Threat Detection by deploying Darknet

Ms. Reena Aparnathi[1] Dr. Vandana Rohokale[2] Gardas Nareshkumar[3]
[1,3]Research Student [2]Professor
[1,2,3]Department of Computer Engineering
[1]GTU PG School, Gandhinagar, India [2]Sinhgadh Institute, Pune, India [3]CDAC, ACTS, Pune, India

Abstract— As the use of internet increasing users need more and more secure network for communication. For maintaining the security of network it has been monitor actively. The detection of threat is must for any network before it will affects to the services of network so for monitoring the network the Darknet was introduced as a network telescope. Darknet is the routed and unallocated IP address space of existing network. Main advantage of Darknet is it provides the anonymous infrastructure and also it will monitor the network passively as there are no services running of network so the packets which are fallen in the Darknet consider as a suspicious packets. Because it is the unused space of the network, no false positive packets cannot be fallen over there. So when any suspicious packets captured to the Darknet it will generate the alert massage to the network. This paper represents the method for detection the threat as well as preventing the threat by deploying the IPS in the Darknet.

Key words: Network Monitoring, Darknet, Network Telescope, Anonymous, Unallocated IP Address Space

I. INTRODUCTION

The Darknet is the network which is created by unallocated IP address space of our network where no active services are running of our network. It is the routed IP address space where you can be route your network traffic. The Darknet is introduced as Network Telescope which is the Chunk of IP Addresses which are not used in network. As there are no legitimate host are connected to the Darknet server it will monitor the network passively. Because Darknet is running only in listening mode it will not reply to the request which is entering towards it.

As there are no Active running services in the Darknet server the captured packets would be the suspicious packets because no one needs to send the request to the unused area of the network though and though someone trying to probe or Scan the network for doing something which will harmful to the network.

Darknet can be used as a host flow collectors, backscatter detector, a sniffer. Most common packets arriving to the Darknet are Dos, malware, misconfiguration. The elegance of Darknet is it can neglect the false positive traffic and only the suspicious traffic will be easily found.

II. DARKNET DEPLOYMENT

For analysis of the network traffic through Darknet user need to deploy the Darknet Sensor Server. Darknet Server will deploy on unused space of the existing network. Darknet server consist Two Network Interface Cards. First will capture Packets and second is connected to Management console for Ssh connection.

To prepare unused space of network recommended amount of address space is a/24. The less address space we given the more it will remain undetectable. The great advantage of the Darknet is we can route our entire traffic towards it and only suspicious will be fallen. Routing will follow the specificity so if u choose 10.0.0.1/24 – 10.0.0.100/24 internally we can deploy the Darknet into 10.0.0.1/8 another thing for deploying the Darknet we need layer-3 device that is router which will route the traffic to the Darknet.

One server with 2 NIC which will work as a packet collector.in that one interface will act as a Darknet interface and another one will act as management interface we can access.

III. PROPOSED MODEL

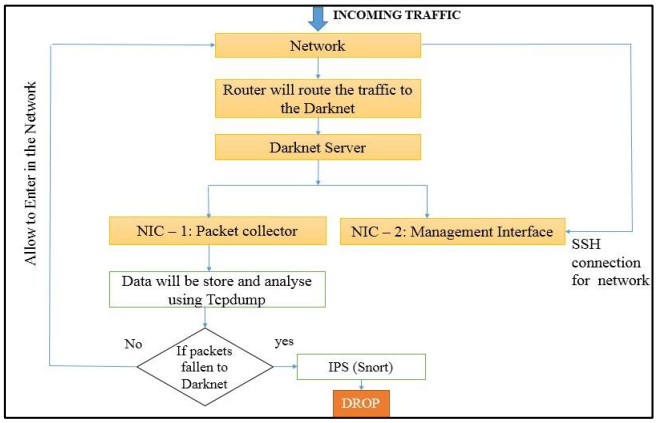

Fig. 1: Proposed model architecture

Darknet is providing anonymity to the user so by deploying the Darknet monitoring system attacker cannot detect that anything is working as a monitoring system

Proposed model represent the detection and prevention of suspicious traffic through Darknet. As shown in figure when traffic will enter to the network it will route to the Darknet by router. The routed traffic will analyze in Darknet by the first interface of Darknet server which is taken as a packet collector. The Tcpdump will analyze the traffic and store it for future use. When the traffic will analyze if any malicious activity is fallen to the Darknet then it will block by deploying the Snort and if no suspicious packets are fallen it will allow to enter in the network. Here second interface in the Darknet server is used to manage ssh connection for network to maintain the server from the main network.

