The Application of ICMP Protocol in Network Scanning

JIANG Wei-hua, LI Wei-hua, DU Jun
Department of Computer Science and Technology,
Northwestern Polytechnical University, Xi'an 710072, China

Abstract: The application of ICMP protocol in network scanning is presented. The paper analyzes the characteristics of ICMP packets and the current detecting methods, and brings forward some new methods and OS fingerprint recognition. An OS detection model based on ICMP is described later.

Keywords: ICMP; Host Detection; OS Fingerprint Recognition

With the extensive application of network technology, new types of network services keep cropping up, bringing about profound changes in the society. In the meantime, network security problems have become increasingly prominent for it they pose a threat to the security base of the whole society. Studies on the strategy, methods, techniques and ways of hacker attack help improve the structure of network security protection system and minimize losses brought about by network security problems.

Data collection is the first step taken by hacker attack, while network scanning is an important means for data collection. At present, the purpose for network scanning is no longer confined to finding out an open port. It is aimed at OS fingerprint recognition, attempting to detect the type and version of the OS used by the targeted host, thus providing information for the attack. The current scanning technology falls into two categories: TCP and ICMP technology. Studies on TCP technology have been rather profound. Therefore, more emphasis should be laid on the application of ICMP technology in the process of OS recognition.

There are three levels in network scanning, first, to detect whether the targeted host is still alive; second, to detect the OS of the targeted host; third, to recognize certain application program or the version of the specified service. This paper focuses on the application of ICMP protocol in the first two ways of detection, introduces some new methods and tests them by using network security tools. In the final part, an OS detection model based on ICMP protocol is set up and its characteristics and development trend are also described.

I. Host detection by using ICMP protocol

The purpose of host detection is first to detect whether the host is still alive and then to further find out the possible protocol observed by the host.

When using ICMP for host detection, Ping is the most frequently used method for a single host, Fping (fast ping) for multiple hosts and broadcast Ping for all the hosts on a subnet. If the target responds to these methods, it shows that the host is alive. Otherwise, the host is switched off or a firewall has been set up and access is forbidden.

In order to find out the possible protocol observed by the host, the protocol field of the IP header should be taken full advantage of when designing the report. In Version IPV4[RFC791], there is a "protocol domain" in the IP data header which uses an eight-digit code to stand for the upper protocol. By using these protocol codes, we can freely fill in the protocol field in the IP header of the original socket with the protocol codes. In doing so, we can construct a special data packet and send it to the target host. According to the returned data, we will be able to tell whether the target host is still alive or not. We may also go a bit further to recognize the protocol observed by the target host.

II. OS fingerprint recognition

For intruders, if they succeed in acquiring information about the type of OS used by the host, they can try the loopholes in the OS one by one and therefore, they can save a lot of time and improve the scanning efficiency and accuracy. There are many ways to recognize the OS and a popular but complicated one is the fingerprint recognition method based on TCP/IP protocol. This method recognizes the type of the OS by the subtle differences in the definition of the protocol given by different OS. According to different ways of realization, it falls into two types, namely, active detection and passive detection.

Active OS detection means that the source host sends specified type of date packets to the target host. Certain field of these data packets includes the characteristics of the OS. The returned packets can show the type of the OS or specify the OS by comparing the OS fingerprint database with the corresponding value of certain field in the data packets.

While in the passive OS detection system, the source host does not need to send detective data packets. It passively hunts reports sent and received by the target host and then finds out the corresponding type of OS by detecting the value of the corresponding field and consulting the fingerprint database.

Although these two methods are different in their realization mechanisms, they are similar in handling and analyzing data packets. In terms of technology, it is categorized into TCP and ICMP technology. Comparatively speaking, the latter has the following advantages. First, it has a high recognition performance and it is particularly precise in recognizing the Windows OS. Second, it is simple to realize. You just need to send

0-7803-7840-7/03/$17.00 ©2003 IEEE.

several logically related data packets and as has been experimented, the number of packets sent is less than four.

3 The application of ICMP in active OS detection

In order to recognize the OS by using active detection, it is imperative to set certain field of the IP header. The following diagram shows the format of the IP header.

