Journal of Applied Science and Engineering Innovation, Vol.3 No.5, 2016, pp. 182-184
ISSN (Print): 2331-9062
ISSN (Online): 2331-9070

Research on Strategy of Network Antivirus under Virtual Network Environment

ZHAO Li-zhen[1] , YANG Fan[2]

[1]*Educational Technology and Computer Center Zhaoqing University, Zhaoqing, Guangdong, China*
[2]*School of Computer Science, Zhaoqing University, Zhaoqing, Guangdong, China .*

Abstract: According to the new characteristics of security threats of campus network virus in college and university, it analyzes the defects of prevention and control strategy of traditional network virus, based on network simulation environment, to make research on the method of preventing network virus attacks through the Internet router, then it proposes network virus prevention and control strategies of combining "core "and" end "isolation method, which makes simulation verification under the virtual network environment, and the results prove that the strategy is effective.

Keywords: Campus Network; Network Virus; Virtual Network; ACL

INTRODUCTION

From the aspect of the codes of designing general campus network, generally speaking, the campus network will set firewall and other security facilities at the exit of network, so as to isolate the internal network and the outer network[1]. Among many of the isolation functions, antivirus isolation is very essential[2]. It can effectively prevent network virus attacks and virus spread to the internal network. However, another security threat of campus network is the virus spreading as well as attacking from the campus network.

In this paper, according to the spread of the virus in the internal campus network as well as the attacking problems, it makes analysis on the defects of virus prevention and control strategy of traditional network, based on GNS3 network simulator and VirtualBox virtual machine technology, making research and analysis on the operating characteristics of network virus program as well as the basic method of campus internal network virus prevention and control method, moreover, it carries out the simulation verification under the virtual network environment, on the basis of this, it makes research and analysis on the influence of network virus prevention on normal network services, which can provide feasible and effective network virus prevention and control strategy for the campus network.

BRIEF INTRODUCTION OF VIRTUAL NETWORK TECHNOLOGY

In this paper, the virtual network environment is constructed by network simulator GNS3, eNSP and VirtualBox virtual machine, which can simulate network products of different manufacturers and build up network, which also can construct different OS platform network services according to the requirement of business, so as to form a virtual network case that is real network engineering application oriented and provide the ability of having research and testing on network function.

Introduction of Network Simulator

eNSP (Enterprise Network Simulation Platform) is a type of network simulator that takes Huawei's network equipment as the simulating object[3], which integrates WinPcap, VirtualBox virtual machines[4], as well as Wireshark software, etc.. Moreover, it is fixed and embedded with Huawei AR series of routers, Huawei S series of switches, Huawei wireless devices, Huawei firewalls and all kinds of terminal devices, connected with Huawei's network equipment, equipment configuration as well as the ability of network function simulation.

GNS3 is a network simulator that takes Cisco network device as the simulation object[5], integrating Winpcap, Dynamips, VPCS, Qemu[6], VirtualBOX virtual machine, Wireshark software and so on, which can not only load different series of IOS of Cisco routing devices, it also through the integration of Qemu virtual technology and the configuration of the corresponding OS virtual image, offering Qemu client, PIX firewall, ASA firewall, Juniper router and the virtual simulation capabilities with IDS and IPS kernel, so as to provide configuration as well as function simulation ability of Cisco network technology (routing, switching, network link, network security, etc.).

Brief Introduction of VirtualBox Virtual Machine

VirtualBox is a kind of free virtual machine platform released by Oracle, which can virtualize 32/64 series of virtual machines, such as Windows 7/8/10 client, Windows server, Linux client /server,

Mac OS X client/server and so on.In the virtual network environment, VirtualBox virtual machine mainly has three functions: the first function is to provide a running environment for virtual network equipment, the second function is to provide an operating environment for the complex network application service, the third function is to simulate the real network client. From the aspect of networking capabilities, VirtualBOX virtual machine can provide six different networking modes[7], which can realize the multiple connection with GNS3 network simulator as well as the real network.

