THE SURVEILLANCE OF INTRUSION DETECTION SYSTEMS AND APPROACHES

Dr.S.Satheesbabu[1], Dr.P.Gokulakrishnan[2], Dr.N.Dhanalakshmi[3]
[1] Associate Professor, PSNA College of Engineering and Technology, Dindigul, India
[2] Professor, PSNA College of Engineering and Technology, Dindigul, India
[3] Professor, PSNA College of Engineering and Technology, Dindigul, India
suresh@psnacet.edu.in

Abstract

With the widespread evolution of new technologies and services, Internet has experienced explosive growth across the market that actively increases the impact of attacks where the attackers continuously find vulnerabilities and attack the system In an information system, intrusions are the activities that violate the security policy of the system. At this instant, it is fundamental to impenetrable the pc gadget which has end up the important problem over the few years so as to observe and forestall attacks. Intrusion detection is a necessary device to display networks for attacks or intrusions and document these intrusions in order to take an action. While Intrusion detection structures are ubiquitous defenses in current networks, there is no rigorous methodology to measure or enhance the effectiveness of the system. This paper is aimed to facilitate the extraordinary kinds of Intrusion detection systems, merits, demerits and the overall performance measurements that are desired. To determine these metrics, we evaluate previous empirical evaluations. We additionally existing the set of hurdles that have blocked the measurements and lookup associated in the direction of enhancing dimension competencies has been supplied.

Keywords: Intrusion Detection, false alarm, traffic

1. Introduction

In the present communication scenario, internet becomes the essential part for every human to complete their daily work routines. Network security is the necessary requirement of our community to tightly closed the private statistics saved in the networks. However, this treasured facts attracts the interest of attackers. In an facts system, intrusions are the things to do that violate the safety coverage of the gadget and intrusion detection is the technique used to perceive intrusions. Within few years,

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

Intrusion detection gadget science has grown extensively and IDS are the trendy tools for securing the giant networks.

For any organization's safety framework, Intrusion detection gadget performs the principal role. Usually, Intrusion detection structures (IDSs) are deployed alongside with preventive safety mechanisms, such as get admission to manage and authentication, as a 2d line of protection that protects records systems. Intrusion detection presents a way to become aware of and hence enable responses to, assaults towards these systems. Security equipment such as anti-virus software, firewalls, packet sniffers and get right of entry to manipulate lists resource in stopping attackers from gaining convenient get admission to to an organization's structures however they are in no way foolproof. An intrusion is described as any set of moves that try to compromise the integrity, confidentiality, or availability of a useful resource [1, 2]

Intrusion should be in many types such as:

- Unauthorized personnel making an attempt to reap get right of entry to to the sources in a device or network.
- Malicious packages that break the device resources, degrades the machine overall performance and manipulates the machine data.
- Authorized personnel making an attempt to acquire extra privileges or get right of entry to to exclusive information, therefore compromising the system's protection policy.

IDS screen all the gadget things to do in order to notice the Intrusion. It searches for protection violation incidents, acknowledges unauthorized accesses, identifies data leakages and intervention of malicious programs. Intrusion might also appear due to machine vulnerabilities or protection bleaches, such as device mis-configuration, person misuse, or software defects [3]. Especially, Intrusion detection is essential in a giant community machine whilst massive quantity of servers and online offerings going for walks in the system.

To perceive intrusions and protection threat, more than a few laptop assaults should be completely studied. Typical hacking techniques are categorized into 5 steps: (1) Information Gathering: The attacker collects the data of the device via the usage of question equipment like nslookup, whois etc., to discover IP addresses, area identify etc., on a goal (2) Probe/Scan

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

vulnerabilities: Using the gathered information, an attacker finds the achievable vulnerabilities in the goal machine thro scanning & gathers the specified data about the community such as variations of the services, community topology, ports used, feasible vulnerabilities and firewall rules. (3) Access gaining: Based on the person legitimacy, there are two approaches to acquire the get entry to to the goal system. An licensed consumer exploits the loop holes in the working device however an illegitimate person will makes use of current community to attach the goal system. For Example: An attacker can attain the get admission to with the aid of R2L (Remote to Local) assault like password guessing, community sniffing, buffer overflow attack,etc. An R2L assault ability an illegitimate consumer tries to reap the get right of entry to to execute command on a target. These assaults normally make the most application flaws, machine misconfiguration, password guessing, or malicious packets, to attain the get right of entry to (4) Escalate Privileges: An illegitimate consumer will reap the get right of entry to to the goal gadget and tries to extract the wished facts from the system [24 and 25]. For Example: An attacker can achieve the get right of entry to by way of U2R (User to Remote) assault the use of gadget vulnerability. A U2R assault is an assault the place an consumer may additionally be an attacker the use of compromised person account, exploits a software program flaw so that it lets in the attacker execute privileged instructions as a root. (5) Launch Planned attack: To hold the non-stop manage over the goal system, an illegitimate consumer will steal or regulate the private or treasured statistics as a stepping stone for future attacks.

