

Unit-5 Basics of Hacking

Contents

5.1 Ethical Hacking

How Hackers Beget Ethical Hackers

Defining hacker, malicious users

5.2 Understanding the need to hack your own systems

5.3 Understanding the dangers your systems face

Nontechnical attacks

Network-infrastructure attacks

Operating-system attacks

Application and other specialized attacks

5.4 Obeying the Ethical hacking Principles

Working ethically

Respecting privacy

Not crashing your systems

5.5 The Ethical hacking Process

Formulating your plan

Selecting tools

Executing the plan

Evaluating results

Moving on

5.6 Cracking the Hacker Mind-set

What you're Up Against?

Who breaks in to computer systems?

Why they do it?

Planning and Performing Attacks

Maintaining Anonymity

5.1 Ethical Hacking: History

Hacking developed alongside "Phone Phreaking", a term referred to exploration of the phone network without authorization, and there has often been overlap between both technology and participants.

Ethical hacking is the science of testing computers and network for security vulnerabilities and plugging the holes found before the unauthorized people get a chance to exploit them.

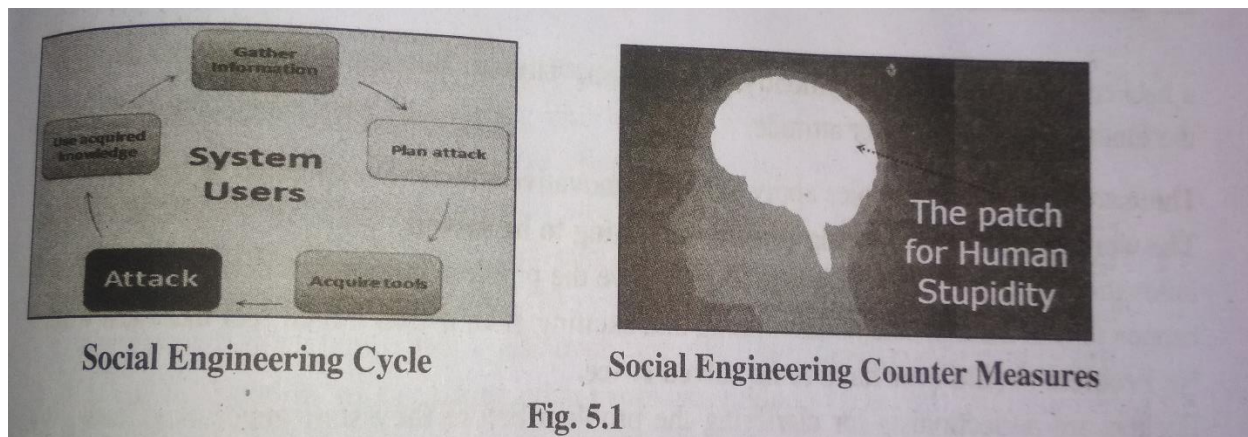


Fig. 5.1

Gather Information: This is the first stage, the learns as much as he can about the intended victim. The information is gathered from company websites, other publications and sometimes by talking to the users of the target system.

Plan Attack: The attackers outline how he/she intends to execute the attack

Acquire Tools: These include computer programs that an attacker will use when launching the attack.

Attack: Exploit the weaknesses in the target system.

Use acquired knowledge: Information gathered during the social engineering tactics such as pet names, birthdates of the organization founders, etc. is used in attacks such as password guessing. Most techniques employed by social engineers involve manipulating human biases. To counter such techniques, an organization can;

- ✓ To counter the familiarity exploit
- ✓ To counter intimidating circumstances attacks
- ✓ To counter phishing techniques
- ✓ To counter tailgating attacks
- ✓ To counter human curiosity
- ✓ To counter techniques that exploit human greed

Summary

- Social engineering is the art of exploiting the human elements to gain access to unauthorized resources.

- Social engineers use a number of techniques to fool the users into revealing sensitive information.
- Organizations must have security policies that have social engineering countermeasures.

Hacker's attitude:

A hacker-cracker separation give more emphasis to a range of different categories, such as white hat (ethical hacking), grey hat, black hat and script kiddie. The term cracker refer to black hat hackers, or more generally hackers with unlawful intentions.

Hackers are problem solvers. They get extract from understanding a problem and sorting out a solution. Their motivation to meet challenges is internal. Hackers do what they do because its extremely satisfying to solve puzzles and fix the up-until-now unfixable. The pleasure derived is both intellectual and practical but one don't have to be a geek to be a hacker. Being a hacker is a mind-set. In Raymond's dissertation, "How to Become a Hacker", he describes the fundamentals of a hacker attitude.

These are very same principles apply to being innovative which are explained as below:

The world is full of fascinating problems waiting to be solved.

Innovation happens because hackers like to solve the problem rather than complaining. If one happen to find these problems fascinating and exciting, then it won't even feel like hard work.

No Problem should ever have to be solved twice.

Hackers are perfectionists for clarifying the problem before they start generating ideas. It's easy to jump to solutions, but sometimes that means wrong problems are solved. A little bit of accuracy on the front end of a problem solving process means one tackles the right and real problem, so one only have to do it once.

Boredom and drudgery (more and more work) are evil.

The best way to lose touch with innovation is to become too repetitive. Innovation requires constant and vigilant creativity It may not be broken enough to fix, but there's no reason not to squeeze it and cut boredom off at the pass.

Freedom is good.

Hackers need freedom to work upon their ideas.

Attitude is no substitute for competence.

They are open-minded and they see problems as interesting opportunities. Innovators are seeking to understand a problem more deeply, puzzling at how an unworkable idea might become workable, increasing their skill set so that they are better problem solvers and can better execute their ideas. Hackers are the innovators of the Internet. Overall hackers are who have got that relentless, curious, problem-solving attitude.

