General IPS: Carapace for Campus Wide Network in Intranet

Archana Wankhade[†], Premchand Ambhore[††], Bandu Meshram[†††]

[†]Faculty of Engineering, Higher and Technical Education Maharashtra State, 444604 India
[††] Research Sch0lar, Engineering and Technology GCOE Amravati, Maharashtra State, India
[†††]Faculty of Engineering, Higher and Technical Education Maharashtra State, 444604 India

Abstract
The proposed software architecture is implemented by using the agile software development process. The proposed software for the defence against attacks deals with the attack generation, attack detection in the intranet and then prevention of attacks. The attack prevention module is flexible as we can add the rule in the firewall to prevent the any known attack. The software is deployed on our collage campus wide network and tested for the intrusion detection and prevention. Due to space problem we considered two attacks on every packet such as ICMP, UDP and TCP packet.

Keywords:
Smurf, Ping of Death, ICMP Flood, LAND, XMAS, TCP Flood, Ping Pong Attack Generation, Firewall rules

1. Introduction

Nations without controlled borders cannot ensure the security and safety of their citizens, nor can they prevent privacy and theft. Similarly, networks without controlled access cannot ensure the security or privacy of stored data, nor can they keep network resources from being exploited by hackers. When internal network is connected to the internet, there is no inherent central point of security control; in fact there is no security at all. With the persistent development and extensive application of network technology, the security of network system is increasingly outstanding, which has been a big hotspot concerned by governments, companies and individual users. In order to safeguard the secure running of network, people have taken diverse protecting measures, and among them, intrusion detection and firewall are adopted more frequently.

Intrusion detection system (IDS) is an independent software and hardware system that can recognize a hostile attempt or action to the computer and network resources and make a response. IDS collect and analyze the data packets from some key spots of network to find the actions that will damage the network security. According to information source, IDS can be divided into Host-based IDS (HIDS) and Network-based IDS (NIDS). The information source of HIDS is system log of host, file system of host and the host actions including service, process, conversation, operation, etc. Analyzing the system log can find an invalid usage of host or an intrusion. For example, when a file is modified, HIDS will compare the new record with the known attack characters and judge whether they are matching. If matching, HIDS will give an alarm to the administrator or make a proper response. The information source of NIDS is the information stream of network. NIDS mainly monitors the corresponding port and detects the intrusions in this segment of network. Once an attack is detected, the response module of NIDS will make a response through the mode of inform, alarm, cutting the network connections, etc. Firewall technology emerged in the late 1980s when the Internet was a fairly new technology in terms of its global use and connectivity. The original idea was formed in response to a number of major internet security breaches, which occurred in the late 1980s. The first paper published on firewall technology was in 1988, when Jeff Mogul from Digital Equipment Corporation (DEC) developed filter systems known as packet filter firewalls is **First generation - packet filters**:. From 1980-1990 two colleagues from AT&T Company developed the second generation of firewalls known as circuit level firewalls. Publications by Gene Safford of Purdue University, Bill Cheswick at AT&T Laboratories described a third generation firewall. Also known as **proxy based** firewalls.

Subsequent generations: In 1992, Bob Braden and Annette DeSchon at the University of Southren California (USC) were developing their own fourth generation packet filter firewall system. In 1994 an Israeli company called Check Point Software Technologies built this into readily available software known as FireWall-1. Cisco, one of the largest internet security companies in the world released their PIX " **P**rivate **I**nternet E**X**change " product to the public in 1997.

At present, firewall is one of the foremost security technologies in the interior network. It is a system or a set of systems, which locates in the boundary of two networks, realizes the security strategy and monitors the network communication. In order to protect the interior network, firewall puts teeth in the access control of the interior network (such as campus network) and the exterior network (such as Internet). The data stream through firewall is monitored, restricted, and transformed by establishing a complete set of rules and strategies. According to recovery mechanism, firewall can be divided into packet filter firewall, proxy service firewall, etc.

