# Survey on Network Security Attacks

Ajay Yadav[1], Hari Krishnan[2],Raju Prasad[3], Deepti Dave[4]
[1,2,3] *U.G. Student, SOE, ADYPU, Lohegaon, Pune, Maharashtra, India*
[4]*Senior Faculty-IT, iNurture, Bangalore, India*

***Abstract -*** Network security consists of the policies and practices adopted to prevent and track unauthorized access, misuse, refinement, or the denial of a network and network-accessible resources. Network security demands the consent of access to knowledge in a very network that is managed by the network administrator. Users usually opt for square measure allotted associate degree ID and a word or a different verified data that enables them to access data and program at intervals for their authority. Network security comprises a range of laptop networks: - both public and personal, that square measure employed in everyday jobs; conducting transactions and communications among businesses, government agencies, and people. Networks are often non-public, like in a corporation, which could be hospitable to public access. Network security is concerned in several forms of establishments such as in organizations and enterprises. It secures the network, yet protective and overseeing operations to get done. One of the most common and easy method of protecting a network resource is by assigning a singular name and a corresponding word.

***Keywords*** **-** Security, Attacks, Prevention, Vulnerability, Detection

## I. INTRODUCTION

Network security starts with authentication, usually with a username and a countersign. One-factor authentication need only one detail authentication, i.e., the users name and the password. While, the two-factor authentication needs something the user has (e.g., a security token or 'dongle', an ATM card, or a mobile phone). In addition to the other two-factors, the third one: the three-factor authentication requires something the user is (e.g. a fingerprint or retinal scan).

A firewall imposes access policies once it is found genuine on the services that are allowed to be accessed by the network users. Though it effectively blocks unauthorized access, this component may fail to examine potentially harmful contents such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system( IPS) helps to detect and inhibit the action of such malwares. An anomaly-based invasion detection system may analyze the networks like Wireshark traffic and will be logged for audit functions and a high-level analysis will be done later. Modern systems combined with autonomous machine learning with full network traffic analysis can detect active network attackers from malicious insiders or targeted external attackers that have compromised a user machine or account.

Communication between 2 hosts employing a network could also be encrypted to take care of privacy Honeypots, essentially decoy network-accessible resources, may be deployed in a network as surveillance and early-warning tools, as the honeypots aren't ordinarily accessed for legitimate functions. Techniques employed by the attackers that plan to compromise these decoy resources square measure studied throughout and once an attack to stay a watch on new exploitation techniques. Such analysis could also be wont to any tighten security of the particular network being protected by the king protea. A king protea can even direct AN attacker's attention faraway from legitimate servers. A king protea encourages attackers to pay their time and energy on the decoy server whereas distracting their attention from the information on the important server. Similar to a king protea, a honeynet is a network set up with intentional vulnerabilities. Its purpose is additionally to ask attacks so the attacker's strategies will be studied which info will be wont to increase network security. A honeynet typically contains one or more honeypots.

## II. STUDY OF NETWORK SECURITY ATTACKS, DETECTION & PREVENTIONS

**A. Denial of Service (DoS)**– A DoS attack renders a network, host, or different piece of infrastructure unusable by legitimate users. Most Internet DoS attacks fall into one of three categories -

**i). Vulnerability attack** -This involves sending a few well-crafted messages to a vulnerable application or operating system running on a targeted host. If the proper sequence of packets is distributed to a vulnerable application or software system, the service can stop or, worse, the host can crash.

**ii). Bandwidth flooding** - The attacker sends a deluge of packets to the targeted host—so many packets that the target's access link becomes clogged, preventing legitimate packets from reaching the server.

**iii). Connection flooding** -The attacker establishes a large number of half-open or fully open TCP connections at the target host. The host will become therefore over-involved with these phony connections that it stops acceptive legitimate connections.

