Indonesian Journal of Electrical Engineering and Computer Science
Vol. 12, No. 3, December 2018, pp. 1117~1125
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v12.i3.pp1117-1125

A Review on Various Sniffing Attacks and its Mitigation Techniques

B. Prabadevi, N. Jeyanthi
VIT University, Vellore, India

Article Info

Article history:

Received Jan 7, 2018
Revised Jul 9, 2018
Accepted Aug 21, 2018

Keywords:

DDoS
DoS
MITM
Packet sniffing
Ransomware
Sniffing attack

ABSTRACT

Security in the era of digital computing plays a vital role. Of various attacks in the field of computing, Distributed Denial of service (DDoS) attacks, Man-in-the-Middle Attack (MITM) and data theft have their major impact on the emerging applications. The sniffing attacks, one of the most prominent reasons for DDoS attacks, are the major security threats in the client-server computing. The content or packet sniffer snorts the most sensitive information from the network and alters or disturbs the legitimate functionality of the victim system. Therefore it is extremely important to have a greater knowledge on these vulnerabilities, their issues, and various mitigation techniques. This study analyses the existing sniffing attacks, variations of sniffing attacks and prevention or detection mechanisms. The reasons for most vital Ransomware are also discussed.

Corresponding Author:

B. Prabadevi,
VIT University,
Vellore, India.
Email: prabadevi.b@vit.ac.in

1. INTRODUCTION

The DDoS attack is an unbreakable security problem in the internet of things. DDoS is one of the variants of Denial of service (DoS) attacks. The major purpose of a DoS attack is to disrupt the victim from servicing its legitimate users. Dos attacks achieve its goal by flooding unserviceable traffic until the processing capacity of the victim's network is sloughed off. This in turn makes the victim computer to deny services to its legitimate users. It achieves its target either by consuming victim network's bandwidth or its connectivity [1-2].

The most promising variants of DoS attacks, the DDoS attacks had contributed about 14% of threats in the cloud environment [2]. In DDoS attack, the attacker causes the attack by a network of remote-controlled and widely isolated nodes which in turn works cooperatively by flooding large volume of traffic at the victim's network. The goal of the attack is not to exploit the data directly but to compromise the victim's resources from servicing its legitimate users.

The DDoS attack network consists of four roles [3] viz., attacker, handlers, agents and victim as depicted in Figure 1. The command for attack is directed from the attacker to handlers which contain information about the type of attack, victim's information and its duration. The handlers in turn propagate this to agents which will send the attack data packets to the victim. Various DDoS attack tools are available as free open source software for launching the DDoS attacks. With the help of these tools, the attacker can launch multiple attacks to multiple victims simultaneously by using various fake packets. Bandwidth depletion and resource depletion are the two categories on which the DDoS attacks are classified [1]. Though various detection and prevention mechanisms for DDoS attacks are available, it remains an emerging issue. The dynamic distributed computing technologies like Cloud provides its services through the internet, has wide applications and tremendously increasing users. Some of the applications of cloud includes the most

commonly used social networking sites like Facebook, Google plus and web stores like Google drive and Drop box. As cloud offers various flavors of services, it has become the best basement for most of the competing industries over the globe. The DDoS attacks have major impact over the technologies like cloud. It is one of the tempting targets for cyber-crime [4]. Of various DDoS attacks [1], the major focus is towards sniffer attacks which sniff the most sensitive information over the transmission channel as data is of major concern for any computing environment.

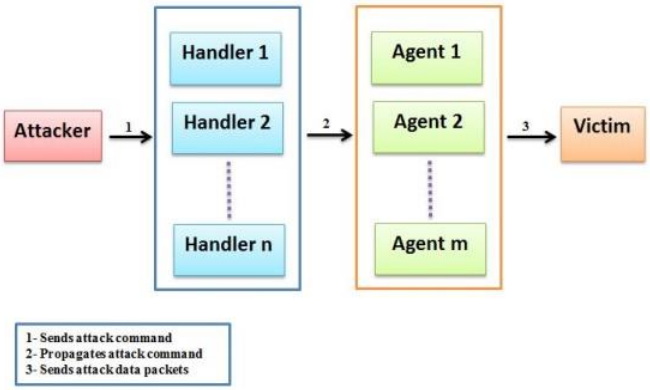

Figure 1. Attack network of DDoS

2. SNIFFER ATTACKS

Sniffing is the process of capturing-decoding-inspecting - interpreting the data from the packets transmitted over the transmission channel eg: TCP/IP network. The sniffer is an application that does the sniffing process. It is also called as network protocol analyzer. A sniffer has two modes of operation as follows:

a) Promiscuous mode- in this mode, the sniffer can steal the information from the traffic passing over the network i.e. from all devices connected to the host system
b) Non- Promiscuous mode- in this mode the sniffer can steal only the information going to and from its host system