Computer Hacking

Computer Hackers have been in existence for more than a century. Originally, "hacker" did not carry the negative implications. In the late 1950s and early 1960s, computers were much different than the desktop or laptop systems most people are familiar with. In those days, most companies and universities used mainframe computers: giant, slow-moving hunks of metal locked away in temperature-controlled glass cages. It cost thousands of dollars to maintain and operate those machines, and programmers had to fight for access time. Because of the time and money involved, computer programmers began looking for ways to get the most out of the machines. The best and brightest of those programmers created what they called "hacks" - shortcuts that would modify and improve the performance of a computer's operating system or applications and allow more tasks to be completed in a shorter time. Still, for all the negative things hackers have done, they provide a necessary (and even valuable) service, which hacking elaborated on after a brief timeline in the history of computer

- **How Hackers Beget Ethical Hackers**

Hacker is a word that has two meanings:

- ✓ Traditionally, a hacker is someone who likes to tamper with software or electronic systems. Hackers enjoy, exploring and learning how computer systems operate they love discovering new ways to work electronically.
- ✓ Recently, hacker has taken on a new meaning 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.

The good-guy (white-hat) hackers don't like being in the same category as the bad guy (black-hat) hackers. Whatever the case, most people give hacker a negative meaning many malicious hackers claim that they don't cause damage but instead are selflessly helping others. In other words, many malicious hackers are electronic thieves. 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.

If one need protection from hacker troubles; one has to become as savvy as the gays trying to attack systems. A true security assessment professional possesses the skills, mind-set, and tools of a hacker but is also trustworthy, He or she performs the hacks as security tests against systems based on how hackers might work.

Ethical hacker's attitude encompasses formal and methodical penetration testing, white hat hacking, and vulnerability testing ,which involves the same tools, tricks, and techniques that criminal hackers use, but with one major difference: Ethical hacking is performed with the

target's permission in a professional setting The intent of ethical hacking is to discover vulnerabilities from a malicious attacker's viewpoint to better secure systems. Ethical hacking is part of an overall information risk management program that allows for on-going security improvements. Ethical hacking can also ensure that vendors' claims about the security of their products are genuine.

Ethical hacking versus auditing

Many people confuse security testing via the ethical hacking approach with security auditing, but there are big differences, namely in the objectives.

Security auditing involves comparing a company's security policies (or compliance requirements) to what's actually taking place. The intent of security auditing is to validate that security controls exist using a risk-based approach.

Auditing often involves reviewing business processes and, in many cases, might not be very technical. Security audits are usually based on checklists. Equally, security assessments based around ethical hacking focus on vulnerabilities that can be exploited. This testing approach validates that security controls do not exist or are incompetent at best.

Ethical hacking can be both highly technical and nontechnical, and although one can use a formal methodology, it tends to be a bit less structured than formal auditing.

Policy considerations

If it is chosen to make ethical hacking an important part of business's information risk management program, one really need to have a documented security testing policy. Such a policy outlines who's doing the testing, the general type of testing that is performed, and how often the testing takes place.

What is Hacking?

Hacking is identifying weakness in computer systems or networks to exploit its weaknesses

To gain access.

Example of Hacking:

Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses.

- ✓ Using password cracking algorithm to gain access to a system.
- ✓ This exposes them to the outside world and hacking. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc.
- ✓ Cybercrimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming up with countermeasures that protect the weaknesses. Ethical hacking is a branch of information security or information assurance which tests an organization's information systems against a variety of attacks. Ethical hackers are also sometimes known as **White Hats**. Many people are confused when the terms "Ethical" and "Hacking" are used together. Usually the term "hacker" has a negative connotation due to media reports using incorrect terminology.

Ethical hackers must abide by the following rules:

- ✓ Get written permission from the owner of the computer system and/or computer network before hacking.
- ✓ Protect the privacy of the organization been hacked.
- ✓ Transparently report all the identified weaknesses in the computer system to the organization.
- ✓ Inform hardware and software vendors of the identified weaknesses.

Definition

Ethical hacking:

- ✓ Refers to the act of locating weaknesses and vulnerabilities of computer and information systems by duplicating the intent and actions of malicious hackers.
- ✓ known as penetration testing, intrusion testing, or red teaming,

An ethical hacker is a security professional who applies their hacking skills for defensive purposes on behalf of the owners of information systems,

By conducting penetration tests, an ethical hacker looks to answer the following four basic

1. What information/locations/systems can an attacker gain access?
2. What can an attacker see on the target?
3. What can an attacker do with available information?
4. Does anyone at the target system notice the attempts?

An ethical hacker operates with the knowledge and permission of the organization for which they are trying to defend. In some cases, the organization will neglect to inform their information security team of the activities that will be carried out by an ethical hacker in an attempt to test the effectiveness of the information security team. This is referred to as a double-blind environment. In order to operate effectively and legally, an ethical hacker must be informed of the assets that should be protected, potential threat sources, and the extent to which the organization will support an ethical hacker's efforts.

Defining hacker, malicious users

Definition of Hacker: A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security. **An Ethical Hacker**, also known as a white hat hacker, or simply a white hat, is a security professional who applies their hacking skills for defensive purposes on behalf of the owners of information systems.

Nowadays, certified ethical hackers are among the most sought after information security employees in large organizations such as Wipro, Infosys, IBM, Airtel and Reliance among others.

What Is a Malicious User?

Malicious users (or internal attackers) try to compromise computers and sensitive information from the inside as authorized and "trusted" users. Malicious users go for systems they believe they can compromise for fraudulent gains or revenge.

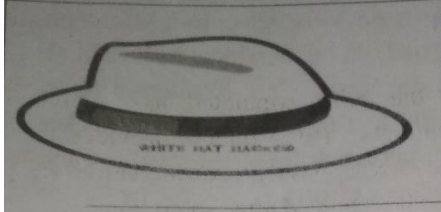
- ✓ Malicious attackers are, generally known as both, hackers and malicious users.
- ✓ Malicious user means a rogue employee, contractor, intern, or other user who abuses his or her trusted privileges it is a common term in security circles.




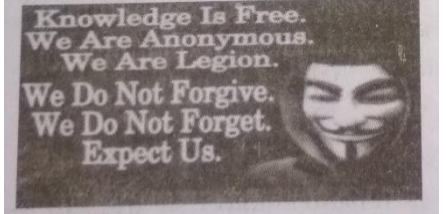

Users search through critical database systems to collect sensitive information, e-mail confidential client information to the competition or elsewhere to the cloud, or delete sensitive files from servers that they probably do not have access. There's also the occasional ignorant insider whose intent is not malicious but who still causes security problems by moving, deleting, or corrupting sensitive information. Even an innocent "fat-finger" on the keyboard can have terrible consequences in the business world.

