A COMPARATIVE STUDY BETWEEN INTRUSION DETECTION SYSTEM AND INTRUSION PREVENTION SYSTEM

Author Details

[1]Dr Mehul Patel, Assistant Professor, SEMCOM, The CVM University, Vallabh Vidyanagar

[2]Dr. Dipal Patel, Assistant Professor, SEMCOM, The CVM University, Vallabh Vidyanagar

Abstract:

Intrusion into the computing environment is a very common unwanted malicious activity that has been going on since the beginning of computing resources. Numerous security measures have been taken over the last three decades, but as the technology grows, security is at risk. Whether the whole world, directly or indirectly, depends on computers, it is a very important issue to prevent malicious activities and threats that hinder the structure of computing. The Intrusion Detection System (IDS) and the Intrusion Prevention System (IPS) are the standards for securing computing resources in most networks. They are deployed in the network to ensure an intrusion-free computing environment. In this paper, we will discuss both techniques in detail to prevent malicious activity on a computer network, their efficiency, their operation and their effectiveness.

Keywords- IDS, IPS, Intrusion, Intrusion Detection, Intrusion Prevention, Firewall, Security

Introduction

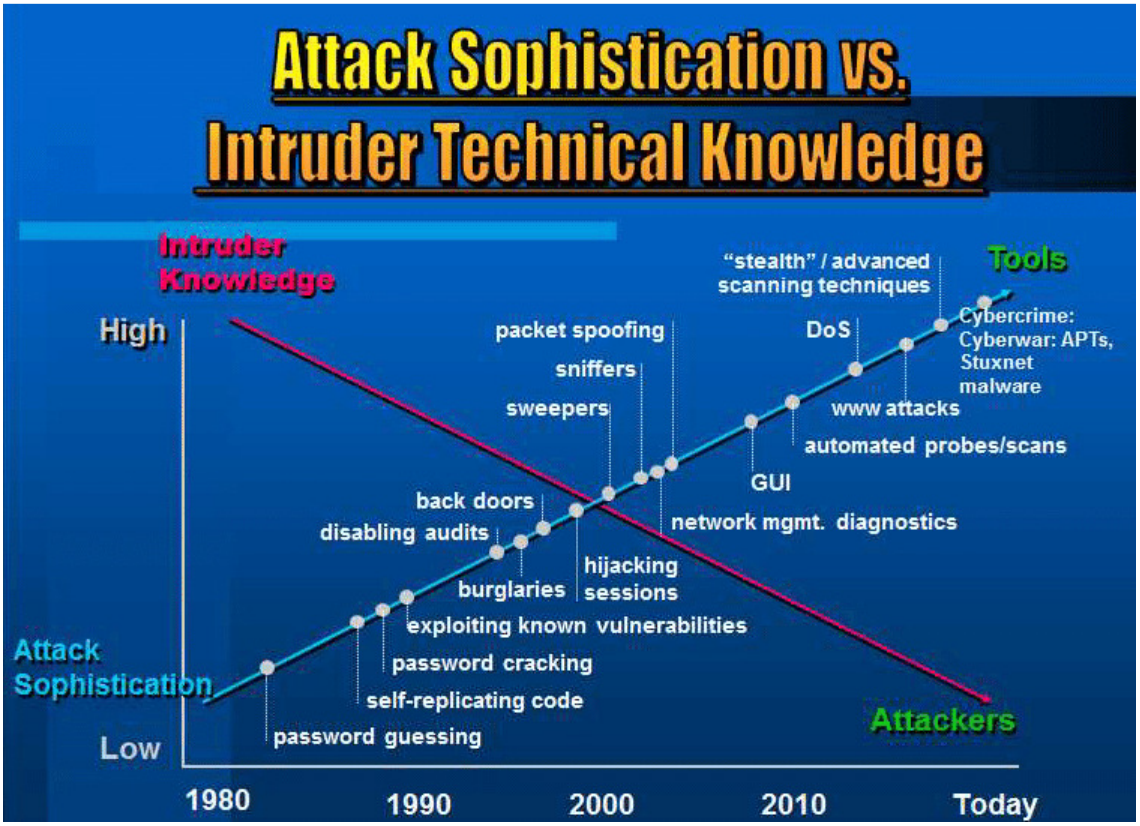
Intrusion are often outlined as unauthorized access to another's property or territory, however in terms of engineering, it's activities that compromise basic electronic network security goals. Confidentiality, Integrity and Privacy. Intrusion detection is that the method of observation events that occur during an automatic data processing system or network and analysing them for signs of attainable prevalence of violations of laptop security practices, acceptable use policies, or normal security policies. An Intrusion Detection System (IDS) could be a piece of code or hardware that automates associate degree intrusion detection method. it's designed to observe events that occur during an automatic data processing system and network and answer incidents that indicate attainable incidents of security policy

violations. The Intrusion Interference System (IPS), on the opposite hand, is each a way for detection intrusive or threatening activities and taking preventive measures to capture them. It mechanically combines the data of IDS.

