ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Network Security and Management Using HIDS

T. Hari Prasadh [1], P.Jennifer[*2]

[1] Assistant Professor, Master of Computer Application, Jerusalem College of Engineering, Chennai, India

[2*] Associate Professor, Master of Computer Application, Bharath University, Chennai, India

ABSTRACT: The Host based intrusion detection system (HIDS). This is mainly for detecting the intrusions that are occurred in the hosts. An intrusion is somebody attempting to break into or misuse your computer system. This can be something as severe as stealing confidential data or misusing your email system for spam. An "Intrusion Detection System (IDS)" is mainly for detecting the intrusions.

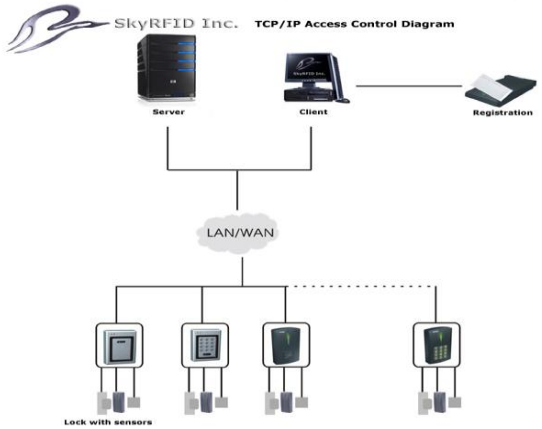
KEYWORDS*:* Port Scanner, net stat command, ping, tcpdump and pine for mail checking.

I.INTRODUCTION

A host based intrusion detection system does not monitor the network traffic, rather it monitors what is happening on the actual target machine. It does this by monitoring security event logs or checking for changes to the system. For example changes to critical system files or to the systems registry. System administrators are constantly being advised to check their systems for open ports and services that might be running that are either unintended or unnecessary.

The most common host-based tool for checking for open ports on Windows or Unix systems is the **netstat** command. But running this command means actually walking or remotely accessing each and every server; and you miss other host systems that might be listening on improper ports.A port scanner is an important tool in the security manager's toolkit. It has, like all of the best security tools today, both offensive and deensive capabilities.

II. DESIGN



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

III.PORT SCAN

A *Port Scan* is one of the most popular reconnaissance techniques attackers use to discover services they can break into [1]. All machines connected to a Local Area Network (LAN) or Internet run many services that listen at well-known and not so well known ports. A port scan helps the attacker find which ports are available (i.e., what service might be listing to a port). Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed further for weakness [2].

A *Port scan* is like ringing the doorbell to see whether someone's at home. The police usually can't do anything about it. They have to wait until a crime is committed. The police might give it more consideration if the doorbell is repeatedly rang causing the homeowner to complain of harassment. Sometimes, if a computer system is affected too much by a port scan, one can argue that the port scan was, in fact, a denial-of-service (DoS) attack, which is usually an offense [3].

The various techniques used in a port scan are summarized below.

Port Scan - Port Numbers

As you know, public IP addresses are controlled by worldwide registrars, and are unique globally [4]. Port numbers are not so controlled, but over the decades certain ports have become standard for certain services. The port numbers are unique only within a computer system. Port numbers are 16-bit unsigned numbers. The port numbers are divided into three ranges:

- Well Known Ports (0 - 1023)
- Registered Ports (1024 - 49151)
- Dynamic and/or Private Ports (49152 - 65535)

Well-Known Ports

Ports numbered 0 to 1023 are considered well known (also called standard ports) and are assigned to services by the IANA (Internet Assigned Numbers Authority) [5]. Here are a few samples:

- echo - 7/tcp - Echo
- ftp-data - 20/udp - File Transfer [Default Data]
- ftp - 21/tcp - File Transfer [Control]
- ssh - 22/tcp - SSH Remote Login Protocol
- telnet - 23/tcp - Telnet
- domain - 53/udp - Domain Name Server
- www-http - 80/tcp - World Wide Web HTTP

Non-Standard Ports

By a non-standard port, we simply mean a port whose number is higher than 1023 [6]. In this range also, several services are "standard." For example:

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

- wins - 1512/tcp # Microsoft Windows Internet Name Service
- radius 1812/udp # RADIUS authentication protocol

Some malicious programs such as Trojans and Viruses have spread so wide that there are a number of ports that if found open, usually indicate that a system may have a virus.