Malicious users are often the worst enemies of IT and information security professionals because they know exactly where to go to get the goods and don't need to be computer savvy to compromise sensitive information. These users have the access they need and the management trusts them, often without question. In short they take the undue advantage the trust of the management.

Hackers are classified according to the intent of their actions.

Table 5.1 Classifications of hackers according to their intent.

Symbol	Description
	Ethical Hacker (White hat): A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments.

	<p>Cracker (Black hat): A hacker who gains unauthorized access to computer systems for The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.</p>
	<p>Grey hat: A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.</p>
	<p>Script kiddies: A non-skilled person who gains access to computer systems using already made tools.</p>
	<p>Hactivist: A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.</p>
	<p>Phreaker: A hacker who identifies and exploits weaknesses in telephones instead of computers.</p>

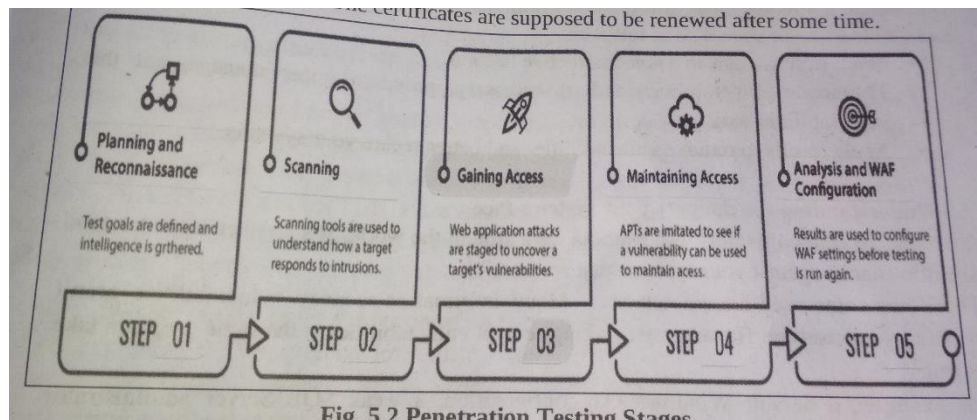
Why Ethical Hacking?

- Information is one of the most valuable assets of an organization. Keeping information secured can protect an organization's image and save an organization a lot of money.
- Hacking can lead to loss of business for organizations that deal in finance such as PayPal. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.

Legality of Ethical Hacking

Ethical Hacking is legal if the hacker abides by the rules stipulated as

The International Council of E-Commerce Consultants (EC-Council) provides a certification program that tests individual's skills. Those who pass the examination are awarded with certificates. The certificates are supposed to be renewed after some time.



5.2 Understanding the need to hack your own systems

To catch a thief, think like a thief. That's the basis for ethical hacking. The law of averages works against security. With the increased numbers and expanding knowledge of hackers combined with the growing number of system vulnerabilities and other unknowns, the time will come when all computer systems are hacked or compromised in some way. Protecting your systems from the bad guys and not just the generic vulnerabilities that everyone knows about is absolutely critical. When the hacker tricks are known, one can see how vulnerable the systems are.

Hacking targets on weak security practices and undisclosed vulnerabilities. Firewalls, encryption, and virtual private networks (VPNS) can create a false feeling of safety. These security systems often focus on high-level vulnerabilities, such as viruses and traffic through a firewall, without affecting how hackers work. Attacking your own systems to discover vulnerabilities is a step to making them more secure. This is the only proven method of greatly hardening your systems from attack. If weaknesses are not identified, it's a matter of time before the vulnerabilities are exploited.

As hackers expand their knowledge, one should also gain the required knowledge of it you must think like them to protect your systems from them. As the ethical hacker, one must know activities hackers carry out and how to stop their efforts. One should know what to look for and how to use that information to spoil hackers' efforts.

One cannot protect the systems from everything. The only protection against everything is to unplug computer systems and lock them away so no one can touch them, not even you. That's not the best approach to information security. What's important is to protect your systems from known vulnerabilities and common hacker attacks, it's impossible to support all possible vulnerabilities on all systems. One can't plan for all possible attacks, especially the ones that are currently unknown.

However, the more combinations you try - the more you test whole systems instead of individual units, the better your chances of discovering vulnerabilities that affect everything as a whole.

Building the Foundation for Ethical Hacking

One should not forget about insider threats from malicious employees. One's overall goals as an ethical hacker should be as follows:

- ✓ Hack your systems in a non-destructive fashion.
- ✓ Enumerate vulnerabilities and, if necessary, prove to upper management that

Vulnerabilities exist.

- ✓ Apply results to remove vulnerabilities and better secure your systems.

5.3 Understanding the dangers your systems face

Systems are generally under fire from hackers around the world. It's another to understand specific attacks against your systems that are possible.

There are some well-known attacks. Many information-security vulnerabilities aren't critical by themselves. However, exploiting several vulnerabilities at the same time can take its toll. For example, a default Windows OS configuration, a weak SQL Server administrator password, and a server hosted on a wireless network may not be major security concerns separately. But exploiting all three of these vulnerabilities at the same time can be a serious issue as:

- ✓ Nontechnical attacks
- ✓ Network-infrastructure attacks
- ✓ Operating-system attacks
- ✓ Application and other specialized attacks

Nontechnical attacks

Exploits that involve manipulating people or end users and even yourself are the greatest vulnerability within any computer or network infrastructure. Humans are trusting by nature, which can lead to social-engineering exploits. Social engineering is defined as the exploitation of the trusting nature of human beings to gain information for malicious purposes.

Other common and effective attacks against information systems are physical. Hackers break into buildings, computer rooms, or other areas containing critical information or property.

Physical attacks can include dumpster diving (searching through trash cans and dumpsters for intellectual property, passwords, network diagrams, and other information).

Network-infrastructure attacks

Hacker attacks against network infrastructures can be easy, because many 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
- ✓ Piggybacking onto a network through an insecure wireless configuration.