2. Intrusion Detection Systems

Intrusion detection gadget (IDS) is a system or [software application] that video display units community and/or machine things to do for malicious things to do or coverage violations and produces reviews to a Management Station [4]. Architecturally, IDS can be labeled into three types: Host primarily based IDS, community based totally IDS and Distributed IDS in accordance to the sources of audit statistics used through every IDS. The host based totally IDS is hooked up on every host the place it receives its audit facts from host audit trails and targets at detecting assaults in opposition to a single host. Its fundamental job is to display the facts that flows to a pc with the aid of accumulating the data that goes via and analyze it. NIDS is extra low cost that collects the packets that float thru the community to the distinctive hosts of the network, then analyzes all the amassed records and sends the end result to a central system, in order to become aware of a feasible attack. This is carried out with the assist of unique sensors that are locations in quite a number factors of the network. DIDS

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

accumulate the audit records from the a couple of hosts aiming at detecting assaults involving a couple of hosts [3, 4].

Recognition of break-ins is achieved both manually or the usage of software program structures that function on logs on the network. When working on intrusion detection, few principal assumptions are to be made. First, person and software things to do has to be observable [5], that is data utilized by using the consumer or machine should be recordable / analyzable. Second, there will be the awesome traits between regular and intrusive behaviors.

HIDS vs. NIDS

To realize attacks, most IDS are deployed as both host primarily based or community based totally systems. These structures appear for unique patterns that point out malicious intent.

Host primarily based structures (HIDS) will appear for the patterns in device log documents that are worried with what is going on on every host. They are in a position to notice movements such as repeated failed get admission to tries or modifications to device files. The foremost difficulty is that patron has to be set up on each and every host related in the community the place every purchaser will be interpreted as techniques and operate evaluation on the audit records gathered locally.

Network based totally structures (NIDS) will pay attention for the patterns in community site visitors and seize & look at packets flowing via the network. i.e., they use uncooked packets as the audit supply with the assist of adapter strolling in the promiscuous mode to reveal and analyze site visitors in actual time. It can in a position to appear payload of a packet to see which precise host utility is accessed and to elevate indicators when attacker tries to take advantage of a bug.

Except the above classification of ID systems, It is been recognized that common intrusion detection processes can be divided into two classes: anomaly detection and misuse detection. Anomaly detection is based totally on the regular conduct of the situation [user or system]. Any occasions or an motion which deviates from the ordinary conduct is viewed to be intrusive. Anomaly detection enforces its thinking on statistical conduct modeling. Here, the audit facts is changed to a layout statistically same to the person profile, the place the person profile will be generated by using the

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

system. To locate out the intrusive behavior, threshold price will be related with the consumer profile. If any deviation takes place audit statistics and the person profile it would be regarded as intrusive.

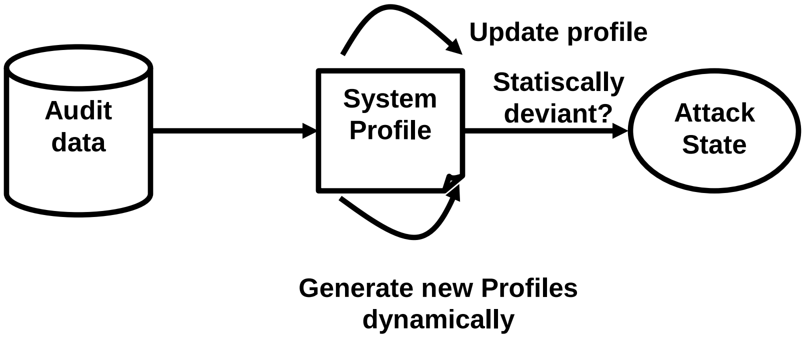


Fig. 2.1. Anomaly detection

Misuse detection is also called a signature detection which catches intrusions regarding known attack characteristics or vulnerabilities in the system. Every action or event consistent with the pattern of a known attack is deemed suspect. The main benefit of misuse detection is the reliable and low false rate detection of known attacks. The main problem is, however, that novel attacks on systems that leave different signatures cannot be detected. Anomaly detection may have an advantage of detecting unknown attacks over the misuse technique. However it suffers from false alarm rate.

