IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Study of Network Security Aspects and its Pervasive Attacks and Tools

Mrs.V.SATHYA, Assistant Professor,
Department of Computer Applications,
Sri G.V.G Visalakshi College for Women, Udumalpet, India.

***Abstract* -** Network security is the process of strategizing a defensive approach to secure our data and resources over the computer network infrastructure against any potential threat or unauthorized access. It uses software as well as hardware technologies to achieve the optimal solution for network defense. The main issue of network security is computing because many types of attacks are increasing day by day. Protecting computer and network security are critical issues now-a-days. There are different kind of attacks that can be sent across the network. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide and all of these required different security techniques. This paper discusses the different kinds of attacks along with Security tools that can be applied according to the network.

***Index Terms* -** Network Security, attacks, hackers, firewalls, encryption, security analysis threat analysis, security vulnerability, malware, communication, internet

I. INTRODUCTION

The world is becoming more interconnected of the Internet and new networking technology. Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, modification in system, misuse, or denial of a computer network and network-accessible resources. Basically, network security involves the authorization of access to data in a network, which is controlled by the network admin. It has become more important to personal computer users, and organizations.

Network security can be defined as protection of networks and their services from unauthorized alteration, destruction, or disclosure, and provision of assurance that the network performs in critical situations and have no harmful effects for the users. The network security is analyzed by researching the following:

- Aspects of Network security and real time applications
- Types of Network security
- Types of security attacks
- Network security tools

II. ASPECTS OF NETWORK SECURITY AND REAL TIME APPLICATIONS

Network security is the process of preventing network attacks across an any network infrastructure. 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, where the chances of threats are more penetrating. A possible hacker could target the communication channel, obtain the data, decrypt it and re-insert a false message. Hence, securing the network is just as important as securing the computers and encrypting the message which we want to be kept private. securing the network is just as important as securing the computers and encrypting the message which we want to be kept private. It deals with the three crucial areas of security **C**onfidentiality, **I**ntegrity, and **A**vailability.

The fundamentals of network security are:

1. Physical security - protection of personnel, hardware, software, networks.
2. Access controls - appropriate access to the data.
3. Authentication - validating the identity of a registered user.
4. Accountability – traceability of actions performed on a system.

There are many aspects that make up network security the main components are prevention, protection and security.

As an example, Figure 1 shows a typical real time security application implementation designed to protect a Public Digital Wireless Network. The Integrated Services Digital Network (ISDN) is the first public digital network. The applications supported by Public Digital Wireless Networks are Public Hot Spot services, Video Surveillance and Security services, Traffic control, Fire Service support, Civil and Health care services. Digital security systems rely on high-speed networks. The connection allows for fast alerts and speedy functions.

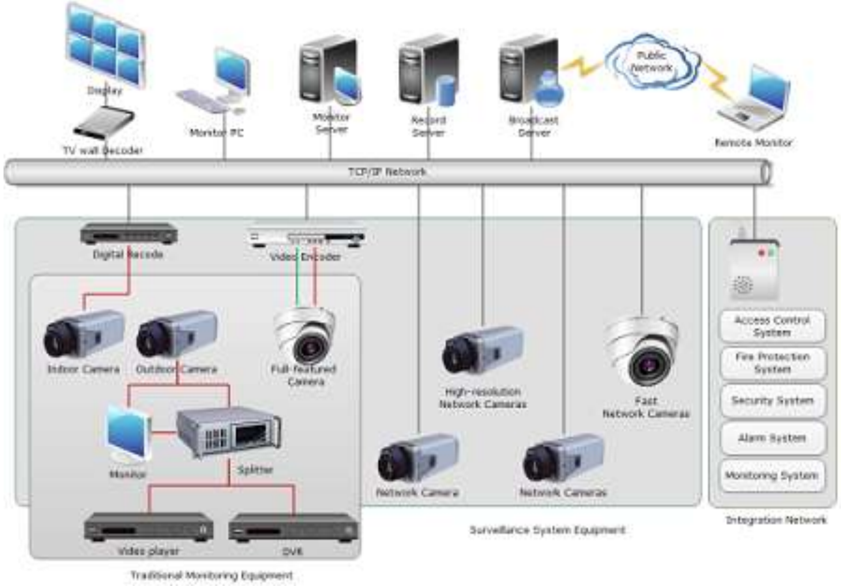

Figure 1. Public Digital Network Security

III. TYPES OF NETWORK SECURITY

Network security works by identifying and targeting a variety of threats, then stops from entering network. It acts as a wall between our network and any malicious activity. This wall will remain penetrable until find the best solution to protect it. There are various types of network security, such as:

