iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4720

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Intrusion Detection and Prevention in IP Based Mobile Network

Manpreet Kaur[1]
[1]*M Tech, Tanita University, Sri Ganganagar*

***Abstract:** This paper presents intrusion detection system (IDS), based on mobile Network, that detects intrusion from outside the network segment as well as from inside. Mobile Companies believes that greater end user knowledge and the possible use of public networks for transportation of telephone traffic will increase threats against telephone networks. The proposed model comprises three major components: The Network Intrusion Detection Component (snort and juniper tool), the Mobile Agent Platform, and sniffer residing on every device in the network segment. The purpose of this paper is to investigate the needs for an Intrusion Prevention System (IPS). It finds existing security features in mobile Companies. It Conclude requirements for an IPS intended for use in Mobile Company's PRAN environment. Analysis is performed to ident if assets in and threats against RAN and to discover Attacks that can be mitigated using an Intrusion Prevention System. The precautions will help researchers to test the measurements efficiently and the list of simulators will guide them to select one according to their needs.*
***Keywords:** Internet protocol, Intrusion detection system, IPS, TCP*

I. INTRODUCTION

IP reduces the need for network lines because it is connection less communication protocol, so it does not communication line between two computers for connect to each other. Information send through packets for communication in two computers. Packet contains information which send to receiver by user, receiver id (receiver IP address) and more. For the mobile telephone alone, it has over 3.2 billion subscribers around the world (GSM Association, 2008). Indeed, many developed countries are experiencing well more than 100% market penetration (ITU, 2007). The modern mobile device can provide a wide range of services over several network connections and is able to store a broad range of information from business to personal data. As a result, many people rely on those services and information to complete their business and personal tasks. Such tasks can include email accessing via wireless network, online shopping through the 3G network, sharing pictures over the Bluetooth connection, and reading word documents. However, those activities can contain sensitive data related to the business and personal private information. The mobile device and mobile network faces several security threats. However, the amount of mobile IDS research is significantly smaller compared to other mobile security projects. Moreover, those existing mobile IDSs were designed to detect the individual security threats: telephony based mobile IDSs only detect telephony service fraud; battery based mobile IDSs only detect battery attacks [5]. Therefore, none of these mobile IDSs can offer the comprehensive detection for the services running on the modern mobile devices. Mobile Company is currently developing a reference solution for an IP network between the Radio Base Station (RBS) and the mobile backbone network. This reference solution comprises what hardware and Software to use, where to place the equipment and how to configure it. The equipment investigated study in this paper will mainly involve those parts that face to the private or semi-public network used as transport medium between the RBS and the backbone network. The analysis of the equipment will focus on finding IPS mechanisms that can be used to protect and detect intrusion attempts against devices used in the PRAN solution. Risk analysis will be performed to rank identified threats in order of loss of assets that a successful attack could result in to the customer and Mobile Company [6]. The paper describes a research programme underway to design, develop and evaluate a novel mobile IDS. The paper then proceeds to present some initial experimental results and concludes with highlighting the future work.

II. INTRUSION DETECTION AND PREVENTION SYSTEM

This paper introduces different types of IPS systems, how they work and what type of attacks they can counter. IPS is an extension of the more commonly used abbreviation IDS (Intrusion Detection System). As there is no proper definition for these abbreviations this paper will use IPS to denote a system that includes both the detection and prevention functionality. Intrusion Detection is the art of detecting inappropriate or suspicious activity against computer or networks systems. Today, it is difficult to maintain computer systems or networks devices up to date, numerous breaches are published each day [8]. IDS monitor the usage of such

systems and detect the apparition of insecure states. This insecure state can be either an attempt from internal users to abuse their privileges or outside users (attackers) to exploit security vulnerabilities.

A. *Host Based IPS*

A Host IPS (HIPS) is usually implemented as a background process which examines logs and system behaviour. It may intercept system calls to the kernel as well as calls to dynamically linked libraries and inspect them for suspicious data or behaviour. A HIPS can also be implemented directly in the IP stack. This makes it possible to examine network packets in any of the TCP/IP layers and take preventive actions before a malicious packet is forwarded to the receiving application.

