Discussion and Development of Network Attack and Prevention

Xiaomeng Li
Department of Computer Science, North China Electric Power University, Baoding, 071000, China
2952331968@qq.com

Keywords: Network Attack, Social Engineering, Network Defense, Firewall.

Abstract. A comprehensive overview of today's cyber-attacks and defenses technology. This paper introduces the application of social engineering in network attack and the principle of intrusion method of man - in - the - middle attack. In the rapid development of network attacks, at the same time, network defense technology is also constantly evolving, on the daily use of firewall defense technology and encryption technology to elaborate. We'll discuss the network attack and defense overall.

1. The research background

With the rapid development of Internet, the network with its open, shared features have an greater impact on the social growing than ever before. Meanwhile, network security issues are getting more and more concern. In 2015, 79790 data leaks occurred in 61 countries worldwide, of which 2122 have been confirmed. Information security events are defined as: any event that causes damage to the confidentiality, integrity, and availability of information security. Data leakage is defined as: data is leaked to any unauthorized party's accident. Therefore, the study of network attack and prevention technology is particularly important today.

The Global Information Leak Event for 2015 is shown in following **Table 1**

Table 1. Global Information Leak in 2015

Event 1	Event 2	Event 3	Event 4	Event 5	Event 6
Russian dating site leaks 20 million user's data	80 million personal information was stolen in Anthern or becoming the largest US healthcare-related leak	medical insurance company in the US CareFirst was disrupted, meanwhile, 1.1 million user information is leaked	2.4 million Internet users were hacked: encrypted credit card data was leaked in British	The worst leak in the history of Britain: the informtion of 400 million people was leaked	54 hotels of Starwood were attacked by implanted POS malware,which makng bank data leak

In the network attack and prevention field, there are white hat, black hat, gray hat such hacker taxonomy. The main attacking practices of malicious Cracker are: getting passwords, placing Trojan, web spoofing, e-mail attacks, attacking another node through a node, network monitoring, finding system vulnerabilities, exploiting Buffer overflow theft privilege and so on. The methods of network monitoring and detection are as follows: ARP (Address Resolution Protocol) technology, DNS technology, the method of network and host responsd time.

2. Network attack technology

At present, hacker attacks increased year by year, while the level of invaders decreased year by year. Hackers use a variety of means of attack to usurp information , to a certain extent, giving personal privacy ,life and property security damage.

The path of the leaked information is shown in the following Figure 1.

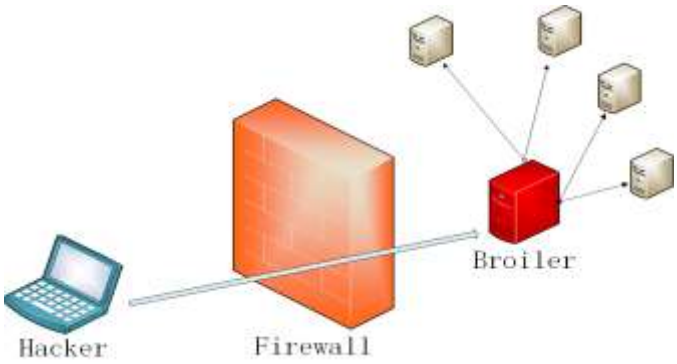

Fig.1 Network attack

2.1 The application of social engineering in network attack

The use of social engineering attacks are becoming mature than before, typical forms include address spoofing, mail spoofing, message spoofing, software spoofing, window spoofing, other deception and so on. Hackers commonly use means of attack are mail spoofing, message spoofing, software spoofing, window spoofing.

Mail spoofing,which attacker use to convince the target to believe an event or lure the target into accessing a link by sending spam, replace the attachment with the Trojan horse program,or bunbles the attachment with the Trojan horse program, is an attack technique,luring us into running to achieve skeletons in the closet.

Message spoofing is an attack technique in which attacker use the network message to send tool and frau information to the target. The most typical is the use of some IM (Instance Messaging) which are chatting tools ,such as QQ, WeChat and so on.

