Darknet Traffic Monitoring using Honeypot

[1]Hemal khorasia,[2]Mr. Girish Khilari
[1]IT Systems & Network Security,
[1]Gujarat Technological University, Ahmedabad, India

***Abstract* - A "Darknet" is a portion of routed, unallocated IP space in which no active services or servers reside. any packet entering a Darknet should not be valid traffic, It could reach it due to errors such as poor security policies The fineness of the Darknet is that it cuts down considerably on the false positives for any device or technology. Darknet monitoring, in which there are no legitimate computers and no reason that legitimate traffic would be monitored. The darknet collects traffic as a result of wide range of events, including misconfiguration (e.g., a human being mis-typing an IP address) High interaction and low-interaction honeypots are trap systems deployed in a darknet that pretend vulnerable computers to attract attacks and collect malware samples. Monitoring network packets on more than one network is important because each network may be biased in the traffic it is receiving. To overcome the bias problem, with distributed multiple networks rather than a single network with large address blocks. We develop network monitoring system for some organization use and try to conduct network monitoring unused address spaces.**

***Index Terms* - DarkIP, honeypot, malware, ids, unused ip, worm, virus, dos, honeyd**

I. INTRODUCTION

As use of internet is increasing exponentially with time, everyone is now trying to get maximum benefit from it. Any organization or individual, whether associated with IT directly or not, use Internet in daily life for different uses. Basically and used to share information not to protect it. So it is security professionals' job to provide the missing feature. Moreover the world is full of bad guys who are eager to exploit any vulnerability as soon an opportunity strikes. Sometimes products and features designed for the benefits of benign end users are used by attackers to exploit loop holes and weaknesses in applications and software.

Now-a-days the products and applications have become so complex it is very difficult to protect them. Security should be provided at various layers. One solution cannot alone provide all the security. Moreover attacks are being advanced and sophisticated in nature. It is very difficult to predict the nature of future attacks and security solutions needed to combat New types of attacks are introduced continuously .So it is required to detect attacks as soon as possible before they harm enterprise or individual beyond repair.[8]

To protect enterprise against threats and attacks ,it is must to provide network security to whole organization. Network security includes any activity designed to secure network. These activities protect the usability ,reliability ,integrity and safety Of network and data. Many network security threats are spread over Internet. The most common include:[6]

- Virus
- Worm
- DOS Attacks
- Trojan Horse
- Identity theft

II. ATTACK MONITORING AND DETECTION SYSTEM USING DARK IPS

it is totally independent monitoring system, No need to communicate with the other machines on the network, so it will not generate ant TCP or UDP packets.

- Monitoring server will be placed in the same intranet where all other systems are placed.[4]
- Monitoring server will receive the packets based on the mac address traffic, so it can also monitor the traffic coming from the internet and traffic coming from the internal network also.[3]

To prepare a Dark IP address spaces, a method in which Monitoring server will automatically defines the Dark IP and monitors traffic destined to that Dark IP. In it real time identification of the Dark IPs based on the ARP requests for the particular IP address. If the machine is up, machine will immediately replies ARP request with its MAC address, if machine is down, the reply of ARP request never responded.

To prepare a Dark IP address spaces, a method in which Monitoring Server will automatically defines the Dark IP and monitors traffic destined to that Dark IP. In it real time identification of the Dark IPs based on the ARP requests for the particular IP address.

If the machine is up, machine will immediately replies ARP request with its MAC address, if machine is down, the reply of ARP request never responded.[11]

III. DARKNET MONITORING USING HONEYPOT

In Darknet Traffic Monitoring using Honeypot there are main three components:

1. Honeyd: Honeyd is a deamon that create more then one honeypot network.honeyd is a collection of honeypot.honeyd can work on many port like FTP,HTTP,SMPT, if we can use honeyd so first it can be configure.honeyd does not intercept any network traffic.honeyd use its own ip address

