International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 14 (2014), pp. 1395-1402

http://www. irphouse.com

Study of Protocols Associated Security Attacks and Proposing Simplified Method for Improvisation

Kuldeep Tomar[1] and S.S. Tyagi[2]

[1]Research Scholar, Department of CSE, MRIU, Faridabad, Haryana
[2] Department of CSE, MRIU, Faridabad, Haryana

Abstract-

With the enormous growth in the usage of computer and communication networks, security threats and security breaches has also increased. Recent survey reports state that not only the large organisations but even smaller organisations are also rapidly targeted. Smaller networks face many types of attacks, but recently the attacks which are initiated or performed by exploiting Protocols has created greater challenges for keeping network secure. There are mechanisms already available for countering these attacks but due to rapid change in technology they are not enough. Also few mechanisms are very complex and very costly, thus it becomes very difficult for small organisations to implement them. In this paper we would first analyze the different types or network attacks, especially which are generated by exploiting protocols. To have an efficient protection mechanism operating system plays an important role. Linux operating system seems to be a better option for providing secure environment because of it is open source, good architecture, tools etc., so we would propose a simplified mechanism which can enhance computer network security for smaller networks.

Keywords: Attacks, Threats, Protocols, Security, Network.

1. INTRODUCTION TO NETWORK SECURITY

With the enormous growth in the usage of computers and communication networks, security threats have also increased. Recent survey reports states that not only large business organisations have faced this threats but even smaller organization are also being targeted. Thus it is very important to secure one internal computer network from network security breaches. To understand Network Security we need to understand its two main components network and security. Definition of security can be:

1. Freedom from any threat or danger.
2. Impediment of threat or risk.

As per fundamental information hypothesis [1], security is accomplished by some essential properties like integrity, information Availability and confidentiality. A computer network is interconnection of two or more computer to share information and data. Even smaller computer networks are being rapidly attacked by many ways. There are many security threats which affect our computer network's few of them are described in next paragraph.

2. NETWORK SECURITY THREATS

Following are few network security threats:

1. **Intrusion Attack:** when unauthorized user achieve access from network to use the system.
2. **Denial-of-service Attack:** DOS is another type of attack on the Internet through which the network will be exhaust [2]. It is of two type:

a. Ping of death
b. SYN attack

3. **Spoofing Attack:** this type of attack is generated by attacker by spoofing the IP through which unauthorized user can alter the packet at Transport layer.
4. **Application level Attack:** This type of attack generally comes at application level. The kind of software as viruses comes at this level.
5. **Protocol based Attacks:** communication between one or more computers and from one network to another is done using protocols. Protocols are some set of standard rules that used to transfer data on the internet or network.

3. PROTOCOL BASED SECURITY ISSUES

As we know protocols are the set of rules so unauthorized user can change the rule and spoof the data. Some of the protocols based issues are given below:

1. **Predicting the Sequence number of TCP:** as we know protocols helps to communicate the user from one network to another and sending the data from one computer to more when data send through the TCP protocol and one can predict the sequence number of TCP [3].
2. **RIP Attack:** as we know the router is route the packet from source to destination as when unauthorized user can attack on the routing information so data will send from source to another unauthorized destination so this is also the major security issue in the protocol [3].
3. **Trojan Attack:** it is another major issue in protocol security. Trojan attack is basically generated at application level and it will use the protocol HTTP and IRC at this level to breach the security of the network [4].
4. **Message reply Attack:** This type of attack is on the authenticity of system so this attack is on the authentication key and protocol [5].

5. **SIP Attack:** SIP is session initiation protocol which uses the HTTP due to the interruption service [6] or flooding of message attack [7] in this protocol it lose data integrity, authenticity as in.

4. ISSUES IN PREVENTION MECHANISM BASED ON PROTOCOL BASED THREATS

There are already mechanisms available which can be used to address issues above. In this paper we wish to propose a simple mechanism which would be user friendly, open source and can enhance security. Because few of the existing mechanisms are very complex to use and only skilled administrator or a person of good computer knowledge can apply that. Also few are very costly. Our proposed approach is very simple and can be effective to block protocols when needed.