Operating-system attacks Hacking

Operating Systems (OSs) is a preferred method of the bad guys (hackers). Operating systems comprise a large portion of hacker attacks simply because every computer has one and so many well-known exploits can be used against them.

Occasionally, some operating systems that are more secure out of the box, such as Novell Net Ware and the flavors of BSD UNIX are attacked, and vulnerabilities turn up. But hackers prefer attacking operating systems like Windows and Linux because they are widely used and better known for their vulnerabilities. Here are some examples of attacks on operating systems:

- ✓ Exploiting specific protocol implementations
- ✓ Attacking built-in authentication systems
- ✓ Breaking file-system security
- ✓ Cracking passwords and encryption mechanisms

Application and other specialized attacks

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 computer systems.

5.4. Obeying the Ethical Hacking Commandments

Every ethical hacker must abide by a few basic commandments. If not, bad things can happen:

- ✓ **Working ethically**

The word ethical in this context can be defined as working with high professional morals and principles. While performing ethical hacking tests against own systems or for someone who has hired for, everything one need to do as an ethical hacker must be above board and must support the company's goals. No hidden agendas are allowed. Trustworthiness is the ultimate principle. The misuse of information is absolutely forbidden. That's what the bad guys or hackers do.

✓ **Respecting privacy**

Treat the information gathered with the greatest respect. All information obtained during testing from Web-application log files to clear-text passwords must be kept private. This information shall not be used to watch into confidential corporate information or private lives. If you sense or feel that someone should know there's a problem, consider sharing that information with the appropriate manager. Involve others in process. This is a "watch the watcher" system that can build trust and support ethical hacking projects.

✓ **Not crashing your systems**

One of the biggest mistakes seen when people try to hack their own systems is inadvertently crashing their systems. The main reason for this is poor planning. These testers have not read the documentation or misunderstand the usage and power of the security tools and techniques. DoS-Denial of Service conditions on the systems are easily created when testing. Running too many tests too quickly on a system causes many system lockups. Things should not be rushed and assumed that a network or specific host can handle the beating that network scanners and vulnerability assessment tools can be useless. Many security-assessment tools can control how many tests are performed on a system at the same time. These tools are especially handy if one needs to run the tests on production systems during regular business hours. One can even create an account or system lockout condition by social engineering, changing a password, not realizing that doing so might create a system lockout condition.

5.5 The Ethical Hacking Process

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.

Formulating your plan

Approval for ethical hacking is essential. What is being done should be known and visible at least to the decision makers. Obtaining sponsorship of the project is the first step. This could be the manager, an executive, a customer, or even the boss. Someone is needed to back up and sign off on the plan. Otherwise, testing may be called off unexpectedly if someone claims they never authorized one to perform the tests.

The authorization can be as simple as an internal memo from the senior-most person or as if one is performing these tests on own systems. If the testing is for a customer, one should have a signed contract in place, stating the customer's support and authorization. Get written approval on this sponsorship as soon as possible to ensure that none of the time or effort is wasted. This documentation works as a proof as what one is doing when someone asks or demands. A detailed plan is needed, but that doesn't mean that it needs volumes of testing procedures. One slip can crash your systems.

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.
- ✓ When selecting systems to test, start with the most critical or vulnerable systems.

For instance, one can test computer passwords or attempt social engineering attacks before drilling down into more detailed systems. What if one is assessing the firewall or Web application, and one takes it down? This can cause system unavailability, which can reduce system performance or employee productivity. Even worse, it could cause loss of data integrity, loss of data, and bad publicity.

Handle social-engineering and denial-of-service attacks carefully. Determine how they can affect the systems you're testing and entire organization. Determining when the tests are performed is something that one must think long and hard about. Do the tester test during normal business hours? How about late at night or early in the morning so that production systems aren't affected? Involve others to make sure they approve tester's timing.

The best approach is an unlimited attack, wherein any type of test is possible. The hackers aren't hacking the systems within a limited scope. Some exceptions to this approach are performing DoS, social engineering, and physical-security tests. One should not stop with one security hole. This can lead to a false sense of security. One should keep going to see what else he/she can discover. It's not like to keep hacking until the end of time or until one crash all his/ her systems, Simply pursue the path he/she is going down until he//she can't hack it any longer. One of the goals may be to perform the tests without being detected, For example, one may be performing his/her tests on remote systems or on a remote office, and he/she doesn't want the users to be aware of what they are doing Otherwise, the users may be on to him/her and be on their best behavior.

Just a basic Extensive knowledge of the systems is not needed for testing understanding is required to protect the tested systems. Understanding the systems which are being tested shouldn't be difficult if one is hacking his/her own in-house systems. If hacking a customer's systems, one may have to dig deeper. In fact, most people are scared of these assessments. Base the type of test one will perform on his/her organization's or customer's needs.

• **Selecting tools**

If one don't have the right tools for ethical hacking, to accomplish the task is effectively difficult just using the right tools doesn't mean that all vulnerabilities will be discovered. Know the personal and technical limitations. Many security-assessment tools generate false positives and negatives (incorrectly identifying vulnerabilities). Some tools may miss vulnerabilities. Many tools focus on specific tests, but no one tool can test for everything. This is why a set of specific tools are required that can call on for the task at hand. The more are the tools, the easier ethical hacking efforts are. Make sure the right tool is being used for the task: To crack passwords, one needs a cracking tool such as LC4, John the Ripper, or pwdump.

A general port scanner, such as Supers can, may not crack passwords.

For an in-depth analysis of a Web application, a Web-application assessment tool (such as Whisker or Web Inspect) is more appropriate than a network analyzer (such as Ethereal). When selecting the right security tool for the task, ask around. Get advice from the 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.

