DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4583

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

DEPLOYMENT OF LOW INTERACTION HONEYPOT IN A PRIVATE NETWORK

Jashanpreet Singh Toor
Department of Computer Engineering
Punjabi University,
Patiala,India

Er. Abhinav Bhandari
Department of Computer Engineering
Punjabi University,
Patiala,India

Abstract: A honeypot is a security system whose value lies in being probed ,attacked .A honeypot is forcefully made to be attacked to gather information about unauthorized activity Our research paper provides a brief explanation of such a system and demonstrate how it can be implemented to improve security of the organization and across critical systems and networks. In the experiment performed in this paper, such a trap is laid in the form of a low interaction honeypot deployed using pentbox 1.8 framework in a private network. The results of deployment are presented.

.

Keywords: Honeypot, network, IDS

1. INTRODUCTION

As the organizations are becoming more and more dependent upon their network infrastructures, these network infrastructures are becoming more and more complicated for providing the necessary services [1]. Due to this added complicacy in the network architectures to provide seamless automation to the organizational day to day routine work the conventional network security devices are failing to provide the level of comfort required by the network administrators Hence there is a need of a context sensitive approach/technique for the prevention, detection and responding to the attacks performed on these complex networks.

A honeypot is deliberately to be attacked to gather information about unauthorized activity (Kinsella, 2005). An intrusion detection system which generates no alerts may be indicator of normal network activity. However a honeypot that does not get attacked is worthless.

Here in this paper we have done such a study by deploying a low interaction honeypot by using pentbox framework in a private network. The results are presented along with benefits and issues involved in such deployments.

2. WORKING OF HONEYPOTS

The concept of honeypot is quite simple. It acts as a resource which has no productive value, it works by deceiving intruders into believing it to be genuine system with genuine data and they attack the system without knowing that they are being observed completely. [3] Honeypots are, in their most basic form, fake information severs strategically-positioned in a test network, which are fed with false information disguised as files of classified nature. When any external system tries to connect to the honeypot, all of its system related information, such as the IP address of the attacker, operating system, port accessed, browser, version etc. will be collected. Most important part of a honeypot system is capturing data, payloads, packets the ability to keep log, alert, and capture everything the attacker is doing.

Features of a honeypots system as suggested by Bouget & Holz

A. To divert the attention of the attacker from the real network, and making sure that the main server is not compromised.

b. To identify the preferred attack methods used more commonly and make similar profiles of attackers as used by law enforcement agencies in order to identify a criminal.

c. To capture new attack entities for future study

d. To identify new vulnerabilities and risks of various operating systems, environments and programs which are not thoroughly identified at the moment [4]

In a more advanced context, a group of Honeypots becomes a Honeynet. It acts as a tool that monitors wide group of possible threats which gives a systems administrator more information for study. It makes the attack more fascinating for the attacker due to the fact that Honeypots can increase the possibilities, targets and methods of attack [5].

HONEYPOT DESIGN AND ITS DEPLOYMENT ISSUES.

On the basis of design deployment of the Honeypot, it can be divided into Production and Research Honeypot [6]

A. Production Honeypot

These honeypots are used to protect the organizations in real production operating environments [7], constant attacks 24/7. These honeypots are constantly gathering more importance due to the detection tools they provide and because of the way they can complement network and host protection. This type of honeypots emulates specific services and sometimes even operating systems to lure the attackers..

A honey pot cannot prevent an unpredictable attack but can detect it. One case where they prevent the attacker is when he directly attacks the server. It will prevent attack on a production system by making the hacker waste his time on a non-sufficient target. [8].

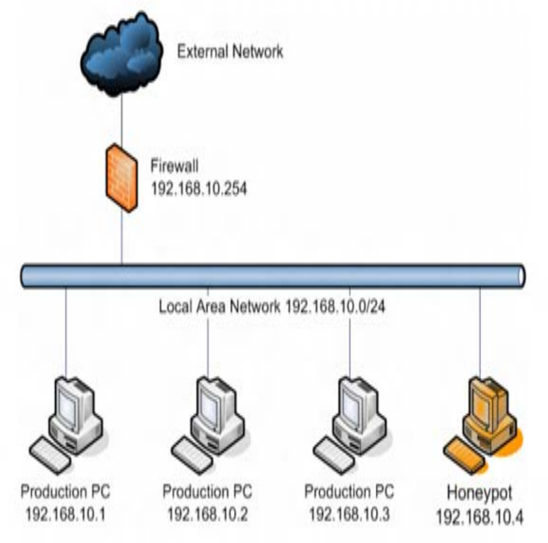


Fig1: Honeypot inside the network

B. Research Honeypot

Research honeypot collects important information about the nature of attacks, their motives and methods and tools used by attackers. Honeypot provides detailed information of the attack i.e. how attack happens, tools used by attackers etc. It is used to research the threats organizations face, and to learn how to provide better protection against those threats.
According to the level of interaction of the honeypot [9], it can be divided into low, medium and high interaction honeypots

