Strategies to Prohibit Intruders Eluding the Detection of Snort through SSH

Siqing Gao
College of information, Linyi Normal University, Shandong Linyi, China
E-mail: Gauss2005@163.com
Pan Qi
China Mobile Shenzhen Company Guangdong Shenzhen
Dihua Liu
Computer science and engineering college, Changchun University of Technology
Changchun, China

Abstract

This paper introduces a method to avoid the detection of snort, a kind of Network Intrusion Detection System (NIDS) software, by using SSH. It also brings up a synthetic strategy, snort collaborating with Intrusion Detection System based on Host(HIDS),to detect this kind of intrusion.

Keywords: Snort , SSH, Intrusion detection, Encrypt

1. Snort Brief introduction

Snort is a cross-platform and lightweight network intrusion detection software. It is one kind of open source code software written by C Language, according to GPL(General Public License).The snort has three kinds of work modes: a Smell explore machine, a wrapping data register, a network intrusion detection system.Smell explore machine mode just reads the wrapping data from network and is successive to flow to the the terminal. The wrapping data register mode with the smell explore machine mode grasp a pack, differently being a wrapping data to write to hard drive daily record.Network's intrusion detection mode is the most complicated, and can be installed. We can make the snort analytical network flowed data to match with some rules of a customer defined, and adopt certain action according to the detection.

Snort mainly detect suspicious discharge through a characteristic, logarithms according the head data of a wrapping data and suspicious clean lotus to match the mode and discover a behavior of intrusion detection from it, for example:Buffer overflows and stealth port scans and CGI attacks and SMB probes etc..It still make use of a statistics packs abnormality detection engine(SPADE) mold to detect no the suspicious discharge of be able to match a characteristic, namely abnormality detection. The latest snort edition is 2.4.3.(Han, Dong-hai, Wang, Chao and Wang, Qun. 2002)

Snort can install at one pedestal machine to carry on surveillance to the whole ether net, through an order to hand over with each other.Snort can be divided into 5 main modules, its data process such as figure 1.Each module is very important to intrusion detection.The first is catch packing equip.It made use of the share characteristic of ether net, because the ether net usage Carrier Sense Multiple Access and Collision Detection (CSMA|CD) technique, adopt a commonly shared channel.Snort makes use of an exterior catching wrap procedure database libpcap(what to use is its Win32 edition winpcap in this text) to grasp a pack.After the original packing data is succeeded in catching ,then being send to the second module-pack decoding machine.Decode machine to translate special agreement chemical element into the internal data structure of the snort system.After at the beginning catching pack to reach agreement code completion, the preprocessor handles discharge.Many Plug-in type preprocessors hand pack over to the next module :Examine engine after carry on check or operation.Examine engine match its rules in order to exame invades of each pack.The last module is a plug-in outputs. It produces an alert to the suspicious behavior.(Jack Koziol, and Wu Bo-feng et al. 2005)

2. SSH and its use

All of SSH Englishes calls to is Secure Shell, is IETF(Internet Engineering Task Force) drawn up a clan negotiate by Network Working Group, its purpose wants on the not- safe network to provide safe telnet and other safe network service.Through using SSH, you can carry on all datas for delivering to encrypt, so attack method in"agent" impossible realization, and can also prevent from DNS and IP beguilement.The attack method of so-called"agent" is "agent" and pretends to be a real server and receives the data that you pass a server, then pretends to be you pass the data to the real server.Server with you of the data of the transmission is turned a hand by"agent", after doing hand and foot,

Will appear a very serious problem.Still additional advantagehave is that the data of delivering is through compressed, so can Accelerate the transmission speed.SSH has very multi-function, it since can replace TELNET, again can for FTP, POP and even PPP provide a safety "passage".

Because of familiar HTTP, FTP, POP3, SMTP, NNTP, and TELNET...etc. much agreement all makes use of expressly to deliver an information in the network, the aggressor of internal network can keep watch on you very easily of the whole conversation process, including user's name, password, mail contents etc. now a lot of audit systems and intrusion detection system(IDS) of internal networks can carry out the information on the application layer.so the application of these agreement is very insecurity.

