Bulletin of Electrical Engineering and Informatics
Vol. 7, No. 4, December 2018, pp. 593~600
ISSN: 2302-9285, DOI: 10.11591/eei.v7i4.1349

Defense-through-deception Network Security Model: Securing University Campus Network from DOS/DDOS Attack

M. A. Naagas[1], E. L. Mique Jr[2], T. D. Palaoag[3], J. S. Dela Cruz[4]
[1]Central Luzon State University, Science City of Munoz, NE, Philippines
[2]DMMMSU-MLUC, City of San Fernando, La Union, Philippines
[3,4]University of the Cordlleras, Baguio City, Benguet, Philippines

Article Info

Article history:

Received Aug 24, 2018
Revised Oct 26, 2018
Accepted Nov 09, 2018

Keywords:

Cybersecurity framework
Defense through deception
Defense-in-depth model
Network security model
Threat modeling

ABSTRACT

Denial of Service (DOS) and (DDOS) Distributed Denial of Service attacks have become a major security threat to university campus network security since most of the students and teachers prepare online services such as enrolment, grading system, library etc. Therefore, the issue of network security has become a priority to university campus network management. Using online services in university network can be easily compromised. However, traditional security mechanisms approach such as Defense-In-Depth (DID) model is outdated in today's complex network and DID model has been used as a primary cybersecurity defense model in the university campus network today. However, university administration should realize that Defense-In-Depth (DID) are playing an increasingly limited role in DOS/DDoS protection and this paper brings this fact to light. This paper presents that the Defense-In-Depth (DID) is not capable of defending complex and volatile DOS/DDOS attacks effectively. The test results were presented in this study in order to support our claim. The researchers established a Defense-In-Depth (DID) Network model at the Central Luzon State University and penetrated the Network System using DOS/DDOS attack to simulate the real network scenario. This paper also presents the new approach Defense-through-deception network security model that improves the traditional passive protection by applying deception techniques to them that give insights into the limitations posed by the Defense-In-Depth (DID) model. Furthermore, this model is designed to prevent an attacker who has already entered the network from doing damage.

Corresponding Author:

M. A. Naagas,
Central Luzon State University,
Science City of Munoz, NE, Philippines
Email: manaagas@clsu.edu.ph

1. INTRODUCTION

Today, institutions of higher education are seeing a greater frequency of Denial of Service (DDoS) attacks. Denial of Service (DoS) and (DDOS) Distributed Denial of Service attacks have become a major security threat to university campus network since most of the students and teachers prepare online services such as enrolment, grading system, library etc. Taking all of these considerations in mind, University campuses must place a greater emphasis on developing secure and scalable network model. Campus network are of unique interest, as security threats like these can have a major effect on a university's ability to provide the proper services and resources to their stakeholders. The scope of information that is provided through the breadth of web properties that universities offer can have serious implications if inaccessible or compromised.

Most of the Universities, however, only used the Defense-In-Depth (DID) model as a best practice [1]-[3]. This model serves as a foundation of protecting a campus network system. This secures a network by limiting security gaps and exposure to threats through firewalls, intrusion prevention systems, network anti-virus protection, and intrusion detection systems. In a sense, Defense-In-Depth (DID) model is the first line of defense, protecting your organization's networks from vulnerabilities, reducing the probability of a breach, and giving insight into threat encounters. This technique cannot meet the requirements of the dynamic and complex network environment [4]. The limitation is that it only provides a passive protection based on known facts and attack mode. They are not capable of defending complex and volatile attacks effectively [5].

To achieve a good level of security model, the security model should not only be interested in the defense mechanisms, but also must rely on deceptive attackers and must have the initiative to disclose the attack when it occurs [6]. A honeypot is a trap that contains valuable information or resources and appears to be a part of the network, but it is actually isolated and monitored [6]. It works by misleading attackers into believing that it is a real system. These purposes help to detect and collect information about the attacker and the source of their attack. Gathering this kind of information is important. By knowing the attack source, countermeasures can be improved, and anomalies can be fixed. Generally, such information gathering should be done without the attacker's knowledge. All the gathered information provides an advantage to the defending side and can therefore be used to prevent attacks in the future. Furthermore, this study also exposes the limitations of passive defense protection by testing the actual DOS/DDOS attack in the target machine. This attack was the proof of concept that the traditional Defense-In-Depth model has limitations in protecting the network assets in the DOS/DDOS attack [7].