2.Honeypot: honeypot can used to network designed, not used to create a lots of traffic in the network. so any traffic can enter or leaving a network and it is comes under the rule of detection and prevention that time honeypot can stop that type of attack or malicious activity. Honeypot is a one type of fake system that can attack to the attacker , and it is look like as original system, so any attacker can attack in honeypot so attack can easily identify using their signature and we can protect our original system easily

3. Monitoring server: This server will first create list of Dark IPs excluding the Live IPs from given list. After that, it will start capturing all the traffic destined for Dark IPs and analyze it for any malicious activities. Dark IPs: Here Dark IPs are addresses which have not been allocated to hosts by DHCP server or have been released by hosts. Such IP addresses are scattered between Live IPs and random in nature as shown in figure below.

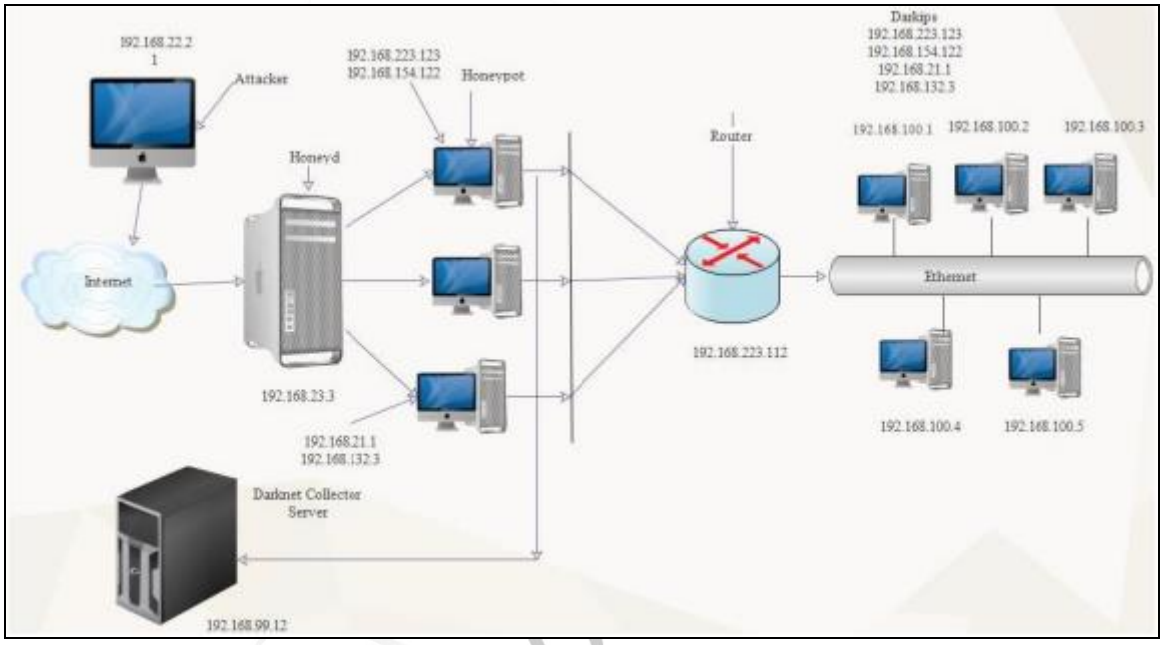


Figure 1 Darknet Monitoring using Honeypot

Honeypot can attract the attacker so we can easaly identified the attackers. we can also used the snort for detecting darkip's or bad traffic and alert the system and also we can analysis that packets and store into our monitoring server. we can block or allow particular ip addresses using iptables or we can also filter addresses, so only good traffic can going to our LAN and our network can easaly safe from unwanted traffic or bad ip addresses.

IV. EXISTING MONITORING SYSTEM OF DARK IP'S

Practical Darknet Measurement[2]

In Darknet Configuration, the method suggested with DHCP and fall through route uses static routing. The subnets used as IMS are continuous and statically configured which is not appropriate in dynamic environment.

Darknet Monitoring on Real Operated Network[5]

They proposed a method for network monitoring which explains unused IP addresses on real-operated network: production network. They considered two major issues.