C. Low Interaction Honeypot

Low interactive honeypots are system which emulates the services and are easy to configure, deploy and setup and has lower interaction performance, It helps to detect known vulnerabilities and measure how often attackers attack

D. Medium Interaction Honeypot

This honeypot deceive the attacker with providing fake interfaces of the attacker and then stores all the activities done by attacker against different services. A medium interaction honeypot is somewhat advance than low interaction honeypot . These can range from simple port listener to a complex complete host just sitting on a network waiting to be attacked.

E. High Interaction Honeypot

These system provide real service to the intruders and full OS access to them.As attacker can get root access so the risk associated with these honeypots is the maximum.

PENTBOX 1.8 FRAMEWORK

Pentbox is a framework that consists of security and stability testing oriented tools that are commonly used in networking. It is developed in ruby and oriented to GNU/Linux systems, but is compatible with every systems where Ruby works.
Tools in pentbox 1.8 :

I .Cryptography tools

- Base64 Encoder & Decoder
- Multi-Digest (MD5, SHA1, SHA256, SHA384, SHA512, RIPEMD-160)
- Hash Password Cracker (MD5, SHA1, SHA256, SHA384, SHA512, RIPEMD-160)
- Secure Password Generator

II .Network tools

- Net DoS Tester
- TCP port scanner
- Honeypot
- Fuzzer
- DNS and host gathering
- MAC address geolocation (samy.pl)

III .Web

- HTTP directory brute force
- HTTP common files brute force

3. HONEYPOT ARCHITECTURE AND CONFIGURATION

A monitoring infrastructure needs to be deployed in a well-controlled lab environment consisting of sensor, honeypot server as well as a logging server. One more sensor Wireshark will be working with the honeypot at the server.

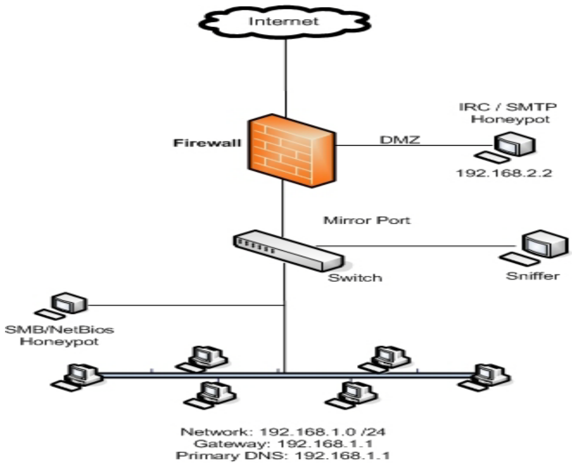


Fig 2 Architecture of honeypot in a network

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark helps us understand what is happening in our network on a microscopic level.

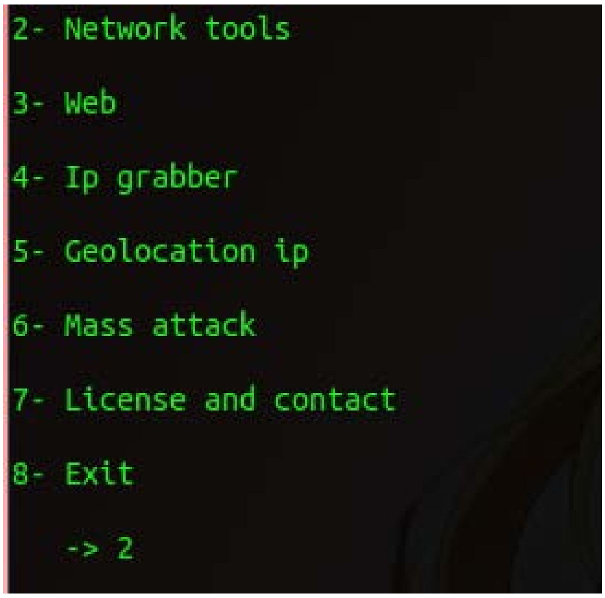
Configuration of honeypot.