B. *Network IPS*

Network IPS (NIPS) is a device connected to the network it is supposed to monitor. It can be a regular PC equipped with IPS software (e.g. Snort), or a dedicated IPS device. Network IPSs can be connected to the network in a variety of different ways depending on the type of network it is deployed in and what functionality it is supposed to deliver. It can be installed as a passive detection system; in this case it can be connected to a mirror port on the switch that the nodes on the network are connected to. A mirror port works by copying traffic from one or several ports to another port that works as the mirror port. An IPS can also be installed using a network tap connected on the cable connecting an unsecure network with a secure one. Network taps are often unidirectional and an IPS connected this way can thus only passively monitor the network and not take any preventive measures. The passive IPS seldom has an IP address assigned to it, and hence all analysis is made in raw network format. This makes it harder to exploit vulnerabilities that might reside in the IPS operating system [9]. The IPS software itself on the other hand might have vulnerabilities that can be exploited in it.

C. *Detection Techniques*

There are two types of IPS detection engines; misuse detection and anomaly detection. The misuse detecting IPS search for attack signatures patterns within the network traffic or log files that indicate suspicious behaviour. The signature of an attack might be an unusual high number of failed log-ins for a specific account or an IP packet containing a certain payload. An anomaly on the other hand does not necessarily constitute an intrusion and the absence of anomalies does not automatically imply the absence of intrusions. For example, an administrator who forgot his password might trigger an anomaly alarm if he does too many login attempts, thus generating a false positive. Anomaly detecting IPSs that continuously update their normality baseline might also be vulnerable to patient attackers who can gradually change the baseline to make malicious traffic part of the normal behaviour – resulting in false negatives. There are also anomalies detecting IPSs that do not use statistical techniques to detect malicious traffic. These systems can for example detect anomalies within a protocol that it examines. A protocol anomaly might for example be a TCP packet with both the SYN and RST flags set, which is an abnormal behaviour according to the TCP RFC specification. IPSs which utilize anomaly detection have greater potential to withstand future demands as signature detecting IPSs databases will grow and lack the ability to detect yet unknown attacks. Because IPSs are a rather new type of system, most of today's commercial products implement the misuse detecting paradigm.

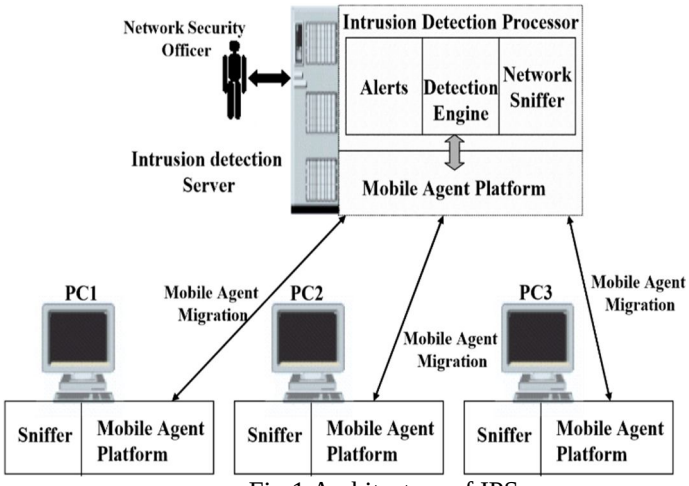


Fig.1 Architecture of IPS

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

III. SYSTEM ARCHITECTURE

This section presents the architecture of our IDPS. The architecture is made up of the following components: (1) an intrusion detection processor, (2) a mobile agent platform, and (3) sniffer.

A. Intrusion Detection Processor

It is responsible for monitoring network segments (subnets), and acts as a central intrusion detection and agent data processing unit. The unit is placed on a strategic node to monitor network traffic for all devices on the segment[4]. Furthermore, it is setup to send real-time alerts that are generated using rule-sets to check for errant packets entering the segment. It has three main capabilities: packet sensing, packet logging, and intrusion detection. Every now and then, log files are sent to the central intrusion processing unit (via mobile network) for packet decoding and processing. The IDP monitors agent's movement in the network and guides them towards critical locations in the network if malicious activities were detected. To guarantee proper interaction with mobile agents, the IDP should exchange data and messages with the mobile agent platform.

B. Mobile Agent Platform

A mobile agent platform (MAP) can create, interpret, execute, transfer, and terminate (kill) mobile agent on mobile network. The platform is responsible for accepting requests made by mobile network users and generating mobile agents plus sending them into the mobile network to handle the tasks (in our case to start sniffing activities within the local network, stop it when necessary, and send the collected data back to the IDP for further analysis).

