European Journal of Computer Science and Information Technology
Vol.4, No.3, pp.53-63, May 2016
Published by European Centre for Research Training and Development UK (www.eajournals.org)

A CONSIDERATION OF THE POSSIBILITY OF DOS AND DDOS ATTACKS THAT COULD GUARANTEE DOWNTIME AND UNAVAILABILITY OF SERVICES TO CUSTOMERS FOR BUSINESSES AND GOVERNMENT INSTITUTIONS IN GHANA.

Edward Danso Ansong[1], James Ben Hayfron-Acquah[2]

[1]Department of Computer Science & Information Technology, Valley View University, Accra-Ghana
[2] Department of Computer Science, Kwame Nkrumah University of Science & Technology, Kumasi-Ghana

ABSTRACT: *This paper discusses the possible security attacks that most services provided by businesses and government organizations are vulnerable to. Specifically exhausting discussion on Denial of Service and Distributed Denial of Service attacks and the measures to address this issue.*

KEYWORDS: DoS, DDoS, Services, Customer, Business, Government, Ghana

INTRODUCTION

The internet was originally developed to enhance communication by connecting computer networks through the Standard Internet Protocol Suite (TCP/IP). Exchange of information has been enhanced due to the internet allowing a single platform for interaction, accessibility is high. The internet is an open space, this therefore allows its users an unlimited amount of freedom to exploit it positively or negatively. It has become the problem of concern to services and customers for businesses and government institutions that most computers which are connected to internet have become vulnerable various forms of attack. Such attacks are Denial of Service (DoS), Distributed Denial of Service (DDOS), Virus infection Attack, Network Sniffing Attack, Eaves Dropping Data Modification Identity Spoofing (IP Address spoofing) Password Base Attack, Man-In-Middle Attack Compromised-Key Attack, Sniffer Attack, Application-Layer Attack, SQL Injection Attack are just to mention a few. Denial of Service (DoS) and Distributed Denial of Service (DDoS) are form of network hacking attempts which is intended to disrupt an organization network services and website services. Denial of Service is an attack which is characterized by explicit attempts by attackers to prevent legitimate users of service from using that service. While Distributed Denial of Service is when an attacker incidentally uses multiple systems to either ping or send computer worm using vulnerabilities in well-known operating systems and application like Windows operating system, and some categories of Linux. DoS attacks has been categorized into 3 major groups namely; *Bandwidth attacks, Protocol attacks and Software vulnerability attacks* according to [1] but technically it is grouped into two major categories that is application and network in [2]. There are nine types of DoS attacks according to [1], this research addresses issues of DoS and DDoS attack that causes downtime and Unavailability for services to customers for businesses and government institutions in Ghana.

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

The problem

Ghanaian companies and business are losing billions of Ghana Cedis on cybercrime and Ghana has been classified as Africa's second ranking in cybercrime according to [3] and it is necessary to put some measures to fore stall such an alarming canker, if the situation is not properly addressed, software and computer viruses , Denial of Service and Distributed Denial of Service may in the future mutate data and alter Internet Protocol addresses in the same manner that AIDS does to the human immune system. This would result in emails being misdirected, web sites being relocated and the internet infrastructure being compromised radically. It has come to the notice that some service providers in Ghana have been blacklisted which is no fault of theirs but because miscreant have been using their services to attack other people services.

History

Denial-of-service attacks surfaced in the last decade of the twentieth century [1]. DDoS attacks emerged in the last few years are sophisticated and lethal, first being seen in late June and early July of 1999. The first well-documented DDoS attack appears to have occurred in August 1999, when a DDoS tool called Trinoo was deployed in at least 227 systems, of which at least 114 were on Internet2, to flood a single University of Minnesota computer; this system was knocked off the air for more than two days. The first well-publicized DDoS attack in the public press was in February 2000. On February 7, '*Yahoo!'* was the victim of a DDoS during which its Internet portal was inaccessible for three hours. On February 8, Amazon, Buy.com, CNN, and eBay were all hit by DDoS attacks that caused them to either stop functioning completely or slowed them down significantly. And, on February 9, 'E*Trade' and 'ZDNet' both suffered DDoS attacks. Analysts estimated that during the three hours Yahoo was down, it suffered a loss of e-commerce and advertising revenue that amounted to about $500,000.

