ISSN: 2581-3404 (Online) IF: 5.68 (SJIF)
IJIRTM, Volume-8, Issue-1, February-2024.

Deployment and Use of Dark net on Private Network: The Future of Intrusion Detection System

Dr. B.K. Verma
Professor, CSE-AI & DS
Panipat Institute of Engineering and Technology, Samalkha, Haryana
Email: bkverma.3474@gmail.com

Abstract. *With the development of computer network, network security has become more important issue to the users and organizations. As the use of computer network is increasing, security of the data and information on the network became a major concern. As the importance and use of the computer network increases, rapid identification of threats at a global level becomes even more complex. Better advance warning benefits the entire world of computer network. A Darknet is a portion of network, a certain routed space of IP Addresses in which there are no active servers or services. I.e., externally no packet should be directed to that address space. Most are the systems are designed for the public internet monitoring. Large or mid-sized organization can also take benefits of the traffic entering on darknets to identify the threats coming on their network. In this paper we have described the issue of identifying dark IPs in the network. We have analysed various methods to identify dark IPs the in private network and proposed method than can be implement on private network to identify dark IPs. This is the research work and it is not fully implemented. The implementation of this research work is on-going.*

Keywords:- Darknet, Dark IPs, Private Network, IDS, Network Security, ARP.

Introduction

Monitoring packets destined to Dark IPs which are also known as unused addresses has become an increasingly important measurement technique for detecting and investigating malicious Internet activity. Any observed traffic on unused address block should be the result of misconfiguration, backscatter from spoofed source addresses, or scanning from worms and other network probing because there are no legitimate hosts or devices in an unused address block. Systems that monitor unused address space have been called darknets.[1]

In its simplest definition, a darknet is an area of routed IP address space in which no active services reside.[2]

While traditionally every client, server, and network device has a unique IP address for each network connection, a darknet is comprised of a range of addresses for which there are no associated valid services or hosts.

What makes a darknet a powerful security tool is that, after initial tuning, any traffic entering it from any source is most likely hostile. In contrast to a traditional network setup, wherein legitimate IP packets are routed to legitimate destination IP addresses and from legitimate source IP addresses, no legitimate packets

should be sent to or from a darknet. Although some packets may enter as the result of misconfiguration, the majority are likely sent by malware that scans for vulnerable devices with open ports in order to download, launch, and propagate malicious code.
While darknets are different from traditional IDSs, they use the same type of detection. But with a darknet, we know immediately that any traffic entering is hostile because there are no advertised services in a darknet. This solves two problems associated with traditional IDSs.[3]

- First, we don't need to classify the source of data. By design, darknet only monitors traffic and serves no other purpose, so you know any data entering the darknet is hostile.

Second, we don't need to inspect the data to know that it's hostile. No one would be probing an empty network space unless he or she was looking for something.

What Makes Darknet Powerful?

Any packet entering a Darknet should not be legitimate. It could reach it due to errors such as poor security policies or poor configuration such as broadcast messages sent to a segment to which the issuer doesn't belong. However, most of these packages would be associated to some action by a suspicious malware or attacker who is actively searching vulnerable devices.
If we install a server within our Darknet that collects, analyzes and processes the traffic entering it, it would help us to gather more information on the anomalous traffic or malware that may be circulating in the network infrastructure of our organization. This will allow us to reduce the number of false positives, detect attacks in real time and new attacks.
Collecting data on all traffic will allow us to analyze patterns of interest and subsequently automate the entire process through an IDS installed on our collector server.

