The Research of Advanced Evasion Attack Method Based On Metasploit And Fragroute

Hong Xia [1, a], Yajuan Xi [1, b] and Qianqian Pei [1, c]
[1] north china electric power university, Beijing, China
[2] north china electric power university, Beijing, China
[3] north china electric power university, Beijing, China

[a]summerday@ncepu.edu.cn, [b]juanyaxi@163.com, [c]peiqianqian1@126.com

Keywords: vulnerability; metasploit; evasion technology; fragroute; attack

Abstract. With the upgrading of network defense technology, network attacks are constantly refurbished. This paper studies the vulnerabilities and advanced evasion attack, using open source Metasploit and fragroute proposed and constructed a new model with evasion attack technology, at the same time, and gives the way to increase the means of attack and evasion. And testing the attack effectiveness of the model, the results show that this way of attack with evasion technology can effectively detect the defensive performance of network protection equipment.

INTRODUCTION

With the rapid development of internet, people from your network convenient ,at the same time, all kinds of attacks on computer networks become more and more. Evasion[1] means is a technique using a variety of ways to disguise attack to avoid network protection equipment testing, recording and audit. With the vulnerability mining technology matures, more and more vulnerabilities are discovered and published. The current network protection device can successfully avoid 91% of the known vulnerabilities, however, when faced with vulnerability attack added evasion technology , its performance is poor.

This paper studies the vulnerabilities and advanced evasion attack, using open source Metasploit and fragroute proposed and constructed a new model with evasion attack technology, at the same time, and gives the way to increase the means of attack and evasion. And testing the attack effectiveness of the model, the results show that this way of attack with evasion technology can effectively detect the defensive performance of network protection equipment.

The Analysis of Attack and Evasion Technology

There are a lot of loopholes in current network attack, 40% of the attack using the technology of evasion. Advanced technology is the way using a vulnerability of the target system as the carrier, adding technology for different levels of evasion, and attacking the target system in order to achieve the target system shell permission. Network protection device is to check the network malformed packets by matching the rules, and find the invasion and aggression. The way to detect the effectiveness of network protection device has the pcap packet replay attack detection and the real code attacks detected. With advances in vulnerability research and technology, the mainstream network protection equipment can identify most of the malicious exploits and close loopholes for the connection service, but due to numerous combinations of advanced evasion technology, network protection equipment can not effectively intercepts and warns to the malicious links and exploit code with evasion technology .

Attack technology analysis. Metasploit is not just a tool, but also a comprehensive framework platform to provide infrastructure support for the automated implementation of the classic, conventional or novel attacks[4]. It allows testers to easily choose the modules of the penetration

attack, payload and encoder modules and conduct easy penetration attacks. Testers can also further write and test updated attack module in the metasploit basis.

Metasploit working principle: first of all, the attacker send the exploit codes containing payload to the target machine. After if exploit code is successfully executed, the attack payload code starts to execute. After the successful implementation of the payload attack, the attacker has access to the target system, then you can on the target machine to upload and download data operation, such as uploading a virus, open the back door, download file that contains the password [5].The attack process is shown in Figure 1.

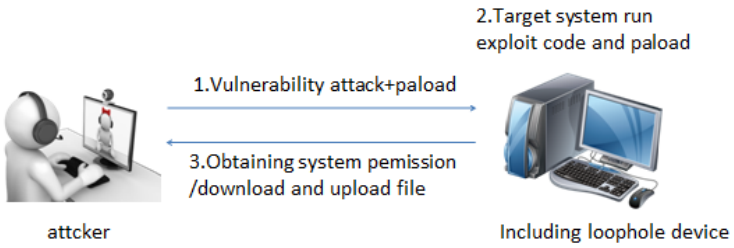

Fig. 1 Metasploit exploits Schematic figure

In the Metasploit framework, users can not only use existing exploit code, you also write and use their own exploit codes. Metasploit classes and methods have good readability and inheritance and use meta programming ideas, so that users can easily and quickly conduct secondary development.When modifying exploit, payload and other modules in Metasploit, users can directly find the corresponding file , modification and save. after restarting the console users can see the own module. Increases exploit, auxiliary modules in Metasploit, the most efficient method is modeled on an existing module format, using the protocol that Metasploit provided. After the module is written in the corresponding directory, we can use the new module in the Metasploit.