C. Sniffer

A sniffer is a device used to tap into networks to allow an application or hardware device to eavesdrop on network traffic. The traffic can be IP, IPX, or AppleTalk network packets. In general, sniffing is used for: (1) Network analysis and troubleshooting, (2) performance analysis and benchmarking or, (3) eavesdropping for clear-text passwords and other interesting tid bits of data. Depending on the IDP's instructions, the agent may run the sniffer for a predetermined period, collect the data, and send it in one batch to the IDP. Alternatively, it may run the sniffer and send data as it is captured to the IDP until it receives instructions to stop sniffing.

D. Working

When the system is initially started, the IDP starts its own sniffer and sends a 'START' request to the MAP. The message specifies the number of agents to be launched and the corresponding IP address sets that each agent is expected to visit. This implies that the IDP has a registry containing all IP addresses in the local network. The MAP, in turn, creates the agents and dispatches them into the network. Now assume that an agent on its trip sends a report to the IDP that triggered an alarm. The IDP will send a 'LUDGE' message to the agent causing it to reactivate the sniffer at its current location and stay there, to gather more evidences on the current attack to study the behaviour. The IDP will prompt the MAP to create a new agent that will take over the agent's task. In this scenario, the number of active sniffers may increase to form an alert stage for faster reaction.

IV. IMPLEMENTATION

A. IDS Prototype

In this paper IDS has been implemented on top of Snort tool [13] and a mobile agent system that was created locally. Snort is a full-fledged opensource network-based IDS (NIDS) that has many capabilities such as packet sniffing, packet logging and intrusion detection [15]. A rule is a set of requirements that will trigger an alert.

