Techno Science
International Scientific
Journal of Technical
Sciences

Ethical hacking in the function of increasing computer network security

ADIS RAHMANOVIĆ

THE FACULTY OF TECHNICAL STUDIES, UNIVERSITY OF TRAVNIK, TRAVNIK, BOSNIA AND HERZEGOVINA

ABSTRACT

The purpose of this article is to contribute to the development of awareness, knowledge and skills in the field of computer network security. The article will deal with the methodology of ethical hacking, its computer tools, benefits and the reasons for its realization. Due to the increasing use of ICT devices and services, as well as the obligation to provide safe and reliable communication through computer networks, security becomes an increasingly challenging and legally binding task..

Keywords: Computer network security, ethical hacking, computer hacking tools

Introduction

We are witnessing an increasing number of ICT devices and services they offer, as well as the application of ICT devices in various areas. Likewise, we are witnessing an increasing mobility of people, goods, services, where information sharing at the global level plays an increasingly important role. To meet the above-mentioned requirements, one of the prerequisites is to significantly increase the share of different networking technologies ranging from mobile, local wired and wireless networks, to global wired and wireless networks, as well as to satellite networking.

Due to the growing number of users, services, devices, the value of exchanged information, the need for reliable and rapid information, both in the business and in the field of education, computer network security plays an increasingly important role today and, as the trend indicates, this could be a major challenge in the future because of the number of factors that can be affected through the computer network. The development of computer tools and knowledge in this area is becoming increasingly challenging due to the function and intent of using them, since a wrong and malicious approach in using such computer tools can not only cause a great deal of damage, but also cause accidents, tragedy and self-destruction at worst.

That is why it becomes imperative to educate new generations, directing them towards a constructive usage of new technologies in the function of further sustainable development of life on our planet. The significance and value of ICT and the information processed by it are becoming greater, hence the need for protection against abuse and various risks becomes an imperative, which is why different legislation and standards are adopted.

The legislation and standards are regulated to ensure that certain institutions already have an obligation to verify and test the security of computer networks and information systems, both in the developed countries and BiH, as well as in the region.

Thus, this challenge will also have to be approached preventively (through the development oawareness and education), as well as correctively through different legal measures functioning as penalties for possible damage.

Computer network security testing

In order to protect their computer network, owners in developed countries with intensive usage of ICT services often hire hackers who, upon agreement, attack and verify security while being obligated to keep their findings confidential, not abused and delivered solely to the organisation - company that hired them with the goal to detect potential dangers and implement measures to increase the security of computer networks and the computer system as a whole. The following are most frequently used for verifying and testing security:

- Ethical hacking
- Penetration testing

Upon the implementation of all the recommended necessary measures in the domain of securing the computer network and the information and computer system as a whole against attack and unwanted breach, i.e. violation of the measures and security policy, it is necessary to verify the performance of the implemented measures. In the testing domain, the methods that should indicate the degree of protection reliability and efficiency have been developed. Attack simulation implies unpredictability and constant devising of ways and methods for accomplishing the goals of violating the security level that had been previously reached. Within the testing segment, we have to take into account the advantages the attacker has, e.g. having more time, the ability to choose the time and the means of attack, i.e. having the advantage of a surprise factor. Conversely, the defence has to be prepared and active at all times and in all places, otherwise the system will probably be jeopardised. In order to be recognised as a person who could become an integral part of the team for security testing and verification, one should possess the following traits:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to bear false witness.
5. Thou shalt not use a computer to steal.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.[1]

Apart from the above-mentioned ethical characteristics from the domain of computer science, an individual also has to possess general ethical and moral norms characterising him/her as a reliable and loyal person. Of course, upon identifying people who meet the requirements for verifying and testing the security, work engagement is defined by very strict contract rules. Therefore, investing in education, morality and ethics is not only a premise for a more peaceful and responsible life, but also a premise and an advantage for obtaining certain types of jobs, including verifying and testing security. Based upon the previously stated, it can be seen that ethical hackers have to be trustworthy and patient, which is one of the most important traits since they have to place themselves in the position of malicious hackers who are otherwise known as very patient because they are prepared to spend days or weeks investigating and monitoring the system, waiting for the opportunity to violate its security.

