Global Information Assurance Certification Paper

Ethical Hacking

GSEC Practical
Version 1.4 (Option 1)

Reto Baumann
November 24, 2002

Table of contents

Abstract

"Is our network secure and the information safe? Do we have some potential vulnerabilities and could a hacker successfully compromise our systems?" These can be questions a security officer is asking himself every day. How can he be sure that his network is secure? Nobody installed a modem that responds to calls and opens up a backdoor to the corporate network which he doesn't know of?

Ethical hacking is an assessment to test and check an information technology environment for possible weak links and vulnerabilities. Ethical hacking describes the process of hacking a network in an ethical way, therefore with good intentions. This paper describes what ethical hacking is, what it can do, an ethical hacking methodology as well as some tools which can be used for an ethical hack.

Introduction

The Internet is still growing[1] and e-commerce is on it's advance. More and more computers get connected to the Internet, wireless devices and networks are booming[2] and sooner or later, nearly every electronic device may have its own IP address. The complexity of networks is increasing, the software on devices gets more sophisticated and user friendly – interacting with other devices and people are a main issues. At the same time, the complexity of the involved software grows, life cycles are getting shorter and maintaining high quality is difficult. Most users want (or need) to have access to information from all over the world around the clock. Highly interconnected devices which have access to the global network are the consequence. As a result, privacy and security concerns are getting more important – in the end, information is money. There is a serious need to limit access to personal or confidential information – access controls are needed. Unfortunately most software is not bug free due to their complexity or carelessness of their inventors. Some bugs may have a serious impact on the access controls in place or may even open up some unintended backdoors.

Security therefore is a hot topic and quite some effort is spended in securing services, systems and networks. On the internet, there is a silent war going on between the good and the bad guys – between the ones who are trying hard to keep information secured and the ones who are trying to get prohibited access to these information. Securing an information technology environment does not just consist of a bunch of actions which can be taken and then everything can be forgotten – there is no fire and forget solution - security is a never ending process. Maintaining a high level of security isn't simple… Questions about an environments security arise every day – Are we secure?

Answering such questions isn't simple at all – how can one tell if an environment is secure?

What is Ethical Hacking

Ethical hacking provides a way to determine the security of an information technology environment – at least from a technical point of view. As the name ethical hacking already tells, the idea has something to do with hacking. But what does "hacking" mean?

> "The word *hacking* has two definitions. The first definition refers to the hobby/profession of working with computers. The second definition refers to breaking into computer systems. While the first definition is older and is still used by many computer enthusiasts (who refer to cyber-criminals as "crackers"), the second definition is much more commonly used." – Definition by Internet Security Systems[3]

[1] http://www.vnnic.net.vn/english/statistics/others/world_asean/Index.htm
[2] WLAN is booming (http://www.semiseeknews.com/press_release4297.htm)
[3] http://www.iss.net/security_center/advice/Underground/Hacking/default.htm

In the context of "ethical hacking", hacking refers to the second definition – breaking into computer systems. It can be assumed that hacking is illegal, as breaking into a house would be. At this point, "ethical" comes into play. Ethical has a very positive touch and describes something noble which leads us to the following definition of ethical hacking:

> Ethical hacking describes the process of attacking and penetrating computer systems and networks to discover and point out potential security weaknesses for a client which is responsible for the attacked information technology environment.

An ethical hacker is therefore a "good" hacker, somebody who uses the methods and tools of the blackhat[4] community to test the security of networks and servers. The goal of an ethical hack is neither to do damage nor to download any valuable information – it's more a service for a client to test his environment on how it would withstand a hacker attack. The final output from an ethical hack is mostly a detailed report about the detected problems and vulnerabilities. Sometimes, the report does even have instructions on how to remove certain vulnerabilities.

Ethical hacking does perfectly fit into the security life cycle (see figure 1). Ethical hacking is a way of doing a security assessment – a current situation (from a technical point of view) can be checked. Like all other assessments (or audits), an ethical hack is a random sample and passing an ethical hack doesn't mean there are no security issues. An ethical hack's results is a detailed report of the findings as well as a testimony that a hacker with a certain amount of time and skills is or isn't able to successfully attack a system or get access to certain information.

