International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-5, Issue-8)

Research Article | **August 2016**

Proactive Network and Surveillance Frame Work Based on Onion Model Defense

Dr. M. P. Vani
Assoc. Prof. SITE, Vellore Institute of Technology,
Vellore, Tamilnadu, India

Abstract:

Security has its root to care for, or be concerned about computer system. The security in computer networks is considered as rapidity growth based on the safety from threats. There is no place where the network has no rapidity in daily lives, let it be in the field of academic or business environment there is proliferation of network. These small networks are further connected to larger networks. The priniciple method of communication on the internet is the TCP/IP. The basis for internet was an experiment which began in 1968 by the defence department information processing techniques office (ARPA/IPTO) to connect computers over a network inorder to ensure command and control over network communications in the event of Nuclear war. The original network was known as ARPA net. In 1980 the number of local area network incremented and this stimulated rapid growth of interconnections to the ARPA Net and other networks. These network interconnection are known today as Internet.

Keyword: TCP, IP, ARPA, IPTO, enamologic, proliferation.

I. INTRODUCTION

Primary network stake holders Hosts and Domain: Computers that communicate across the Internet are known as host computer or simply hosts [SG96] a hosts connection to the Internet can be continuous or part time. Time, it can be through dialup or directconnection [Lot96] . Each host computer is identified by both a unique 32 bit IP address and FQDNC (Fully qualified domain name) out of each of these two parts one specifies the host computer and another specifies the location of the host computer. IP address are generally written as four decimal numbers each between 0 and 255 and each representing an 8 octet of the address. The numbers are separated by a dots and the notation is called dotted decimal notation. E.g. 172.31.1.6.

1.1 World Internet Usage and population statistics:

Letter has estimated the growth in the number of host and domainson the internet since 1981m since 1986 estimates were made using the zone (zeolite of Name Edification) program [Lot92]. In July 1996, the internet connected together a minimum of approximately 13 million host computers. In July 197, the Domain survey was not able to count a significant portion of the hosts in the domain.

1.2 A Preamble to Network security:

Security is optimized by lack of access, connectivity is optimized by complete access. Internet enabled organizations wireless connectivity and roaming clientage have made network peripheral relatively transparent. All the protocols, design techniques and troubleshooting method were not defined or engineered with much thought of security because the Internet underlying technology were developed among collegial group of scientists and engineers during 1970's. In a computer network technological aspects are often the strongest point of defence from the outside attacks.

A Firewall or IDS can do nothing to protect against inside attacks, rather a firewall can provide a false sense of security because it is common assumption that the firewall blocks all unwanted access which is not completely true-firewall allows many type of Traffic to pass, some of which may be malicious. Inside threats, although they create some of the most hazardous and ubiquitous risks to networks. Networks are often overlooked by security strategies [RB04]. Every network security implementation is based on some model which could be either specified or assumed. Mostly perimeter security model is based on Firewalls and/or IDS.

Keeping this in view, it is proposed to design and develop, a proactive network surveillance framework. The framework aims to provide learning vision to the network attacks. The objective of this paper is to bring improved network security through:

- Exploring and analysing various Exploits and their detrimental effects on the network security.
- Exploring various Honeypots and Analyzing their work
- Configuring Honeypots at workplace.
- Development of a proactive network surveillance frame work.
- Creating a bootable Enhaced Linux distributor , to analyze and enhance security
- Deployment and testing of the framework.
- Learning and monitoring network in real time.