According to book seller 'Amazon.com', its widely publicized attack resulted in a loss of $600,000 during the 10 hours it was down. During their DDoS attacks, Buy.com went from 100% availability to 9.4%, while 'cnn.com' website users went down to below 5% of normal volume and 'Zdnet.com' and 'E*Trade.com' were virtually unreachable. Schwab.com, the online venue of the discount broker Charles Schwab, was also hit but refused to give out exact figures for losses. One can only assume that to a company that does $2 billion dollars weekly in online trades, the downtime loss was huge [4].

Issues in Ghana

In 2012, a report of a DoS attack on the Ministry of Justice and Attorney General website which was captured on most of the social media like myjoyonline.com and ghanafilla.net [5]. Another attack was on **Kenya's State Law Office or Office of the Attorney General** which was defaced by an Algerian hacker [6]. Measures to curb this issue require utmost importance in order to secure future investments in e-commerce in Ghana. It is necessary to take steps to fore stall such canker which is eating the fabric of our country because some business organizations trade online, advertise, execute transactions which require, Master card, ATA card, Visa card, Credit card. Another aspect of DDoS attacks have long been used for criminal purposes, but recently they have increasingly been used as a form of protest against the activities of both governments and major corporations. Such attacks receive widespread publicity in the mass media and are usually the subject of investigations by law enforcement agencies. We can expect to see the sites of government bodies in various countries increasingly come under attack as DDoS-based protests gain in popularity. This does not mean that DDoS attacks are no longer

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

used for extortion and blackmail. The victims, however, rarely acknowledge such incidents in order to protect their reputation. "Cybercriminals are also increasingly using DDoS attacks as a diversionary tactic when launching more sophisticated attacks such as those on online banking systems. Complex attacks of this nature are particularly damaging in that they can cause significant losses for the financial institutions as well as their clients" according to Yuri Namestnikov [7].

Factors to the Problem

The issues of DoS and DDoS attack is gradually trending in Ghana, services that are incapable of responding to requests in a timely manner as expected might under such attacks provided the obvious vulnerabilities are present in such services. Social engineering is a technique that contributes to such attacks.

How to find service to target

The first step to mounting DoS is to find a service you can target. This would be something with open ports, something with vulnerabilities, and certainly something that will accept incoming connections. Some of these services include:

a. Web servers
b. DNS servers
c. Email servers
d. FTP servers
e. Telnet servers
f. VoIP

These services almost always accept incoming connections. Often times, they even accept unauthenticated connections. Once you've found a service to attack, the next step would be to overcome that service.

Ideally, it should be a service that doesn't have a maximum limit to the number of connections. The best way to find out whether a service doesn't have an upper boundary on number of connections is to send it a few hundred thousand connections and then observe what happens.

But to achieve optimal effect, you have to send specific queries and information. For example, if you're targeting a Web server with a search engine, do not just request a web page or slap F5 a bunch of times. Instead, request a complex search query or something that's going to consume a significant amount of horsepower to resolve.

If doing that just once already has a noticeable impact on the backend, then doing that a hundred times a second would probably bring that server down. You can do the same thing against a DNS server. You can force it to resolve complex DNS queries that aren't cached. Do it often enough to bring that service down. For an email service, you can send lots of large email attachments if you can get a legitimate account on its server. If you can't, it's pretty easy to spoof that kind of attack. Those are some simple service-based Denial-of-Service attacks that you can mount almost universally. Again, it's just a matter of finding the services that will allow you to do this.