STRATEGY RESEARCH OF CAMPUS NETWORK ANTIVIRUS

Network Antivirus Characteristics and Prevention and Control Strategy Analysis

Different from the ordinary computer virus, the basic characteristics of network virus is the rapid spread as well as the remote attacks, its core is to use the connectivity of network, via e-mail, instant messaging, web browsing, shared folders and other ways to spread quickly, so as to conduct attacking behavior by TCP or UDP protocol as well as the specific port, the aim of which is to shut down network service and steal the information of users and so on[8]. For example, Worm. Blaster a kind of blaster virus, using RPC loopholes in Windows system, using TCP protocol and port 135 when it attacks, this port is corresponded to Windows DCOM port RPC service process, which can cause the service process to be collapsed. At the same time, this virus can use 4444 port of TCP as the back door monitoring port to implement remote control, which also can use 69 port of UDP to download file. In general, the way of a kind of virus spreading and attacking may be mixed with a variety of different ways to improve the technical difficulty of prevention. Table 1 presents us the characteristics of several network viruses as well as the use of ports.

Table 1 Characteristics of Several Network Viruses and Using Circumstance of Ports

Name of virus	Characteristics of virus	Protocol and port
Worm.Blaster blaster	Using RPC loopholes in Windows system, opening the back door process, monitoring host computer of network, downloading network file.	TCP4444， UDP69， TCP 135
Win32.Lioten.KX worm	This is a worm that spreads through the network share and exploit vulnerabilities.	TCP135，TCP139，TCP445
W32.Sasser worm	Using multiple processes to scan different ranges of Internet addresses, trying to find the "easy affected" LSASS component on 445 port.	TCP 135、139、445 TCP 1025, 5554 (using this port to transmit worm program) TCP 9996 (using port during attacking).

At present, campus network virus prevention and control strategy is based on the concept of prevention and control of "computer virus" so as to construct the "end" control strategy, the main methods have three kinds, one method is to install system patches in time, another method is to install personal firewall, the last method is to install antivirus software. In practice, many students install a variety of antivirus software and firewall on the network host computer because of the lack of common sense and professional knowledge, who only install them but never set them, which makes the installation of the firewall software difficult to play the role of isolation, but also often leads to the result that LAN can not use, more serious result is to cause the performance of host computer decline due to the large consumption of resources of the computer. The available types of antivirus software in the market are taking "detecting the characteristics of virus" as the premise, through scanning and matching the characteristics of virus, using the method of isolating or deleting the infected files so as to prevent network host system from the "virus", facing the network virus that takes "network spreading" as the basis, this "end" isolation method seems "powerless".

Constructing Network Antivirus Virtual Environment

In order to verify the spreading route and attacking characteristics of network virus in the real network, the network can be constructed under the virtual network environment, which can be shown in Fig.1. Win2003 is a web server that provides Web service and LAN file sharing service; WinXP is the network client, using web services; R2 is the Internet router, which can simulate subnet layer router in campus network; sw1 is LAN switch. Based on this environment, first of all, it can simulate the propagation process of network virus in the virtual network, then it can simulate the attacking behavior of network virus. In this process, the router for interconnection purpose can have play a decisive role in the spreading and attacking behavior, if the antivirus rule can be deployed on R2 router, namely,

"core" isolation can effectively prevent network virus from spreading and attacking.

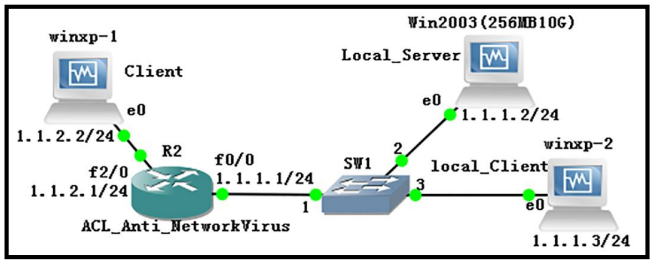

Fig. 1 Antivirus Simulation Network

Configuration of Network Antivirus Rule

The basic approach of "core" isolation is through the analysis of the spreading and attacking if network virus, it can get the remote protocol and the port number used by network virus attack (TCP or UDP), by using ACL rules, applying "deny" operation to the corresponding data flow, so as to prevent network virus attacks. In order to prevent the implementation of the three kinds of network virus attacks shown in Table 1, the following ACL rules can be configured on the Internet router R2, which also can be applied to the inlet direction of f0/0 port.

