Intrussion detection by penetration test in an organization network

N. Y. Hamisi, Student MIEEE, N. H. Mvungi, MIEEE, D. A. Mfinanga, B. M. M. Mwinyiwiwa, Member, MIEEE
University of Dar es Salaam
P. O. Box 35131,
Dar es Salaam
Tanzania

Abstract— **This paper presents a study made on network security in an organization's local area network (LAN). Intrusion detection test in a campus network was performed using penetration test methods and the results analyzed. The objectives were to identify different form of network attacks and methods used to capture the hacking. During the study, the risks and attacks caused by hackers to the network were evaluated. The results obtained are seen as a good indicator of the security state of the network. Hence, an organization network that responds well to penetration test can be given a certificate. Such certificate will provide a positive sign and confidence to the network users. The study was conducted in a dynamic situation by doing experiments during different periods of time. The case study was a campus LAN, The network administrator permitted network information like internet protocol (IP) address to be gathered and analyzed and to performed the penetration test that enabled , hackers and attackers methods to be dentified. It was realized that 90% of network the users has no fear of the network security risk inspite of the finding that network security rating of the case study is at 50 percent.**

Index Terms – hacker, footprinting, scanning

I. INTRODUCTION

In Tanzania, the application of computer network is still at minimum. According to figures presented by Tanzania Communications and Regulations Authority (TCRA) 2006-2007 annual report [1], about 6,328,099 which is just 16% of the population in Tanzania is using network services. Efforts to bring in many users are on progress, but the network security is considered as a major problem that is hampering the efforts. In developing world, network security has expanded quite significantly over the last decade [2]. Though studies show that despite of the high level of security risk (i.e. 7 to 9 out of 10 [2]), network services are extensively used in the government, enterprises and by individuals. Network security extends beyond protecting the secrets of corporations and governments. It includes consumers sharing resources with others within and outside that LAN. In Universities, academic reports are being processed through networks. In Governments, budget distribution and payments are now relying on centralized network processing. Many network users, prefer to store online their sensitive information. The temptations for those who have the tools to dip and hack the pool of confidential data should, therefore, not be ignored [2].

In developing countries like Tanzania, the existing laws are silent or weak on hacking activities. Network security is another area where efforts to seek new knowledge is vital for professionals. This paper contains the findings from the study going on at the University of Dar es Salaam, about the network threats from network hackers. Our objectives are education: a paramount element in the continual fight against hackers. The study aims to equip those with the network expertise with more information to protect their LANs and the way to respond to different network attacks. The study is meant to compliment other security measures and tests and it gives some kind of security guarantee within a LAN.

In 2001, the industry survey in the United States shows 91% of the survey respondents detected attacks on their companies, while 384 of the surveyed companies reported $380m in financial losses from network services, according to Endler et al hacking threat has exponentially increased than that reported in 2001 [3], [4]. In order to tacle the problems, security professionals need more knowledge than network criminals. Through the University of Dar es Salaam, where the research is being conducted, security knowledge will be expanded, encouraged and enable a new generation of IT security experts to be more security conscious and in turn guaranteeing network security. Hence, this attract more network users. Whereas the government wishes to increase the number of network-resources in its activities, such as payment and taxing systems, procurement activities, voting and banking, the hackers' community has also been growing. As a prevention measure, there is a need to establish some mechanism which will be authorized to penetrate into the network.. That authority appropriately shares information on hackings, threats, vulnerabilities, exploits, crimes and laws. If we are to take control of hackers who has infinite and instant access to the trade's most current tactics and schemes, we must be equipped with more knowledge, taking into account that that hacking has shifted to moneymaking crimes targeting vulnerable information like less protected supplies of countless credit card numbers to old hacker's motivation of notoriety and curiosity that targeted tightly secured installations. The results obtained from this work will be used to educate security professionals and those in administrative roles to provide them with the resources necessary to protect most valuable asset including that of average citizens and their data [4].

It is true that with the expansion of resources of user - created content, the future of the web has become clearly dependent on user's contributions. Hence, a researcher can sell a brilliant idea or research output without involving a physical a bookshop. However, the network must be safe for the users and content, must be kept alive at all times, and it must be prevented from the restrictions based on fear-induced activities

This research is sponsored by University of Dar es Salaam and Sida SAREC – Engineering Capacity Building Project.