5. LINUX BASED PROTOCOLS BLOCKING SYSTEM (LBPS)

Here, we will be denying communicating or entertaining certain protocols, person responsible for maintaining network would be allowing or blocking protocols. Let us say if he felt FTP operations should not be allowed so he would feed in the name of the protocol and then with the help of script written and Linux tools that protocol would be blocked and if it needed to be allowed then it would be allowed.

As we know Protocols are some set of standard rules that are uses for transferring messages or say transferring packet over the network without hampering the actual contents of the packet. Often other protocols are used very frequently with the Internet protocol for data that for one reason or another must have extremely high fidelity. Below is the activity diagram of the proposed system, where at the initial state a person with a very basic knowledge can act as system administrator, can switch on the Linux server containing our script, i.e server mounting and the can proceed to selection of protocol name. Then with a simple command (sh) he/she can run the script provide the protocol to block, if it is already present then override else would add the name to the database i.e black list and further with our script and Linux tools and utilities that protocol would be blocked.

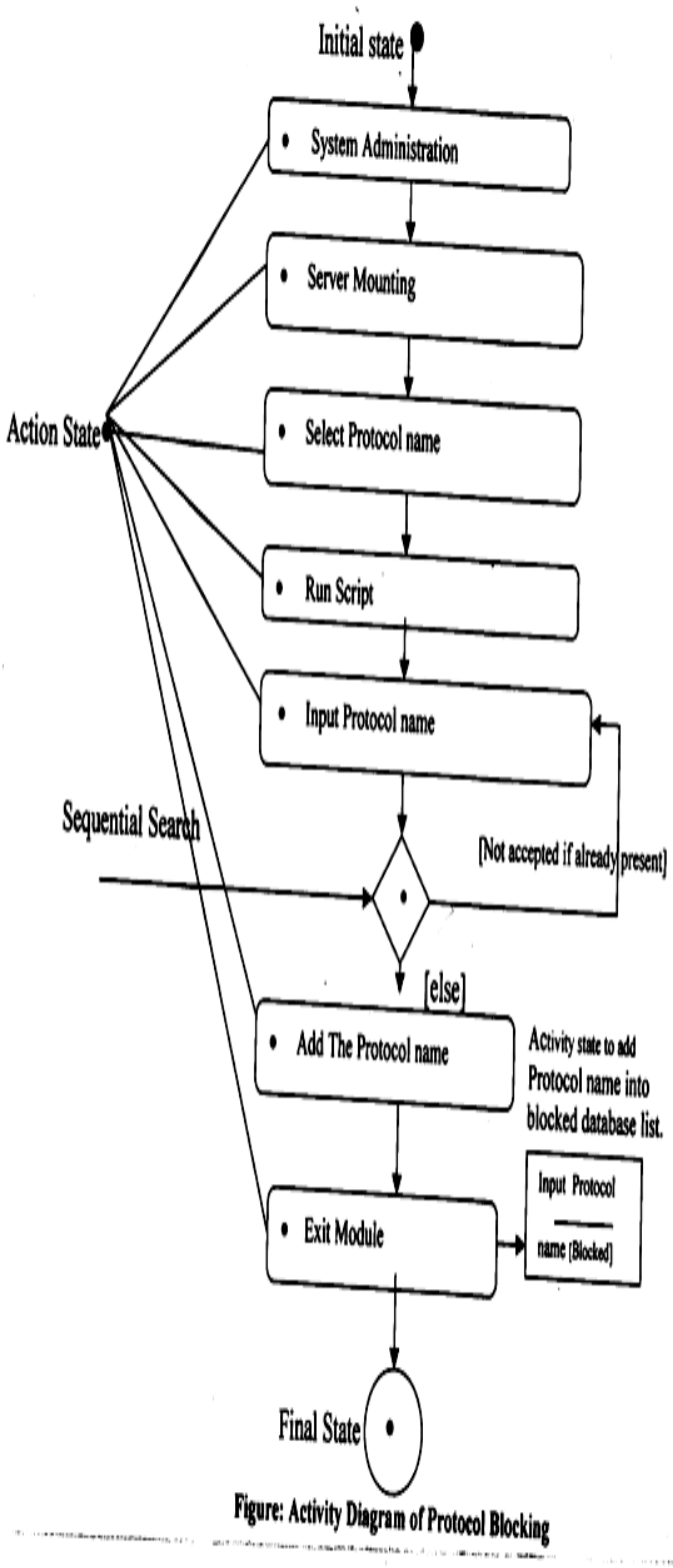

Fig. 1: Activity Diagram of LBPS

5.1 SIMULATED ENVIRONMENT IN LINUX (FEDORA)

The simulated environment is developed using Linux (Shell Script) as scripting language is a menu based system which will work in steps. In our scripts we will use the help of Linux inbuilt tools & utilities as well as would be implementing advanced algorithm for the efficient working of the module.

