XVIII IMEKO WORLD CONGRESS
Metrology for a Sustainable Development
September, 17 – 22, 2006, Rio de Janeiro, Brazil

THE SECURITY OF LINUX SERVERS WITH A VIA NETWORK MONITORING AND CONTROL SYSTEM

Miroslav Matýsek [1], *Milan Adámek* [2], *Petr Neumann* [3]

[1] Tomas Bata University in Zlín, Faculty of Applied Informatics, Czech Republic, matysek@fai.utb.cz
[2] Tomas Bata University in Zlín, Faculty of Applied Informatics, Czech Republic, adamek@fai.utb.cz
[3] Tomas Bata University in Zlín, Faculty of Applied Informatics, Czech Republic, neumann@fai.utb.cz

Abstract: With regard to repeated assaults from Internet area on Linux servers where the monitoring and controlling system based on the TCP/IP protocol has been debugged and tested, there was designed and applied an effective firewall based on packet filtering for those servers. This firewall is able to defend the Linux server against most common attacks. Our own Linux distribution based on Debian/GNU distribution was designed and debugged. This distribution is loadable from a CD or a compact flash memory in case of an unfiltered Internet attack.

Keywords: Safeguard of Linux servers, Network monitoring and controlling system, TCP/IP protocol, Heartbeat.

1. INTRODUCTION

The computer security or information security or data security have a complex content and we can perceive them in many levels. The information system generally process and it stores data holding information. The typical information system covers hardware, software and data. These three items are assets worth to be protected against passive or active threats and attacks.

2. FIREWALL

The firewall is a program, which controls the access to the protected network together with the router. The controlled access to the network from the outer unprotected area is the main concern of commercial Internet users running their local networks. They are also the pillars of private networks like intranet and extranet. The firewalls are reconfigurable programs which setup designates the restriction rate on passing packets. The firewall configuration corresponds to the security politics of the organization running the protected network. The firewall is a barrier defending the network against the unauthorized accesses, i.e. against direct attacks. The firewall cannot protect the network against the indirect attacks like the misuse of authorized access (like hitting the password, for instance).

It must to protect various local networks because of database servers and website servers (company, university, state organization servers) which are attack-target-object more and more nowadays.

2.1. The Firewall varieties

2.1.1. The Packet firewall

This procedure filters and let through the IP, TCP or UDP protocol data packets according to the header parameters analysis. It is possible to allow or suppress explicitly particular network services. The higher security grade represents the specification of allowed network services offered by the protected local network servers.

There is possible to arrange by means of packet filtering for particular protocols like TELNET, HTTP, HTTPS, POP, News clients and some others such a situation when local network clients have the open doorway to Internet servers but Internet clients do not have access to intranet.

However, the operation of FTP, SMTP protocols and UDP based application protocols (namely DNS) is slightly questionable. The FTP protocol problem is solved by the help of so-called passive FTP. The SMTP and DNS problem is untwisted with the exclusive communication between Internet and intranet license for only one particular computer.

The UDP protocol problems are solved by the means of so-called active filters. That procedure makes it possible to send datagram from the local network to the Internet but responses are accepted only in a very short time period. Unexpected responses are thrown away.

2.1.2. The Proxy server

The Proxy servers represent a special arrangement where the firewall interposes the client transaction between the outer unprotected network and the inner protected network server. The end-points if such communication channels are not directly connected. They are composed from two separated connections.

The firewall becomes the check point where data comply with rules fixed for a particular sort of network service. Now, the client communicates with the proxy server that transfers its requirements to the server and vice versa, the

server responses are transformed in messages for the client. The real IP addresses of the servers do not appear in the responses for the client.

The proxy server can act as a circuit level gateway or application gateway. the circuit level gateway evaluates the transport relations unlike the application gateway controls access to the local network according to the rules conditioned for the particular network service or for the particular user data format (data streams for the H.323 video data format, for instance).

The application gateways act in a much more sophisticated way than packet filters and circuit gateways which decide depending on the header data whether to let packet in or block it. We differentiate among following proxies:

The standard proxy – the client logins to the proxy and tells it the target server name. The proxy connects him with the target server. The standard proxy apply namely for FTP, TELNET, HTTP and HTTPS protocols.

Generic proxy – the client cannot tell proxy the name of target server because he is unable to do it and that is why the generic proxy is directed to only one particular target server. The generic proxy applies for POP protocols, news reading, company applications etc. Transparent proxy – the client addresses the target server directly.