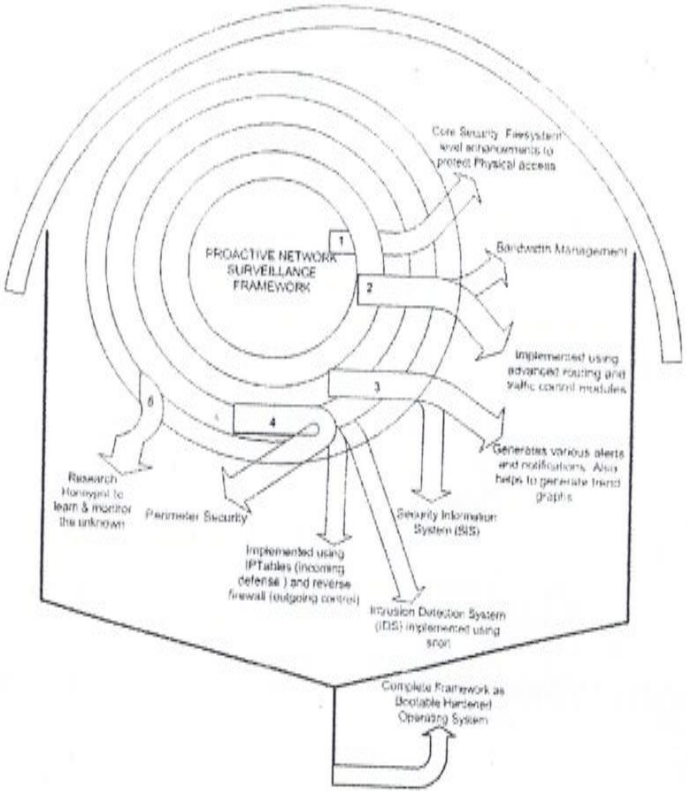
II. PROPOSEDPROACTIVE NETWORK SUREVEILLANCE FRAMEWORK

Design and implementation details.

The framework consists of layer-by-layer similar to onion model of defence where each layer has a predefined job to perform. The five layer comprises of the complete framework visualized at various maturity level with a associated functionality that in some case already exist in the solution. For example in one layer it identifies proactive defence measure, whereas in other layer it addresses physical security issues. The whole layer is controlled by the third layer using web interface as well as SSH access to the administrative clients. SSH is a strategy to allow only public key method of login. SSH command line access displays a simple menu driven interface for controlling the other layer.

Core security layer:

This layer addresses the physical security issue and ensures that only authorized nodes with appropriate public private key pair is able to access the system. This layer also recommends changes in the file system level to enhance physical security of the installed framework.



Ftg: 1: Proposed Framework

Implementation details:

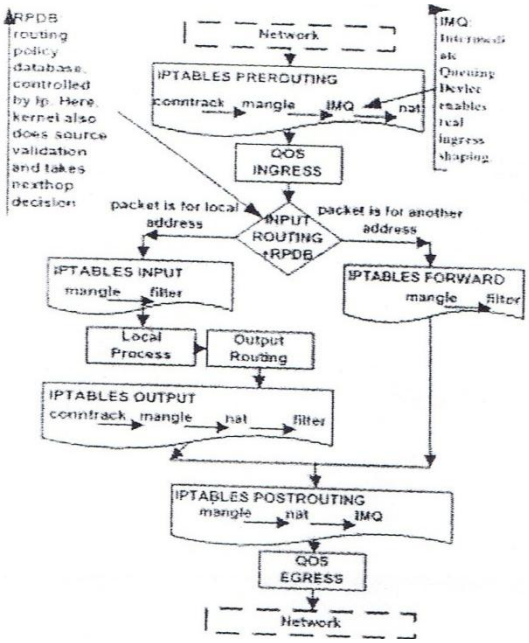


Fig: 2: Packets Journey Through Kernel

A loadable module which implements a file system must register that file system with the (virtual file system) (VFS) layer.

The new file system Initialization code is as given below:

```
int –initnewfs—register(void0
{
return register-filesystem(&newfs_type);
}
```

Where newfs_type structure is setup as

The basic data structure which describes a filesystem type to the kernel is as shown below.

```
Static structfile_system_typenewfs_type
{
   Owner=This_Module,
   Name=”newfs”
get_sb=newfs_get_sb,
kill_sb=kill_litter_super;
};
```

