Mahmood, J Comput Sci Syst Biol 2018, 11:3
DOI: 10.4172/jcsb.1000275

Journal of
Computer Science & Systems Biology

Research Article Open Access

The Use of Honeynets to Detect Exploited Systems Across the Wireless Networks

Mahmood I*

CS Department, Aptech Computer Education, Wah Cantonment, Punjab, Pakistan

Abstract

Any to internet is target of hackers and intruders. Every organization/institution system connected uses some kind of network security software to protect its data from unauthorized use. Software's used by organization/institution are antivirus firewall etc. There are many types of services that are run on organization/institution networks and it is important to detect intrusion. Due to large bandwidth, monitoring is very hard and impossible. In developing, where the cyber-crimes are very easy to commit and there are not very strong lows Honeynet scheme, is use to help system administrator in detecting intrusion or malicious content. Honey net is so proposed solution because it helps in understanding the intention and ways attacker use to compromise security systems. In this paper a basic honeynet framework is proposed.

Keywords: Cyber; Cyber crime; Hacking; Intrusion detection; Honeynet

Introduction

Honeynet is not tool used for offence or defense. It allows us to measure flaws or vulnerabilities in our system. Honeynet provide an information gathering approach to security; there sole purpose is to gather Information about threats in the network. A Honeynet is an interactive type of honeypot which provides real systems and application for attackers to attack and thus capture real information on a real attack [1]. Technically the Honeynet is only deception. They deceive the attacker that he is conquering the real systems or applications. But there every activity is closely watched and monitored. this information is used to improved the system security and avoid such attacks in future. Honeypot can be used as another security layer to the network as the firewalls and network intrusion detection systems (NIDS) but they have some limitations. Limitations are that firewalls are placed on the edges of network [2]. Which receives the data traffic from internet to internal network and vice visa, they have the capability to monitor the information which is coming from internet but they are not able to monitor the traffic which is generated within the organization. Some attacker can also bypass the firewall by simply doing encryption due to which data analysis becomes useless. if there is problem of encrypted data then we have to improve the IDS to collect the encrypted data and use security measures to decrypt the data for analysis Keeping in view honeynet is best possible solution, which is not only reliable but also inexpensive.

Honey net is a better solution because it is set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security [3,4]. secondly the value of this solution is an easy and cost effective Honeynet for research and development [5].

Related Work

Honeynet are classified on the basis of how attacker is allowed to penetrate in our system. In literature honeynet are classified into two types (Table 1).

Low interaction honeynet

In this scenario a false environment is provided to attacker nothing to do with our actual environment. This approach is also very careful approach in which we are not very sure that up to what extent we would be able to protect our system from attacker. By playing safe we are able to collect data from given set of environment variables. but this is not as effective as it should be because we are using false system not actual environment. A low-interaction honeynet uses emulated systems and applications for the attacker and the system usually uses some scripts to respond to the hacker's activities. They are easy to deploy and most of their output is data or log files, which can be used to study attack pattern. This is used for future design of IDS. There is very low risk involved in deploying the Low-interaction honeynet. Drawback can be full extent of damage on real system can be assumed only [6].

High interaction honeynet

This is aggressive approach which allows the attacker to penetrate in a system. The attacker is allowed to attack on real time environment which actually exist in our organization. The attacker is allowed to have actual servers and applications to play with but he is monitored very carefully. Log file are created for future use and for crating pattern or signature based IDS. The benefit of using High interaction honeynet is collection of real time data [7,8]. Give the detail of a low-interaction honeynet, developed by Niels Provos, Honeyd which is designed to run

Features	Low-interaction honeynet	High interaction honeynet
Knowledge to Develop	Low	Mid high
Knowledge to Run	Low	High
Risk	Low	High
Real Operating System	No	Yes
Degree of Involvement	Low	High
Maintenance Time	Low	Very high

Table 1: A comparison between High interaction and low interaction Honeynet.