To support our claim, the researchers established a real network environment in order to test the vulnerability of the traditional Defense-In-Depth (DID) model against DOS/DDOS. The White Box penetration testing was also used in this study. The experiment was tested and implemented at Central Luzon State University and the researchers used the most common tools and practices that the University have used to protect their network. The configuration best practices [8], [9] used by the researchers were adapted from linux iptables or any proprietary hardware providers like cisco, untangle, juniper, checkpoint, etc. Raspberry-pi based honeypots as a decoy are also used in this study.

2. DEFENSE-IN-DEPTH MODEL

According to CISCO Systems, Defense-In-Depth (DID) is a defense mechanism which confronts different attack methods through multi-layed network security architecture. The concept originates from military principle that it is more difficult to defeat a multi-layered defense system than a single barrier. In a computer network, Defense-In-Depth (DID) not only intercepts intruder's attacks on the network but also give more time for a network administrator to inspect and repair the systems, thereby reducing the chance of a successful invasion and subsequent impact.

The Defense-In-Depth (DID) implies embedded layers where an onion can be used as an analogy. Using the analogy of the onion you can get a better view what the DID looks like. The onion analogy has a various different layers representing different security tactics such as firewall, IPS, IPS, Anti-Virus, Proxy and hardened server configuration, etc. If you take the time to analyse the network system today and the onion analogy is outdated in today's complex network. Many systems dispersed in different location and different external and internal network. It is hard to put an onion layer wrapper in the whole system. Firewall, IDS, IPS, Network Antivirus (NAV), Proxy, etc are the major components of DID model. However, Most of the IDS/IPS/NAV/Proxy functionalities are now being merged into Next Generation Firewalls (NGFW). Because of this, the Next Generation Firewalls is considered as a DID in a modern network environment [8]. According to the reports of the CORERO Network Security [10], none of the NGFW vendors address the DOS/DDoS problem, indicating the need for a separate dedicated solution for preventing DDoS attacks. In Figure 1 shows the Defense-In-Depth New Generation Firewall Model of typical Campus Network Security.

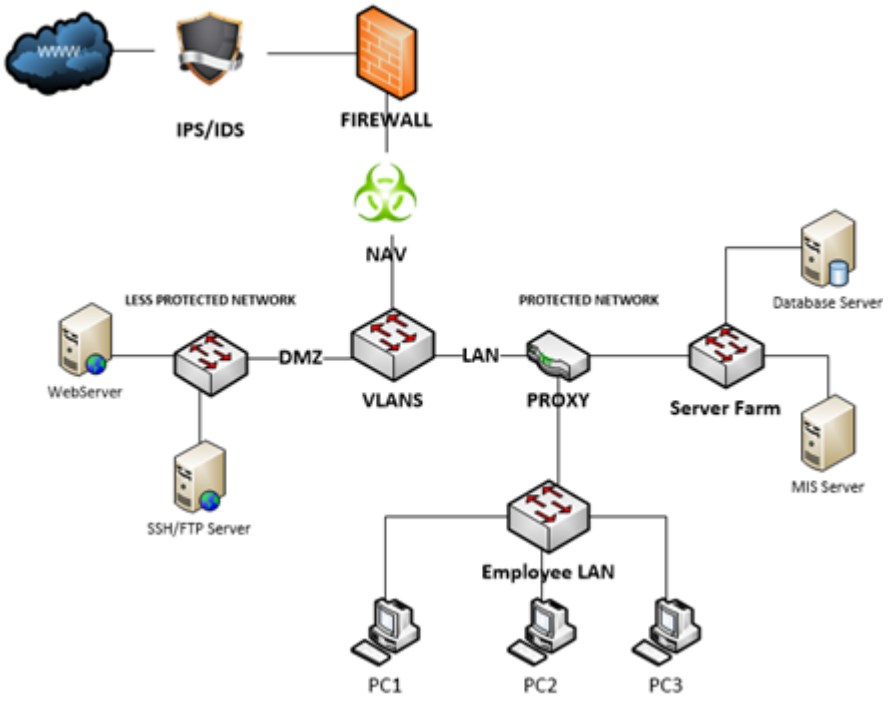

Figure 1. Defense-In-Depth new generation firewall model of typical campus network security