Software spoofing is an attack technique which attacker use to release malicious code or virus software to Internet which users download and install,the malicious software plays a role immediately.that is because the user execute it actively, making the security extremely high .

Window spoofing is mostly window spoofing on the web page. Attackers using the user's greedy psychology, give a fall of the sky, "pie", to induce users to visit the page or do related operations in the way specified by the attacker to achieve the anticipatory attack purposes.

2.2 The method of intrusion of man attack

Man-in-the-Middle Attack (MITM) is a long-standing invading means of network, and today there is still a wide range of development space, such as SMB session hijacking, DNS spoofing attacks. In short, MITM attacks are attack technique that attacker tamper and sniff data by intercepting the normal network communication data without any knowledge of the communication.

Nowaday, MITM attacks are becoming more and more diversified. Initially, the attacker can achieve purpose, as long as the network card disguising as a proxy server is set to mixed mode to monitor specific traffic. Later, with the switch insteads of the hub, a simple sniffer attack has been unable to succeed, you must do ARP spoofing first.

3. Network defense technology

With the improvement of network attack technology, information security requirements are getting higher and higher. network defense work has become particularly important, meanwhile ,defense means are constantly improving. Network defense includes a reasonable configuration of the firewall, security authentication means, encryption technology.

The commonly used network defense is shown in the following **Figure 2**

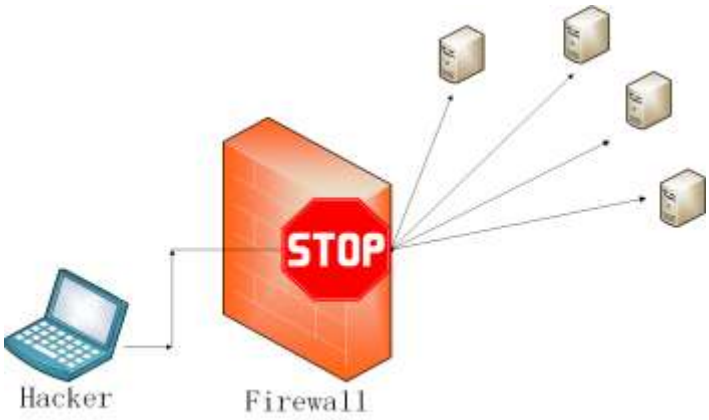

Fig.2 Network defense

3.1 Firewall technology

As an effective network security mechanism firewall has been widely used in network systems, to maximize the prevention of computer network insecurity invading. In the computer network, the configuration of the firewall that controls the implementation of the network communication access,has a clear access to people and data to enter the network system, can intercepte not allowed or other illegal elements and data in time, which can effectively prevent Hackers or illegal elements into the destruction of the network.

3.2 Encryption technology

Encryption technology switchs the plaintext data to the encrypted data in a certain conversion method. Viruses and hackers are generally cause damage to the database from the subtle loopholes.However,the use of encryption technology to encrypt sensitive data can effectively ensure data security, so as to ensure the safe and reliable operation of the computer system.

4. Conclusion

As network attacks implement more complex and easier, and the number of cyber attacks are continuing to increase,the education and training at all stages of the attack becomes critical,which must be used as an important part of the protection strategy in order to achieve attack management. At the same time, we should test and evaluate available new technology in the system and the market constantly. We should check the bypass deployment detection tool repeatedly and consider deploying a hybrid solution that protects our information security in attacks that could block Internet pipelines, thus ensuring the safety of individuals and enterprises.

Reference

[1]. Global Data Security Event in 2015.
[2]. http://www.enkj.com/idcnews/Article/20160104/8784
[3]. Application and Prevention of Social Engineering in Network Attack.
[4]. http://security.ctocio.com.cn/tips/457/8560457_2.shtml
[5]. Demonstration and prevention of man-in-the-middle attacks against SSL.
[6]. http://security.ctocio.com.cn/105/12477605.shtml