The best candidates for ethical hackers should have relevant experience in working with computers and computer networks, programming, installing operating systems used on computers and performing administrative tasks on them. It would be good that they have already published scientific papers, that they have a history indicating a good knowledge in the field of security, or that they have created open source security programs. One of the rules that major corporations adhere to is not to hire former black hat hackers, regardless of their relevant knowledge and skills in performing the job successfully, which is the crucial rule of absolute trust (characterised by ethics, morality), eliminating such candidates. An ethical hacker should perform his/her job by looking for answers to the following basic questions:

1. What can an attacker see in the target system?
2. What can an attacker do with this information?
3. Has anyone noticed the attacker's attempt or success?

[1] Institut za računarsku etiku (The Computer Ethics Institute): 10 zapovjesti računarske etike (Ten Commandments of Computer Ethics

When a client requires a security assessment, it is necessary to do a lot of interviews and fill out paperwork with a series of questions like: What do you want to protect? What do you want to protect from? How much time, effort, resources and money are you willing to spend to get adequate protection? After the interview, it is necessary to create a plan for identifying the system to be investigated, the test mode and possible limitations during the test. Once the plan is viewed from both sides, a contract between the client and the ethical hackers is jointly drawn up. This contract is also called a "get out of jail free card", and its goal is to protect ethical hackers from prosecution because most of the activities they carry out in assessing security are illegal in many countries. The contract must be highly accurate, especially in the domain of operational activities that contain a description of the test, the network address of the system to be tested, since a small error may lead to the evaluation of the wrong client system or the evaluation of another company's system, resulting in a series of consequences.

The best security assessment can be created with a no holds-barred approach, which in real terms is usually not an option. Some of the limitations that clients impose on ethical hackers are: To abort the tests after detecting the first flaw. They determine the moment of security assessment or ask for a "last-minute" estimate, etc. Ethical hacking can be performed in several ways to assess security by means of: a remote network, a remote network through various connections, a local network, a stolen portable computer (laptop, smartphone, etc.), social engineering and physical intrusion. Each of the stated tests has to be performed from three perspectives: as a "bad guy" from the outside (outsider), as a combination of outsider and insider "semi-outsider", and as a "bad guy" from the inside (insider), i.e. a regular user of the system.

Upon completion of the above-mentioned steps for verification and testing, a final report containing a set of information found by an ethical hacker during the system or network security verification is created. The found vulnerabilities and procedures for their removal are described in detail. The techniques used for testing are never revealed because the person who submits the report cannot be sure who will come to the possession of that document when it comes out of the client's hand. Report delivery is a very delicate matter. If vulnerabilities are detected, the report may be extremely dangerous if it comes into the wrong hands. The competition can use this information for industrial espionage, and malicious hackers can use them to invade the computer network and the client's system. Upon report delivery by the ethical hacker, the client may conclude the following: "Alright, if I fix these flaws, I will be completely safe, won't I?" This is sadly not the case. People work on computers and client's networks and they make mistakes, while security is not a current state but a process, and therefore, as more time passes after testing, the security drops. A segment of the report necessarily contains recommendations that the client needs to follow in order to reduce the impact of these errors in the future.

Penetration testing

In the aforementioned section, we have demonstrated the aspects of verification and the characteristics of individuals who meet the requirements for ethical hacking, while below, we will discuss the methodology and testing procedures. Penetration testing is a method of assessing and verifying the safety of a computer network by simulating an attack that would otherwise have been done by a malicious hacker. Examining the possibility of a breach includes an active system analysis in terms of weaknesses, technical deficiencies and vulnerabilities. The analysis is conducted from the perspective of a potential attacker with the goal to penetrate the network and thus detect vulnerabilities. All the information we obtain during this analysis must be given to the system owner, together with an assessment of the impact which the detected vulnerabilities may have on system security and the suggestion of technical solutions for removing or reducing the impact of the detected vulnerabilities. Tests of this type have to be conducted on each system which will be set up and exposed to hostile influence (especially if the computer is connected to the Internet). They have to be conducted before the system is set up and exposed to the above-mentioned risks.
The usual hacker attack on a computer network consists of the following phases:

- Reconnaissance,
- Recording,
- Gaining Access,
- Privilege escalation,
- Exfiltration,
- Covering Tracks,
- Creating a back door,
- Withholding services (possibly).