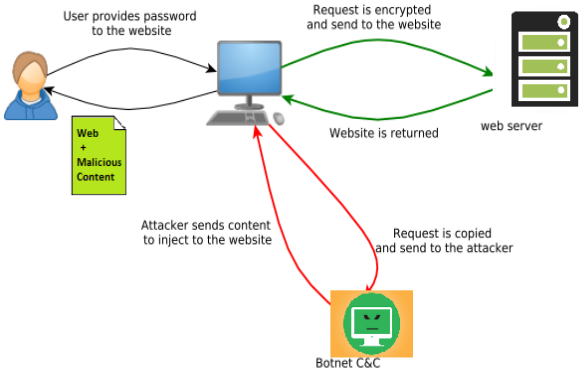


Figure 1

Distributed denial-of-service is one quite the foremost highlighted and most significant attacks of today's cyberworld. With straightforward however extraordinarily powerful attack mechanisms, it introduces an immense threat to current Internet community. In this article, we present a comprehensive survey of distributed denial-of-service attack, prevention, and mitigation techniques. We provide a scientific analysis of this kind of attacks as well as motivations and evolution, analysis of various attacks thus far, protection techniques and mitigation techniques, and attainable limitations and challenges of existing research. Finally, some important research directions are outlined which require more attentions in near future to ensure successful defense against distributed denial-of-service attacks. [1]

**B. Distributed DoS (DDoS)** – DDoS is a type of DOS attack where multiple compromised systems, are used to target a single system causing a Denial of Service (DoS) attack. DDoS attacks investing botnets with thousands of comprised hosts area unit a typical prevalence nowadays. DDos attacks are much harder to detect and defend against than a DoS attack from a single host.

Distributed Denial of Service (DDoS) attack may be a vital threat to the Web-based and Client-Server applications and resource allocation to defense the DDoS attack has become a significant challenge. To overcome these challenges, in this paper we proposed a HTTP GET Flooding Detection and Confidence-Based filtering method for DDoS Attack Defense in Web application. HTTP Get flooding attack is the most critical and frequently attempted attack.

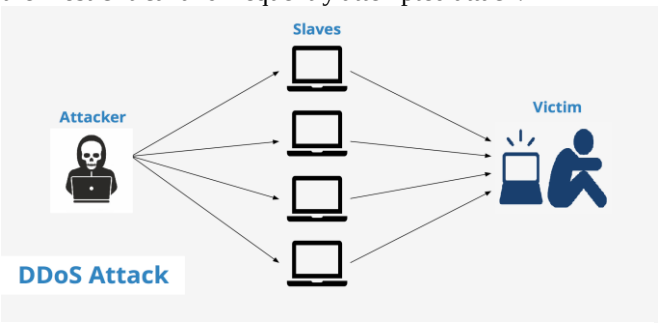


Figure 2

To overcome this attack AN early stage HTTP, GET Flooding Detection technique is connected. The dynamic resource allocation is applied to mechanically coordinate the offered resources (CPU, Memory, I/O and Bandwidth) of a server to relieve DDoS attacks on individual clients. After CBF (Confidence-Based Filtering) score is calculated for every packet, resource analysis is completed to work out whether or not to discard the packet/request or not.[2]

**C. Packet sniffer** – A passive receiver that records a duplicate of each packet that flies by is named a packet soul. By putting a passive receiver within the locality of the wireless transmitter, that receiver will acquire a duplicate of each packet that's transmitted! These packets will contain all types of sensitive info, including passwords, social security numbers, trade secrets, and private personal messages. some of the most effective defenses against packet sniffing involve cryptography.

Packet sniffing may be a technique of sound every packet because it flows across the network. It is a way during which a user sniffs information happiness to different users of the network. It is effective on each switched network and non-switched network. Packet sniffers will operate as Associate in Nursing body tool or for malicious functions. It depends on the user's intent. This paper discusses how sniffing can be done in case of hub and switched network, various packet sniffing methods, different methods that Anti Sniff uses to detect these sniffing programs are also discussed.[3]

Packet sniffers are often operated in each switched and non-switched atmosphere. be understand by everyone. In this technology all hosts square measure connected to a hub. There square measure an outsized variety of business and non-commercial tools square measure offered that produces doable eavesdropping of network traffic. Now a problem comes that how this network traffic can be eavesdropping; this problem can be solved by setting network card into a special "promiscuous mode".[4]

**D. IP Spoofing** – The ability to inject packets into the web with a false supply address is thought as information processing spoofing, and is however one in all many ways within which one user will masquerade as another user. To solve this problem, we will need end-point authentication, that is, a mechanism that will allow us to determine with certainty if a message originates from where we think it does. IP spoofing hides the information processing address by making information processing packets that contain bastard information processing addresses in a trial to impersonate alternative connections and conceal your identity once you send info. It is a typical methodology that's employed by spammers and scammers to mislead others on the origin of the data they send.

