INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Network Security - Catastrophic Risks And Countermeasures

Gaurav Kumar Thakur
Dronacharya College of Engineering, Greater Noida, India
Harshit Agrawal
Dronacharya College of, Engineering, Greater Noida, India
Jainender Thakur
Dronacharya College of Engineering, Greater Noida, India
Kishlay Kaushal
Dronacharya College of Engineering, Greater Noida, India

Abstract:

Security is crucial to networks and applications. So with the huge explosion of public internet, ecommerce, private computers it has become necessary to secure them properly otherwise they are increasingly vulnerable to malicious attack and various threats. Network structure itself allows many security threats to occur because of many loopholes and improper maintenance. This paper discusses various network threats and proposes their preventive methods which helps in protecting individuals, organisations from intruders and ensures that the information or data travelling on network is safe and protected.

General Terms: *Network Security, Spoofing, Spamming, Phishing, Flooding, Trojans, Viruses, Malwares, Honeypots*

Key words: *Packet sniffing, Address Resolution Protocol (ARP), Media Access Control address (MAC) attacks, MAC flooding, Denial of Service (DOS) attacks, Intrusion Detection System (IDS) Intrusion prevention system (IPS)*

1.Introduction

Network security is an essential term that describes the policies and procedures involves the authorization of access to data in a network, implemented by a network administrator to avoid and keep track of unauthorized exploitation, modification, or denial of the network and network resources.

Network security is a precarious requisite. In emerging networks, there is a significant dearth of security methods that can be easily alleviated. When considering network security, it must be emphasized that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, and decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message. When developing a secure network, the subsequent critical key points need to be considered.

- Access Authorized users are delivered the means to communicate to and from a particular network.
- Authentication Certify the users of the network are who they pretend to be.
- Confidentiality Information within the network remains isolated.
- Integrity Ensure the message has not been reformed in transit.
- Non-repudiation Ensure the users does not controvert that they used the network.

Security administration for networks is diverse for all kinds of circumstances. A home or small scale organization may only involve straightforward security, while outsized industries might require extraordinary-upkeep and cutting-edge software and hardware to thwart wicked attacks from spamming and hacking. There is an outsized volume of individual, marketable, martial, and government information on networks. Network security is fetching of countless prominence because of intellectual property that can be easily attained through the internet. The vast subject of network security is analyzed by exploring the following

- Importance of network security
- Security issues related to a network
- Threats and attacks
- Preventions

Established on research, imminent in network security is forecasted. New drifts that are emergent will correspondingly be considered to comprehend where network security is heading.

2.Related Work

Pallavi Asrodia et.al [1] "A sniffer package permits a user to lookout all network traffic over any network interfaces linked to the host machine. This technique works by keeping the network card into monitor mode. A sniffer package can watch various protocols like TCP, IP, UDP, ICMP, ARP and RARP. A sniffer keeps lookout on port specific traffic for checking http (80), ftp, telnet, etc. A sniffer can interrupt packets from a victim host (hosts) on the LAN proposed for alternative host on the LAN by falsifying ARP replies". Sumit Dhar [2] "Information Security Management Team Reliance Infocomm a Sniffer is a program of a device that eavesdrops on the network traffic by grabbing information travelling over a network, Internet Security ECOM 5347 Lab 1 Sniffing practical implementation of sniffing. http://ettercap.sourceforge.net/" [3] "freely available software which uses different plugins and different types of scripts, to attack on a network and this tool can be easily misused". The APWG Report on Phishing Activity Trends 2nd Quarter 2012 Unifying the Global Response to cybercrime April-June 2012 published September 2012[4] The APWG Phishing Activity Trends Report analyze Phishing attacks reported to the APWG by its members and partners. It also measures the evolution, proliferation, and propagation of crime ware by doing research in member companies. [7] Survey on Malware Detection Methods, Vinod P., V.Laxmi, M.S.Gaur, Malaviya NIT, Jaipur.

3.Packet Sniffing

Packet sniffer is a software package running in network devices that impassively collects all data link layer frames short-lived over the device's network adapter, also known as Ethernet Sniffer or Protocol Analyser.

A sniffer package permits a user to lookout all network traffic over any network interfaces linked to the host machine. A sniffer package can watch various protocols like TCP, IP, UDP, ICMP, ARP and RARP. A sniffer keeps lookout on port specific traffic for checking http (80), ftp, telnet, etc. A sniffer can interrupt packets from a victim host (hosts) on the LAN proposed for alternative host on the LAN by falsifying ARP replies.

