Sparse Darknet: A Novel Approach In Intrusion Detection Methods

Ms. Khyati Shah

GTU PG School, Gandhinagar

Abstract

Darknet is increasingly being proposed as a means by which network administrators can monitor for anomalous, externally sourced traffic. Packets arriving at Darknet addresses generally represent either misconfiguration of hosts outside the Darknet, backscatter from network attacks targeted elsewhere on the Internet, or probes/scans by hosts that are speculatively mapping the Darknet itself. Regardless of their motives, the sources usually do not realize they are sending packets into a monitored Darknet space. Current Darknet designs require large, contiguous blocks of unused IP addresses - not always feasible for enterprise network operators. Sparse Darknet - a region of IP address space that is sparsely populated with 'Dark' addresses is interspersed with active (or 'lit') IP addresses. Along with that sparse Darknet is configured specifically to detect insider attacks and suspicious traffic in private IP address space.

1. Introduction

As the 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 various purposes. Basically Internet is designed, implemented 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 adversaries who are eager to exploit any vulnerability as soon an opportunity strikes.

Now-a-days the products and applications have become so complex it is very difficult to protect them. It is not enough to protect only front gate. 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 them. 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.

To protect enterprise against threats and attacks, it is must to provide network security thoroughly. Network security includes any activities designed to secure network. These activities protect the usability, reliability, integrity and safety of network and data. [1] Effective network security targets a variety of threats and stops them from entering or spreading on network. Many network security threats are spread over Internet. The most common include malware (e.g. virus, Trojan horse, worms, backdoors etc.), spyware, adware, zero-day attacks, DoS / DDoS attacks etc.

There is no single security solution can protect against a variety of attacks. It needs multiple layers of security. A network security system usually consists of many components which work together to minimize maintenance and improve security. Such components include anti-virus, anti-spam solutions, firewall, Intrusion Detection / Prevention systems, VPN etc. Here Darknet is being proposed as a part of Intrusion Detection System which can effectively detect the attacks that may have gone unnoticed from other security solutions.

2. What is Darknet?

To prevent any attack, it is first necessary to detect it as soon as possible. This can be possible using Intrusion Detection System – IDS. IDS can be placed to monitor the traffic for suspicious activities. In this context, IDS becomes first step in providing security against any attack. So as a part of IDS, Darknet also captures the network traffic for specific addresses and analyse them to get information which can be used to detect malicious activities in the network.

Basically Darknet is a portion of routed, allocated IP space in which no active services or servers reside. These are "dark" because there is, seemingly, nothing within these networks. [2] A Darknet does in fact include at least one server, designed as a packet vacuum. This server captures the traffic destined for

Dark IPs for real time analysis or post event network forensics. According to the definition of Darknet, packets which enter the Darknet are considered malicious because there are no active hosts or services reside in Darknet. So the packets destined for Darknet addresses may come due to misconfiguration (for example DNS misconfiguration or router misconfiguration) or network scanning in attempt to find active and vulnerable hosts or services or back scatters.

So Darknet can be used as an efficient tool for information gathering and analysis. [3] Efforts to analyse traffic are significantly reduced because there is no need to differentiate legitimate traffic from malicious traffic. False positive can be reduced because any traffic that enters Darknet is suspicious in nature.

2.1 Limitations in practical use of Darknet

Even if Darknet provides an efficient way to detect malicious activities with little efforts, there are some requirements and factors which affect the performance of Darknet thus limiting the use of Darknet. Following section describes the requirements for Darknet implementations.

2.1.1 Contiguous block of unused IP addresses

There are few projects currently under going on traffic analysis using Darknet on real time public networks. Based on the performance of different models, it has been derived that a contiguous block of unused IP addresses is required for monitoring purpose. Minimum a subnet of /24 addresses are required to get accurate results. [4] This requirement seems feasible for large organizations like ISPs, research facilities, etc. But it is not possible for small and midsized organization to allocate such a large block of public IP addresses for monitoring.

2.1.2 Traffic consideration for analysis

Traffic consideration for analysis also plays an important role in detection. As Darknet captures all the packets destined for the Dark IPs, only those packets are analysed further which have external source addresses. [5] This means packets from the outside networks only are considered for analysis process. So packets coming from the different subnets of the same network will not be considered as malicious. Thus any malicious activities in inside network will go undetected.

2.1.3 Size and placement of Darknet

Size and placement of the subnet allocated for monitoring also affect the detection capabilities. If the subnet is large, possibility to detect malicious activities increases. Similarly if the Darknet is placed among the subnets with live IP addresses, possibility of detecting malicious activities increases. [6]

3. Sparse Darknet

The main limitation of the Darknet is allocation of contiguous block of unused IP addresses for monitoring. This requirement is very difficult to fulfil for small and midsized organization. To overcome this limitation a different approach can be chosen for implementation.

- Instead of allocating contiguous block of public IP addresses, scattered unused IP addresses are used for monitoring. So there will be Dark IP addresses among live, used IP addresses being monitored for malicious activities. Such IP addresses can be obtained with the help of DHCP server or ARP requests.
- Another deviation to improve the detection capabilities is to consider packets with internal source IP addresses for traffic analysis. This will increase the performance of Sparse Darknet by making it able to detect insider malicious activities.