Manuscript received October 5, 2013
Manuscript revised October 20, 2013

Packet filter firewall is based on the information of IP packet. It filters the IP source address, IP destination address, encapsulating protocol, port number, etc, and closes the door to the invalid IP packets. Proxy service firewall adopts the protocol filter of application layer in network. Between client and server, it entirely obstructs the duplex data exchange. Because there is no direct data channel between the exterior and interior system, vicious attacks from the exterior can't damage the interior system.

The Paper is organized as below: the second section describes the literature survey required for the implementation of Intrusion Protection Systems. The third section describes our proposed architecture of IPS and the algorithms used in the implementation.

2. Literature Survey

We have studied various attacks, open source IDS and Firewalls

2.1 Network Attacks

Attacks can be divided into many categories as below Teardrop, Smurf, Satan, Ipsweep, Ping of death (pod), phf, perl, Multihop, Loadmodule, land, Imap, Guess Passwd/Dictionary

2.2 IDS

The classification of IDS is as Shown in the Figure 1

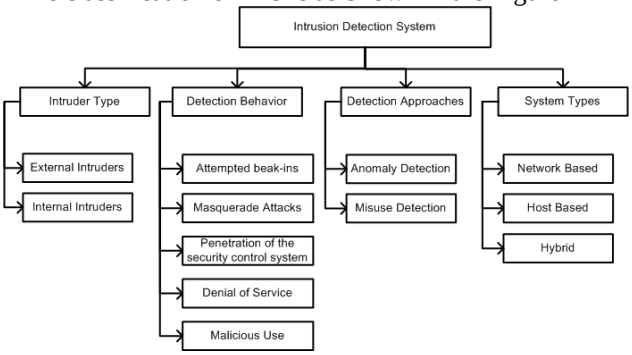

Figure 1 Classification of IDS System

IDS Analysis Approaches: Intrusion detection systems must be capable of distinguishing between normal and abnormal user activities, to discover malicious attempts in time. The activity of the user in IDS may fall into any one of the following category. Normal ,Unpredictable ,Abnormal

Anomaly based Detection Approach : It identifies any unacceptable deviation from expected behavior. An anomaly might include Users logging in at strange hours ,Unexplained reboots or changes to system clocks, Unusual error messages from mailers, daemons, or other servers , Multiple failed login attempts with bad passwords ,Unauthorized use of the 'su' command to gain UNIX root access ,Users logging in from unfamiliar sites on the network.

Misuse-based detection Approach : Misuse-based detection approach identifies patterns corresponding to known attacks. This includes passive protocol analysis which is the use of sniffers in promiscuous. It also includes signature analysis which is the interpretation of a series of packets that are determined, in advance, to represent a known pattern of attack**.**

Network IDS or NIDS: NIDS are intrusion detection systems that capture data packets travelling on the network media (cables, wireless) and match them to a database of signatures. Depending upon whether a packet is matched with an intruder signature, an alert is generated or the packet is logged to a file or database. One major use of Snort is as a NIDS [HYPERLINK ¥l "Das08" 30].

Host IDS or HIDS: Host-based intrusion detection systems or HIDS are installed as agents on a host. These intrusion detection systems can look into system and application log files to detect any intruder activity. the HIDS is installed and alert you in real time26]**}**.

Protocol based IDS: Orifice based IDS is installed on a server and it analyzes the server. IT sits at the fromt end of the server, monitoring and analyzing the dynamic behavior and state of the communication protocol between a connected device and server.

Application protocol based IDS: Application protocol based IDS normally sit between group of services/processes monitors and analyze the behavior and state of application protocol in use by the system between two connected devices.

Anomaly based IDS: Anomaly based IDS detects computer intrusions by monitoring system activity and classifying it is either normal or anomalous

Misuse Based: It is also called as Signature based IDS. It performs the simple process of matching patterns corresponding to a known attack type. It is also known as pattern based IDS.