***Corresponding author:** Mahmood I, CS Department, Aptech Computer Education, Wah Cantonment, Punjab, Pakistan, Tel: +923345127920; E-mail: Im_mah2002@yahoo.com

Received March 16, 2018; **Accepted** May 03, 2018; **Published** May 06, 2018

Citation: Mahmood I (2018) The Use of Honeynets to Detect Exploited Systems Across the Wireless Networks. J Comput Sci Syst Biol 11: 219-223. doi:10.4172/jcsb.1000275

primarily on unix systems, Honeyd works on the concept of monitoring unused IP space. Anytime it sees a connection attempt to an unused IP, it intercepts the connection and then interacts with the attacker, pretending to be the victim. By default, Honeyd detects and logs any connection to any UDP or TCP port. In addition, you can configure emulated services to monitor specific ports, such as an emulated FTP server monitoring TCP port 21. When an attacker connects to the emulated service, not only does the honeynet detect and log the activity, but it captures all of the attacker's interaction with the emulated service. In the case of the emulated FTP server, we can potentially capture the attacker's login and password, the commands they issue, and perhaps even learn what they are looking for or their identity. It all depends on the level of emulation by the honeynet [9]. Most emulated services work the same way. They expect a specific type of behavior, and then are programmed to react in a predetermined way. If attack A does this, then react this way. If attack B does this, then respond this way. The limitation is if the attacker does something that the emulation does not expect, then it does not know how to respond. Most low-interaction honeynet, including Honeyd, simply generate an error message [10-12].

A high-interaction honeynet is a conventional computer system, such as a commercial off-the-shelf (COTS) computer, a router, or a switch. This system has no conventional task in the network and no regularly active users. Thus, it should neither have any unusual processes nor generate any network traffic besides the regular daemons or services running on the system. These assumptions aid in attack detection. Every interaction with one of our honeynets is suspicious and could point to a possibly malicious action. This absence of false positives is one of the key advantages of high-interaction honeynet compared to intrusion detection systems (IDS). To quote Rutherford D. Roger, "We are drowning in information and starving for knowledge." This may be a common phenomenon for IDS, but not for honeynet [13].

Further says that High interaction honey pot can be used to collect in-depth information about the procedures of an attacker. We can observe the "Reconnaissance phase" that is, how he searches for targets and with which techniques he tries to find out more about a given system. Afterward, we can watch how he attacks this system and which exploits he uses to compromise a machine. And finally, we can also follow his tracks on the honeynet itself. We monitor which tools he uses to escalate his privileges, how he communicates with other people, or the steps he takes to cover his tracks. Altogether, we learn more about the activities of an attacker his tools, tactics, and motives. This is an interesting field, and this methodology has proven to be successful in the past. For example, we were able to learn more about the typical procedures of phishing attacks and similar identity theft technique since we observed several of these attacks with the help of high-interaction honeynet.

Proposed Honeynet Framework

Honeynet work step by step using following techniques.

Data control

This very important function when implementing Honeynet, It is required that attacker feels that he is free to launch an attack. It is important to implement different data control layers (Figures 1 and 2) [13].

- Counting outbound connections.
- Intrusion prevention gateways.
- Bandwidth restrictions.