Operating and Testing of Simulation

In the simulated network environment shown in Fig. 1, Win2003 can simulate a web server, which can provide web services and LAN file sharing service, starting TCP 80, 135, 139 and 445 port, winxp-1 can simulate the host computer that is infected with "W32.Sasser worm" virus, while winxp-2 can simulate the uninfected host computers. When it operates network, starting antivirus rule ACL_Anti_NetworkVirus in R2, through the continuous operation and detection of network status, it can find out that data packets sent by winxp-1 port 135, 139, 445 are all blocked by R2, Win2003 file sharing service has not got the attack, from winxp-2 it can still access to the shared folder, but winxp-1 can not normally access to share folder. The result of simulation showed us that for all types of network viruses, it can have a similar rule configuration in R2, which can effectively prevent the occurrence of aggressive behavior between each sub network in the campus network, so as to protect the internal network from network viruses. But at the same time, the network services of the same port will not be able to use.

```
R2(config)#Access-list 101 deny udp any any eq 69
R2(config)#Access-list 101 deny tcp any any eq 135
R2(config)#Access-list 101 deny tcp any any eq 139
R2(config)#Access-list 101 deny tcp any any eq 445
R2(config)#Access-list 101 deny tcp any any eq 1025
R2(config)#Access-list 101 deny tcp any any eq 4444
R2(config)#Access-list 101 deny tcp any any eq 5554
R2(config)#Access-list 101 deny tcp any any eq 9996
R2(config)#int f0/0
R2(config-if)#ip access-group 101 in
R2(config-if)#exit
```

CONCLUSION

In this paper, it puts forward the "core" isolation antivirus method, which can be applied in all network areas of campus network (such as the experimentation area, dormitory area, teaching area, library and office area, etc.) with convergence router as well as the corresponding anti-virus rules, therefore, it can effectively prevent network attacks among the network areas of the campus network, with the combination of updating system patches by network edge user's host computer and effective allocation of personal firewall strategy, which can form the the basic strategy of campus network internal preventing for network virus attacks. So as to reduce and even replace the dependence of nonfunctional "anti-virus software" for the end users[9].

REFERENCES

[1]Yi Jianxun, etc.. Computer Network Design (The Second Edition)[M]. Beijing: Posts and Telecommuni cations Press, 2012:170-185

[2] Qi Hongwei. Research and Realization of Security Protection for Campus Network Information [D]. [Inner Mongolia University Master's Thesis]. Inner Mongolia: Inner Mongolia University, 2010

[3]HUAWEI, eNSP Helping Manual [EB/OL]. http://down. 51cto.com/data/643160, 2014

[4]Oracle, the VirtualBox User Manual[EB/OL]. https: //www.virtualbox.org/manual/UserManual. html, 2016

[5]GNS3, GNS3 Documentation[EB/OL]. https://www. gns3.com/support/docs/glossary-of-terms, 2016

[6]Qemu Documentation/Networking [EB/OL]. http://wiki. qemu.org/Documentation/Networking#Network_backen d_types, 2012-12-16

[7]Oracle, Virtual networking [EB/OL]. https://www. virtualbox.org/manual/ch06.html,2016

[8] Liu Benfa. The Characteristics of Computer Network Virus and Prevention Measures [J]. Guide for Software, 2011-06,10 (6): 131-132

[9] Network antivirus software can only play its function as much as one tenth for preventing the virus [EB/OL]. http://network. Pconline. com. cn/814/8143905. html, 2016-07-16