DDoS attack, the attacking packets come from tens or hundreds of addresses rather than just one, as in a "standard" DoS attack. Any DoS defense that is based upon monitoring the volume

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

of packets coming from a single address or single network will then fail since the attacks come from all over. Rather than receiving, for example, a thousand gigantic Pings per second from an attacking site, the victim might receive one Ping per second from 1000 attacking sites.
DDoS attack can be used to send so many traffics or simply flood a host with traffic. That can still work, except that the attack might not be as elegant and would certainly require a bit more traffic. The Ping of Death is a large ICMP packet. The target receives the ping in fragments and starts reassembling the packet. However, due to the size of the packet once it is reassembled, it is too big for the buffer and overflows it. This causes unpredictable results, such as reboots or system hangs. Windows NT is capable of sending such a packet. By simply typing in "ping -165527 -s 1 target" you can send such a ping

How to mount dos and ddos attack

The Ping of Death is a large ICMP packet. The target receives the ping in fragments and starts reassembling the packet. However, due to the size of the packet once it is reassembled, it is too big for the buffer and overflows it. This causes unpredictable results, such as reboots or system hangs.

Windows NT is capable of sending such a packet. By simply typing in "ping -165527 -s 1 target" you can send such a ping command or using ping command to know the number of bit of data that can be transmitted within a web server (ping 192.168.1.10 –f –l 1472 or 1473) interesting several ping command or capture a machine by installing Trojan horse on the client machine and used it to attack the server or attacker compromises 400 or more computers by installing special client software to send commands to 400 or more computers to direct them to flood a victim network.

After that, you choose a port that is open by using some utilities tools like Nmap, Zenmap, Freeport scan to check the port that are open and then accepts incoming connections. For example, I would choose port 80 to mount a Web-based attack. I would then select TCP to specify which resources I want to tie up.

Depending on the situation, one client attacking this way may or may not immediately affect the performance of the server. But a Denial of Service attack doesn't have to stop with just one client.

In a typical DoS attack, you would mount this attack against different ports at different times and try to footprint whether your actions are affecting services, impacting them in a noticeable way, or, better yet, able to shut the server down.

If not, you could scale this up by running the Low Orbit Ion Cannon on a dozen machines or even a hundred machines at the same time. A lot of this can be scripted. Meaning, you can capture the traffic and replay it at the command line on different targets or play it as part of a script from different attackers, which could be your peers, your zombies, or both.

Another form that a DDoS and DoS attacker does is to use some utility software like HTTrack to mirror your site to understand the structure of the site and under the language it was used to design the site. The attacker can find the loop holes in it and capitalize on it.

This process may start to slow down a little bit, partially because you'll be consuming resources on the client and also because the server itself would either be running out of resources or starting to defend itself against your attack. Some hosts can be configured to look for patterns

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

to identify attacks and start defending itself. To counter their defense you could, for example, stop the attack momentarily (by clicking the same button you clicked to mount the attack) and change the port you're attacking. To add a little confusion, you could slow the attack a little bit.

In addition, we'll change the port from port 80 to port 88, actually port 80 is sometimes open. Once you're done changing the settings, you can resume the attack.

With that, you would be attacking a different port, which amounts to a different service, at a slightly different way, and at a different speed. Speed is really only important if you're attacking from one client. If you have a hundred different clients attacking at the same time you can slow things down at each individual client and still be able to mount quite an effective attack.

Secondly the Distributed Denial of Service (DDoS) attack would be practically that same attack carried out by many different people at exactly the same time. A DDoS attack is only complex in terms of scale. The attack itself from the perspective of each attacker.

One reason why some people use malware to launch these attacks is because malware can be timed to launch the attacks at exactly the same moment.

One of the other disconcerting things about DDoS attacks are that the handler can choose the location of the agents. So, for example, a handler could target several Ghana Police Service sites as victims and employ agents that are all in countries know to be hostile in Ghana Police Service. The human attacker, of course, might be sitting in China. Like DoS attacks, all of the DDoS attacks employ standard TCP/IP messages -- but employ them is some non-standard ways. Common DDoS attacks have such names as Tribe Flood Network (TFN), Trin00, Stacheldraht, and Trinity.