The following is to make use of the Snort2.0 obtains FTP application data in the log:

```
02|24-09:31:34.939428 172.18.25.108:1038 -> 172.18.25.110:21
TCP TTL:128 TOS:0x0 ID:239 IpLen:20 DgmLen:50 DF
***AP*** Seq:0xD072FE65    Ack:0x7C2C7FFF    Win:0x4455    TcpLen:20
55 53 45 52 20 71 69 70 0D 0AUSER qip..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
02|24-09:31:34.946834 172.18.25.110:21 -> 172.18.25.108:1038
TCP TTL:128 TOS:0x0 ID:304 IpLen:20 DgmLen:72 DF
***AP*** Seq:0x7C2C7FFF    Ack:0xD072FE6F    Win:0xFFF5    TcpLen:20
33 33 31 20 50 61 73 73 77 6F 72 64 20 72 65 71    331 Password req
75 69 72 65 64 20 66 6F 72 20 71 69 70 2E 0D 0A    uired for qip...
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
02|24-09:31:35.169671 172.18.25.108:1038 -> 172.18.25.110:21
TCP TTL:128 TOS:0x0 ID:240 IpLen:20 DgmLen:40 DF
***A**** Seq:0xD072FE6F    Ack:0x7C2C801F    Win:0x4435    TcpLen:20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
02|24-09:31:40.245848 172.18.25.108:1038 -> 172.18.25.110:21
TCP TTL:128 TOS:0x0 ID:241 IpLen:20 DgmLen:53 DF
***AP*** Seq:0xD072FE6F    Ack:0x7C2C801F    Win:0x4435    TcpLen:20
50 41 53 53 20 39 31 32 30 31 38 0D 0APASS 912018..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
```

We can clearly obtain the customer's account number and password from the above data analysis, so the way FTP delivers its statements overtly shows great risks.

More popular SSH tool is a SSH2 now.SSH2 not only support encrypt of deliver to the user's name and the password, and can carry out a public key authentication mechanism.When the client to link with SSH2 servers, will automatically receive the public key that the server carries, use this public key to encrypt to the user's name and the password while verifying, the server is decrypted with his own private key and carry on a comparison, prove whether the customer inputed a correct password.If adopting a public key verification, the customer carries them and wants right to upload the server of needing the interview, this method is safer than the ex-1 kind.

3. Make use of SSH to Evade Snort Examination Experiment

Although SSH is a kind of good and safe data delivers tool, but some malice invaders can make use of SSH to break Snort supervision and bring hidden danger to the network.Use SSH to encrypt to the instruction, can keep Snort from Sniffer access of the real delivering data, so making use of this method can evade the examination of Snort2.0.

We give some concrete experiments below to explain this kind of elusion process.

The server host installed F-Secure SSH Server, provide service in 22 ports, moreover still installed Snort2.0, the movement was intrusion detection mode.Customer's machine installed F-Secure SSH Client.

The F-SECURE supports 3 kinds of conjunctions of modes, the second is so-called SFTP.SFTP uses the SSH connect tunnel of 22 ports to delives document, the whole process only have a port 22 work in the long range, with traditional FTP's needing active and passive portses to work compare ,it is a different mode, so very safety and easily control.

After Linking the server for the first time, we need to accept the KEY document(Public Key) to save locally.After keeping the server public key, then inputing an user's name to carry on an identification.After attestation completes, we need to provide the client 's password of the long range host to make sure the identity of the client.If the password is correct, then we can get into SFTP mode.In this experiment, it delivers a malicious executable programe from customer's interface. In the whole process, Snort has never produced alert document. Open the log catalogue of Snort2.0, the recorded data delivers process as follows:

```
02/24-09:57:40.611775 172.18.25.108:1036 -> 172.18.25.110:22
TCP TTL:128 TOS:0x0 ID:193 IpLen:20 DgmLen:128 DF
***AP*** Seq: 0x580C45B5 Ack: 0x5BBB23D Win: 0x4470 TcpLen: 20
A6 DA 9A A3 20 C4 6F AD 37 21 A6 0C 48 22 46 62 .... .o.7!..H"Fb
33 0C C8 AE D0 D3 0C 59 3C 1C 83 DA D9 EC EB 72   3......Y<......r
DE DB A4 31 28 A7 21 75 1C 5D 1D 4B 41 83 26 6E   ...1(.!u.].KA.&n
9A D2 C4 1F 2B 7C ED 83 B5 7F 7F 08 C3 96 6A 9E   ....+|........j.
C4 91 A1 32 F3 3E 54 FB 7D EB C4 F7 43 E8 6F 79   ...2.>T.}...C.oy
67 73 2D 99 25 C1 76 7B                           gs-.%.v{
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
02/24-09:57:40.612673 172.18.25.110:22 -> 172.18.25.108:1036
TCP TTL:128 TOS:0x0 ID:550 IpLen:20 DgmLen:136 DF
***AP*** Seq: 0x5BBB23D Ack: 0x580C460D Win: 0xFE27 TcpLen: 20
AC 55 64 F8 8E C0 79 50 EC 2E A9 45 52 83 B2 40 .Ud...yP...ER..@
05 26 62 A0 C4 79 D7 65 37 63 5F EE 6D A5 BC 1D .&b..y.e7c_.m...
54 1C 4E F3 9C AF AA 3B B5 0F 5B F6 FA BD 74 AD T.N....;..[...t.
CC B5 0C DC 0B 01 00 20 21 C5 83 4A F6 46 7E 55 ....... !..J.F~U
89 F2 C5 5B F3 F9 82 61 E6 2B D9 10 B2 D0 45 1B ...[...a.+....E.
87 B5 EF 38 2E E5 B4 DB 42 90 F4 52 73 CE DB 74 ...8....B..Rs..t
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
```