This is tremendously effective way of sniffing traffic on a switch. Determine the local network device gateway of an unknown network via passive sniffing. Flood the local network with random MAC addresses (switches to fail open in repeating mode to facilitating sniffing). [1]

Develop as a simple password sniffer by slightly parsing each application protocol, and saving the "interesting" pieces. Output all demanded URLs sniffed from HTTP traffic in CLF (Common Log Format) used by web servers, appropriate for offline post-processing with log investigation tools. Send URLs sniffed from a client to local web browser for display, updated in real-time (that is, as the target surfs, the local browser surfs along). [1]

Packet sniffing is a technique that permits eavesdropping on traffic itinerant among networked computers. The packet sniffer wills seizure data that is addressed to further machines, saving it for future examination. All information that trips across a network is sent in "packets."

Packet sniffing can be prepared by the technique called honeypots. Honeypot is usually defined as an information system resource whose value lies in illegal or unlawful use of those resources. Honeypots are merely unsecured Wi-Fi access points that hacker's setup and trick people into consuming them. Characteristically, these honeypots are setup in public places such as coffee shops, trains, and the Wi-Fi network is named like "Public Wi-Fi". Unwary individuals then sign onto the tainted network and the packet sniffer then clutches their individual information when they enter belongings like their credit card info into a site or any other personal information.

Network cards have the capability to move in promiscuous mode (monitor mode), which allows them to listen to all network traffic regardless of if it's directed to them. Packet sniffers can seizure belongings like clear-text passwords and usernames or other sensitive material allows intruder to read out the actual e-mail., basic authentication and reads out financial transactions and credit card numbers. Sniffing is possible on non-switched and switched.

4.Network Analysis

Network traffic inspection might be well-defined the consequence of information from scrutiny of network Traffic comprised data. In general, Analysis categorized by time

criteria and by the purpose of the study. Any network traffic analysis can be classified in one of the following three categories:

- Real-time analysis: - It is implemented over the data as per it is acquired, or using small sets habitually so-called buffers to capably evaluate data. The response time is the time elapsed amongst assured events ensues and is calculated or noticed. Real-time analysis though, has usually high computational resources requirements.
- Batched analysis: - Batched scrutiny accomplishes by analysis periodically, where the period is enough to collect data in so-called data batches. Dependent on the batching policies, the reaction time and accompanying computational resources, in broad-spectrum it offer a higher response time and lower computational resources wants than real-time analysis and they need higher storage size.
- Forensics analysis: - Forensics examination are investigation performed when a particular event occurs (triggered analysis) for instance when an intrusion is discovered to a specific host. This kind of analysis entail that data had been previously stored to be analyzed, and may also require of human intervention. Network analyzers like tcpdump, Wireshark are some examples of packet Decoding applications. [1]

5.Packet Sniffing - Threats

There are three types of sniffing methods. Some methods work in switched networks while others work in non-switched networks. The sniffing methods are:

5.1.IP-based sniffing

This technique solitary works in non-switched networks. This is the genuine way of packet sniffing. This technique works by keeping the network card into monitor mode, and sniffing all packets identical the IP address filter. Usually, IP address filter not set so it can seizure all the packets. It simply shows traffic that permits on network interface. Though, if the sniffer is on a switch, it won't show any results. [2]

5.2.MAC-Based Sniffing

This technique works by setting the network card into monitor mode and sniffing all packets identical the MAC address filter. MAC-based sniffing is just similar to IP-based sniffing, but it filters founded on a system's MAC address in its place of its IP address. When a network device on a LAN needs to dialogue to a device that is *not* within the LAN, the traffic is sent to the LAN's default network device gateway. The gateway forwards it to its external destination. Since any traffic intended for the external devices must be sent to the local network device gateway, the Ethernet MAC address of those packets will be that of the network device gateway. By sniffing traffic with a terminus MAC address of your network.