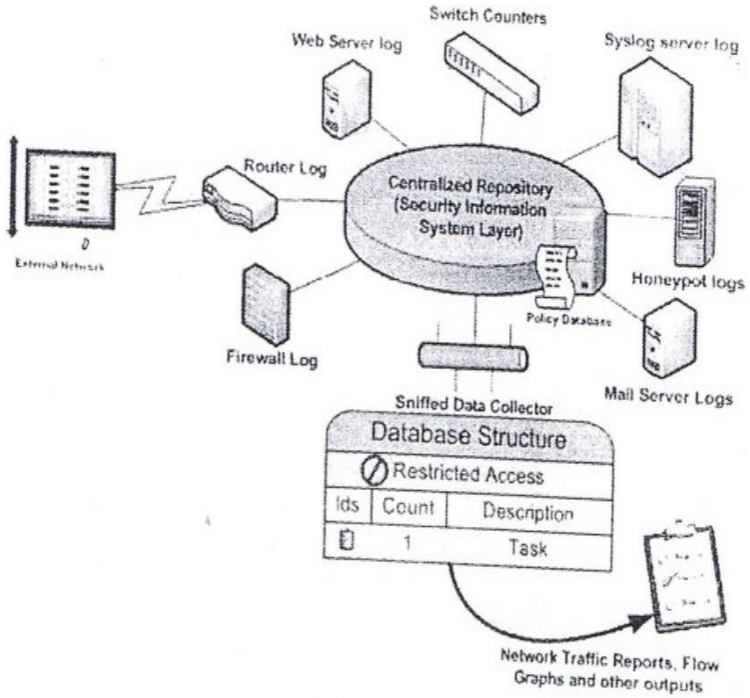


Fig: 3: Security Information System Layer

Implementation details: SSH login key-pair

Step1: establish only SSH based password-free login procedure.
Step 2: Machine presents a login screen usually when hacker attempts to logon.
Step 3: The prompting for the password by the user is avoided by the SSH password free login.
Step 4: only the designated machine whose public key is already copied on to the server will have access to the machine.
Step5: secondly no password need to be remembered one restriction is that log-on can be achieved from the designated machine only.
Classification of outbound and inbound packet is done with the help of IP tables

For outbound Traffic:

Step1: Mark all packets as 0*03 as this is default to place all the packets into the lowest priority queue.
Step2: Mark ICMP packets as 0X00. This will force ping to show the latency for the highest priority packets.
Step 3: Mark all packet that have destination port 1024 or as 0x01 in order to give priority to SSH service.
Step 4: Mark all packets that have destination port of 25 (SMTP) as 0x03, inoder to avoid the swaming of large attachments sent by someone through an email.
Step 5: Mark “small” packets as 0x02

For inbound Traffic:

Step1: place all non-TCP traffic in the 0x00 class.
Step2: place “small” TCP packets also in 0x00 class.
Step3: place all TCP traffic in the 0x01 class.

Both Inbound and Outbound traffic routing control demonstrates the usefulness of the routing and traffic control.

Security information system layer: this layer reduces the complexitby giving intelligence to the network. This layer helps in providing report and detailed analysis of network Logs.it helps in identifying malfunctioning nodes on the

network sending malicious traffic. The framework consists of desparate data from firewall, IDS(intrusion detection system,mysql history logs, operating environment logs,ssh logs integrated with daemon web logs, mail logs,and trend logs these form the basis of real time data generation over the network.

Implementation details:
Step1: framework establishes the startup flow through inittab
Step 2: then flowing through the rc.d/init.d/rc.sysinit script.
Step 3: re.sysinit allows to do customization.

Inittab:
```
  # Run gettys in standard runlevels
1:2345:resoawn:/sbin/mingetty tty1
rc.sysinit:
#let's dump the syslog ring somewhere so we can find it later
dmesg –s 131072 > /var/log/dmesg
#create the crash indicator flag to warn on crashes, offer fsck with timeout touch/.autofsck
Sleep 1
Kill – TERM '/sbin/pidofgetkey' >/dev/null 2>&1
} &
If ["$PROMPT" != "NO"]; then /sbin/getkeyni&& touch /var/run/confirm
fi
wait
/bin/sh /etc/startup.sh
cp –f /etc/rc.sysinit.org /etc/rc.d/rc.sysinit
```
step 4: after initialization is done admin users is offered a shell with startup script
following script snippet shows the experts from /etc/passwd file and user.sh file:
```
/etc/passwd:
ldap:x:55:55:LDAP User:/var/lib/mysql:/bin/bash
mysql:x:27:27:MyySQL Server:/var/lib/mysql:/bin/bash
admin:x:0:0::/home/admin:/usr/local/user.sh
/usr/local/commands/user.sh: #!/bin/sh
Commands () {echo "command available: arp, arping, clear, cpuinfo, dmesg, diskuse, exit, ifconfig, ip, ismod, meminfo, netstat, ping, quit, reboot,route, shutdown, tc, tcpdump, telnet, traceroute, uptime "}
Main() { echo "command shell" shell}
Main
```
User is given a jailed environment, where onlt specified command can be executed. SSH as per the core security layer.Perimeter security layer: it sites the placement of reactive security components within the network hierarchy and implements network traffic regulation rules based on network profiles and policies this layer also implements intrusion detection mechanism

Implementation details:
Firewalls are implemented using a dedicated or a non-dedicated firewall hardware and system platform. Proposed framework implemented firewall based on IP tables under non-dedicated mode. "proper installation" is achieved by means of operating system hardening and mainly for this reason no service going beyond the necessary minimumis run on the framework.