History and development

Protecting data from the installation of computers and the beginning of their enormous applications is a major issue. The study of intrusion detection has been an active field of research for over three decades. It began in 1980 with the publication of John Anderson's Computer Security Threat Monitoring and Surveillance, one of the earliest research papers in the field. The "Intrusion Detection Model", published in 1987, by Dorothy Denning's seminal paper, provides a systematic framework that has inspired a number of researchers. Since then, over the past two decades, despite significant research and huge commercial investments, intrusion detection technology has been immature and ineffective.

In the early days of computers, hackers rarely used automated tools to gain access to systems. They were gifted with a high level of expertise and followed their own method of performing such actions. The current scenario is now quite different. A huge number of intrusive tools and applications are now available that can be used to exploit scripts that exploit widely known vulnerabilities. Figure 1 shows the relationship between the attackers and the relative sophistication of the attackers from the 1980s to the present day.



Source: https://images.app.goo.gl/nSPYCAPecPyrkTbN7

Prior to the development of modern IDS, intrusion investigations included manual searches for inconsistencies. With the availability of sufficient processing speeds, it is now possible not only to detect an instance of an attack after an event has occurred, but also to monitor it in "real-time" and to alert if intruders have been detected.

Due to the financial loss caused by downtime from the computer, loss of image or even intelligence is being affected, in recent years not only warning but also demand to stop the attack has become an absolute necessity. Especially with the introduction of Daniel Service F Service (DOS) and Distributed Daniel Service F Service F Service (DDOS) attacks, market demand has become stronger for Intrusion Prevention Systems (IPS) rather than just intrusion investigations.

Intrusion detection system

Intrusion detection is that the act of police investigation unwanted traffic on a network or device. The Intrusion Detection System (IDS) could also be a chunk of code or physical device put in that monitors network traffic to notice unwanted activity and unwanted and

malicious traffic, traffic violating safety policy, and traffic violating acceptable use policies. Several IDS tools will store the detected event in an exceedingly review log at a later date or mix the events with alternative knowledge to form policy or loss management selections. the most functions of IDS will be noticed as follows-

1. Recording info associated with determined events.
2. Notify the directors of the determined necessary determined events.
3. Reports generate reports.

Methodology of intrusion detection methodology

Different types of intrusion detection strategies are offered because of variations in network configuration.

Each of them has its own blessings and drawbacks that got to be explored, designed and priced.

1 Artificial primarily based investigation

The signature could be a pattern that corresponds to identified threats. In signature-based investigations, determined events are compared to spot probably unwanted traffic compared to pre-determined signatures. this kind of detection technique is extremely quick and simple to tack together.

Signature-based investigations are terribly effective in sleuthing identified threats however for the most part ineffective in sleuthing antecedent unknown threats, hidden threats victimization discontinuous techniques, and plenty of sorts of identified threats. associate degree wrongdoer will slightly modify associate degree attack to render undetectable by signature-based IDS. Still, IDS employing a signature-based methodology is terribly correct, despite its restricted capabilities.

2 Individual primarily based investigation

Inconsistency-based investigation is that the method of comparison definitions of what's thought-about traditional to activity against determined events to spot vital deviations. IDS victimization inconsistency primarily based checks have profiles that represent common behaviours like users, hosts, network connections or applications. Profiles are developed by perceptive the characteristics of typical activity over an amount of your time.

The big advantage of Oma politico primarily based detection technology is that they will be terribly helpful for sleuthing unwanted traffic that's not notably identified. as an example, associate degree inconsistency-based IDS can sight that net Protocol (IP) packets are malicious. It cannot sight that it's contaminated in any specific approach, however suggests that it's incompatible.

3 Mounted protocol analysis

Stateful protocol analysis is that the method of comparison the planned profile of usually accepted definitions of benign protocol activity for every protocol state against the determined events to spot deviations. The stateful protocol examination to an inconsistency primarily based investigation, however it may also analyse traffic on the network and transport layer and vendor-specific traffic on the applying layer, that can't be associate degree inconsistency primarily based investigation.