We have used Ubuntu operating system for setting up the server. After firing up the terminal we start the pentbox 1.8 framework .Pentbox honeypot will only work if we give sudo privileges.

First go to the pentbox directory and the path of its ruby module.

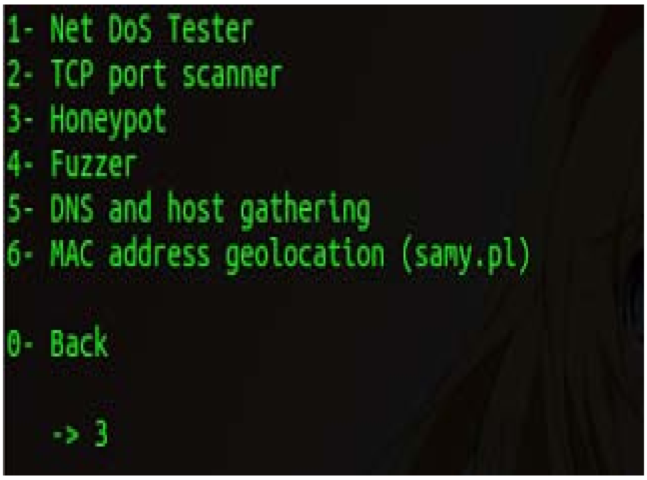
```
Cd pentbox-1.8 / sudo ./pentbox.rb
```

Then select option **2. Network Tools**.



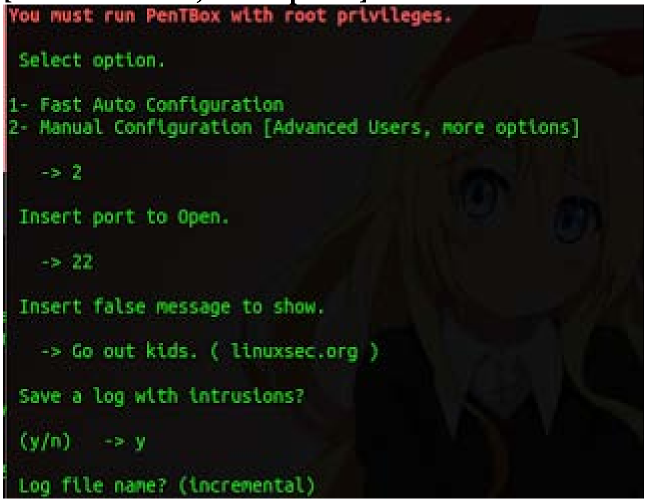
```
2- Network tools

3- Web

4- Ip grabber

5- Geolocation ip

6- Mass attack

7- License and contact

8- Exit

   -> 2
```

Next select number **3. Honeypot**.



```
1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)

0- Back

   -> 3
```

Then select the number 2- **Manual Configuration [Advanced Users, more options]**

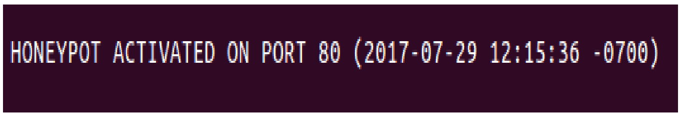


```
You must run PenTBox with root privileges.

 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   -> 2

 Insert port to Open.

   -> 22

 Insert false message to show.

   -> Go out kids. ( linuxsec.org )

 Save a log with intrusions?

 (y/n)   -> y

 Log file name? (incremental)
```

.

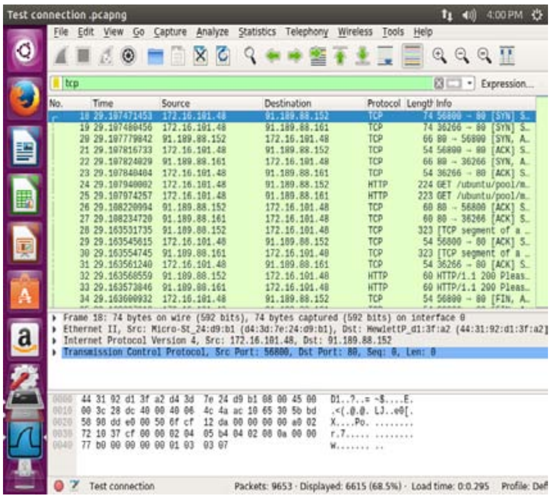
Enter the port, message, and also where the log file will be stored.