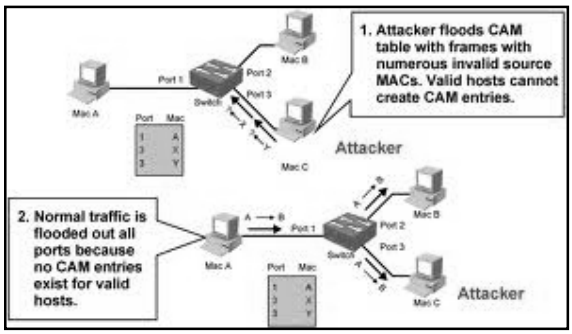

Figure 1

5.3.ARP-Based Sniffing

This technique works a slight dissimilar. It doesn't put the network card into monitor mode. This isn't essential because ARP packets will be sent to us. This occurs because the ARP protocol is stateless. Though, sniffing can be done on a switched network. Performing this kind of sniffing, first we have to poison the ARP cache of the two hosts that you want to sniff, categorizing yourself as the other host in the connection. When the ARP caches are poisoned, the two hosts start their dialogues, but in its place of directing the traffic directly to the other host it received to us. We then make log of that traffic and advancing it to the real intended host on the other side of the connection. It is known as man-in-the-middle attack. Until now we know that sniffers work only on hubs, where network packets broadcast to all linked machines on the hub. Entirely it's not true. Sniffers work only when network packets in between other machines are enforced to pass through the network interface of the sniffing machine. Sniffer can get linked to a hub is the simple way to achieve this. Other way to achieve this is configure a specific

switch port so that all traffic on the switch also diverted to that switch monitoring port.[3]

6.Arp Spoofing Attack- Anatomy

The basic principle behind ARP spoofing is to exploit the mentioned vulnerabilities in the ARP protocol .ARP spoofing attacks can be course from a compromised host on the LAN, or attacker's device that is linked straight to the target LAN. The attacker could then choose to:

- Inspect the packets, and forward the traffic to the actual default gateway (interception)
- Modify the data before forwarding it (man-in-the-middle attack).
- Entrance a denial-of-service outbreak by causing certain or all of the packets on the network to be fell.

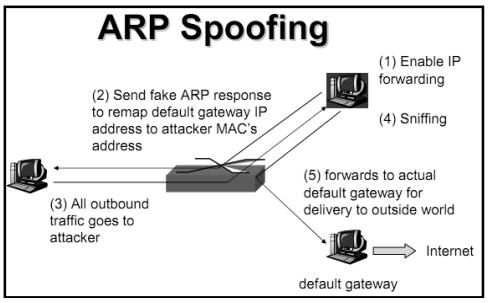

Figure 2

7.Tools For Analysis – Threat

Packet sniffers can capture things like clear-text passwords and usernames or other sensitive material. Our main goal in this admittedly brief section is to make the student aware of the existence of these tools that are freely available. A lot of very practical, devious, and possibly catastrophic features are buried in ettercap[4] and many others are there which can be misused by attackers.

- Ettercap is a network sniffer for switched LANs practices ARP poisoning after that man-in-the-middle technique to sniff all the connections between two hosts. It can inject characters to server (emulating commands) or to client (emulating replies) while maintaining an established TCP connection.[2]

- Tcpdump It is a common packet analyzer that runs underneath the command line. Permits the user to interrupt and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.
- Wireshark/ethereal Wireshark is a free and open-source packet analyzer. It runs on various Unix-like operating systems and on Microsoft Windows

8.Sniffing – *Detection*

"Prevention is better than cure" an idiom explains it all

It is not easy to distinguish Sniffers. If your network performance unexpectedly takes a hit, it is probable someone has triggered the switch to go into the failopen mode, or if users suddenly claim that something went wrong on network. It mostly due to the sniffing attacks on network. The best way to secure against sniffing is using encryption it will prevent you from sniffer as well as ensure that data flows through network must not be in readable forms. Much organization's using encryption as the counter tool against sniffing.

8.1.ARP Testing

A machine caches ARPs and make attackers network device to respond forcefully. It is done in two steps

- Arp caches: - A network device caches ARPs, to send a non-broadcast ARP. A machine that is not in monitor mode would never see the packet, since it wasn't intended to them, therefore it wouldn't reply. If a machine is in monitor mode, the ARP request would be seen by it.
- Ping packet broadcast: - Sending a ping packet broadcast, ping packet with network IP, but different MAC address. An attacker's network device MAC address from sniffed ARP frame will respond to the broadcasting Ping.