The information stealth by the sniffer is very sensitive such as user credentials like IDs and passwords, account details, network specifics, credit card numbers, email texts, file transfers, DNS Queries, chat sessions, web pages being visited etc. Sniffing causes some risky type of attacks which are difficult to detect. Thus, sniffing can be categorized under a "passive" type of attack where the attackers can be mute or imperceptible over the network. The protocols in which either password or data are sent in a clear text and where both password and data are sent in a clear text are vulnerable to these sniffing attacks. For example Telnet, HTTP, SMTP, NNTP, POP, FTP and IMAP are some of the protocols vulnerable to sniffing.

Why and how the hackers/ attackers sniff?

The hacker performs the sniffing process either to get the sensitive information directly or to find the technical details about the network to cause further attacks. This can be achieved by using commercial or open source software tools. There are three ways to sniff a network

a) Wireless sniffer- specifically designed to capture data on wireless networks. Also called as wireless packet sniffer or wireless network sniffer.
b) External sniffer – This kind of sniffer has the capability of externally monitoring all inbound and outbound traffic from an external locality to a web server by gathering information about the server. In simple terms, sniffing from the third -party external location or sniffing data from the external interface using the sniffer tools.
c) Internal sniffer – These sniffers were designed to exploit the internal co-operate network. In this sniffer, the intruder compromises a machine on internal network and runs a sniffer to steal the data for compromising other computers connected over the network.

In this context, the term sniffing refers to "the information that can be stealth". The ways are as follows:

a) A LAN sniff: - A sniffing tool will be installed in the internal LAN. The sniffer/ attacker scans the IP addresses of all the hosts connected in the LAN. Through this, the information (like open ports,

active hosts, server portfolio, etc.) can be stealth. The port specific attacks can be launched with this information.

b) A protocol sniff: - The attacker sniffs information about the network protocols used. The attacker performs the following steps:
   a) A broad list of protocols is determined from the information sniffed.
   b) The above list is segregated based on the type of attacks that can be launched and distinctive type of sniffers will be developed to perform this.

For example if the list contains the UDP protocol, then a special UDP sniffer will be initialized to capture and decrypt the details of associated applications like DNS, Telnet and so.

c) An ARP sniff: - By sniffing through this resolution protocol, the attacker gets the set of IP addresses and accompanying MAC addresses too. This information will be sufficed to launch router attacks, spoofing attacks and ARP Poisoning attacks.
d) TCP session stealing: - The network interface acting as a sniffer will seizures entire traffic between source and destination. The attacker interested in the details like ports used, IP addresses, services offered, sequence numbers of TCP packets, control information and data, will launch this attack. With these details the attacker can even create a fabricated sessions between the communicating devices and can behave as man-in-the-middle either to disrupt services or pretends to capture sensitive data.
e) Application-level sniffing: - The application specific attacks will be launched through this sniffing by getting the list of active applications on the victim. The attacker sniffs the packets to get the information about the applications either to steal them or to cause further attacks based on the nature of the information. Eg: By sniffing user credentials sniffer can execute SQL Injection attacks, fingerprinting, etc.
f) Web password sniffing: - As web communications are done over HTTP, the attacker can steal the HTTP sessions and parse it for user credentials causing cookie poisoning attacks. Though SSL provides security mechanisms for HTTP, the emerging sniffing tools are more efficient and most of the internal websites are vulnerable.
g) The sniffing is termed as

PACKET SNIFFING- It is the process of monitoring every packets on the network. This is done by inserting a program that will monitor the data packets and forwards a copy of it to the attacker. Packet sniffing is always done in the promiscuous mode. By receiving first 125 keystrokes of the packets the attacker can learn the user credentials [5].