Hybrid based: Hybrid based IDS combines one or more approaches. Host agent data is combined with network information to form a comprehensive view of the network.

3. Proposed IPS System

Due to space problems, we have considered very few attacks and their defence mechanisms. The implementation of proposed system is divided into following process: Attack Generation algorithms, Defence Against Attack (Attack Prevention algorithms) , Attack Detection Algorithms. Some of the sample attack detection and prevention rules are discussed below:

3.1 Attack Generation algorithms

Packet Capture: We o used TCP dump and window dump to capture the incoming flow of information and analysed this traffic by using the proposed IDS. Attack Generation Process can use different tools like NMAP, Nessus, hping3 and Scapy to generate different kinds of trailer made packet to do the attack.

For **Attack Generation we used the** following tools Scapy(**http://www.scapy.org**),Nmap(**http://www.nmap.org**),Hping3**http://www.hping.org**)

3.1.1 Land Attack Generation

#hping3 –a –spoof -flood <src_ip> <dst_ip>
where a:spoof source address
flood: sent packets as fast as possible. Don't show replies.
src_ip : source ip address which is spoofed
dst_ip : destination ip address

3.1.2 XMAS Attack Generation:

Using the Hping #hping3 –c 1 –V –p 80 –s 5050 –M 0 –UPF 192.16.0.103
Where c: count V: command line switch for addition information about the packet
p : port no , s: source port, M: set the sequence

3.1.3 SYN Flood Attack Generation

Using the command: hping3 –S –fast –a <src_ip> <dest_ip>
where S : SYN packets are generated
fast : 10 packets per second
a:for spoofing option
src_ip : is a Source ip

3.1.4 XMAS Attack Generation

Using Scapy
#hping3 –c 1 –V –p 80 –s 5050 –M 0 –UPF 192.16.0.103
Where:
src :source ip ,
dst :destination ip
flags : FPU-FIN,PUSH,URGENT
count : no of packet to generate.

3.2 Attack Detection Algorithms

Attack detection task will be carried out through Snort IDSwww.snort.org),SPADE(www.silicondefence.com/Spice_JCS.pdf,www.silicondefense.org), NIDES(www.nides.org),HONEYPOT(www.Honeydpot.org),KESENSOR(www.keyfocus.net/kfsensor), HONEYD(www.Honeyd.org),TRIPWIRE(www.tripwire.org)

3.2.1 ICMP Attacks Detection

If protocol:ICMP and tyop: Request
check if state[ipaddress] : active
else if state[ipaddress] :active and returncheck if lastpacket.time < 1 [1in 1sec] count[ipaddress]++
else cout[ipaddress] : 0 if count[ipaddress] > 25 [70 in 1sec]
reset count[ipaddress]:0 and lastpacket.time :0
set alarm flag

3.2.2 Smurf attack Detection:

Alert icmp $External_net any : $home_net any (msg:"icmp smurf attack detected"; dsize:4; icmp_id:0 ;icmp_seq:0 ; itype:8 ; classtype: attempted – recon ; sid:78787878;)

3.2.3 SYN Flood Attack Detection

If protocol: TCP and Type: Syn
check if state[ipaddress] : active
else if state[ipaddress] : active and return
check if lastpacket.time < 1 [1in 1sec] count[ipaddress]++
else cout[ipaddress] : 0 if count[ipaddress] > 25 [70 in 1sec]
reset count[ipaddress]:0 and lastpacket.time :0
set alarm flag

3.2.4 LAND Attack Detection

If protocol:TCP and type: SYN,
if Sourceip port == Destination port ,
if Sourceip ip : Destination ip, set alarm flag
Udp Attacks

3.2.5 XMAS Attack Detection:

Alert tcp any any : any any (msg: "X mas attack detected" flow: stateless; flags: **FPU**,12; sid: 1234556;)