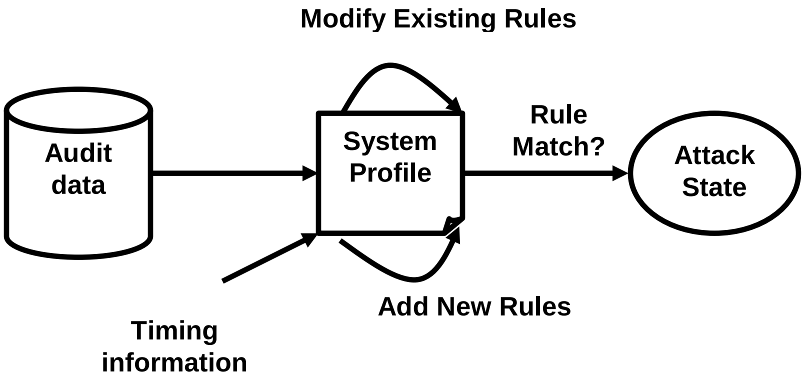


Fig. 2.2. Misuse detection

Audit records are the data which will be used by way of IDS the use of which intrusive data can be recognized and it can be gathered and processed whilst the host is both on line (connected to the network) or offline (disconnected from the network). In on line mode, the audit statistics is gathered and processed actual time continuously. If it is HIDS, a host will collect statistics as lengthy

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

as it is linked with the network. If it is NIDS, a machine will display the site visitors of the hosts during the time they related with the network. If any intrusive happens then an alert will be notified to different hosts. In offline mode, the audit statistics is now not processed actual time however periodically. A host primarily based gadget will collect data when it is now not linked with the community and a community based totally machine will display the community site visitors of the host periodically and intimate the nation of chance to different host when it occurs.

3. Survey of IDS

Issues of current of Intrusion detection techniques

Wireless ad-hoc networks does now not have constant community infrastructure. So it would be tough to follow intrusion detection methods designed for wired community to wi-fi networks. In case of wired network, visitors monitoring and evaluation is generally completed at switches, routers and gateways. But in wi-fi network, it does no longer have such factors the place the IDS can accumulate their audit records and it be counted solely on partial audit facts from the host and verbal exchange units taken location inside a range.

Another most important problem in the wi-fi community is that the adaptation of disconnected operations [7] being held on cell devices. This is incurred due to bandwidth limitations, battery constraints and regularly occurring disconnects. Existing intrusion detection methods failed to decide such operations and discover them as intrusions.

Lack of protocol requirements will facilitate challenge in defining assault signatures for the wi-fi environment. In universal signatures are described from the characteristics, vulnerabilities and the topologies of the routing protocol.

Choices of Anomaly Detection Techniques

Anomaly detection bases its concept on statistical behavioral modeling and it appears for conduct that deviates from regular device use.

NIDES/STAT

The next generation intrusion detection statistical machine (NIDES/STAT) observes situations on a monitored pc gadget and learning what is common to character-makers such as customers and businesses (Axelsson, 1999). The determined behaviour, when distinguishing from the expected behavior of the subject that is saved in its challenge profile is indicated as an achievable intrusion. Various measures are employed to measure one of the components in the behavior of a subject. Think about M1,M2, for the great illustration... Mn is the action used to mannequin ate behavioral difficulty. When S1, S2,... The sn values are the peculiar ones for M1, M2.

T2=S12+S22+….+Sn2

During the audit facts processing, the machine will robotically generates statistical profile (T2) of the subject. Since, NIDES/STAT adaptively learns a subject's conduct patterns. It offers the users to manually regulate the profiles that introduces the opportunity of an attacker steadily "training" the profile to think about his/her intrusive things to do as ordinary behavior.

Haystack

This algorithm is a host based totally device [8] that makes use of a statistical anomaly detection, which works with the aid of changing audit path generated from a host to a CAT (Canonical audit trail) format. Using which, an algorithm generates session vectors for representing the things to do of person sessions. These vectors will be analyzed in opposition to intrusive things to do to calculate anomaly rankings in three methods particularly (a) calculation of Bernoulli vector (b) calculation of weighted intrusion rating and (c) calculation of suspicion quotient. If there is a deviation, warning reviews can also be generated.

Bernoulli vector is generated from the session vectors to symbolize the a range of attributes that are out of vary for a precise session as properly as the threshold vectors the place a threshold vector T = , the place ti is a tuple of the structure , is used to aid this step. The threshold vector is saved in a user's profile. The Bernoulli vector B = is generated so that bi is set to 1 if xi falls outdoor the vary ti, and bi is set to zero otherwise.

Next, an algorithm generates weighted intrusion rating from Bernoulli vector and a weighted intrusion vector for a unique intrusion kind and session. It is used to assign a suspicion price to the session. This price is decided by way of proportion of random classes have a weighted intrusion rating much less than or equal to the weighted intrusion rating of the cutting-edge session.

This machine tries to discover countless sorts of intrusions: break-ins, masquerade attacks, penetration of the system, data leakage and dos. It can be deployed in wired network. For a wi-fi system, it requires a central administrator the usage of which audit information can be retrieved from different hosts linked in the network.

Indra

Indra (INtrusion Detection Rapid Action) is a dispensed IDS scheme based totally on statistics sharing between relied on friends in a network. It is distinctive as a protect device that takes a proactive and P2P strategy to the community security. It does go monitoring i.e., the hosts on the P2P community be a part of collectively such that every host distributes statistics on tried assaults amongst friends in the network, which permits the device to react proactively when it is hooked up on the gateways.

The performance of indra is got with the assist of daemons walking on the host. Each host on the community may additionally run a one of a kind daemon which watches out intrusion attempts. These daemons can be configured by way of gadget administrator for exceptional stages of security. Though the machine is effortless it is very hard to for the deployment due to believe degree and coverage of the network. As we recognize that IDS lacks with centralized relied on authority to furnish digital certificates. Thereby indra requires sure degree of have confidence between host so that the daemons strolling on the host can have confidence the messages obtained from the hosts.

Machine Learning and Data mining Techniques

Time based totally Inductive Machine

Teng et., al proposed TIM (Time primarily based Inductive machine) to seize conduct sample of the user. It is a device that discovers patterns based totally on the regulations for the person events, which represents repetitive activities. These patterns are generated from the enter facts the use of a logical inference known as “Inductive generalization”. An IDS will makes use of these sequential patterns for malicious activity. An instance of a simplified rule produced in TIM is

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

E1 - E2 - E3 → (E4 = 95%; E5 = 5%),

where E1, E2, E3, E4, and E5 are protection events.

This rule says that if E1 is observed by means of E2, and E2 is accompanied by using E3, then there is a 95% threat (based on the preceding observation) that E4 will follow, and a 5% threat that E5 will follow. TIM can produce greater generalized guidelines than the above. For example, it may additionally produce a rule in the form E1 - * → (E2 = 100%),

where an asterisk suits any single event. Any quantity of asterisks is allowed in a rule. The main trouble of TIM is that it solely considers the without delay following relationship between the determined events. That is, the guidelines solely characterize the match patterns in which occasions are adjoining to every other.

Data Mining

Data Mining algorithms can be correctly carried out on cell nodes. Using which audit records can be analyzed. Here mining algorithms does the extraction of information from massive repositories [9]. Classification is the key manner the place a facts is mapped with predefined categories. The classification algorithms use “classifiers” which are in the shape of bushes / rules. In order to categorize unseen audit data, ample ordinary and strange audit qualities has to be gathered earlier than the deployment of an algorithm.

Neural Network

Fox et., al ,modeled the machine the usage of neural community the place they had deployed with the preference of SOM (Self-Organizing Map), which is a unsupervised getting to know method that can find out the shape of data. It is been used as a device to screen intrusive things to do with eleven parameters that are recognized as the enter to the SOM structure.

Ghosh et al. proposed a Back-propagation community to display packages going for walks on the systems, which is developed for supervised learning. It wishes coaching information to construct the intrusion detection model. This community consists of an input layer, at least one hidden layer and an output layer.

With regard to BPN, neurons in the same or one layer are not connected with neurons in a preceding layer. The BPN is coached in 2 phases. In the first phase, the entry is sent to the community and distributed through the network to the output. The second stage contrasts the preferred output with the output of the network. The community updates the masses starting at the output neurons if vectors disagree. Then weight changes are calculated for the previous layer and cascade through the neuron layers to the neurons inside the layer. One benefit is that they obtained a multiplied degree of detection via the usage of randomly generated statistics as anomalous input. By thinking about this, the community receives extra education statistics that is complementary to the proper coaching data.

The principal difficulty is that the consequences this device had simulated with one virus attack, which might also no longer be adequate to draw serious conclusions.

Demerits of Anomaly Detection

Anomaly detection can seize unknown patterns of attacks. A frequent trouble of this method is that the conduct of the problem is modeled based totally on the audit information gathered over a duration of everyday operation. If there is any undiscovered intrusive things to do happen throughout this period, these will be regarded as everyday activities. In addition, a subject’s conduct typically modifications over time, the IDSs that use the above tactics generally enable the profile of the difficulty to exchange gradually. It offers an intruder to teach the IDS and trick it into accepting intrusive things to do as normal. Finally the cutting-edge anomaly detection methods go through from a excessive false-alarm rate.

Another challenging trouble in constructing anomaly detection fashions is how to determine the facets to be used as the enter of the fashions (e.g., the statistical models). In the present models, the enter parameters are generally determined by means of area professionals (e.g., community protection experts) in advert hoc ways. It is no longer assured that all and solely the aspects associated to intrusion detection will be chosen as enter parameters. Although lacking necessary intrusion-related elements makes it challenging to distinguish assaults from everyday activities, having non-intrusion-related points should introduce “noise” into the fashions and accordingly have an effect on the detection performance.

4.0 System description

4.1 Packet Sniffer

This module includes taking pictures all visitors passing via the network. The sniffer will be established on the quit device in a community on which the visitors has to be captured. The sniffer[10] captures all community visitors with the aid of working the community adapter in promiscuous mode.

4.2 Determination of assault signatures

Attack Signatures [13, 14] refers to the sample of assault traffic. Signatures are modeled primarily based on the packet header sample a precise assault follows. It entails a depend of packets from a unique goal or a specific supply or vacation spot port or it may also even be modeled with the assist of different important points in the packet such as header size, Time to Live (TTL), flag bits, protocol.

4.3 Identification of assaults

This includes extracting beneficial statistics from captured nearby visitors such as supply and vacation spot IP addresses, protocol type, header length, supply and vacation spot ports and many others and examine these important points with modeled assault signatures to decide if an assault has occurred.

4.4 Reporting assault small print

This includes reporting the assault to the administrator so that he may additionally take evasive action. Reporting includes specifying attack small print such as supply and sufferer IP addresses, time stamp of assault and extra importantly the kind of attack

4.5 Experimental results

4.5.1 Signature based totally intrusion detection

Signature-based IDSs function analogously to virus scanners, i.e. by means of looking out a database of signatures for a recognised identification – or signature – for every unique intrusion event. In signature-based IDSs, monitored occasions are coordinated in opposition to a database of assault signatures to realize intrusions.

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

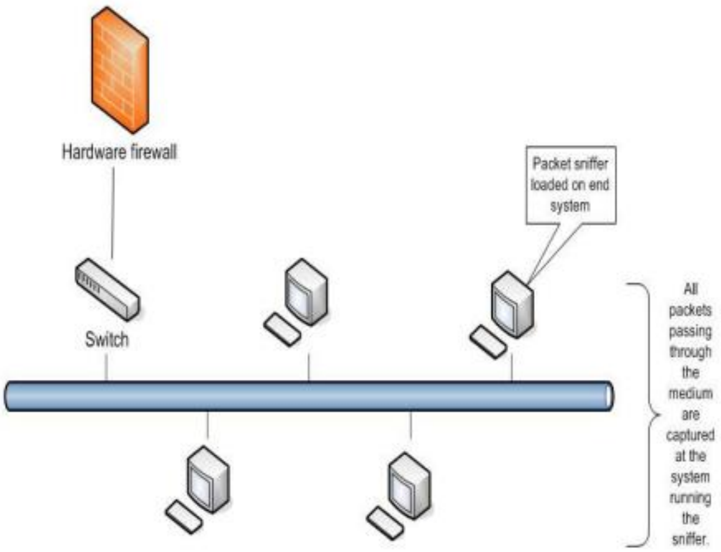

Hardware firewall
Packet sniffer loaded on end system
Switch
All packets passing through the medium are captured at the system running the sniffer.

Fig. 4.1 IDS in promiscuous mode

Signature-based IDS [15] are unable to observe unknown and rising assaults when you consider that signature database has to be manually revised for every new kind of intrusion that is discovered.

In addition, as soon as a new assault is found and its signature is developed, regularly there is a ubstantial latency in its deployment throughout networks [13]. The most nicely acknowledged signature-based IDS encompass SNORT [14], Network Flight Recorder [16], NetRanger [17], RealSecure [18], Computer Misuse Detection System (CMDS™) [20], NetProwler [21], Haystack [22] and MuSig (Misuse Signatures) [23].

This gadget follows the signature based totally IDs methodology for ascertaining attacks. A signature primarily based IDS will display packets on the community and examine them in opposition to a database of signatures [19] or attributes from acknowledged malicious threats.

4.5.2 Packet sniffing and promiscuous mode

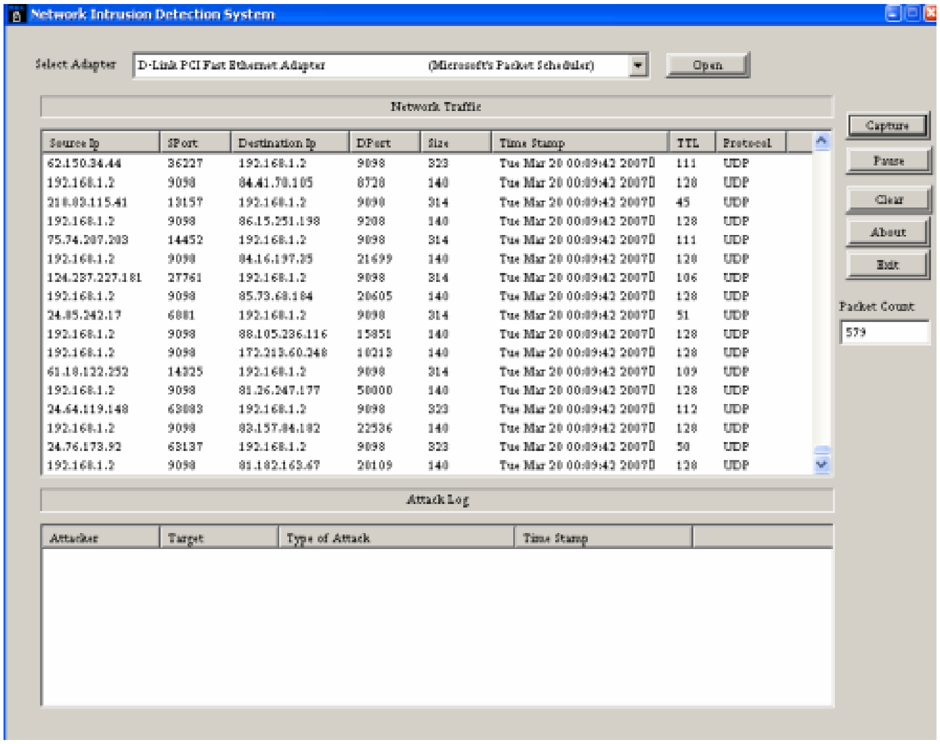
Typically, packet sniffers require a promiscuous Community interface. The packet sniffer usually requires administrative privileges in order to manipulate the hardware in a promiscuous way on the desktop as the packet sniffer in Figure 4.1.

This device uses a community test to seize uncooked packet information and then we retrieve packet information such as IP address for supply and vacation place, supply and holidays place ports, flags, header length, checksum, Time to Live (TTL) and protocol type using this uncooked packet record. We use this data to then evaluate and perceive threats to the network by recognized attack signatures, as shown in discernment 3. Section 4.2 shows the experimental consequences in display photographs.

4.5.3. Attacks captured

An IGMP denial-of-service attack mainly based on the exploration of the huge stack envelopes and IP spoofing of the stack. KOD (Kiss of Death) is a denial-of-service attack which is the result of a computer's "Blue Screen" error message, or instant reboot. KOD will ship the IGMP (Internet Group Management Protocol) malformed victim pc packets to fail.

affected.



Select Adapter: D-Link PCI Fast Ethernet Adapter (Microsoft's Packet Scheduler)

Network Traffic

Source Ip	SPort	Destination Ip	DPort	Size	Time Stamp	TTL	Protocol
62.150.34.44	36227	192.168.1.2	9098	323	Tue Mar 20 00:09:42 2007	111	UDP
192.168.1.2	9098	84.41.70.105	8728	140	Tue Mar 20 00:09:42 2007	128	UDP
210.83.115.41	13157	192.168.1.2	9098	314	Tue Mar 20 00:09:42 2007	45	UDP
192.168.1.2	9098	86.15.251.198	9208	140	Tue Mar 20 00:09:42 2007	128	UDP
75.74.207.203	14452	192.168.1.2	9098	314	Tue Mar 20 00:09:42 2007	111	UDP
192.168.1.2	9098	84.16.197.25	21699	140	Tue Mar 20 00:09:42 2007	128	UDP
124.237.227.181	27761	192.168.1.2	9098	314	Tue Mar 20 00:09:42 2007	106	UDP
192.168.1.2	9098	85.73.68.184	20605	140	Tue Mar 20 00:09:42 2007	128	UDP
24.85.242.17	6881	192.168.1.2	9098	314	Tue Mar 20 00:09:42 2007	51	UDP
192.168.1.2	9098	88.105.236.116	15851	140	Tue Mar 20 00:09:42 2007	128	UDP
192.168.1.2	9098	172.213.60.248	10213	140	Tue Mar 20 00:09:42 2007	128	UDP
61.18.122.252	14325	192.168.1.2	9098	314	Tue Mar 20 00:09:42 2007	109	UDP
192.168.1.2	9098	81.26.247.177	50000	140	Tue Mar 20 00:09:42 2007	128	UDP
24.64.119.148	63083	192.168.1.2	9098	323	Tue Mar 20 00:09:42 2007	112	UDP
192.168.1.2	9098	83.157.84.182	22536	140	Tue Mar 20 00:09:42 2007	128	UDP
24.76.173.92	63137	192.168.1.2	9098	323	Tue Mar 20 00:09:42 2007	50	UDP
192.168.1.2	9098	81.182.163.67	20109	140	Tue Mar 20 00:09:42 2007	128	UDP

Packet Count: 579

Attack Log

Attacker	Target	Type of Attack	Time Stamp

Fig. 4.2 Results

5.0. Conclusion

This paper presented with different types of Intrusion detection systems, merits, demerits and the performance measurements that are desired. To assess those metrics, past empirical evaluations are considered. Even after five years of research, there are still several difficult problems with the intrusion detection community. An unresolved problem remains how to detect unknown attack

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

patterns without generating enough false alerts, although several findings have shown that there is a possible solution to the problem recently. With reference to the evaluation, the target IDS environment would be a DIDS, which is a heterogeneous network of system. It is a complete defense against DOS attack which will be provided using DAD framework [20], I believe that DIDS will able to detect the host intrusion that are flagged by other IDSs such as IDES, Sense[10].

6.. References

[1]. T. Jayasankar, S. Shanthi, R.M. Bhavadharini and C. Thiruvengadam, "A Multicast Effective Intrusion Detection System for MANET**",** Bioscience Biotechnology Research Communications, Special Issue Recent Trends in Advanced Information and Communication Technology, Vol. 13, No.2, March (2020),pp.132-136

[2]. R. Kiruba Buri and T. Jayasankar," Intelligence Intrusion Detection Using PSO with Decision Tree Algorithm for Adhoc Network", Bioscience Biotechnology Research Communications, Special Issue Recent Trends in Computing and Communication Technology, Vol. 12, No.2, March (2019),pp.27-34.

[3]. Feiertag, R., Rho, S., Benzinger, L., Wu, S., Redmond, T., Zhang, C., Levitt, K., Peticolas, D., Heckman, M., Staniford, S., & McAlerney, J. (2000). Intrusion detection inter-component adaptive negotiation. Computer Networks, 34, 605--621.

[4]. Fox, K.L., Henning, R.R., Reed, J.H., & Simonian, R.P. (1990). A neural network approach towards intrusion detection. In NIST (Ed.), Proceedings of 13th National Computer Security Conference (pp. 125--134), National Institute of Standards and Technology (NIST), Baltimore, MD.

[5]. Frincke, D., Tobin, D., McConnell, J., Marconi, J., & Polla, D. (1998). A framework for cooperative intrusion detection. In NIST (Ed), Proceedings of the 21st national information systems security conference (pp. 361-373), National Institute of Standards and Technology (NIST), Baltimore, MD.

[6]. Ghosh, A.K., Wanken, J., & Charron, F. (1998). Detecting anomalous and unknown intrusions against programs. In K. Keus (Ed),Proceedings of the 14th annual computer security applications conference (pp. 259--267). IEEE Computer Society, Los Alamitos, CA.

[7]. Hofmeyr, S., Forrest, S., & Somayaji, A. (1998). Intrusion detection using sequences of system calls. Journal of Computer Security, 6, 151--180.

[8]. Ilgun, K., Kemmerer, R.A., & Porras, P.A. (1995). State transition analysis: A rule-based intrusion detection approach. IEEE Transactions on Software Engineering, 21 (3), 181--199.

[9]. Ko, C., Ruschitzka, M., & K. Levitt (1997). Execution monitoring of security-critical programs in distributed systems: a apecification-based approach. In G. Dinolt & P. Karger (Eds.), Proceedings of 1997 IEEE symposium of security and privacy (pp. 175-187), IEEE Computer Socitey, Los Alamitos, CA

[10]. http://www.winpcap.org/ - Obtained drivers for packet capture with wpcap.dll and packet.dll driver.

[11]. http://www.karalon.com - Obtained Karalon IQ professional tool for testing our network intrusion detection system.

[12]. http://www.securityfocus.com – White papers for intrusion detection techniques and methodologies.

[13]. R. Lippmann, The Role of Network Intrusion Detection, In Proceedings of the Workshop on Network Intrusion Detection, H.E.A.T. Center, Aberdeen, MD, March 19-20, 2002

[14]. SNORT Intrusion Detection System, www.snort.org, 2004 Snort-Wireless Intrusion Detection, http://snort-wireless.org, 2003.]

[15]. NFR Network Intrusion Detection, http://www.nfr.com/products/NID/, 2001. Cisco Systems, Inc., NetRanger-Enterprise-scale, Real-time, Network Intrusion Detection System,

[16]. http://www.cisco.com/univercd/cc/td/doc/product/iaabu/netrangr/, 1998.

[17]. Internet Security Systems, Inc., RealSecure, http://www.iss.net/prod/rsds.html, 1997.

[18]. Intrusion.com, Intrusion SecureHost, white paper available at: www.intrusion.com/products/hids.asp , 2003.

[19]. A.Thomas Paul Roy and K.Balasubadra, “DAD: A Secured Routing Protocol for Detecting and Preventing Denial-of-Service in Wireless Networks”, Wireless Personal communications, DOI 10.1007/s11277-015-3022-x,Aug 20, 2015

[20]. N. Weaver, V. Paxson, S. Staniford and R. Cunningham, A Taxonomy of Computer Worms, In proceedings of the The Workshop on Rapid Malcode (WORM 2003), held in conjunction with the 10th ACM Conference on Computer and Communications Security, Washington, DC, October 27, 2003.

[21]. Wheel Group Corporation, Cisco Secure Intrusion Detection System,

[22]. http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/index.htm , 2004

[23]. Patwardhan, A. Parker, J., Joshi,A., Karygiannis, A., and Iorga,M. “Secure Routing and Intrusion Detection in Ad Hoc Networks”, Third IEEE International Conference on Pervasive Computing and Communications, Kauai Island, Hawaii, 2005.

[24]. K.Vinoth Kumar,T. Jayasankar, V. Eswaramoorthy,V. Nivedhitha, ” SDARP: Security based Data Aware Routing Protocol for ad hoc sensor networks,”, International Journal of Intelligent Networks (2020),vol.1,2020,pp. 36–42

[25]. Radhika Baskar, Sudhakar Sengan, S.Sumithra, R.Purushothaman, T. Jayasankar,” An Improved Routing Schema with Special Clustering using Hybrid GA-ACO-PSO for Heterogeneous Wireless Sensor Network”, International Journal of Advanced Science and Technology, Vol.29, No.5, (2020), pp.6661–6672, ISSN: 2005-4238.