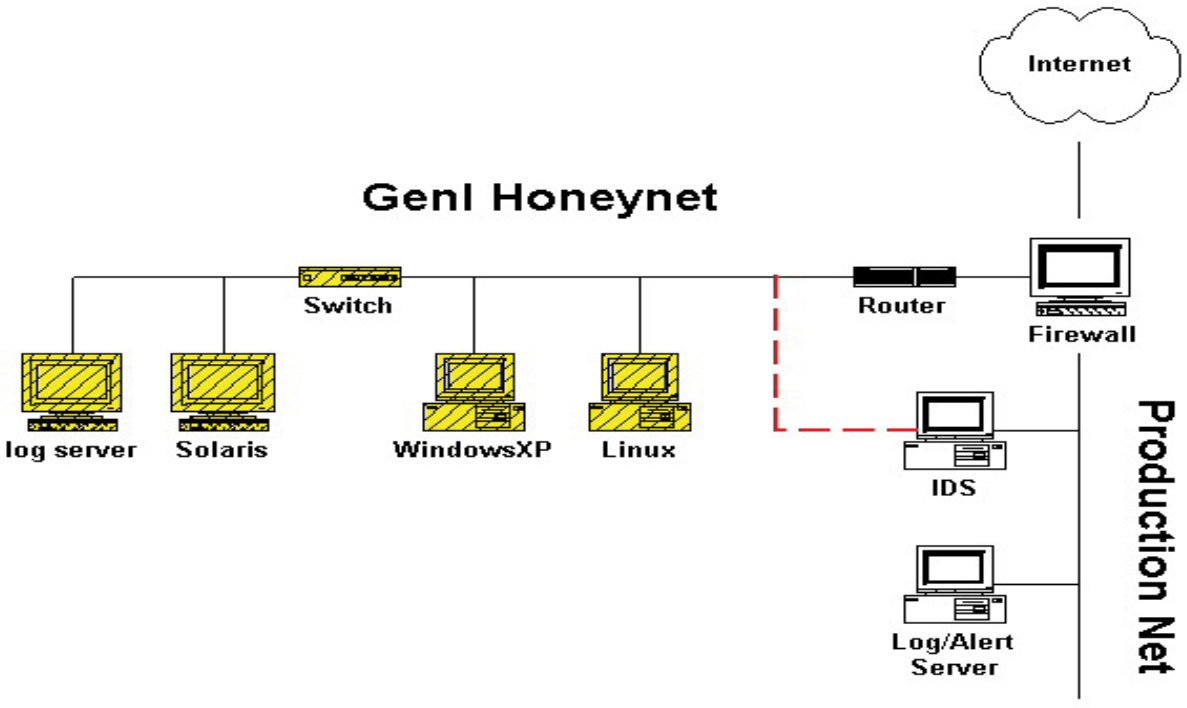


Figure 1: Frame work overview.

Data capture

There should be process of data collection which collects data of attack on Honeynet by attacker. The data is monitored and analyzed log file should be maintained for future use these log files can also be used as proof of his attacks. Many tools can be used to captured the data examples can be Wireshark, sebek etc here W3af is used to collect the data about iqra website. Result indicate uninterrupted data capture from Iqra university for 12 minutes 30 seconds.

An intrusion detection system

Very important part of Honeynet is IDS software called snort is used which is between the internet and Honeynet l. It generates alerts and reports the data traffic (Figure 3).

Firewall logging

Firewall is used to log all data traffic coming in and out of Honeynet. Also maintains log files for connections denied or refused (Figure 4).

Data analysis

The final part of Honeynet is data analysis which is very important and final part in making a complete report of attacks and there pattern. Based upon the input data log attacker is blocked (Figures 5 and 6) [13].