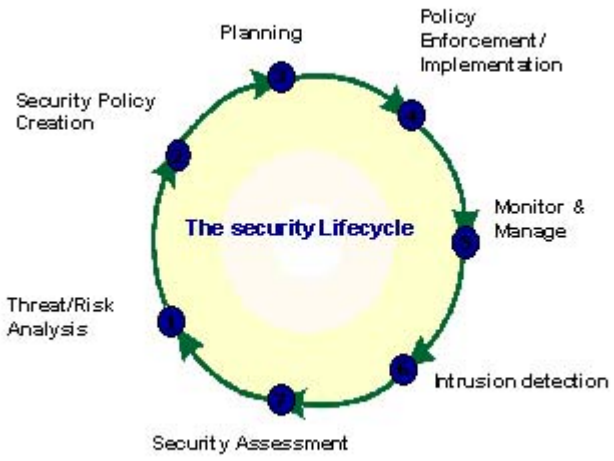

Figure 1: Security Life Cycle, www.securityfocus.com

[4] Blackhats use their knowledge on how to hack a system for illegal activities

One can sometimes read about discussions, if an ethical hack is a risk analysis or not. I would definitively vote against it. A risk analysis (or assessment) deals with risk, their probability and their potential damage. The goal of a risk assessment is to have a certain amount of money attached to certain risks. An ethical hack sometimes rate vulnerabilities and categorizes them from low to high-risk but can't be considered a risk assessment just because of that. An ethical hack never deals with potential money loss and also never categorizes the vulnerabilities according to the importance for a business process. I would like to quote Charl van der Walt[5] which describes these two steps in the life cycle very well:

> "A risk analysis is typically performed early in the security cycle. It's a business-oriented process that views risk and threats from a financial perspective and helps you to determine the best security strategy. Security assessments are performed periodically throughout the cycle. They view risk from a technical perspective and help to measure the efficacy of your security strategy. The primary focus of this paper is on this kind of assessment."

Ethical hacking is can be categorized as a security assessment, a kind of training, a test for the security of an information technology environment. It's comparable to friendly match in soccer, where two teams are testing how well they would perform in a "live action". An ethical hack shows the risks an information technology environment is facing and actions can be taken to reduce certain risks or to accept them.

Who's an Ethical Hacker

Ethical hackers are mostly people with a good technical knowledge about operating systems and computer networks. An ethical hacker's knowledge is very much comparable to the one of a "real" hacker. It is known, that some blackhats have been converted to whitehats[6] and are now using their knowledge on how to hack a system in an ethical way. Hiring ex-hackers as ethical hackers is very controversial. After all, an ethical hacker will see sensitive information and needs to be extremely trustworthy. During his assignment an ethical hacker may get access to sensitive and confidential customer information where he will see and discover customers weak points – As C. C. Palmer writes in his article[7] "the ethical hacker often holds the keys to the company". A lot of companies therefore won't employ former hackers for doing their ethical hacks as the risk and uncertainty is to high, although they may know the craft very well and even have connections to the underground for getting the newest tools and exploits.
As already pointed out, one of the main requirements for an ethical hacker is its trustworthiness. The customer needs to be 100% certain that information found by the ethical hacker won't be abused. Another very important ability is patience.

[5] Internet Security Risk Assessment, http://online.securityfocus.com/infocus/1591
[6] Whitehats are the opposite of blackhats. They use their knowledge to "do good".
[7] Ethical hacking by C. C. Palmer - http://www.research.ibm.com/journal/sj/403/palmer.html

Professional hackers are known to be very patient and persistent. Sometimes they listen to network traffic or scan through newsgroups for days just to find a piece of information which could help hacking a system. Unfortunately, most ethical hackers don't have "every time on earth" as most contractors don't want to pay for such an extensive listening phase. For an ethical hacker it is therefore even more important keeping up to date with the current exploits and attack techniques, as he hasn't the time for extensive research.
Having all these requirements, it's not very astonishing that most ethical hackers are not evolving from the security practice – they especially need a good understanding for operating systems as well as network equipment. They got their security education and awareness on their careers as network or system administrators. For an ethical hacker it's more important to know a system inside out than to know what security processes on a business levels have to be in place to provide a certain level of corporate information security.