Evasion technology analysis. Advanced technology is focused on escaping atoms can evasion any combination. Currently found in 49 species of atoms evasion, the model can be combined as shown in Table 1.

Table 1 Evasion atomic composition table

TCP/IP	evasion protocol	The number of atoms evasion	evasion technology portfolio theory numerical
Application	HTTP，NetBIOS/SMBMSRPC…	≥27	$\geq 2^{49} = 2^{27+16+6}$
Transport	Tcp…	≥16	
Network	Ip…	≥6	

So far, these simple evasion techniques in some cases can still be an effective evasion.Fragroute is a software used to cheat network protection devices, which can handle the data stream sent from local to the remote place, fragroute can be able to intercept, modify and rewrite the outward sending message and have most of the spoofing technologies for the network protection devices, including IP, TCP layer and packet data fragmentation, overlapping,etc.Fragroute has good encapsulation and inheritance.We can increase the mod module that fragroute unrealized, and integrate the new module into fragroute. By increasing and improving mod module, fragroute can possess all known evasion methods. so fragroute can avoid all known methods.

In this paper, the framework fragroute added random_tcp_seg module, TCP segment size can be set to a certain range to achieve the purpose of evasion. The module Process shown in Figure 2.

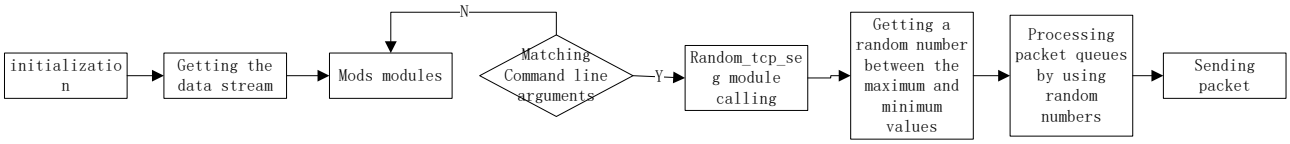

Fig. 2 random_tcp_seg module flow figure

Implementation of attack and evasion model

Overall framework includes scanning, attack, and the adding of evasion.

Vulnerability. This article will use the MS08_067 super vulnerability to perform. This vulnerability is broke having super powerful and high lethal int the end of 2008. The exploit use the target machine port that is the default open 445 SMB service port sending malicious data to the port to cause buffer overflow .Finally, attacker can get the remote target system permission and control the remote system of the target machine.

In VMware [6]virtual machine, building a windows target system possessing ms08-067[7,8] vulnerability and using the MSF on the host machine(kali system) attacks the target system. Network protection devices use snort (open source Intrusion Detection System). In snort, we can observe that when we not use the advanced evasion system, protection devices can prevent attacks, after opening the evasion system ,protection devices can not prevent attacks successfully, test environmental shown in Figure 3.

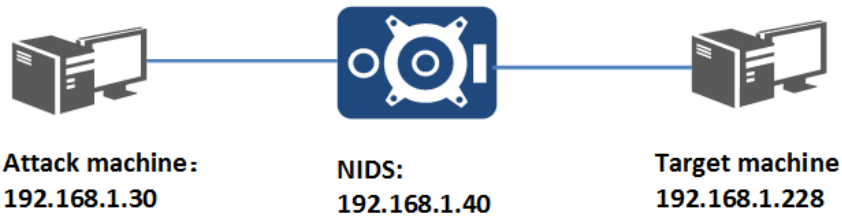

Fig. 3 Setting up test environment figure

Exploit process.1）In the MSF, using windows / windows / smb / ms08-067_netapi load MS08-067 vulnerability module and set the parameters in the command line .