3. ISSUES IN DEFENSE-IN-DEPTH MODEL

The researchers conducted a survey in the selected State Universities and Colleges in the Philippines. The survey shows that the Firewall, Intrusions Detection System (IDS), Intrusions Protections System (IPS), Network-Antivirus (NIDS) are the common elements of the Defense-In-Depth that most of the Higher Education Institutions acquires to protect their systems. 93% of the Higher Education Institutions believe that firewalls protect their systems in any threat vectors, 53% installed an Intrusions Detection and Prevention System and only 53% used a Network AntiVirus as their protection against DOS/DDOS attack. According to NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report,

> "Firewall protection solves an important security problem–unauthorized data access. To do this job effectively, enterprise firewalls need to perform stateful packet inspection-maintaining records of all connections passing through the firewall. They determine whether a packet is the start of a new connection, part of an existing connection or invalid. But as stateful and inline devices, enterprise firewalls add to the attack surface and can become DOS/DDoS attack targets. Firewall protection has no inherent capability to detect or stop DOS/DDoS attacks because attack vectors use open ports and protocols". As a result, enterprise firewalls are prone to become the first victims of DOS/DDoS as their capacity to track connections is exhausted."

Over half of respondents had firewalls or IPS devices that experienced a failure or contributed to an outage during a DOS/DDoS attack while stateful security devices can play a useful role, they are especially vulnerable to state-exhaustion attacks [11]. Even the latest firewalls are susceptible to DOS/DDoS attacks, so these issues remain consistent year-on-year.

4. DEFENSE-IN-DEPTH PENETRATION TESTING TEST RESULTS

The Table 1 shows the difference between Attacks and the different network set up. Five set of attacks were tested on to three different network, first with a network w/o firewall, second to an online network with firewall and lastly to a local area network w/o firewall. Five types of attacks with 5 iterations were tested on three networks. Using two way Anova with replication at 5 percent significance level, the data shows significant difference in the CPU utilization using different attacks. Figure 2 which shows high cpu consumption of the machine attacked by DOS/DDOS also strengthens the claim. Likewise, as seen in Table 2, there is a significant difference in the cpu utilization on the 3 networks. The interaction between the attacks used and the network type is present. It can be inferred that the combination of the 3 attacks show higher cpu utilization as compared with other attacks although other attacks show variation s in its effect to cpu utilization. With regards to the network security, Network without firewall shows higher cpu utilization as

compared with network with firewall. Hence, CPU utilization is affected by the interaction of the attacks used and the type of network.

Table 1. Anova: Two-Factor with Replication

SUMMARY	W/OFW	W/F_WEB	W/F_LAN	Total
Attack -L				
Count	5	5	5	15
Sum	494.9	402.5	494	1391.4
Average	98.98	80.5	98.8	92.76
Variance	0.352	13.555	0.42	84.62114
Attack -H				
Count	5	5	5	15
Sum	493.4	413.5	485.7	1392.6
Average	98.68	82.7	97.14	92.84
Variance	1.422	21.885	2.608	62.90971
Attack -J				
Count	5	5	5	15
Sum	481.4	369.2	456	1306.6
Average	96.28	73.84	91.2	87.10667
Variance	11.707	32.898	3.175	112.5478
Attack -N				
Count	5	5	5	15
Sum	496.2	438.3	489.5	1424
Average	99.24	87.66	97.9	94.93333
Variance	0.428	16.888	5.865	35.28381
L J N				
Count	5	5	5	15
Sum	500	500	500	1500
Average	100	100	100	100
Variance	0	0	0	0
Total				
Count	25	25	25	
Sum	2465.9	2123.5	2425.2	
Average	98.636	84.94	97.008	
Variance	3.963233	93.8175	11.74243	