3.1 Antivirus and Antimalware Software

This software is used for protecting against malware, which includes spyware, ransomware, Trojans, worms, and viruses. Malware can also become very dangerous as it can infect a network and then remain calm for days or even weeks. This software handles this threat by scanning for malware entry and regularly tracks files afterward in order to detect anomalies, remove malware, and fix damage.

3.2 Application Security

It is important to have an application security since no app is created perfectly. It is possible for any application to comprise of vulnerabilities, or holes, that are used by attackers to enter your network. Application security thus encompasses the software, hardware, and processes you select for closing those holes.

3.3 Behavioral Analytics

In order to detect abnormal network behavior, user have to know what normal behavior looks like. Behavioral analytics tools are capable of automatically discerning activities that deviate from the norm. So, security team will be able to efficiently detect indicators of compromise that pose a potential problem and rapidly remediate threats.

3.4 Data Loss Prevention (DLP)

Organizations should guarantee that their staff does not send sensitive information outside the network. They should thus use DLP technologies, network security measures, that prevent people from uploading, forwarding, or even printing vital information in an unsafe manner.

3.5 Email Security

Email gateways are considered to be the number one threat vector for a security breach. Attackers use social engineering tactics and personal information in order to build refined phishing campaigns to deceive recipients and then send them to sites serving up malware. An email security application is capable of blocking incoming attacks and controlling outbound messages in order to prevent the loss of sensitive data.

3.6 Firewalls

Firewalls place a barrier between your trusted internal network and untrusted outside networks, like the Internet. A set of defined rules are employed to block or allow traffic. A firewall can be software, hardware, or both. The free firewall efficiently manages traffic on our PC, monitors in/out connections, and secures all connections when you are online.

3.7 Intrusion Prevention System (IPS)

An IPS is a network security capable of scanning network traffic in order to actively block attacks. The IPS Setting interface permits the administrator to configure the ruleset updates for Snort. It is possible to schedule the ruleset updates allowing them to automatically run at particular intervals and these updates can be run manually on demand.

3.8 Mobile Device Security

Mobile devices and apps are increasingly being targeted by cybercriminals. 90% of IT organizations could very soon support corporate applications on personal mobile devices. There is indeed the necessity for you to control which devices can access your network. It is also necessary to configure their connections in order to keep network traffic private.

3.9 Virtual Private Network (VPN)

A VPN is another type of network security capable of encrypting the connection from an endpoint to a network, mostly over the Internet. A remote-access VPN typically uses IPsec or Secure Sockets Layer in order to authenticate the communication between network and device.

3.10 Wireless Security

The mobile office movement is presently gaining momentum along with wireless networks and access points. However, wireless networks are not as secure as wired ones and this makes way for hackers to enter. It is thus essential for the wireless security to be strong. It should be noted that without stringent security measures installing a wireless LAN could be like placing Ethernet ports everywhere. Products specifically designed for protecting a wireless network will have to be used in order to prevent an exploit from taking place.

3.11 Network Access Control (NAC)

This network security process helps us to control who can access our network. It is essential to recognize each device and user in order to keep out potential attackers. This indeed will help you to enforce your security policies. Noncompliant endpoint devices can be given only limited access or just blocked.

IV. TYPES OF NETWORK SECURITY

Network security attacks are unauthorized actions against private, corporate or governmental IT assets in order to destroy them, modify them or steal sensitive data. As more enterprises invite employees to access data from mobile devices, networks become vulnerable to data theft or total destruction of the data or network.

4.1 Passive Attack

A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. It includes traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords.

4.2 Active Attack

In an active attack, the attacker tries to bypass or break into secured systems in the going on communication. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

4.3 Virus

A virus is not self-executable; it requires the user's interaction to infects a computer and spread on the network. An example is an email with a malicious link or malicious attachment. When a recipient opens the attachment or clicks the link, the malicious code gets activated and circumvents the systems security controls and makes they inoperable. In this case, the user inadvertently corrupts the device.