a) NETWORK SNIFFING: the network sniffing attacks [6] can be of different forms viz.
b) Client side sniffing: This is launched using scripting languages inferred by the user agent.
c) Server side sniffing: This is done from server side using communication protocols [6].
d) Browser sniffing: Uses the websites and web applications to launch the attacks. This kind of sniffer makes use of the information from browser caches and browser history. By misconstruing the scripting codes the attacker can sniff the private information and can bring NIC to promiscuous mode by installing sniffer tool [6].
e) Content sniffing: Also termed as MIME sniffing or Media type sniffing. To mimic changes in the Web applications the attacker changes the content type or file format. This harms both client and server side. The victim can avoid this by customizing the browser options for contents [7-8].
f) Password sniffing: The sniffer steals the most private and sensitive information from the packets such as user credentials especially passwords through which all the information can be stealth. One of the approaches to avoid this is using data triggers [6].

Figure 2 depicts the information an attacker can gain at each layer of OSI by sniffing a network. Abdul and Syed suggested the various attacks at Network layer of OSI model [9].

The sniffing can be performed by three methods [7] viz.

a) IP Based sniffing: The packet sniffing method sets the NIC to promiscuous mode and sniffs all the packets based on IP filter and works in non-switched type of networks.
b) MAC Based sniffing: This method similar to IP based sniffing with the exception that sniffs packets based on MAC address filters.
c) ARP Based sniffing: Unlike above two methods, it does not set NIC to non-promiscuous mode and works on a switched network. In this method the ARP request-reply message are used and poisons the ARP caches of communication entities and redirects traffic of attacker's interest based on the configuration done.

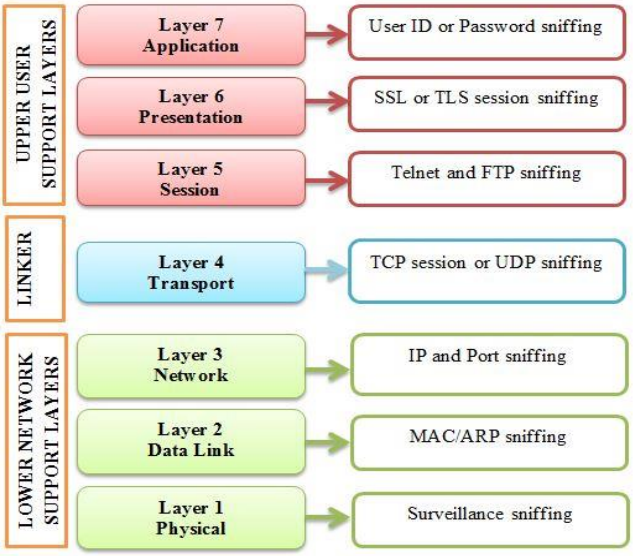

Figure 2. Possible ways of sniffing at various OSI layers

3. SNIFFING ATTACKS AND TOOLS

Sniffing process is executed either manually or by using software programs. These software programs are called as sniffing tools which performs sniffing and used for launching various attacks in the network.

3.1 Mac Attacks

These type of attacks is the variation of Denial of Service (DoS) by which the sniffer gains the information access. MAC flooding attack takes place by flooding the networking device 'switch' with numerous requests from different source MAC addresses. Now switch enters a 'failopen' mode which in turn acts as a hub broadcasting requests to all the ports in the network rather than to correct port. Since the switch has limited memory (i.e. Content Addressable memory to map the MAC addresses to physical address) the attacker floods the switch with voluminous MAC addresses utilizing its full capacity. Now the sniffer installed can capture the sensitive information. Figure 3 depicts the MAC flooding attack [10].

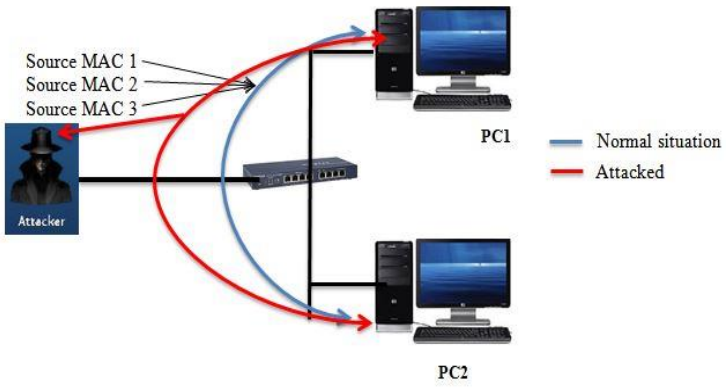

Figure 3. MAC flooding Attack

3.2.1 Preventing MAC flooding attacks

The 'switchport' port-security feature by CISCO which allows restricting the input from unauthorized hosts by examining the MAC addresses. The three types of secure MAC addresses include Static secure, dynamic secure and Sticky secure MAC addresses which are configured manually, dynamically and by either way respectively [10].