Simple Port Scan Techniques

The simplest port scan tries (i.e., sends a carefully constructed packet with a chosen destination port number) each of the ports from 0 to 65535 on the victim to see which ones are open [7].

TCP connect():

The connect() system call provided by an OS is used to open a connection to very interesting port on the machine. If the port is listening, connect() will succeed, otherwise the port isn't reachable [8].

Strobe :

A strobe does a narrower scan, only looking for those services the attacker knows how to exploit. The name comes from one of the original TCP scanning programs, though now virtually all scanning tools include this feature [9].

The ident protocol allows for the disclosure of the username of the owner of any process connected via TCP, even if that process didn't initiate the connection. So, e.g., one can connect to port 80 and then use identd to find out whether the HTTP server is running as root [10].

Stealth port scan

One problem, from the perspective of the attacker attempting to scan a port, is that services listening on these ports log scans. They see an incoming connection, but no data, so an error is logged. There exist a number of stealth scan techniques to avoid this. A stealth scan is a kind of scan that is designed to go undetected by auditing tools [11]. Obviously, this is a race between the hacker and firewall vendors – what are considered stealth scans now may not be so in a few months once the firewall. **vendor becomes aware of such techniques.**

Port scanners scan a host rapidly by firing off packets at different ports. So, scanning very slowly (taking a day or more) becomes a stealth technique. Another stealth scanning technique is "inverse mapping", where you try to find out all hosts on a network by generating "host unreachable" ICMP-messages for those IPs that do not exist [12]. Since these messages may be generated by any TCP/IP packet one may send meaningless packets .

IV.TCP DUMP

Tcpdump is a powerful tool that allows us to sniff network packets and make some statistical analysis out of those dumps. One major drawback to tcpdump is the size of the flat file containing the text output. But tcpdump allows us to precisely see all the traffic and enables us to create statistical monitoring scripts.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

In our case, looking at an ethernet segment, tcpdump operates by putting the network card into promiscuous mode in order to capture all the packets going through the wire. Tcpdump runs using BSD Packet Filter (BPF) which is the method of collecting data from this network interface running into promiscuous mode. BPF receives copies from the driver of sent packets and received packets. Before traveling through the kernel all the way up to the user process the user can set a filter so only interesting packets go through the Kernel. SUN OS uses Network Interface Tap (NIT) which only allows to capture packets received from the interface but no packets sent by the host. Still the SUN OS tcpdump does the trick but it performs its own filtering at the user process level which means that more data goes through the kernel.

What do we Measure:

We use tcpdump to measure the response time and the packet loss percentages. It can also tell us about lack of reachability for some distant server.Using tcpdump we have a view on any TCP/UDP connection Establishment and Termination. TCP uses a special mechanism to set and close connections (we will discuss this later on); we measure the time lapse between the packets involved with this mechanism in order to know how fast some connections operate.

timestamp source -> destination : flags

Flags can be any of the list

S -> SYN (Synchronize sequence numbers - Connection establishment)
F -> FIN (Ending of sending by sender - Connection termination)
R -> RST (Reset connection)
P -> PSH (Push data)
. (No flag is set)

We can also find ACK (Acknowledgement) and URG (Urgent) flags following the ones above.

Line 1 :
1412042008:1412042008(0) is the sequence number of the packet and the number of data sent.

starting sequence number:ending sequence number(data bytes)

Line 2 :
This is the acknowledgement of the following packet; ack 1412042009 means that packet number 1412042008 has been received and 1412042009 can be sent. What we're interested in is the connection establishment and termination. It takes three segments to open a connection and four to close it.