Some of the widely used commercial, freeware, and open-source security tools:

- EtherPeek
 - Nmap
 - SuperScan
 - QualysGuard
 - WebInspect
 - LC4 (formerly called LOphterack)
 - 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). Some of these tools are complex. Whichever tools are being used, one should be familiarized with them before starting to use them. Here are ways to do that:

- ✓ Read the readme and/or online help files for tools.
- ✓ Study the user's guide for commercial tools.
- ✓ Consider formal classroom training from the security-tool vendor or another third-party training provider, if available.
- ✓ One should Look for these characteristics in tools for ethical hacking:
- ✓ Adequate documentation.
- ✓ Detailed reports on the discovered vulnerabilities, including how they may be exploited and fixed.
- ✓ Updates and support when needed.
- ✓ High-level reports that can be presented to managers or non-techie types.
- ✓ These features can save time and effort when writing the report.

• Executing the plan

Ethical hacking can take persistence. Time and patience are important. One should be careful when performing ethical hacking tests. A hacker in network or a seemingly gentle employee looking over one's shoulder may watch what's going on. This person could use this information against tester. It's not practical to make sure that no hackers are on one's systems before starting. Just one has to make sure to keep everything as quiet and private as possible. This is especially critical when transmitting and storing own test results. If possible, one should encrypt these e-mails and files using Pretty Good Privacy (PGP) or something similar. At a minimum, password-protect them. In an investigation mission, attach as much information as possible about the organization and systems, which is what malicious hackers do.

Start with a broad view and narrow down the focus:

1. Search the Internet for own organization name, computer and network system names, and the IP addresses. Google is a great place to start for this.
2. Narrow the scope, targeting the specific systems to be tested or being tested. Whether physical-security structures or Web applications, a casual assessment can turn up much information about the systems.

3. Further narrow down focus with a more critical eye. Perform actual scans and other detailed tests on the systems.

4. Perform the attacks, if that's what one choose to do.

Evaluating results

Assess the results to see what has been 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. One will end up knowing his/her own systems as well as anyone else. This makes the evaluation process much simpler moving forward. Submit a formal report to upper management or to the customer, outlining results. Keep these other parties in the loop to show that efforts and their money are well spent.

Moving on

When finished with ethical hacking tests, one still need to implement his analysis and recommendations to make sure that the systems are secure.

New security vulnerabilities continually appear . Information systems constantly change and become more complex. New hacker exploit and security vulnerabilities are regularly uncovered. Security tests are snapshot of the security postures of the system.

At any time, everything can change, especially after software upgrades, adding computer systems, or applying patches. Plan to test regularly (for example, once a week or once a month).

5.6 Cracking the Hacker Mindset

Before assessing the security of systems, one may want to understand something about the hackers mind-set. Many information security product vendors and other professionals claim that one should protect the systems from the bad guys, both internal(Insiders) and external(Outsiders).

Knowing what hackers and malicious users want help understand how they work helps to look at your information systems in a whole new way. This understanding better prepares for ethical hacking tests.

What you're Up Against

Thanks to sensation in the media, public perception of hacker has transformed from harmless tamperer to malicious criminal. Hackers often state that the public misunderstands them, which is mostly true. Its easy to prejudge what is not understood. Unfortunately, many hackers stereotypes are based on misunderstanding rather than fact, and that misunderstanding fuels constant debate.

Hackers can be classified by both their abilities and their underlying motivations. Some are skilled, and their motivations are benign; they're merely seeking more knowledge. At the other end of the spectrum, hackers with malicious intent seek some form of personal gain. Unfortunately, the negative aspects of hacking usually overshadow the positive aspects and promote the negative stereotypes.

Hackers hacked for the pursuit of knowledge and the thrill of the challenge. Hackers see what others often overlook. They wonder that would happen if a cable was unplugged, a switch was flipped, or lines of code were changed in a program. These old-school hackers think they can improve electronic and mechanical devices by "rewiring them!" More recent evidence shows that many hackers may also hack for political, social, competitive, and even financial purposes, so times are changing. Hackers who perform malicious acts don't really think about the fact that human beings are behind the firewalls, wireless networks, and web applications they're attacking. They ignore that their actions often affect those human beings in negative ways, such as put in danger their job security and putting their personal safety at risk.

These people don't hack in the way people normally suppose. Instead, they root around in files on server shares; probe into databases they know they shouldn't be in; and sometimes steal, modify, and delete sensitive information to which they have access. This behavior is often very hard to detect. This activity is continued if these users passed their criminal Background and credit checks before they were hired. Past behavior is often the best predictor of future behavior, but just because someone has a clean record and authorization to access sensitive systems doesn't mean he or she won't do anything bad. Criminals may have to start from somewhere.

As negative as breaking into computer systems often can be, hackers and malicious users play key roles in the advancement of technology. In a world without hackers, odds are good that the latest intrusion prevention technology, data leakage protection, or vulnerability scanning tools would not exist. Such a world may not be bad, but technology does keep security professionals employed and keep the field moving forward. Unfortunately, the technical security solutions can't ward off all malicious attacks and unauthorized use. Because hackers and (sometimes) malicious users are usually a few steps ahead of the technology designed to protect against their disobedient actions. However, when the stereotypical hacker or malicious user is being viewed, one thing is certain: somebody will always try to take down computer systems and compromise information by poking and prodding where he or she shouldn't, through denial of service attacks or by creating and launching malware. One must take the appropriate steps to protect his/her systems against this kind of intrusion.

- **Thinking like the bad guys**

Malicious attackers often think and work just like thieves, kidnappers, and other organized criminals you hear about in the news every day. The smart ones constantly devise ways to fly under the radar and exploit even the smallest weaknesses that lead them to their target. The following are examples of how hackers and malicious users think and work:

- ✓ **Evading an intrusion prevention system** by changing their MAC address or IP address every few minutes to get further into a network without being

Completely blocked

- ✓ **Exploiting a physical security weakness** by being aware of offices that have Already been cleaned by the cleaning crew and are unoccupied (and thus easy to Access with little chance of getting caught), which might be made obvious by, For instance, the fact that the office blinds are opened and the curtains are pulled Shut in the early morning.