Three independent switch configuration s with External, Internal and DMZ(Demilitarized zone) is proposed.

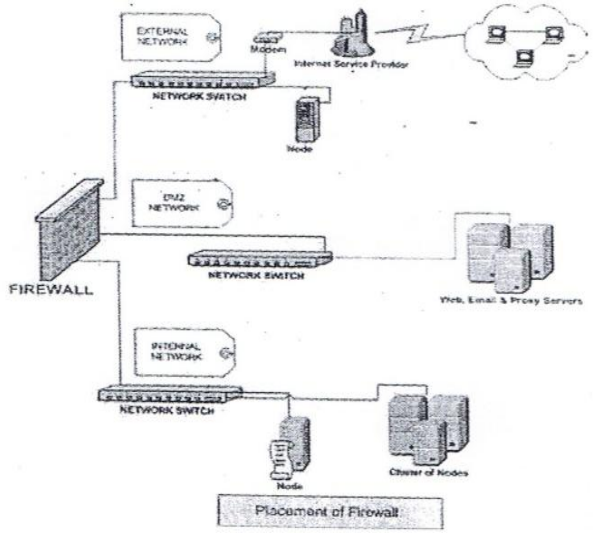


Fig: 4: Firewall Placement Inside Network Security Hierarchy

Example firewall rules are following in nature:

1. External To DMZMail External ANY (External) w.x.y.z (DMZ) MailServices Accept
2. External HTTP Masq
   Internal To External

1. Internal to external 192.168.1.2 (Internal) 0.0.0.0/0 (External) All services Masq framework follows the flow-graph for the implementation of the firewall. IPTables script pfwall.sh (code snippet is as below)is started at the system runtime from/etc/re.d/init/iptables script.

#Set the connection outbound limits for different protocols.

SCALE="hour" #second, minute, hour, etc.

TCPRATE="15" # Number of TCP connections per $SCALE

UDPRATE="20" #Number of UDP connections per $SCALE

OTHERRATE="15" #Number of other IP connections per $SCALE

Implementation details: IDS

IDS is used as in proposed framework as second line of defense inside perimetric layer security.

Step1: in the proposed framework network intrusion detection is used.

Step2: each Snort rule describes the features of a packet which are the characteristics of known attacks.

Step3: signature database consists of known attack signatures.

Step4: the rules are expressed in asci format it has two rules rule header and rule option.

Snippet illustration of sample Snort rule,

alerttcp any any -> 192.168.1.0/24 111 (content:"100 01 86 a5|";msg:"mounted access";)

Implementation details: Hardening Steps

Many unwanted programs were installed by default, so in the proposed framework setup was selected to entirely layout own Linux distribution which is customized for robustness. The LFS (Linux from scratch) system was built by using a previously installed Red Hat Linux distribution. This base system consisted of all compiler, linker, and assembler tools installed to build a new system. After successful compilation of various packages as per [Bee06], following hardening steps are carried out, by an automated script "hardos.sh".

Step1: if physical access is viable one can boot linux into single user modeby typing following command LILO :linex single (if LILO is the boot loader)

GRUB:kernel/boot/vmlinuz-2.6.9-34ELsmp ro root=LABEL=/ single (in case if GRUB is the boot loader.

Step2:proposed framework made following changes by modifying the /etc/inittab file as follows:

id:3:initdefault: changed it to –

id:3:initdefault: :S:wait:/sbin/sulogin

this will need the root password before continuing to boot inti single –user mode

Step3: Set login time out for root account: TMOUT variable is settime in seconds by editing /etc/profile file TMOUT T-1800 this auto logout will apply for all users

Step4: disabling shutdown command : this is done by removingca::ctrlaltdel: /sbin/shutdown –t3 –r now from the /etc/inittab file.

Step 5: the /etc/security file: in the proposed framework /etc/security has following contents

[root@proactive /etc]# lesssecuretty tty1, tty2, vc/1 this will not allow root to login from tty1,tty2 and vc/1.

Step 6: changing attributes of other important files In the proposed framework it is by default mounted as read-write.--

#chmod R 700 /etc/rc.d/init.d/* changed to cp –f /etc/issue /etc/issue.net

Step 7:securing root owned programs in OS hardening step suid bit is disabled with chmod command.