2）Setting snort between the attacker and the target machine to detect the attack aircraft to send data streams setting IP 192.168.1.40 to snort and using routing mode.

3）After setting the parameters, using the exploit command conduct penetration attack. through the echo information ,we can see that when the evasion system does not open ,the attack is failed and intercepted by snort, as shown in Figure 4 and figure 5.

```
Matching Modules
================

   Name                                 Disclosure Date  Rank   Description
   ----                                 ---------------  ----   -----------
   exploit/windows/smb/ms08_067_netapi  2008-10-28       great  MS08-067 Microsoft Serv
er Service Relative Path Stack Corruption


msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set rhost 192.168.1.228
rhost => 192.168.1.228
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.31:4444
[-] Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.1.228:445) was
 unreachable.
msf exploit(ms08_067_netapi) >
```

Fig. 4 attack failure figure

```
Dec 14 17:37:15 rockyvirtuald7 snort: [1:2465:7] NETBIOS SMB-DS IPC$ share acces
s [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 10.0.200
.8:10030 -> 10.0.200.13:445
Dec 14 17:37:15 rockyvirtuald7 snort: [1:2008722:1] ET EXPLOIT Microsoft Windows
 NETAPI Stack Overflow Inbound - MS08-067 - Known Exploit Instance (2) {TCP} 10.
0.200.8:10030 -> 10.0.200.13:445
Dec 14 17:37:15 rockyvirtuald7 snort: [1:666677:1] bug {TCP} 10.0.200.8:10031 ->
 10.0.200.13:6049
```

Fig. 5 snort intrusion prevention logs figure

4）Establishing fragroute profile, vim /usr/share/doc/fragroute/1.conf.

Profile content: IP_frag 32 old mean ip fragment size is 32 (fragment size in multiples of 8) Print

5）opening fragroute command： fragroute -f /Downloads/1.conf 192.178.1.228.

6）Using metasploit again attack the target,you can see the attack is successful. From Figure 6,it can be seen that attacker has successfully obtained the target machine shell.

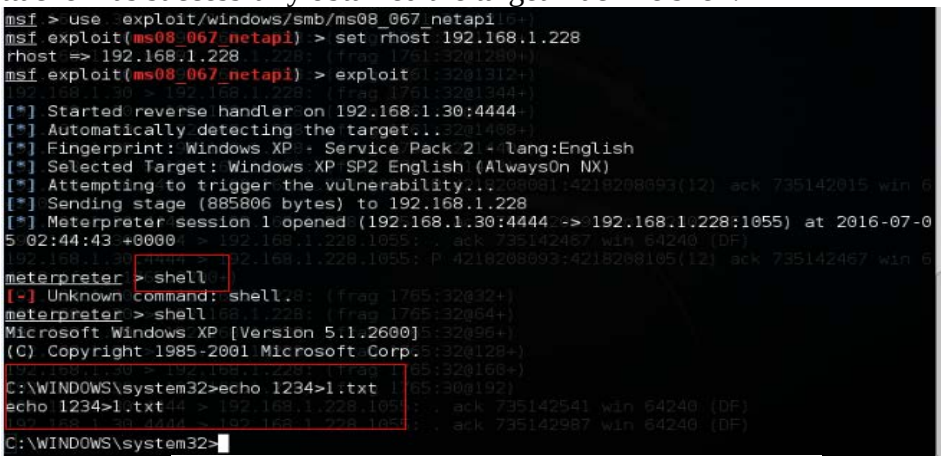

Fig. 6 Opening evasion system successful attack figure

Packet Analysis. Capturing packet by wireshark software, data packets can be seen from the entire attack process containing a three-way handshake, normal conversation, sending data packets including attack stream and the end of session. When turned on ip fragment, you can see the IP fragment packet length is 66, as shown in 7 figure.