It also enforced three security violations to which the switch reacts when the no. of MAC addresses reaches the limit on the concerned port. In such scenarios, the victim either drops the packets (with anonymous MAC address) or exhibit shutdown status [10]. The restriction for installing the sniffer should be mandated. IPv6 with encrypted sessions can be used instead of IPv4. Port security feature confines these attacks and locks down by sending SNMP trap [11].

3.2 DHCP Attacks

DHCP is Dynamic Host Configuration Protocol, a network protocol used for dispensing the configuration details dynamically. The configuration information includes IP address, Routers, subnet Mask, DNS servers and so. It involves following steps [11]:

1) The client requests for the configuration details from the available servers through DHCP DISCOVER broadcast message.
2) The DHCP server dynamically assigns the IP address from the pool of IP address for assignment with the lease time. Also provides with additional information through DHCP OFFER unicast message optionally. DHCP REQUEST is the broadcast message used for getting optional details from the server by the client. DHCP ACK is the unicast response message from the server.

DHCP has three ways for allocating IP address [12] to clients viz., Automatic, Manual and Dynamic allocation which allocates permanent IP address, admin selected IP address and pre-specified IP addresses with lease time respectively. Because of this address allocation it has some of the issues where the DHCP server will be in the passive mode and has limited security features.

a) A Rogue DHCP server : Because of which the attacker can pretend to be DHCP server i.e. a rogue DHCP server and communicates with clients making the victim's network to shut down. The clients respond to the requests through default gateway which can be tracked by the attacker exploiting the entire domain via DNS information and other configuration parameters. This can be termed as Man-In-The-Middle (MITM) Attacks which is difficult to detect.
b) Malevolent DHCP client : By pretending as DHCP client the attacker can use Gobbler like tools to attack the DHCP server by DHCP flood [13]. To provide secured interactions Yun and Jia [13] proposed a SAKA Encryption algorithm for DHCP protocol.
c) DHCP Starvation Attack :

The "DHCP Starvation Attacks" happens by flooding the DHCP requests with spoofed MAC using attack tools. The attackers dissipate the entire address space by sending enough requests. Latter the attacker can set up a rogue DHCP server as mentioned above. Yaibuates et.al, proposed ICMP based detection method for anomalous DHCPREQUEST by attackers [14]. Many researchers had proposed various techniques for preventing DHCP attacks namely through Digital signatures and public key cryptography, by maintaining a predefined list of authenticated MAC addresses [15-16]. The most widely preferred mitigation techniques by CISCO for DHCP attacks is DHCP snooping - a network security feature, which filters the unauthorized DHCP messages using a binding database known as DHCP snooping binding table. The messages are filtered by means of switch ports through which DHCP communicates, since the binding table keeps track of all the ports both untrusted and trusted. Through trusted ports the devices can respond to the messages whereas the devices waiting to communicate through untrusted ports are deprived of service by shutting down the ports, so these untrusted ports holds only requests [12]. Port Security feature is other feature for avoiding this attack, by restricting the unwanted input to the ports by limiting the MAC addresses accessing the ports [11-12].

3.3 SYN Attacks

SYN is the synchronization bit used in TCP during three-way handshaking. The SYN flooding attack is responsible for mounting most of the prominent attacks in internet [17] and internet of things. One such attack is DoS. These attacks are launched by sending in numerous SYN requests which are spoofed and exceeds the victim's capacity to handle the requests as depicted in the Figure 4. The attacker gains this SYN information by spoofing the FIN/RST requests which are related to SYN by sequence numbers of packets as SYN-ACK pair holds full information about TCP connections [18]. The attacks are vulnerable during half-open state of victim server during which it receive requests from the clients. [18] detects the SYN attacks by SYN-ACK and CliACK pair's behaviour. Wang et al. [19] proposed a scheme called SYN-dog based on behaviour of SYN-ACK pair to sniff the SYN attack sources. Lihua Miao et al, [20] proposed a scheme for detecting the SYN attacks using Netflow information, through which most of the internet based SYN attacks are detected and presented a scenario for detecting the zombies.