Forms of Intrusion Detection System

There square measure many sorts of IDS techniques that monitor the categories of events and also the method they organize. Here during this document we'll discuss the subsequent four types-

1. Network Based primarily IDS
2. Wireless IDS
3. Network Behaviour Anomaly Detection
4. Host Based IDS

1 Network Based primarily IDS

Network-based IDS (NIDS) monitors network traffic for a particular network section and analyses network and application protocol activity to spot suspicious activity. it's sometimes deployed on the boundaries of networks like routers, firewalls, virtual personal networks, etc.

The main disadvantage of this kind of IDS is that it's just one purpose of failure. Moreover, it's susceptible to DS attacks. It monitors the complete network and deploys to the boundaries of the network. however, it's not appropriate for safeguarding each host within the network. If AN interloper might bypass it, all network systems would be in hassle.

.

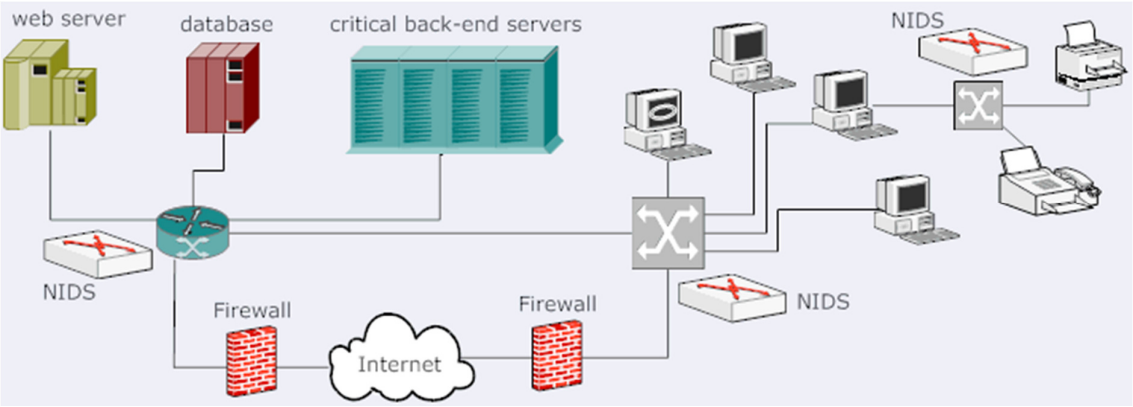


Figure 2 shows the operation of NIDS

Source: https://www.cse.wustl.edu/~jain/cse571-07/ftp/ids/fig2.gif

2 Wireless ID

Wireless native space Network (WLN) IDS is comparable to NIDS in this it will analyse network traffic. However, it will analyse wireless-specific traffic, together with scallywag APs, users outside the company's physical realm, and WLN IDs engineered into the AP, attempting to attach external users to purpose access points (APs). because the network progressively supports wireless technologies at varied points within the topology, WLN IDS can play a significant role in security. several previous NIDS tools can embody enhancements to support wireless traffic analysis.