In the test preparation stage, it is necessary to provide the needed resources comprised out of the team, i.e. human resources with the necessary

knowledge, competences and skills, the equipment and other resources needed, as well as the time required for these steps in order to achieve the quality and deliver the required results. Prior to implementing the methodology used in testing the security breaches, it is necessary to consider the legal and ethical (moral) standards, sign a contract, set the rules of engagement, plan the attacks, assemble a team, select the computer and other testing tools and plan the attack strategy through some of the available methodologies (e.g. OSSTMM – Open Source Security Testing Methodology Manual). Reconnaissance and recording are also conducted through the process of passive reconnaissance, i.e. through system monitoring, where we gather information coming to us as a result of regular activities, and active reconnaissance performed by active operations in some parts of the system or the system as a whole. The principal steps in penetration testing are shown in the following image:

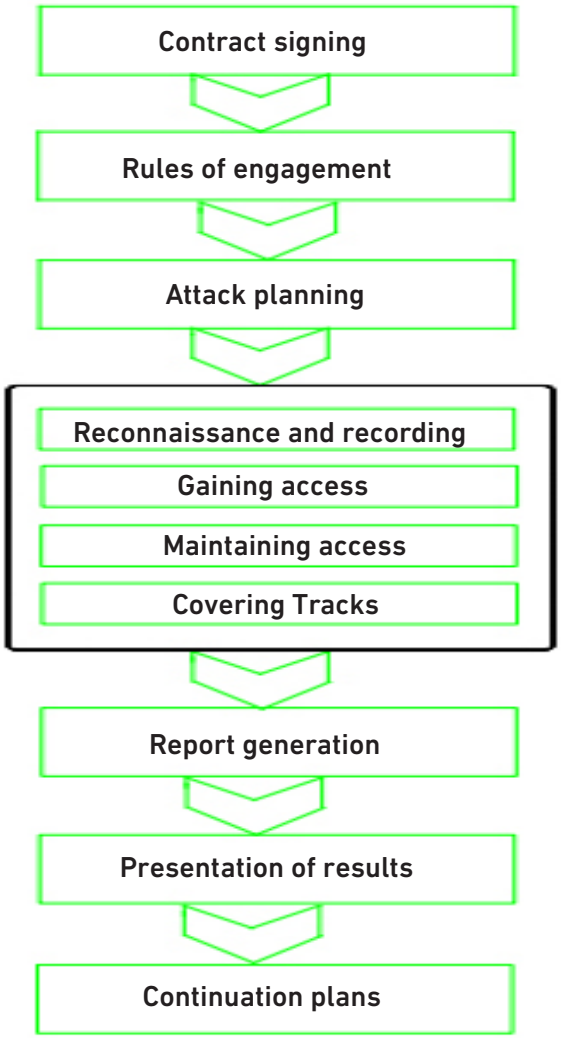

Image 1: The principal steps in penetration testing

The procedure for conducting the test consists of gaining access through various methods among which the most frequent are:

- Session hijacking - first, the user who conducts the testing kicks out the user with an active session on the server, and then takes over the session in a way that the sever is not aware of the session hijacking.
- Web server attacks - if it is within the infrastructure, it is due to the exploitation of information obtained from it and if it is outside of the infrastructure, it is for entering and receiving information.
- Password cracking - strict access control measures are usually founded on at least four elements (something that a person knows, e.g. a PIN number or a password, something that a person has, e.g. a security ID card, something that a person is - biometrics based on physical characteristics, something that a person does - biometrics based on behavioural characteristics).
- Network attacks (using various tools and information).
- Wireless network attacks (using various tools and information).
- A server breach with different types of operating systems (UNIX, Linux, and Windows) - privilege escalation followed by further scanning using rootkit tools...
- Throughout the breach testing procedure, i.e. penetration testing, it is important to ensure access maintenance, as well as covering potential tracks. Finally, a report on flaws and risks is presented, which should have the following parts: executive summary, project scope, trials and results, report summary and annexes. It is important to emphasize the flaws, the potential for damage incurrence, and to make plans for their removal.

Ethical hacking computer tools

Maintaining the security of computer networks is a demanding and ongoing process that involves continuous research, learning, understanding and developing new computer tools and techniques in order to act preventively and maintain the level of security within acceptable limits. That is why computer tools play an increasingly important role in preventing, testing, scanning, performing administrative tasks, optimising, detecting and eliminating errors and potential dangers.

It is important that they provide a quick and easy way of identifying specific flaws, and the choice of computer tools, along with the above-mentioned conditions, for ethical hackers themselves represents a very important component in protecting the system and information.