6. SHELL SCRIPT FOR PROTOCOL BLOCKING:

Few basic shell scripts of our proposed LBPS system are below:

6.1 PROTOBLOCK.sh

```
echo -e "\n\n\t\t\t\t  \033[1;36;44m PROTOCOL BLOCKING \033[0m"
echo\n\n\t\t\033[1;34m@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@\
n\t\t@\t\t\t\t\t\t\t\t@\n\t\t@\033[0m\033[1;31m\t\tEnter
Protocol\033[34m\t\t\t\t\t@\n\t\t@\t\t
\t\033[1;35m1. Enter the Protocol to
block\t\t\t\t\033[1;34m@\n\t\t@\t\t\t\033[1;35m2. Enter the Protocol to
allow\t\t\t\t\033[1;34m@\n\t\t@\t\t\t\033[1;35m Enter your
choice\033[1;31m\t\t\t@\t\t\n\t\t@\t\t\t\t\t\t\t\t@\n\t\t@\t\t\t\t\t\t\t\t@\n\t\t@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@\033[0m"
tput cup 13 50
read num
 if [ $num -eq 1 ]
then clear
./protoblock1.sh
elif [ $num -eq 2 ]
then clear
./protoblock2.sh
else clear
./mainmenu.sh
Fi
```

6.2 PROTOBLOCK1.sh

```
clear
echo "Please enter protocol name to block"
read v1
echo $v1 >> /etc/blockedproto
```

6.3 PROTOBLOCK2.sh

```
clear
echo "Please enter the protocol name to be deleted"
read n1
echo $n1 >> deleteproto
```

```
if grep -v "$n1" /etc/blockedproto > /etc/f4
then
cat /etc/f4 > /etc/blockedproto
cat /etc/blockedproto
else
echo"no"
fi
```

In the above scripts we have used some files names like blockedproto, mainmenu.sh, deleteproto etc which are the files which contain our own scripts and few act as black lists (database) files.

7. WORKING OF LBPS

This blocking technique is used to block the services provided by protocol for example HTTP, FTP. One thing all users using internet know that if protocol is blocked we can't access do variety of things like blocking FTP means that one can't perform file transfer transactions in network because it also plays role of utility for Linux. The process as follows:-

NAME – When a user enters the name of protocol, the action will be taken at same time by restarting the SQUID services and the protocol will be blocked.

OPEN – Now to open protocol services users have to delete the protocol name from the .sh file, to access the services provided by that protocol etc.

8. SCREEN SHOT OF PROTOCOL BLOCKING:

Shown below is just one of the screens shot of our work there few others also.