Table 2. ANOVA–Difference in CPU Utilization between Type of Network and Attacks

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Sample (Type of Network)	1292.377	4	323.0941	43.58167	4.15E-17	2.525215102
Columns (Attacks)	2798.895	2	1399.448	188.7693	1.30E-26	3.150411311
Interaction	891.3675	8	111.4209	15.0294	7.94E-12	2.096968313
Within	444.812	60	7.413533			
Total	5427.451	74				

Figure 2. CPU consumption of the machine attacked by DOS/DDOS

5. PROPOSED DEFENSE-THROUGH-DECEPTION MODEL

The test results in Table 1 and 2 in this study exposed the weaknesses of Defense-In-Depth (DID) model in defending against the DOS or DDOS attack. A leading computer security expert and a Professor from Purdue University, Gene Spafford, reminds us that "we will never have a 100% secure system". The key to understanding and enacting comprehensive Internet security is in covering the bases and doing enough to make it difficult to hack you. Attackers look for the most vulnerable marks so the more you protect your system, the more likely they are to move on to someone easier to hack. To address this issue, the researchers

proposed a Defense-through-Deception Security Model. This model is designed to prevent an attacker who has already entered the network from doing damage in the legitimate system. The model uses traps to misdirect the attacker and delay or prevent from going deeper into the network system and reaching the intended target. If an attacker is spending time and energy breaking into a fake server, the defender is not only protecting valuable assets, but also learning about [the attacker's] objectives, tools, tactics and procedures. Sun Tzu, also advice, “when your enemy seeks an advantage, lure him further”. "The idea is to mask real high-value assets in a sea of fake attack surfaces," said Ori Bach, VP of products and marketing at TrapX Security. "By doing so, attackers are disoriented”. The Honeypot was introduced in this model as a deception tool to attract the attacker.

Figure 3 shows the proposed Defense-through-Deception Model for Campus Network Security. The proposed solution for protection from DDoS attacks would use a combination of Low-Medium/High Interaction Honeypots to protect the network system. In the network topology that is shown in Figure 3, explains that there are two potential threat actors (hackers), one comes from the outside (DMZ) and the other one is in the inside (LAN) of the Network. This model combines deception capabilities to trap, bait and engage the attackers, presenting deception attack surfaces that best match attacker’s activity [7]. This model creates a tempting environment for attackers within the campus network. Low Interaction traps were used that creates virtual hosts on a network. The hosts can be configured to run arbitrary services, and their personality can be adapted so that they appear to be running certain operating systems. The low interaction honeypots emulate vulnerabilities rather than presenting real vulnerable systems and therefore the attacker is not able to interact with it on all levels [12]. For this reason, they are safer, in that you do not have to worry about the actions of the attacker on the system but are less flexible. On the otherhand, high-interaction honeypots were also deployed, these traps offer real services or systems rather than virtual hosts to the attackers to interact with (for instance HTTP, Telnet, DNS, SSH and FTP), which makes them more risky than low interaction honeypots [13]. Furthermore, a low and high Interaction honeypot are designed primarily for research and to gather information on the attacker’s identity. This helps to determine whether it is an actual person or a bot interacting with the host. The information gathered can also reveal not only normal connection information but also session information revealing the procedures, techniques and tactics used by the attacker [14].