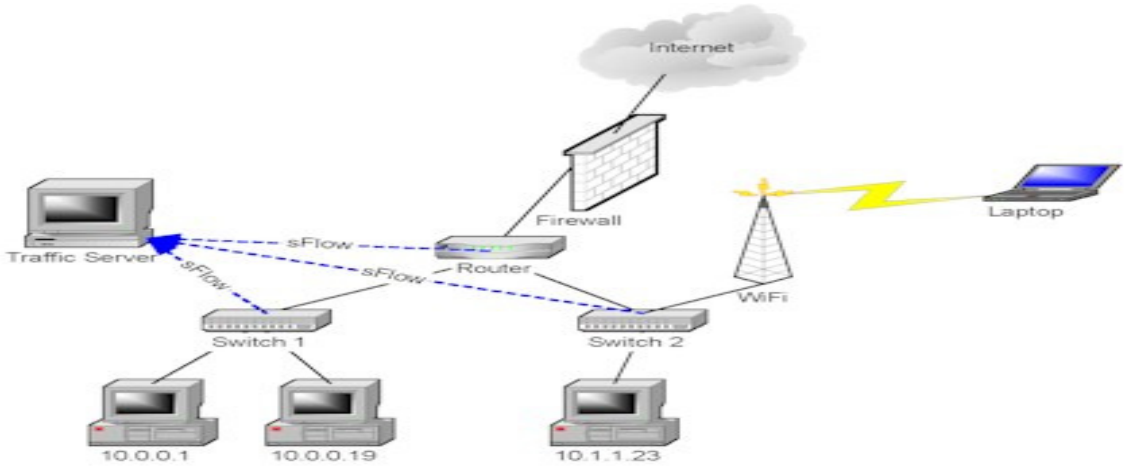


Figure 3: Wireless Ids

Source: https://inmon.com/img/tutorials/ids_map.jpg

3 Abnormal investigation of network behaviour

The Network Behaviour Incompatibility Check (NBAD) appearance at traffic on network segments to work out if inconsistencies exist within the quantity or sort of traffic. Segments that sometimes see little or no traffic or simply segments that see a selected sort of traffic will amendment the quantity or sort of traffic if an unforeseen event happens. NBAD needs several sensors to make a decent pic of the network and benchmarking and base lining to work out the nominal quantity of section traffic.

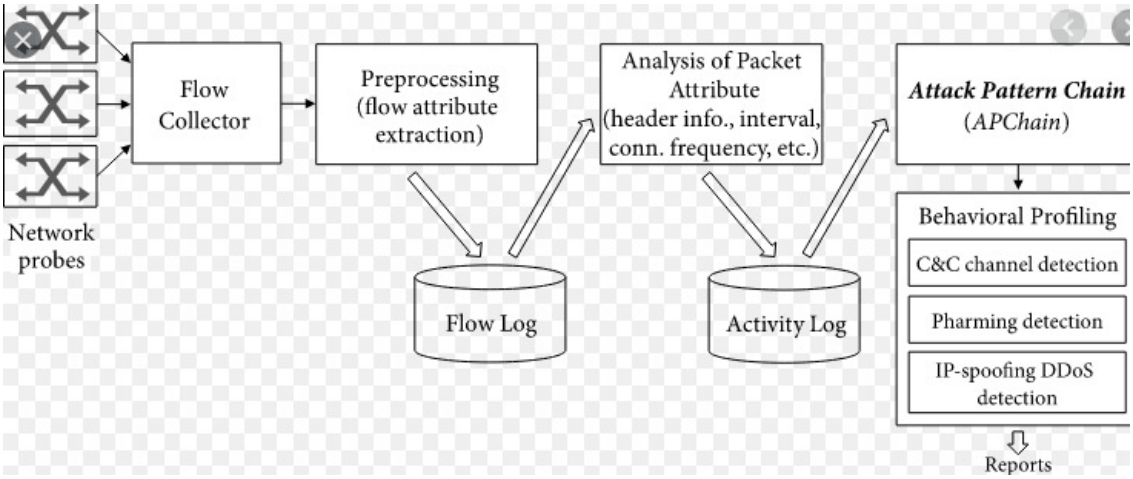


Figure 4: Abnormal investigation of network behaviour

Source:https://static-01.hindawi.com/articles/scn/volume-2018/9706706/figures/9706706.fig.001.svgz

4 Host primarily based ID

In host-based IDS (HIDS) technology, computer code computer code agents square measure put in on every laptop host within the network to watch what's happening within that host. HIDS analyses network traffic and system-specific settings like computer code computer code calls, native security policy, native work, its dates and additional. It provides log analysis, file integrity verification, policy watching, rootkit detection, period of time alerts and active feedback. HIDS is typically deployed on complicated hosts like publically accessible servers and sensitive info servers.

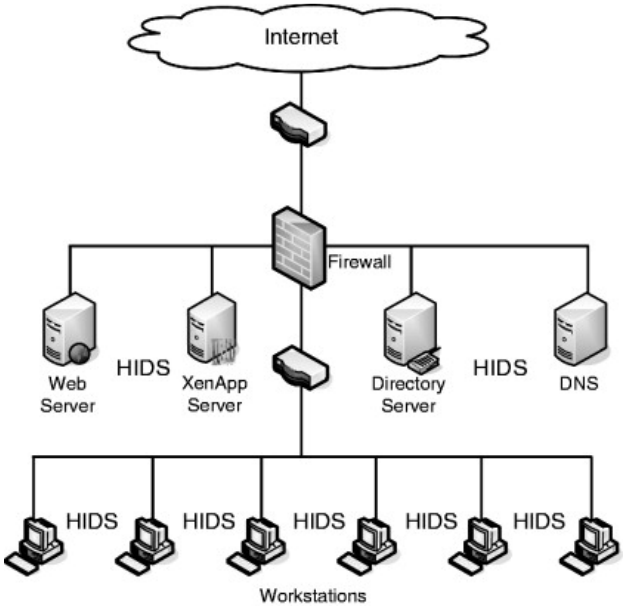


Figure 5: Host primarily based ID

Source: https://ars.els-cdn.com/content/image/3-s2.0-B978159749281200007X-gr3.jpg

