computing@tanet.edu.te.ua
www.tanet.edu.te.ua/computing

ISSN 1727-6209
International Scientific Journal of Computing

MODERN APPROACH TO PROTECTION OF COMPUTER SYSTEMS AND NETWORKS

Valerij Dudykevych [1)], Andrian Piskozub [2)], Igor Lomnytskyj [3)]

1) Doctor of Technical Sciences, professor, National University "Lvivska Polytechnica",
S. Bandery St., 12, Lviv, 79046, UKRAINE, vdudykev@polynet.lviv.ua
2) PhD, associate professor, National University "Lvivska Polytechnica",
S. Bandery St., 12, Lviv, 79046, UKRAINE, piskozub@polynet.lviv.ua
3) Postgraduate, National University "Lvivska Polytechnica",
S. Bandery St., 12, Lviv, 79046, UKRAINE

Abstract: *This article is dedicated to the use of firewalling method and intrusion detection method, which can be applied both separately and together to computer systems and networks, to expedience of the use of that or other method, tools, that perform these methods. We will try to carry out the analysis of the modern state of security questions in computer networks, to give recommendations how to attain the greatest level of protection of computer systems and networks by most effective way - within the shortest time interval, with minimum financial expenditures.*

Keywords: - *firewalls, intrusion detection systems, scanners, vulnerability assessment tools, penetration testing*

1. INTRODUCTION

Recently the question of providing information security in computer systems and networks (CSN) comes out to one of the leading places by actuality. In literature on information security in CSN a lot of attention is paid to the firewalling method as one of key protection facilities of these systems from unauthorized intrusion. Although the firewalling method is indisputably very effective, what a plenty of firewalls practically for any platforms testifies, but it is not a panacea for providing a 100-percent security of the systems, networks and information, that they contain. There are other effective methods, which not only complement the firewalling method, but also are considered better sometimes from latter as those that provide a higher level of CSN security. This article is dedicated to all these methods, which can be applied both separately, and together to CSN, to expedience of the use of that or other method, tools, that perform these methods. We will try to carry out the analysis of the modern state of security questions in computer networks, to give recommendations how to attain the greatest level of CSN protection by most effective way - within the shortest time interval, with minimum financial expenditures.

2. FIREWALLS: DESCRIPTION, IMPLEMENTATION AND APPLICATION

In world practice the researches connected to the study of security of information systems (IS) of different departments and establishments have been repeatedly carried out. Groups of experts (tiger teams) , invited for this purpose, repeatedly proved, that in most cases a man could not fix the attacks realized during conducting of experiment. Such specialists are used now as well, but services of such experts are expensive and do not guarantee that after some time as a result of changes in computer system configuration, or as a result of exposure of new exploits in software the computer system appears to have the security vulnerability.

As a number and frequency of attacks all time are multiplied, it becomes very important to identify attacks on the early stage of their development and in time react on them. In the critical cases interference in the attack should be realized much faster, than the person can react. Other reason for automation of process of attacks detection consists in more frequent use of the automated facilities of attack realization by intruders.

The IS must be protected. With this thesis nobody argues. To provide safety one should prevent all attempts of unauthorized access by creating the fully safe system. However in practice it cannot be realized for some reasons [l]. At first,

creating the absolutely protected system is impossible due to presence of different errors in software. The error free software is still the dream. And practice is such, that producers not always try to develop such software. They aim to let the product out as quickly as possible and get maximal benefits here. But the most interesting thing is that the security facilities suffer from the presence of different errors as well. One could often hear the reports about the vulnerability exposures found in firewalls, authentication servers, etc. Secondly, even the most secured system surrenders before "expert users". The privileged users can violate the requirements of security policy, which can result in the decline of protection level. And finally, thirdly, the more secured system we have, the less comfortable it is to work with it.

Thus, if we cannot build the absolutely protected system, then we should realize such security policy that will minimize the risk of compromising the system by blocking access to unnecessary services and providing possibility of work for only those applications and those users who require this according to the policy. Firewalls are those facilities that accomplish this task.

Shortly characterizing firewalls, we will mark that there are known three their types – packet filters, application gateways and statefull inspection firewalls, which are chosen according to the following reasons.