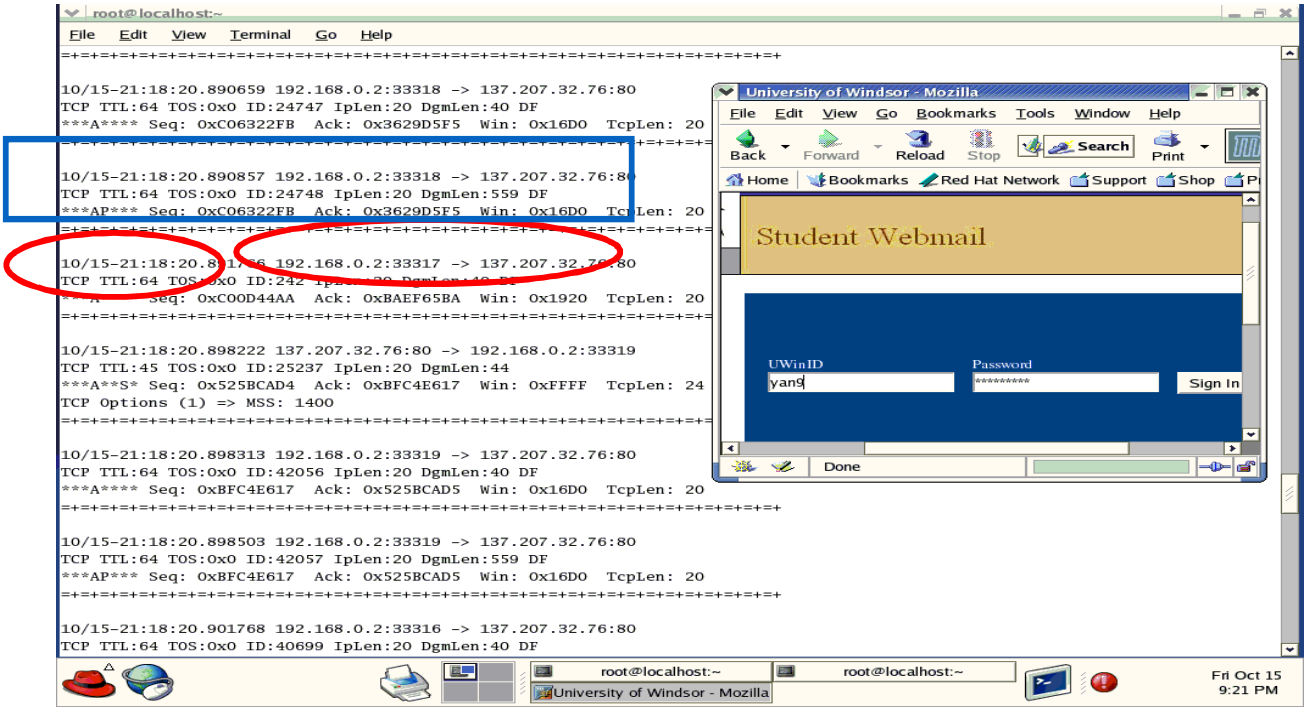


Fig. 2 Webmail packet detect using snort tool

Snort-based IDS contains the following components

1) *Packet Decoder* -It takes packet from different network interface, send to preprocessors and detection engine.
2) *Preprocessors*-it can rearrange the string so that it detectable by detection engine, it can also reassemble small unit of information and send the whole packet for signature test.

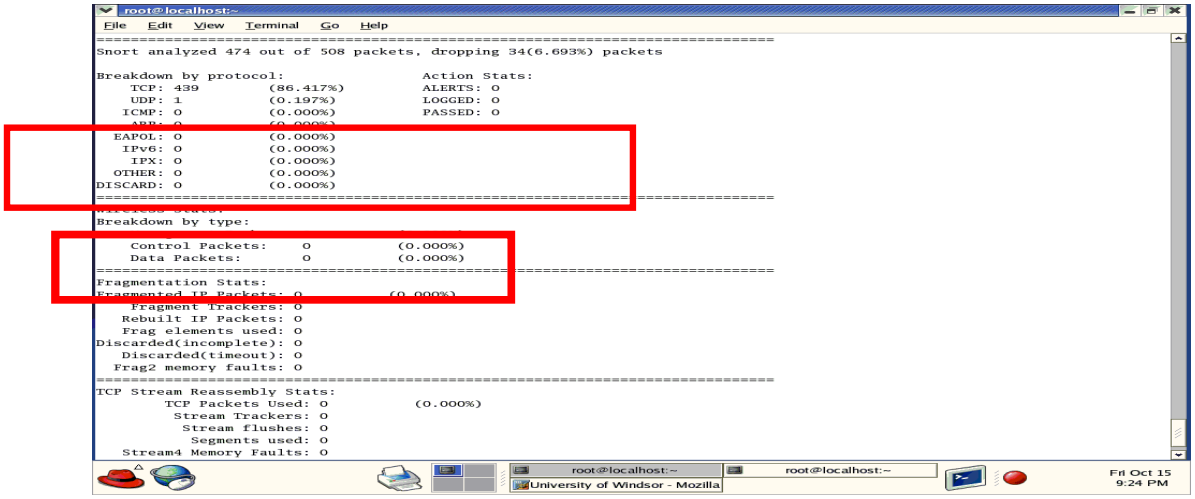


Fig.3 Result of Packet scanning and broke down in Fragmentation

3) *Detection Engine*- It is responsible for scan the packets of information.it can dissert a packet and apply rule on them.
4) *Logging and Alerting System*- The captured packet may be used to log the activity or generate an alert. 1.Logs are kept in 2. Simple text files 3. tcpdump-style files and some other form log files are stored under /var/log/snort folder by default.
5) *Modules*- Depending on the configuration, output modules can do things like the following:1. Simply logging to /var/log/snort/alerts file 2. Sending SNMP traps 3. Sending messages to syslog facility 4. Logging to a database like MySQL or Oracle. 5.Generating XML output 6. Modifying configuration on routers and firewalls.

B. *Juniper IDP*

it is an intrusion prevention system for IP based networks. Juniper IDP is shipped with a database containing attack signatures for over 50 protocols, with a total amount of over 5000 signatures. Of these 50 protocols only 6 protocols are of interest for the PRAN solution, these are presented in Table 4 below. IDP offers the ability to create customized signatures through their management system NetScreen Security Manager (NSM). This makes it possible to write new signatures. IDP also offers protocol conformance check for the network, transport and application layer to detect / prevent suspicious traffic. The device supports high availability features using NSRP, which is Juniper's enhanced proprietary version of the VRRP protocol. It supports several features for centralized logging, i.e. syslog and SNMP. It can reassemble packets before forwarding them to detect attacks that are fragmented. If configured, the IDP can record packets preceding as well as succeeding a detected attack, which is useful for traceability when trying to filter out false positives,

C. *Mobile Platform*

MORPHEOUS [16] is a prototypical mobile agent system that was developed as a final year project at the American University of Beirut. The system was chosen as the mobile agent platform because of its availability (including C# source code), ease of running, and support for mobile agents. It consists of four entities: the agent factory (AF), the listeners, the officer agents (OA), and the soldier agents (SA). The core of the agent system is the agent factory. It accepts requests made by the network users (in our case the Snort requests), generates the mobile agents and sends them to the network to handle tasks.