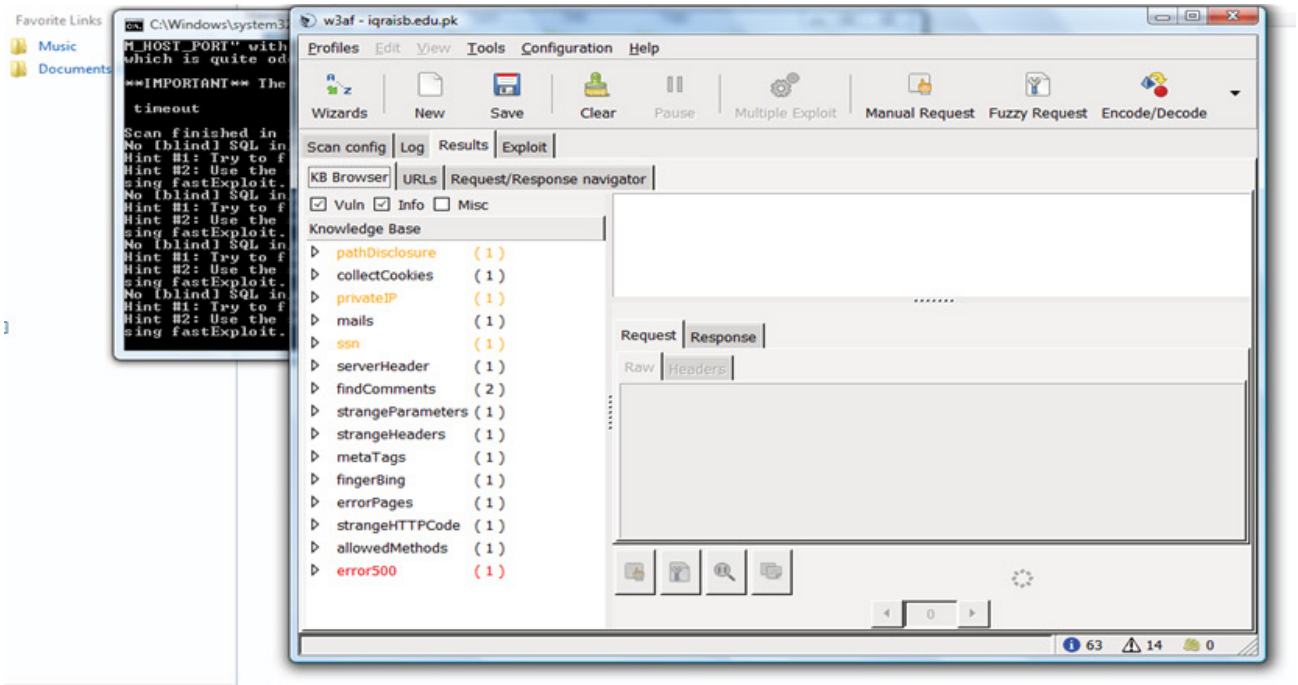
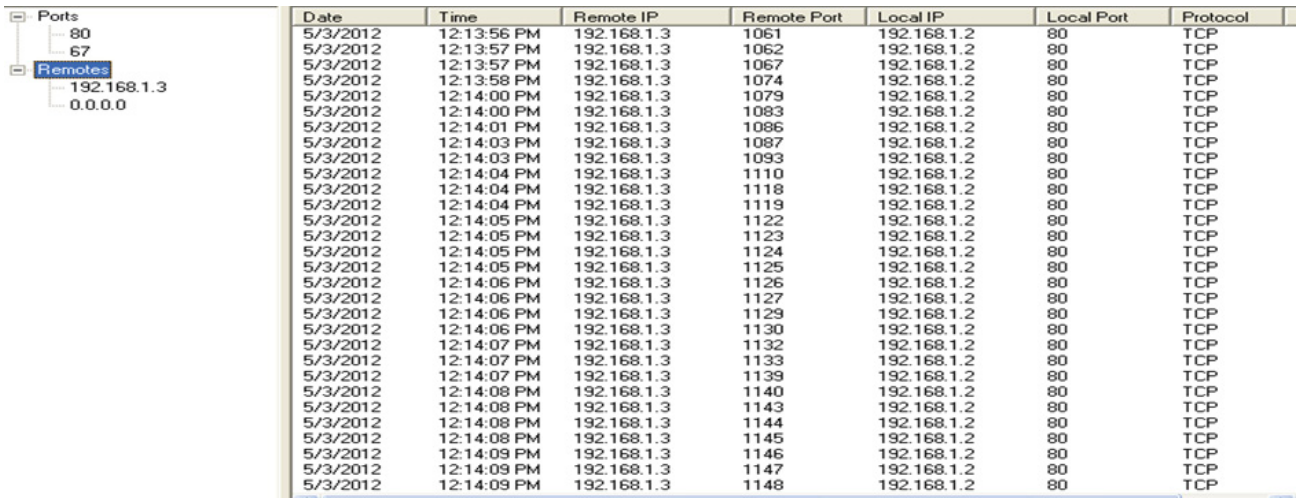
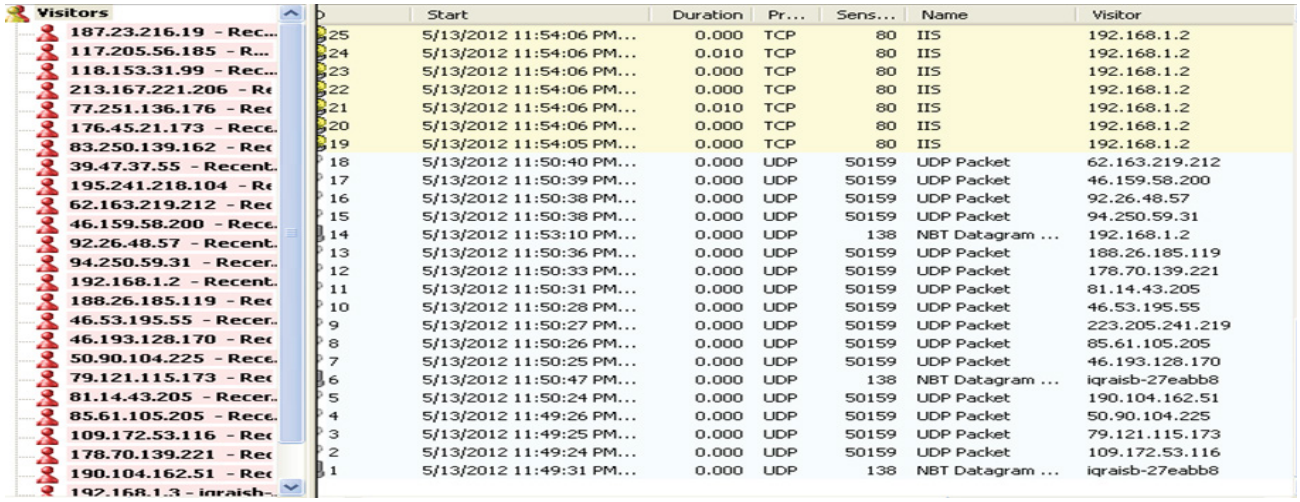


Figure 2: W3af Data capture results.



Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol
5/3/2012	12:13:56 PM	192.168.1.3	1061	192.168.1.2	80	TCP
5/3/2012	12:13:57 PM	192.168.1.3	1062	192.168.1.2	80	TCP
5/3/2012	12:13:57 PM	192.168.1.3	1067	192.168.1.2	80	TCP
5/3/2012	12:13:58 PM	192.168.1.3	1074	192.168.1.2	80	TCP
5/3/2012	12:14:00 PM	192.168.1.3	1079	192.168.1.2	80	TCP
5/3/2012	12:14:00 PM	192.168.1.3	1083	192.168.1.2	80	TCP
5/3/2012	12:14:01 PM	192.168.1.3	1086	192.168.1.2	80	TCP
5/3/2012	12:14:03 PM	192.168.1.3	1087	192.168.1.2	80	TCP
5/3/2012	12:14:03 PM	192.168.1.3	1093	192.168.1.2	80	TCP
5/3/2012	12:14:04 PM	192.168.1.3	1110	192.168.1.2	80	TCP
5/3/2012	12:14:04 PM	192.168.1.3	1118	192.168.1.2	80	TCP
5/3/2012	12:14:04 PM	192.168.1.3	1119	192.168.1.2	80	TCP
5/3/2012	12:14:05 PM	192.168.1.3	1122	192.168.1.2	80	TCP
5/3/2012	12:14:05 PM	192.168.1.3	1123	192.168.1.2	80	TCP
5/3/2012	12:14:05 PM	192.168.1.3	1124	192.168.1.2	80	TCP
5/3/2012	12:14:05 PM	192.168.1.3	1125	192.168.1.2	80	TCP
5/3/2012	12:14:06 PM	192.168.1.3	1126	192.168.1.2	80	TCP
5/3/2012	12:14:06 PM	192.168.1.3	1127	192.168.1.2	80	TCP
5/3/2012	12:14:06 PM	192.168.1.3	1129	192.168.1.2	80	TCP
5/3/2012	12:14:06 PM	192.168.1.3	1130	192.168.1.2	80	TCP
5/3/2012	12:14:07 PM	192.168.1.3	1132	192.168.1.2	80	TCP
5/3/2012	12:14:07 PM	192.168.1.3	1133	192.168.1.2	80	TCP
5/3/2012	12:14:07 PM	192.168.1.3	1139	192.168.1.2	80	TCP
5/3/2012	12:14:08 PM	192.168.1.3	1140	192.168.1.2	80	TCP
5/3/2012	12:14:08 PM	192.168.1.3	1143	192.168.1.2	80	TCP
5/3/2012	12:14:08 PM	192.168.1.3	1144	192.168.1.2	80	TCP
5/3/2012	12:14:08 PM	192.168.1.3	1145	192.168.1.2	80	TCP
5/3/2012	12:14:09 PM	192.168.1.3	1146	192.168.1.2	80	TCP
5/3/2012	12:14:09 PM	192.168.1.3	1147	192.168.1.2	80	TCP
5/3/2012	12:14:09 PM	192.168.1.3	1148	192.168.1.2	80	TCP

Figure 3: Honey bot data log.

