IJCTA, 8(4), 2015, pp. 1309-1317
© International Science Press

Analysis, Impact and Proposed Defense Mechanisms of DoS Attacks

Aman Singh,* Divya Anand, Salil Batra*****

Abstract: In this paper, we have discussed about execution of DoS attacks, its impact and proposed defense mechanisms in Wired LAN. ARP cache poisoning and DNS spoofing attacks have been executed as a form of DoS attacks. This research work is divided into five parts – Elemental Concepts, Preparing and Planning for the Attacks, Executing the Attacks, Impact of Attacks (in terms of bandwidth consumption) and Proposed Defense Mechanisms. Backtrack operating system is used to attack the target hosts. In-built command line utilities “arpspoof” and “ettercap” are used for ARP cache poisoning and DNS spoofing attacks respectively. Key motive behind the attack is to prevent trusted users of a legitimate network from accessing internet services. Results of these live attacks and their impact on the target network bandwidth are depicted through images. Defense mechanisms have also been proposed to detect and prevent these attacks.

Keyword: DoS Attacks, ARP Cache Poisoning, DNS Spoofing, Address Resolution Protocol, Domain Name Server

1. INTRODUCTION

In this section, we have discussed about DoS attacks, its consequences, reason for executing and a concise description about wired LAN. Apart from it, a brief description of the content to be covered in Elemental Concepts, Preparing and Planning for the Attacks, Executing the Attacks, Impact of Attacks and Proposed Defense Mechanisms.

DoS attacks prevent trusted users from accessing legitimate services in a network segment. These attacks either effect a specific target or disrupt the entire network [1]. Consequences of DoS attacks are slowing down network performance, dramatic increase in malicious packets over network, blocking of system requests, inability to access any specific network resource and unavailability of required services [2]. Reason for executing DoS attacks to the target organization network are: to make necessary network services unavailable, to cause financial or reputation loss, to disrupt the internet services, to execute phishing attacks and to do identity theft. For the experimentation of these attacks a wired LAN infrastructure Lab has been setup that consists of 36 systems connected together via a switch. Linux and Windows OS are installed in each system using dual boot mode but former is the default operating system. This lab is extendable up to 100 systems for supporting temporary hosts. Temporary hosts refer to those who attached their systems to wired LAN for accessing internet services for a limited period of time. Each machine is communicating with each other through a switch. It is assumed that the attacker is an internal user having malicious intensions to harm the organization. For attacks, intranet network is considered because security administrators usually concerned about safeguarding their network from external users due to which internal attackers befool network administrators and disrupt network services easily. A conventional wired LAN LAB setup uses ethernet cables to connect systems through switches. Using ethernet network has several advantages viz high speed, reliability, better performance and security [3]. Ethernet is a technology introduced for local area networks (LANs) in which systems communicate by sending data in form of frames containing source and destination addresses along with an error checking functionality (through which scratched data can be detected and re-transmitted).

* Department of Computer Science and Engineering, Lovely Professional University Jalandhar, Punjab, India, 144411
Email:amansingh.x@gmail.com & divyaanand.y@gmail.com & salilbat13@yahoo.com

As already stated, this research work is a step by step process. In elemental concepts, working of ARP protocol and DNS server is discussed. Preparing and Planning for the Attacks section deals with techniques used to gather information about target networks. Information gathering includes finding IP addresses range, gateway address, services running on network, operating systems in use, daemon banner grabbing and DNS addresses of target network. Executing the Attacks section is regarding tools used for ARP cache poisoning attack, DNS spoofing attack and their results received which are shown through images. The next section covers impact of attacks, in terms of bandwidth, during various phases. In last section, defense mechanisms are proposed to detect and prevent both the attacks.

2. ELEMENTAL CONCEPTS

In this section, working of ARP Protocol and DNS server is discussed. Address Resolution Protocol (ARP) is used to find physical address of a machine if its IP address is already known [4]. Physical address is also called hardware or MAC address. ARP works at data link layer of OSI model and internet layer of TCP/IP model. It uses two types of packets namely - ARP request and ARP response [5]. ARP request packet is of broadcast nature while ARP response packet is of unicast nature. For example if system A wants to communicate with system B, but system A doesn't have MAC address of system B. In this scenario, system A broadcasts an ARP request packet to entire network segment. This packet contains IP address of system B in destination protocol address field and MAC address as FF:FF:FF:FF:FF:FF in destination hardware field. FF:FF:FF:FF:FF:FF signifies broadcast MAC address which means destination system MAC address is unknown. Each host in the network receives that broadcast message but, system having same IP address as in destination IP field of the packet replies. As packet is intended for system B, this time it sends a unicast ARP response packet to system A, containing its own MAC address. ARP protocol has its own limitations which allow an attacker to execute ARP cache poisoning attack on victim system/gateway in a LAN. ARP doesn't provide any authentication service that prevents attackers from sending spoofed ARP responses. Attacker can easily redirect network (LAN) traffic to its own machine by poisoning cache table of victim's system [7]. This spoofed packet contains IP address of target system X and MAC address of attacker. When target system receives this spoofed ARP response packet it immediately updates its own ARP cache table for further communication. Next time when any host sends data packets to system X, they are actually received by attacker system. Because MAC address associated with system X IP addresses is of attacker's machine [6, 8]. This is the basic working of ARP cache poisoning attack. Another form of DoS attack is DNS spoofing. In this, attacker poisons the gateway of a LAN with false IP address information regarding DNS server and redirects user DNS requests to his own system [9,10]. The first step in this attack is to poison the switch and redirect all DNS requests to attacker's machine. Next time, whenever any user sends DNS request to switch, it automatically forwards that request to attacker's system. The system replies to the user with a fake IP address. This fake IP address is either of attacker system itself or of any other machine on which fake websites are set up. Now it's his choice either to redirect user's request to real website or block all data packets [11]. If attacker's motive is to only sniff user's credentials without his prior knowledge then his system will simply redirect it to real website but if motive is to execute DoS attack then he simply blocks requests sent by victim machine and also disrupt internet services.