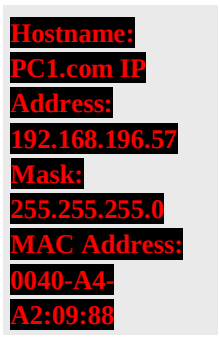
D. *Sniffer*

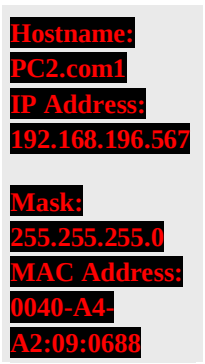
WinDump [17] is the porting to the Windows platform of TcpDump that runs on all the operating systems supported by WinPcap, i.e. Windows 95, 98, ME, NT4, 2000 and XP. It was selected in the prototype because of its lightweight, popularity, support of multiple operating system, and ability to dynamically reconfigure its execution state.

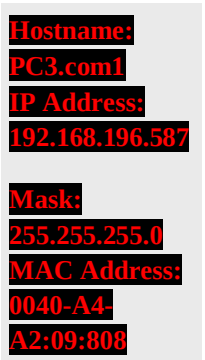
V. DISCUSSION OF RESULT WITH EXAMPLE

We present the prototype network that we used to proof-concept our work. The network comprises a Linux server and two Windows hosts. Network credentials about the four computers are shown in the figure. The system is configured as follows: The Linux box is set as the intrusion detection processor where Snort is installed and is running in addition to the mobile agent platform. The other two Personal Computers have WinDump installed on each as well as the mobile agent platform.

When the system starts up, Snort sends MORPHEOUS an HTTP request to start sniffing and provides it with the IP addresses (192.168.196.0 class) of computer1(198.168.196.57 and host name-PC1.com) and Computer2(198.168.196.567 and host name-PC2.com). MORPHEOUS creates an agent, assigns to it the task of starting and stopping WinDump and then dispatches it into the network. The MAP listens to Snort at a specific IP address and port number. When a request is sent, the MAP checks for the type of the message (START, PROCEED, or LODGE). A summary of possible message exchanges between Snort, MAP, and the agent are detailed in Table 1. Using several experiments, the overall trip of the agent took roughly 3.42 sec (aprrox 3 sec are for activating the sniffers and 0.42 sec for agent migrations, messaging between the components, and processing activities).







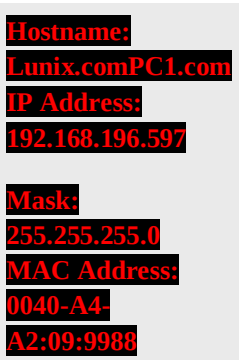


Fig.4 A Practical example to test IDP using snort tool

VI. ANALYSIS

A. *Risk Analysis*

The risk model used in this paper is qualitative. Risks are classified based on impact (Consequence) and probability of threat materialization. The risk is calculated using the formula:

Risk = Impact * Probability

This is quite different from the model described in the theory section with the greatest difference being that the value of the asset is not explicitly used in the formula.

