Security Prevention with Effective Hacking from Malicious Hackers

[1]Devendra R. Bandbuche

Assistant Professor, MCA Department
P.R.M.I.T. & R. Bandera, Amravati, Maharastra India

1. Introduction :

The internet has considerably enhanced various business critical operation of companies of different industry sector across the globe. However, as more and more organization become partially or completely dependent on internet, computer security and the threat of computer criminals come to the foreground. A single network infiltration can cause severe losses totaling in millions of dollars. Unfortunately, most organization across the globe continue to remain oblivious o to the threat posed by computer criminals, corporate espionage and cyber terrorism. Ethical Hacking – also known as penetration testing or white-hat hacking involves the same tools, tricks, and techniques that hackers use, but with one major difference: Ethical Hacking is legal. Ethical Hacking is performed with the target’s permission. The intent of ethical hacking is to discover vulnerabilities from hacker’s viewpoint so system can be better secured. It is part of an overall information risk management program that allows for ongoing security improvements. Ethical Hacking can also ensure that vendor’s claims about the security of their products are legitimate.

Ethical Hacking term is us to describe hacking performed by a company or individual to help identify potential threats on a computer or a network. An Ethical Hackers attempts to bypass way past the system security and search for any weak points that could be exploited by malicious hackers. This information is then used by the organization to improve the security, in an effort to minimize or eliminate, any potential attacks.

The world increasing numbers of governments and public authorities are relying on IT infrastructures to perform a wide range of duties. Almost everything is interconnected nowadays, and people in all positions are accustomed at shuttling information where it is needed. News reports on the alarming growth of information technology- related crimes have reached the general public. Some incidents have been widely publicised, resulting in an overall impression. A deliberate criminal action can target information wherever it sits [3].

2. Literature review :

The growing dependence and importance regarding information technology present within our society is increasingly demanding that professionals find more effective solutions relating to security concerns. Individuals with unethical behaviors are finding a variety of ways of conducting activities that cause businesses and consumers much grief and vast amounts annually in damages. As information security continues to be foremost on the minds of information technology professionals, improvements in this area are critically important. One area that is very promising is penetration testing or Ethical Hacking. The purpose of this paper is to examine effective offerings within public and private sectors to prepare security professionals. These individuals must be equipped with necessary tools, knowledge, and expertise in this fast growing proactive approach to information security. Following this examination a proposed model of Ethical Hacking instructional plan will be addressed. One of the more effective ways of testing network security is penetration testing or ethical hacking. activities focus on the identification and exploitation of security vulnerabilities, and subsequent implementation of corrective measures (Using an Ethical Hacking Technique). Organizations are increasingly evaluating the success or failure of their current security measures through then use of ethical hacking processes. According to some “’ethical hacking’ may be one of the most effective ways to proactively plug rampant security holes”. Moreover, many security experts encourage organizations to hire ethical hackers to test their networks (Leung, 2005). Ethical Hacking according to those within the security field, more information technology professionals going back to class to learn the "latest hacking techniques” [3].

In fact, many consider the three to five day seminars to be less expensive than hiring consultants. The average cost is $2,000 to $8,000 per person while consulting services range from $10,000 to $100,000. According to the 2005 Computer Crime and Security Survey, virus attacks continue as the source of greatest financial loss. Unauthorized use increased slightly over the previous year, while unauthorized access to information and theft of proprietary information significantly increased in average dollar loss per respondent. Even more alarming, web site incidents have increased significantly over the previous year. Some of the more prominent programs at community colleges and universities vary in intensity and course content. Syracuse University offers a Cyber Security Boot Camp to prepare future technology security professionals. Topics include cyber security, cryptography digital forensics, network security, and wireless security.

Some of the more prominent programs at community colleges and universities vary in intensity and course content. Syracuse University offers a Cyber Security Boot Camp to prepare future technology security professionals. Topics include cyber security, cryptography, stegnography, digital forensics, network security, and wireless security. There are stringent rules for entry into the program, and the Boot Camp ends with "Hack fest" which is a hands-on event putting into practice the theoretical concepts covered within the course. In Paris, Zi Hackademy, offers hacking courses to a wide variety of students. The school's philosophy is "only if you become a hacker can you understand how hackers think and operate". The University of Glamorgan and a leading information security firm 7Safe offer certifications in penetration testing and information security with additional topics [5].