8.2.Latency Method

It is an assumption based method that sniffers use parsing. In this technique huge data is send on network and the attacker's network device is pinged before and after the data flooding on the network. If the machine in monitor mode, it will parse data and increase the load on network. It will take extra time for response of ping broadcasted packet. Point here is that packet gets overdue because of the load on network.

8.3.Sniffing- Detection Tools

Anti Sniff: L0pht Heavy Industries product "Anti Sniff". It has aptitude to monitor a network and discover if any computer is in monitor mode.

- ARP Watch: ARPWatch keeps track of Ethernet/IP address combinations. This is beneficial when you suspect that you are actuality spoofed.
- Snort: outstanding Intrusion Detection System (IDS) and its ARP-spoof preprocessor can be used to identify instances of ARP Spoofing, which might be an indication that network is getting sniffed.[3]

9.Phising

Phishing is the action of obtaining information such as usernames, passwords, and credit card particulars by sending a fake e-mail to a user and wrongly claiming to be an acknowledged or authorized enterprise for deceiving the user to surrender personal information for the motive of theft. By clicking on that mail it directs the user to visit a Web site where they are asked to update their individual information for instance passwords, credit card details and bank account numbers. The fake Website; however is to set up only to steal the user's information. It is a kind of decoy used in hope that the victim will get trapped by clicking a malicious link or attachments, in which case their financial information and passwords may then get stolen.

- Planning - Phishers decide which businessman to target and determine how to get e-mail addresses for the customers of that business.
- Setup - Once they know which business personality to deceive and who their victims are, phishers try to deliver the fake message and collect the data which involves e-mail addresses etc.
- Attack – In this the phisher sends a fake message that appears to be from a reputable source.
- Collection - Phishers record the information victims enter into Web pages or popup windows.
- Identity Theft and Fraud - The phishers use the information they've gathered to make illegal purchases or to commit fraud. [4]

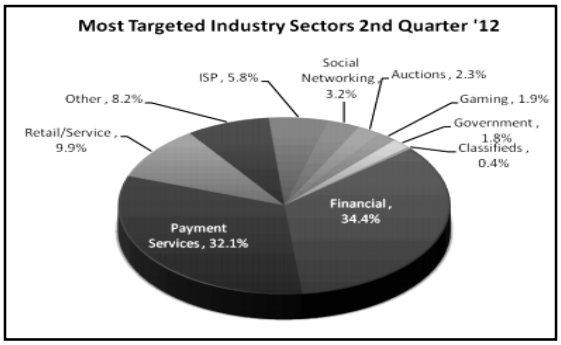

Figure 3

10.Phishing- Types

10.1.Spear Phishing

It is a type of phishing attack aimed at specific individuals or company, addressed on behalf of someone within the company at a reputated position and requesting information such as login IDs and passwords.Attackers try to gather as much personal information as he can about target to increase their probability ofsuccess.Once hackers get the personal information they can gain access to the secured networks of a company.[5]

10.2.Clone Phishing

It is a type of phishing attack where phisher creates an identical email. He do this process by getting information such as content and recipient addresses from an authorised email which was supplied previously, then he sends the same email with links replaced by malignant ones. He deceives the victim by employs address spoofing so that the email appears to be from the original sender. This technique could be used to gain a foothold on another machine, by manipulating the social trust associated with the inferred connection due to both parties receiving the original email.

10.3.Whaling

It is a kind of hoax meant to target upper managers in private companies**.** The objective is to deceive the upper manager into divulging the confidential company information on their hard drives.

11.Phishing- Solutions

11.1.Content Verification Certificates (CVC)

Content Verification Certificates (CVCs) makes easier the verification of website pages materials. They are build, spread, and revoked using proven Public Key Infrastructure method to provide the highest level of security for web page content. It simplifies the deployment of verified login boxes, navigation panes and accreditation/association logos. CVC's gives authority to enterprises to take stern and preventative measures to reduce phishing attacks thereby protecting the content of a web page and allowing verification.

11.2.Email Certificates

Spam is one of the most dangerous phishing transport medium and the incapability of a user to trace the correct source of the Email provides no guaranteed mechanism. Both organizations and individuals are vulnerable to such threats. One of method to prevent from phishing attack is Email Certificates that are digitally signed or encrypt e-mail to provide that level of confidence.

11.3.Self Awareness of User

"URL checkers" are available on internet so user should check URL'S online to prevent from phising.