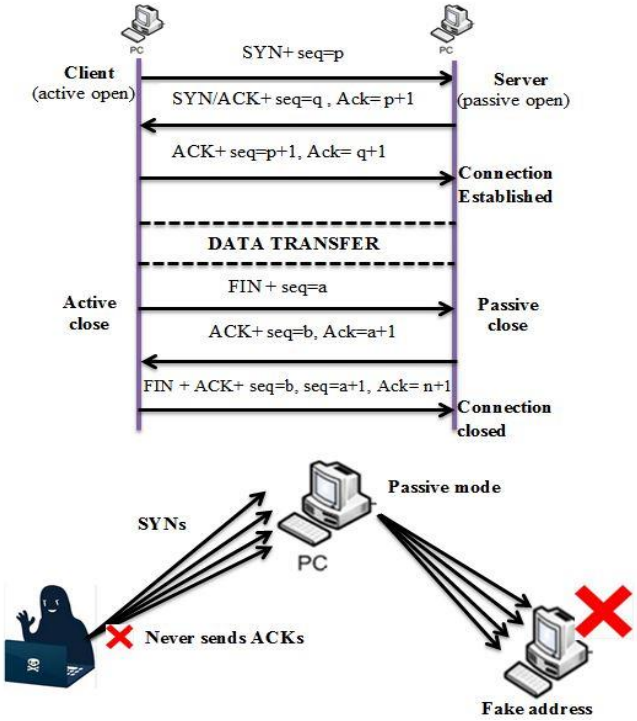

Figure 4. TCP SYN flood attack

3.4 DNS Poisoning Attacks

This is DNS cache poisoning attacks or DNS spoofing attacks. It is known that, DNS is widely used for resolving the domain name to IP address and vice versa. This type of attack takes place when the DNS server itself is compromised by which the attacker can alter or falsify the DNS table. So the DNS directs its clients to spurious IP address or domain. Or the attacker can gain information from the reverse lookup table which contains the list of IP addresses related to attacker's machine [17]. Sometimes the host uses the DNS servers provided by the host's organization or from ISP. In the former case to improve the response the frequently resolved queries are cached. The attacker takes this opportunity to exploit or poisoning the cache in turn diverting the users to illicit websites. In this scenario, the user gets responses from poisoned server. To mitigate these attacks some of the researchers proposed various techniques like Secure DNS – DNSSEC, DNSCurve Security proxy and TSIG which are used for protecting on the wire attacks [22]. Most of the organizations adopt various security features to mitigate these attacks. Yu and et al., used source port randomization and setting Time to Live field to protect the servers after DNS cache poisoning [23]. DNS poisoning may lead to phishing, some of which are detected by Kim and Hu [24] using network performance parameters with naïve Bayesian and K-nearest neighbouring algorithm. Tongguang et al., proposed a detection technique for protecting DNS servers from DDoS attacks [25]. Also Nhuong, suggested a security policy to prevent DDoS attack against future networks which guarantees users with advanced services [26].

3.5 ARP Poisoning Attacks

The Address Resolution Protocol operates on link layer of ISO i.e. works only on LAN for converting the given IP address into corresponding MAC address. This protocol is used by any network devices to communicate with each other [27]. Request and Response are two operations with ARP. The unsolicited structure of ARP makes it vulnerable to any attacker who has access to the LAN. The user requests the ARP with IP address to know the MAC address, the response is saved on to the cache for the future use. Because of lack of authentication in ARP, the attacker can send spoofed ARP responses causing ARP spoofing attack, as shown in Figure 5. When this is cached in the victim's system, the attacker himself will pretend to be the owner of IP address and send the fake ARP responses. Also the attacker gains access to the traffic directed by the victim. The attackers can even acts as a router directing the traffic to legitimate user by configuring his machine. This attack in turn can execute DoS attacks (dropping the packets destined for the legitimate user), by launching the MITM attack. Nugraha et al., proposed techniques for mitigating broadcast storms on Ethernet [28]. Some of the mitigation methods for the above said attacks are: Dynamic