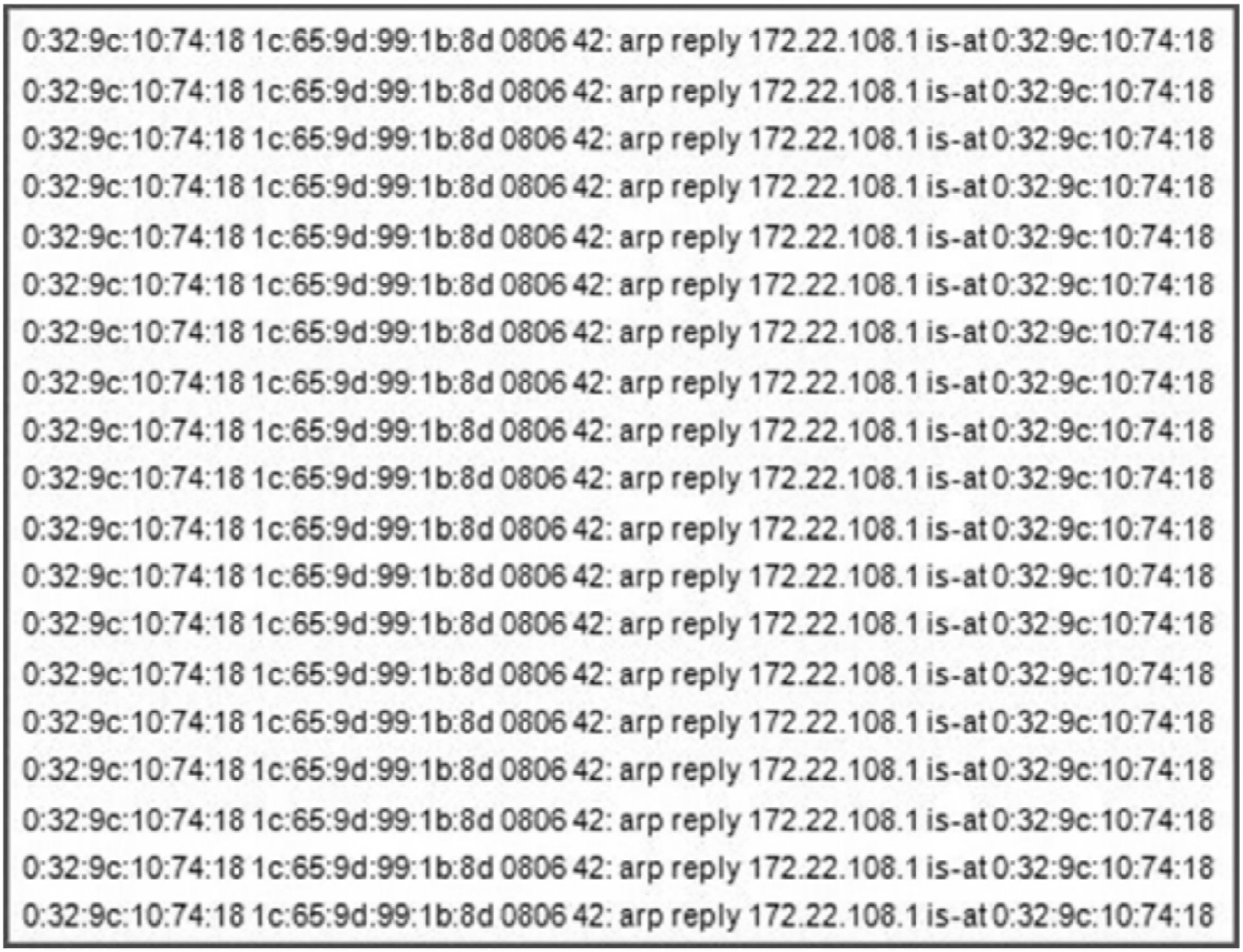
3. PREPAIRING AND PLANNING FOR THE ATTACKS