4.4 Malware

Malware attack is one of the most severe cyberattacks that is specifically designed to destroy or gain unauthorized access over a targeted computer system. Most malware is self-replicating, it means when it infects a particular system, it gains entry over the internet and from thereon, infects all the systems connected to the internet in the network. An external endpoint device if connected, will also get infected. It works exceptionally faster than other types of malicious content.

4.5 Worm

A worm can enter a device without the help of the user. When a user runs a vulnerable network application, an attacker on the same internet connection can send malware to that application. The application may accept the malware from the internet and execute it, thereby creating a worm.

4.6 Phishing

Phishing is the most common types of network attacks. It stands for sending emails purporting as from known resources or bankers and creating a sense of urgency to excite user to act on it. The email may contain malicious link or attachment or may ask to share confidential information.

4.7 Botnet

It is a network of private computers which are a victim of malicious software. The attacker controls all the computers on the network without the owner's knowledge. Each computer on the network is considered as zombies as they serve the purpose of spreading and infecting a large number of devices or as guided by the attacker.

4.8 DoS (Denial of Service)

A Denial of Service is a crucial attack that destroys fully or partially, victim's network or the entire IT infrastructure to make it unavailable to the legitimate users.

4.9 Distributed Denial of Service (DDoS)

It is a complex version of a DoS attack and is much harder to detect and defend compared to a DoS attack. In this attack, the attacker uses multiple compromised systems to target a single DoS attack targeted system. The DDoS attack also leverages botnets.

4.10 Man-in-the-middle

A man-in-the-middle attack is someone who stands in between the conversation happening between you and the other person. By being in the middle, the attacker captures, monitors, and controls your communication effectively. For example, when the lower layer of the network sends information, the computers in the layer may not be able to determine the recipient with which they are exchanging information.

4.11 Packet Sniffer

When a passive receiver placed in the territory of the wireless transmitter, it records a copy of every packet transmitted. These packets can contain confidential information, sensitive and crucial data, trade secrets, which when flew over a packet receiver will get through it. The packet receiver will then work as a packet sniffer, sniffing all the transmitted packets entering the range. The best defense against packet sniffer is cryptography.

4.12 DNS Spoofing

It is about compromising a computer by corrupting domain name system (DNS) data and then introducing in the resolver's cache. This causes the name server to return an incorrect IP address.

4.13 IP Spoofing

It is the process of injecting packets in the internet using a false source address and is one of the ways to masquerade as another user. An end-point authentication that ensures the certainty of a message originating from the place we determined would help in defending from IP spoofing.

4.14 Compromised Key

An attacker gains unauthorized access to a secured communication using a compromised key. A key refers to a secret number or code required to interpret secured information without any intimation to the sender or receiver. When the key is obtained by the attacker, it is referred to as a compromised key which serves as a tool to retrieve information.

V. NETWORK SECURITY TOOLS

Network security tools can be either software- or hardware-based and help security teams protect their organization's networks, critical infrastructure, and sensitive data from attacks. These include tools such as firewalls, intrusion detection systems and network-based antivirus programs.

5.1 Intrusion Prevention System (IPS)

Intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. Major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it and attempt to block or stop it. Intrusion prevention systems are contemplated as augmentation of Intrusion Detection Systems (IDS) because both IPS and IDS operate network traffic and system activities for malicious activity.

IPS typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IPS can also respond to a detected threat by attempting to prevent it from succeeding. They use various response techniques, which involve the IPS stopping the attack itself, changing the security. Intrusion Prevention System (IPS) is classified into 4 types:

5.1.1 Network-based intrusion prevention system (NIPS)

Network-based Intrusion Prevention Systems (NIPS) are the network security appliances or applications that monitor the network traffic comprising network segments or devices, and analyze the network and the protocol activities for any suspicious activities. The main functions of intrusion prevention systems are to protect the network from threats such as identify malicious or suspicious activities, log information about these activities, attempt to block or stop them, and report them. It monitors the entire network for suspicious traffic by analyzing protocol activity

5.1.2 Wireless intrusion prevention system (WIPS)

A wireless intrusion prevention system (WIPS) is a dedicated security device or integrated software application that monitors a wireless LAN network's radio spectrum for rogue access points and other wireless threats. It monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.