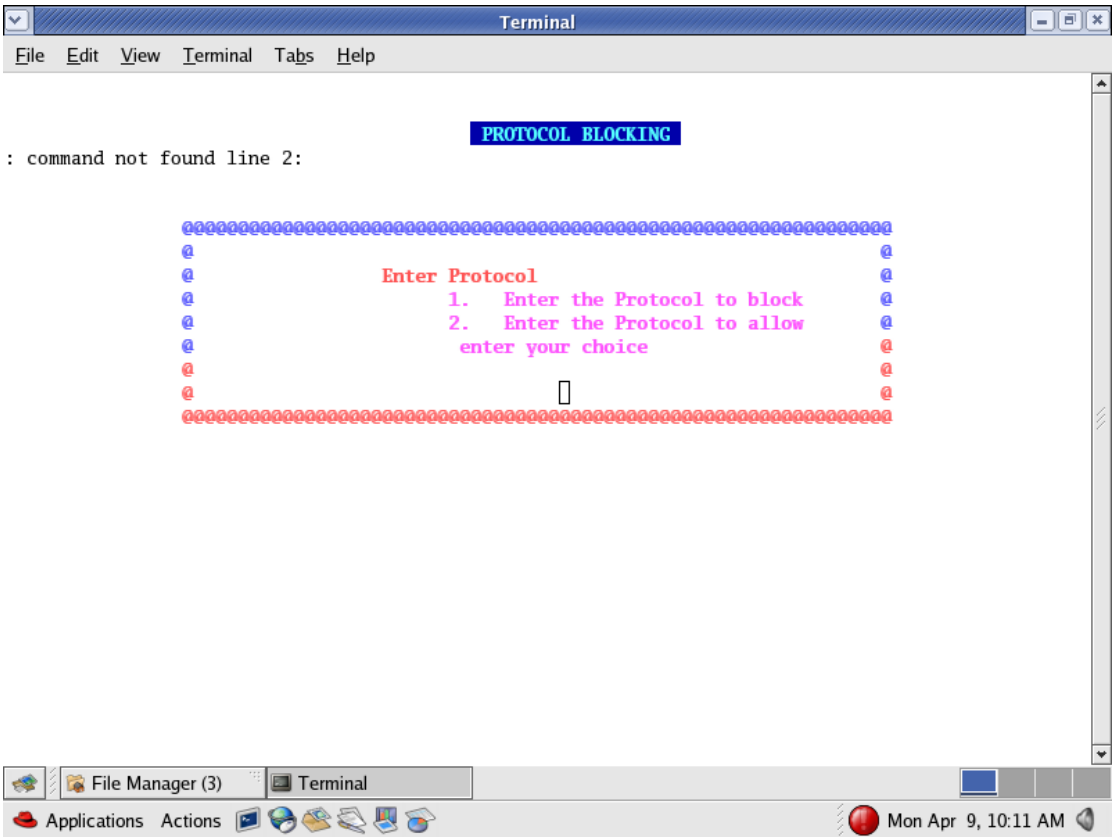

Fig. 2: Protocol blocking

9. CONCLUSION AND FUTURE WORK

Several tools have been developed to provide security for computer networks, preventing networks from attacks completely is a very difficult task. So as to enforce security completely then we may have to compromise with certain privileges. Security is a very difficult topic. Everyone has a different idea about ``security'' is, and up to what level we can compromise with the risk. We have to be very clear while defining security levels within our organization. This proposed work can be effective enough to deal with many threats and provides a much safe network communications. Our proposed script is very easy to implement with a little knowledge of basic commands of Linux. That system proposed is very simple and can provide security because it will only have our script. This work can describe types of protocol based security issues and a simplified mechanism which can provide security to a smaller network or a computer which can make our communication over the network more secure. When we had started developing the script, it was only meant to be for home use but as we went on with it we realized that it could be further extended and we can use advance ACL's and pattern matching algorithms to make it a professional tool, which can be used, in corporate networks.

REFERNCES

[1] A.J. Menezes P.C Oorschot, and S.A Vanstone, “Handbook of applied Cryptography”, CRC Press, Boca Raton FL, 1997.

[2] Panayiotis kotzanikolaou, Christos douligeris, “Computer network security: basic background and current issues”, institute of electrical and electronics engineers, Inc. 2007.

[3] S.M. bellovin, “Security problem in TCP/IP protocol suite”, Computer Communication Review, Vol. 19, No. 2, pp. 32-48, April 1989.

[4] Sílvia Farraposo, Laurent Gallon, Philippe Owezarski, “Network security and DOS attack”. April 2005.

[5] Sen Xu, Manton Metthews, Chin-Tsar Huang, “Security issue in privacy and key management protocols of IEEE 802.16”, ACM SE’06, Melbourne, Florida, USA, March 10-12, 2006.

[6] Aws Naser Jaber, Chen-Wei Tan,Selvakumar Manickam and Ali Abdulrazzaq Khudher, “Session Initiation Protocol Security: A Brief Review”, Journal of Computer Science 8 (3): 348-357, 2012.

[7] Gaston Ormazabal, Sarvesh Nagpal, Eilon Yardeni, and Henning Schulzrinne, “Secure SIP: A Scalable Prevention Mechanism for DoS Attacks on SIP Based VoIP Systems”, Springer-Verlag Berlin Heidelberg 2008.