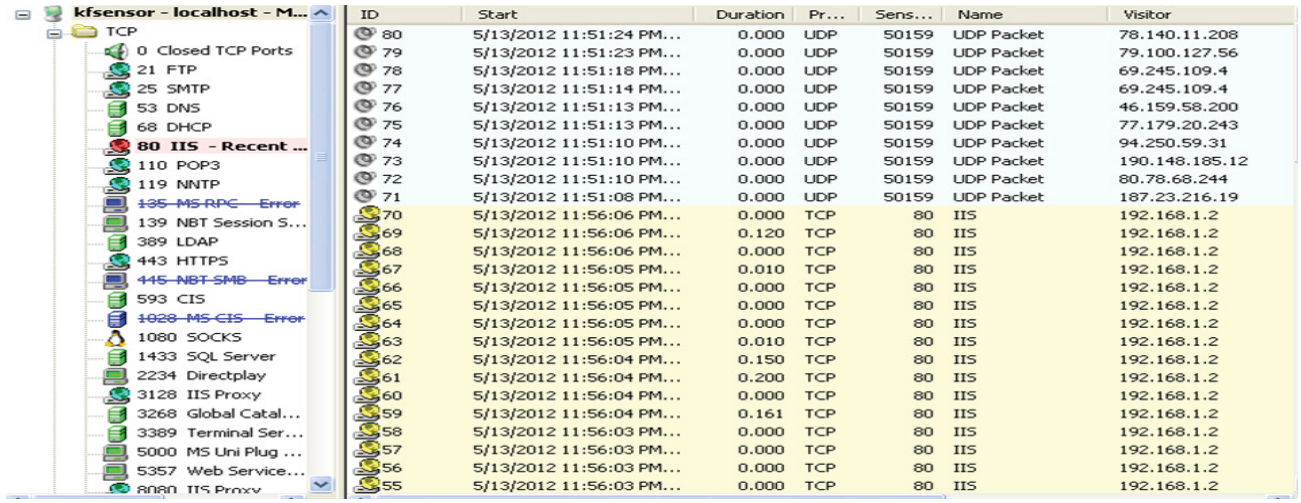


Visitors

187.23.216.19 - Rec...
117.205.56.185 - R...
118.153.31.99 - Rec...
213.167.221.206 - Re
77.251.136.176 - Rec
176.45.21.173 - Rece.
83.250.139.162 - Rec
39.47.37.55 - Recent.
195.241.218.104 - Re
62.163.219.212 - Rec
46.159.58.200 - Rece.
92.26.48.57 - Recent.
94.250.59.31 - Recer.
192.168.1.2 - Recent.
188.26.185.119 - Rec
46.53.195.55 - Recer.
46.193.128.170 - Rec
50.90.104.225 - Rece.
79.121.115.173 - Rec
81.14.43.205 - Recer.
85.61.105.205 - Rece.
109.172.53.116 - Rec
178.70.139.221 - Rec
190.104.162.51 - Rec
192.168.1.3 - igraish-

	Start	Duration	Pr...	Sens...	Name	Visitor
25	5/13/2012 11:54:06 PM...	0.000	TCP	80	IIS	192.168.1.2
24	5/13/2012 11:54:06 PM...	0.010	TCP	80	IIS	192.168.1.2
23	5/13/2012 11:54:06 PM...	0.000	TCP	80	IIS	192.168.1.2
22	5/13/2012 11:54:06 PM...	0.000	TCP	80	IIS	192.168.1.2
21	5/13/2012 11:54:06 PM...	0.010	TCP	80	IIS	192.168.1.2
20	5/13/2012 11:54:06 PM...	0.000	TCP	80	IIS	192.168.1.2
19	5/13/2012 11:54:05 PM...	0.000	TCP	80	IIS	192.168.1.2
18	5/13/2012 11:50:40 PM...	0.000	UDP	50159	UDP Packet	62.163.219.212
17	5/13/2012 11:50:39 PM...	0.000	UDP	50159	UDP Packet	46.159.58.200
16	5/13/2012 11:50:38 PM...	0.000	UDP	50159	UDP Packet	92.26.48.57
15	5/13/2012 11:50:38 PM...	0.000	UDP	50159	UDP Packet	94.250.59.31
14	5/13/2012 11:53:10 PM...	0.000	UDP	138	NBT Datagram ...	192.168.1.2
13	5/13/2012 11:50:36 PM...	0.000	UDP	50159	UDP Packet	188.26.185.119
12	5/13/2012 11:50:33 PM...	0.000	UDP	50159	UDP Packet	178.70.139.221
11	5/13/2012 11:50:31 PM...	0.000	UDP	50159	UDP Packet	81.14.43.205
10	5/13/2012 11:50:28 PM...	0.000	UDP	50159	UDP Packet	46.53.195.55
9	5/13/2012 11:50:27 PM...	0.000	UDP	50159	UDP Packet	223.205.241.219
8	5/13/2012 11:50:26 PM...	0.000	UDP	50159	UDP Packet	85.61.105.205
7	5/13/2012 11:50:25 PM...	0.000	UDP	50159	UDP Packet	46.193.128.170
6	5/13/2012 11:50:47 PM...	0.000	UDP	138	NBT Datagram ...	iqraisb-27eabb8
5	5/13/2012 11:50:24 PM...	0.000	UDP	50159	UDP Packet	190.104.162.51
4	5/13/2012 11:49:26 PM...	0.000	UDP	50159	UDP Packet	50.90.104.225
3	5/13/2012 11:49:25 PM...	0.000	UDP	50159	UDP Packet	79.121.115.173
2	5/13/2012 11:49:24 PM...	0.000	UDP	50159	UDP Packet	109.172.53.116
1	5/13/2012 11:49:31 PM...	0.000	UDP	138	NBT Datagram ...	iqraisb-27eabb8