978-1-4244-3523-4/09/$25.00©2009 IEEE

and regulations. Such restrictions impede brilliant advances in technology and communications. To guarantee quality of security services, and ensuring that law enforcement agencies, governments, and international collectives are active network users; collaboration among stakeholders and continuous state-of the art research and education are necessary. Investing for research in this area will tremendously help companies and states fight cybercrime [5].

II. METHODOLOGY

We did intrusion detection by penetration test inside a LAN. It was mandatory for us to seek the permission from the network service provider (NSP) to allow us to conduct the test. In return, the NSP had to issue a certificate which was bound to include the following: period and hours of testing, off tests limitations, social engineering, war dialing and driving, denial of services (DoS) and defined boundaries of test end points. Bernado Perazi stated that telling many people about penetration test may invalidate the test although elevation procedures shows that it is risky not to tell [14].

The conducted test was divided into two strategies, which, respectively treated the network and the systems as a black box and a white box. The test was conducted sequentially by using the following techniques: footprinting, scanning, fingerprinting, identification of vulnerable services, exploitation of vulnerability and fixing of the problem [15]. Due to the complexities of network security and the fact that hackers use different methods to penetrate into the network, we used the case study approach. The concept of intrusion detection within the campus network at UDSM was new; hence, there was no established guidance on the way to conduct the study. Therefore, the case study approach was adopted in this work by looking at similar studies that had been carried in other campus networks [14]. This enabled us to explore the possible in-depth benefits of performing intrusion detection within the campus network.

III. CASE STUDY

We did the tests by footprinting, scanning, and enumeration. The three were found to be necessary steps an attacker could employ to hack a campus LAN. We also performed hacking countermeasures that were of interest in this study.

A. Data collection

1) Footprinting

The physical gathering of the network information was done by scoping targets of interest like identification of office locations, users and everything that one has to know about that target and how it interrelates with everything around it including the target's related or peripheral entities. The combination of tools and techniques that attackers can take unknown entity and reduce it to a specific range of domain names (whois and nslookup), network blocks, subnets, routers, and individual IP addresses of systems directly connected to the network, as well as many other details pertaining to its security posture were dealt in detail. There was also a scooping test in order to gather personal information by using social engineering, internet search engines, and specific web sites like <we.register.it>

It was found that although there are many types of footprinting techniques, most of them are primarily aimed at discovering information in internet, intranet, remote access, and extranet environment [3]. We noted that through footprinting, a security person can picture what the hacker sees, and therefore understand potential security exposures and take the necessary measures to avert hacking. Therefore, footprinting was found to be one of the most important steps that must be properly controlled and accurately performed.

It was observed that an attacker performs network reconnaissance or footprint into the network in many different ways. We limited our test to commonly used tools and techniques, bearing in mind that new tools are released frequently and hackers are dynamic. Table 1, presents the results obtained from footprinting tests based on information available publicly to network users.

By considering that every attack is accompanied by an updated risk rating derived from the first three components. Security experts dynamically and authoritatively should give security updates based on standard scales as:-

a) Popularity: The frequency of use in the wild against live targets, with 1 being the rarest, 10 being widely used.

b) Simplicity: The degree of skill necessary to execute the attack, with 1 being a seasoned security programmer, 10 being little or no skill.

c) Impact: The potential damage caused by successful execution of the attack, with 1 being revelation of trivial information about the target, 10 being super user-account compromise or equivalent.

d) Risk Rating: The overall risk rating (average of the preceding three values.

B. Scanning

The basic difference between footprinting and scanning is that the former is equivalent to a black box or casing a place for information; the later is equivalent to a white box or knocking on the walls to find all the doors and windows. During footprinting, we obtained a list of IP network blocks and IP addresses through a wide variety of techniques using Whois and Nmap tools and techniques. These provided the valuable information about the target network, such as; what services and operating systems each is running, employee names, phone numbers, IP address ranges, Domain Name Server (DNS), and mail servers. We also found which systems are listening for inbound network traffic. Then we determined what addresses are reachable from the Internet using a variety of tools and techniques such as ping sweeps and port scans. Some tests were carried after bypassing the firewalls in order to scan systems supposedly being blocked by filtering rules [5].