With the use of darknets, security administrators can spot scanning activity without using complicated analysis technology committing already overburdened resources, and, with a reduced occurrence of false positives. By significantly reducing the effort to analyze traffic, and at the same time improving intelligence gathering, darknets are an efficient tool for providing organizations critical information to help them protect the security and availability of their information assets [2**].**

Related Work

Michael Bailey et al describe and analyze the important measurement factors associated with the deployment of the darknet. [4] Since a darknet monitor observes traffic to unused addresses, the upstream router must be instructed to forward undeliverable packets to the monitor. They proposed approach to configure the upstream router to statically route an entire address block to the monitor server.
Seiichro Mizoguchi et al presented the result of real operated network monitoring. [5] They setup monitoring servers with several configuration and monitor darknet traffic on production network and analyze the data obtained by each sensor. For the dark IP address space they used the DHCP server installed on real operated network. On the live organizational network, mainly a DHCP service is used to manage IP addresses for production computers. If a computer is connected to the network, DHCP server will automatically assign an IP address to it. Several IP addresses are assigned for the DHCP service. So, there may be many unused addresses which are not assigned, means unused.

Public Projects

One of the easiest ways for organizations to take the benefits of a darknet is to participate in any one of a number of public darknet projects. There are several projects developed to monitor public dark ips by security organizations and universities.

A. Internet Motion Sensor: (ims.eecs.umich.edu)

Internet Motion Sensor (IMS) is the globally deployed distributed darknet monitoring system. The servers of the IMS are deployed in various ISP networks, major service providers, large enterprise networks and academic networks.

There are total 18 such organizations and 60 darknet blocks which monitors 17 million IP addresses which represents

1.25% of all routed IPv4 address space.

B. The Darknet Mesh Project: (projects.oucs.ox.ac.uk/darknet/)

The Darknet Mesh Project is a collaborative project between the Network Security Team at OUCS (Oxford University Computing Services), and other security teams at UK universities to produce a collaborative means to detect and report on traffic hitting a collection of darknets.

Participants within a darknet mesh must register their address space in CIDR notation, and an alert email address. This data is then fetched by each participant within the mesh to determine what addresses should be monitored by the darknet code. Once installed and configured, the script monitors for traffic from participating organizations, collects flows flowing to the darknet and emails the appropriate administrator for the network.

Private Darknet

Mid-sized to large organizations can also take benefit from implementing their own private darknet. The greater the number of users is in an enterprise, the more devices administrators have to manage, and the greater the need is for safer, faster, and more reliable network traffic analysis.

With a private darknet, organizations can quickly differentiate between legitimate and malicious traffic on their networks. This practice can be especially useful for organizations that communicate regularly with international partners.

For these organizations, it is not an option to block all traffic from specific source countries in order to reduce their security risk; with online business activities traversing the globe, international enterprises must remain accessible to partners and associates regardless of their location. Darknets provide a tool for allowing authorized connections from around the globe while also singling out unauthorized connection attempts from any source, near or far.[2]

However, before organizations invest in a private darknet, they must have a proven test environment in place. Once space is allocated in this test environment, the organization can distribute known bad traffic to ensure it reaches the darknet test environment and that security administrators understand what to do with that data.

When the test period is complete, the organization can then identify the unused network space to be allocated to the darknet, monitor it for a period of time to ensure it is not being used, then, if necessary, implement network changes to make sure no legitimate traffic is routed to that space. A collector must also be set up within the darknet that captures any traffic that enter.

Issues in Darknet

Most are the systems are designed for the public internet monitoring. Large or mid-sized organization can also take benefits of the traffic entering on darknets to identify the threats coming on their network. By definition, the Dark IPs does not send ant packet or sent any packet.

If the Dark IP receives any packet than it should not be replied in any way. In the sense, darknet should not send any TCP or UDP packets on the network. After the study of the current darknet scenario we can identify the two major issues related to the darknet:

- Preparing the IP address spaces for monitoring.
- Design of algorithm to identify the attack on network.

In this paper we will only discuss about the first problem: Preparing the dark IP address space or identify dark IPs in live network.

In most of the systems which we have studied earlier proposed to prepare the IP address space for monitoring and then monitor the traffic on Dark IPs.

In most of the systems which we have studied earlier proposed to prepare the IP address space for monitoring and then monitor the traffic on dark IPs. If we allocate a whole subnet for monitoring [4], we need large IP address space which is not feasible in mid-sized organization and the IP address blacklisting problem may be arise. Attackers may detect the dark IPs based on the no reply strategy.