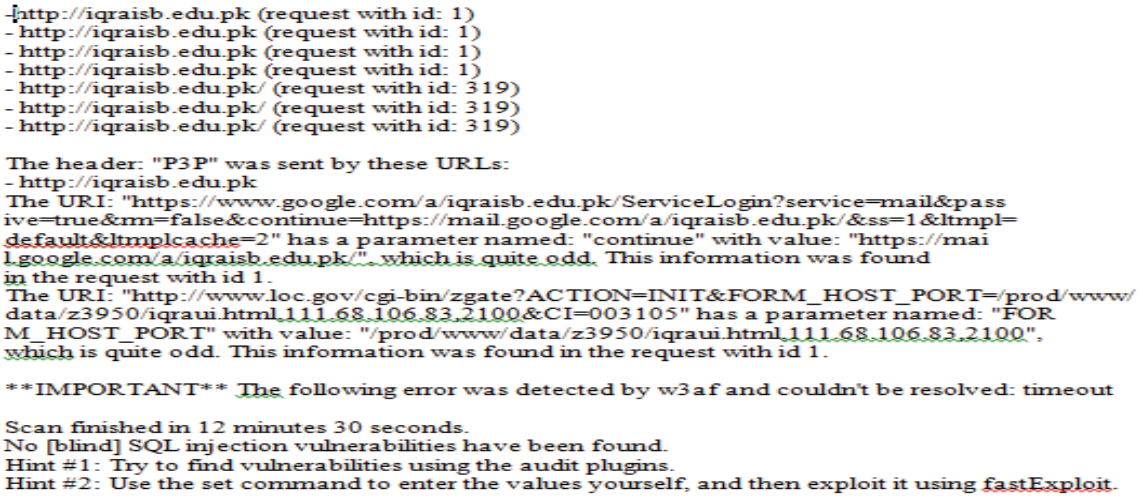
Figure 4: KFSensor firewall log.



kfsensor - localhost - M...
TCP
0 Closed TCP Ports
21 FTP
25 SMTP
53 DNS
68 DHCP
80 IIS - Recent ...
110 POP3
119 NNTP
135 MS RPC - Error
139 NBT Session S...
389 LDAP
443 HTTPS
445 NBT SMB - Error
593 CIS
1028 MS CIS - Error
1080 SOCKS
1433 SQL Server
2234 Directplay
3128 IIS Proxy
3268 Global Catal...
3389 Terminal Ser...
5000 MS Uni Plug ...
5357 Web Service...
8080 IIS Proxy

ID	Start	Duration	Pr...	Sens...	Name	Visitor
80	5/13/2012 11:51:24 PM...	0.000	UDP	50159	UDP Packet	78.140.11.208
79	5/13/2012 11:51:23 PM...	0.000	UDP	50159	UDP Packet	79.100.127.56
78	5/13/2012 11:51:18 PM...	0.000	UDP	50159	UDP Packet	69.245.109.4
77	5/13/2012 11:51:14 PM...	0.000	UDP	50159	UDP Packet	69.245.109.4
76	5/13/2012 11:51:13 PM...	0.000	UDP	50159	UDP Packet	46.159.58.200
75	5/13/2012 11:51:13 PM...	0.000	UDP	50159	UDP Packet	77.179.20.243
74	5/13/2012 11:51:10 PM...	0.000	UDP	50159	UDP Packet	94.250.59.31
73	5/13/2012 11:51:10 PM...	0.000	UDP	50159	UDP Packet	190.148.185.12
72	5/13/2012 11:51:10 PM...	0.000	UDP	50159	UDP Packet	80.78.68.244
71	5/13/2012 11:51:08 PM...	0.000	UDP	50159	UDP Packet	187.23.216.19
70	5/13/2012 11:56:06 PM...	0.000	TCP	80	IIS	192.168.1.2
69	5/13/2012 11:56:06 PM...	0.120	TCP	80	IIS	192.168.1.2
68	5/13/2012 11:56:06 PM...	0.000	TCP	80	IIS	192.168.1.2
67	5/13/2012 11:56:05 PM...	0.010	TCP	80	IIS	192.168.1.2
66	5/13/2012 11:56:05 PM...	0.000	TCP	80	IIS	192.168.1.2
65	5/13/2012 11:56:05 PM...	0.000	TCP	80	IIS	192.168.1.2
64	5/13/2012 11:56:05 PM...	0.000	TCP	80	IIS	192.168.1.2
63	5/13/2012 11:56:05 PM...	0.010	TCP	80	IIS	192.168.1.2
62	5/13/2012 11:56:04 PM...	0.150	TCP	80	IIS	192.168.1.2
61	5/13/2012 11:56:04 PM...	0.200	TCP	80	IIS	192.168.1.2
60	5/13/2012 11:56:04 PM...	0.000	TCP	80	IIS	192.168.1.2
59	5/13/2012 11:56:04 PM...	0.161	TCP	80	IIS	192.168.1.2
58	5/13/2012 11:56:03 PM...	0.000	TCP	80	IIS	192.168.1.2
57	5/13/2012 11:56:03 PM...	0.000	TCP	80	IIS	192.168.1.2
56	5/13/2012 11:56:03 PM...	0.000	TCP	80	IIS	192.168.1.2
55	5/13/2012 11:56:03 PM...	0.000	TCP	80	IIS	192.168.1.2