Start Wireshark and then click on the network interface you want to use to capture the data. On a wired network, it will likely be eth0. On the honeypot we use wireshark to monitor the network traffic .We have activated honeypot on port 80



```
HONEYPOT ACTIVATED ON PORT 80 (2017-07-29 12:15:36 -0700)
```

Port 80 is the port number assigned to commonly used internet communication protocol, Hypertext Transfer Protocol (HTTP). It is the port from which a computer sends and receives Web client-based communication and messages from a Web server and is used to send and receive HTML pages or data



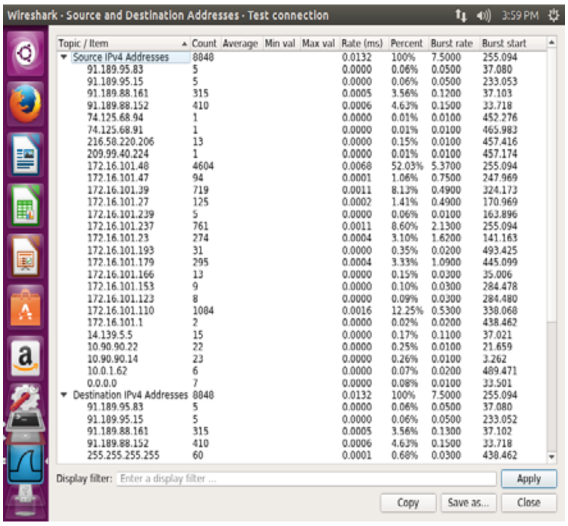
Test connection .pcapng
4:00 PM
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Expression...

```
No.  Time          Source          Destination     Protocol Length Info
  18 29.107471453  172.16.101.48   91.189.88.152   TCP       74 56800 → 80 [SYN] S…
  19 29.107480456  172.16.101.48   91.189.88.161   TCP       74 36266 → 80 [SYN] S…
  20 29.107779842  91.189.88.152   172.16.101.48   TCP       66 80 → 56800 [SYN, A…
  21 29.107816733  172.16.101.48   91.189.88.152   TCP       54 56800 → 80 [ACK] S…
  22 29.107824029  91.189.88.161   172.16.101.48   TCP       66 80 → 36266 [SYN, A…
  23 29.107840404  172.16.101.48   91.189.88.161   TCP       54 36266 → 80 [ACK] S…
  24 29.107940002  172.16.101.48   91.189.88.152   HTTP     224 GET /ubuntu/pool/m…
  25 29.107974257  172.16.101.48   91.189.88.161   HTTP     223 GET /ubuntu/pool/m…
  26 29.108220994  91.189.88.152   172.16.101.48   TCP       60 80 → 56800 [ACK] S…
  27 29.108234720  91.189.88.161   172.16.101.48   TCP       60 80 → 36266 [ACK] S…
  28 29.163531735  91.189.88.152   172.16.101.48   TCP      323 [TCP segment of a …
  29 29.163545615  172.16.101.48   91.189.88.152   TCP       54 56800 → 80 [ACK] S…
  30 29.163554745  91.189.88.161   172.16.101.48   TCP      323 [TCP segment of a …
  31 29.163561240  172.16.101.48   91.189.88.161   TCP       54 36266 → 80 [ACK] S…
  32 29.163568559  91.189.88.152   172.16.101.48   HTTP      60 HTTP/1.1 200 Pleas…
  33 29.163573846  91.189.88.161   172.16.101.48   HTTP      60 HTTP/1.1 200 Pleas…
  34 29.163600932  172.16.101.48   91.189.88.152   TCP       54 56800 → 80 [FIN, A…

▸ Frame 18: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: Micro-St_24:d9:b1 (d4:3d:7e:24:d9:b1), Dst: HewlettP_d1:3f:a2 (44:31:92:d1:3f:a2)
▸ Internet Protocol Version 4, Src: 172.16.101.48, Dst: 91.189.88.152
▸ Transmission Control Protocol, Src Port: 56800, Dst Port: 80, Seq: 0, Len: 0

0000  44 31 92 d1 3f a2 d4 3d  7e 24 d9 b1 08 00 45 00   D1..?..= ~$....E.
0010  00 3c 28 dc 40 00 40 06  4c 4a ac 10 65 30 5b bd   .<(.@.@. LJ..e0[.
0020  58 98 dd e0 00 50 6f cf  12 da 00 00 00 00 a0 02   X....Po. ........
0030  72 10 37 cf 00 00 02 04  05 b4 04 02 08 0a 00 00   r.7..... ........
0040  77 b0 00 00 00 00 01 03  03 07                     w....... ..

Test connection      Packets: 9653 · Displayed: 6615 (68.5%) · Load time: 0:0.295    Profile: Def
```

Fig3 Screen shot of Real time capture of tcp packets using Wireshark.