ARP Inspection (DAI), the Network traffic inspection tools like PWatch, ARPWatch, and XARP [29] can be used to identify the spoofing attacks, ARP Central server (ACS) [30] which maintains table of IP-MAC relationship. Also ARP Cache poisoning attacks are detected using many of firmware's like OpenWrt, new Efficient and Secure (ES-ARP) protocols, modified ICMP [31] protocols. A comparative study on various mitigation techniques with factors like approaches adopted, detection type, protocols used was done [32]. From the study of various attacks, it's been flawless that no attacks are independent. E.g.: MITM remains vestige for most of the attacks. These attacks can be launched by open source tools [29] and few of them are listed in the Tab. 2. One can able to detect the network sniffer by using any ant-sniffing tools. Of the four prominent anti-sniffer tools Promi-Scan, PMD, L0pht AntiSniff, and SupCom antisniffer [33], SupCom detects most of the hosts involved in sniffing by conducted tests over different operating systems [33-34]. Mohd Anaur et al., used Key Exchange protocol to overcome relay and timing attacks [35].

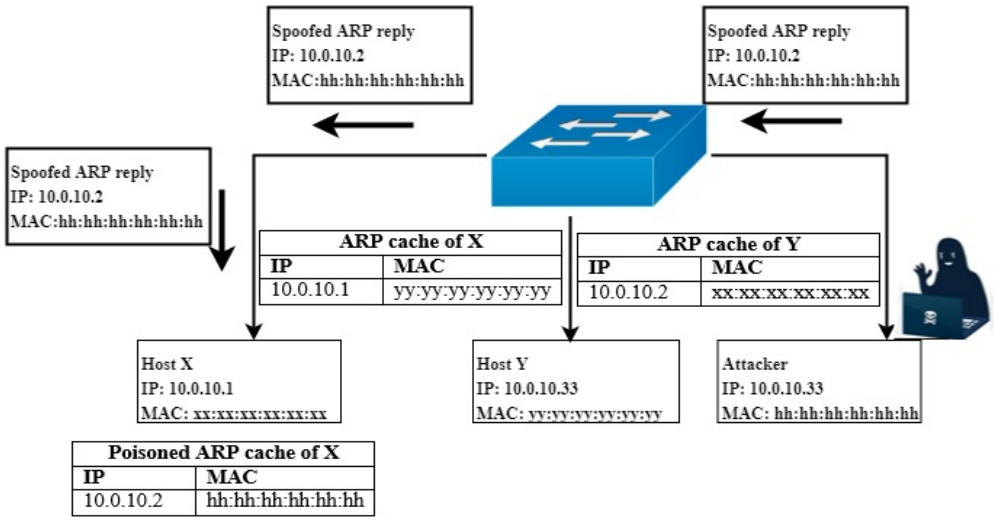

Figure 5. ARP Cache Poisoning Attack

The vulnerability statistics of various sniffing attacks take from the sources like Symantec's Intelligence Report [36], PhishMe [37] and MyCERT [38] are stated in the Table 3.

Table 2. List of Network Packet Analyzers/ Sniffers

TOOL	TYPE
ENDACE	Deep Packet Analyser
wireshark	Network protocol analyzer used for examining data in a static and dynamic network
Tcpdump	Network sniffer used for sorting the network problems
Dsniff	Passive sniffs the network for sensitive information and implements arpspoof, MITM attacks and dnsspoof
Etherpeek	Protocol analyser
Sniffit	Network analyser
etherflood	Designed for the white hat hacking purpose
ETHERCAP	Packet sniffer that launches MITM attacks
Insider	Network scanner
P0f	Examines packets to identify the OS
NetworkMiner	Passive sniffer and forensic analyser of networks
Ettercap	Sniffer that dissects active and passive protocols, identifies MITM attacks and also sniffs dynamic connections
KISMET	Passive sniffer sniffs UDP, ARP, DHCP, TCP for attacks
Cain and Abel	Sniffer used for cracking passwords that can launch ARP spoofing attack
NetStumbler	Active sniffer
Ntop	Determines the network status
Ngrep	Packet sniffer identifies UDP, TCP, ICMP packets
EtherApe	Network traffic monitor/ Packet sniffer
KisMAC	Network discovery tool identifies counter attacks to authenticated networks
Aircrack-ng SUITE	Provides various software for analysis, detection of network packets and creates encrypted packets used for injection

Table 3. Vulnerability statistics of various sniffing attacks

Types of Attacks	Volume	Source
DDoS	83%	Symantec's Global Intelligence Network, 2016
DDoS by IoT devices	1Tbps	Symantec's Global Intelligence Network Report on the victim French hosying company
Email Phishing	53%	Global Email spam rate
Email Spams Detected	~98K	MyCERT
Spam Containing Virus	1.2K	MyCERT

PhishMe states that of various Email phishing delivering other malwares, Email phishing delivering ransomware is more (i.e 93%) by first quarter end of 2016 [36]. ISTR 2017 [35] states that malwares created by email phishing was increasing progressively, though email phishing has been reduced from 1 in 220 mails (2015) to 1 in 131 mails (2016).