Packet filters can block a traffic that passes through firewall using information, which is contained in the headers of packets – type of protocol, source port number and destination port number. This type of firewalls is easily configured, they are considered enough stable and inexpensive comparing with two other types of firewalls. Some packet filters have support of the VPN decisions and enciphering, but these functions are executed in them at a base level and are not compatible with similar decisions of other producers. Packet filters can be both software made and hardware made – the latter are considered the fastest among all types of firewalls. But, unfortunately, packet filters are considered firewalls with the lowest level of security. Packet filters practically do not have facilities for the user management, remote control and other options that the firewalls of other types have. As soon as packet filters conduct monitoring of network layer only, they are vulnerable to IP-spoofing attacks, DoS-attacks (e.g., "ping of death", SYN flood-attacks, etc.). The Cisco PIX firewalls [2] are the most typical representatives of hardware packet filters. FWTK for Unix-platforms [3], Iptables for Linux [4] (although Iptables is considered to be a representative of statefull inspection firewalls as well) are the most typical representatives of software packet filters.

The application gateways are software made and operate on a general purpose hardware with many network operating systems. They are considered to be the most typical representatives of firewalls and offer a lot of functional possibilities, in particular, they have the best level of traffic management (they can look over the packets content) and good possibilities of registration of this traffic. However this type of firewalls has a number of drawbacks – they strongly rely on stability of the operating system, hardware computer components, such as speed of hard disk, processor (especially at enciphering the traffic), productivity of computer and RAM. The application gateways require much more configuration, than packet filters, do not protect against DoS-attacks at a network level. The typical representatives of application gateways are SQUID [5], Microsoft Proxy Server [6], Black Ice [7], and representatives of the improved application gateways (with additional functional possibilities, such as enciphering, VPN-decisions, etc.) – BorderWare [8], Axent Eagle (former Raptor) [9], and NAI Gauntlet [10].

Many security specialists consider the third type of firewalls –statefull inspection firewalls– to be the most scalene and such, that provide the highest security level. Security specialists explain it by the fact that the last type of firewalls is able to connect in themselves the functional possibilities of both packet filters and application gateways. Besides they are able additionally to save state information of network connections in so called "table of the states". In the end, the statefull inspection firewalls have a number of drawbacks – although they operate faster, than application gateways, but do not reach the speed of packet filters. As well as proxy systems, they strongly rely on stability of the operating system. Statefull inspection firewalls also do not provide those proxy services that offer the application gateways (e.g., in case with RealAudio). And finally, statefull inspection firewalls are one of the most difficult products in the class, it is difficult to configure, support them. Therefore they are the most expensive in the class. The typical representatives of statefull inspection firewalls are CheckPoint FireWall-1 [11] and NetGuard Guardian [12].

Marking general lines of firewalls, we will point reasons that testify that securing CSN using only firewalls is insufficient.

There are three stages of attack realization [13]. The first, preparatory stage consists in the search of pre-conditions for realization of that or other attack. On the given stage vulnerabilities are searched, the use of which makes it possible in principle to

perform an attack that is the second stage by itself. On the third stage the attack is completed, tracks are "sweeped", etc. Thus the first and third stages in themselves can be attacks. For example, search made by intruder by means of security scanners such as nmap or Nessus is considered the attack by itself.

The existing security mechanisms, performed in firewalls, work on the second stage only. That is, they are facilities blocking and not preventing attacks. In most cases they protect from the attacks that are already being found in the process of realization. And even if these mechanisms were able to prevent that or other attack, prevention of attacks would be much more effective, that is removal of pre-conditions of realization of penetrations. The complex system of providing information security should work on all three stages of attack realization. And providing adequate protection on the third finishing stage is no less important, than on the first two. Only in this case it is possible really to estimate a loss from the "successful attack", and also develop measures on the removal of subsequent attempts to realize a similar attack.

There are a number of attacks, which neither of the mentioned above three types of firewalls can recognize. It is explained, that firewalls – they are simply the systems, based on the rules that allow or deny passing traffic through them. Even statefull inspection firewalls do not allow saying with exactness, whether attack is present in the traffic or not. They can only report, whether the traffic answers to the rule, or not. The example of such attacks through tunnels in firewalls is the Loki attack, which allows tunneling of different commands in the ICMP Echo Request queries and reactions on them in ICMP Echo Reply answers, that substantially changes the size of the data field in comparison with standard one. One more example of tunneling attacks are attacks on the application level, which are related to practice of vulnerabilities use in the application programs by sending packets, directly related to these application programs. Thus, it is possible to take advantage of "weak point" in Web-server by sending HTTP-command that allows attacker to execute any command on that server.