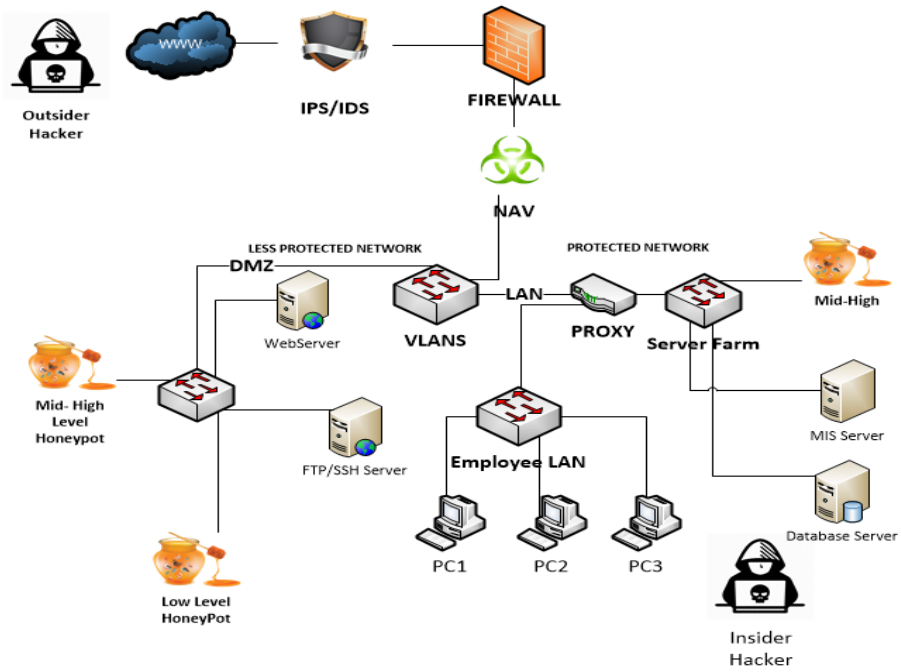

Figure 3. Defense through deception model for campus network security

6. DEFENSE-THROUGH-DECEPION MODEL TEST RESULTS

During the experiements, two honeypots (Low/Medium-High Interaction) were deployed in both the DMZ and Local Area Network (LAN) of Campus. As a result of our testing, Table 3 shows the attack methods and number of minutes that the attackers consumed attacking a wrong system. The researchers use

common DOS tools freely available in the internet. Three (3) DOS attacks have been simulated. In the first simulated attack in the honeypot; the Online DOS Attack took 21.88 mins, LAN DOS Attack consumed 92.33 Mins and Figure 4 shows the sample completed test result screenshot and lastly, High Orbit Ion Cannon (HOIC) was also used and this is the common tool used by the group 'Anonymous' in taking down the website. The test result in HOIC took 26.47 mins before the honeypot has overloaded. This test result reveals that once our honeypots have been hacked, this cause a delay on the attacker before the real systems will be compromised and it gives an alarm or warning to the Network administrator to prepare for the countermeasures and future damage to the real system.

Table 3. Attack Methods and Time Consumed by Attacker

Attack Methods	Time Consumed by Attacker
DOS ATTACK-ONLINE	21.88 Mins
DOS ATTACK -LAN	92.33 Mins
DOS ATTACK –HOIC Online	26.47 Mins