Statistic Report

According to our statistics for 2011, 89% of DDoS traffic was generated in 23 countries. The distribution of DDoS sources was fairly evenly spread among those countries, with each accounting for 3-5% of all DDoS traffic.

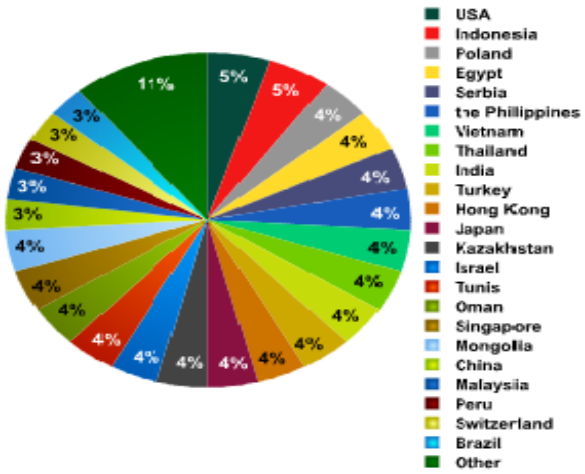

Fig.1 Distribution of DDoS attacks by country in 2011

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

Most attacks came from the US and Indonesia with each country accounting for 5% of all DDoS traffic.

The US's leading position is down to the large number of computers in the country. Last year, US law enforcement authorities waged a successful anti-botnet campaign which led to the closure of a number of botnets. It is quite possible that cybercriminals will try to restore the lost botnet capacities and the number of DDoS attacks will increase.

Meanwhile, the large number of infected computers in Indonesia means it also ranks highly in the DDoS traffic rating. In Q2 of 2011, almost every second machine (48%) on the Indonesian segment of Kaspersky Security Network, Kaspersky Lab's globally-distributed threat monitoring network, was subjected to a local malware infection attempt. Such a high percentage of blocked local infection attempts is the result of a large number of unprotected computers being used to spread malware.

Those countries responsible for less than 3% of all DDoS traffic included countries with high levels of computerization and IT security (Japan, Hong Kong, Singapore) as well as countries where the number of computers per person is significantly lower and antivirus protection is far from perfect (India, Vietnam, Oman, Egypt, the Philippines, etc.).

Distribution of attacked websites by online activity

In Q2, online trading sites, including e-stores, auctions, buy and sell message boards etc., were increasingly targeted by cybercriminals – websites of this category accounted for a quarter of all attacks. This is hardly surprising: online trading largely depends on a website's availability, and each hour of downtime results in lost clients and lost profits. This explains why these types of sites were targeted most often – competitors or straightforward extortion were usually behind the attacks.

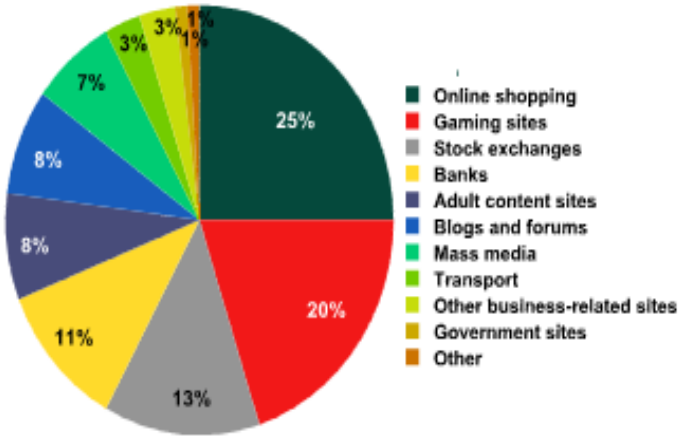

Fig.2 Breakdown of attacked sites by areas of activity. Q2 2011

Gaming-related sites were the second most popular targets. As Kaspersky Lab's monitoring system indicates, most attacks targeted EVE Online and its related websites. The MMORPG space-themed game had 357,000 active gamers as of late 2010. One site in particular that publishes EVE Online news experienced one of the most prolonged attacks, DDoS bots targeted it for 35 days. WoW and Lineage were also subject to some unwanted cybercriminal attention, although it was the games' various pirate servers that suffered most.