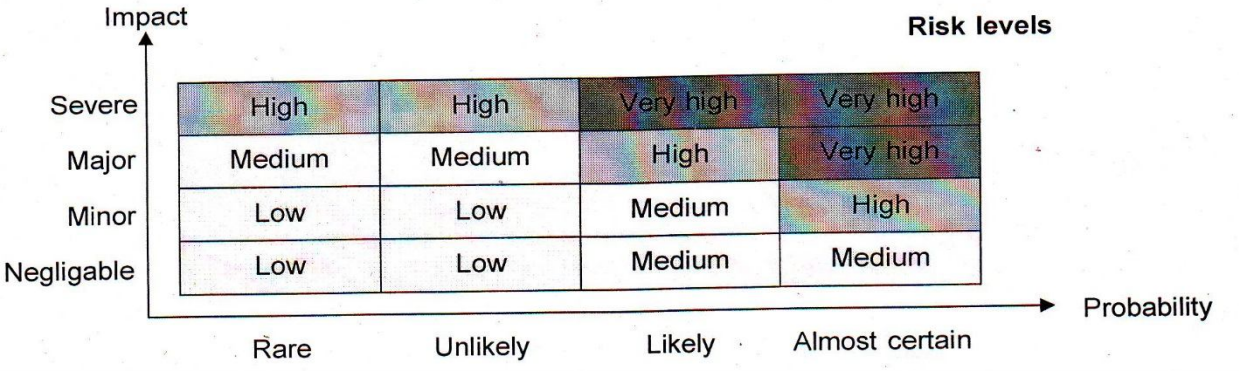


Fig.5 Risk Analysis Chart

B. *Security Analysis*

In this paper purposed intrusion and detection system reduce risk of attack performed on protocol of network. we calculated a picturization result for understand the accuracy of this system**.**

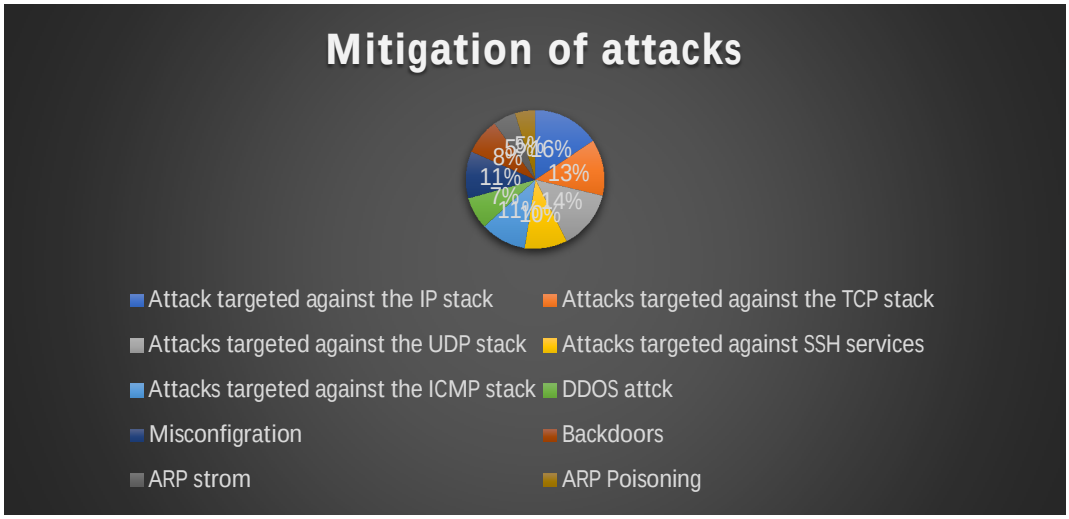


Fig.6 A ration of mitigation of attack by purposed system

C. Testing

Testing is achieved by simulating different measurements**.** Simulators are the most common tools used for testing the IDS. Therefore, we add some precautions for choosing a simulator and a list of available simulators. The precautions will help researchers to test the measurements efficiently and the list of simulators will guide them to select one according to their needs. Simulation is an often-used tool to test and analyse MANET, according to the survey done in [12]. In this paper the list of simulators will guide them to select one according to their needs Moreover, they conclude that the most used simulator is Network Simulator version(NS-2).