3. INTRUSION DETECTION SYSTEMS: DESCRIPTION, IMPLEMENTATION AND APPLICATION

Another method of improving the CSN protection level, which effectively complements the firewalling method, is intrusion detection method. Its essence consists in finding all (or practically all) violations of security policy and proper reaction on them. To expose, block and prevent violation of security policy is possible by three ways [13]:

1) recognition of attacks, that are being performed already. In accordance with the mentioned above classification of implementation phases of attacks the given method functions on the second stage and is used in classic intrusion detection systems (IDS);
2) prevention of attacks before their realization. This method will be realized on the first stage of attack realization by search of systems vulnerabilities that can be used for attack realization. The systems, that allow to expose vulnerabilities of IS, are named vulnerability assessment systems or security scanners. Also here belongs another class of facilities of attack detection – deception systems. In our opinion, the new class of facilities under the name penetration testing systems belongs here as well;
3) recognition of attacks on the third stage of attack realization. Systems that operate on this stage expose already performed attacks by means of verification of integrity of resources (system integrity verifiers), and on the basis of log analysis (log file monitors).

We will consider in detail every category of software products that realize the varieties of intrusion detection.

IDS are relatively new systems based on real time recognition of intrusion attempts. The characteristics of IDS-systems are: *strategy of development, information source, methods of attack detections, frequency of implementation of data analysis, reaction on the originating of attack, abuse or abnormal activity.*

Strategy of development of IDS-systems: The IDS-systems are divided into "network-based" (are located on a network) and "host-based" (are located on host) IDS.

Information source for IDS-systems: network-based IDS (NIDS) estimate the information obtained from monitoring the traffic and carry out their analysis for the purpose of attack presence. They contain software, which is installed on separate hosts in the critical places of network – before firewall, Web-server or e-mail server.

Host-based IDS (HIDS) estimate the information obtained from host – it can be contents of the operating system, file system, applications, log files, and so forth. In this case the subject of the analysis can be hosts – workstations, peripheral units (printers), specialized servers (Web-, FTP-servers), network components (firewalls, routers, switches). HIDS use program modules, which are installed on every controlled host, and carry out monitoring of log files and audit records.

Methods of attack detections: there are two methods of detection of network attacks – recognition of attacks by their signature (the rule-

based systems) and detection of anomalies (adaptive systems). In the first method network traffic is compared to known attack signatures, written down in the signature base. This method is simple in realization, gives better results on attack detection, than the second method, however has one substantial drawback– if signature of the given attack is not present in a base, this attack does not turn out. Permanent renewal of signature bases by the firms-producers of these systems is the decision of this problem. The second method which allows to detect the unknown for today attacks, is far heavier in realization, because bounds with area of artificial intelligence and expert systems. The given attacks can be recognized as definite unexpected changes in the conduct of the computer system, for example, sudden increase of traffic, considerable use of resources of central processing unit, activity of hard disk, etc.

In the systems based on rules two approaches are taken: preemptory and reactionary. When using preemptory approach IDS-system really looks over information, that acts on a network and when using reactionary – looks over log files.

Frequency of implementation of data analysis by IDS-systems: depending on the fact how IDS analyses data, there are two variants: data analysis in the real time and data analysis in the mode of data batch processing, which are fixed in log files with definite periodicity.

Reaction on the originating of attack, abuse or abnormal activity: there are two base directions how IDS reacts on the originating of attack, abuse or abnormal activity – passive and active reaction. The passive reaction means simply informing the responsible personnel about the origin of definite event. It can be executed by means of the reports to console, e-mail box, pager, record in log files. The active reaction means definite action from the IDS, indicated by a system administrator, for example, adjustment of system vulnerability, start of the separate program for treatment of concrete event, disconnection of user, selective increase of monitoring, reconfiguring of firewall, disconnection of port, etc.

A lot of IDS of different purposes from different producers are known now, however we will point the list of those products that in our opinion occupy dominant positions in the class.