We can use some another technique to detect the dark IPs like, using DHCP server [5] Several IP addresses are assigned for the DHCP service. So, there may be many unused addresses which are not assigned, means unused. We can make use of that unused IP addresses for monitoring purpose in our system. But in this system the monitoring server should be communicate with the DHCP server, which is against the default definition of the darknet (never generate tcp/udp packets). And also we have to be dependent on the DHCP server.

For the configuration of the monitoring server, most of the proposed system make the decision of the malicious traffic based on the fail connection maid with the darknet. The main goal of the darknet is less false positive and false negative compared to the traditional IDS / IPS.

Identifying Dark IPs

After studying the limitation of existing system, we proposed a totally independent monitoring system which is not rely on any legitimate system on the network.

- Monitoring system itself prepares the Dark IPs presented on the network and monitors the traffic entering on the darknet.
- No need to communicate with the other machines on the network, so it will not generate any TCP or UDP packets.
- Monitoring server will be placed in the same intranet where all other systems are placed.
- 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.

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

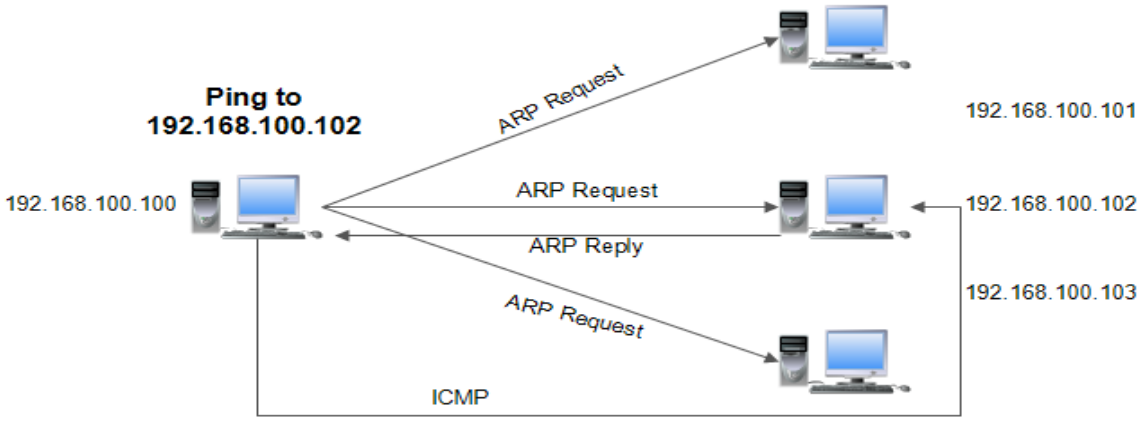

Fig. 1: describes the basic use of ARP request.

Above figure describes the basic use of ARP request. When any machine want to communicate with another machine, it needs MAC address of that machine. If the sender machine does not have the MAC address of receiving machine, it will broadcast the ARP request which includes the IP address of the receiving machine. After receiving the ARP request the correspond machine with the IP address in ARP request will reply that request with its MAC address.

When any packets come from the internet, first it will arrive to the gateway. Now the gateway needs the MAC address to successfully deliver that IP packet to the destination machine. If the destination IP is the Dark IP than gateway will broadcast the ARP request for that source IP. Since the IP address for which the ARP request is broadcasted is dark, the reply for that ARP request will never be responded.

Fig. 2: ARP request will not response.

The same situation will arise if some internal machines try to communicate with the Dark IP. Internal machine first broadcast the ARP request for that Dark IP. Now the request for that ARP request will never be responded.

Since the ARP request is always broadcasted, the Monitoring Server also get all ARP request. Monitoring Server will monitor all ARP requests. For some IP address, if ARP request is continuously generated than it can be said that machine for that IP address is down. That means IP address of that ARP request is Dark IP.