The leaders of the program protest that unethical individuals are not attracted to the course due to the high cost of the program and the availability of free hacking tools and web sites on the Internet. In addition, applicants to the program must sign a legally binding document in which they agree to use their skills for only ethical and legal activities (Goodwin, 2004). A group of individuals called the Ghetto hackers are trying to change way society views hackers. They enable people that are curious about information security to get hands on experience without any harm to others. Their mission is to change culture from within and to better educate the public at large concerning hacking. In addition, their main focus is to stress the importance of teaching ethics as well general hacking concepts. ethical is an often overused and misunderstood word, the Merriam-Webster dictionary defines ethical perfectly for the context of this book and the professional security testing techniques that cover that is, conforming to accepted professional standards of conduct.

Ethical hacking — also known as penetration testing or white-hat hacking involves the same tools, tricks, and techniques that hackers use, but with one major difference: Ethical hacking is legal. Ethical hacking is performed with the target's permission. The intent of ethical hacking is to discover vulnerabilities from a hacker's viewpoint so systems can be better secured. It's part of an overall information risk management program that allows for ongoing security improvements. Ethical hacking can also ensure that vendors' claims about the security of their products are legitimate.

2.1 Ethical and Legal Concerns -

When creating a lab of this nature, it is necessary to answer the relevant ethical and legal questions. In this case, there are two questions that need to be addressed.

1.The first is whether it is ethical (and responsible) to instruct students in the tools and techniques of computer attack?

2. The second question is what ethical and legal dangers are there in mistakes occurring with a lab that encourages dangerous tool Use?

There are three positions with regard to systems attack instruction: first, that any attack, regardless of motive and Second, for academic attack/Defend purpose is unethical tools and there is a some students to use the techniques in an responsible manner and therefore instructors should not take on the responsibly of teaching new hackers. The last infrastructure of tomorrow. Denying computer security students practical knowledge of computer security, and "hacking" poorly prepares them for the work they will do in industry, government, and business. RADICL is a necessary part of preparing students at the University of Idaho for their careers. One cannot build or architect defenses for attacks that one does not truly understand.

The second question to address is of the legal responsibility if the lab were intentionally or mistakenly misused. The liability can be mitigated by educating the lab users on their ethical responsibilities. Pursuant to the US v Morris decision, an individual is liable for the accidental release of malicious software under the Computer Fraud and Misuse Act liability can be mitigated by educating the lab users on their ethical responsibilities. Pursuant to the US v Morris decision, an individual is liable for the accidental release of malicious software under the Computer Fraud and Misuse Act (18 USC 1030) [1]. There are basic precautions in place to protect networks outside of the RADICL lab. First, RADICL is an isolated, air-gaped network. Second, information does not leave the lab in any form other than hand written notes and printed paper. This prevents malicious code from affecting other machines. Our first line of defense is the moral and ethical education of our students. Ultimately any lab or network must rely on the ethical conduct of its participants. Ethical behavior is a mandatory part of our computer science curriculum.

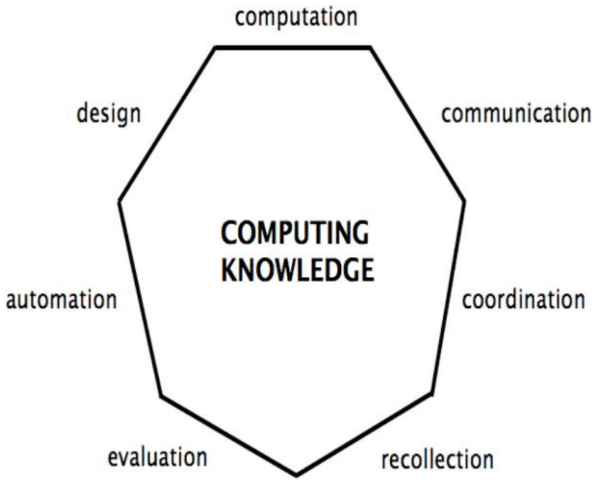


Figure. Categories of the Great Principles (GP) framework

The next three sub-sections describe three common DOS attacks, namely, the Land, the TCP SYN flood, and the Teardrop attacks. For each DOS attack, the corresponding hands-on lab exercise implementation is described. The learning objective of the lab exercises is for students to learn how to implement and detect the DOS attacks in isolated network laboratory environment.