11	8.156870	0(192.168.1.228	192.168.1.30	TCP	468	1055→4444 [PSH, ACK] Seq=75 Ack=187 Win=63746 Len=414
12	8.166695	0(192.168.1.30	192.168.1.228	TCP	54	4444→1055 [ACK] Seq=187 Ack=489 Win=64240 Len=0
13	8.214725	0(192.168.1.228	192.168.1.30	TCP	128	1055→4444 [PSH, ACK] Seq=489 Ack=187 Win=63746 Len=74
14	8.227742	0(192.168.1.30	192.168.1.228	TCP	54	4444→1055 [ACK] Seq=187 Ack=563 Win=64240 Len=0
15	8.229099	0(192.168.1.228	192.168.1.30	TCP	208	1055→4444 [PSH, ACK] Seq=563 Ack=187 Win=63746 Len=15
16	8.239193	0(192.168.1.30	192.168.1.228	TCP	54	4444→1055 [ACK] Seq=187 Ack=717 Win=64240 Len=0
17	11.019044	(192.168.1.30	192.168.1.228	IPv4	66	Fragmented IP protocol (proto=TCP 6, off=0, ID=0710)
18	11.019182	(192.168.1.30	192.168.1.228	IPv4	66	Fragmented IP protocol (proto=TCP 6, off=32, ID=0710)
19	11.019264	(192.168.1.30	192.168.1.228	IPv4	66	Fragmented IP protocol (proto=TCP 6, off=64, ID=0710)
20	11.019340	(192.168.1.30	192.168.1.228	IPv4	66	Fragmented IP protocol (proto=TCP 6, off=96, ID=0710)
21	11.019414	(192.168.1.30	192.168.1.228	TCP	64	4444→1055 [PSH, ACK] Seq=187 Ack=717 Win=64240 Len=13
22	11.019710	(192.168.1.228	192.168.1.30	TCP	128	1055→4444 [PSH, ACK] Seq=717 Ack=325 Win=63608 Len=74
23	11.020517	(192.168.1.228	192.168.1.30	TCP	208	1055→4444 [FIN, PSH, ACK] Seq=791 Ack=325 Win=63608 L
24	11.031549	(192.168.1.30	192.168.1.228	TCP	54	4444→1055 [ACK] Seq=325 Ack=791 Win=64240 Len=0

Fig. 7 packet analysis figure

Conclusion

This paper studies the exploits and evasions technology, designing a full attack model with evasion, setting up the environment and conducting recovery attack. In the basis of overall evasion attack model, improving attack and evasion technology and building environment test the mainstream network protection devices to achieve the goal of finally,rapidly improving the performance of network protection devices.

References

[1]Rebecca Bace, Peter Mell, Instrusion Detection Systems[EB/OL],Special Publication 800-31.National Insititute of StaIldards and Technology(NIST), Technology Administration， U.S.Department of Commerce.

[2] Wang Yong,Zhang Xijun,YANG Huihua. one kind of Windows Host Intrusion Detection System [J]. Computer Engineering, 2006,(10): 132-134

[3] Rapid7. Metasploit_InstallationGuide_Windows_4.6.1.pdf. Nov.2013

[4] Zhang Hongrui,Lu Yangang,Feng Xiuyan,Xi Yafeng .Overflow simulation-based MSF Windows system vulnerabilities [J], laboratory research and exploration, 2012,31 (12)

[5] James C. Foster.Buffer Overflow Attacks Dect,Exploit,Prevent.

[6] wu liu,jian-ping wu.hai-xing duan. Constructing efficient network security experimental bed with VMware [J] Computer Applications，2005. In Chinese

[7] James C. Foster.Buffer Overflow Attacks Dect,Exploit,Prevent.

[8] Song Jun, Zhang pick, Song Yang, et al. Windows buffer overflow vulnerability exploit [J], Computer Engineering, 2007, (17): 162-164.