[root@proactive /] # chmod a-s /bin/ping

Implementation details: Honeypot:

It simulates virtual hosts on a network and it is efficiently used in the fifth layer of the proposed framework. A virtual honeypot is simulated by different machine that answers to network traffic sent to the virtual honeypot.

To simulate virtual network, a cisco router personality is created and binded to the 172.31.1.100/24 IP address

Step1: create the router

Step2: set router personality "Cisco IOS 11.3 – 12.0(11)"

Step3: set router default tcp action reset

Step4:set router default udp action reset

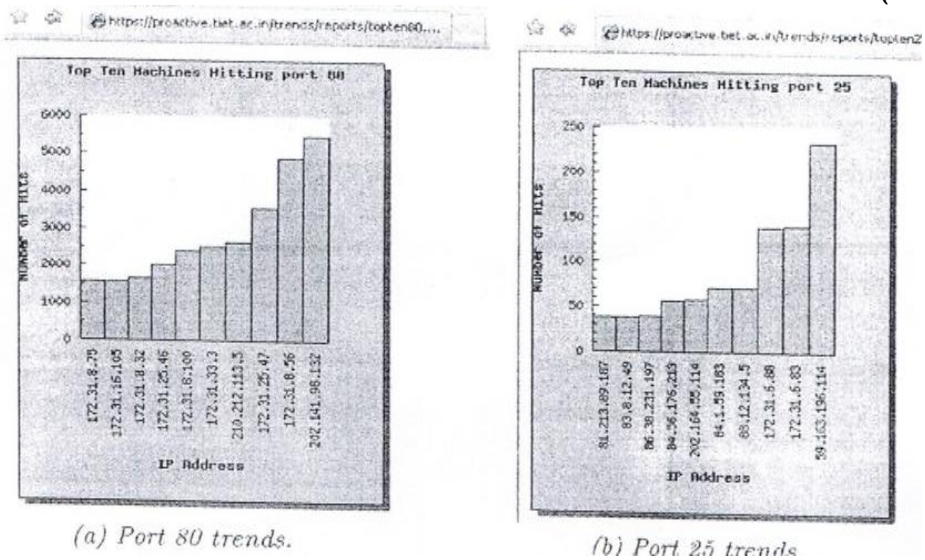
Step5: add router tcp port 23 "/usr/bin/per1 scripts/router/cisco

Step6: /router-telnet.p1"

Step7:set router uid 32767 gip 32767

Step8:set router uptime 5184000

Step 9:bind 172.31.1.100 router



(a) Port 80 trends. (b) Port 25 trends

Fig: 5: Bar Graph Showing Machines Hitting Port 80 and 25

III. CONCLUSION AND FUTURE ENHANCEMENT

Proactive network surveillance framework is proposed designed and implemented. The framework is based on onion model of defence. The first layer design of new file system would provide a secure mounting, this layer architecture gives complete defence in depth within routing and traffic control. The core security level in the second layer use IMQ which is emphasized for both egress and ingress shaping. The third layer use database logging and trend generation to give the details of the implementation report. The fourth layer recommends the placement of reactive security within network hierarchyand implemented IPtables and Snort.fifth layer implements hardening steps and low interaction honeypot.

in future this research can be put on dedicated hardware platform with embedded linux functionality,another point which is left is integration of the database dumps into graph generation engine manual work of graph takes lot of effort and lot of steps this portion of work also can be automated

REFERENCES

[1] Gene Spafford Simson Garfinkel practical UNIX and internet security:second edition o'reilly&associates,Inc 1996[SG96].
[2] D.Litchfieldwindows Heap Overflows http://blackhat.com/presentations/win-usa-01/bh-win-04-litchfield/bh-win-04-litchfield.ppt, 2004 [Lit04].
[3] Mahindersingh, seemabawa and s.csaxena" proactive network surveillance framework for improving security."international review on computersand software (IRECOS) vol1.july 2006 pp 43-51.
[4] Marcus J Ranum, False Positives: a users guide to making sense of IDS Alarms. ICSA labs IDSC, 2003.
[5] Marty Roesch Snort, opensource Intrusion Detection system http://www.snort.org.1998.
[6] W.richardstevens. UNIX Network programming Prentice Hall, NJ.,1990.
[7] Lance Spitzner. HoneyPots: tracking hackers. Addison-Wesley, 2003
[8] William Stallings. Network and Internet security Principles and practice, Prentice Hall, EnglewoodCliffs.N.J., 1995.