They have considered to major issues in darknet:

1. Preparing of IP address space for monitoring.
2. Configuration of Monitoring Server.

Problems identified in the existing monitoring system

In self registration algorithm the problems are,

1. Only used for large networks.[7]
2. First divided traffic through router the monitoring perform.[9]
3. large ip address needed to identified attacker.[1]

V. IMPLEMENTATION

IMPLEMENTATION OF MODULE 1

Module 1: Implementation of the proposed Architecture.

Sub Module 1: Configuration of the honeypot and inside honeypot i have configured Honeypot using – honeyd and snort

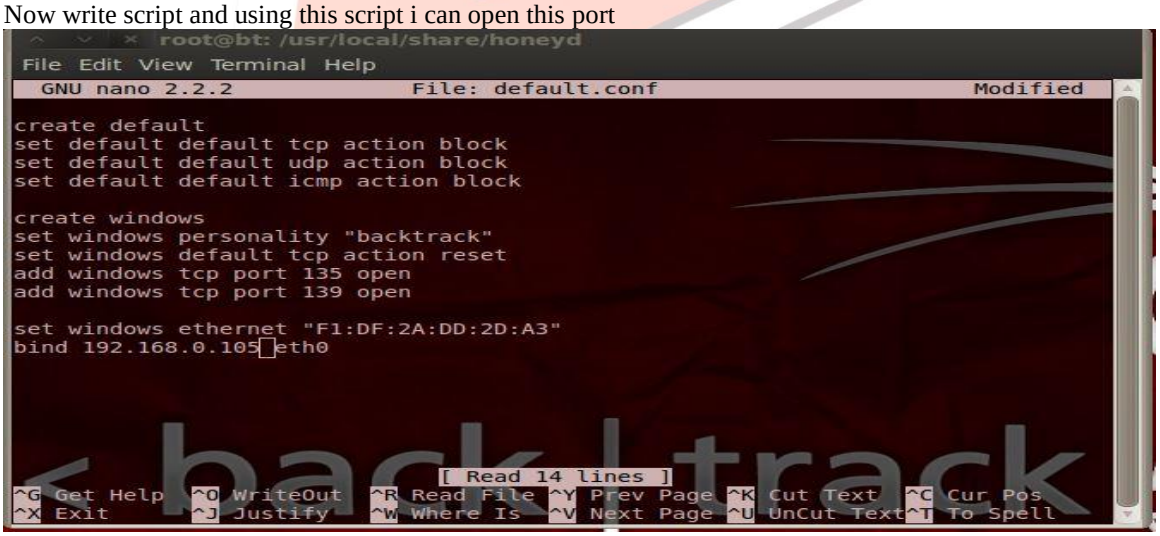
9.1.1 Sub Module 1: Configuration of honeypot

In this phase I used two system
1)backtrack(ip:192.168.0.105)
2)Kali Linux(ip:192.168.0.108)

Now I am create homeypot in backtrack machine and perform port scanning or other attack perform using kali linux and result of scanning port are close.

Display port 135 and 139 are closed

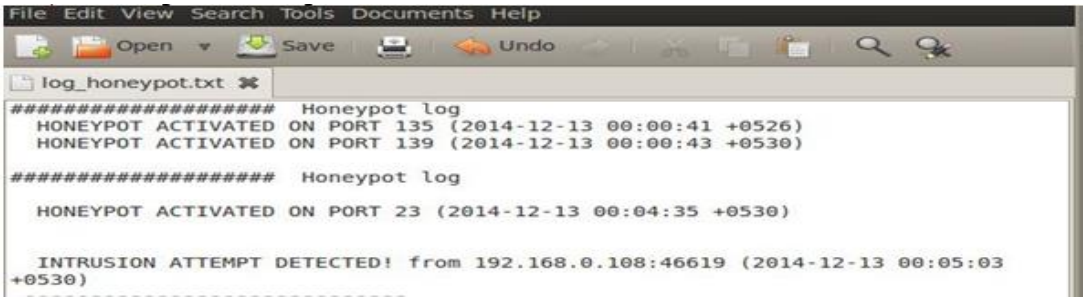
Now write script and using this script i can open this port