What are Ethical Hackers doing

Ethical hackers are working on a contract basis with a customer to attack his systems. A customer is interested in the following three questions:

1. What can an intruder see?
2. What can he get access to?
3. What kind of valuable information can he retrieve?

Ethical hackers are acting like they are real hackers – using the same methods and tools. Due the fact that hacking is illegal in most countries, an ethical hacker will not start his mission as long as he has not an "out-of-jail-letter". This is a paper where the contractor states that he hired the hacker to hack his designated systems. As soon as the liability and legal aspect is cleared, an ethical hacker can start his work. Depending on the kind of ethical hack which has to be performed his actions may vary. One can distinguish multiple types of ethical hacks depending on their point of origin, level of knowledge and awareness of the company who gets attacked.

An Ethical Hack can be categorized according to three characteristics (as can be seen in figure 1):

1. Point of Origin
2. Knowledge
3. Announcement

The point of origin describes the connectivity a hacker has. Does he sit inside the corporate network or does he attack from the outside, therefore from the Internet or via remote access facilities. The point of origin has a notable significance as the goal of an ethical hack is directly correlated. If a client is more interested in the security of his internal system, therefore the safety of the servers compared to employees who have access to the internal network, an internal ethical hack is chosen. If a customer is more interested in whether a hacker can access his

information from the internet or remote access or not, an external ethical hacking is selected.

Figure 2: Ethical Hack Types

The knowledge of an attacker about the network, company, involved systems and especially the network architecture can have a tremendous impact. An outsider certainly has not as much information as a former administrator. Most of the time an ethical hackers receives more information as a "real" hacker would have at the beginning. Most times, it is only a question of time for the attacker to collect all the information. Therefore it isn't wrong to supply additional information for the ethical hacker to reduce the required time. Revealing information as network topology shouldn't even affect the overall security, as "security through obscurity" is never a working solution.
Another characteristic is the fact, if the internal employees (especially the administrators or security personal) do know about the upcoming attack. An ethical hack is a good opportunity not only to check the security of the equipment as well as to check the established security procedures and how to react on an incident (or to check if the incident will even get noticed). Unfortunately this is like playing with fire as it can also be a shoot in the back. It is wise to inform at least the security officer so that he can end the "drill" as soon as it's running out of control.

After these initial steps have been negotiated with a client, an ethical hacker can launch his attacks. The attack itself is going to happen very similar to a real hackers attack – reconnaissance, probes and attacks.

An ethical hacker in contrary to a "normal" hacker has to be careful not to destroy anything. It can even be a problem if a system is crashing due to certain attacks. Due the sensitivity of the involved actions, a log file should be written at all times to reconstruct encountered problems. Depending on the available time, an ethical hack is more sophisticated and involves writing pieces of software, extensive listening phases or social engineering[8].

[8] Social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures – http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html

Ethical Hacking Methodology

An ethical hacking methodology is quite similar to a hacking methodology[9] as there are more or less the same goals. Anyhow, some differences exist.
An ethical hacker doesn't need to take that much care in hiding his traces and tracks. He can chose a more aggressive way and doesn't need to bother with slowing down portscans (to avoid detection) or evading intrusion detection systems – at least most of the time unless it is specially desired by the client. Mostly, an ethical hacker just hasn't the time to be that careful in blurring his traces and tracks unless the customer pays for. Nevertheless, a lot of similarities can be found to a hacking methodology[10].

An ethical hacking methodology overview can be seen in figure 2. A similar setup could be used by a hacker for his attacks. The ethical hacking methodology described is based on eight possible phases where interactions between the phases are possible, even required as hacking is an iterative process; going back to an earlier phase is absolutely possible (and needed).

