP update, the flow table item is updated, and when the communication ends, the flow table item is deleted.

The network dynamic defense system based on the DHCP protocol not only ensures the security of the intranet equipment, but also ensures the normal communication between the equipment, so it adds the data flow table management module. When the internal network device is in communication and the IP address changes, it can still maintain normal communication.

5. Conclusion
The network dynamic defense technology based on DHCP protocol proposed in this paper can effectively solve the internal and external network security threats mentioned above:

(1) Mac authentication mode based on 802.1x protocol and MAC fingerprint matching mode based on MAC, Option 12, 55 and 60 of DHCP can ensure that legitimate terminals access the network and randomly assign IP, while malicious or illegal terminals cannot access, and can resist MAC address counterfeiting attack.

(2) The periodic dynamic and random IP assignment of device terminals based on DHCP protocol makes it difficult for attackers to detect the network topology and device characteristics in the network and build attack chain. At the same time, all behaviors of accessing idle IP can be regarded as being attacked, and all devices in the isolated subnet can be regarded as violating devices, so as to achieve the purpose of early warning.

(3) While ensuring the randomness of Intranet IP, the normal communication between devices can be ensured by building data flow table.

References
[1] Shin S, Yegneswaran V, Porras P, et al. (2013) AVANTGUARD: Scalable and vigilant switch flow management in software-defined networks. Proc of ACM CCS’13. New York: ACM, 2013:413-424.
[2] Zhou bin, He tonglin.(2012) Research and implementation of DHCP network access and access authentication based on embedded terminal. Computer CD software and Application. pp.23:171.
[3] Wang tao, CHen Hongchang. (2017) SGuardA lightweight SDN safeguard architecture for DoS attacks. China Communications.pp.14(6):113-125.
[4] Zhang Peng, Wang Huanzhuo, Hu Chengchen, et al. (2016) On denial of Service attacks in software defined networks. IEEE Netwrok. pp.30(6):28-33.
[5] ARZT S, RASTHOFER S, FRITZ C, et al. (2014) FlowDroid: precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for Android apps. ACM Sigplan Conference on Programming Language Design and Implementation. pp.259-269.