The implementation of the hands-on lab exercises requires heavy involvement of the students. At the beginning of each hands-on lab exercise the instructor briefly summarizes the theoretical concepts related to the DOS attacks which have been already taught in the lecture.

Then, the instructor provides the students with the required network architecture setting, the necessary tools to generate and sniff the DOS attack traffic, the network devices (switch and/or routers), and the Intrusion Detection System

(IDS) tool to be used to detect the generated DOS attacks. During the hands-on lab exercises, students work in small groups (three or four students in each group) and are asked to perform mainly the following tasks within one hour:

1. Set up the required network architecture
2. Generate the DOS attacks using packet builder tools
3. Sniff the generated DOS attack traffic using sniffer tools
4. Configure the IDS tool to detect the generated DOS attacks
5. Each group, submit a report including mainly:

Screen shots for the generated DOS attack traffic where they show the contents of the packet's fields corresponding to the DOS attacks

Screen shots for the event logs generated by the IDS tool.

2.2 Types of attacks in Ethical hacking :

Attacks from the Internet to public services
- Attack targets, aggressors and methods
- Information gathering
- IP address and port scan
- Searching for vulnerabilities
- Performing tests and attacks
- Manual and automated checks

Attacks against the internal network with insider help
- Preparing an attack: planning for obtaining insider help
- Social engineering and information gathering
- Performing the attack
- Phishing
- Installing and exploiting backdoors
- Inside-out attacks
- Firewall rule evasion

Attacks against data confidentiality
- Tapping information in a networked environment
- Man-in-the-middle attacks: tapping SSL connections from an Internet Café
- Attacking wireless networks in semi-public environments (e.g. hotel)
- Sniffing in a switch-based environment

Attacks against Network-infrastructure
- Connecting into a network through a rogue modem attached to a computer behind a firewall.
- Exploiting weaknesses in network transport mechanisms, such as TCP/IP and NetBIOS.
- Flooding a network with too many requests, creating a denial of service (DOS) for legitimate requests.
- Installing a network analyzer on a network and capturing every packet that travels across it, revealing confidential information in clear text.
- Piggybacking onto a network through an insecure 802.11b wireless configuration.

2.3 Who are Ethical hackers

Hacker is a word that has two meanings:

1) Traditionally, a hacker is someone who likes to tinker with software or electronic systems. Hackers enjoy exploring and learning how computer systems operate. They love discovering new ways to work electronically.

2) someone who maliciously breaks into systems for personal gain. Technically, these criminals are crackers (criminal hackers). Crackers break into (crack) systems with malicious intent. They are out for personal gain: fame, profit, and even revenge. They modify, delete, and steal critical information, often making other people miserable.

2.4 Types of Ethical Hacker

The good-guy (white-hat) hackers don't like being in the same category as the bad-guy (black-hat) hackers. (These terms come from Western movies where the good guys wore white cowboy hats and the bad guys wore black cowboy hats.) Whatever the case, most people give hacker a negative connotation. Many malicious hackers claim that they don't cause damage but instead are altruistically helping others. Yeah, right. Many malicious hackers are electronic Thieves

Hackers (or bad guys) try to compromise computers.
Ethical hackers (or good guys) protect computers against illicit entry.
Hackers go for almost any system they think they can compromise. Some prefer prestigious, well-protected systems, but hacking into anyone's system increases their status in hacker circles.