So by deploying the IPS in the Darknet threats can be detected and prevented

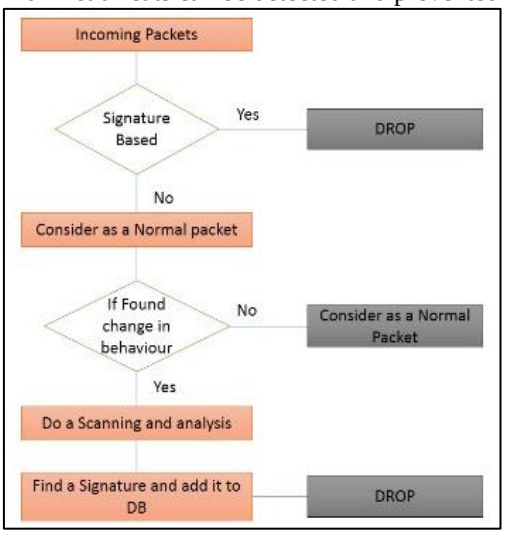

Fig. 2: Flow of malicious Activity Found

Fig 2 represents the flow for finding the malicious activity. Whenever request packet is coming to the network the IPS mechanism will analyses its signature if there is no match found then consider as a malicious and directly DROP that packet otherwise next it will check the behavior based approach. Analyze the behavior of that packets and if there is no change in behavior than it will consider as a normal packet but if any change identifies then first do a full scanning like port scan , payload & header check and then store all the details in database and then drop that packets.

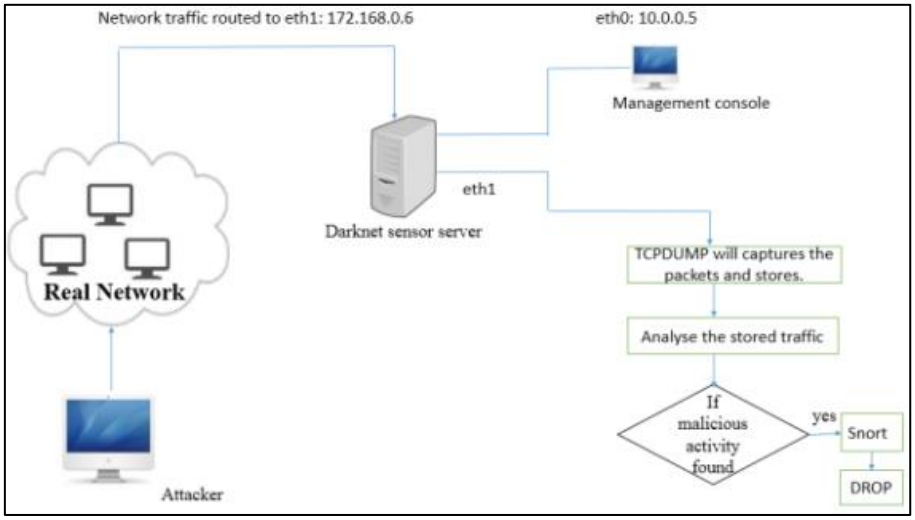

Fig. 3: System Architecture

As we above discussed in flow diagram whenever any attacker request comes to the network the router will route the traffic to the Darknet sensor server.

This sensor server is having 2 NIC eth0 & eth1 respectively, as shown in figure eth0 is having 10.0.0.5 ip address which is using for management console and eth1 that is 172.168.0.6 is connected to real network where all the traffic will be route.

When any request is comes to the network if it is only for real network it will be logged over Darknet server but if anything like someone tries to scanning the network so that kind of packets will be directly fallen to the Darknet sensor and the Tcpdump will analyse that packets as there are no active service is resides on the Darknet any packets which falls over there consider as a suspicious.

So, when activity is found as a malicious snort rule will directly drop that packets.

IV. RESULT AND ANALYSIS

For implementing the propose scenario first network traffic should route to Darknet server.