In this step, attacker is more concerned about gathering information of target network. Details such as IP addresses of systems in LAN, gateway IP address, network blocks, intranet DNS IP addresses, internet DNS IP addresses, checking live hosts, subnet mask plays a vital role. Information such as gateway address will be needed for spoofing ARP cache table and subnet mask is used to calculate number of hosts in a network segment. Identity can be hidden by IP and MAC address spoofing or by any one of the two. Spoofing depends on type of configuration on the network. If a fixed number of MAC addresses are allowed to communicate, then it is difficult to use any random MAC address in order to hide identity. Ping utility is used to find IP addresses information. Ping requests are sent to victim system to check whether it is alive or not. If availability of multiple hosts is to be checked then ping sweeping technique will be used. Nmap tool is also used to gather important information regarding target network [12, 13. 14, 15]. “arp” command is used to check local cache entries of IP - MAC address pairing of entire wired LAN. List of some commands used to gather information is mentioned below.

ping 172.18.18.144 (victim IP address), ping -c 6 172.18.18.144 (-c → to send number of pings), nmap -sP 172.18.18.144 (scan single IP address), nmap -sP -v 172.18.18.144 (ping scan), nmap -sP –PE 172.18.18.140-180 (scan multiple systems), nmap -sP 172.18.18.140/26 (scan entire network), nmap -sS 172.18.18.144 (TCP SYN scan), nmap -O 172.18.18.144 (operating system detection), nmap -sU 172.18.18.144 (UDP port scan), ping 172.19.5.168 >result.txt (save output in text file), arp -a (display current ARP table), ifconfig (check IP address), route –n (shows IP address, netmask, gateway address), netstat -n (check content of routing table), netstat -rn (check content of routing table), ifconfig eth0 (display current configuration), ifconfig eth0 172.18.18.145 (assigning an IP address).

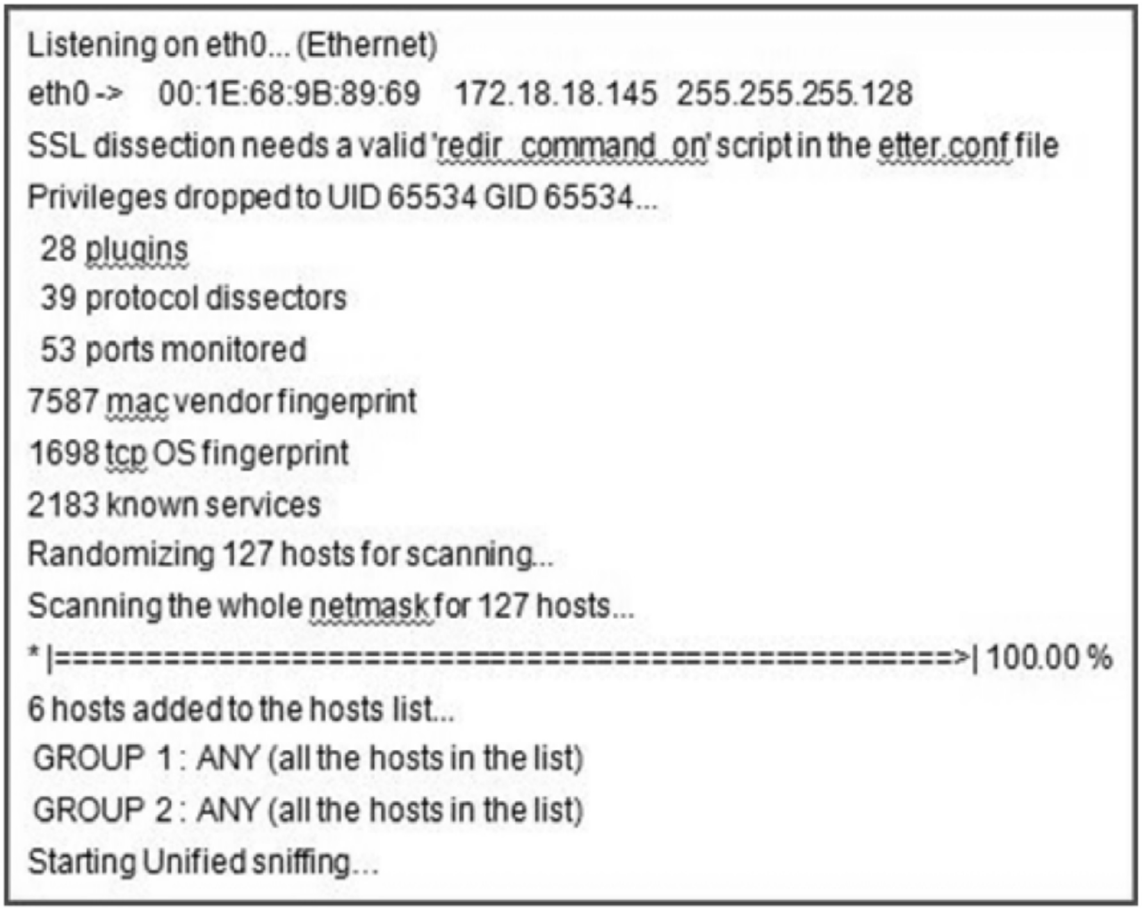
4. EXECUTING THE ATTACKS

Once attacker has successfully gathered all necessary information, next step is to execute the attacks either on a single system or on entire network using backtrack. It is one of the most widely used operating system used by penetration testers and forensic experts in network scannings. Backtrack is largely used for information gathering, vulnerability assessment, exploiting networks, privileging escalation, maintaining access, stress testing, reverse