IP Spoofing Detection for preventing DDoS Attacks in Cloud Computing provides techniques for detection and hindrance that are OS primarily based. This is simpler and authentic means of detection and hindrance. It includes "OS

fingerprinting" technique to sight and stop the DDoS attacks in Cloud Computing. It monitors the incoming packet to determine the OS the source is running on.[5]


Figure 3

IP spoofing is employed to commit criminal activity on-line and to breach network security. Hackers use information processing spoofing so that they don't get caught spamming and to move denial of service attacks. These are attacks that involve huge amounts of knowledge being sent to computers over a network in a trial to crash the complete network. The hacker doesn't get caught as a result of the origin of the messages cannot be determined because of the bastard information processing address. IP spoofing is additionally employed by hackers to breach network security measures by employing a bastard information processing address that mirrors one in all the addresses on the network. This eliminates the need for the hacker to provide a user name and password to log onto the network.[6]

**E. Man-in-the-Middle Attack** – As the name indicates, a man-in-the-middle attack happens once somebody between you and therefore the person with whom your act is actively watching, capturing, and dominant your communication transparently. For example, the aggressor will re-route a knowledge exchange. When computers area unit act at low levels of the network layer, the computers won't be ready to verify with whom they're exchanging information.

The Man-In-The-Middle (MITM) attack is one in all the foremost well-known attacks in pc security, representing one in all the most important issues for security professionals.[7]

MITM attack works in such a way that it makes the users troublesome to know if they're connected to the particular secure affiliation or to the same non-secure affiliation. When the user tries to establish a connection with the network, the user first sends packets which include the information about the user device to the necessary network.

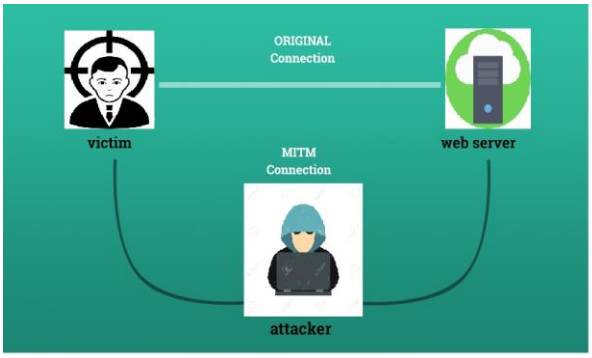


Figure 4

The network then creates a digital certificate which incorporates the encrypted affiliation key and therefore the user device address. Since the certificate that's being passed throughout the affiliation format is insecure, the aggressor will simply gain access to the digital certificate and modify the data within the certificate leaving the approval of the certificate to the user. Many users don't have enough data to visualize concerning the whereabouts of the solid and duplicate certificates and therefore the attacks akin to them, therefore they settle for the certificates and allow connection to the non-secure network making way for the attackers to implement the attack.

**F. SQL Injection Attack** - SQL Injection Attack: SQL Injection Attack may be a code injection technique accustomed attack websites and login with administrator privileges. The poorly designed websites area unit the victim of this attack. The attacker can inject SQL commands and gain access to obtain the data from the database Firewalls or IDS cannot protect the data against the SQL injection attack. Countermeasure: Patches for OS, software, and antivirus are to be regularly updated. A proper validation of computer file will mitigate SQL Injection attack. Access Control permission on the database must be strictly defined.[9]

The hash functions are automatically generated using Hash Algorithms. Now, once the consumer enters the username and secret then hash perform is generated and is transferred to the server facet for verification. Everything which takes place over here is in encrypted form. If the username and password is same as stored in the database which is matched with its hash functions. Hence, there is negligible chance for intrusion into the database.[10]


Figure 5

## III. EAVESDROPPING ATTACKS

Eavesdropping attacks are easier and can be passive, that is, a piece of software can simply be sitting somewhere in the network path and capturing all the relevant network traffic for later analysis. The assaulter doesn't ought to have any current association to the software package in the slightest degree. An attacker can insert the software onto a compromised device by direct insertion or by a virus or other malware, and then come back some time later to retrieve any knowledge that's found or trigger the software package to send the information at some determined time. Modification attacks have the same need as eavesdropping attacks to get to the right point in the network, but they also have a timing requirement. The attacks are only useful if one can modify the communications stream while the communication is taking place. The attacker also has to insert software in the network path in a true man-in-the-middle (MiTM) attack where one is able to not just observe packets, but actually receive the packets, modify them, and send them on.