script to open port

output of that open port

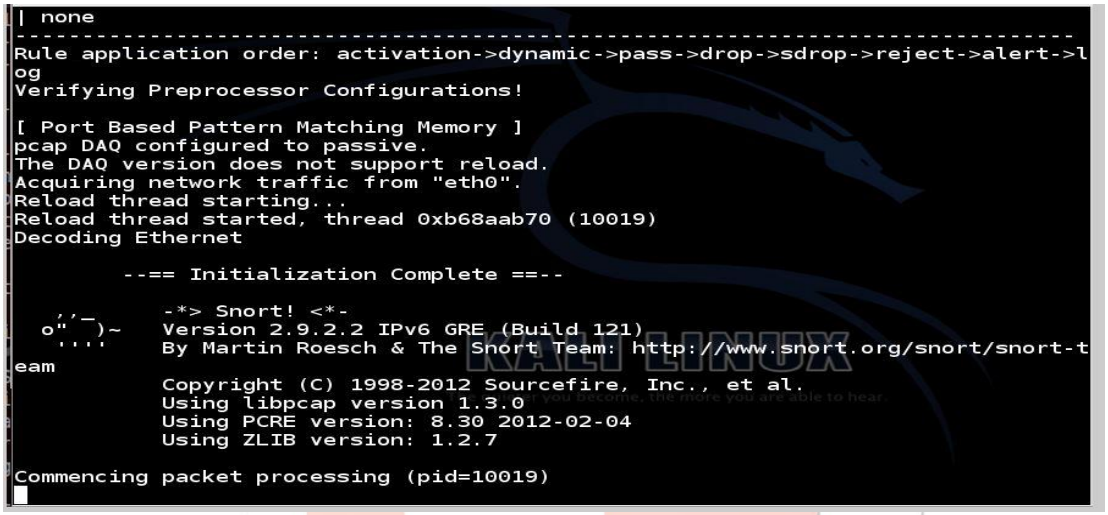
now i have also generate the log file:



now i can use snort as IDS:

```
snort -i eth0 -c /etc/snort/snort-test.conf -l /var/log/snort
```

run snort



initializing snort

```
alert icmp any any -> any any (msg:"ICMP Packet"; sid:477; rev:3;)
```