Figure 3: Ethical Hacking Methodology

[9] A hacking methodology describes the process and method of attacking a computer system or network
[10] Hacking methodology examples: http://www.cybertrace.com/papers/hack101.html; http://adsm-symposium.oucs.ox.ac.uk/1999/papers/neil/tsld008.htm

Reconnaissance

To be able to attack a system systematically, a hacker has to know as much as possible about the target– reconnaissance is inevitable. It is important to get an overview of the network and the used systems. Consulting the whois, ripe and arin databases is a good staring point. Information as DNS servers, administrator contacts and IP ranges can be collected. Searching the usenet for old postings of an administrator may reveal problems they had (or even still have) as well as used products and sometimes even configuration details.
An initial scan of the hosts may show up some interesting services where some in depth researching may lead to interesting attack possibilities.
Another issue is looking up possible numbers for the company and trying to connect to a modem. Scanning telephone networks for answering devices and collecting these numbers for a later access attempt may lead to a first entry into the network. Such scans of telephone networks are usually referred to as "war dialing"[11] and were heavily before the Internet existed in such a dimension as it exists today.
The reconnaissance phase may even consider going through trash bins or visiting loading docks of the target to collect additional information which could be of help later on.

During the reconnaissance phase different kind of tools can be used – network mapping, network and vulnerability scanning tools are the commonly used. Cheops[12] (see figure 4 for a screenshot) for example is a very good network mapping tool which is able to generate networking graphs. They can be of great help later on during the attack phase or to get an overview about the network. A network mapping tool is especially helpful when doing an internal ethical hack (from outside there is often not much to see).

For getting a fast report on possible vulnerabilities and security weaknesses, a vulnerability scanner can be helpful. These tools scan specified IP ranges for services and possible, known vulnerabilities. A widely used vulnerability scanner is Nessus[13] which is available for Unix-like operating systems. The vulnerability database is updated frequently and contains a huge collection of possible problems and weaknesses.

At the end of the reconnaissance phase, an attacker should have a bunch of information about the target. With all these pieces of information, a promising attack path can be constructed.

[11] War dialing - http://www.wikipedia.org/wiki/War_dialing
[12] Cheops - http://www.marko.net/cheops/
[13] Nessus Project - http://www.nessus.org/

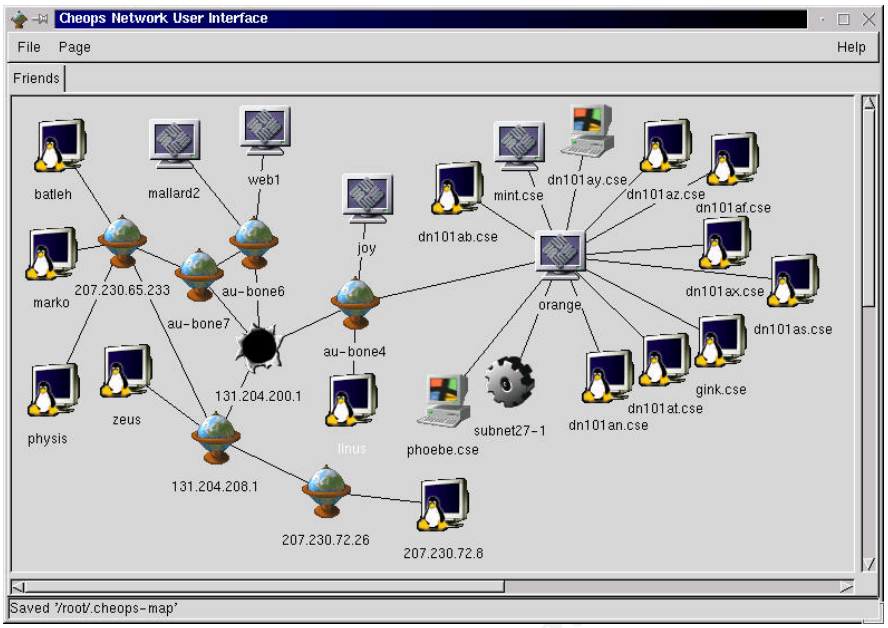

Figure 4: Cheops Screenshot (Source Cheops homepage)

Probe and Attack

The probe and attack phase is about digging in, going closer and getting a feeling for the target. It's time to try the collected, possible vulnerabilities from the reconnaissance phase. Tools for launching buffer overflows or using other weaknesses are heavily used. At the same time, password guessing does take place including guessed and well known default passwords as well as brute force attacks. Painting a security map, which shows dependencies and trust relationships may even allow spoofing or hijacking or may show up some miss configurations which enable to slip past security measures.