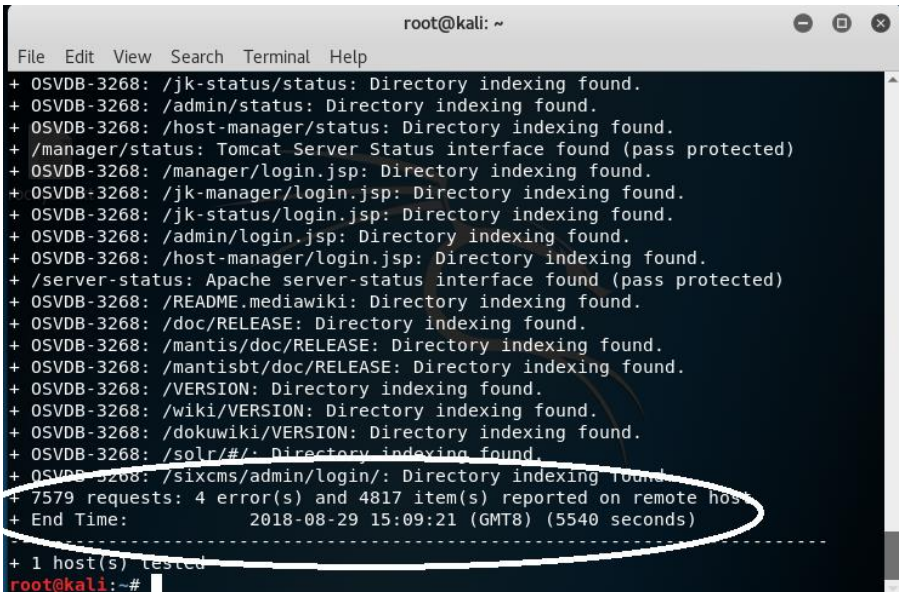

Figure 4. DOS attack test result

Furthermore, Figure 5 shows the play log of the captured attacker in our honeypot. This log reveals that we are dealing with this kind of BOT and the attacker used an automated tool called SSH Mirai Botnet [15]. The following code snippets show the worm checking for different files within the system for write access and attempting to find a part of the system open for a root exploit. In both • echo -e '\x47 \x72\x6f \x70/' > //.nippon cat //.nippon rm -f //.nippon • echo -e '\x47 \x72\x6f \x70/tmp' > /tmp/.nippon cat /tmp/.nippon rm -f /tmp/.nippon show the user trying to deposit a hidden file in file names that start with "." and in "tmp" respectively. After the attacker has probed the file, the final "rm command" is used to clean up all evidence that the attacker did anything to that file and to the system.

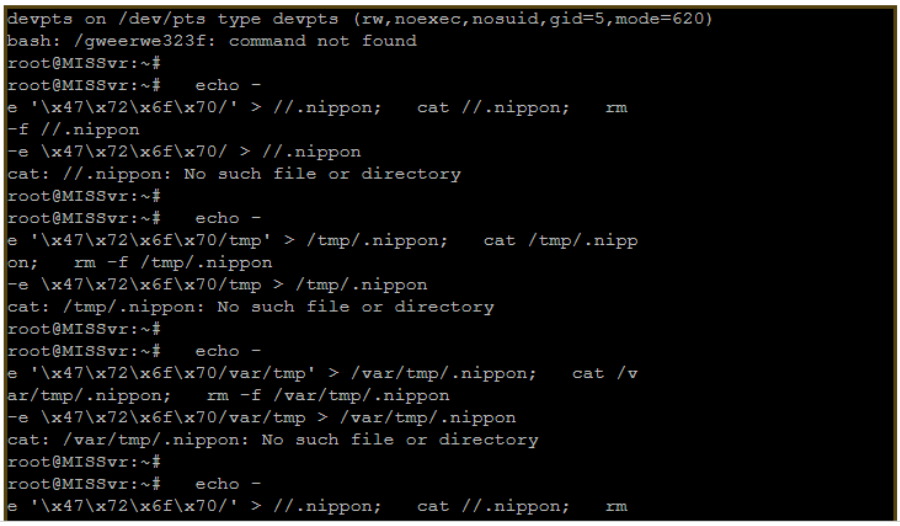

Figure 5. Attacker log

7. CONCLUSION

The Denial of Service/Distributed Denial of Service (DOS/DDoS) attacks on campus networks become increasingly common, university administrators should consider investing in a solution that safeguards their networks from these debilitating attacks. However, most of the Universities use the traditional solution defense-in-depth model and playing an increasingly limited role in DOS and DDoS protection. To address the limitation, the researchers introduced new approach and this approach would not stop the DOS/DDOS attack, instead, the approach assumes that a determined attacker will always be able to breach the perimeter. Once the perimeter is breached, defense-in-depth strategy employs additional defensive layer which is the deception model that is designed to delay the attacker so that an effective response can be mounted by bringing additional resources to counter the attacker; Lure the attacker into "trap" where the honeypots may be concentrated; Cause an attacker to consume the resources it needs to sustain an attack; and lastly, Cause an attacker to disperse their resources over a wide area, making the attack ineffective. In this sense, a defender may give up physical space to an attacker in order to gain time to organize defensive measures or countermeasures. Once the identity of the attacker is revealed, legal action against the attacker must be served.