5.1.3 Network behavior analysis (NBA)

Network behavior analysis (NBA) is a network monitoring program that ensures the security of a proprietary network. NBA helps in enhancing network safety by watching traffic and observing unusual activity and departures of a network operation. Conventional methods of defending a network against harmful data include packet checking, signature recognition and real-time blocking of malicious sites and data. It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy violations.

5.1.4 Host-based intrusion prevention system (HIPS)

A host-based intrusion prevention system (HIPS) is a system or a program employed to protect critical computer systems containing crucial data against viruses and other Internet malware. Starting from the network layer all the way up to the application layer, HIPS protects from known and unknown malicious attacks. It is an inbuilt software package which operates a single host for doubtful activity by scanning events that occur within that host.

5.2 Detection Method of Intrusion Prevention System

5.2.1 Signature-based detection

Signature-based detection is a process where a unique identifier is established about a known threat so that the threat can be identified in the future. In network detection systems like IDS, signatures are defined to look for characteristics within network traffic Signature-based IDS operates packets in the network and compares with pre-built and preordained attack patterns known based as signatures.

5.2.2 Statistical anomaly- detection

Anomaly based IDS monitors network traffic and compares it against an established baseline. The baseline will identify what is normal for that network and what protocols are used. However, It may raise a false alarm if the baselines are not intelligently configured. A statistical anomaly occurs when something falls out of normal range for one group, but not as a result of being in that group.

5.2.3 Stateful protocol analysis detection

Stateful protocol analysis identifies deviations of protocol state similarly to the anomaly-based method but uses predetermined universal profiles based on "accepted definitions of benign activity" developed by vendors and industry leaders. This IDS method recognizes divergence of protocols stated by comparing observed events with pre-built profiles of generally accepted definitions of not harmful activity.

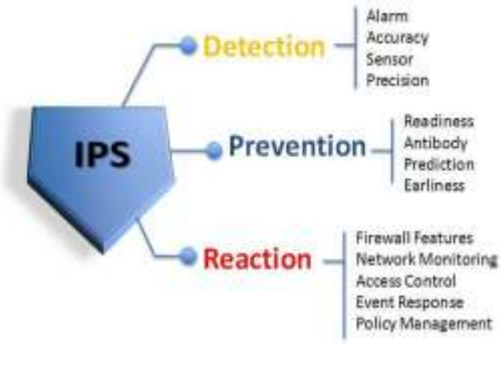

Figure 1. Features of IPS

As seen from Figure 1, the feature function of IPS is shown Intrusion Prevention provides numerous capabilities at both the host level and the network level, but from a high-level perspective, the capabilities provided by IPSs fall into two major categories: (i) Attack prevention, and (ii) Regulatory compliance. Additionally, much type of IPSs potentially avoid the weakness of signature-based intrusion detection systems and it can learn classes of harmful system behavior and the types of events that they attempt to produce in targeted system. Therefore, it is much better suited to react appropriately to zero-day attacks. Hence, from this analysis, it is identified that. IPS will also become more proficient because IDS, early detection, intrusion response is a fundamental aspect when intrusion prevention in developing.

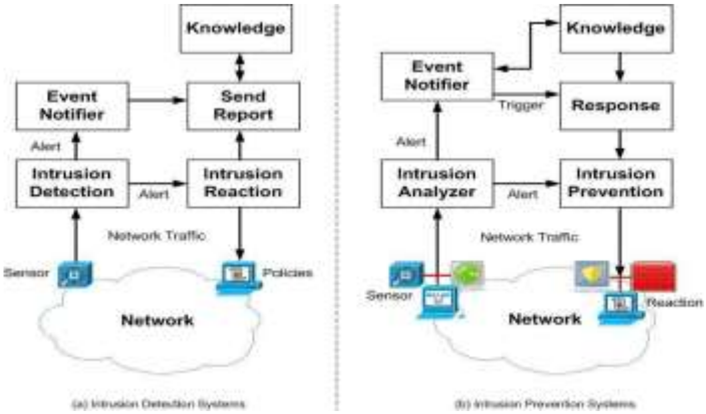

Figure 2. Basic Fundamental IDS / IPS

The address difference of challenge of detection, response and prevention, various analysis techniques have been proposed in recent years. Figure 2, Basic fundamentals of IDS/IPS in the Network security system. The Network analyze the data through the devices and it alert the system.There are some significant gaps, challenges and preliminary results for future direction in IPS to improving, mining and reducing false alarm, this work is improvement of statement on research gaps and extension from performed work.