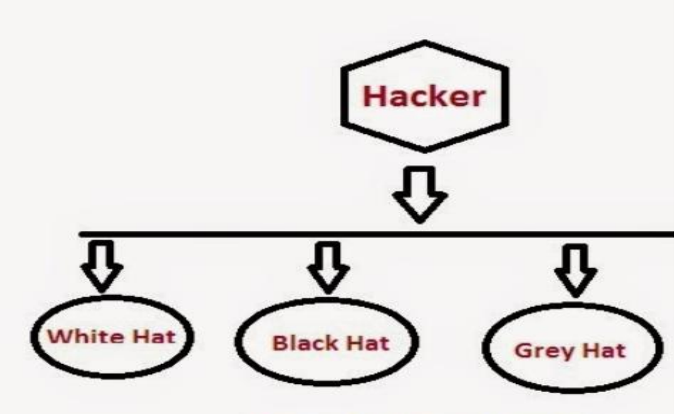


Figure: 1.1 Types of Hacker.

3. Architecture

Like practically any IT or security project, ethical hacking needs to be planned in advance. Strategic and tactical issues in the ethical hacking process should be determined and agreed upon. Planning is important for any amount of testing — from a simple password-cracking test to an all-out penetration test on a Web application.

3.1 Formulating your plan

Approval for ethical hacking is essential. Make what you're doing known and visible at least to the decision makers. Obtaining sponsorship of the project is the first step. This could be your manager, an executive, a customer, or even yourself if you're the boss. You need someone to back you up and sign off on your plan. Otherwise, your testing may be called off unexpectedly if someone claims they never authorized you to perform the tests. Get written approval on this sponsorship as soon as possible to ensure that none of your time or effort is wasted. A well-defined scope includes the following information:

- Specific systems to be tested
- Risks that are involved
- when the tests are performed and your overall timeline
- How the tests are performed
- How much knowledge of the systems you have before you start testing
- What is done when a major vulnerability is discovered
- The specific deliverables this includes security-assessment reports

and a higher-level report outlining the general vulnerabilities to be addressed, along with countermeasures that should be implemented The best approach is an unlimited attack, wherein any type of test is possible. The bad guys aren't hacking your systems within a limited scope, so why should you? Some exceptions to this approach are performing DoS, socialengineering,

and physical-security tests Don't stop with one security hole. This can lead to a false sense of security.

3.2 Selecting tools

As with any project, if you don't have the right tools for ethical hacking, accomplishing the task effectively is difficult The more tools you have, the easier your ethical hacking efforts are. Make sure you that you're using the right tool for the task:

To crack passwords, you need a cracking tool such as LC4, John the Ripper, or pwdump.A general port scanner, such as SuperScan, may not crack passwords.

For an in-depth analysis of a Web application, a Web-application assessment tool (such as Whisker or WebInspect) is more appropriate than a network analyzer (such as Ethereal). When selecting the right security tool for the task, ask around. Get advice from your colleagues and from other people online. A simple Groups search on Google (www.google.com) or perusal of security portals, such as SecurityFocus.com, SearchSecurity.com, and ITsecurity.com, often produces great feedback from other security experts Hundreds, if not thousands, of tools can be used for ethical hacking — from your own words and actions to software-based vulnerability-assessment programs to hardware-based network analyzers.

The following list runs down some of commercial, freeware, and open-source security tools:

- Nmap
- EtherPeek
- SuperScan
- QualysGuard
- WebInspect
- LC4 (formerly called L0phtcrack)
- LANguard Network Security Scanner
- Network Stumbler
- ToneLoc

Here are some other popular tools:

- Internet Scanner
- Ethereal
- Nessus
- Nikto
- Kismet
- THC-Scan

The capabilities of many security and hacking tools are often misunderstood. This misunderstanding has shed negative light on some excellent tools, such as SATAN (Security Administrator Tool for Analyzing Networks) and Nmap (Network Mapper).

3.3 Executing the plan

Ethical hacking can take persistence. Time and patience are important. Be careful when you're performing your ethical hacking tests. A hacker in your network or a seemingly benign employee looking over your shoulder may watch what's going on. This person could use this information against you. It's not practical to make sure that no hackers are on your systems before you start. Just make sure you keep everything as quiet and private as possible. This is especially critical when transmitting and storing your test results. If possible, encrypt these e-mails and files using Pretty Good Privacy (PGP) or something similar. At a minimum, password-protect them.