3. CONCLUSION

An extensive survey on sniffing attacks, various forms of sniffing, various ways to sniff and various sniffing methods is accomplished. Also the tools that used to launch sniffing attacks and various mitigation factors for the attacks are identified. From this survey it is vibrant that most of the attacks are contagious to some other attacks. Of various sniffing attacks phishing and DDoS were the most devasting attacks which had exploited lot of resources. The future study is to focus on implementing a mitigation technique to detect the variants of sniffing attacks.

REFERENCES

[1] Prabadevi B. and Jeyanthi N. "Distributed Denial of service Attacks and its effects on Cloud Environment- a Survey". *Proceedings of IEEE 2014 International Symposium on Networks*, Computers and Communications, 2014: 1-5.

[2] Douligeris, Christos, and Aikaterini Mitrokotsa. "DDoS attacks and defense mechanisms: classification and state-of-the-art" .*Science Direct Computer Networks,*2004; 44(5): 643-666.

[3] S. Dietrich, N. Long, and D. "Dittrich.Analyzing Distributed Denial of Service Tools: The Shaft Case", in *Proceedings of the 14th USENIX Conference on System Administration*, New Orleans, Louisiana, United States of America , 2000:329-340.

[4] John Harauz, Lori M. Kaufman, Bruce Potter. "Data security in the world of cloud computing". *IEEE Conference on Data Security in the World of Cloud Computing*,2009: 61-64.

[5] Information Security—Computer Attacks at Department of Defense Pose Increasing Risks: A Report to Congressional Requesters, 1996.

[6] Anubhi Kulshrestha and Sanjay Kumar Dubey. "A Literature Review on Sniffing Attacks in Computer Network". *International Journal of Advanced Engineering Research and Science*, 2014; 1(2): 32- 37.

[7] S. Pandey and A. S. Chauhan. "Secure Content Sniffing for Web Browser: A Survey". *International Journal of Advanced Research in Computer and Communication Engineering*, 2013; 2(9): 3595 – 3601.

[8] Syed Imran Ahmed Qadri and Kiran Pandey. "Tag Based Client Side Detection of Content Sniffing Attacks with File Encryption and File Splitter Technique". *International Journal of Advanced Computer Research*.2012; 2(5),No-3: 215-221.

[9] *Azeem Mohammed Abdul, Syed Umar*. "Attacks of Denial-of-Service on Networks Layer of OSI Model and Maintaining of Security", *Indonesian journal of Electrical Engineering and Computer Science*, 2017, 5(1):181-186.

[10] Kunal Gopal Thakur, Vishal Shirguppi, Justin Francis and Shazia Ali. *Packet sniffer, A seminar Report.* 2010.

[11] "Configuring Port-Based Traffic Control". In: *B. Catalyst 2960 and 2960-S Switch Software Configuration Guide*. 12.2(55)SE. City: CISCO. 2009: 1-18.

[12] Yusuf Bhaiji. "Layer 2 attacks & mitigation techniques", Cisco Expo, 2009.

[13] Yun Yang and Jia Mi. "Design of DHCP protocol based on access control and SAKA encryption algorithm". *IEEE 2nd International Conference on Computer Engineering and Technology (ICCET)*, 2010; 6:V6-264,V6-267:16-18.

[14] Yaibuates M. and Chaisricharoen R. "ICMP based Malicious Attack Identification Method for DHCP". 2014 *4th Joint International Conference on Information and Communication Technology, Electronic and Electrical Engineering (JICTEE)*, 2014:1-5.

[15] Dinu, D.D. and Togan M. "DHCP server authentication using digital certificates", 2014 *10th International Conference on Communications (COMM)*, 2014:1-6

[16] H. Altunbasak, S. Krasesser, H. Owen, J. Sokol, and J. Grimminger. "Addressing the weak link between layer 2 and layer 3 in the internet architecture". *Proceedings of the 29th Annual IEEE international conference on Local Computer Networks*, 2004: 417-418.