1) Mapping

One of the most basic steps is mapping out a network. This is performing an automated ping sweep on a range of IP addresses and network blocks to determine if individual

devices or systems are alive. Ping is traditionally used to send Internet Control Message Protocol (ICMP) ECHO packets to a target system in an attempt to elicit an ICMP ECHO_REPLY indicating the target system is alive. Ping is acceptable to determine the number of systems alive in a small-to-midium size network. Since our network is generally small with less than 2000 hosts, available ping techniques were used to discover live systems.

TABLE I. PUBLICLY AVAILABLE INFORMATION

PUBLICLY AVAILABLE INFORMATION	Popularity	Simplicity	Impact	Risk Rating	%Risk Rating
Web page	5	9	5	6.3	72
Organization UDSM	9	9	4	7.3	81
Location detail	6	6	4	5.2	57
Employees: Phone numbers e-mail address personal details	1	1	9	3.6	40
Current events Udasa mail Web site ARIS Noticeboard	5	5	5	5	55
Privacy and security policies	1	1	5	2.3	25
Archived information	1	1	5	2.3	25
Disgrunted employees	1	1	5	2.3	25
Search engine, usenet and resumes	8	8	5	7	77
Student access	5	5	7	4	44
Risk Rating	**5.1**	**5.6**	**5**	**5.5**	**61**

2) Ping Sweeps Countermeasures

It was found that it is important to detect ping activity when it happens. In all security paradigms, Ping cannot be blocked.

From a host-based perspective, it was noted that if one begins to see a pattern of Internet Control Message Protocol (ICMP) echo packets from a particular system or network, it may indicate that someone is performing network reconnaissance on the site. It is recommended to pay close attention to this activity, as a full-scale attack may be imminent.

It was noted that Microsoft, McAfee, Norton, Symantec, and ISS can detect ICMP, TCP, and UDP ping sweeps. However, just because the technologies exist to detect this behavior, it does not mean that someone will be watching when it occurs.

3) Port scanning

Port scanning is the process of sending packets to TCP and UDP ports on the target system to determine what services are running or are in a LISTENING state. Identifying listening ports is critical to determine the running services, and consequently the vulnerabilities present from remote system. Additionally, one can determine the type and version of the operating system and applications in use. Depending on the type of path, it may allow an unauthorized user to gain access to systems that are misconfigured or running a version of software known to have security vulnerabilities.

In the ongoing work, the focus is on popular port-scanning tools and techniques that will provide a wealth of information and give a window into the vulnerabilities of the system. The portscanning techniques that follow differ from those previously mentioned, when trying to just identify systems that are alive. The following steps assume that the systems are alive, and it is being attempted to determine all the listening ports or potential access points on the target. When port-scanning the target system(s), several objectives are to be accomplished. These include:

- Both the TCP and UDP services running on the target system
- The types of operating systems of the target system
- Specific applications or versions of a particular service

Scan Types

Various port-scanning techniques available are Nmap, SoftPerfect, LANguard, and Fyodor. Fyodor has incorporated numerous scanning techniques into his Nmap. Fig. 1 and Fig 2 presents a Nmap and Nessus reports from the experiments conducted on the campus network.

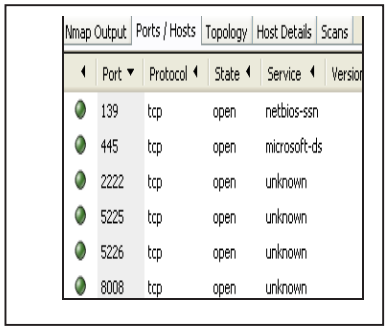

Figure 1. Scanning Host 1 port state report by Nmap test

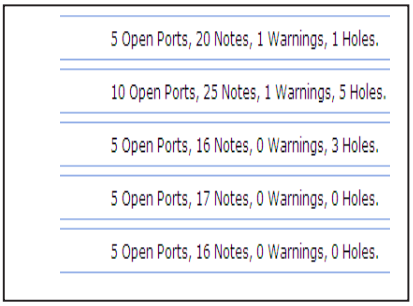

Figure 2. Vulnurability testing report by Nessus test

4) Zero day attack

This is an attack that takes place immediately after security vulnerability is announced. After scanning the network, a hacker could make use of holes found. If a user discovers vulnerability, it might wind up on one or two blogs, and the

news travels fast. If a software vendor finds it, the tendency is to keep it under censorship until it has a patch to fix it. However, in many cases, vendors have to announce the flaw because users may be able to avoid the problem by steering clear of a Web site or being sure not to open a certain e-mail attachment.