snort icmp alert

```
ping -c 1 8.8.8.8
```

Figure 19 Ping on google Public DNS for Detecting of Ping

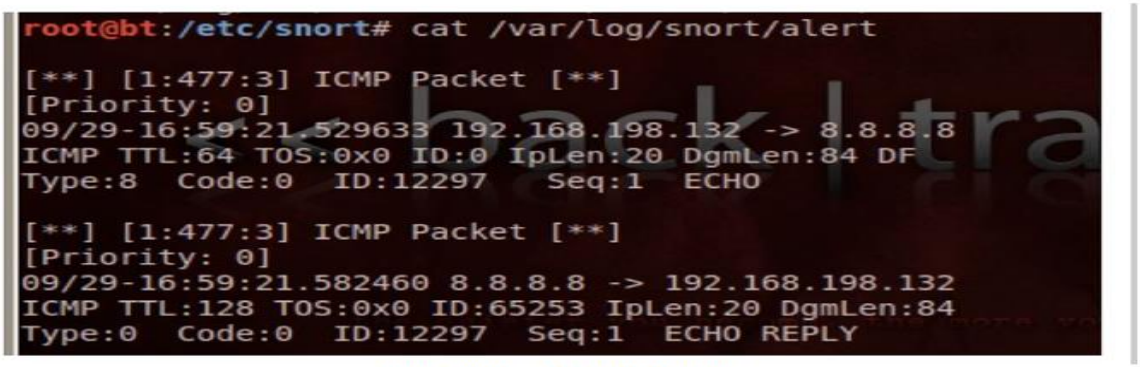


Figure 20 Result if ICMP Detection

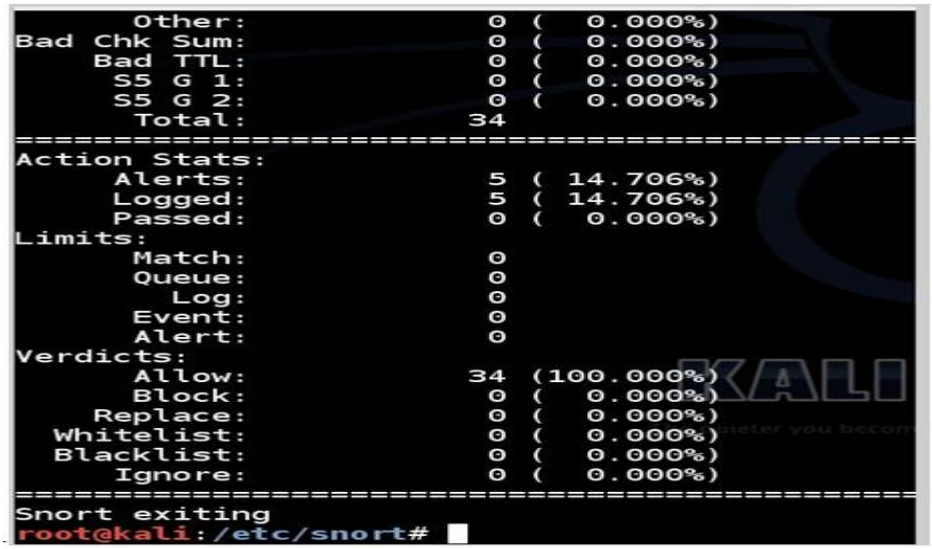
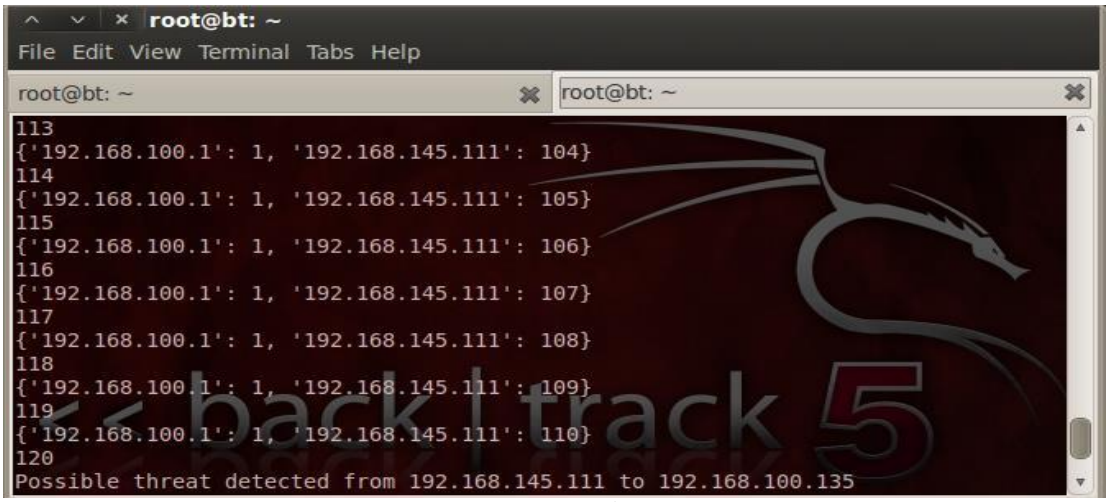


Figure 21 Final Detection Result using Snort

Modual 2: This module contains actual implementation of algorithm to identify possible threat source and block that source for further communication with any machine in the internal network. This module contains sub modules from which I have implemented. Detail implementation of the sub modules are described in detail further. This module starts with implementing sniffer to capture packets than algorithm to identify Dark IP, Targeted Attack, Random Attack and ends with blocking the possible threat source.