Figure 5: Analysis of data KF sensor.



- http://iqraisb.edu.pk (request with id: 1)
- http://iqraisb.edu.pk (request with id: 1)
- http://iqraisb.edu.pk (request with id: 1)
- http://iqraisb.edu.pk (request with id: 1)
- http://iqraisb.edu.pk/ (request with id: 319)
- http://iqraisb.edu.pk/ (request with id: 319)
- http://iqraisb.edu.pk/ (request with id: 319)

The header: "P3P" was sent by these URLs:
- http://iqraisb.edu.pk

The URI: "https://www.google.com/a/iqraisb.edu.pk/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/a/iqraisb.edu.pk/&ss=1&ltmpl=default&ltmplcache=2" has a parameter named: "continue" with value: "https://mail.google.com/a/iqraisb.edu.pk/", which is quite odd. This information was found in the request with id 1.

The URI: "http://www.loc.gov/cgi-bin/zgate?ACTION=INIT&FORM_HOST_PORT=/prod/www/data/z3950/iqraui.html,111.68.106.83,2100&CI=003105" has a parameter named: "FORM_HOST_PORT" with value: "/prod/www/data/z3950/iqraui.html,111.68.106.83,2100", which is quite odd. This information was found in the request with id 1.

IMPORTANT The following error was detected by w3af and couldn't be resolved: timeout

Scan finished in 12 minutes 30 seconds.
No [blind] SQL injection vulnerabilities have been found.
Hint #1: Try to find vulnerabilities using the audit plugins.
Hint #2: Use the set command to enter the values yourself, and then exploit it using fastExploit.

Figure 6: Data Capture.

Conclusion and Future Work

In this growing IT environment, there is also a need to strengthen its security. Preventive, Detective and Responsive measures have to be undertaken in order to improve IT Security. Technique used in the paper is well defined but the tool uses for instruction detection are not up to mark for an Enterprise environment. there is a need of comprehensive study to generate an integrated set of tools to fully implement the honynet. to detect new exploits launched against the organization/institution network. An area for further research would involve the establishment of a distributed Honeynet across the any Enterprise network.

References

1. Pravesh G (2018) Honeypots-and-Honeynets.
2. Zentyal (2018) Firewall configuration with Zentyal.
3. Spitzner L (2002) Honeypots Tracking Hackers.
4. Spitzner L (2018) Honeypots Tracking Hackers.
5. Warkentin M (2008) Enterprise Information Systems Assurance and System Security Cohen F. Internet Holes - Internet Lightning Rods Network Security Magazine.
6. Cohen F (1992) Operating System Protection Through Program Evolution Computers and Security.
7. Honeynet (2018) The Honeynet Project.
8. Cohen F, Phillips C, Swiler LP, Gaylor T, Leary P, et al. (1998) A Preliminary Classification Scheme for Information System Threat s, Attacks, and Defenses; A Cause and Effect Model; and Some Analysis Based on That Model. The Encyclopedia of Computer Science and Technology.
9. Honeynet (2018) The Honeypet Project.
10. IJCST (2018) Honeypot: A Survey.
11. Atomic Software Solutions (2018) HoneyBOT is a medium interaction honeypot for windows.
12. Honeynet (2018) The Honeypet Project.
13. Honeyd (2018) Honeypot Background.