3.1 How to get Dark IPs?

Dark IPs are the core requirement of any Darknet implementation. To monitor the network traffic, first one needs to get the list of IPs which are unused and eligible for Darknet monitoring. As for Sparse Darknet, Dark IPs should be scattered in nature, there are 2 methods to get such IP addresses for monitoring.

3.1.1 Monitoring ARP requests and response traffic

This is one method to determine whether an IP address is being used by any host of not. Initially the monitoring server will have a list of all the IP addresses for given subnet range. Monitoring server will track all the ARP request and response packets and discard the IP addresses included in such packets as they are already in use. So after a certain period of time, monitor server can have a list of IP addresses which are not being used by any hosts.

But this method is not reliable. Because it is possible that an IP address is being used by a host and it is not having any conversations with other machines thus lacking any ARP traffic.

3.1.2 DHCP server

If a network where Sparse Darknet is to deploy has a DHCP server for dynamic IP allocation then with the help of DHCP server one can get list of allocated IP addresses for a particular time period. From that list it is easy to derive the list of unused Dark IP addresses.

This method is more reliable and preferred over previous method. Moreover it does not need to monitor traffic to get the Dark IPs. Once a DHCP server provides list of allocated IP addresses, monitor server can start capturing traffic for Dark IPs straight away.

3.2 Traffic Capturing and analysis

To capture traffic for Dark IPs on monitor server, there are lots of traffic capturing tools are available. Among them Wireshark and tcpdump are preferred. Because these tools are open source software and have capability to capture traffic for specific IP addresses as well as specific characteristics like traffic for certain application protocols or packets having specific flags set etc. efficiently. Using these tools captured traffic can be stored for further analysis.

In analysis part once again Wireshark can be used. Wireshark can access the file having captured packets and retrieve the specific information such as Source IP addresses, Source and destination ports, time stamps, flags, frame numbers etc. Payload of the packets can be used to determine the type of malicious activities. Thus one monitoring server with the capability of packet capturing and analysis can help detect malicious activities effectively.

4. Advantages of Sparse Darknet over traditional Darknet

The basic principal of Sparse Darknet remains the same as traditional Darknet which is to monitor unused IP addresses to detect malicious traffic. But the allocation of IP addresses and traffic analysis consideration makes Sparse Darknet preferable over traditional Darknet for small and midsized organizations. Following section describes some advantages of Sparse Darknet over traditional Darknet.

4.1.1 No requirement of contiguous block

As the basic idea behind the Sparse Darknet is to make use of scattered unused IP addresses for monitoring, it removes the need for contiguous IP address block. Many of the organizations may have some IP addresses which are unused and scattered among the live, used IP addresses. Such IP addresses can be used for monitoring the network traffic.

4.1.2 Better performance

As the Dark IPs are scattered among Live IPs, the possibility of detecting malicious activities increases. For example, an adversary tries to get information about active hosts and services by scanning the whole network. In this situation Dark IPs will also received packets along with Live IPs. Analysis of such packets will reveal the crucial information about the adversary.

Same results may be gained in case of worm propagation. Thus scattered nature of Dark IPs will increase detection capabilities.

Moreover the scattered nature of Dark IPs will decrease the chances of being detected by adversaries. In traditional set up of Darknet when whole block is being monitored, no response from the whole subnet may alert the adversaries about the presence of Darknet. But if the Dark IPs are scattered among Live IPs it is practically very difficult to detect them.

5. Conclusion

As detection is the very first step in the process of dealing with attacks against any network, detection methods play very important role in network security.
In recent time Darknet is being proposed as a part of Intrusion Detection System by security professionals, limitations in implementation and practical use of Darknet prove to be road blocks in its acceptance. But the small changes in implementation and analysis as described above can overcome those limitations and make the Darknet monitoring an efficient tool for traffic monitoring. Sparse Darknet can make efficient use of unused resources and provide useful information about the insider as well as the outsider attacks.

6. References

[1] "What is Network Security? – Cisco Systems," Cisco Systems, [Online]. Available: http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business

[2] "The Darknet Project - Team Cymru," [Online]. Available: http://www.cymru.com/Darknet/index.html.

[3] M. Maite, "Introduction to Darknet," 11 02 2013. [Online]. Available: http://www.securityartwork.es/2013/02/11/introduction-to-dark

[4] R. Berthier and M. Cukier, "The Deployement of a Darknet on an Organization-Wide Network: An Empirical Analysis," *2008 11th IEEE High Assurance Systems Engineering Symposium*, pp. 59-68, December 2008.

[5] M. ,. C. E. ,. J. F. M. A. Bailey, "Practical Darknet Measurements," *40th Annual Conference on Information Sciences and Systems*

[6] B. Irwin, "A Baseline Study of Potentially Malicious Activity Across Five Network Telescopes," *5th International Conference on Cyber Conflict*, 2013