Among the class of commercial NIDS are the following: Anzen Flight Jacket (AFJ) [14], NetProwler [15], Cisco Systems IDS (Formerly NetRanger) [16], SecureNet PRO [17], SessionWall-3 [18].

Among the class of commercial IDS, that contain both host-based and network-based-components, indisputable leaders are the products RealSecure [19] and Centrax [20].

Among the class of commercial HIDS are the following: Computer Misuse Detection System (CMDS) [21], CyberCop Monitor (CCM) [22], Intruder Alert (ITA) [23], Kane Security Monitor (KSM) [24].

Among the class of freeware NIDS are the following: Snort [25], Hummer (also known as a system HummingBird) [26], AAFID [27], Network Flight Recorder (NFR) [28].

Among the class of freeware HIDS is HostSentry (it is part of Abacus project) [29].

Most known among system integrity verifiers are Tripwire [30] and AIDE [31], among log file monitors – SWATCH [32], Logsurfer [33], and among deception systems – Deception Toolkit [34].

Security scanners, in their turn, are divided into two types – system scanners and network scanners. System scanners analyze the system from the point of view of presence of configuration problems, weak points and potential dangers, detect vulnerabilities of local buffer overflow type, wrong access rights on files or catalogues, etc. Such are freeware scanners COPS and Tiger [35] and commercial product System Scanner (a part of SAFEsuite project) of the American company Internet Security Systems, Inc. [19].

Network scanners recently have received large popularity due to their wide use by intruders as the automated facilities of remote CSN vulnerabilities detection in the Internet. But do not forget that they, first of all, are intended for use by administrators to detect vulnerabilities of their systems. Since we have quite a lot of such programs now, in our opinion, it is advisable to take advantage of recommendations of hacker Fyodor, author of known nmap port scanner, which were formed by him on the basis of questioning members of the mailing list nmap-hackers [36] concerning the list of the best 75 computer security programs (we will consider only security scanners from this list) [37]. Such are nmap port scanner [38], freeware network scanners Nessus [39] and SARA [40] (SARA is a network scanner that was derived from the infamous SATAN scanner), commercial scanners ISS Internet Scanner [19], GFI LANguard [41], Retina [42], SAINT [43], Shadow Security Scanner [44], specialized Web-server scanners – freeware (Whisker/Libwhisker [45], Nikto [46]), commercial software (N-Stealth [47]).

These system scanners are recommended to be used at the initial installation of the host, or network, and then - regularly through the definite interval of time with the purpose of the detection of new vulnerabilities.

The article would be incomplete, if we do not give information about the penetration testing systems.

A penetration test is a localized, time-constrained and authorized attempt to breach the information security architecture of a system using attackers' techniques. Penetration testing or ethical hacking, unlike hacking, has a constructive intent: to improve the IS posture of an organization. Penetration testing goes much further than simple vulnerability auditing. Many of the methodologies used are the same as for vulnerability auditing but it goes much further. Active attempts will be made to exploit the vulnerabilities identified to determine whether they are indeed exploitable. This cannot be done on an automated basis since it involves a variety of different tools and techniques, most often handcrafted, to try and see if penetration is achievable.

But the company Core Security Technologies [48] succeeded in releasing a commercial product under the name CORE IMPACT, which presents the automated system of penetration testing. In contrast to vulnerability scanners IMPACT offers the only comprehensive framework for penetration testing from start to finish, without being reliant on external software packages or varied methodologies. The architecture of CORE IMPACT has among others the following characteristics: a methodology for penetration testing, always current commercial-grade exploit code, transparent pivoting (the execution subsystem of IMPACT permits modules to run from intermediate compromised hosts without modification. This powerful capability allows to stage proxy attacks seamlessly through intermediate hosts. It also elevates the value of exploit code developed inside the framework), complete logging of the tester's activities.

4. CONCLUSION

Summarizing the given material, it is necessary to note that nobody can achieve absolute 100-percent security. Neither security scanners nor IDS are a panacea for securing information in the computer systems, nor are firewalls. And neither will any decision or method taken separately. Here we neither can ignore security of separate hosts nor security of the whole network. The improvement of security level is possible only at the expense of the coordinated actions of many components – first of all, experienced personnel, which skillfully will dispose of mentioned here methods of firewalling, scanning and vulnerability detection.