3.2.6 Fraggle Attack Detection:

alert udp $EXTERNAL_NET any : $HOME_NET any (msg:"UDP_Flood Attack!!!!!"; content:"UDP Flood Test"; flow:stateless; threshold:type threshold, track

by_dst, count 1000, seconds 60; classtype:attempted-dos; sid:1000001; rev:7;)

3.3 Defence Against Attack(Attack Prevention algorithms)

For Prevention Purpose we used iptable/Netfilter , fwSnort firewall which is deployed on host machine which is in inline mode on network gateway, Examples of Firewall which is currently available in Market are Squid, CCProxy , KerioWinroute , WinGate which can be used for writing the attack prevention rule.

3.3.1 ICMP Flood/Ping Flood Prevention Rule

INPUT iptable rule:
iptables :A INPUT :p ICMP s <src_ip> d <dst_ip> -j DROP
where A : append rules ,p : set policy for the chain for the given target, s : source specifications , d : destination specifications

3.3.2 Smurf attack Prevention rule

$iptables -A INPUT p ICMP icmp type echo request m pkttype pkttype broadcast j DROP
Where A : append rules, p: set policy for the chain for the given target,s : source specifications ,j : specifies the action if match found, d : destination specifications m -> match option

3.3.3 SYN Flood Attack Prevention Rule:

INPUT iptable rule: ***iptables -A INPUT -p tcp -d <dst_ip> --tcp-flags ALL SYN -j DROP***
where ,A -> append, rules,p -> set policy for the chain for the given target, j -> specifies the target of the rule(what to do if find a match), d -> destination specifications

3.3.4 Land Attack Prevention rule:

iptables -A INPUT -s 172.18.61.50/32 -j DROP
iptables -I INPUT -s ${my_ip} -d ${my_ip} -j DROP

3.3.5 XMAS Attack Prevention rule:

iptables -A INPUT -p tcp –tcp-flags ALL FIN,PSH,URG -j DROP
Where ALL = all flags set ,
FIN = Finish flag, PSH =Push flag, URG = Urgent flag will be set

3.3.6 Fraggle Attack Prevention rule:

$iptables A INPUT p UDP m pkttype pkt-type broadcast j DROP

$iptables A INPUT p UDP-m limit --limit 3/s j ACCEPT
Where A = append rules, p = set policy for the chain for the given target
s = source specifications, j = specifies the action if match found
d = destination specifications, m = match option

4. Conclusion

Critical literature survey is made in order to carry this work. Security of Campus Wide Network (CWN) was an afterthought at the outset. Enterprise's general purpose Application firewall / IDS evolved in way that has created conundrum for security. So, prime goal is provide emerging solution which gives hybrid functionality of Intrusion Detection System (IDS), Intrusion Prevention System (IPS),, and Firewall functionality in single box which would be practical and easy to maintain.
We have studied various packet generation tools such as Nmap, Nessus, hping3 and Scapy. Then we have made experimentation for the detection of attacks using the open source tools such as Snort IDS, NIDES, HONEYPOT KESENSOR, HONEYD, TRIPWIRE, then we run the various firewalls such as iptable/Netfilter, fwSnort Squid, CCProxy, Kerio Winroute, WinGate in order to write a attack prevention rule. The proposed software for the defence against attacks deals with the attack generation, detection, prevention of the attacks. We considered attacks on ICMP, UDP and TCP Packet.

References

[1] J. Zongpu , L. Shufen, and W. Guowei, "Research and Design of NIDS Based on Linux Firewall," in , 2006.
[2] http://www.snort.org , www.Silicondefense.org , www.sdl.sri.com/projects/nides/ , www.Keyfocus.com
[3] J. 2. "Internet Domain Survey. (January 2001) Internet Software Consortium,. [Online]. HYPERLINK "file:///H:¥¥,%20http:¥¥www.isc.org¥¥", ttp://www.isc.org/
[4] Netcraft. (April 2012) "The Netcraft Web Server Survey", [Online]"http://www.netcraft.com/survey/" http://www.netcraft.com/survey/
[5] CERT/CC Statistics. (2012,) Computer Emergency Response Teams Coordination Center. [Online]. "http://www.cert.org/stats/cert_stats.html" http://www.cert.org/stats/cert_stats.html
[6] Gibson. GibsonResearch corporate. [Online]. "https://www.grc.com" https://www.grc.com
[7] R. K. C. Chang, "Defending against Flooding-Based Defending against Flooding-Based".
[8] V. Varadharajan, "Internet Filtering Issues and Challenges," in , 2010.