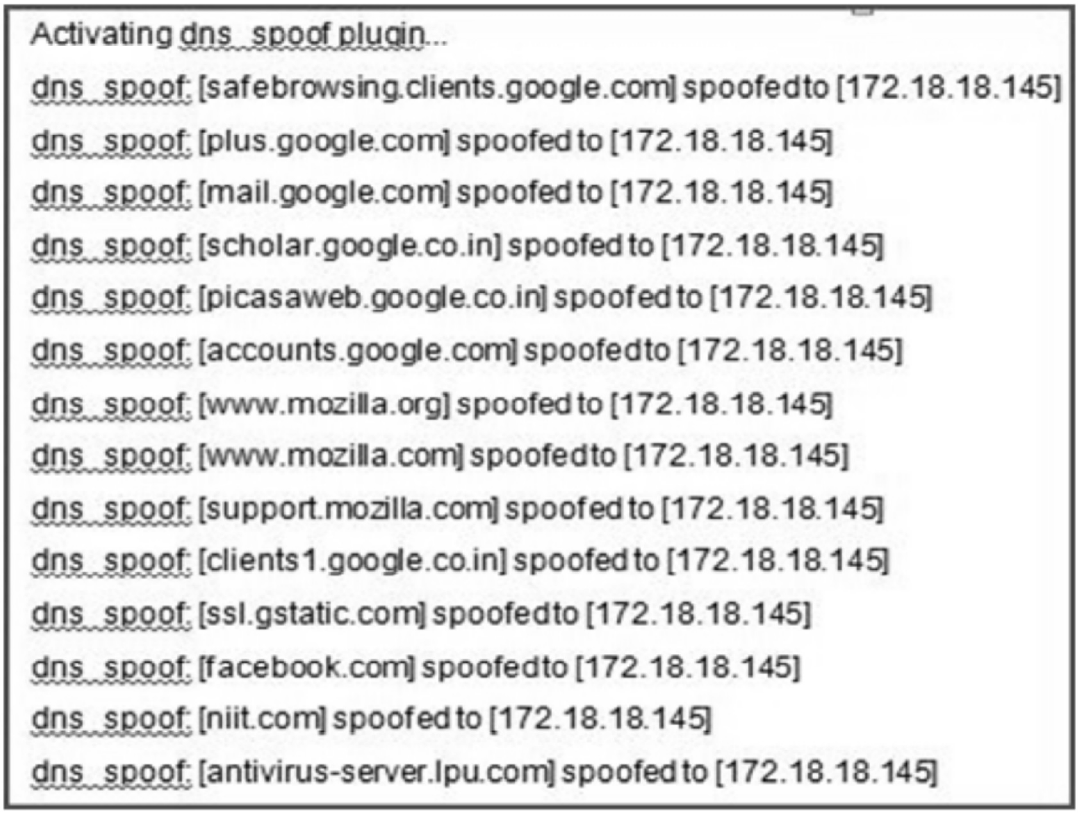
```
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
0:32:9c:10:74:18 1c:65:9d:99:1b:8d 0806 42: arp reply 172.22.108.1 is-at 0:32:9c:10:74:18
```

Figure 1: Results of ARP cache poisoning attack



```
Listening on eth0... (Ethernet)
eth0 ->    00:1E:68:9B:89:69    172.18.18.145  255.255.255.128
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to UID 65534 GID 65534...
  28 plugins
  39 protocol dissectors
  53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services
Randomizing 127 hosts for scanning...
Scanning the whole netmask for 127 hosts...
* |==================================================>| 100.00 %
6 hosts added to the hosts list...
 GROUP 1 : ANY (all the hosts in the list)
 GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...
```

Figure 2: Results of ARP cache poisoning attack



```
Activating dns_spoof plugin...
dns_spoof: [safebrowsing.clients.google.com] spoofed to [172.18.18.145]
dns_spoof: [plus.google.com] spoofed to [172.18.18.145]
dns_spoof: [mail.google.com] spoofed to [172.18.18.145]
dns_spoof: [scholar.google.co.in] spoofed to [172.18.18.145]
dns_spoof: [picasaweb.google.co.in] spoofed to [172.18.18.145]
dns_spoof: [accounts.google.com] spoofed to [172.18.18.145]
dns_spoof: [www.mozilla.org] spoofed to [172.18.18.145]
dns_spoof: [www.mozilla.com] spoofed to [172.18.18.145]
dns_spoof: [support.mozilla.com] spoofed to [172.18.18.145]
dns_spoof: [clients1.google.co.in] spoofed to [172.18.18.145]
dns_spoof: [ssl.gstatic.com] spoofed to [172.18.18.145]
dns_spoof: [facebook.com] spoofed to [172.18.18.145]
dns_spoof: [niit.com] spoofed to [172.18.18.145]
dns_spoof: [antivirus-server.lpu.com] spoofed to [172.18.18.145]
```