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

The websites of electronic stock exchanges and banks occupy third and fourth places respectively. Cybercriminals attack trading platforms in order to cover their tracks after fraudulent transactions rather than to extort money. Typically, both the financial organizations and their clients lose money when such operations are performed. Therefore, how robust a service is against DDoS attacks is a factor that directly affects its reputation.

Interestingly, quite a substantial proportion of DDoS attacks targeted mass media sites (7%), and blogs and forums (8%), which are essentially a form of social mass media. We have already discussed the attacks on LiveJournal above. There is always someone who disagrees with a freely expressed opinion and it appears DDoS attacks are now being used as a means to silence media channels.

Governmental sites make up 1% of all attacked websites, although this statistic does not include attacks carried out by the group Anonymous using the "voluntary" botnet based on LOIC, a program used to arrange attacks. DDoS attacks are increasingly being used to lead protests against government agencies in many countries, and we can expect to see more similar attacks in the future, especially at crucial stages in the political processes of societies.

Types of DDoS attacks: In Q2, Kaspersky Lab's botnet monitoring system intercepted over 20,000 web-borne commands to initiate attacks on different sites.

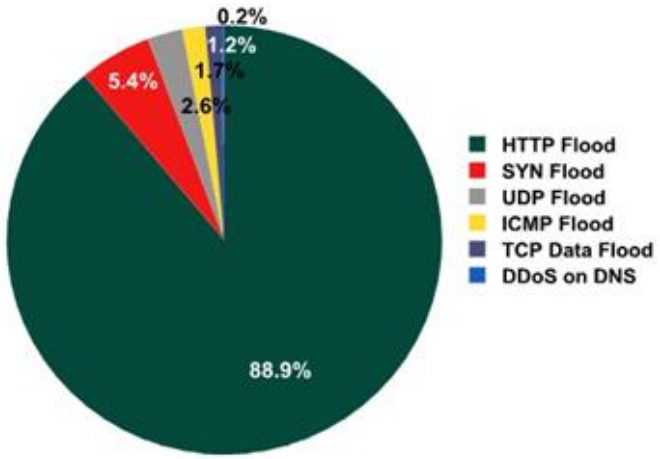

Fig 3. Chart of the types DDoS flooding attacks

HTTP flood is the most popular (88.9%) method of attacking a website: a huge number of HTTP requests are sent to the targeted site over a short period. In most cases they look just like regular user requests, making it difficult to filter them out. This makes this type of DDoS attack more popular among cybercriminals than others.

SYN Flood attacks are the second most popular type of attack (5.4%). During such attacks, botnets send multiple data packages to the web server in order to establish a TCP connection. Cybercriminals manipulate packages so the server connections are left half open rather than established. Since a server can only maintain a limited number of connections at any time and botnets can generate lots of requests in short periods of time, the targeted server soon becomes unable to accept connections from regular users.

DDoS attacks on DNS servers (0.2%) were the least popular type of attack. As a result of this kind of attack DNS servers are unable to convert site names into IP addresses, so the sites

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

serviced by the targeted server become unavailable to users. This type of attack is particularly damaging in that a single attack can render hundreds or even thousands of websites unavailable. During a DDoS attack on one web resource, the bots received commands to send requests to an average of two web pages on the targeted site. If we compare the number of attacks delivered on site names and those on IP addresses, it can be seen that it is mostly IP addresses that are attacked: 72% of all attacks targeted IP addresses.