The transparent proxy accepts the connection to the target server and it learns the target server address from the accepted datagram and the client proxy area can set the link to the server immediately. From the client point of view, the transparent proxy appears as a router so that the client does not know about the proxy existence between him and the server. The transparent proxy applies namely for TELNET and FTP protocols.

Transparent generic proxy – whereas the generic proxy enables the connection to one particular server for various clients, the transparent generic proxy enables the connection to various servers for various clients. The transparent generic proxy is oriented namely at company applications.

2.1.3. State filters

State multilayer inspection gateways are according their function range the most complex and consequently most demanding firewalls in the technological aspect. Their activity is based on the dynamic filtering of incoming packets. They function with protocol state tables across the TCP/IP architecture layers. They can perform a contextual decision making on accepting packets to the protected local network following the precedent states knowledge.

3. THE FIREWALL IMPLEMENTATION IN LINUX

3.1. The basic facts and history

There is a firewall implemented directly in the core in OS Linux. The utility IPFWDM has been available since the core version 2.0. The utility IPCHAINS was available in core version 2.2. The Net-filter/IP-tables utility is inbuilt in current core version 2.4 and unlike its foregoers, it includes many innovations.

3.2. The important Linux core settings

The following options are necessary to be set in the Linux core for the correct function of the Net-filter:

CONFIG_PACKET,
CONFIG_NETFILTER,
CONFIG_IP_NF_CONNTRACK,
CONFIG_IP_NF_FTP,
CONFIG_IP_NF_IPTABLES,
CONFIG_IP_NF_FILTER,
CONFIG_IP_NF_NAT,
CONFIG_IP_NF_MATCH_STATE,
CONFIG_IP_NF_TARGET_LOG,
CONFIG_IP_NF_MATCH_LIMIT,
CONFIG_IP_NF_TARGET_MASQUERADE.

3.3 The packet route via Net-filter

There are three tables to be passed through by a packet in the net-filter. These tables are MANGLE, NAT a FILTER. Each table contains items called “chain”. According to the packet destination, its route goes via various chains in various tables. The packet route is illustrated in the Fig.1.

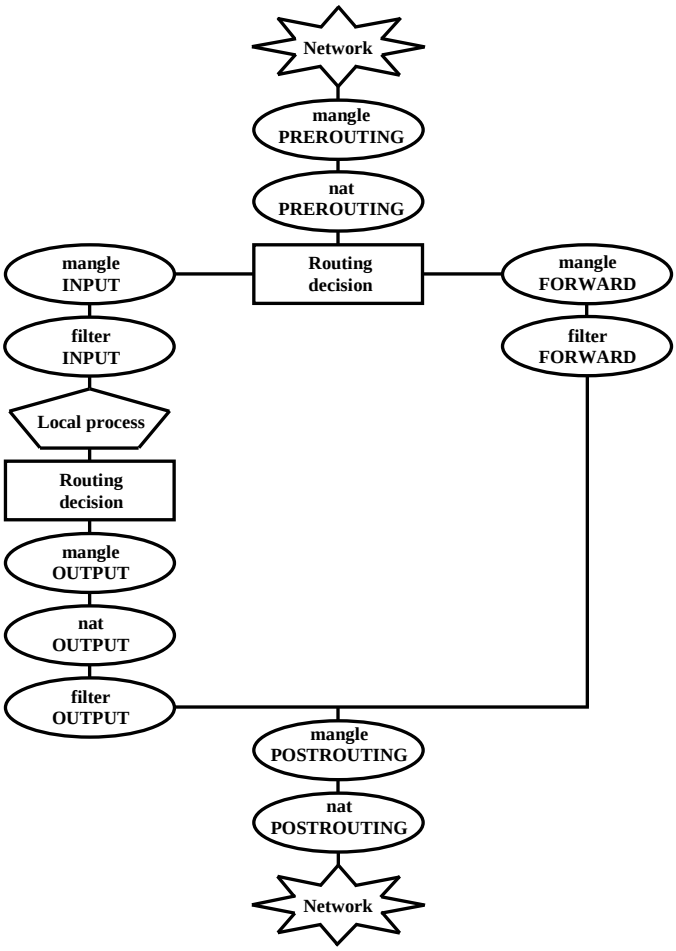

Fig. 1. The packet route

We discern three different packet destinations: the packet is specified for a local service from network, the packet is send out from a local service into network and the packet is forwarded from network to network, e.g. from Internet to localnet. In this case date goes through tables mangle PREROUTING, nat PREROUTING, mangle FORWARD, filter FORWARD, mangle POSTROUTING and nat POSTROUTING.