Figure 3: Results of ARP cache poisoning attack

engineering and cyber forensics. It contains number of tools used to scan and attack networks. But we are only concerned with two of these i.e. “arpspoof” and “ettercap”. The former is used to execute ARP cache poisoning attack while the later is for DNS spoofing attack. In arpspoof tool, attacker has to specify which interface to use, a particular target host to poison ARP cache table and gateway address [16]. DNS spoofing attack is executed by using ettercap (used for packet sniffing and network protocol analysis), which is an inbuilt tool in backtrack. First step in DNS spoofing attack is to configure etter.dns file. Use “locate” command to search etter.dns file. Then use gedit command to edit that file. After that, run ettercap command using dns_spoof plugin in order to poison the switch and redirect all LAN traffic to attacker’s system [17,18]. Now numerous things can be done with this traffic, either simply intercept it or block it to interrupt internet services. Figure 1 shows the results of ARP cache poisoning attack and Figure 2 and 3 shows the results of DNS spoofing attack.

5. IMPACT OF ATTACKS

After executing ARP cache poisoning attack and DNS spoofing attack on wired LAN, next step is to examine bandwidth before the attack (Figure 4), during the attack (Figure 5) and after the attack (Figure 6). The key point

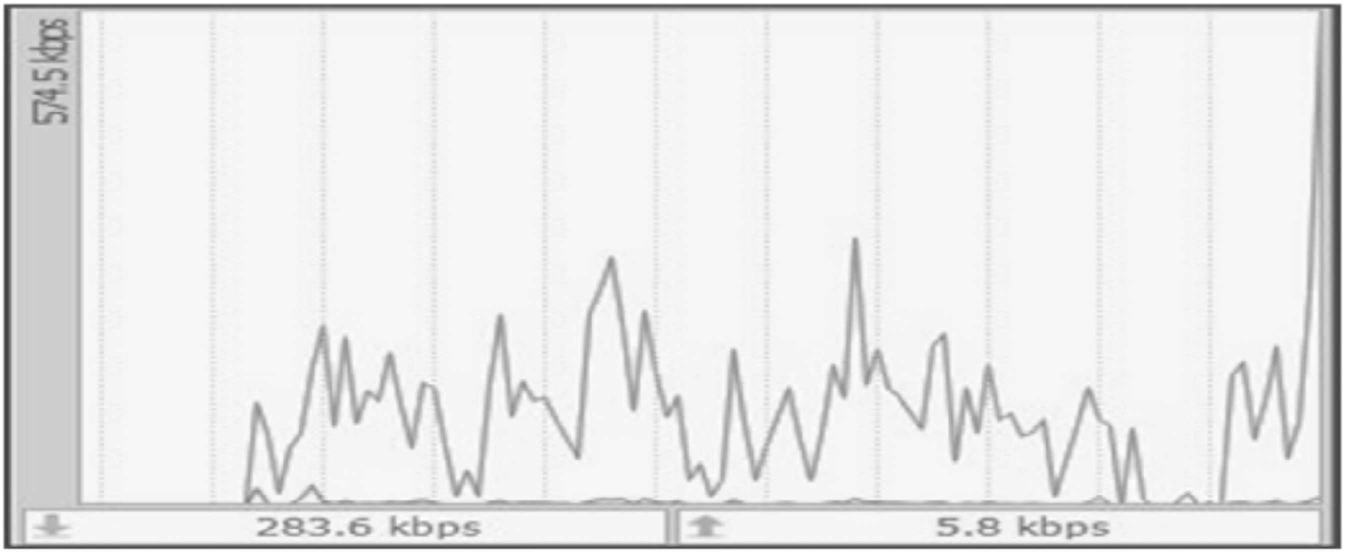


Figure 4: Bandwidth measured before the attack

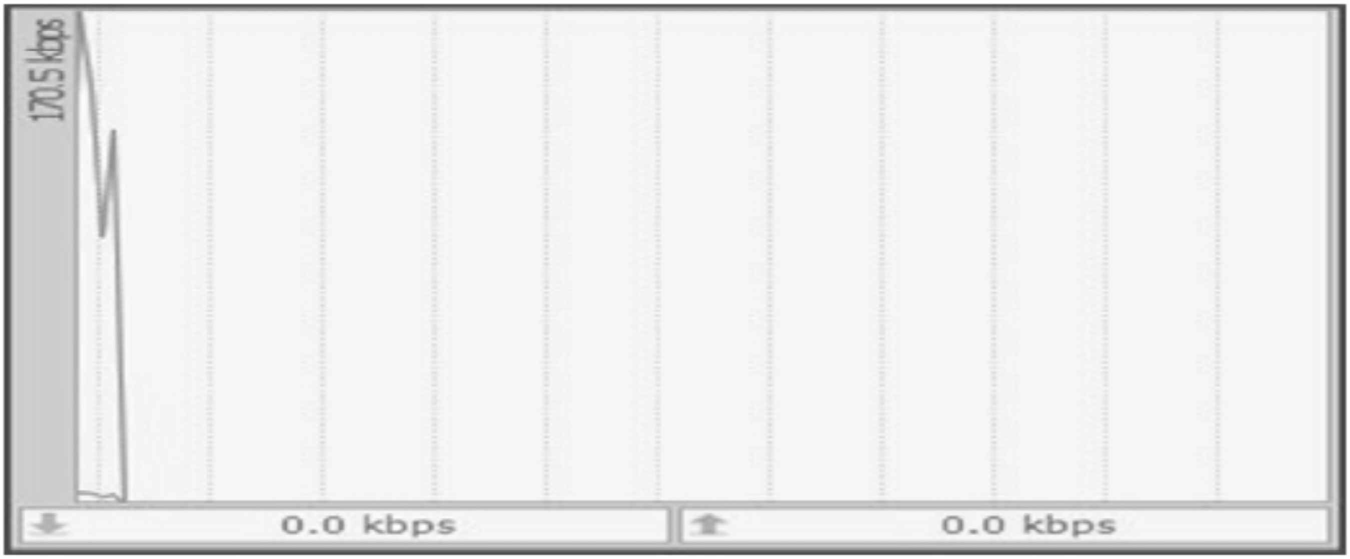


Figure 5: Bandwidth measured during the attack

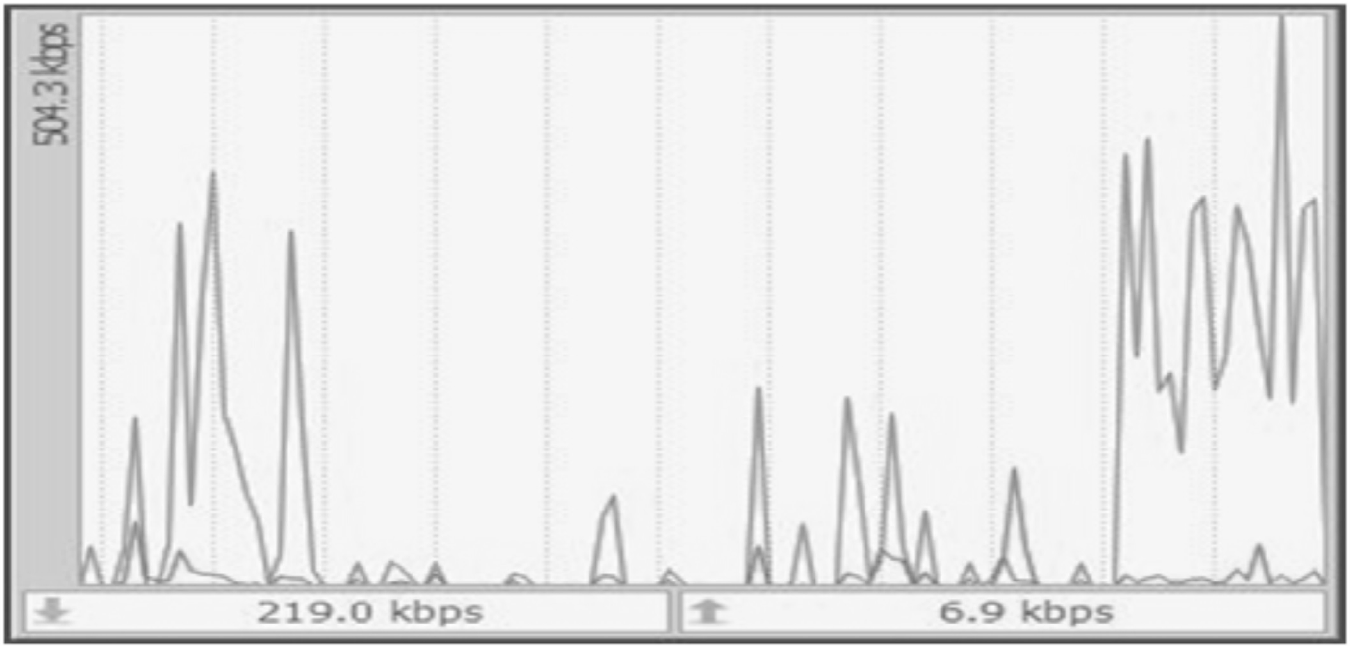


Figure 6: Bandwidth measured after the attack

to note down is that bandwidth goes down to zero during the attack phase. It signifies that DoS attack causes an effective impact to disrupt internet services of target networks. DU Meter tool is used to measure the bandwidth in all three stages of the attack. This tool is developed by 'Hagel Technologies' and it also includes some good functionalities like extensive reporting facility, flexible notifications and events system.

6. PROPOSED DEFENSE MECHANISMS

In case of ARP cache poisoning attack, the proposed defense mechanism is to overcome stateless nature of ARP protocol. This mechanism is proposed to all manufacturers of switches that they need to apply this mechanism in switching firmware itself. So that by default functioning of switch protects network hosts from ARP cache poisoning attack and will also trace the attacker in a wired LAN.