Tools which can be used during the "Probe and Attack" phase are many-sided as web exploits, buffer overflows as well as brute-force can be required. Even Trojans like NetBus (see figure 5) can be deployed to capture keystrokes, get screenshots or start applications and a host.

The probe and attack phase can be very time consuming, especially if brute force attack techniques are used or when individual pieces of software have to be developed or analyzed.

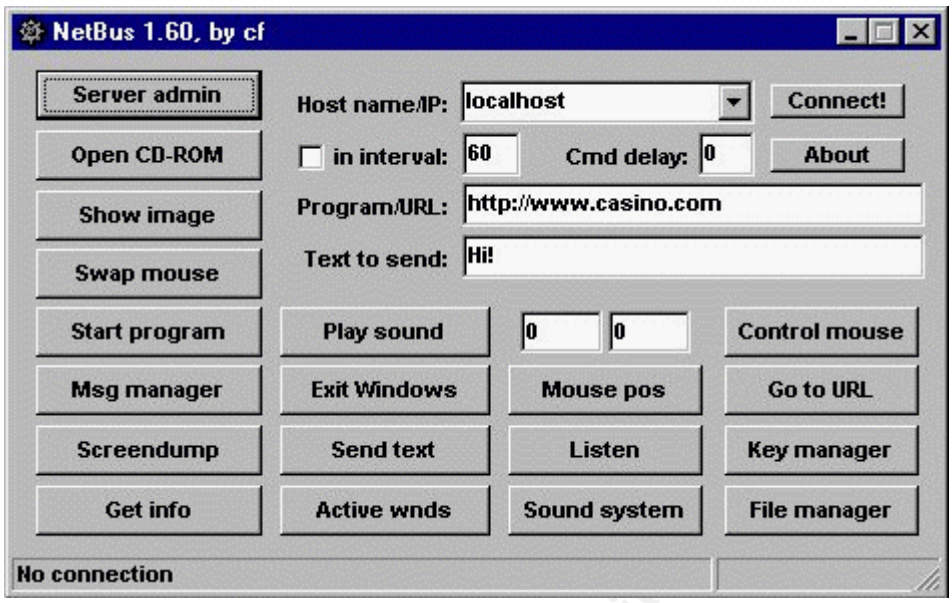

Figure 5: NetBus screenshot

Listening

Attacking a system directly according to so found vulnerabilities doesn't always lead to a successful compromise. Listening to network traffic or to application data can sometimes help to attack a system or to advance deeper into a corporate network. Listening is especially powerful as soon as one has control of an important communication bottleneck. Sniffing network traffic does not only reveal important passwords and usernames but can also give information about the network architecture and used networking equipment (like sniffing Cisco Discovery Protocol packets) or used operating systems and running services.

Listening and sniffing is not restricted to network traffic. By using pieces of software, it is also possible to capture screenshots or keystrokes. These techniques can be extremely helpful when encrypted communication channels are used and sniffing wouldn't be of much help.

Sniffers are heavily used during the listening phase. Multiple sniffers, from very simple to more complex, from console based to GUI driven exist for all operating systems. Some sniffers, like ettercap[14] (see figure 6), can even poison ARP tables to enable sniffing in switched environments and open totally new opportunities for listening to network traffic.

[14] Ettercap - http://ettercap.sourceforge.net/

Figure 6: Ettercap screenshot (Source Ettercap homepage)

The listening phase is often a waiting game – does the ethical hacker has enough patience to wait for the interesting information and is he attentive enough to see it pass by?