5. REFERENCES

[1] Aurobindo Sundaram. An introduction to Intrusion Detection. 1996.
[2] http://www.cisco.com/
[3] http://www.fwtk.org
[4] http://www.netfilter.org
[5] http://www.squid.org
[6] http://www.microsoft.com
[7] http://www.networkice.com
[8] http:// www.borderware.com
[9] http://www.axent.com/
[10] http://www.nai.com/
[11] http://www.checkpoint.com
[12] http://www.netguard.com
[13] Lukatskyj A.V. Attack Detection. –SPb.: BHV-Petersburg, 2001.
[14] http://www.anzen.com
[15] http://www.axent.com/
[16] http://www.alliancedatacom.com/manufacturers/ cisco-systems/security_vpn/ids.asp
[17] http://www.intrusion.com/
[18] http://www.abirnet.com
[19] http://www.iss.net/
[20] http://www.cybersafe.com
[21] http://www.ods.com
[22] http://www.nai.com/
[23] http://www2.axent.com/
[24] http://www.intrusion.com/
[25] http://www.snort.org/
[26] http://www.cs.uidaho.edu/~hummer
[27]http://www.cs.purdue.edu/coast/projects/autonomous-agents.html
[28] http://www.nfr.net
[29] http://www.psionic.com/abacus/hostsentry/
[30] http://www.tripwiresecurity.com
[31] http://www.cs.tut.fi/~rammer/aide.html
[32] http://www.stanford.edu/~atkins/swatch/
[33] http://www.cert.dfn.de/eng/logsurf/
[34] http://www.all.net/dtk/dtk.html
[35] http://www.net.tamu.edu/network/tools/tiger.html
[36] http://lists.insecure.org
[37] http://www.insecure.org/tools.html
[38] http://www.insecure.org/
[39] http://www.nessus.org/
[40] http://www-arc.com/sara/
[41] http://www.gfi.com/lannetscan/
[42] http://www.eeye.com/html/Products/Retina/
[43] http://www.saintcorporation.com/saint/
[44] http://www.safety-lab.com/en2/products/1.htm
[45] http://www.wiretrip.net/rfp/
[46] http://www.cirt.net/code/nikto.shtml
[47] http://www.nstalker.com/nstealth/
[48] http://www.coresecurity.com

Dudykevych Valeriy

Graduated from Lviv polytechnic institute in 1963 on the speciality "Electric measuring technique". In 1971 has defended a candidate thesis on the subject "Development and research of digital methods and devices for low and infralow frequencies measurement" and received PhD degree. In 1973 has got academic status of associate professor. In 1991 has defended a doctoral thesis on the subject "Numerical-pulse measuring converters" and received degree of Doctor of Technical Sciences. In 1993 has got academic status of professor. In 1996 was accepted as Member, and in 1997 – as Fellow of Institution of Electrical Engineers (UK). Author of over 200 scientific articles and over 190 patents.

Current position: associate director of Institute of Computer Technologies, Automation and Metrology, head of the department of automation and telemechanics of the National university "Lviv polytechnic".

Areas of interests: transformers of time-frequency parameters of signals, functional converters, technical information security

Piskozub Andrian. *Graduated from Lviv polytechnic institute in 1993 on the speciality "Automation and Telemechanics". In 1997 has defended a candidate thesis on the subject "High accuracy logarithmic analog-to-digital converters" and received PhD degree. In 2002 has got academic status of associate professor. Author of over 20 scientific articles.*

Current position: associate professor at the department of automation and telemechanics of the National university "Lviv polytechnic".

Areas of interests: computer network security, firewalls, intrusion detection systems, scanners, vulnerability assessment tools, penetration testing, computer network and system administration, technical information security.

Lomnytskyj Igor. *Graduated from National university "Lviv polytechnic" in 2001. In 2000 has received a bachelor degree on speciality "Computerized systems of automation and control". In 2001 has received a master's degree on speciality "Information security in computerized systems of automation and control".*

Current position: postgraduate at the department of automation and telemechanics of the National university "Lviv polytechnic". The subject of candidate thesis is "Development and research of high speed cryptographic algorithms of the asymmetric encryption"

Areas of interests: development and research of algorithms and means of asymmetric encryption and decryption that will allow the usage of asymmetric cryptosystems for encryption of data, sound, video and other types of information during transfer in the communication channels in the real time scale