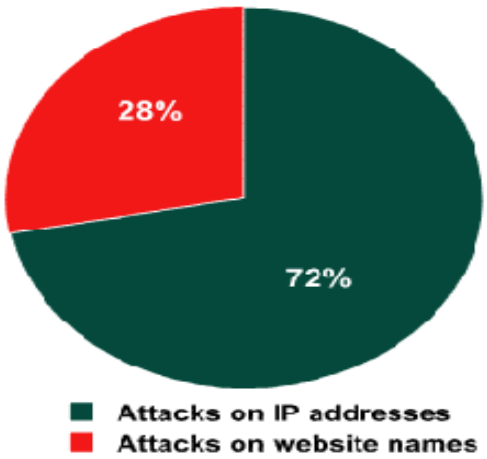

Fig.4 Attacks on IP addresses and on website names

Breakdown of DDoS attacks by targets: site names vs. IP addresses quarter 2 in 2011:Having analyzed all the available data, we can say on which days of the week cybercriminals prefer to carry out their attacks to bring down a site.

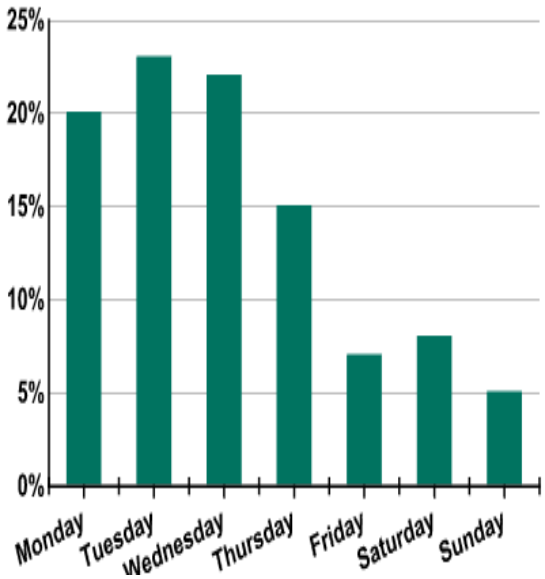

Fig.5 Breakdown of DDoS attacks by days of the week in 2011

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

Weekdays see the most active use of the Internet. It is on these days that various web resources are most in demand and that DDoS attacks are likely to inflict the maximum amount of damage on websites. Another important factor is that greater numbers of computers are switched on on weekdays, so there are more active bots. As a result, cybercriminal activity peaks from Monday to Thursday on these days an average of 80% of all DDoS attacks take place.

This is vulnerability list which was captured in 20 January 2014 to 20 February 2014 by Kaspersky. It represents the vulnerability of some countries. Ghana rank six in vulnerability list in Africa, vulnerable our networks to such an attack

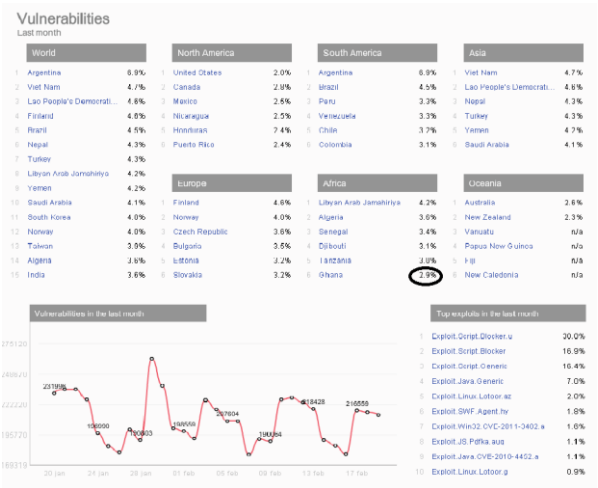

Fig 6. Vulnerabilities Ranking

Reasons for ddos and dos attack

Distributed denial-of-service attacks are no longer being carried out simply to make a profit. Cybercriminals are increasingly targeting government resources or the sites of big companies to show off their skills, demonstrate their power or, in some cases, as a form of protest. These are exactly the sort of attacks that get maximum publicity in the media.