First Access

Sooner or later the "Probe and Attack" or "Listening" phase will hopefully lead to a compromise of a system. "First Access" is about using this probably small entry point to widen the attack possibilities, to gain a toehold. This phase is not about getting root access, it's about getting any access to a system be it a user or root account. Once this option is available it's time to go for higher access levels or new systems which are now reachable through the acquired system. This can include running unauthorized programs (like suid enabled programs on Unix based systems), changing files which can enable new access patterns (like .rhosts file), intercepting communications or browsing local files for useful pieces of information.

Advancement

Using exploited systems to go in further is the main task of the "Advancement" phase. During all phases of a hack, the attacker has to be creative and find ways to use vulnerabilities, miss configurations and human interaction to reach his goal.

The advancement phase is probably the most creative demanding stage, as unlimited possibilities are open. Sniffing network traffic may unveil certain passwords, needed usernames or e-mail traffic with usable information. Sending

mails to administrators faking some known users may help in getting desired information or even access to a new system. Probably one also has to alter configuration files to enable or disable services or features. Last but not least, installing new tools and helpful scripts may help to dig in deeper or to scan log files for more details. Advancement is like a new hack inside a hack as you can think of starting over with new systems.

Stealth

Some systems may be of high value – systems which act as routers or firewalls, systems where a root account could be acquired or systems which do play an important role in a thrust relationship. To have access to such systems at a later time it is important to hide all traces and install some alternative doors in case the used vulnerability gets patched. Installing rootkits[15] and cleaning relevant log files is imperative to stay undercover, to go stealth.

Takeover

You're finally there, you've won one battle of an entire war – you gained root or administrative privileges. Once root access could be attained, the system can be considered won. From there on it's possible to install any tools, do every action and start every services on that particular machine. Depending on the machine it can now be possible to misuse trust relationships, create new relationships or disable certain security checks.

Cleanup

The cleanup phase is probably the most important phase for a hacker as he doesn't want to get captured. For an ethical hacker it's another issue. He doesn't need to be scared about getting caught or being sued. Never the less, cleanup is also needed on one or the other form in an ethical hack. This could be instructions in the final report on how to remove certain rootkits or trojans but most of the time this will be done by the hacker itself. Removing all traces as far as possible is kind of a duty for the hacking craft. Removing Trojans and backdoors is especially important as these doors could be used by other hackers to gain entry, which brings me to an interesting point. An ethical hack always

[15] A rootkit is a collection of tools (programs) that a hacker uses to mask intrusion and obtain administrator-level access to a computer or computer network. The intruder installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. The rootkit then collects userids and passwords to other machines on the network, thus giving the hacker root or privileged access. A rootkit may consist of utilities that also: monitor traffic and keystrokes; create a "backdoor" into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to circumvent detection. – Definition by http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci547279,00.html

poses a certain risks if not properly done. A hacker could use the deployed tools or hide his attacks in all the attacks from the ethical hack. He could also try to attack the attackers system, therefore gain entry to the ethical hackers system and collect all information “free of charge” and already sorted and prepared. Preparing an ethical hack and hold a high level of security is a challenging task which should only be done by professionals.

Methodology Summary

Some or even multiple steps may be bypassed as a result of an early success in attacking a system – the reconnaissance phase is the only one which is always performed. Getting as much information about the target is inevitable and helps a lot in performing a successful and organized attack.

The goal of the ethical hack may also alter and influence the methodology. If a vulnerability scan is all there is asked, gaining some level of access is not a goal and therefore left out. After all, the customer can decide what he would like to have tested and what he’s expecting as a result of an ethical hack.

The outlined methodology provides an easy to follow frameset to perform an ethical hack in an organized form.

Tools

The tools chapter lists some utilities and applications which can be used in one or more phases of an ethical hack. The list is definitively not complete or may even list tools which vanished or do no longer exist.