On hacker side, zero day exploit capitalizes on vulnerabilities immediately after discovery. Zero-day attacks occur before the security community or vendor of the software knows about the vulnerability or has been able to distribute patches to repair it. For this reason, these exploits allow crackers to wreak maximum havoc on systems. In a campus network, zero hour attack was found to be used by dishonest students who normally try to crack teachers computers.

5) Detecting the operating system

With port information, one can determine if the listening port has potential vulnerabilities. The most important information discovered was the determination of the operating system running. The Stack fingerprinting was looked at which is a powerful technology that allows quick ascertain for each host's operating system with a high degree of probability.

6) ARP Spoofing

Fig. 3 presents the test arrangement used for Address Resolution Protocol (ARP) spoofing. Three computers named gateway, attacker, and victim were used. Tools that were used are WinP Cap 4 series, which were installed into the computer. ARP spoofing were possible from the results obtained from Footprinting and Scanning. During the test, we sent fake ARP messages to an Ethernet LAN. Generally, the aim was to associate the attacker's MAC address with the IP address of another node and in this case, it was the default gateway so that any traffic meant for that IP address would be mistakenly sent to the attacker. When the victim started to forward the traffic to the actual default gateway (passive sniffing), the attacker also launched a denial-of-service attack against a victim by associating a nonexistent MAC address to the IP address of the victim's default gateway. That resulted in routing the traffic through the attacker machine, which breached the security of the victim.

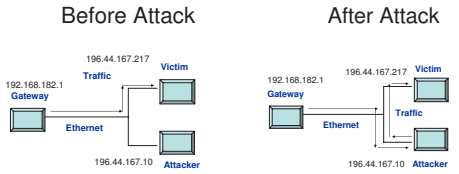

Figure 3. ARP Spoofing attack

C. Vulnerabilities identification

Vulnerability is the tendency of the system to be damaged or attacked; many network vulnerabilities are caused by the weakness in the software used in the network systems. The weakness in software may be due to the following reasons:

No Risk Analysis: It is quite common for software to be developed without any security issues in mind. If a software engineer does not take time to think about potential risks and a suitable security policy for the software during the analysis phase, it is clear that the final software product will probably contain much vulnerability.

Biased Risk Analysis: The risk analysis is often performed by only one of the stakeholders in a given information system. Hence, the formulated security requirements will reflect the position of that particular stakeholder, and will not take into account requirements of other stakeholders. Security is often about mutual distrust, and the risks of all parties involved should be taken into account in a risk analysis.

Unanticipated Risks: This category covers all cases where the developer and the user have failed to recognize a certain risk, and hence have failed to include a corresponding security requirement measure.

Tenable's Nessus is a network vulnerability scanner that contains a large number of tests for known vulnerabilities in a web server software. Hence, Nessus was used to check for vulnerabilities and after running Nessus the following vulnerabilities were detected:

Backdoor: a backdoor in a computer system attack due to the process of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program, or could be a modification to an existing program or hardware device.

Etherleak: vulnerability occurs when multiple platform Ethernet Network Interface Card (NIC) device drivers incorrectly handle frame padding, allowing an attacker to view slices of previously transmitted packets or portions of kernel memory. This vulnerability is the result of incorrect implementations of request for comment (rfc) requirements and poor programming practices. The combination of which results in several variations of this information leakage vulnerability.

Buffer overrun: allows code execution of the attacker's choice.

*Buffer overflow***:** since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information [9]-[12].

Data modification attack: this is due to the availability of file sharing system, so the hacker can read or write to the user information which leads reduced data confidentiality.

Table II presents the vulnerability risk rating of the network under test. As explained earlier, it is based on author's experience, and that every security scenario deserves to be risk rated. Although these facts may not depict the actual situation, but the basic aim of the experiment was to go through standard procedures for guaranteeing the network security. The most important thing is the exploitation of vulnerabilities [6]-[8].