[17] Marco de Vivo, Gabriela O. de Vivo, Germinal Isern. "Internet security attacks at the basic levels", *ACM SIGOPS Operating Systems Review*, 1998; 32(2): 4 – 15.

[18] Changhua Sun,Chengchen Hu,Yachao Zhou,Xin Xiao and Bin Liu. "A More Accurate Scheme to Detect SYN Flood Attacks". *IEEE INFOCOM Workshops*, 2009: 1-2.
[19] Haining Wang, Danlu Zhang and Shin, K.G. "SYN-dog: sniffing SYN flooding sources". *22nd IEEE International Conference on Distributed Computing Systems*, 2002:421-428.
[20] Lihua Miao, Wei Ding and Jian Gong. "A real-time method for detecting internet-wide SYN flooding attacks". *IEEE International Workshop on Local and Metropolitan Area Networks (LANMAN)*, 2015 :1-6.
[21] Geetha K. and Sreenath N. "SYN flooding attack — Identification and analysis". *IEEE International Conference on Information Communication and Embedded Systems (ICICES)* 2014:1-7.
[22] Trostle J., Van Besien B. and Pujari A. "Protecting against DNS cache poisoning attacks", *6th IEEE Workshop on Secure Network Protocols (NPSec)*,2010:25-30.
[23] Yu Xi, Chen Xiaochen and Xu Fangqin. "Recovering and Protecting against DNS Cache Poisoning Attacks. *International Conference on Information Technology, Computer Engineering and Management Sciences (ICM)*, 2011: 120-123.
[24] Kim H. and Huh J.H. "Detecting DNS-poisoning-based phishing attacks from their network performance characteristics", *IEEE Electronics Letters*,2011; 47(11):656,658.
[25] Tongguang Ni, Xiaqing Gu and Hongyuan Wang. "Detecting DDoS Attacks Against DNS Servers Using Time Series Analysis", *Indonesian Journal of Electrical Engineering*, 2014; 12(1): 753-761.
[26] Dac-Nhuong Le. "DDoS attack Defense in Next Generation Networks using Private Security Policy", *International Journal of Information and Network Security*, 2014; 3(3):
[27] Zdrnja, B. "Malicious JavaScript Insertion through ARP Poisoning Attacks, Security & Privacy", *IEEE* ,2009; 7(3):72-74.
[28] Nugraha, Beny, Bayu Fitrianto, and Fahraini Bacharuddin. "Mitigating Broadcast Storm on Metro Ethernet Network Using PVST+". *TELKOMNIKA (Telecommunication Computing Electronics and Control)* 14, no. 4 (2016): 1559-1564.
[29] www.securityfocus.com/ tools.
[30] Kumar S and Tapaswi S. "A centralized detection and prevention technique against ARP poisoning". 2012 *IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, 2012:259-264.
[31] Arote P. and Arya K.V. "Detection and Prevention against ARP Poisoning Attack Using Modified ICMP and Voting", 2015 *IEEE International Conference on Computational Intelligence and Networks (CINE)*, 2015:136-141.
[32] Tripathi, N. and Mehtre, B.M. "Ansalysis of various ARP poisoning mitigation techniques: A comparison", *2014 IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*,2014:125-132.
[33] Trabelsi Zouheir, and Hamza Rahmani. "An Anti-Sniffer Based on ARP Cache Poisoning Attack", *Information Systems Security, 2005;* 13(6):.23-36.
[34] http://sectools.org/tag/sniffers/
[35] *Mohd Anuar Mat Isa, Habibah Hashim, Syed Farid Syed Adnan, Nur Nabila Mohamed, Yasin Fitri Alias.* "Side-Channel Security on Key Exchange Protocol: Timing and Relay Attacks", *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, 2018, 11(2):688-695.
[36] Symantec's 2017 Internet Threat Report: https://www.symantec.com/security-center/threat-report?inid=globalnav_scflyout_istr, ISTR, 2017 Vol.22.
[37] PhishMe Q1 2016 M8, alware Review: https://phishme.com/project/phishme-q1-2016-malware-review/, 2016.
[38] MyCERT Incident Statistics Available at https://www.mycert.org.my/statistics/2017.php , 2017.