Mechanism for opening a connection :

The three way handshake can be described as follows :

1. The client sends a SYN segment with the port number of the server it wants to connect to and the client's initial sequence number (Line1).

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

2. The server responds with its own SYN segment containing its initial sequence number (Line 2). This segment also contains an ack flag. So this segment acknowledges the client SYN (segment 1412042008 +1).

3. The client acknowledges this SYN from the server by sending another segment containing the "." flag and ack (Line 3).

Mechanism for closing a connection :

TCP is full-duplex which means that data can flow in either direction and in an independent manner. Either of the two communication ends can send an end of transmission segment (containing the FIN flag) when it has finished transmitting data. This FIN is usually the consequence of an application's CLOSE command. It is said that the first host to issue a FIN performs the active close , then the other and second one becomes the passive close. Usually applications don't take advantage of the fact that you can still send data in one direction having the other one closed.

V.PINE

Pine® is the University of Washington's "**P**rogram for **I**nternet **N**ews and **E**mail." It is intended to be an easy-to--+use program for sending, receiving, and filing Internet electronic mail messages and Internet News (Usenet) messages. Pine supports the following Internet protocols and specifications:

- SMTP Simple Mail Transport Protocol
- MIME Multipurpose Internet Mail Extensions
- IMAP Internet Message Access Protocol
- NNTP Network News Transport Protocol

MIME allows you to attach any kind of file to your message, provided that your recipient also has MIME-capable mail software (which is readily available for most types of computers, although some proprietary mail systems do not yet support MIME). IMAP allows access to mailboxes on remote mailservers as if they were local.

Although originally designed for inexperienced email users, Pine has evolved to support many advanced features. There are an ever-growing number of configuration and personal-preference options, though which of them are available to you is determined by your local system managers.

What PINE Does...

Pine is a "mail user agent" (MUA), which is a program that allows you to compose and read messages using Internet mail standards. (Whether you can correspond with others on the Internet depends on whether or not your computer is connected to the Internet.) Pine also allows reading and posting messages on the Internet Usenet News system, provided that your site operates a suitable news server.

VI.LOG FILES MONITORING

In order to trace any unwanted activity on your computer, you should keep complete and accurate logs. On Linux machines, logging is handled by the syslog daemon, syslogd. Syslogd reads its configuration from the /etc/syslog.conf

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

file. You can set the facilities to be logged, the log priority, and the files in which to log information here. The default values in most distributions do not give you enough information.

Log files of systems and applications contain invaluable information such as operation status & results, errors, and much more. Monitoring the log files helps IT administrators to know the performance of the systems and mission critical applications such as Oracle, SAP, ERP, IIS, etc. in real-time.

OpManager offers agent-based log file monitoring to monitor system and application logs. The agent deployed on the end Windows system monitors the text log files in real-time

A sensible log policy is to log almost everything in /var/log/messages and /var/log/syslog and then to have each individual facility log to its own separate file, as shown in the example below:

--- Begin Example syslog.conf-----

```
# Log anything 'info' or higher, but lower than 'warn'.
# Exclude mail.  This is logged elsewhere.
*.info;*.!warn;mail.none                -/var/log/messages
# Log anything 'warn' or higher.
# Exclude mail.  This is logged elsewhere.
*.warn;                                 -/var/log/syslog

# Debugging information is logged here.
*.=debug                                -/var/log/debug

# Kernel related logs:
kern.*                                                          -/var/log/kernel

# Private authentication message logging:
authpriv.*                              -/var/log/secure

# Cron related logs:
cron.*                                  -/var/log/cron

# Mail related logs:
mail.*                                  -/var/log/maillog

# Daemon related logs:
daemon.*                                -/var/log/daemonlog

# User related logs:
user.*                                  -/var/log/userlog

# Mark logs:
```

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

mark.* -/var/log/marklog

Emergency level messages go to all users consoles:
*.emerg *
--- End Example syslog.conf-----

Note the dash before the log files' names. This tells syslogd not to sync after every log. The disadvantage of this is that log information may be lost in the event of a system crash. Removing the dash, however, can cause a performance loss with heavy logging. If you want to be able to track logs in real time, you can open a log file using the command tail -f /var/log/messages. In order to keep accurate logs, ensure that your system clock is accurate at all times. You should look to using Network Time Protocol (NTP) to maintain your system clock's accuracy. The easiest way to do this is to regularly run ntpdate some.time server from a cron job.