3.4 Evaluating results

Assess your results to see what you uncovered, assuming that the vulnerabilities haven't been made obvious before now. This is where knowledge counts. Evaluating the results and correlating the specific vulnerabilities discovered is a skill that gets better with experience. You'll end up knowing your systems as well as anyone else. This makes the evaluation process much simpler moving forward. Submit a formal report to upper management or to your customer, outlining your results. Keep these other parties in the loop to show that your efforts and their money are well spent.

4. Methodology

An ethical hacking methodology is quite similar to a hacking methodology 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 port scans (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. 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).

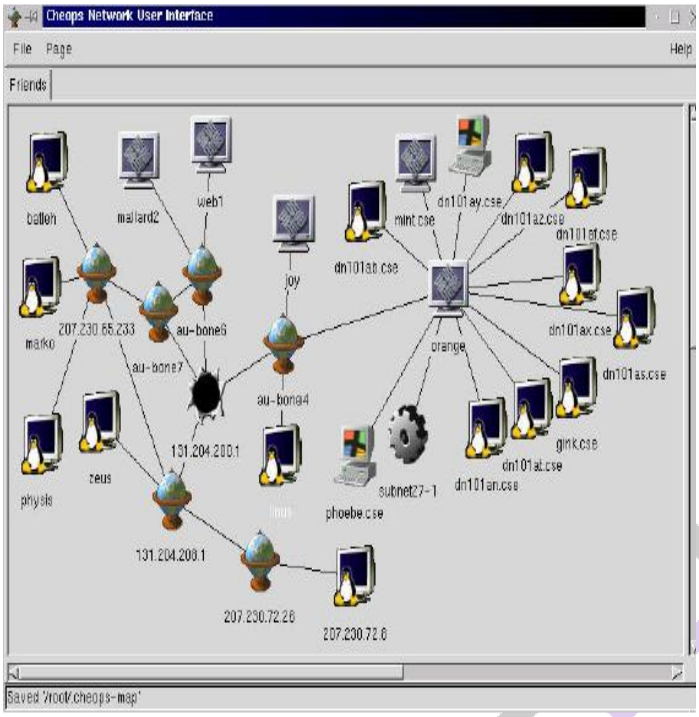


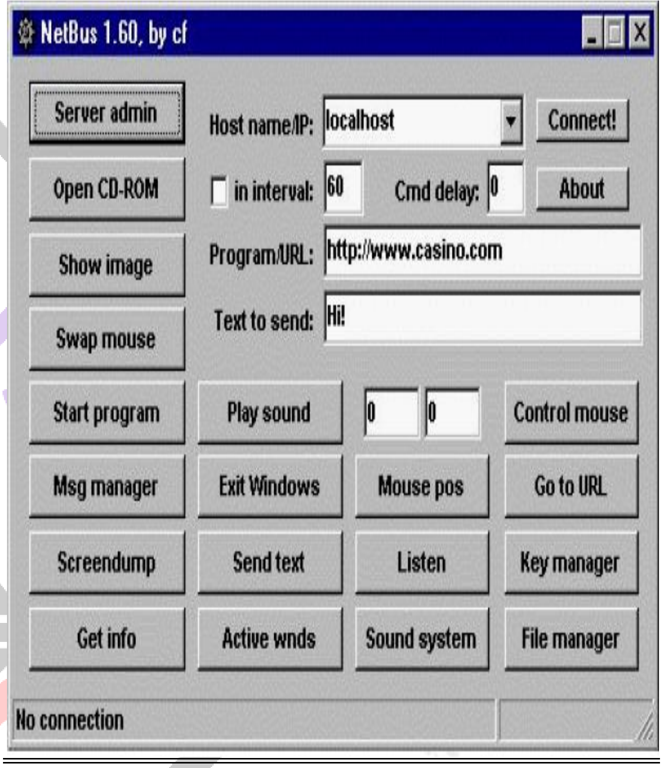
Fig. Cheops Screenshot (Source Cheops homepage)

4.1 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 who is, 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. 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.

4.2 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 Net Bus (see figure) 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.



Host name/IP: localhost

☐ in interval: 60 Cmd delay: 0

Program/URL: http://www.casino.com

Text to send: Hi!

0 0

No connection

Fig. NetBus screenshot

4.3 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.