Table 1. Comparison IDS and IPS

	Intrusion Detection System	Intrusion Prevention System
Usefulness	IDS design just only identify and examined to produce Alarm	IPS design is to enhance data processing ability, intelligent, accurate of itself.
OSI Layer	Layer 3	Layer 2, 3,4 and 7
Signatures Action	• Simple pattern matching • Stateful pattern matching • Protocol decode-based analysis • Heuristic-based analysis	• Recognize attack pattern • Blocking & response action • Stateful pattern matching • Protocol decode-based analysis • Heuristic-based analysis
Activity	• A passive security solution • Detect attack only after they have entered the network, and do nothing to stop attacks only just attacks traffic and send alert to trigger.	• Reactive response security solution • Early Detection, proactive technique, early prevent the attack, when an attack is identified then blocks the offending data
Component	• Cannot expect to detect all malicious activity at all time • Handling alert to trigger false positive or false negative Alarm	• Can be detect new signatures or behavior attack • Handling alert to trigger false positive or false negative alarm
Blocking future traffic	Cannot integrated with filtering rules security to stop traffic from attacking	Have the capability to block and can apply policy perimeter router or firewall
Event Response	Capability only to recognize and report to security operator in the event of attack.	• Have mechanism allow, block, log, and report • Integrated mechanism threat management to security operator

VI. CONCLUSION

Computer network security is a complicated issue, involving many aspects of computer technology, network management, network usage and maintenance. In order to increase computer network security, we should mix various types of applications for protection measures. It is necessary to develop more effective security solving measures, thereby to improve the computer network security prevention and. It is a long way to go to ensure the normal operation of large-scale network system and communication and maintain sustainable and efficient transport network. One integration system for detection, prevention and reaction may still be valid today for network management, countermeasure against, monitoring internal networks and for behavioral analysis.

VII. **ACKNOWLEDGEMENT**

The author is very thankful to **Sri G.V.G Visalakshi College for Women and Management.**

REFERENCES

[1] P. Aruna Devi, International Journal of P2P Network Trends and Technology – Volume 3 Issue 2 March to April 2013.

[2] "Security Overview," www.redhat.com/docs/manuals/enterprise/RHEL-4- Manual/security-guide/ch-sgs-ov.html.

[3] X. Chen, K. Makki, K. Yen, N. Pissinou, "Sensor network security: a survey", IEEE Communications Surveys & Tutorials, Vol. 11(2), 52-73, 2009.

[4] K. Kumar, "Securing communication using function extraction technology for malicious code behavior analysis," *Computers & Security*, vol. 28, Feb. 2009, pp. 77-84.

[5] Ghorbani A.A, *Network Intrusion Detection and Prevention : Concepts and Technique*, Springer, 2009.

[6] M. Alsaleh, D. Barrera, and P.C.V. Oorschot, "Improving Security Visualization with Exposure Map Filtering," *2008 Annual Computer Security Applications Conference (ACSAC)*, Dec. 2008, pp. 205-214.

[7] Shobha Arya1 And Chandrakala Arya2, "Malicious Nodes Detection In Mobile Ad Hoc Networks", Journal of Information and Operations Management, ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, 2012, pp-210-212.

[8] Siddharth Ghansela "Network Security: Attacks, Tools and Techniques" , ijarcsse Volume 3, Issue 6, June 2013.

[9] Predictions and Trends for Information, Computer and Network Security [Online] available: http://www.sans.edu/research/security-laboratory/article/2140

[10] A White Paper, ―Securing the Intelligent Network‖, powered by Intel corporation.

[11] Network Security [Online] available: http://en.wikipedia.org/wiki/Network_security.

[12] Network Security: History, Importance, and Future‖, University of Florida Department of Electrical and Computer Engineering, Bhavya Daya.

[13] Ateeq Ahmad, ―Type of Security Threats and its Prevention**",** Ateeq Ahmad, Int.J.Computer Technology & Applications, Vol 3 (2), 750-752.