4. THE HEARTBEAT PRINCIPLE

The basic High-Availability cluster consists of two nodes at least (www.linux-ha.org). Those nodes can be interconnected with the RS232 or SCSI cable. Such connections are called non-IP heartbeat. We can use also Ethernet (interface eth1) and the communication is ensured with the help of UDP protocol. These interconnections are recommended to combine in such a way that the nodes have more communication possibilities to find out their actual state. The UDP communication in the Ethernet is enciphered and we can choose from MD2, MD5, SHA1.

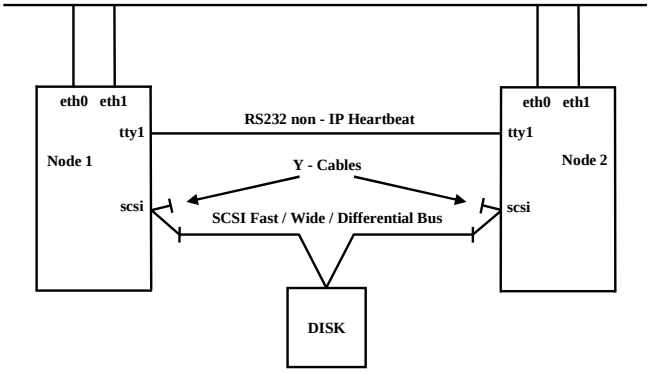

Fig. 2. Heartbeat

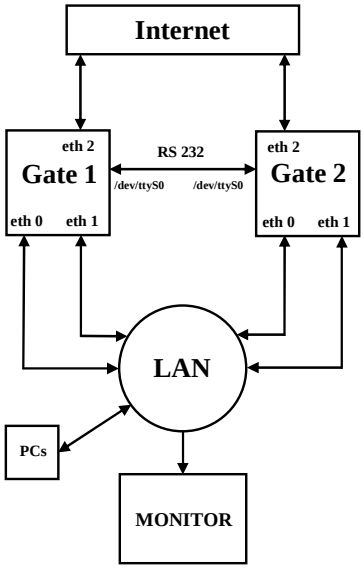

Fig. 3. The final firewall version block diagram

5. THE APPLIED REALISATION

We have applied the above stated theoretical piece of knowledge in the final stage and we have realised the OS Linux distribution bootable from a CD-ROM. Furthermore, we have created floppy discs with configurations for individual nods (Gate 1, Gate 2) and the Monitor system configuration.

We have selected the Debian/GNU Linux distribution as an initial distribution but any other distribution could bring same results.

Gate1 and Gate 2 in the Fig. 3, work in heartbeat system and they communicate between themselves via RS232 and Ethernet card, interface eth1. Gate 1 and Gate 2 are diskless stations. Monitor is a disc station, it monitors heartbeat system, e.g. Syslog of Gate 1 and Gate 2.

Internet is a non secure network and LAN behind firewall on Gate 1 and Gate 2 is a secure network. PCs are stations, on which the network monitoring and control system runs.

5.1. The ISO CD-ROM creation

The operation system installation from a CD-ROM can be performed with the help of the Isolinux tool (http://syslinux.zytor.com). There is necessary to have an Isolinux directory with the isolinux.bin loader and its configuration isolinux.cfg. The kernel should be located in the same directory. If we have a CD-RW drive, we can create an ISO image (root_fs) and burn it.

5.2. The installation from a Compact Flash

As the start from a Flash memory with a standard Lilo loader was knotty, we have employed the Syslinux for the system boot. The configuration resembles the Isolinux. However, Syslinux needs a bootable section with the FAT16 file system for its operation.

ACKNOWLEDGMENTS

The work has been supported by the grant VZ 7088352102 the Ministry of Education (MŠMT) of the Czech Republic. This support is very gratefully.

REFERENCES

[1] L. Dostálek, “Velký průvodce TCP/IP protokoly: Bezpečnost”, Praha, Computer Press, 2001, ISBN 80-7226-513-X.

[2] Collective team. 1998. “Linux Dokumentační projekt”, Praha, Computer Press, 1998, ISBN 80-7226-114-2.

[3] A. S. Tanenbaum, A. S. Woodhull, “Operating systems: design and implementation”, Prentice-Hall, 1998, ISBN 0-13-368677-6.

[4] W. R. Stevens, “TI - UNIX network programming”, Prentice-Hall, 1998, ISBN 013490012X.

[5] G. Silberschatz, “*Operating systems concepts*”, John Wiley & sons, Inc., 2002, ISBN 0-471-41743-2.