HIDS eliminates difficulties with network-based IDS technology for securing individual hosts in a very network. However, they cause vital overhead for the hosts World Health Organization run them.

INTRUSION PREVENTION SYSTEM

The Intrusion Prevention System (IPS) is the process of conducting responsive actions on intrusion activities or threats and intruders and threats detected in both networks. The IPS is monitoring real-time packet traffic with malicious activities or that matches specific profiles and will stimulate the creation of alerts and can block real-time traffic in the network. Primarily IPS countermeasures are to prevent attacks in progress.

IPS can be said to be an extension of IDS with access control exercises to prevent exploitation of computers. IPS is an intelligent device capable of performing preventive actions not only to detect malicious activities, but also to protect the host or network.

Simply put, IDS may be appropriate for network attack monitoring and for alerting administrators of the danger of mer. But its speed, performance and passive limitations have paved the way for IPS to challenge it as an active defense weapon of choice.

The main functions performed by IPS are as follows.

1. IPS detects and takes preventive action against malicious attacks

2. IPS only prevents attack
3. IPS changes the security environment
4. Modifies IPS attack content

IDS vs. IPS

Deciding between an intrusion detection system (IDS) and an intrusion prevention system (IPS) is a particularly challenging and time consuming task for most security practitioners. Both systems offer the same benefits and the markets are occupied by the same vendors.

IPS is better than firewall. There are firewalls and IPS control devices. They sit in a line between two networks and control the traffic passing through them. But the basic difference between firewalls and IPS is that they handle network traffic. While a firewall denies all requests that do not meet its security definition, IPS accepts all requests except those whose content appears to be malicious and dangerous to the system.

On the other hand, if IPS is a control tool, then IDS is a visibility tool. Intrusion detection systems sit on the side of the network, monitor traffic at many different points, and provide visibility to the network's security posture. Comparing IDS with Protocol Analyser is a good analogy. A protocol analyser is a tool that a network engineer uses to see the deep inside of a network and see what's happening, sometimes in exciting details. The ID for a security engineer is a "protocol analysers". IDS looks at the depth of the network and what is happening from a security standpoint.

From their definitions alone, we can infer that the IPS starts working from where the IDS closes. IDS can not only detect an error, but IPS can detect it and fix the problem.