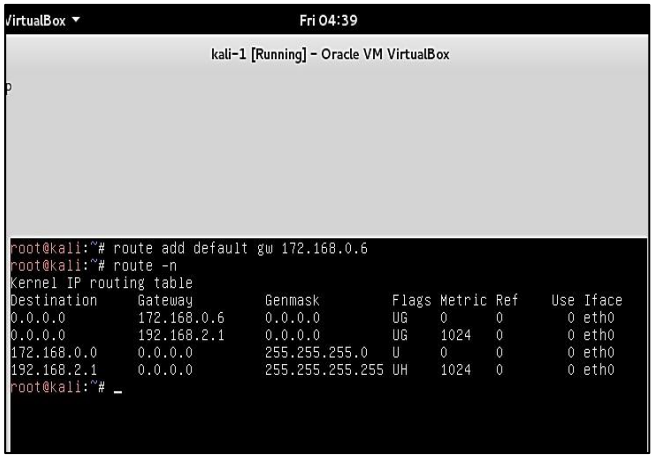

Fig. 4: Traffic route to Darknet

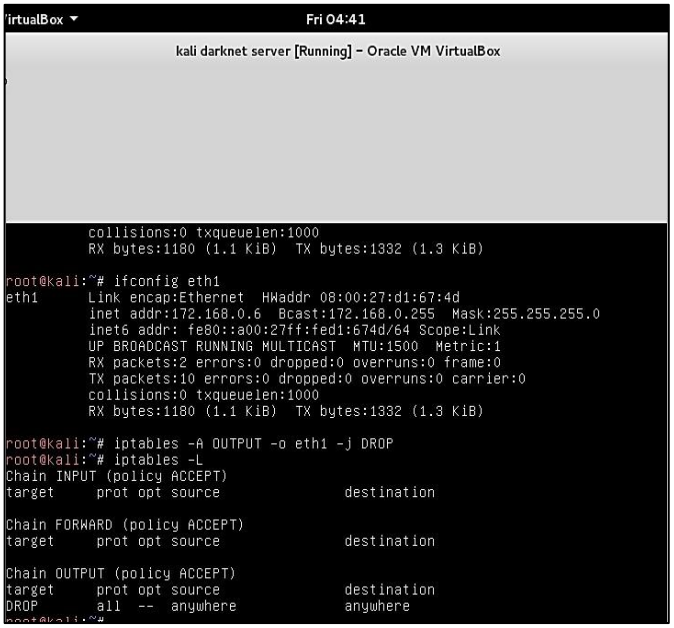

Fig. 5: Darknet Server rules

Fig. 5 shows the server process for make the Darknet working.

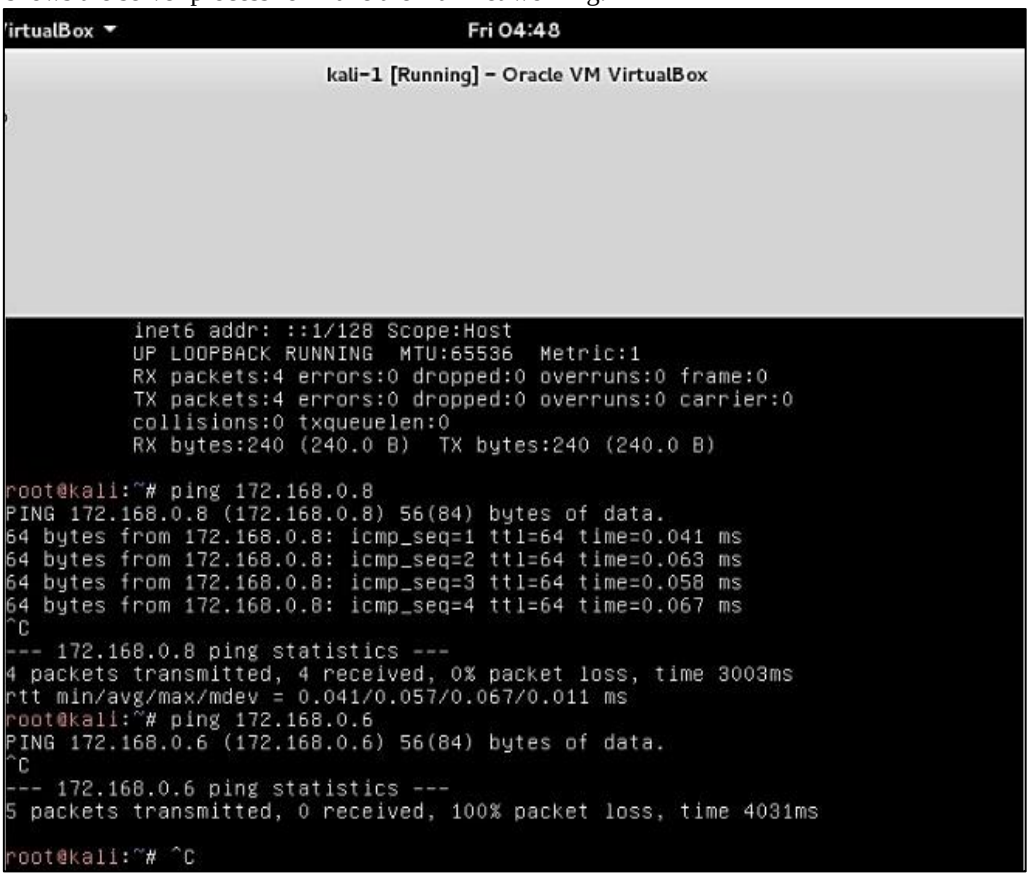

Fig. 6: Sending the packets from main network

Fig. 6 shows the process off main network sending the request to Darknet.