TABLE II. DETECTED VULNERABILITIES RATING

Popularity	**3**
Simplicity	**9**
Impact	**6**
Risk Rating	**6**

D. Discussion of footprinting and scanning resuls

After identifying vulnerabilities present in the network, real attack of those vulnerabilities will be conducted in order to determine which attacks can be possible launched before the attacker takes advantage of the situation in the network. Typically someone, a hacker group, a security company, or a researcher discovers a specific way to violate the security of a network. The discovery may be accidental or through directed research; the vulnerability, of various levels of detail. The proper way to handle the danger would be to release the findings to the security community. Another way would be to pin down the hacker. This is the most complicated procedure as it involves a law of the land and technology that can give unquestionable evidences. The study is still going on, and as advised by [9], security is a continuous process. The guidelines given in the ISO 17799 security policy framework, and the new ISO 27000–series standards [10]-[13]. The task of the test is to constantly guarantee that networks are operating with confidentiality, integrity, availability, and accountability.

Consider a Local Area Network which its operation is typically driven by legal, finance, and education activities. Definitely, security management will be very important. Elsewhere, we are seeing firm's licenses to observe security compliances. This is shifting the focus of information security away from being a backend information technology function, behind network layers of services, toward an integrated and resource shared business level responsibility integrated with security risks present in the environment [6].

The requirement for successful information security requires skills sets to achieve successful security. Policy development, program management, enforcement and verification are all valuable and necessary functions. The skills and knowledge of a practiced and solid security professional that have lived the security trench warfare and survived are vital in developing well-defined security policies and standards, along with a strong compliance program needed. It is important to understand that an open port is an open vulnerability that is a gateway into your data [7].

To achieve solid security in any environment, it is essential that technical skill sets are developed continuously to those who have responsibility to protect the network systems. The staff involved in any level of security lifecycle irrespective of their technical strength including non-technical security staff should be exposed to network security continuously so that all appreciate and understand the depth and sophistication of the attackers' knowledge. Network users should be able to deliver effective risk-based security management in their own environment.

Authorization: It was found necessary to process and obtain appropriate authorization to conduct such study in a campus network as a part of security measure and consciousness in the part of the researchers. It is worthwhile noting that sometimes it is necessary that the security professionals wishing to perform penetration test must take an oath from a legal entity, to ensure that they will not abuse the test or infringe rights of other network users.

E. Common network threats inside the organization that can be detected.

Consider an organization network where a problem of intruders inside the organization is critical. It is widely considered by network experts that it is impossible to build a network system that completely prevents unauthorized intrusions. The most effective defense is the use of intrusion detection systems. Since 1980 the intrusion detection community divided intruders into two categories based on the intruder's access to a system, which are internal intruders having legitimate access through user accounts and external intruders who break into a system without benefit of a user account. This work considered common attacks in the organization networks that include denial of services, unauthorized access, Internet Protocol (IP) session hijacking, IP spoofing, and viruses [2]-[7].

1) Denial-of-Service (DoS)

The problem of DoS attacks is that it is very easy to launch, difficult to track and not easy to refuse the requests of the attacker, without also refusing legitimate requests for service. The DoS attack sends more requests to the host computer than it can handle. There are toolkits available in the hackers community that make this a simple matter by running a program and telling it which host to blast with requests. The attacker's program makes a connection on some service port, perhaps forging the packet's header information that says where the packet came from, and then dropping the connection. If the host is able to answer 20 requests per second, and the attacker is sending 50 per second, obviously the host will be unable to service all of the attacker's requests, much less any legitimate requests. Such attacks were fairly common in late 1996 and early 1997, but are now becoming less popular.

2) Unauthorized Access

Unauthorized access is a very high-level term that refers to a number of different sorts of attacks. The goal of these attacks is to access resource from other machine or a server that your machine should not. A security hole may happen when a host or a web server provides anyone with web pages request. However, that host should not provide command shell access without being sure that one who should get it, such as a local administrator, receives the person making such a request.

3) IP Session Hijacking.

IP Session Hijacking is another common attack in a campus. The user's session is taken over, being in the control of the attacker. If the user was in the middle of email, the attacker will look at the email, and then can execute any commands he wishes as the attacked user. The attacked user simply sees his session dropped, and may simply login again, perhaps not even noticing that the attacker is still logged in and hacking.

4) IP Spoofing.