It is thus clear that Snort can only obtain disorderly code form of application layer data after encrypting, but it can not discover a real data.Even the client add malicious code this transmission, Snort then can not identifies them in time either, also can not make use of mode match method to detect the invasion.

4. Counterplans

Current Snort is use of sniffer capture form, mainly in the way of matching by the mode examination and analysis invade, but it can not handle and analytical wrapping data after encrypting.SSH can adopt 1024 bite RSAs to carry on a data operation, Snort basically can not break.If aggressor then slowly and soon scan and much change the shell code, and fragment overlap...etc. evades the knot of examination method handiness to put together, still can very easyly evade a Snort examination.

However from above test we can see, the SSH application carries at the client -server mode.The customer carries if want to carry to carry on a safety and encrypt correspondence with server, have to acquire the identity attestation of the server carries.If oneself's machine up installed a SSH server, have to strictly work well each item to defend to invade measure, can not make the invader easily obtained SSH the applied legal power of service.

For canning in time examine a invade that make use of SSH, the following severals order is need to be noticed:

(1) Allocation reasonable fire wall

The fire wall contributes to protecting a computer, prevent unauthorized users access to computer access through the network or Internet.

In the Evade experiment above, if the host opened a installed perfect fire wall, client need a long time to get into an user's name verification, some time basically can not carry on a verification, so the good fire wall is the first barrier for a system safety.

(2) enabled antivirus software update

when a SSH's encrypted information attain a server, has to carries on decrypting with the private key of server, so all client original informations will pass by the system memory of the server host. Antivirus software enabled memory monitoring, vulnerability monitoring, file monitoring and other functions, to find the disease in a timely alarm.The memory supervision can supervise and control the running procedure of the computer, when discoves a virus running can obstruct it’s running and clearance in time;The loophole attack supervision can intercept the attack which make use of system loophole in the computer ;The document supervision can supervise and control whether the document in the computer is been infected by the virus and keep virus from dissemination through thedocument.

(3) The software of SSH server carries use 22 as the default port, but this constitution can be changed and suggest that changing to a secret port is more safe, can lower several rates that the quilt invader makes use of.

(4) Intrusion detection system Snort according to the network and other intrusion detection system based on host add each other, Snort can as early as possible provide the warning of aiming at the attack, while the host part then can make sure whether the attack succeeds.

HDIS can completely control a customer's behavior

HDIS mainly throuth surveillance and analysis audit record and log document of host to examine invades. Log include not and usually on the system and proof of don't expect activity.These proof can point out that someone is invading or has already successfully invaded system. Throuth inspect a log document, can discover the attempt of invade or successfully invade, and very soon start correspond meet an emergency to respond to procedure.In addition, HDIS can monitor system, affairs, safe record on Windows NT and system record in UNIX environment, discover suspicious behavior from it.Many HDISs still wiretap the activity of host port, and report to the managing person when the particular port is visited.(Luo Shou-shan. 2005)

HDIS can also supervise and control some activities of system very easily, such as to the access of the sensitive document, catalogue and procedure or the port.For example it can examine all circumstance of customer logging and withdraws, can also monitor the implementation of the non-normal behavior that usually a managing person only can carry out. Snorts basically could not monitor these activity, but HDIS can report invade in time.The most important one is, because of HDIS install at host whith wanting to supervise and control, so still can collect information which in environment of SSH encrypted.