VII.CONCLUSION

The need for IDS is growing for better protection of information and properties. IDS will be one of the necessary components for internet security. Applied fields of **intrusion** detection systems are easily located in the Internet environment. Progress of **intrusion** detection technology is needed.

REFERENCES

1. http://searchsecurity.techtarget.com/definition/HIDS-NIDS
2. Lydia Caroline M., Vasudevan S.,"Growth and characterization of l-phenylalanine nitric acid, a new organic nonlinear optical material", Materials Letters, ISSN : 0167-577X, 63(1) (2009) pp. 41-44.
3. http://www.hidglobal.com/partners/networked-access
4. Langeswaran K., Gowthamkumar S., Vijayaprakash S., Revathy R., Balasubramanian M.P., "Influence of limonin on Wnt signalling molecule in HepG2 cell lines", Journal of Natural Science, Biology and Medicine, ISSN : 0976-9668, 4(1) (2013) PP. 126-133.
5. http://www.hidglobal.com/press-releases/hid-global-omnikey-dsp-software-drives-converged-physical-access-and-network-security
6. Jayalakshmi T., Krishnamoorthy P., Ramesh Kumar G., Sivamani P., "Optimization of culture conditions for keratinase production in Streptomyces sp. JRS19 for chick feather wastes degradation", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 3(4) (2011) PP.498-503.
7. http://en.wikipedia.org/wiki/Host-based_intrusion_detection_system
8. Jebaraj S., Iniyan S., "Renewable energy programmes in India", International Journal of Global Energy Issues, ISSN : 0954-7118, 26(4Mar) (2006) PP.232-257.
9. http://www.darkreading.com/privacy/hid-global-and-consortium-partners-recei/240163214
10. Gopalakrishnan K., Prem Jeya Kumar M., Sundeep Aanand J., Udayakumar R., "Thermal properties of doped azopolyester and its application", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) PP. 4722-4725.
11. http://www- 03.ibm.com/software/products/en/subcategory/SWI30
12. http://blog.buypsa.com/blog/bid/308540/Using-HID-Global-s-EasyLobby-Visitor-Management-System-to-Enhance-Facility-Security.
13. B Karthik, TVU Kirankumar, MS Raj, E BharathKumaran,Simulation and Implementation of Speech Compression Algorithm in VLSI, Middle-East Journal of Scientific Research 20 (9), PP 1091-1092, 2013
14. M.Sundararajan & R.Pugazhanthi," Human finger print recognition based biometric security using wavelet analysis", Publication of International Journal of Artificial Intelligent and Computational Research, Vol.2. No.2. pp.97-100(July-Dec 2010).
15. .M.Sundararajan & E.Kanniga," Modeling and Characterization of DCO using Pass Transistor", proceeding of Springer – Lecturer Notes in Electrical Engineering-2011 Vol. 86, pp. 451-457(2011). ISSN 1876-1100.(Ref. Jor- Anne-II)
16. .M.Sundararajan & C.Lakshmi, "Wavelet based finger print identification for effective biometric security", Publication of Elixir Advanced Engineering Informatics-35(2011)-pp.2830-2832.
17. .M.Sundararajan, "Optical Instrument for correlative analysis of human ECG and Breathing Signal" Publications of International Journal of Biomedical Engineering and Technology- Vol. 6, No.4, pp. 350-362 (2011). ISSN 1752-6418.(Ref. Jor-Anne-I
18. M.Sundararajan, C.Lakshmi & D.Malathi, "Performance Analysis Restoration filter for satellite Images" Publications of Research Journal of Computer Systems