This is where one host claims to have the IP address of another. Since many systems (such as router access control lists) define which packets may and which packets may not pass based on the sender's IP address, this is a useful technique to an attacker who can send packets to a host, perhaps causing it to take some sort of action.

5) Virus

A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the user. The term "virus" is also commonly but erroneously used to refer to other types of malware, adware and spyware programs that do not have the reproductive ability.

A true virus can only spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance because a user sent it over a network or the Internet, or carried it on a removable medium such as a floppy disk, CD, or USB drive. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer.

F. Hacking techniques

When one access the Internet, the computer sends a message over the Web that uniquely identifies a computer and where it is located. This allows the information requested to be returned. During hacking process, this requested information sometimes carries with it unwanted hidden software created by hackers and online criminals. This software installs itself in the computer and can either be just a nuisance or pose a more serious threat to the owner, people's identity and sensitive financial information. Usually the nuisances are visible and easy to identify, while the more dangerous threats are typically invisible, silent, and difficult to detect until it is too late [5].

Also hackers attack systems by throwing their bag of tricks at a network device and sneaking in through any cracks they find. However they do not just attack computers any more; they are targeting anything with an IP address, such as routers, printers, network-attached storage units, wireless access points and backup appliances with ultimate aim of having IP address to hack through.

With all these potential threats, it was considered necessary to conduct investigation on security hardness of the campus network and use the experience to improve security of the network and other similar networks.

IV. ACKNOWLEDGMENT

Authors are grateful to Kaijage, Z. for her precious time during the experiment.

V. RECOMMENDATIONS AND CONCLUSION

It is recommended that in any LAN, it is important to minimize the amount and types of information leaked outside the LAN and that LAN administrators should constantly perform vigilantly LAN monitoring.

In this paper, the popularity, simplicity, impact and security risk in the organization network have been discussed. The risk rating for the network studied, was found to be rated at between 5 and 6. However, care must be taken as the time used for testing may influence the result showing low risk rating. The network security is the process and not a research or a project.

Holes and areas of weakness a hacker may wish to take advantage and exploit the network have been identified. By using the information gathered from intrusion detection by penetration test, one can make a network safe, so as to attract many potential users to share network resources.

REFERENCES

[1] Tanzania Communications and Regulations Authority (TCRA) annual report 2006-2007, report published by TCRA June 2007.

[2] Stuart Mcclure, Joel Scambray and George Kurtz, Hacking Exposed, Network Security Secrets & Solutions, by The McGraw-Hill Companies 2009, ISBN: 978-0-07-161375-0, MHID: 0-07-161375-7.

[3] David Endler and Mark Collier, "Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions", published by McGraw-Hill/Osborne, 2007.

[4] Vacca, J. R, "Computer Forensics - Computer Crime Scene Investigation," Book published by Charles River Media, Inc. Hingham, Massachusetts, 2001.

[5] David F. Palai, "Computer Forensics", book printed by Charles River Media, Inc, 2002.

[6] Matt Curtin, "Introduction to Network Security", document published by LaTeX2HTML translator Version 97.1, July 1997.

[7] Robert S. Sielken, "Application Intrusion Detection", MsC Thersis in Computer Science, published by University of Virginia, 1999.

[8] Mark Handley and Vern Paxson, "Network Intrusion Detection: Evasion, Traffic Normalization, and end to end Protocal Semantics", report by AT&T Centre for Internet Research at ICSI, 2008.

[9] Solomon & Russinovich, "Inside Windows 2000", 3rd Edition by. Microsoft Press, 2000.

[10] Dabak, Phadke, and Borate, "Undocumented Windows NT", published by IDG, 1999.

[11] LaMacchia et al "NET Framework Security",. published by Pearson Education, 2002.

[12] Joel Scambray, Mike Shema, and Caleb Sima, "Hacking Exposed Web Applications, 2nd Edition", published by McGraw-Hill, 2006.

[13] Brownell K, C, "The Pseudo-Internal Intruders: A New Access Oriented Intruder Category", A Thesis presented to the Faculty of the School of Engineering and Applied Science – University of Virginia, 1999.

[14] Bernardo Pelazzi, "Penetration Test", Universita Deghi Studi Roma Tree-Departmento di Informatica e Automizione, 2008.