[9] www.triwire.com , www.Honeyd.org
[10] J. Reynolds, and J. Postel. (October 1994,) "Assigned Numbers", RFC 1700,. [Online]. "http://www.ietf.org/rfc/rfc1700.txt" http://www.ietf.org/rfc/rfc1700.txt
[11] K. E. P. Srisuresh. (January 2001,) "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022,. [Online].http://www.ietf.org/rfc/rfc3022.txt" http://www.ietf.org/rfc/rfc3022.txt
[12] D. C. Plummer. (November 1982,) "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware", RFC 826,. [Online]. HYPERLINK "http://www.ietf.org/rfc/rfc826.txt" http://www.ietf.org/rfc/rfc826.txt
[13] Richard Power, ""2001 CSI/FBI Computer Crime and Security Survey",," in Computer Security Institute, Computer Security Issues & Trends, http://www.gocsi.com/prelea_000321.htm, Sprin 2001.
[14] Richard Bartley. (March 2001,) "Corporate Information Security Strategy − how to avoid giving free information to attackers",. [Online]. HYPERLINK "http://www.xinetica.com/tech_explained/general/avoid_giving_free_info/wp_avoid_giving_free_info.htm" http://www.xinetica.com/tech_explained/general/avoid_giving_free_info/wp_avoid_giving_free_info.htm
[15] Rainforest Puppy. (May 2001) "Whisker information, scripts, and updates",. [Online]. HYPERLINK "http://www.wiretrip.net/rfp/p/doc.asp?id=21" http://www.wiretrip.net/rfp/p/doc.asp?id=21
[16] Lance Spitzner. (May 2000) "Know Your Enemy: Passive Fingerprinting",Honeypot Project, . [Online]. HYPERLINK "http://project.honeynet.org/papers/finger/" http://project.honeynet.org/papers/finger/

Premchand Bhagwan Ambhore: received the B.E. Computer Science and Engineering Degree from at Government College of Engineering Amravati, India, in 1995 and M.E.Computer Science and Engineering 2004, respectively. He is currently PhD student at the Department of Computer Engineering at the Government College of Engineering Amravati, His research interest in firewall, IDS; System includes information security, and network security.

Bandu B.Meshram: He is Professor and Head of Computer Technology Department of V.J.T.I. Matunga Mumbai. received the Ph.D. (2003) Computer Engineering, M.E. (1995) Electronics Engineering B.E. (1991) Computer Engineering From SGGS Institute Of Technology, Nanded(Autonomous Institute) Summary of Experience is Ph. D Guide: 10 students in Progress M.Tech (Computer Engineering) Guide: More than 60 Projects B.Tech (Computer Engineering) Guide: More than 80 Projects Organized Conferences and workshops at VJTI Delivered Lectures at workshops and Conferences Obtained sponsored lab of worth Rs. 1 Crore from Newtech Computers Ltd. Mumbai Interview expert at MPSC, MHADA, Nehru Science Centre, University etc. Prepared proposals for AICTE, HRD For research and Development. MHADA Consultant. Administration at Institute and Department Level Analysis and Design of Campus Wide Network, VJTI Signed the MOU with Industries for consultancy and Fund raising Editor for the Journal of **“**International Journal of electronic and Computer. Research Publications are Patent -01, National Journal -01, International Journal -70, National Conferences-38, and International Conferences-91.