Phase	Topic	Tool
Reconnaissance	Network Mapping	Cheops, traceroute
	Network Scanning	tcpdump, nmap, strobe, rprobe
	Security and Vulnerability Scanning	Nessus, ISS, Cybercop
	Firewall Scanning	FireWalk
	Application Scanning	Whisker, Archilles, Legion
	War Dialing	Phone Sweep, ThcScan, LoginH
	OS Fingerprinting	nmap, queso
	Banner Enumeration	banner enumeration, Enum, ruser
	WLAN	NetStumbler, dsnort
Probe and Attack	Web Exploits	Showcode, Unicode exploits
	Local Exploits	sechole, pwddump, dumpacl, PamSlam
	Remote Exploits	PCAnywhere, nfs exploits, NetOp, sadminX
	Buffer Overflows	BFS, Slugger2
	Trojans	NetBus
	Brute Force	AccessDiver, GoldenEye, L0pth Crack, Jack the Ripper
	Security Scanner	Nessus, ISS
	Network Attack	DoS Tools (trinoo, TFN, …)
Listening	Sniffers	Ethercap, tcpdump, juggernaut
	Application	XKey, WebSpy
First Access	Password Cracking	John the Ripper, L0pth Crack
	MailBombing	Avalanche
	Hijacking	Arp0c, ArpRedirect, Ethereal
Stealth	Rootkits	Different rootkits depending on OS
	Trojans	Netbus, BackOrifice

Conclusion

"Ethical hacking" seems to be a new buzz word although the techniques and ideas of testing security by attacking an installation aren't new at all. Administrators tested their systems already decades ago and even discussed their ideas and findings in public[16]. Nevertheless, ethical hacking provides results which can be used to strengthen a information technology environments security nearly immediately. The revealed vulnerabilities and problems may lead to a successful compromise of one or multiple systems – ethical hacking provides data which is based on real tests, which have been successful after all. Problems detected by an ethical hack are for real and should be treated in such a way – fixing the security holes is required. An ethical hack per se doesn't fix or improve the security at all – it does provide information about what should be fixed.

In order to fully evaluate a client environment security, a complete ethical hacking is required. Testing internal, external as well as connections to partner networks are needed to draw a comprehensive picture. Testing all these networks and systems does need time – time a professional has to spend to scan, test and attack systems. Ethical hacking is not a process which can be automated – human interaction is needed or the ethical hacking is degraded to a simple vulnerability scan. This is one reason why an ethical hack does have a certain price tag. Unfortunately a lot of companies are offering so called ethical hacking services for a bargain – if they are really conducting an ethical hack is open but I do have my doubts.

After all, ethical hacking will play a certain role in the security assessment offerings and certainly has earned its place among other security assessments.

[16] SATAN (Security Administrator Tool for Analyzing Networks) was one tool that was developed in 1995 for administrators to test their environment for vulnerabilities. The developers discussed their findings on usenet and decided to write a document for the administrators on how to attack their systems to test the security. More information can be found at http://www.fish.com/satan/

References

Palmer, C. C. “Ethical Hacking”
URL: http://www.research.ibm.com/journal/sj/403/palmer.html (22.11.2002)

Shell, B. “Ethical Hacking”
URL: http://css.sfu.ca/update/ethical-hacking.html (22.11.2002)

RattleSnake. “Ethical Haking”
URL: http://neworder.box.sk/tomread.php?newsid=921 (22.11.2002)

Chapple, Jim. “Vulerability Assessments: An Ethical Hacker’s Perspective”.
URL: http://www.csc.com/features/2002/uploads/EthicalHackingWhitePaper.doc (22.11.2002)

Van der Walt, Charl. “What is Risk Assessment?”
URL: http://online.securityfocus.com/infocus/1591 (22.11.2002)

Ryan Net Works. “Security – Hacking Methodology”
URL: http://www.cybertrace.com/papers/hack101.html (22.11.2002)

Long, Neil J. “Securing your assets?”
URL: http://adsm-symposium.oucs.ox.ac.uk/1999/papers/neil/tsld001.htm (22.11.2002)

McClure, Stuart. Hacking Exposed 3rd Edition. Osborne/McGraw-Hill, 2001

Skoudis, Ed. Counter Hack. Prentice Hall, 2002

Chirillo, John. Hack Attacks Revealed. John Wiley & Sons, Inc, 2001

Anonymous, Maximum Linux Security, Sams Publishing, 1999