The HIDS main advantage includes:

(1)Be applicable to encrypt and exchange environment very much.

(2)Near solid of examination and should answer.

(3)Don't need additional hardware.

Snort and HIDS all have respectively of advantage, both add mutually. These two kinds of methods can discover the other party can not examine of some invade behavior. Snort carry on an detection through checking head of pack and payload, while HIDS doesn't look into the head of a pack .Many refused serve attack and fragment attack according to the IP, can only be identified through looking into the pack head that they deliver through a network. Snort can study the contents of load, check to seek order or phrasing to be used in the particular attack, such attacks can be quickly identified by Snort real-time checks packet sequences.And HIDS can not see a load, therefore can not also identify embedded load attacks. Unite an usage according to the host and according to network these two kinds of methods can attain better examination effect. For example HIDS uses the daily record of system as an examination basis, therefore they compare with Snort to have larger accuracy while making sure if the attack has already obtained success. In this aspect, HIDS is good to add to Snort, people completely could use Snort to provide to alert in early days, but used HIDS to verify if the attack obtains success. Big parts of bureau area nets in now intrusion detection system, is all way that adopted NIDS and HIDS cooperation, switch part deployment NIDS, at important server host deploy HIDS, protect the host safety. Such as figure 2.

Test verification, this detection system can availably detect invasion which made use of SSH.

5. Conclusion

In this paper, by analyzing Snort should not use the weakness to gain access to encrypted information to avoid the surveillance of the experiment, and for current network intrusion detection system to put forward what time reasonable suggestion. Although the malice invader can make use of the loophole of the NIDS software to evade its examination, However, we do a good job as long as stringent precautions, a adoption synthesizes examination means, all establish examination mold piece from network to hosts, can examine a malice to invade in time.

References

Han, Dong-hai,Wang, Chao and Wang, Qun. (2002). Intrusion Detection System Analysis examples. 1st edition, Beijing:Tsinghua University Press,2002:42-45 .

http://www.51cto.com/html/2005/1125/12248.htm .

http://www.snort.org/

Jack Koziol, and Wu Bo-feng et al. (2005). Snort Intrusion Detection integrated solutions. The first edition, Beijing: Mechanical Industry Press, 2005: 35.

Luo, Shou-shan. (2004). Intrusion Detection. 1st edition, Beijing: Beijing University of Posts and Telecommunications Press, 2004 :21-22.

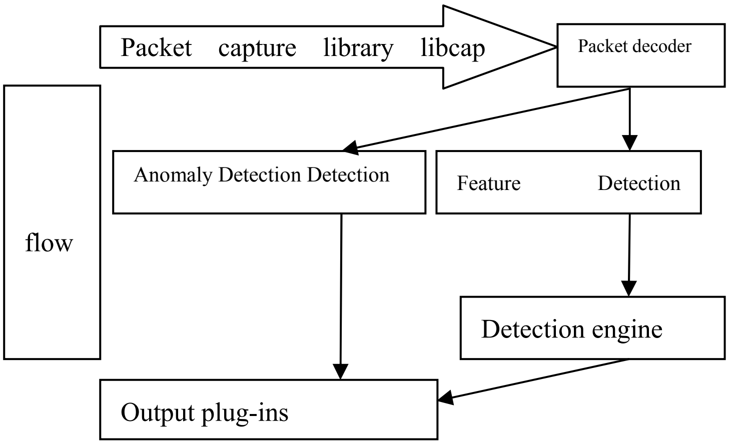

Figure 1. Snort data flow chart

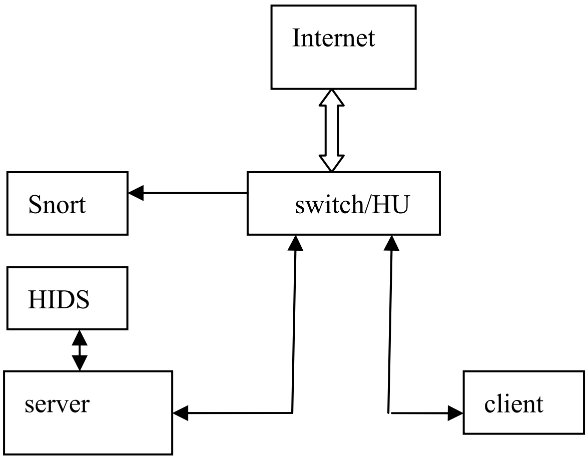

Figure 2. sketch plan of LAN intrusion detection system