The server is usually the IP the TCP SYN packets are sent to, while the source of the SYN packets in the client. So you could filter on the SYN packets using "tcp.flags==2" and see which IPs are targeted.

One way is to click Statistics>Conversations this will open a new window and you can click ipv4 or tcp option to check out the Destination IP/src IP/src port/dst port



Wireshark · Source and Destination Addresses · Test connection
3:59 PM
Display filter: Enter a display filter ...
Apply
Copy
Save as...
Close

```
Topic / Item                 Count  Average  Min val  Max val  Rate (ms)  Percent  Burst rate  Burst start
▾ Source IPv4 Addresses      8848                              0.0132     100%     7.5000      255.094
    91.189.95.83             5                                 0.0000     0.06%    0.0500      37.080
    91.189.95.15             5                                 0.0000     0.06%    0.0500      233.053
    91.189.88.161            315                               0.0005     3.56%    0.1200      37.103
    91.189.88.152            410                               0.0006     4.63%    0.1500      33.718
    74.125.68.94             1                                 0.0000     0.01%    0.0100      452.276
    74.125.68.91             1                                 0.0000     0.01%    0.0100      465.983
    216.58.220.206           13                                0.0000     0.15%    0.0100      457.416
    209.99.40.224            1                                 0.0000     0.01%    0.0100      457.174
    172.16.101.48            4604                              0.0068     52.03%   5.3700      255.094
    172.16.101.47            94                                0.0001     1.06%    0.7500      247.969
    172.16.101.39            719                               0.0011     8.13%    0.4900      324.173
    172.16.101.27            125                               0.0002     1.41%    0.4900      170.969
    172.16.101.239           5                                 0.0000     0.06%    0.0100      163.896
    172.16.101.237           761                               0.0011     8.60%    2.1300      255.094
    172.16.101.23            274                               0.0004     3.10%    1.6200      141.163
    172.16.101.193           31                                0.0000     0.35%    0.0200      493.425
    172.16.101.179           295                               0.0004     3.33%    1.0900      445.099
    172.16.101.166           13                                0.0000     0.15%    0.0300      35.006
    172.16.101.153           9                                 0.0000     0.10%    0.0300      284.478
    172.16.101.123           8                                 0.0000     0.09%    0.0300      284.480
    172.16.101.110           1084                              0.0016     12.25%   0.5300      338.068
    172.16.101.1             2                                 0.0000     0.02%    0.0200      438.462
    14.139.5.5               15                                0.0000     0.17%    0.1100      37.021
    10.90.90.22              22                                0.0000     0.25%    0.0100      21.659
    10.90.90.14              23                                0.0000     0.26%    0.0100      3.262
    10.0.1.62                6                                 0.0000     0.07%    0.0200      489.471
    0.0.0.0                  7                                 0.0000     0.08%    0.0100      33.501
▾ Destination IPv4 Addresses 8848                              0.0132     100%     7.5000      255.094
    91.189.95.83             5                                 0.0000     0.06%    0.0500      37.080
    91.189.95.15             5                                 0.0000     0.06%    0.0500      233.052
    91.189.88.161            315                               0.0005     3.56%    0.1300      37.102
    91.189.88.152            410                               0.0006     4.63%    0.1500      33.718
    255.255.255.255          60                                0.0001     0.68%    0.0300      438.462
```