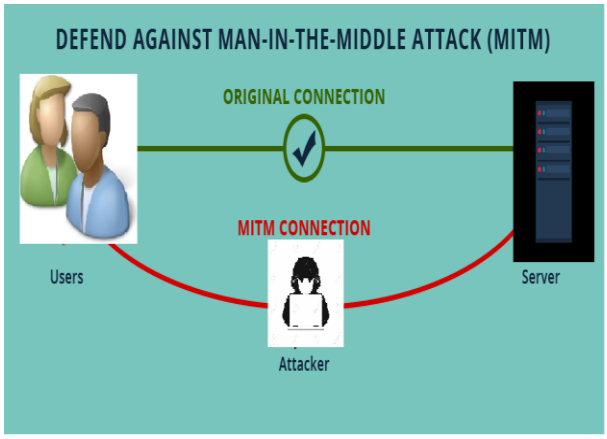


Figure 6

Modification attacks could be performed by code that is inserted and left behind, particularly if the target media is text-based such as IM, but other tools do require the active participation of the attacker to get the right timing.

**Phishing** – Phishing has become a major threat to net users. Phishing attacks usually use legitimate-looking however pretend emails and websites to deceive users into revealing personal or money info to the offender. Users may be tricked into downloading and putting in hostile software package, that searches the user's laptop or monitors on-line activities to steal personal info. The offender creates web site an internet site a web site} the same as the first website, like banking web site. DNS cache poisoning permits the user to navigate to the attacker's pretend web site mechanically.

Phishing attacks are on the rise. According to the Anti Phishing Working Group (APWG), 2870 phishing sites appeared in March 2005, a 28% increase per month since July 2004. [ 11] A survey sponsored by trust found 70% of the respondents had visited a phishing site; over 15-mitted to having provided personal data to a phishing site; and US consumers have lost an estimated $500 million as a result of these attacks.

Figure 7

Many proposals for stopping phishing attacks place confidence in a security toolbar that displays warnings or security-related info within the net browser's interface

Spoof Stick [12] displays the website's real domain name, in order to expose phishing sites that obscure their domain name. An attack may use a legitimate wanting name as a sub-domain

Net craft Toolbar [13] displays information about the site, including the domain's registration date, hosting country, and popularity among other toolbar users. This info is assumed to be useful in sleuthing phishing sites as a result of most phishing sites area unit short lived compared to the legitimate sites they imitate, and an outsized range of phishing sites spoof US-based firms however area unit registered in alternative countries.

• Trust bar makes secure web connections more visible by displaying the logos of the website and its certificate authority. This is helpful against phishing as a result of several legitimate websites use SSL to code the user's sensitive knowledge transmission, but most phishing sites do not. Attackers avoid SSL as a result of getting associate SSL certificate from a well-known CA, such as VeriSign, requires site identity information that can be traced, and because using a CA that is not known to the browser will trigger a warning and thus might raise the user's suspicion.

• eBay's Account Guard shows a green icon to indicate that the current site belongs to eBay or PayPal, a red icon to indicate a known phishing site found on a blacklist maintained by eBay, and a gray icon for all other sites.

• Spoof Guard calculates a spoof score for the current web page using a set of heuristics derived from previous phishing attacks. It then interprets this score into a traffic light: red for spoof scores higher than a threshold, indicating the page is probably hostile; yellow for scores in the middle; and green for low scores, indicating the page is perhaps safe.

**DNS spoofing** – DNS (Domain Name System, DNS) is a hierarchical and distributed database system which mapping the domain name to the IP address. It is the Internet's basic service, which security plays a vital role in the entire

Internet. While there do many security, risks exist in the DNS system itself especially in 2009, a variety of DDoS (Distributed Denial of Service) events happened frequently around the world. In May 19th, hackers' attack led to the paralysis of a lot of Domain Name Resolution Servers, and many provinces' network interrupted, like Jiangsu, Anhui, Guangxi, and Hainan. In July 28, a new vulnerability appeared through BIND. This raises concerns of DNS service and the threat of security. This paper states the working principle of DNS, analyses the main security problems faced by the DNS system, and raises the corresponding solutions and defense programs from the aspects of deploying DNS severs, preventing DDoS attack and preventing DNS spoofing.