This research also reveals that it is impossible to secure our network 100% especially in DOS/DDOS attack. This is to recommend to the Higher Education Institutions to consider the effective security measure to protect their assets by prioritizing cybersecurity mitigation plan in their organization and train personnel that will have a knowledge that is required to perform the job role of a cybersecurity analyst in a threat-centric security operations center.

REFERENCES

[1] J. Snyder (2007). Six Strategies for Defense-in-Depth: Securing the Network from the Inside Out. Retrieve 08-Jun-2007 from Tucson, Arizona: www.opus1.com/www/whitepapers/defense-in-depth.pdf.

[2] Shamim, Azra, Bushra Fayyaz, and Vimala Balakrishnan. Layered Defense in Depth Model for IT Organizations. (2014).

[3] Weia, G. U. O., and Y. U. Ya-huab. *Building Defense-in-depth Architecture for Campus Networks [J]. Journal of Jianghan University (Natural Sciences)* 2 (2007): 016.

[4] P. Small (2011). Defense in Depth: An Impractical Strategy for a Cyber World. Retrieve November 14, 2011 from SANS Institute InfoSec Reading Room: www.sans.org/reading-room/whitepapers/warfare/defense-depth-impractical-strategy-cyber-world-33896.

[5] M.Solomon (2017). Defense-in-Depth has Failed Us. Retrieve March 16, 2017 from ThreatQuotient: https://www.securityweek.com/defense-depth-has-failed-us-now-what

[6] Das, Vinu. (2009). Honeypot Scheme for Distributed Denial-of-Service Attack. 2012 International Conference on Advances in Computing and Communications. 497-501. 10.1109/ICACC.2009.146.

[7] Srivathsa S Rao,Vinay Hegde , Boruthalupula Maneesh, Jyothi Prasad N M, Suhas Suresh, Web based honeypot network International Journal of Scientific and Research Publications, Volume 3, Issue 8, August 2013

[8] Solanki, Dr. Vijender & Pal Singh, Kumar & Venkatesan, M. (2012). Firewall's Best Practices in an Organization. IJCA Proceedings on National Conference on Communication Technologies & its impact on Next Generation Computing 2012 CTNGC (3): 9-11, November 2, Volume: CTNGC - Number 3.

[9] Solanki, Dr. Vijender & Pal Singh, Kumar & Venkatesan, M & Raghuwanshi, Sudhanshu. (2013). Firewalls policies enhancement strategies towards securing network. 32-36. 10.1109/CICT.2013.6558057.

[10] Corero Network Security (2013). A Network's New First Line of Defense®. Retrieve from Hudson, Massachusetts: https://www.corero.com/resources/files/whitepapers/cns_whitepaper_firstlineofdefense.pdf

[11] ArborNetworks (2017). INSIGHT INTO THE Global Threat Landscape NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report. Retrieve from netscout: https://www.arbornetworks.com/report/

[12] Daniel Andrew, Hongmei Chi, An empirical study of botnets on university networks using low-interaction honeypots, Proceedings of the 51st ACM Southeast Conference, April 04-06, 2013, Savannah, Georgia.

[13] Nicomette, Vincent & Kaaniche, Mohamed & Alata, Eric & Herrb, Matthieu. (2011). Set-up and deployment of a high-interaction honeypot: Experiment and lessons learned. Journal in Computer Virology. 7. 143-157. 10.1007/s11416-010-0144-2.

[14] Anuar, Nor & Zakaria, Omar & Wei Yao, Chong. (2006). Honeypot through Web (Honeyd@WEB): The Emerging of Security Application Integration. Issues in Informing Science and Information Technology. 3. 10.28945/871.

[15] Kolias, Constantinos & Kambourakis, Georgios & Stavrou, Angelos & Voas, Jeffrey. (2017). DDoS in the IoT: Mirai and other botnets. Computer. 50. 80-84. 10.1109/MC.2017.201.