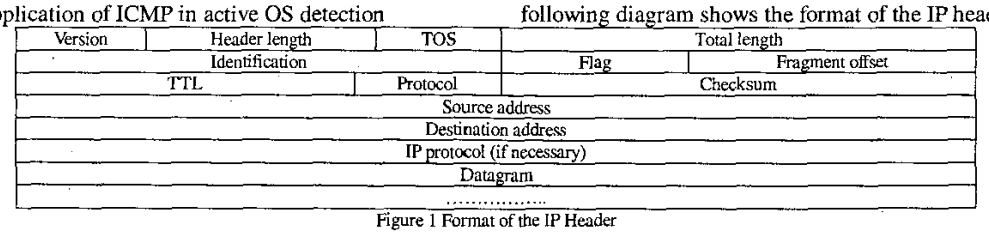

Figure 1 Format of the IP Header

ID Field: Most OS returns with their own ID number and some OS, such as Linux machine based on 2.4.0—2.4.4 kernel will set the IP identifier to zero in the ICMP query request and reply information.

DF Field: Some TCP/IP stacks will set DF digits in a wrong ICMP data packet. Others (such as Linux) will copy all the eight digits and set some of them to zero. The rest will ignore the original DF and set some value related to itself.

TTL Field: There are two independent values in the IP TTL field of the ICMP data packet, one is ICMP query information and the other is query reply setup. The TTL value of the reply packet will reduce by one when passing through each router from the target host to the source host. In accordance with the TTL value in the report and with the reference to the statistics of the TTL value of all types of OS from the following URL---http:/www.switch.ch/ttl_default.html, we can speculate on the original TTL of the target host and then find out the type of its OS.

TOS Field: Generally speaking, as provided for by RFC 1349, the ICMP reply information should use the same TOS field value in the corresponding ICMP request information. But some OS do not abide by this principle. TOS service field includes three fields, first, a priority field {RFC 791} which is three-digit long and has eight priority levels; second, service type field which is four-digit long and describes the type of service operating on the network. It includes the minimal delay, the maximal throughput, the highest reliability and the lowest cost. Third, the last useful digit field must be set to zero. And the TOS digits and the last field will be replaced in implementing the service type mechanism. If all the four digits are zero, it means ordinary service.

We have combined all these fields together and found out some methods for OS recognition by using Ping, Snort and other tools and with the reference to all types of ICMP reports.

1.Combine the address mask request report with the fragments symbol DF

If the target host responds to the address mask request report, then it is Solaris, HP-UX11.0X, ULTRIX, OpenVMS, Win 95/98/98SE/NT (version lower than SP4). For these OS, we send the address mask request report with fragments symbols to them again. If in the response report, the returned value is address mask and then the systems are ULTRIX, OpenVMS and Win95/98/98SE/NT (version lower than SP4). Then we will differentiate them by the TTL value. When TTL equals to 255, the systems are ULTRIX and OpenVMS. When TTL equals to 128, the systems are Win95/98/98SE/NT (version lower than SP4). Generally speaking, systems with no response are Solaris, HP-UX11.0X.

2. Combine the return request report with the fragment symbol DF

If the target host is sent with the ICMP return request report with the setup of DF symbol, there are two types of response reports. One is not to return the DF symbol. Then the common systems are Linux 2.2.x, ULTRIX, Novell Netware. All these common systems can be further differentiated by TTL value. When TTL equals to 128, it is Novell Netware. When TTL equals to 255, it is Linux 2.2.x, ULTRIX. For Linux 2.2.x and ULTRIX, we will further send ICMP address mask request report, the one with response is ULTRIX and the one without response is Linux 2.2.x.

For those OS that do not return the DF symbol, we will once again send the address mask request report with the DF digit setup. The OS which return the DF digits is Solaris, HP-UX11.0X, OpenVMS and the OS which does return these digits is Win 98/98SE.

3.Apply TOS digits

(1). Send return report with precedence which is not zero

There are two types of return reports: return report with the original precedence value and report with precedence which is zero.

For the first type of OS, we will send the time-stamp with the precedence which is not zero for requesting report. In the return report, if the precedence is zero, it is usually Win 98/98SE and OpenVMS. Then we will make judgment according to the TTL value. When TTL equals to 225, it is OpenVMS. When TTL equals to 128, it is Win98/98SE/ME. Then we will further send address mask request report. If there is response, it is Win98/98SE. If there is no response, it is Win ME.

For OS whose precedence is set to zero in the return report, it is usually Win2000, Ultrix and HPUX11.X. Then we will make further judgment according to the TTL value. When TTL equals to 128, it is Win2000. When TTL equals to 225, it is Ultrix and HpUX11.X.

(2) Send report with the type of service field which is not zero.

There are two types of return reports: TOS is not zero and TOS is zero.