- **Script to identify possible Targeted Attack**

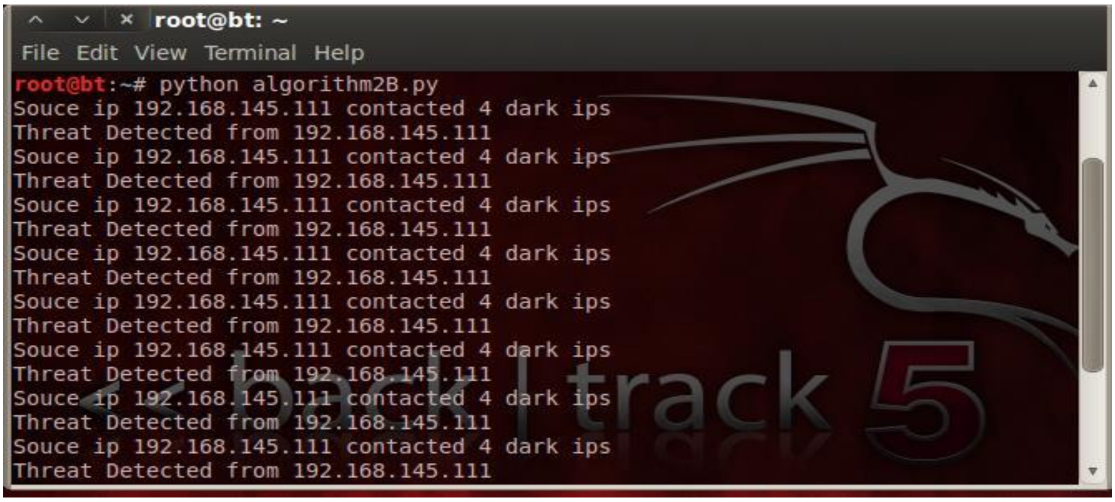
```
    if eth_protocol == 8 :

            ip_headerp = pkt[eth_length:20+eth_length]        # First 20 characters
            ip_headerup = unpack('!BBHHHBBH4s4s' , ip_headerp) # Unpack IP packet

            version_ihl = ip_headerup[0]
            version = version_ihl >> 4
            ihl = version_ihl & 0xF
            iph_length = ihl * 4
            ttl = ip_headerup[5]
            protocol = ip_headerup[6]
            ip_source_addr = socket.inet_ntoa(ip_headerup[8]);
            ip_destination_addr = socket.inet_ntoa(ip_headerup[9]);

            if ip_source_addr != "192.168.100.130" and source_mac != "00-0c-29-6f-12-0d":
                    if ip_source_addr in ip_dic:
                            ip_dic[ip_source_addr]=ip_dic[ip_source_addr]+1
                    else:
                            ip_dic[ip_source_addr]=1
                    print ip_dic
                    end_time=int(time.time()-start_time)
                    print end_time
                    if end_time % 20==0:
                            for key in ip_dic:
                                    if ip_dic[ip_source_addr] >=30:
                                            print"Possible threat detected from "+str
(ip_source_addr)+" to "+str(ip_destination_addr)
                                            os.system(ipt)
                                            f=open("assign.txt",'rU')
                                            assign=f.read()
                                            f.close
                                            pat=re.compile("ifconfig eth0:\d "+str
(ip_destination_addr))
                                            down=re.findall(pat,assign)
                                            for ent in down:
                                                    cmd=str(ent)+" down"
                                                    os.system(cmd)
                                            ip_dic[ip_source_addr]=0
```