4.4 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 suidenabled programs on Unix

based systems), changing files which can enable new access patterns (like file), intercepting communications or browsing local files for useful pieces of information.

4.5 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. ending 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.

4.6 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 rootkits15 and cleaning relevant log files is imperative to stay undercover, to go stealth [5].

5. Advantages & Disadvantages

Advantages

Most of the benefit of are obivious but most of them are overlooked. the advantage range from simply preventing malicious hacking to prevent national security. These advantages include:

1. Fighting against terrorism and national security breaches.
2. Having a computer system that prevent malicious hackers from gaining access.
3. Having adequate preventive measure in place to prevent security breaches.
4. Understanding hackers techniques.
5. Finding vulnerable areas.
6. Preparing for hackers attacks.

Disadvantages

As with all activities which have a darker side, there will be dishonest people presenting drawbacks. The possible disadvantage of ethical hacking include:

1. The ethical hackers using the knowledge they gain to do malicious hacking activities.
2. The possibility that ethical hacker will send and/or place malicious code, viruses, malware, and other destructive and harmful things
3. Allowing the company's financial and banking details to be seen.
4. Massive security breach.

6. Application :

Applications take a lot of hits by hackers. Programs such as e-mail server software and Web applications often are beaten down:

- Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) applications are frequently attacked because most firewalls and other security mechanisms are configured to allow full access to these programs from the Internet.
- Malicious software *(malware)* includes viruses, worms, Trojan horses, and spyware. Malware clogs networks and takes down systems.
- *Spam* (junk e-mail) is wreaking havoc on system availability and storage space. And it can carry malware.

Ethical hacking helps reveal such attacks against your computer systems.

Networks can be reached from anywhere in the world via the Internet. Here are some examples of network-infrastructure attacks:

- Connecting into a network through a rogue modem attached to a computer behind a firewall
- Exploiting weaknesses in network transport mechanisms, such as TCP/IP and NetBIOS.
- Flooding a network with too many requests, creating a denial of service (DOS) for legitimate requests.
- Installing a network analyzer on a network and capturing every packet that travels across it, revealing confidential information in clear text.

Treat the information you gather with the utmost respect. All information you obtain during your testing from Web-application log files to clear-text passwords must be kept private. Don't use this information to snoop into confidential corporate information or private lives. If you sense that someone should know there's a problem, consider sharing that information with the appropriate manager.

7. Conclusion & Future scope :

Conclusion

Ethical hacking is legal. Ethical hacking is performed with the target's permission. The intent of ethical hacking is to discover vulnerabilities from a hacker's viewpoint so systems can be better secured. It's part of an overall information risk management program that allows for ongoing security improvements Never underestimate the attackers or overestimate our existing posture. To protect against an attack, understanding where the system are vulnerable is necessary. Ethical hacking helps to first comprehend their risk and then, manage them. Effective ethical hacking course offerings are being provided by 3universities as well as “boot camps” offered by private organizations. A variety of programs indicate a wide array of content, target audience, cost, and duration. The community college system provides a very effective platform for offering ethical hacking course concepts and applications [2].

Future scope

In india companies like wipro , Infosys, and IBM are interested in employing ethical hackers. Moreover, salaries are higher than other areas of IT. If your are well versed with the inner workings of a system and have the capabilities to discover new weakness in an otherwise secure system, then you will find it easy to build your career and take it to the next higher level.Ethical hacking can be taken as career option.

References :

Book:

1. Ankit fadiya , e-book-ca-corporate-security-excerpt

Research paper:

[1] P. J. Denning, Great principles of computing, Communications of the ACM, 46(11)15-20, 2003
[2] Cisco Systems, Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide
[3] J Harris Maintaining ethical standards for computer security curriculum Proc of the 1st Annual Conference on Information Security Curriculum Development
[4] CRITICAL INFRASTRUCTURE AND COMPUTER SECURITY
[5] RTFn Enabling Cyber security Education through a Mobile
[6] Hacking For Dummies
[7] D. Yuan, and J. Zhong, A lab implementation of SYN flood attack and defense, Proc. of the 9th ACM SIGITE conference on Information Technology Education, ACM, pp. 57-58, 2008.
[8] Ethical Hacking R. Hartley .