6.1. The Guarding Algorithm For ARP Cache Poisoning Attack

Step 1: Setup a trusted ARP cache table in switch. Regularly add/update hosts (IP-MAC address pairing) in it.

Step 2: For a new arp_request/arp_response packet update its entry in trusted ARP cache table. For an old packet send it for verification.

Step 3: In verification process, values in the packet are matched with values stored in trusted ARP cache table. Said source IP address and source MAC address in the packet are checked separately with IP and MAC addresses values.

Step 4: If source IP address value and source MAC address value is already on trusted cache table, then check MAC address corresponding to source IP address and check IP address corresponding to source MAC address.

Step 5: If source IP-MAC address pairing in arp_response packet matches with IP-MAC address pairing value stored in trusted ARP cache table, then switch updates its cache table and forwards it to its destination host in wired LAN.

Step 6: If source IP-MAC address pairing in arp_response packet doesn't match with IP-MAC address pairing value stored in trusted ARP cache, then arp_response packet is considered as spoofed packet and switch will not update its cache table.

Step 7: Once arp_response packet is considered as spoofed, find original IP address associated with source MAC address of arp_response packet and original MAC address associated with source IP address of arp_response packet via trusted ARP cache table entries or by sending ARP and RARP request to source IP and MAC address of spoofed arp_response packet respectively.

Step 8: Source IP address in spoofed arp_response packet is considered to be of victim and source MAC address is considered to be of attacker because switch forwards data packets by referring to MAC addresses of destination hosts. For example if any data packet is intended for victim IP address, switch first checks MAC address corresponding to victim's IP address. If attacker has successfully spoofed ARP cache table of switch then it must store an entry in which MAC address of attacker is found correspond to victim's IP address. So in this way all data packets that are originally intended for victim's IP address will redirect to attacker's machine.

Step 9: As source MAC address in spoofed arp_response packet is found to be of attacker system, set value of threshold count = 1, block update to cache table and notify system administrator of potential attempt to poison cache.

Step 10: When threshold count > = 1, trace the attacker. Note down the source MAC address value from spoofed arp_response packet. Find corresponding IP address to this MAC address. Blacklist this IP – MAC address paring and update threat list. Monitor each and every data packet that contains this IP – MAC address pairing. If suspicious behavior occurs again, simply block this pairing permanently.

Step 11: Calculate ARP packets uncertainty in order to confirm a destructive attack. Assume that for each request goes in or out at gateway maintains a counter for it.

Request IN: Counter gets incremented each time an ARP request received at gateway.

Request OUT: Counter gets incremented each time an ARP request goes out from gateway.

Reply IN: Counter gets incremented each time an ARP reply entering at gateway.

Reply OUT: Counter gets incremented at an ARP reply going out from gateway.

Calculate ARP Packets Uncertainty:

ARP Packets Uncertainty = Request OUT - Reply IN

Now there can be three different values:

1. ARP Packets Uncertainty > 0
2. ARP Packets Uncertainty = 0
3. ARP Packets Uncertainty < 0

If value of ARP Packets Uncertainty is greater than zero, means number of arp_request packets are greater than number of arp_response packets. In this scenario there is no chance of attack as for executing arp cache poisoning attack number of arp_response packets will always be greater than number of arp_request packets. If value of ARP Packets Uncertainty is equal to zero, it means there is a balance between both type of packets (arp_request and arp_reply) and chance of attack is negligible. If value of ARP Packets Uncertainty is less than zero, it means number of arp_response packets is greater than number of arp_request packets. This signifies that attack has taken place [19]. If attacker is smart enough and has sent bogus arp_request packets to balance the amount of arp_response packets then use the formula given below.

ARP Packets Uncertainty = ARP Packets Uncertainty – Request IN

If a value in result of this formula is more negative, means more number of bogus requests are sent by attacker.

Step 12: If negative values increases continuously, notify administrator about surety of arp cache poisoning attack and suddenly take the countermeasure given below:

```
While [1]
        do
                arping -f 172.18.18.129
                sleep 4
        done
```

Simply, Run this shell script (An FTP link is provided to systems for downloading this script) in order to effectively prevent systems from the attack. This script will run at background which means client system is sending regular arping requests to its gateway after a periodic interval and gateway replies its own MAC address in a unicast arp_response packet that keeps client ARP cache table updated. 172.18.18.129 is the IP address of gateway. Arping request is of broadcast nature that is send to each host in a network for keeping client arp cache table updated.

6.2. Defense Mechanism against DNS Poisoning Attack

This defense mechanism is proposed against intranet DNS spoofing attack. By using this mechanism, gateway tries to stop the attack and also traces the attacker's identity back. Intranet DNS spoofing attack is a technique in which attacker poisons gateway of wired LAN and redirects all DNS requests to his own machine.

Step 1: One primary and two secondary DNS servers that are connected to LAN gateway in this mechanism.

Step 2: When gateway receives a DNS request from client, it automatically forwards it to primary DNS server.

Step 3: At the same time, gateway also transmits two duplicate DNS requests of the same packet to both secondary DNS servers.