Result of Script

- **Script to identify Random Attack:**

```
        if eth_protocol == 8 :

                ip_headerp = pkt[eth_length:20+eth_length]        # First 20 characters
                ip_headerup = unpack('!BBHHHBBH4s4s' , ip_headerp) # Unpack IP packet

                version_ihl = ip_headerup[0]
                version = version_ihl >> 4
                ihl = version_ihl & 0xF
                iph_length = ihl * 4
                ttl = ip_headerup[5]
                protocol = ip_headerup[6]
                ip_source_addr = socket.inet_ntoa(ip_headerup[8]);
                ip_destination_addr = socket.inet_ntoa(ip_headerup[9]);

                if source_mac != "00-0c-29-6f-12-0d":
                        if os.path.exists('/root/darkip.txt'):
                                f=open("darkip.txt",'rU')
                                addr=f.read()
                                f.close()
                                if ip_destination_addr in addr:

                                        if os.path.exists('/root/source ip/'+str
(ip_source_addr)) == False:

                                                f=open('/root/source ip/'+str
(ip_source_addr),'w')

                                                f.close()

                                        else:
                                                f=open('/root/source ip/'+str
(ip_source_addr),'rU')

                                                addr=f.read()
                                                f.close()

                                                if ip_destination_addr in addr:
                                                        continue
                                                else:
                                                        f=open('/root/source ip/'+str
(ip_source_addr),'a')

                                                        f.write(str(ip_destination_addr)+'\n')
                                                        f.close()

                                        if os.path.exists('/root/source ip/sip.txt') == False:
                                                        f=open('/root/source ip/sip.txt','w')
                                                        f.close()


                                        else:
                                                f=open('/root/source ip/sip.txt','rU')
                                                saddr=f.read()
                                                f.close()

                                                if ip_source_addr in saddr:
                                                        continue
                                                else:
                                                        f=open('/root/source ip/sip.txt','a')
                                                        f.write(str(ip_source_addr)+'\n')
                                                        f.close()
```



output of script

VI. CONCLUSION

We have already studied some existing Darkip Monitoring System to mitigate Darkip's , but these do not provide complete protection against attack. Although This architecture will be capable of detecting attack host and port scanning performed by external hosts. It will also identify the outsider attacks. Dynamic and distributed nature of Dark IPs will increase the chances of threat and attack detection. I hope that the proposed system will provide accurate and valuable information for network as other existing systems and models provide information for public networks.

VII. ACKNOWLEDGMENT

I would like to thank to all who supported me and guided me throughout the survey. I am very thankful to them. It was impossible to complete this without them.

REFERENCES

[1] R. Berthier and M. Cukier, "The Deployement ofa Darknet on an OrganizationWide Network: An Empirical Analysis,"*2008 11th IEEE High Assurance Systems Engineering Symposium*, pp. 59-68, December 2008.
[2] Practical Darknet Measurement Michael Bailey,Even Cooke,Frnam Jahanian, ndrewMyrick,Sushantsinha.IEEE 2008
[3] B. Irwin, "A Baseline Study of Potentially Malicious Activity Across Five Network Telescopes," *5th International Conference on Cyber Conflict* , 2013.
[4] Investigating the Dark Cyberspace: Profiling, Threat based Analysis and Correlation.Claude Fackkha,Elias BouHarb,Amine Boukhtaouta,Son Dinh, Farkhund Iqbal,MouradDebbabi IEEE 2012
[5] S. Mizoguchi, Y. Fukushima, Y. Kasahara and Y. Hori, "Darknet Monitoring on Real Operated Networks," *IEEE Conference on Broadband, Wireless Computing,Communication and Appliactions*, pp. 278-285, November 2010.
[6] The Deplyment of a darknet on an organization wide network: An Empirical Analysis. Robin Berthier and Michel Cukier. IEEE2008.
[7] "The Darknet Project - Team Cymru," [Online]. Available: http://www.cymru.com/Darknet/index.html.
[8] "The UCSD Network Telescope," The Cooperative Association for Internet Data Analysis, 20 08 2012. [Online]. //www.caida.org/projects/network_telescope/.
[9] "WhatisNetworkSecurity?CiscoSystems,"CiscoSystems,[Online].Available:http://www.cisco.com/cisco/web/solutions/sm all business/resource_center/articl es/ secure_my_business/what_is_network_security/index.html.
[10] M.Maite,"IntroductiontoDarknet,"11022013. [Online]. Available: http://www.securityartwork.es/2013/02/11/introduction-to-dark nets/?lang=en.