For the OS whose TOS is not zero, we will further send time stamp with TOS which is not zero for requesting report. If the TOS is zero in the reply report, then it is Win95/98/98SE/ME. We will then make judgment according to the address mask request report.

For the OS whose TOS is zero, it is usually Win2000, Ultrix and Novell Netware. As explained earlier, we will then make judgment according to the TTL value.

III. Construct a testing model by using a logical tree

From the abovementioned tests, judging the OS by using ICMP protocol has the following features. First, the reports sent are logically and strongly linked together and can be described by the concept of a tree. The key is how to properly arrange the level and sequence of the data packets. Second, it is simple and easy. The number of reports sent is less than four. Third, it is well covered up and difficult to be discovered by the target system. Based on these features of ICMP in OS recognition, we have designed an OS recognition system based on ICMP by using the idea of a logical tree. The recognition model is as follows:

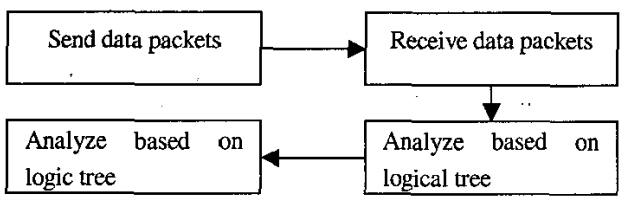

Figure 2 OS Recognition Model Based on ICMP

In the process of realization, UDP data packets are sent to the closed port of the target so as to trigger report that the ICMP port is inaccessible. By detecting the returned data information, some features of the target host is found out. Then the direction of the branches of the protocol tree is chosen according to these features. Specified data packets will be sent at the node and information provided by the returned data packet will further determine the direction of the logical tree until the type of the OS is finally identified.

Logical tree is composed by organizing the interrelated data packets used for OS recognition. For example, the data packets sent in the testing stage can be used as a part of the logical tree. The branches of a simple logical tree are as follows: when getting the report that the ICMP port is inaccessible, there are two branches. One group is the OS responding to the precedence report and the other is the OS that does not respond to the precedence report. Systems that respond to the precedence report include: Linux 2.0.X, 2.2.X, 2.4.X, CISCO IOS 11.X-12.X, Extreme Network Switches and etc. Then we will use the size of wrong ICMP quoting to differentiate them. Linux abides by RFC1122 and will include 576 eight-digit group data in the ICMP wrong information, while other systems in the group only include 8 eight-digit groups. We can use the TTL value and the IP ID field in the ICMP reply packet to distinguish all kinds of Linux kernels.

The advantage of this testing model is its simplicity because it uses the tree structure. Its disadvantage is that it needs enormous data collection to construct a practical protocol tree. On the other hand, with the increase of new types of systems, the protocol tree will become rather bulky and complicated, which will in turn lead to low speed for the query and therefore, affect efficiency.

5 Summary

The paper has made in-depth analysis and study on the application of ICMP in network scanning. By experimenting and testing the features and functions of all kinds of ICMP data packets, it summarizes effective detection methods for OS recognition. On this basis, it puts forward a scanning model based on ICMP protocol for OS recognition and analyzes its working principles and features.

References

[1]PROTOCOLNUMBERS[EB/OL].http://www.iana.org/assignments/protocol-numbers, 2001-12

[2]Request for Comments[EB/OL].http://www.Ietf.org/rfc.html, 2000-3

[3]George Kurtz, Hacking Exposed. Network Security Secrets & Solutions [M], McGraw-Hill Companies, 2001

[4]Douglas E. Comer & David L. Stevens, Internet working With TCP/IP [M], Prentice Hall, 1999

[5]Mingtian Zhou, Wenyong Wang, The Theory of TCP/IPNetwork and Its Techniques,Tshinghua Univ. Publisher,1996.

[6]Xiaobing Zhang,Wangjia Yan,Analysisof Hacker and Its Defence Technologies,Tshinghua Univ. Publisher,1999.

[7]Yuanmin Nie,Ping Qiu,Network Security Technologies, Science Publisher,2001.

[8]Peter Norton, Mike Stockman,Handbook of Network Securities,2002.

Profile of the authors

Jiang Weihua (1973-), male, a native of Anhui Province, lecturer, Ph.D. Field of study: computer networks, information and network security.

Li Weihua (1951-), male, a native of Hubei Province, professor, doctoral mentor. Field of study: computer networks, intelligence decision supporting system, information and network security, network and multimedia communications.

Dujun (1979-), male, a native of Anhui Province, MS. Field of study: information and network security, network and multimedia communications.