Rootkit tools

Rootkit is a set of small and useful programs allowing the attacker to maintain root access, i.e. the user with the greatest privileges. Rootkit, as a set of programs and codes, can provide permanent, consistent, undetected presence in the system, computer network, or a computer. Rootkit tools are in fact a very useful technologythat can be abused because of its features and thus become very dangerous. Some of the features are: it is designed to hide the program code and system information, as well as to enable remote access and eavesdropping, for example, for network packet sniffing.
An attack on a rootkit-based system is performed in four stages:

- Gathering information on the target system (e.g. the operating system, the version of the core, existing user accounts).
- Obtaining administrator rights, i.e. the rights of a root user, necessary for the installation.
- Installing rootkit tools.
- Establishing control over the target system.

Rootkit tools can be divided into two groups:
- Rootkit tools as utility applications - operate like all other applications in user mode.
- Rootkit tools integrated in the core, operating in kernel mode.

The two types of tools are distinguished by the place in the system they are in and the way they hide their presence in the system. Rootkit tools as utility applications operate in such a way that they replace legitimate applications with malicious files. The inserted files enable the attacker to conceal their presence and perform the desired activities in the system (providing the back door, i.e. the hidden entrance the attacker can use).
The group of programs the attacker changes so as to hide includes programs with the following tasks:

- Hiding malicious files, folders the attacker planted (ls, find, clu).
- Hiding the processes initiated by the attacker (ps).
- Preventing the termination of processes initiated by the attacker (kill, killall)
- Hiding the attacker's activities on the network - open ports, network connections (netstat, ifconfig).
- Hiding the entry in the crontab file.
- Hiding log file entries on the attacker's connections with the remote system (syslogd).

Kernel-level rootkit tools are harder to detect than those functioning as utility applications because they are integrated into the operating system core, and can be bypassed by the system integrity verification conducted in unprivileged mode. Kernel rootkit tools are based on the fact that the core of a Linux system is modular - a user with root privileges can load a module into the core (LKM - Loadable Kernel Module) and in such a way expand the operating system's capabilities. The rule used for worms and viruses also applies for rootkit tools. It is easier to prevent these tools from being installed than detect and remove them afterwards. Administrators have a large number of programs intended for detecting rootkit tools at their disposal, including the following: Chkrootkit, Rscan, Rkdet, RootkitRevealer.
Therefore, for rootkit tools, it is important to use them for the purpose they are designed for, better administration and optimization of computer processes, as well as to detect their malicious use on time.

Nmap

Nmap ("Network Mapper") is a free and open-source search tool, network monitoring and security auditing tool. It is used by a large number of network administrators in everyday activities, as well as in the field of security risk monitoring. Nmap uses IP packet traffic in a variety of ways to determine which users are present on the network, which types of services are offered, which operating systems are available, what type of firewall is used to filter traffic and dozens of other features. It is designed to rapidly scan large networks, but can also be used effectively to scan traffic and services on a single computer. It is created to run on different operating systems such as Linux, Windows and Mac OS X.

Nmap has the following features: it is

- ***Flexible***: supports dozens of advanced techniques for mapping out networks.
- ***Powerful:*** Nmap has been used to scan huge networks of literally hundreds of thousands of machines.
- ***Portable***: supports most operating systems, including: Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX,

NetBSD, Sun OS, Amiga, and more.
- ***Easy:*** regardless of a large number of options, it a relatively simple tool to the average user.
- ***Free:*** The goal was to help make the Internet and network environment a little more secure.
- ***Well Documented:*** Significant effort has been put into providing appropriate study materials.
- ***Supported***. Regardless of it being free, due to good networking and team work, this tool constantly progresses.
- ***Acclaimed:*** Nmap has won numerous awards,
- ***Popular:*** Thousands of people download it every day.

KALI Linux

Kali Linux is a Debian-derived Linux distribution. It is designed for digital forensics, penetration testing and hacking. It is maintained and funded by Offensive Security Ltd. Kali Linux has hundreds of preinstalled penetration-testing programs. It can run natively when installed on a computer's hard disk, can be booted from a live CD or a live USB, or it can run within a virtual machine. When running from a bootable USB/DVD the following options occur: installation, live boot or forensic mode.
When Kali Linux is booted in live mode or installed on a computer, the main menu contains the following options:

- INFORMATION GATHERING
- VULNERABILITY ANALYSIS
- WIRELESS ATTACKS
- WEB APPLICATIONS
- EXPLOITATION TOOLS
- FORENSICS TOOLS
- STRESS TESTING
- SNIFFING & SPOOFING
- PASSWORD ATTACKS
- MAINTAINING ACCESS
- REVERSE ENGINEERING
- HARDWARE HACKING
- REPORTING TOOLS.