Step 4: As first DNS response comes from primary DNS server, gateway blocks it and waits for the replies from other two secondary servers.

Step 5: Gateway compares all DNS responses and propagates the one that is having the majority. For example if one server is responding with value x and other two servers are responding with values y. So in this case DNS response having value y will be propagated.

Step 6: As attacker is unaware about other two secondary servers and switch always forwards DNS requests to primary DNS server by default. In this attack, attacker machine will act as a primary server, the moment he successfully poisons the gateway of LAN. It means DNS response that is sent by attacker's machine is a spoofed response as it is only the attacker who will try to redirect the traffic to his own machine in order to perform DoS attack. So in this step, gateway notes the IP address value stored in DNS response packet that was sent by primary DNS server. It means this IP address is of attacker system as only his machine is acting as primary server in the LAN.

Step 7: As this IP address is of a system that is the part of wired LAN and is acting as a primary server, in this scenario gateway generates an attack alert to notify system administrator about the potential attempt and increase the attack counter by one.

Step 8: When value of attack counter is equal to or greater than a certain threshold value, IP address of the attacker machine will be blocked.

7. FUTURE WORK

DDoS attacks are the extended version of DoS attacks which involves number of compromised machines simultaneously attacking a single system or the entire network. Botnets are used to launch these attacks. Botnet is a client-server architecture in which there is one botnet server and many botnet clients. Botserver acts as a controller that controls hundreds, thousands or may be more than this number of botclients. Hackers use botnet clients to execute attacks on target networks and systems. Hackers find vulnerabilities in systems. exploit them and make it to act as botclient. When a system is exploited and becomes a botclient, then it can scan a new one for finding vulnerability, exploit it and make new botclient. Like this the chain of recruiting botclients goes on. Botnets play an essential role in attacking target systems and networks. Important uses of botnets are sniffing passwords, scanning for vulnerable systems, yield identity information about target (victim) and most important use of botnets is to execute DDoS attacks. So this research work can be extended by executing DDoS attacks on networks that makes impact of attack more effective and also makes it difficult to trace attacker's identity.

8. CONCLUSION

In this research, we proposed a feasible solution to the problem of ARP cache poisoning attack and DNS spoofing attack. Once the default functionality of switch changes as mentioned in the proposed defense mechanisms then it becomes difficult for an attacker to launch these attacks. The type of DoS attacks mentioned in this work is also working in wireless LAN. I have thoroughly tested it by attacking target systems that are connected through an access point. These proposed defense mechanisms can also be applied in case of wireless LAN.

Acknowledgment

This research was supported by my research mates. I would also like to thank the Head of Labs in Computer Science Department (HOL) who provided me sufficient resources during my experiments.

References

[1] S. Prowell, M. Borkin and Rob Kraus, "Seven Deadliest Network Attacks", Syngress, pp. 2-5, 2010.

[2] http://www.cert.org/tech_tips/denial_of_service.html

[3] h10032.www1.hp.com/ctg/Manual/c00389927.pdf

[4] T. Lammle, "CCNA: Cisco Certified Network Associate", Wiley Publishing, pp. 90-91, 2007.

[5] D. C. Plummer, "An Ethernet Address Resolution Protocol", RFC 826.

[6] G. N. Nayak and S. G. Samaddar, "Different flavors of Man-in-the-Middle attack, Consequences and feasible solutions", 978-1-4244-5540-9, 2010.

[7] Y. Liu, K. Dong, L. Dong and B. Li, "Research of the ARP Spoofing Principle and a Defensive Algorithm", ISBN: 978-960-6766-69-5, Communications & Information Technology 2008.

[8] X. Hou, Z. Jiang, X. Tian, "The detection and prevention for ARP Spoofing based on Snort", 978-1-4244-7237-6, International Conference on Computer Application and System Modeling, 2010.

[9] F. Guo, J. Chen and Tzi-cker Chiueh, "Spoof Detection for Preventing DoS Attacks against DNS Servers", 0-7695-2540-7, International Conference on Distributed Computing Systems, 2006.

[10] G. Kambourakis, T. Moschos, D. Geneiatakis and Stefanos Gritzalis, "A Fair Solution to DNS Amplification Attacks", 0-7695-2941-0, International Workshop on Digital Forensics and Incident Analysis, 2007.

[11] M. Janbeglou, M. Zamani, S. Ibrahim, "Redirecting Outgoing DNS Requests toward a Fake DNS Server in a LAN" 978 14244-6055-7, 2010.

[12] http://nmap.org/book/man.html

[13] http://seclists.org/nmap-hackers

[14] www.csc.villanova.edu/~nadi/csc8580/S11/nmap-tutorial.pdf

[15] http://www.gnulinuxclub.org/index.php?option=com_content&task= view&id=350&Itemid=31

[16] http://www.backtrack-linux.org/forums/

[17] http://indobacktrack.or.id/

[18] http://www.hackingarticles.in/

[19] Marco Antônio Carnut and João J. C. Gondim, "Arp Spoofing Detection on Switched Ethernet Networks: A Feasibility Study", Symposium Security in Informatics, 2003.