- ✓ **Bypassing web access controls** by changing a malicious site's URL to its Dotted decimal IP address equivalent and then converting it to hexadecimal for Use in the web browser

- ✓ **Using unauthorized software that would otherwise be blocked at the Firewall** by changing the default TCP port that it runs on

- ✓ **Setting up a wireless "evil twin"** near a local Wi-Fi hotspot to entice Unsuspecting Internet surfers onto a rogue network where their information can Be captured and cagily manipulated

- ✓ **Using an overly trusting colleague's user ID and password** to gain access to Sensitive information that would otherwise be highly improbable to obtain

- ✓ **Unplugging the power cord or Ethernet connection to a networked security Camera** that monitors access to the computer room or other sensitive areas and subsequently gaining unmonitored access.

- ✓ **Performing SQL injection or password cracking against a website** via a neighbor's unprotected wireless network in order to hide the malicious user's own identity.

- **Who Breaks into Computer Systems**

In a world of black and white, describing the typical hacker is easy. A general stereotype of a hacker is an antisocial, unpleasant mind-set personality. But the world has many shades of gray and many types of hackers. Hackers are unique individuals, so an exact profile is hard to outline. The best broad description of hackers is that all hackers aren't equal. Each hacker has his or her own unique motives, methods, and skills. Hacker skill levels fall into three general categories:

- ✓ **Script kiddies:** These are computer beginners who take advantage of the hacker tools, vulnerability scanners, and documentation available free on the Internet but who don't have any real knowledge of what's really going on behind the scenes. They know just enough to cause headaches but typically are very sloppy in their actions, leaving all sorts of digital fingerprints behind.

- ✓ **Criminal hackers:** These are skilled criminal experts and nation states who write some of the hacking tools, including the scripts and other programs that the script kiddies and ethical hackers use. These people also write such malware as viruses and worms. They can break into systems and cover their tracks.

Advanced hackers are often members of collectives that prefer to remain nameless. These hackers are very secretive and share information with their subordinates only when they are deemed worthy. Typically, for lower-ranked hackers to be considered worthy, they must possess some unique information or prove themselves through a high-profile hack.

These hackers are possibly some of the worst enemies in information security.

- ✓ **Security researchers:** These uber-hackers are highly technical and publicly known IT professionals who not only monitor and track computer, network, and application vulnerabilities but also write the tools and other code to exploit them.

If these guys didn't exist, ethical hackers wouldn't have much in the way of open source and even certain commercial security-testing tools.

There are good-guy (white hat) and bad-guy (black hat) hackers. Gray hat hackers are a little bit of both. There are also blue-hat hackers who are invited by software vendors to find security flaws in their systems.

A recent study at the Black Hat security conference found that everyday IT professionals even engage in malicious and criminal activity against others. And people wonder why IT doesn't get the respect it deserves? Perhaps this group will evolve into a fourth general category of hackers in the coming years. Perhaps more important than a hacker's skill level is his or her motivation.

- ✓ **Hactivists** try to distribute political or social messages through their work. A hactivist wants to raise public awareness of an issue. In many situations, criminal hackers will try to take the person down if he/she expresses a view that's contrary to theirs. Examples of hactivism include messages about legalizing drugs, protests against the war in Iraq, protests centered around wealth envy and big corporations, and just about any other social and political issues,

- ✓ **Cyber-terrorists** (both organized and unorganized) attack government computers or public utility infrastructures, such as power grids and air-traffic control towers. They crash critical systems or steal classified government information. Countries take the threats these cyber-terrorists pose so seriously that many mandate information security controls in crucial industries, such as the power industry, to protect essential systems against these attacks.

- ✓ **Hackers for hire** are part of organized crime on the Internet. Many of these hackers hire out themselves or their botnets for money and lots of it. These criminal hackers are in the minority. Like the spam kings of the world, many of the wicked acts from members of collectives that prefer to remain nameless are carried out by a small number of criminals. Many other hackers just love to tinker and only seek knowledge of how computer systems work. One of the greatest threats works inside premises and has an access badge to the building and a valid network account, so don't discount the insider threat.

Why They Do It?

Reasons:

- ✓ Hacking is a casual hobby for some hackers. They hack just to see what they can and can't break into, usually testing only their own systems.

- ✓ Many hackers get a kick out of outsmarting corporate and government IT and security administrators. They thrive on making headlines and being notorious cyber outlaws.

- ✓ Hackers often promote individualism or at least the decentralization of information because many believe that all information should be free.

- ✓ They think cyber-attacks are different from attacks in the real world. Hackers may easily ignore or misunderstand their victims and the consequences of hacking.

- ✓ They don't think long-term about the choices they're making today. Many hackers say they don't intend to harm or profit through their bad deeds, a belief that helps them justify their work.

- ✓ Some common motives are revenge, basic bragging rights, curiosity, boredom, challenge, vandalism, theft for financial gain, sabotage, blackmail, extortion, corporate intelligence, and just generally speaking out against "the man." Hackers

Regularly cite these motives to explain their behavior, but these motivations tend to be cited more commonly during difficult economic conditions.

- ✓ Many business owners and managers

Administrators believe that they don't have anything that a hacker wants or that hackers can't do much damage if they break in. This indifferent kind of thinking helps support the bad guys and promote their objectives.

- ✓ Hackers can compromise a seemingly unimportant system to access the network and

Even

Some network and security

Use it as a launching pad for attacks on other systems, and many people would be none the wiser because they don't have the proper controls to prevent and detect malicious use.

- ✓ Hackers often hack just because they can. Some hackers go for high-profile systems, but hacking into anyone's system helps them fit into hacker circles. Hackers exploit many people's false sense of security and go for almost any system they think they can compromise. Electronic information can be in more than one place at the same time, so if hackers merely copy information from the systems they break into, it's tough to prove that hackers possess that information.

Computer openings continue to get easier to execute yet harder to prevent for several

Reasons:

- ✓ Widespread use of networks and Internet connectivity
- ✓ Anonymity provided by computer systems working over the Internet and often on

The internal network (because, effectively, logging and especially log monitoring rarely takes place)

- ✓ Greater number and availability of hacking tools
- ✓ Large number of open wireless networks that help hackers cover their tracks
- ✓ Greater complexity and size of the codebase in the applications and databases being developed today
- ✓ Computer-savvy children
- ✓ Unlikelihood that attackers will be investigated or prosecuted if caught

A malicious hacker only needs to find one security hole whereas IT professionals and business owners must find and block them all.