[14] Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257.

[15] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, ―A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks‖, *(IJCSIS) International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009.*

[16] Network Security Types of attacks [Online] available: http://computernetworkingnotes.com/network-security-access-listsstandardsand-extended/types-of-attack.html.

[17] Adeyinka, O., "Internet Attack Methods and Internet Security Technology," *Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on*, vol., no., pp.77-82, 13-15 May 2008.

[18] Charles J. Kolodgy Christian A. Christiansen, ―Network Security Over watch Layer: Smarter Protection for the Enterprise‖, Sponsored by: Trend Micro, November 2009.

[19] A. R. F. Hamedani, "Network Security Issues, Tools for Testing," School of Information Science, Halmstad University, 2010.

[20] Intrusion Prevention System: A Survey - Deris Stiawan, Hanan Abdullah, Yazid Idris Journal of Theoretical and

Applied Information Technology · June 2012.

[21] H. Read, a Blyth, and I. Sutherland, “A Unified Approach to Network Traffic and Network Security Visualisation,” *2009 IEEE International Conference on Communications*, Jun. 2009, pp. 1- 6.

[22] K. Alsubhi, E. Al-shaer, and R. Boutaba, “Alert Prioritization in Intrusion Detection Systems,” *IEEE proceeding Network Operations and Management Symposium*, 2008, pp. 33-40.

[23] W. Junqi and H. Zhengbing, “Study of Intrusion Detection Systems (IDSs) in Network Security,” *IEEE. Wireless Communications, Networking and Mobile Computing. WICOM 08*, 2008, pp. 1-4.

[24] W. Li and S. Tian, “An ontology-based intrusion alerts correlation system,” *Expert Systems with Applications*, vol. 37, Oct. 2010, pp. 7138-7146.

[25] A.Ghorbani, W. Lu, and M. Tavallaee, “Network Intrusion Detection and Prevention,” *Network Intrusion Detection and Prevention*, Boston, MA: Springer US, 2010, pp. 129-160.

[26] N. Stakhanova, S. Basu, and J. Wong, “A taxonomy of intrusion response systems,” *International Journal and Computer Security*, vol. 1, 2007, pp. 169-184.

[27] K. Salah and a Kahtani, “Performance evaluation comparison of Snort NIDS under Linux and Windows Server,” *Journal of Network and Computer Applications*, vol. 33, Jan. 2010, pp. 6- 15.

[28] R.A. Martin, “Managing Vulnerabilities in Networked Systems,” *Computer*, vol. 34, 2001, pp. 32-38.

[29] P.P. Tsang, A. Kapadia, C. Cornelius, and S.W. Smith, “Nymble : Blocking Misbehaving Users in Anonymizing Networks,” *IEEE Transaction Dependable and secure computing*, 2009, pp. 1- 15.

[30] Z. Zhou, T. Song, and Y. Jia, “A High- Performance URL Lookup Engine for URL Filtering Systems,” *IEEE ICC 2010*, 2010, pp. 1-5.

[31] S.R.G. Gopi K. Kuchimanchi, Vir V. Phoha, Kiran S. Balagani, “Dimension Reduction Using Feature Extraction Methods for Real-time Misuse Detection Systems,” *Analysis*, 2004, pp. 10-11.

[32] O. Depren, M. Topallar, E. Anarim, and M.K. Ciliz, “An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks. Expert Systems with,” *Expert System with Application*, vol. 29, 2005, pp. 713- 722.

[33] K. Hwang, M. Cai, Y. Chen, S. Member, and M. Qin, “Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes,” *IEEE Transactions on Dependable and Secure Computing*, vol. 4, 2007, pp. 41-55.

[34] H. Artail, H. Safa, M. Sraj, I. Kuwatly, and Z. Al- masri, “A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks,” *Computer & Security*, vol. 25, 2006, pp. 274-288.

[35] P. Garcıa-Teodoro, J. Dian-Verdejo, G. Macia- Fernandez, and E. Vazquez, “Anomaly-based network intrusion detection : Techniques , systems and challenges,” *Computer & Security*, vol. 28, 2009, pp. 18-28.

[36] Suramwar, M.V. and S. Bansode, *A Survey on different types of Intrusion Detection Systems.* International Journal of Computer Applications, 2015. 122(16).