Secondly if user is aware of this problem then user firstly should enter the wrong information or data so that it can mislead the intruder and then enter his/her right information or data.[5]

12.DoS ATTACKS

A DoS attack attempts to make a web resource unavailable to its users by flooding the target URL with more requests than the server can handle. This implies that during the attack period, normal traffic on the website will be either slowed down or totally interrupted. The specific purpose of DoS attacks is to to make a machine or network resource unavailable to its proposed users and to destruct the services offered to target. When the attack is going on, and no countermeasures has been taken to fix the problem,

the victim would not be able to access services on the internet. DOS attacks take benefit of flaws and weakness in IP Protocols stack in order to disrupt internet services.[6]

One common method is the attacker would start the ping command on their computer, aim it at their victim address, and let it run at maximum speed, trying to overflow the other side with ICMP Requests, or ping packets which saturates the target machine so that it cannot respond to true traffic also perform slow response to them and pretends unavailable. Such attacks usually lead to a server overload. DoS attacks are executed by either making the targeted computer to reset, or overwhelming its resources so that it won't be able to provide its intended service or blocking the communication media between the proposed users and the victim so that they can no longer communicate adequately.

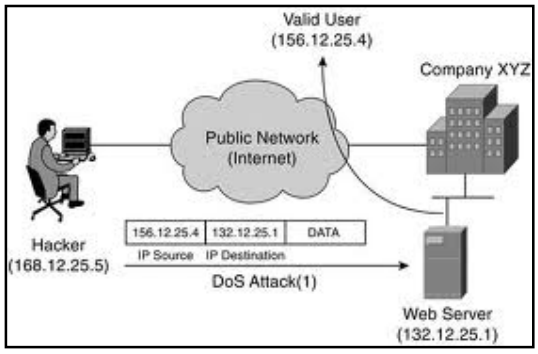

Figure 4

12.1.DoS - Effects

A DoS attack can be performed in different ways. The five basic types of attack are:

- Consumption of computing resources, such as disk space, bandwidth and CPU time.
- Disruption of configuration data, such as routing information.
- Disruption of formal information, such as unsolicited resetting of TCP sessions.
- Disruption of physical network modules.
- Blocking the communication media between the projected users and the target so that they can no longer communicate effectively.

12.2.DoS attacks- Solutions

12.2.1.Firewalls

Firewalls can be set up to have simple rules such to allow or deny protocols, ports or IP addresses which can be used

Keep a network secure. Its primary objective is to prevent unauthorized Internet users from accessing private networks connected to the Internet and to control the incoming and outgoing network traffic by analyzing the data packets and all messages entering or leaving the intranet pass through the firewall, which test every message and obstruct those that do not meet the specified security criteria.

12.2.2.IPS Based Prevention

The main functions of intrusion prevention systems is to identify malicious activity to find every information about this activity, try to block or stop it, and report it.Intrusion-prevention systems (IPS) are effective if the attacks have signatures associated with them.. It yields policies and set of rules for network traffic along with an intrusion detection system for alerting system or network administrators to untruthful traffic, but allowing the administrator to take the action upon being alerted.

12.2.3.DDS Based Defense

DDS protects IT infrastructure by preventing DDoS attacks from crippling your firewalls, intrusion prevention systems (IPS), switches and targeted web and DNS servers. It Detects and mitigates both traditional network-layer DDoS attacks and more advanced application-layer attacks helps to protects network, allowing legitimate communications to pass without delay .It provides automated real-time defence against identified DDoS attack sources . With position and location technology, permits enforcement of security policy founded on national origin of IP addresses.

12.2.4.Blackholing And Sinkholing

With blackholing, all the traffic to the attacked DNS or IP address is sent to a "black hole" . It can be managed by the ISP to be more active and avoid affecting network connectivity

Sinkholing routes traffic to a valid IP address which analyzes it and rejects bad ones. Sinkholing is not proficient for most severe attacks.[6]

13.Malware

Malware is software used or created by attackers to disarray computer operations, to collect sensitive information and to gain access to private computer systems. It may occur in the form of code, scripts, active conten etc.

Malware can take form of viruses, worms, and Trojan horses. Damaging malware can utilize popular communication tools to spread through your computer, which includes worms sent through email and instant messages, Trojan horses dropped from web sites to destroy the computer, and virus-infected files downloaded from peer-to-peer connections. Malware will also seek to unfairly use existing vulnerabilities in the system which makes their entry quiet and easy.