Algorithm to Identifying Dark IPs

- Capture only ARP request packets.
- Retrieve destination IP address from the captured packets and compile list of unique destination address.
- Count the total number of ARP request for each destination IP address in list.
- If for any destination IP exceeds predefined number of ARP request, consider it as a Dark IP and compile list of the Dark IPs.

The Monitoring Server will capture only ARP request packets on Monitoring server. For all unique source IP, system will maintain a list of number of ARP requests to all IP addresses. If for any destination IP address, ARP request is not responded for several ARP requests, Monitoring server declare that destination address as Dark IP.

Conclusion

The Information produced by darknet can be useful to identify new threats coming from internet or from private network. The main issue regarding darknet is to identify dark IPs to monitor traffic. Drak IPs or darknet cannot receive legitimate traffic in any case. Monitoring traffic destined to darkIPs can be useful to identify threats on network. Private network can take benefits of ARP request messages to identify Dark IPs in the network. System will automatically define Dark IPs in network by analyzing ARP request broadcasted in network. It will than analyze IP packets destined to Dark IPs and identify possible targeted or random attack on network and take action to block threat source addresses.

References

[1]. The Darknet Project- Team Cymru: www.teamcymru.org/Services/darknets.html
[2]. Michael Smith – Symantech Global Services:“Darknet: Security’s Bright Future.” www.infosectoday.com/Articles/Darknets.html\
[3]. Jonathan Yarden: “Learn how darknets can serve as an early warning detection system for network threats.” On November 18, 2005. www.techrepublic.com/Articles
[4]. Michael Bailey, Evan Cooke, Farnam Jahanian, AndrewMyrick, Sushant Sinha: “Practical Darknet Measurement”. In 2006 40th Annual conference on Information Science and Systems. IEEE Published Year 2006s, Pages: 1496-1501
[5]. Seiichro Mizoguchi, Yoshiro Fukushima, Yoshiaki Kasahara, Yoshiaki Hori, Kouicjhi Sakurai : “Darknet Monitoring on Real Operated Networks.” In 2010 International Conference on Broadband, Wireless Computing, Communication and Application. IEEE Published Year: 2012, Pages: 278-285
[6]. Robin Berthier and Michel Cukier: “The Deployment of a darknet on an organization wide network: An Empirical Analysis.” In 2008 11th IEEE High Assurance Systems Engineering Symposium. IEEE Published Year:2008, Pages :59-68

[7]. Masashi Eto, Daisuke Inoue, Mio Suzuki and Koji Nakao: "Multipurpose Network Monitoring Platform using Dynamic Address Assignment." In 2012 Seventh Asia Joint Conference on Information Security. IEEE Published Year: 2012, Pages: 79-84
[8]. David Moore, Colleen Shannon, Geoffrey M. Voelker, and Stefan Savage. "Network telescopes: Technical report." Department of Computer Science and Engineering, University of California, San Diego, 2004.
[9]. Akihiro Shimoda, Shigeke Goto. "VirtuaL Dark IP for Internet Threat Detection." In APAN Network Research Workshop 2007. Pages: 44-51.
[10]. Claude Fackkha, Elias Bou-Harb, Amine Boukhtouta, Son Dinh, Farkhund Iqbal, Mourad Debbabi. "Investigating the Dark Cyberspace: Profiling, Threat based Analysis and Correlation." In 2012 7th International Conference on Risks and Security of Internet and Systems. IEEE Published Year: 2012, Pages: 1-8.
[11]. Barry Irwin: "A Baseline study of potentially malicious activities across five network telescopes." In 2013 5th International conference on cyber conflicts. IEEE Published Year: 2013, pp. 1-17.
[12] R Dubey, D Rathore, D Kushwaha, JP Maurya, "An empirical study of intrusion detection system using feature reduction based on evolutionary algorithms and swarm intelligence methods", International Journal of Applied Engineering Research 12 (19), 2017. pp. 8884-8889.
[13] Deepak Rathore, Anurag Jain, "Design Hybrid method for intrusion detection using Ensemble cluster classification and SOM network", International Journal of Advanced Computer Research, Vol-2,Issue-3, 2012.