The resolution process of Domain Name System is described as follows:

1) Users appeal to the local DNS server to inquire DNS and request for resolving the IP address
2) There are no corresponding records in the local DNS server, and then it turned to the root DNS server for help.
3) Root DNS server returns to the DNS server address of com domain.
4) The local DNS server appeals to the DNS server of com domain for resolution requests of domain name.
5) The DNS server of com domain returns to the DNS server address of test.com domain.
6) The local DNS server continues to make requires to the DNS server of test.com domain for domain name resolution.
7) The DNS server of test.com domain returns the IP address of www.test.com to the local DNS server.
8) The local DNS server returns the results of the domain name resolution to the Client, at the same time it also updates its cache records.

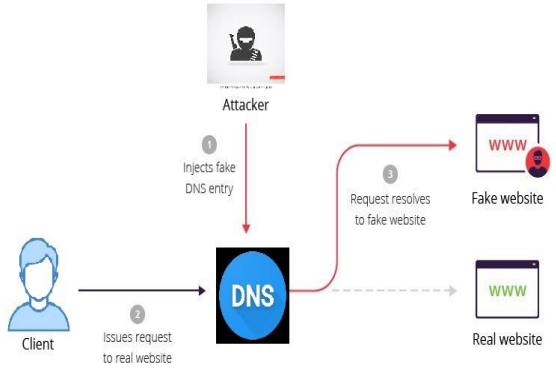


Figure 9

After receiving the reply packet, the client program will inquire whether the serial number and port number match the inquiries made by their own, if they match, the client program will accept the results, if not, it will discard the reply packet. This is the whole process of DNS service.

## IV. REFERENCES

[1]. International Journal of Distributed Sensor Networks 2017, Vol. 13(12) The Author(s) 2017 DOI: 10.1177/1550147717741463 journals.sagepub.com/home/dsn
[2]. Advances in Computational Sciences and Technology ISSN 0973-6107 Volume 10, Number 8 (2017) pp. 2257-2272 © Research India Publications http://www.ripublication.com
[3]. 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6–7 March 2009
[4]. [4] Tom King, "Packet sniffing in a switched environment", SANS Institute, GESC practical V1.4, option 1, Aug 4th 2002, updated June/July 2006.
[5]. International Journal of Scientific and Research Publications, Volume 7, Issue 11, November 2017 24 ISSN 2250-3153
[6]. IEEE STUDENT BRANCH UIET IEEE Student Conference on Cognizance of Applied Engineering & Research UIET, PANJAB UNIVERSITY, CHANDIGARH Paper ID: UE 0158201
[7]. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO. 3, THIRD QUARTER 2016 2027 A Survey of Man in The Middle Attacks
[8]. IJSTE - International Journal of Science Technology & Engineering | Volume 2 | Issue 09 | March 2016 ISSN (online): 2349-784X All rights reserved by www.ijste.org 277 A Survey on Man in the Middle Attack
[9]. William G.J. Halfond, Jeremy Viegas, and Alessandro Orso, "A Classification of SQL Injection Attacks and Countermeasures", ACM TISSEC, Vol. 13, Feb. 2010.
[10]. ] S. P. Singh and M. UpendraNathTripathi, "Detection and prevention of sql injection attack using hashing technique," International Journal of Modern Communication Technologies & Research, vol. 2, 2014.
[11]. Anti-Phishing Working Group. Phishing Activity Trends Report, March 2005. http://antiphishing.org/ APWG_Phishing_Activity_Report_March_2005.pdf
[12]. Chou, N., Ledesma, R., Teraguchi, Y., Mitchell, J.C. Client Side Defense Against Web-Based Identity Theft. 11th Annual Network and Distributed System Security Symposiu
[13]. Herzberg, A., Gbara, A. Trust Bar: Protecting (even Naïve) Web Users from Spoofing and Phishing Attacks. 2004. http://www.cs.biu.ac.il/~herzbea/Papers/ ecommerce/spoofing.html.
[14]. Netcraft Toolbar. 2004