The most active hacker groups in the second quarter of 2011 were LulzSec and Anonymous. They organized DDoS attacks on government sites in the US, the UK, Spain, Turkey, Iran and several other countries. The hackers managed to temporarily bring down sites such as the US Central Intelligence Agency (CIA) and the British Serious Organized Crime Agency (SOCA). This shows that even government sites safeguarded by specialist agencies are not immune to DDoS attacks. The same incident happen in Ghana in 2013 when the ministry of Justice and Attorney General Website was threatened with an attack.

Attacking government sites is a risky business for hackers because it immediately attracts the attention of law enforcement authorities. In quarter 2 of 2011, for example, more than 30 members of Anonymous were arrested on suspicion of launching DDoS attacks on government sites [7]. More arrests are likely to follow as authorities continue their investigations. However, not all those involved are likely to be convicted because participation in the organization of a DDoS attack is still not considered illegal in many countries [7].

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

The consequences of such attacks in Ghana

As the Ghanaian government and Institution are migrating into e-platform like the introduction of e-policing services it necessary to take measures because people engage in advance countries and a lot of people are losing their credit cards and companies are collapsing. Some groups of people have turned it in a form of gains by shutting down people website and destroying company's machines. This attackers are purposely perpetrated by the youth and as technology is advancing and population increasing, it is necessary to take measures to curb this menace, as people are hired to carry such attacks on organizations' do disrupt service productivity. This attacks clear room for other security vulnerability attacks.

RECOMMENDATION

A system administrator should scan all servers and client port to know the open and close port frequently by using manually or software utilities like Zenmap, Freeport scanner etc. the administrator should find out the loop holes or vulnerabilities in all the operating system and the application software that they are using. Keep an audit trail that describes what was changed and reasons why. Test your network both locally and externally by using most of the hacking utilities. There should be firewall installed in the network to protect an intrusion attack on a network (that is an organizations or personal) and a proper antivirus should be installed on all client and server computer to avoid any malware or virus and worm infection. Because human beings are the weakest link in terms of security implementation within an organization, serving personnel within every organization, government or non-government must undergo a thorough systems security safety measures orientation.

REFERENCES

[1] Tariq, Muhammad, "Dos and DDoS Attack Types and Preventions," Pakistan.

[2] ollmann, Gunther, "Understanding the Modern DDoS Threat".

[3] "My Joy Online," Myjoyonline.com, 31 July 2013. [Online]. Available: http://edition.myjoyonline.com/pages/news/201307/110530.php. [Accessed 18 August 2014].

[4] G. C. Kessler, November 2000. [Online]. Available: http://www.garykessler.net/library/ddos.html. [Accessed 21 August 2014].

[5] P. Kwasi, "Ghanafilla.net," 26 November 2012. [Online]. Available: http://www.ghanafilla.net/attorney-generals-website-hacked-by-argentine-group/. [Accessed 12 August 2014].

[6] E. Kovacs, "softpedia.com," 30 April 2013. [Online]. Available: http://news.softpedia.com/news/Website-of-Kenya-s-Office-of-Attorney-General-Hacked-349529.shtml. [Accessed 12 August 2014].

[7] Kaspersky lab, "Kaspersky.com," Kaspersky, 29 August 2011. [Online]. Available: http://www.kaspersky.com/au/about/news/virus/2011/Expect_More_DDoS_Attacks_Tomorrow. [Accessed 22 August 2014].

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

[8] M. Danseglio, "pluralsight.com," 15 November 2012. [Online]. Available: http://blog.pluralsight.com/videos/ethical-hacking-how-to-create-a-dos-attack. [Accessed 10 August 2014].

[9] "The Hack FAQ," [Online]. Available: www.nmrc.org/pub/faq/hackfaq/hackfaq-05.html. [Accessed 18 August 2014].

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)