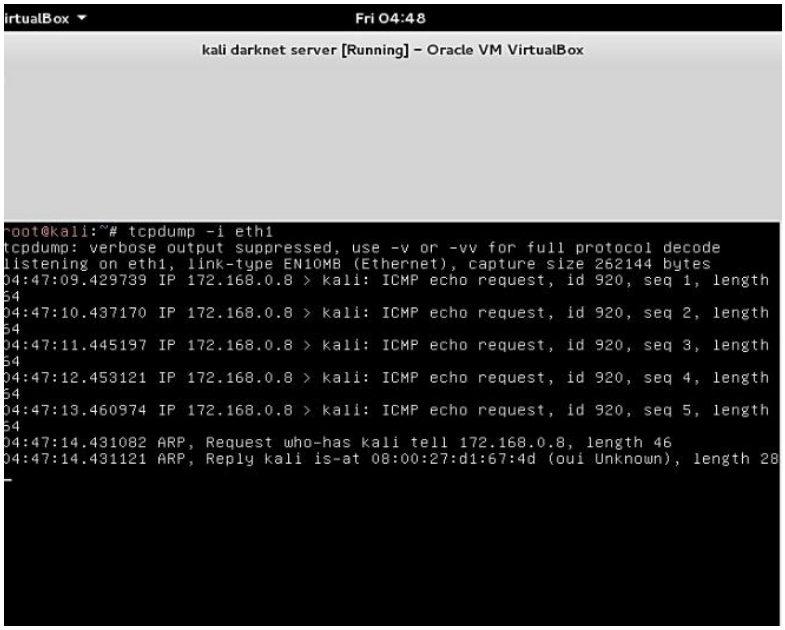

Fig. 7: Tcpdump process

Tcpdump will analyses the traffic and detect the source on the Darknet server.

V. CONCLUSIONS

As user need more secure network the deployment of Darknet is the easiest way for detection of the threat and by that user get alert about the intrusion. Proposed work is detecting the threat by analyze the traffic using Tcpdump. Darknet is setup as if any real request is entering to the network it will allow to enter but if any suspicious packets are trying to enter it will not reached to network and when packets are fallen to the Darknet server then it will be block by Snort which is working as a IPS. Deploying the IPS in the Darknet is the feasible solution for threat prevention.

REFERENCES

[1] R. Azrina, R. Othman, Normaziah A. Aziz, M. ZulHazmi, M. Khazin, J. Dewakunjari, "Network Forensics – Detection and Mitigation of Botnet Malicious Code via Darknet" ACM 2012
[2] Jun Liu, Kensuke Fukuda, "Towards a Taxonomy of Darknet Traffic" IEEE 2014
[3] Sangun Ko, Kyuil Kim, Younsu Lee, Jungsuk Song "A Classification Method of Darknet traffic for advance security monitoring and response" pages 357– 364 Springer 2014
[4] Nobauki furutani, Jun kitazono, Seiichi Ozawa, Tao ban "Adaptive DDOS event detection from big Darknet traffic data" pages 376 – 383 springer 2015
[5] Daisuke Inoue, Mio Suzuki, Masashi Eto, Katsunari Yoshioka, Kojj nakao "DAEDALUS: Novel Application of Large-scale darknet monitoring for practical protection of live Networks" pages 381-382 Springer 2010.
[6] Ruibin Zhang, Lei Zhu, Xiaosong Li, Shaoning Pang1,Abdolhossein Sarrafzadeh, and Dan Komosny, "Behavior Based Darknet Traffic Decomposition for Malicious Events Identification" Springer 2015
[7] Satoru Akimoto, Yoshiaki Hori, and Kouichi Sakurai "Collaborative behaviour visualization and its detection by observing Darknet traffic" pages 212-226 springer 2012
[8] Claude Fachkha and Mourad Debbabi "Darknet as a source of cyber intelligence: survey taxonomy & characterization", IEEE, 2016
[9] Atul Kant Kaushik, Emmanuel S. Pilli, and R.C. Joshi, "Network Forensic Analysis by Correlation of Attacks with Network Attributes", Springer 2010
[10] Jinoh Cho1, Seunghae Kim1, Hyunhun Cho1, and Gihwan Cho, "Design and Construction of Sinknet for KREONET Attack Detection", Springer 2015
[11] Hemal khorasiya, Mr. Girish khilari "Darknet monitoring using honeypot" pages 518 – 524 IJEDR 2015
[12] Seiichiro Mizoguchi, Yoshiro fukusima, Yoshiaki Kasahara, yoshiaki Hori, Kouchi sakurai "Darknet monitoring on real operated networks ", IEEE, 2010