14.Malware- Types

14.1.Viruses

A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses has the property to copy themselves as fast as possible. They are mostly man-made. A simple virus replicates itself over and over again and are relatively easy to produce. Even such a simple virus can be damaging because it can quickly use all available memory of the systemand bring it to a halt.Most dangerous type of virus is one which is capable of transmitting itself across networks and bypassing security systems.

14.2.Worms

It is a kind of program or algorithm that replicates itself over a computer network and usually performs malicious activities, for instance using up the computer's resources and possibly shutting down the system. *WORM* is an acronym for "*write once,read many"(times) which is* an optical disk technology that permits you to write data onto a disk just once. After that, the data becomes permanent and can be read any number of times.

14.3.Spyware

Spyware is a collective term for software which monitors andgathers personal information about the user like the pages frequently visited, email address, credit card number, keypressed by user etc. It generally enters a system when free ortrial software is downloaded.

14.4.Trojans

A Trojan horse is kind of non self replicating malware which appears to perform a desirable function but instead facilitates unauthorized access to the user's computer system. Trojans not try to inject themselves into other files like a virus. Trojan horses are used to steal information and to harm their host computer systems. Trojans can be injected by use drive-by downloads or by installing via online games or internet-driven applications in order to reach target computers.[7]

15.Conclusion

Network security is one the most important field that is increasingly gaining attention as internet and internet users are expanding day by day.

The security issues in our networked system as described in this paper identify some of the work that needs to be done, and the urgency with which concern needs to be addressed which we have tried with our paper.As the density of network increases, necessity for translational participation in improving network security increases. The increase in number of technologies and the potential for changing threats is taxing our understanding our threats and how to deal with them. We are becoming more networked society, the financial benefits for intruders in a network increase. Number of attacks and there complexity increasing trying to breach a network continues. We can deal it with continue to educate the personnel which are tasked with network security and also educate their workforce on the newest type of attacks and make the necessary preparation to prevent against them.Network security is an important concern that must be seriously taken. The number of attacks are rising day by day as the use of internet become increasingly popular and more people are becoming aware of some of vulnerabilities at hand.

Sniffers are known as administrator's wickedest nightmarish. Sniffing detection software may satisfy to work out admins from some conditions, but it is not as simple as we think so. Nobody has really come up with a good solution, except smart bridges, routers that keep track of *MAC addresses***.** Sniffing a network is easy to do but it is difficult to detect and cumbersome task, because they are practically impossible to detect. The above discussed software's can aid's in detection. Thus we are forced to make an optimized software or framework that can optimally detects the vulnerabilities on the network as well as protect against them up to mark. Network administrators need to look continuously for new attacks on the internet and take the appropriate action and precaution. Through our paper we have tried to aware people regarding network security and solutions so that all the internet users all over the world can protect their network and data from the possible threat.

16.Reference

1. Pallavi Asrodia, Hemlata Patel (IJERA) ISSN: 2248-9622 www.ijera.com vol. 2, Issue 3, May-Jun 2012, pp.854-856 854 | P a g e Network Traffic Analysis Using Packet Sniffer Pallavi Asrodia, Hemlata Patel (Computer Science, dept., Jawaharlal Institute of Technology, Borawan, Khargone (M.P.) India.)
2. Sniffers Basics and Detection [version 1.0-1] Sumit Dhar Information Security Management Team Reliance, Infocomm,Internet Security ECOM 5347 Lab 1 SniffingTo fill
3. http://ettercap.sourceforge.net,

   http://linux-sec.net/Sniffer.Detectors/snifferdetection.pdf
4. APWG Phishing Activity Trends Report 2nd Quarter 2012 Unifying the Global Response to cybercrime April-June 2012 published September 2012.
5. Trend Micro Incorporated Research Paper2012 Spear-Phishing Email: Most Favored APT Attack Bait.
6. Saurabh Ratnaparikhi(M.tech CSE CMJ,University) and Anup Bhange(Asst Prof.) DDOS Attacks on Network; Anomaly Detection using Statistical Algorithm December 2012
7. Survey on Malware Detection Methods, Vinod P., V.Laxmi, M.S.Gaur, Malaviya NIT, Jaipur