There are a number of features provided by such a computer tool, among which we highlight:

1. Verifying the security of network components (e.g. routers).
2. Possibility of computer invasion.
3. Seizing control of the services and the computer.
4. Collecting, analysing, attacking, breaking codes, maintaining connections, tools for diagnosing attacks and determining damage and evidence for a judicial process. It is important to have the ability to determine reverse engineering, because, through reverse analysis in real time, we can detect and eliminate errors and flaws that cannot be seen on a regular basis.

KALI Linux is a computer tool that can be used not only in the domain of security and breach testing, but also as a tool that provides many more features, even in the domain of forensics. Since it was created on a Linux platform, it has a series of security flaws. In order to achieve significant results with the use of this tool, it is necessary to have great knowledge and experience in using not only this tool, but also the various platforms for security testing.

Concluding remarks

In view of the above, computer network security is becoming more challenging, and, due to an increasing usage of ICT services, it is becoming all the more significant, while in some segments of ICT application, it is becoming an imperative. In order to ensure a sufficient level of security as a process, it is necessary to engage every institution ranging from educational to state institutions so as to, through educational measures, increasingly act in a preventive manner, and, from the state institutions' point of view, act both preventively and correctively. Investing in awareness raising and education with the purpose of using IT equipment for constructive purposes will play an increasingly important role.

Moreover, it is necessary to invest more funds in staff education and procuring IT equipment, as well as computer tools, all with the goal to provide a more secure environment which will be required in legal terms and, through standards, test and verify its security in defined intervals, as well as solve the perceived anomalies both continually and preventively, along with performing corrective activities on increasing the security to the extent equal to the value of that which is being protected. One of the prerequisites for further expanding the use of ICT equipment and services is to address the challenges imposed by computer network security as an ongoing process. Particular importance and a significant role will be placed on individuals acting as ethical hackers both in the domain of verification and penetration testing, report generation and providing suggestions for improvements, as well as through repeated penetration testing upon implementing the measures. By way of this domain, it can be seen that intensifying investments in education, especially in the ICT domain, represents a premise for involving BiH and the region in recent trends.

References

1. Bača, M. Uvod u računalnu sigurnost, Zagreb, Narodne novine, 2004.
2. Centar informacijske sigurnosti, Modeliranje sigurnosnih prijetnji (Threat Modeling), Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu, Zagreb, 2012.
3. Gledec, G., Mikuc, M., Kos, M. Sigurnost u privatnim komunikacijskim mrežama, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, 2008.
4. Institut za računarsku etiku (The Computer Ethics Institute): 10 zapovjesti računarske etike (Ten Commandments of Computer Ethics), 2001.
5. Rahmanović A., Saračević M., Mujević M., Sukić Ć. (2018), Possibilities of applying video surveillance and other ICT tools and services in the production process, TEM Journal: Association for Information Communication Technology Education and Science, Vol.7, No.1, ISSN: 2217-8309, Published by: UIKTEN, indexed in Thomson Reuters Emerging Science Citation Index, Indexed in SCOPUS (Elsevier).
6. Rahmanović A., Saračević M., Selimi A. (2018), Design And Implementation Of Electronic Payment System In The Specific Case Study, KNOWLEDGE - International Journal, Vol.7, No.1, ISSN: 1857-923X (accepted)
7. Strebe, M. Firewalls: zaštita od hakera : u praksi : [za administratore]. Čačak : Kompjuter biblioteka, 2003

Etičko hakiranje u funkciji povećanja sigurnosti računarskih mreža

SAŽETAK
Cilj ovog članka je doprinijeti razvoju svijesti, znanju i vještinama iz područja sigurnosti računarske mreže. U članku će se obraditi metodologija etičkog hakiranja, njegovi računarski alati, benefiti, razlozi za realizaciju istog. Zbog sve većeg korištenja IKT uređaja i usluga i obaveze obezbjedjenja sigurne i pouzdane komunikacije pomoću računarskih mreža, sigurnost postaje sve veći izazov i zakonska obaveza.

Ključne riječi: Sigurnost računarskih mreža, etičko hakiranje, računarski alati pri hakiranju

---

Received: February 19, 2018 / Accepted: February 29, 2018
Correspondence to: Adis Rahmanović, University of Travnik, Faculty of Technical Studies, Travnik, Bosnia and Herzegovina
E-mail: cefes06@gmail.com