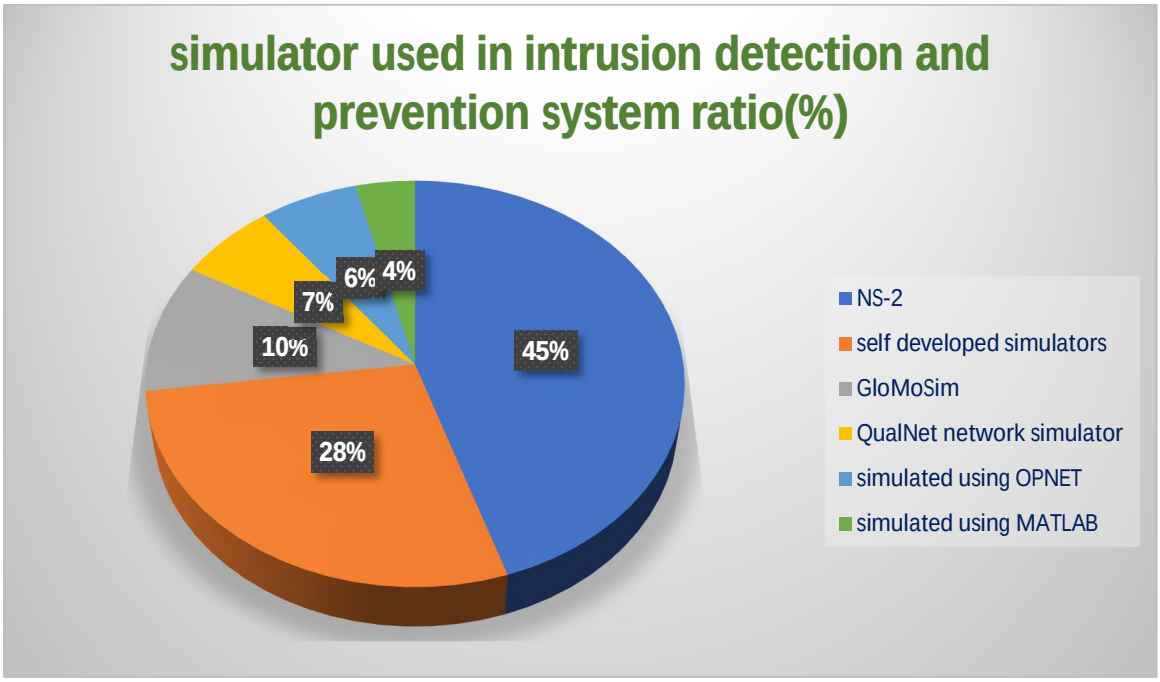


Fig.7 Ratio of used simulators

VII. CONCLUSIONS

Inspired from real life where policemen roam city streets looking for dangerous people and when they suspect something, they watch and follow more closely. we discussed an architecture for Intrusion Detection and prevention System based on mobile Network. In this paper we also discussed simulator ratio (%) for testing of purposed IPS. We conclude a survey of Intrusion Detection and prevention System to mitigated attacks performed on different protocols. In future this purposed system prototype should be implement in mobile company and its practical approach should be improved to reduce the risk of many attacks which performed by intrusion.