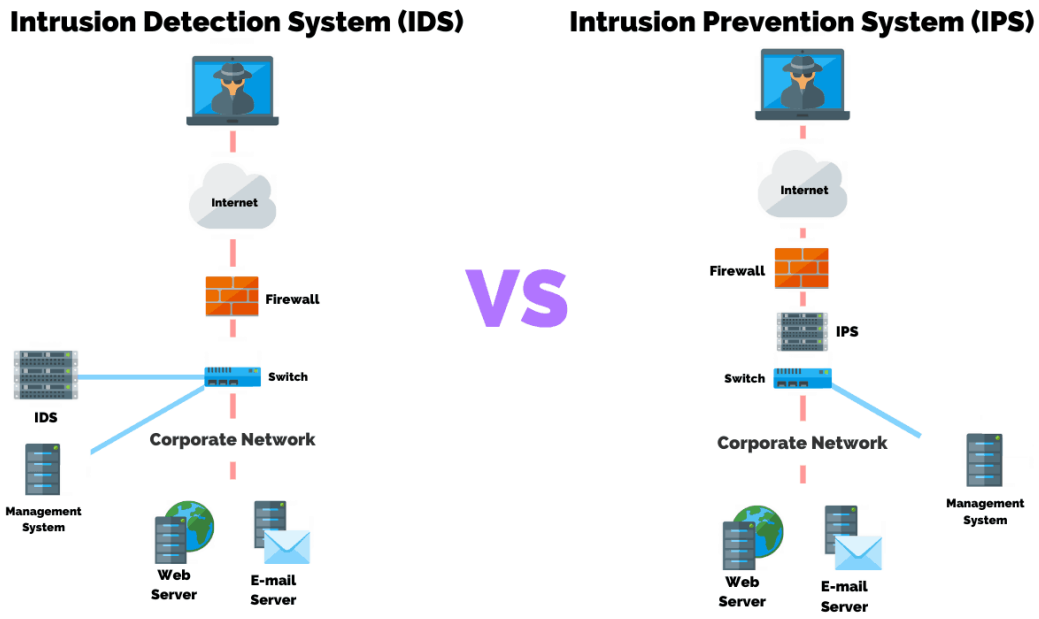


Figure 6: IDS vs. IPS

Source:https://purplesec.us/wp-content/uploads/2019/11/Intrusion-Detection-IDS-VS-Intrusion-Prevention-IPS-What%E2%80%99s-The-Difference.png

Conclusion

There is square measure several technologies on the market these days to assist firms fight inevitable network and system attacks. IPS and IDS. Having techno several is simply two of the various resources that may be deployed to extend visibility and management in an exceedingly company computing surroundings. IDS and IPS aim to supply a foundation of technology that meets pursuit needs, distinguishing network attacks that may be detected by logs of IDS systems and preventing action by IPS systems. If the host is with essential systems, intelligence and strict compliance rules, then it's far better to use IDS, IPS or each within the network surroundings.

REFERENCES

1. J.P. Anderson, Computer Security Threat Monitoring and Surveillance, tech. report; James P. Anderson Co., FortWashington, Pa., 1980.
2. D.E. Denning, “An Intrusion Detection Model,” IEEE Trans. Software Eng., Vol. SE- 13, No. 2, Feb. 1987, pp.222–232.
3. E. Amoroso and R. Kwapniewski, “A Selection Criteria for Intrusion Detection Systems,” Proc. 14th Ann.Computer Security Applications Conf., IEEE Computer

Soc. Press, Los Alamitos, Calif., 1998, pp. 280–288.

4. J. Allen et al., State of the Practice of Intrusion Detection Technologies, Tech Report CMU/ SEI-99-TR-028, Carnegie Mellon Univ., Software Engineering Inst., Pittsburgh, 2000
5. Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth, SANS Institute, 2004.
6. Karen Scarfone , Peter Mell, " Guide to Intrusion Detection and Prevention Systems (IDPS)", National Instituteof Standards and Technology,2007.
7. Debar, H., An Introduction to Intrusion Detection Systems, IBM Research, Zurich Research Laboratory
8. Kent, Karen & Warnock, Matthew (2004). Intrusion Detection Tools Report, 4th Edition.
9. Herndon, VA:Information Assurance Technology Analysis Center (IATAC).
10. Jennifer Jabbusch , "IDS vs. IPS: How to know when you need the technology", 22 November 2010
11. Pete Lindstrom, "Intrusion prevention systems (IPS): Next generation firewalls", A Spire Research Report –March 2004 by, Spire Security
12. Paul Helman, Gunar Liepins, and Wynette Richards; Foundations of intrusion detection, in Proceedings of the Fifth Computer Security Foundations Workshop, Franconic, NH, June 1992
13. Teresa Lunt and R. Jagannathan; A prototype real-time intrusion-detection expert system; in Proceedings of the 1988 Symposium on Security and Privacy, Oakland, CA, April 1988
14. Jan Vykopal, "Security Analysis of a Computer Network", Masaryk University Brno, master thesis, 2008.
15. B. Mukherjee, L.T. Heberlein, and K.N. Levitt, "Network Intrusion Detection," IEEE Network, Vol.8, No. 3,May-June 1994
16. Charlie Kaufman, Radia Perlmon and Mike Speciner; Network Security; Private
17. Communication in a PublicWorld, 2nd Edition, Prentice Hall of India
18. William Stallings, Cryptography and Network Security: Principles and Practices, Pearson Education, 4thEdition, 2011.
19. https://supportforums.cisco.com/community/netpro/security/intrusion-prevention

20. http://www.cisco.com/en/US/products/ps5729/Products_Sub_Category_Home.html
21. http://www.windowsecurity.com/articles/intrusion-detection-systems-faq.html
22. www.networkworld.com/topics/ids-ips.html
23. http://www.pcsecurityworld.com/79/intrusion-detection-systems-for-enterprise-security.html
24. http://www.gslis.utexas.edu/~netsec/ids.htm
25. http://www.airtightnetworks.com/home/solutions/wireless-intrusion-prevention.html