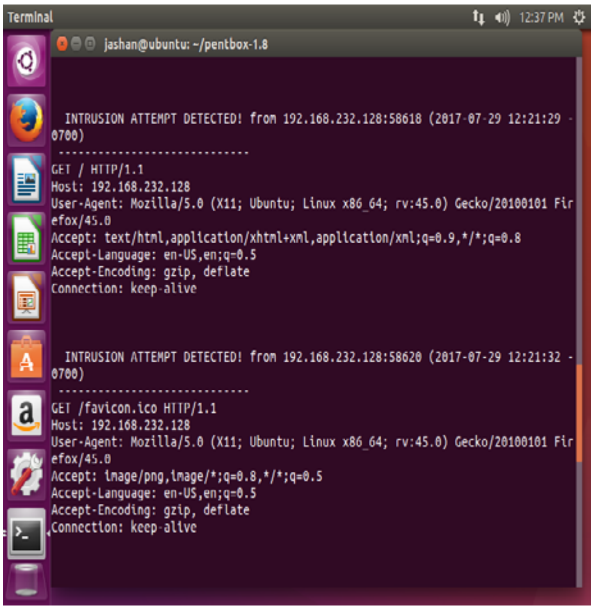
Fig4 Screenshot of Wireshark statistical analysis for source and destination addresses.

4. RESULT AND CONCLUSION

After the service runs we will see how pentBox will record every connection made.

Honeypots, by definition, see only "bad" traffic. Honeypots only report the connections they receive and most of these will be real attacks. Whenever a system tries to connect with the honeypot server, the server records its information.

.



```
  INTRUSION ATTEMPT DETECTED! from 192.168.232.128:58618 (2017-07-29 12:21:29 -
0700)
 -----------------------------
GET / HTTP/1.1
Host: 192.168.232.128
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:45.0) Gecko/20100101 Fir
efox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive


  INTRUSION ATTEMPT DETECTED! from 192.168.232.128:58620 (2017-07-29 12:21:32 -
0700)
 -----------------------------
GET /favicon.ico HTTP/1.1
Host: 192.168.232.128
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:45.0) Gecko/20100101 Fir
efox/45.0
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

Fig 5 Screen shot of Honeypot showing the information about every connection that is detected.

Information recorded by our honeypot.

INTRUSION ATTEMPT DETECTED! From 192.168.232.1:52419 (2017-07-29 12:16:03 -0700)

GET / HTTP/1.1

Host: 192.168.232.128

Connection: keep-alive

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,/*;q=0.8*

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.8

INTRUSION ATTEMPT DETECTED! From 192.168.232.128:58618 *(2017-07-29 12:21:29 -0700)*

GET / HTTP/1.1

Host: 192.168.232.128

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv: 45.0) Gecko/20100101 Firefox/45.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/*; q=0.8*

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: keep-alive

After knowing which IPs are trying to attack, we can do prevention by blocking the ip or applying our tools as required. As you can see, we now know where the attacker came from, what exploit method was used and the time the exploit was attempted.

Honeypots can be used in securing the network of an organisation. Honeypots acts as early alarming tools to secure the organization technologies. Still IDS technology is not such powerful to protect global information infrastructure completely. In this paper we have reviewed a basic honeypot. Hence we can safely conclude that different types of honeypots can be used to detect different types of attack signatures and rules can be defined to filter the traffic based on information gathered.

REFERENCES

[1] Saurabh Chamotra, J.S.Bhatia, Raj Kamal, A. K. Ramani "Deployment of a Low Interaction Honeypot in an Organizational Private Network" IEEE 2011.

[2] QassimNasir and Zahraa A. Al-Mousa "Honeypots Aiding Network Forensics: Challenges and Notions",(Journal of Communications Vol. 8, No. 11, November 2013

[3] Carlos Francisco Lerma Reséndez, Miguel Hernández y López "Honeypots: Basic Concepts, Classification and Educational Use as Resources in Information Security Education and Courses" Informing Science & IT Education Conference (InSITE) 2008

[4] Spitzner, L. (2002). Honeypots: Tracking hackers Boston: Addison-Welsey.

[5] http://www.honeynet.org.pt/index.php/HoneyMole

[6] John Harrison,J.H (2003) Honeypots: The sweet spot in network security.

[7] Miguel Hernández y López .(2008). Honeypots: Basic Concepts, Classification and Educational Use as Resources in Information Security Education and Courses. Proceedings of the Informing Science & IT Education Conference (InSITE) 2008

[8] http://www.infosec.gov.hk/english/technical/files/honeypots

[9] Neha Sahu, Vineet Richhariya 'Honeypot: A Survey' IJCST Vol. 3, Issue 4, Oct - Dec 2012

[10] Mohd. Junedul Haque "An Approach for Intrusion Detection using Honeypots to Improve Network Security" (IJRASET-2015)