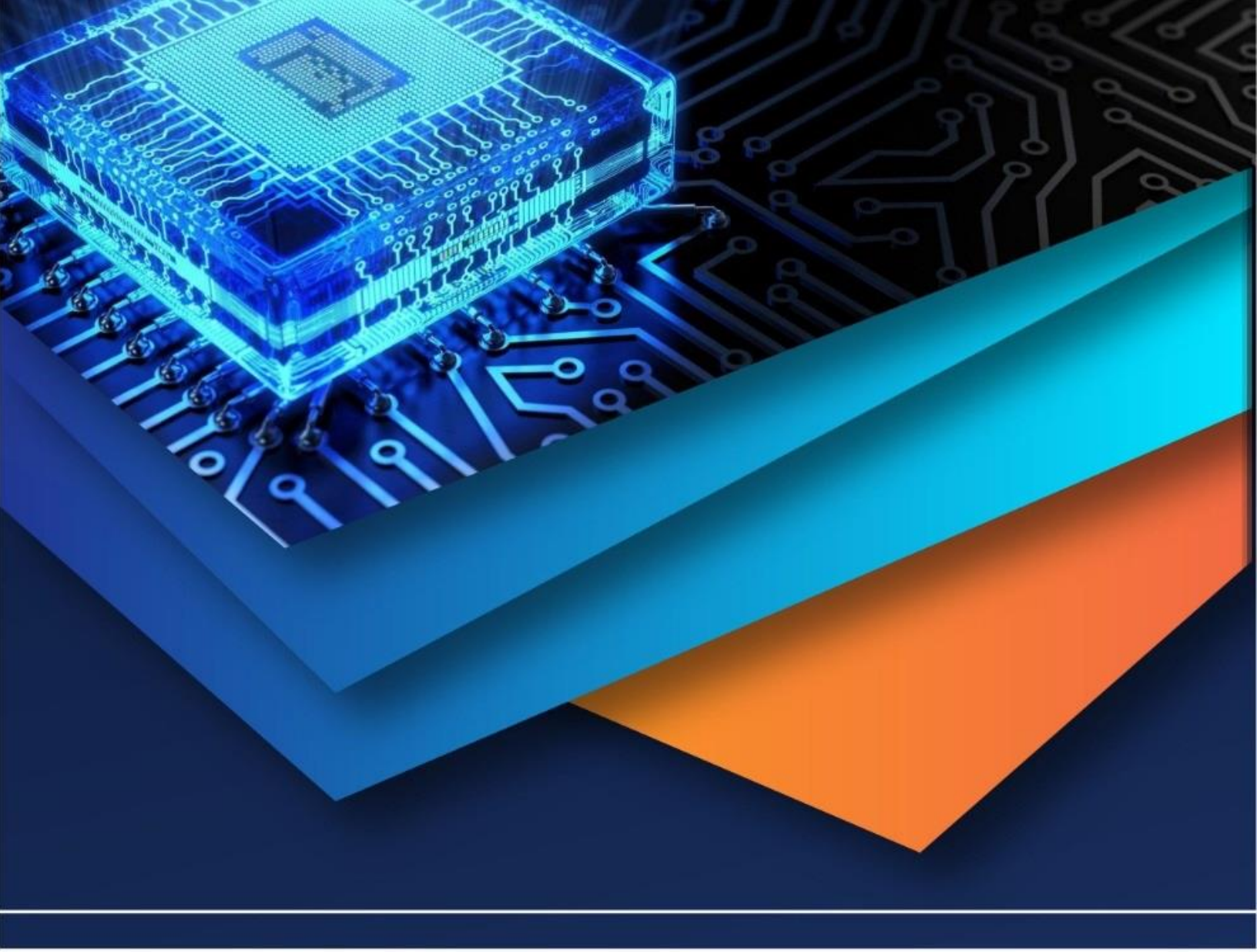
REFERENCES

[1] Gollmann, Dieter (2006). Computer Security, 2nd edition. John Wiley & Sons, Ltd. ISBN 0-470-86293-9.
[2] http://netsecurity.about.com/od/intrusiondetectionid1/a/aafreeids.htm.
[3] Scut (Sep 1, 2001). Exploiting Format String Vulnerabilities. URL: http://julianor.tripod.com/bc/formatstring-1.2.pdf
[4] IETF RADIUS Working Group. Remote Authentication Dial In User Service (RADIUS).RFC 2138.
[5] IETF Network Working Group. Diameter Base Protocol. RFC 3588.
[6] Aboba, B. et al (Nov, 2000). Criteria for Evaluating AAA Protocols for Network Access.URL: http://www.ietf.org/rfc/rfc2989.txt.
[7] Tony Bautts (Aug 21, 2003). Slow Down Internet Worms with Tarpits. URL: http://www.securityfocus.com/infocus/1723 (2008-01-31).
[8] Vaughn, R. and Evron, G. (Mar 17, 2006). DNS Amplification Attacks. URL: http://www.isotf.org/news/DNS-Amplification-Attacks.pdf.
[9] IEEE 802.3 Ethernet Working Group. URL: http://grouper.ieee.org/groups/802/3/
[10] Mohan, R. (May 1, 2006). Amplified DNS Distributed Denial of Service Attacks and Mitigation. URL: http://www.cert-in.org.in/training/1stmay06/dotIN-DNS-DDoS.pdf
[11] Honeynet Project (Apr 26, 2001). Know your enemy: Honeynets. URL: http://www.securityfocus.com/infocus/1209
[12] Insecure.org. Port scanning techniques. URL: http://nmap.org/man/man-port-scanning-techniques.html (2008-02-01).
[13] . Laing, B and Alderson, J (2000). Internet Security Systems: How to implement a network-based intrusion detection system. URL: http://www.snort.org/docs/iss-placement.pdf (2008-02-04)
[14] Snort – the de facto standard for intrusion detection / prevention. URL: http://www.snort.org (2008-02-04).

[15] Stein, G. et al (2005). Decision tree classifier for network intrusion detection with GA- based feature selection. Proceedings of the 43rd annual Southeast regional conference - Volume 2. ISBN 1-59593-059-0.

[16] Soule, A. et al (2005). Combining filtering and statistical methods for anomaly detection. Proceedings of the 5th ACM SIGCOMM conference on Internet measurement. ArticleNo.31.

[17] Shyu, M-L. et al (2007). Network intrusion detection through Adaptive Sub-Eigenspace Modeling in multiagent systems. ISSN 1556-4665.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY