International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue IX, September 2017- Available at www.ijraset.com

Real-time Intrusion Prevention System to Increase Computer Security in Wireless LAN

S V Athawaler[1], M A Pund[2]
[1, 2] *Research scholars, Computer department, SGBAU, Amaravti, Professor, PRMIT & R, Badnera – Amravati.*

Abstract: Network intrusion hindrance systems offer a crucial proactive defence capability against security threats by detective work and block network attacks. This task may be extremely complicated and ancient firewall system ar presently ineffective of handling quick attack through the package. The issues arise once several exploits commit to cash in of weaknesses in each protocols that ar allowed through our perimeter firewalls, and once the net server has been compromised, this will usually be used as a springboard to launch extra attacks on alternative internal services. Thus, iptables additionally referred to as Netfilter can even be implement as AN intrusion hindrance system. Iptables works by filtering the traffic flow between your pc and therefore the web. It will limit access to and from the net to solely specific computers on your network. It can even limit the kind of communication, by selection allowing or denying numerous web services. Hence, to harden the iptables rule, another tool got to be apply to figure with the iptables rule script.

Keywords: Network Intrusion prevention system, attacks, iptable, firewall, netfilter.

I. INTRODUCTION

Today's knowledgeable hackers have advanced well on the far side scanning for open ports on network firewalls and area unit currently targeting applications directly. They need devised refined attacks that simply circumvent ancient intrusion detection systems (IDS) and network firewalls.

This trend has given rise to two differing types of next-generation security merchandise --Intrusion hindrance Systems (IPS) and Application Firewalls. each IPS merchandise and application firewalls area unit capable of block attacks that bypass ancient firewalls. Thence each are with success deployed in a number of the most important networks within the world.

Whilst it's true that firewalls, routers and even Intrusion Detection System devices all have intrusion hindrance technology enclosed in some kind, it's believe that there area unit comfortable grounds to make a brand new market sector for true Intrusion hindrance System (IPS). These systems area unit proactive defence mechanisms designed to notice malicious packets among traditional network traffic (for example, one thing that the present breed of firewalls don't truly do) and stop intrusions, block the sinning traffic mechanically before it will Associate in Nursingy harminstead of merely raising an alert .

Within the IPS market place, there area unit 2 main classes of product: Host IPS and Network IPS (Neil Desai,Gregorian calendar month 2003). In Host IPS, the Host IPS depends on agent that area unit put in directly on the system which will be protected. It binds closely with the software kernel and services closely so as to stop the attack similarly as log them. whereas in Network IPS (NIPS), it's regarding the mix of a customary IDS, Associate in Nursing IPS and a firewall. Sometimes, it's decision as Associate in Nursing In-line IDS or entrance IDS. The NIPS has a minimum of 2 network interfaces, one is style as internal and another one as external. As packet appeared at either interface, they're well-versed the detection engine for review whether or not the packet ought to be transmit or drop. once the NIPS notice a malicious packet, instead of raising Associate in Nursing alert, it'll discard the packet and mark that flow as unhealthy.

Many people don't notice that iptables also can act as Associate in Nursing Intrusion hindrance System. The iptables firewall or conjointly referred as Netfilter is that the default firewall tool for UNIX operating system software. Iptablesis mostly thought-about to be additional advanced than ipchains. However, iptables offer additional powerful and versatile feature. The iptables feature works by having information science packets that is network information that enter or leave the firewall laptop, traverse a collection of chains that outline the tasks that area unit through with the packet. every rule that area unit add basically will each of the subsequent ; (1). Checks if a specific criterion is metlike that a packet requests a specific service or comes from a specific address. (2). Takes Associate in Nursing action (such as dropping, accepting, or additional process a packet).

Different set of rules area unit enforced for various varieties of tables. However, most of the foundations you produce can relate to the filter table. lots of nice options area unit designed into iptables. a number of the options area unit as a clear proxy, port forwarding and intrusion hindrance system.

II. LITERATURE REVIEW

An intrusion hindrance system (a laptop security term) is any device that exercises access management to safeguard computers from exploitation. "Intrusion prevention" technology[1] is taken into account by some to be associate degree extension of intrusion detection (IDS) technology, however it's really another type of access management, like associate degree application layer firewall. (Wikipedia, the free encyclopaedia) Intrusion hindrance systems were made-up severally by Jed Haile and Vern Paxon to resolve ambiguities in passive network monitoring by putting detection systems in-line. a substantial improvement upon firewall technologies, IPS create access management decisions supported application content, instead of information science address or ports as ancient firewalls had done. (Wikipedia, the free encyclopaedia) Some time later IPS was commercialised by One Secure that was eventually acquired by NetScreen Technologies that was successively acquired by Juniper Networks 2004[2, 3]. It is vital to know that no resolution will defend against completely all attacks. owing to the dynamic attack landscape, it's not possible to predict and defend against everything that would probably be used against a network. The inherent complexness of network traffic, which incorporates the various range of protocols at each the network (IP, TCP, UDP, ICMP, etc.) and application (HTTP, FTP, SMTP, DNS, POP3, IMAP, etc.) layers, provides [4, 5] attackers ample vulnerabilities to use. mix the inherent complexness with the very fact that attacks are available in completely different shapes and forms, and attackers have a virtual buffet to decide on from after they area unit assaultive your network. The secret is to attenuate your exposure to attacks [6, 7, 8]. As a result, the comprehensiveness of protection provided by AN intrusion detection and interference system is crucial to its ability to assist organizations maintain a suitable risk level [9]. The answer should support a broad vary of protocols and defend against a various set of attack varieties to supply price.

Whether AN intrusion detection and interference system will stop the attack from ever reaching its victim is that the cornerstone to its interference capabilities [10, 11, 12]. However effective is AN intrusion detection system that has got to trust another system to undertake to stop an attack? the solution is clear, [13] however several intrusion detection merchandise do exactly that, causation letter of invitation to a firewall or perhaps the victims themselves to undertake to finish the attack [14]. All of those mechanisms come back once the attack has already reached the victim, thus even once triple-crown, they need the network administrator to analyse precisely what proportion the attack was ready to do before it absolutely was stopped. Any device that introduces latency to the interference response isn't ready to supply true interference. A very effective resolution will actively stop attacks throughout the detection method and drop the malicious traffic [15, 16]. This ensures it ne'er reaches its supposed victim, keeping the enterprise network and sensitive, mission-critical knowledge safe and secure.

III. TYPE INTRUSION PREVENTION SYSTEM

A. Network-based intrusion interference

Network intrusion monitors area unit hooked up to a packet-filtering router or packet someone to observe suspicious behavior on a network as they occur. they give the impression of being for signs that a network is being investigated for attack with a port scanner, that users area unit falling victim to best-known traps like .url or .lnk, or that the network is really underneath AN attack like through SYN flooding or unauthorised tries to realize root access (among alternative varieties of attacks).

B. Host-based intrusion interference

As with Host IDS systems, the Host IPS depends on agents put in directly on the system being protected. It binds closely with the software package kernel and services, observation and intercepting system calls to the kernel or Apis so as to stop attacks likewise as log them.

IV. PROPOSED NETWORK BASED IPS FRAME WORK

Combining “Best of Breed” Host and Network IPS technology leads to a a lot of comprehensive and sturdy defensive posture, which means fewer roaring attacks, a lot of economical use of scarce security resources and lower in operation prices than merely deploying one technology or the opposite. AN intrusion or compromise consists of multiple stages: intelligence operation, Scanning, Gaining Access, Maintaining Access, and Clearing Tracks. though each Host and Network IPS have the power to forestall every stage, each technologies don't seem to be equally adept at police work and block every stage (Figure 1). integration the strengths of every design provides an answer whose add is larger than its elements[17].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue IX, September 2017- Available at www.ijraset.com

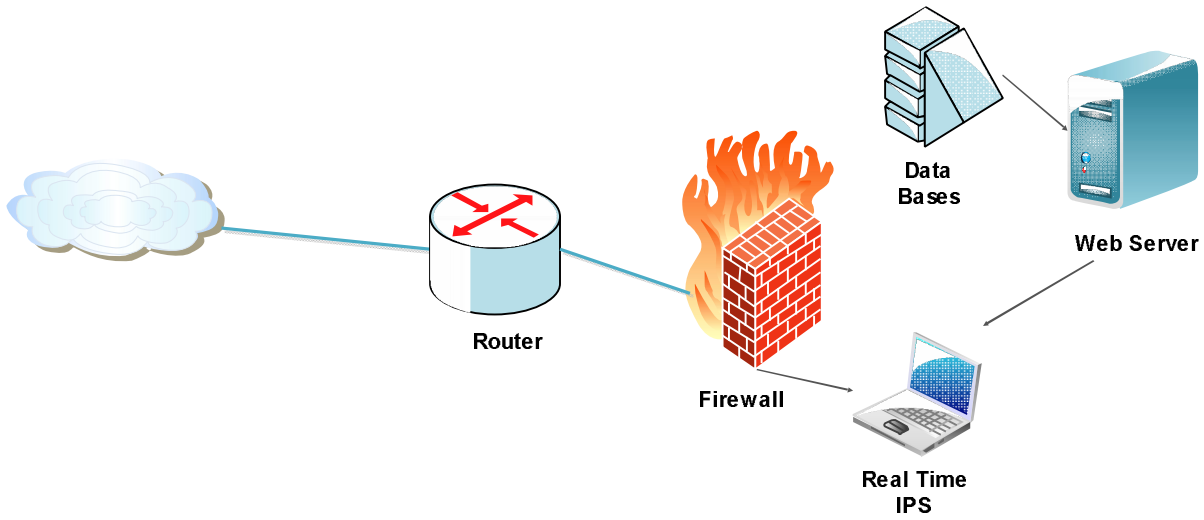

Fig. 1 System frame work

A. Inline network intrusion detection system

Although it's referred to as as Inline Network Intrusion Detection System however it performs as associate degree intrusion bar system. Most NIDS would be designed with 2 NICs, one for management and one for detection (Fig 2). The NIC that's designed for detection typically doesn't have associate degree IP address appointed thereto, creating it a "stealth" interface. Since it doesn't have associate degree IP address appointed thereto nobody will send packets thereto or cause the NIDS to reply victimisation that interface. associate degree inline NIDS offers the good capabilities of an everyday NIDS with the block capabilities of a firewall. Like most NIDS, the user will monitor, [18] during this case shield, several servers or networks with one device. this could be each a blessing and a curse. If the system were to fail or crash the traffic wouldn't get through the device. (ISS Guard really fails open once the merchandise crashes). If you're involved regarding period of time and SLAs, this may cause a giant issue for your network. These IPSs can feel most comfy within the hands of security groups that already upset NIDS. as a result of these IPSs area unit variants of existing NIDS, writing rules for them is extremely straightforward and offers the way to catch new attacks. to dam unknown attacks with a signature-based inline NIDS, you'd got to have some generic rules, like yearning for NOOP sleds. This doesn't, however, stop all new attacks.

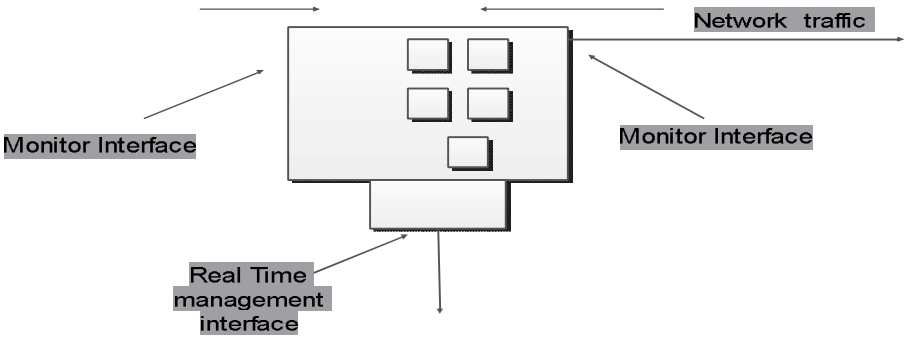

Fig. 2 Real time inline Network based IPS

V. SIMULATION RESULTS WITH ON-LINE PREVENTION SYSTEM (REAL-TIME IPS)

Simulations area unit allotted for all the information flows explained in Section III, singly with FTP traffic for communications protocol and cosmic microwave background radiation traffic for UDP. Performance is measured in terms of, throughput and Latency as explained in next Section.

A. Throughput

This can be measured because the range of data packets transferred associate exceedingly in a very network over an observation time. Throughput is measured bits per second. Figure eight shows the variation in turnout with modification in information Flows, for protocol and UDP protocols. From the obtained results it may be ended that just in case of UDP the throughput for 'parallel

information flow' is high. Turnout decreases incessantly with increase in information flow attributable to increase in traffic in network. Just in case of protocol, turnout is constant the least bit the info flows. It's attributable to less traffic in network, since in protocol, the info packet is shipped solely once [19].

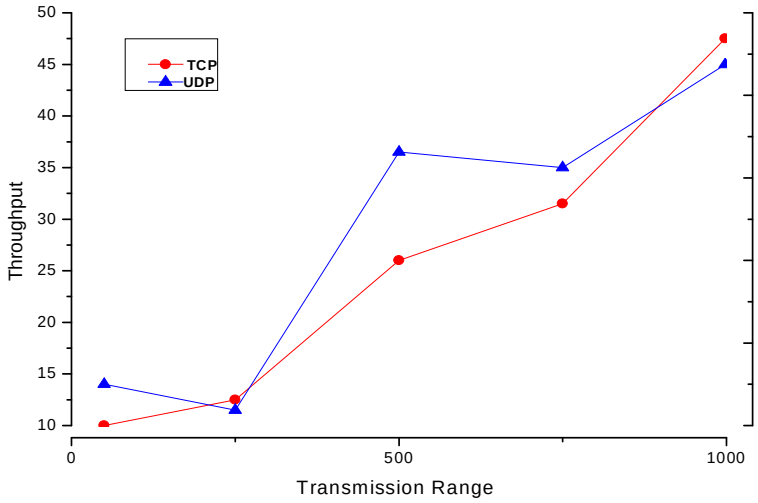

Fig. 3 Throughput Vs Transmission range

B. Latency

The latency for the UDP ought to be low compared to protocol as a result of UDP will conduct a lost packet and there is no provision of acknowledgment in UDP. Just in case of protocol, the sender waits for Associate in Nursing acknowledgment once causation every packet. Protocol conjointly has the availability to conduct a lost packet. However, from our simulation results we've observed that UDP takes longer compared to protocol. This may be owing to the amount of hops taken by the data packets is additional in UDP. It's determined throughout the simulation run that packets took longer ways (instead of straight link between supply and several destination), which may have contributed to end-to-end delay [20].

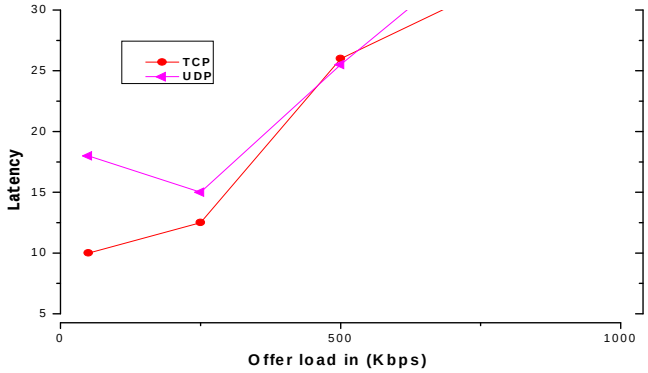

Fig.3 Latency Vs offerload

VI. CONCLUSIONS

In this paper, we tend to conferred a sensible period of time network primarily based network intrusion hindrance system (RT-IPS) model which might be used with existing well-known communications protocol and UDP protocol with ns-2 simulations. Our RT-IPS we tend to conferred however we tend to mix hybrid approach the experimental results showed that the performance. Thus, we tend to developed a brand new period of time IPS victimization the inline hindrance technique.

The performance analysis results showed that our period of time IPS is economical in terms of period of time detection speed and consumption of output and latency. Our analysis work has many contributions as follows. (1) we tend to gift associate uncomplicated IPS model which might be simply applied with existing NS-2 simulations. (2) No human professional is required to

examine or establish the attack. (3) This little range of options will considerably improve the on-line (real-time) IPS and consumption of laptop resources.

In future work, we tend to attempt to implement a mixture technique for misuse findion and anomaly detection with additional nodes so as to higher detect unknown attack sorts.

VII. ACKNOWLEDGMENT

The authors wish to acknowledge the support of the Sant Gadge Baba Amravati University research centre, Amravati, India to carry out this research work.

REFERENCES

[1] Guanlin Chen1, et al.An Intelligent WLAN Intrusion Prevention System Based on Signature Detection and Plan Recognition,2010 Second International Conference on Future Networks,p 168-172, 2010.
[2] S V Athawale,D N Chaudhari,Towards effective Client-Server based Advent Intrusion Prevention system for WLAN,IEEE International Conference on Computer, Communication and Control,p 1-5,2015.
[3] Yujia Zhang et al. An Overview of Wireless Intrusion Prevention Systems,2010 Second International Conference on Communication Systems, Networks and Applications, p 147-150,2010.
[4] Yaqing Zhang,Srinivas Sampalli,Client-based Intrusion Prevention System for 802.11 Wireless LANs,2010 IEEE 6th Intemational Conference on Wireless and Mobile Computing. Networking and Communications 100-107,2010.
[5] Wang Zhenyu et al. Design and Implementation of Wireless Trusted Access Protocol for Embedded Trusted End points 1-8, 2005.
[6] Phurivit Sangkatsanee et al.Practical real-time intrusion detection using machine learning approaches 2227–2235, 2011.
[7] N. Wattanapongsakorn, S. Srakaew et al.A Practical Network-based Intrusion Detection and Prevention System,p 2010-2014, 2012.
[8] L. Felipe Perrone, ,Samuel C. Nelson,A Study of On-Off Attack Models for Wireless Ad Hoc Networks,2006.
[9] Shikha Goel,Sudesh Kumar,An Improved Method of Detecting Spoofed Attack in Wireless LAN,First International Conference on Networks & Communications,p 105-108,2009.
[10] Samer Fayssal,Byoung Uk Kim,Performance Analysis Toolset for Wireless Intrusion Detection Systems,p 484-490,2010.
[11] Tahir Saleem et al.Performance Issues of Routing Protocols in Mobile Ad-hoc Networks,p 32-38,2010.
[12] Khalid Alsubhi et al.Rule Mode Selection in Intrusion Detection and Prevention Systems,IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2011 proceedings,p 1-6,2011.
[13] L. Felipe Perrone, et al.A Study of On-Off Attack Models for Wireless Ad Hoc Networks, p 1-10,2006.
[14] Xiao qiang Peng et al. The intrusion Detection System design in WLAN based on Rogue AP,p.432-436,2010.
[15] Alexandros Tsakountakis et al.Towards effective Wireless Intrusion Detection in IEEE 802.11i,Third International Workshop on Security Privacy and Trust in Pervasive and Ubiquitous Computing,2007.
[16] C.H. Liu et al.Wavelet-enabled Massive Data Compress Algorithm,201O International Conference on Computer Application and System Modeling (ICCASM 2010),p 515-517,2010.
[17] S V Athawale, Dr M A Pund."ACIPS: Improvement of Client-Server based Intrusion Prevention System for Wireless LAN",International Journal of Innovative Research in Computer and Communication Engineering,(IJIRCCE)Vol. 5, Issue 4,p.6868-6871,2017.
[18] S V Athawale1, M A Pund,"Intrusion Prevention System for Wireless LAN Security: A Study", International Journal of Advanced Research in Computer and Communication Engineering,(IJARCCE),Vol. 5, Issue 10,p.421-423,2016.
[19] S V Athawale1, M A Pund,"A Novel Algorithm to Determine the Attacks Intention in Wireless Ad hoc Networks", International Journal Of Engineering And Computer Science, Volume 5 Issue 12, p.19283-19287, 2016.
[20] S V Athawale1, M A Pund,"The Modern Approach in Wireless Intrusion Prevention System for Ad hoc Network: A Target Oriented Approach", International Journal of Advanced Research in Computer Science and Software Engineering,(IJARCSSE),Volume 7, Issue 2,p..1-7,2017.