Although many attacks go unnoticed or unreported, criminals who are discovered are often not pursued or prosecuted. When they're caught, hackers often rationalize their services as being unselfish and a benefit to society: They're merely pointing out vulnerabilities before someone else does.

The same goes for malicious users. Typically, their troubles go unnoticed, but if they're trapped, the security breach may be kept secret in the name of shareholder value or not wanting to disturb any customer or business partner. However, recent information security and privacy laws and regulations are changing this because in most situations breach notification is required. Sometimes, the person is fired or asked to resign. Although public cases of internal breaches are becoming more common, these cases don't give a full picture of what's really taking place in the average organization.

Hacking in the name of liberty?

Many hackers exhibit behaviors that contradict their stated purposes. They fight for civil liberties and want to be left alone, while at the same time, they love prying into the business of others and controlling them in any way possible.

Many hackers call themselves civil libertarians and claim to support the principles of

Personal privacy and freedom. However, they contradict their words by intruding on the Privacy and property of others. They often steal the property and violate the rights of Others, but are willing to go to great lengths to get their own rights back from anyone who Threatens them.

This applies to external hacks, internal breaches, and even something as seemingly gentle As a lost mobile device or backup tapes.

Planning and Performing Attacks

Attack styles vary widely:

- ✓ Some hackers prepare far in advance of an attack. They gather small bits Of information and methodically carry out their hacks. These hackers are the Most difficult to track.

- ✓ Other hackers They think through the consequences. Such hackers may try, for example, To telnet directly into an organization's router without hiding their identities. Other hackers may try to launch a Do's attack against a Microsoft Exchange Server without first determining the version of Exchange or the patches that Are installed. These hackers usually are caught.

- ✓ Malicious users are all over the map. Some can be quite savvy based on Their knowledge of the network and of how IT operates inside the Usually the inexperienced script kiddies - act before Organization.

Many of the hackers, especially advanced hackers don't share information With the crowd. Most hackers do much of their work independently in order To remain anonymous.

Hackers who network with one another use private message boards, anonymous e-Mail addresses, hacker websites, and Internet Relay Chat (IRC). One can log in to Many of these sites to see what hackers are doing.

Following are the aspects of real-world security:

- ✓ The majority of computer systems aren't managed properly. The Computer systems aren't properly patched, hardened, or monitored. Attackers can often fly below the radar of the average firewall, an Intrusion Prevention system (IPS), or an access control system. This is especially true For malicious users whose actions are often not monitored at all while, at the Same time, they have full access to the very environment they can exploit.

- ✓ Most network and security administrators simply can't keep up with The deluge of new vulnerabilities and attack methods. These people often Have too many tasks to stay on top of and too many other fires to put out. Network and security administrators may also fail to notice or respond to Security events because of poor time management and goal setting, but That's for another discussion.

- ✓ Information systems grow more complex every year. This is yet another Reason why overburdened administrators find it difficult to know what's Happening across the wire and on the hard drives of all their systems, Mobile devices such as laptops, tablets, and phones are making things Exponentially worse.

Time is an attacker's friend and it's almost always on his or her side. By attacking through computers rather than in person, hackers have more control over the timing for their attacks:

- ✓ Attacks can be carried out slowly, making them hard to detect.
- ✓ Attacks are frequently carried out after typical business hours, often in the middle of the night, and from home, in the case of malicious users.

If one wants detailed information on how some hackers work or want to keep up with the latest hacker methods, several magazines are worth checking out:

- ✓ 2600- The Hacker Quarterly magazine
- ✓ Magazine
- ✓ PHRACK

Malicious attackers usually learn from their mistakes. Every mistake moves them one step closer to breaking into someone's system. They use this knowledge when carrying out future attacks. As an ethical hacker, one needs to do the same.

Maintaining Anonymity

Smart attackers want to remain as low-key as possible. Covering their tracks is a priority, and many times their success depends on them remaining unnoticed. They want to avoid raising suspicion so they can come back and access the systems in the future.

Hackers often remain anonymous by using one of the following resources:

- ✓ Borrowed or stolen remote desktop and VPN accounts from friends or previous employers
- ✓ Public computers at libraries, schools, or kiosks at the local mall
- ✓ Open wireless networks
- ✓ Internet proxy servers
- ✓ Anonymous or disposable e-mail accounts from free e-mail services
- ✓ Open e-mail relays
- ✓ Infected computers also called zombies or bots at other organizations
- ✓ Workstations or servers on the victim's own network

If hackers use enough stepping stones for their attacks, they are hard to trace.

Ethical Hacker: Job Description, Requirements

Ethical hackers are trained hackers who use their skills to identify security problems with Computer networks,

Career Definition of an Ethical Hacker

Ethical hackers are cyber security professionals who are capable of breaching security Systems. They conduct tests on computer networks and try to hack into the networks to access Information without authorization. The purpose of this is to identify weaknesses in the Security systems that are in place and help determine how to improve Internet security.

The primary objective of an ethical hacker is to ensure that the computer systems they Work with are safe and cannot be accessed without authorization.

They need to be aware of new software and hardware that can improve computer security Since they play a key role in determining the security needs of their employer or clients. When They attempt to hack into the system, they produce reports detailing their attempts and the Conclusions they've reached about the effectiveness of the security systems that are in place.

Educational Requirements

Bachelor's degree and certification

Job Skills

Analytical Skills, interpersonal skills, communication Skills, customer service skills, attention to detail, problem-Solving skills

Job Outlook (2016-2026)

28% (information security analysts)

Required Education

In order to become an ethical hacker it's necessary to have a bachelor's degree in a related field, such as computer science. Ethical hackers need to have computer programming experience and familiarity with a range of different programming languages. It's common for employers to require ethical hackers to have Certified Ethical Hacker (CEH) certification and other recognized certifications, such as CompTIA, that prepare them to work as experts in cyber security.

Required Skills

Ethical hackers need to have:

- ✓ Strong analytical skills because their work involves reviewing a lot of data to identify potential issues with computer network security.
- ✓ Consulting with clients, explaining their findings to managers or clients, and collaborating with other professionals who are involved with information security.
- ✓ Excellent customer service skills and strong interpersonal skills.
- ✓ Communication skills are also important so that they can effectively explain their test results to clients and co-workers.
- ✓ Exceptional problem-solving skills and attention to detail are fundamental since ethical hackers need to be thorough in their attempts to breach the security systems in place.
- ✓ Develop new and often innovative strategies that enable them to identify problems with the security systems they work on.

The good guys of the hacking world
ETHICAL HACKERS wear the 'WHITE HAT'
WHAT THEY DO
Computer security for businesses
And organizations with the
THE ATTRACTION OF THIS JOB
ROLES
Working in Information security

Fig. 5.3 what knowledge is required to become an ethical hacker?

Steps to become A Hacker:

- Step 0: Read the Hacking
- Step 1: Learn To Program in C
- Step 2: Learn More Than One Programming Language
- Step 3: Learn UNIX
- Step 4: Learn More Than One Operating Systems
- Step 5: Learn Networking Concepts

- Step 6: Start Simple: Read Some Tutorials about Hacking
- Step 7: Learn Cryptography
- Step 8: Experiment A Lot

Some of the things you may need to keep in mind when doing experiments

- ✓ Keep a backup before any experiment.
- ✓ Start small and have check points.
- ✓ Know when to stop.
- ✓ Keep improvising

- ✓ Automate repetitive tasks

Step 9: Read Some Good Books from Experts

Step 10: Participate In Hacking Challenges: Apart from that, there are some websites listed below that regularly offer hacking challenges online.

- ✓ Hackquest.de
- ✓ Page on hacktissite.org
- ✓ www.trythisOne.com
- ✓ www.hackchallenge.net
- ✓ Home: Hacking-Lab.com

Step 11: Go Next Level: Write Vulnerability

Step 12: Contribute To Open Source Security Projects

Step 13: Continue Learning and Keep Listening To Security Talks

Above are few exhaustive steps that can teach how to be a hacker and help to walk the road of Being an expert hacker. However, one should be a responsible citizen and be selective, Ensuring one don't use this skill to breach the security of important institutions, as it may land You in dire straits. One should always remember, for every hacking tool, there is always a Counter hacking tool. Therefore, be a smart hacker and more importantly, be a responsible Hacker.

Ethical Hacking Related Careers

Ethical hackers spend most of their time working on computers and must be capable of Writing computer programming code. Those interested in this career field may be interested in The other occupations linked to here that involve writing computer code, protecting data stored On computer networks and creating secure computer networks.

- ✓ Back-End Developer: Job Description & Salary
- ✓ Become a Software Developer: Education and Career Roadmap
- ✓ Computer Networking Specialist: Job Description and Requirements

Hacking Tools: are computer programs and scripts that help you find and exploit Weaknesses in computer systems, web applications, servers and networks. There is a Variety of such tools available on the market. Some of them are open source while others Are commercial solution.

Tools for Ethical hacking of web applications, servers and networks:

- ✓ **Nets parker** is a ways to use web application security scanner that can Automatically find SQL Injection, XSS and other vulnerabilities in your web Applications and web services. It is available as on-premises and SAAS solution. Acunetix is a fully automated ethical hacking solution that mimics a hacker to keep one step ahead of malicious intruders. The web application security scanner accurately scans HTML5, JavaScript and Single-page applications. It can audit complex, authenticated webapps and issues compliance and management reports on a wide range of web and network vulnerabilities.

- ✓ **Probelycontinuously** scans for vulnerabilities in your Web Applications. It allows its customers to manage the life cycle of vulnerabilities and provides them with some guidance on how to fix them. Probely is a security tool built having Developers in mind.

- ✓ **InsightVM** is a top-ranked vulnerability risk management solution focused on detecting, prioritizing, and remediating vulnerabilities. With InsightVM, you can automatically assess and understand security risk across your entire infrastructure.

✓ **SaferVPN** is an indispensable tool in an Ethical hacker's arsenal. You may need it to check target in different geographies, simulate non-personalized browsing behavior, undiscovered file transfers, etc.

✓ **Burp Suite** is a useful platform for performing Security Testing of web applications. Its various tools work seamlessly together to support the entire pen testing process. It spans from initial mapping to analysis of an application's attack surface.

✓ **Ettercap** is an ethical hacking tool. It supports active and passive dissection includes features for network and host analysis.

Aircrack is a trustable ethical hacking tool. It cracks vulnerable wireless connections. It is powered by WEP WPA and WPA 2 encryption Keys.

Angry IP Scanner is open-source and cross-platform ethical hacking tool. It scans IP addresses and ports.

✓ **GFI LanGuard** is an ethical tool that scans networks for vulnerabilities. It can act as your 'virtual security consultant' on demand. It allows creating an asset inventory of every device.

✓ **Savvius**: It is an ethical hacking tool. It performance issues and reduces security risk with the deep visibility provided by OmnipEEK. It can diagnose network issues faster and better with Savvius packet intelligence.

✓ **Qualys guard** helps businesses streamline their security and compliance solutions. It also builds security into their digital transformation initiatives. This tool can also check the performance vulnerability of the online cloud systems.

✓ **WebInspect** is automated dynamic application security testing that allows performing ethical hacking techniques. It provides comprehensive dynamic analysis of complex web applications and services.

✓ **Hashcat** is a robust password cracking ethical hacking tool. It can help users to recover lost passwords, audit password security, or just find out what data is stored in a hash.

✓ **L0phtCrack 6** is useful password audit and recovery tool. It identifies and assesses password vulnerability over local machines and networks.

✓ **RainbowCrack** is a password cracking tool widely used for ethical hacking. It cracks hashes with rainbow tables. It uses time-memory tradeoff algorithm for

✓ **Hashcat** is a robust password cracking ethical hacking tool, It can help users to recover lost passwords, audit password security, or just find out what data is stored in a hash.

asodind siyn

✓ **IKECrack** is an open source authentication crack tool. This ethical hacking tool is designed to brute-force or dictionary attack. This tool also allows performing cryptography tasks.

✓ **IronWASP** is an open source software for ethical hacking tool. It is web application vulnerability testing. It is designed to be customizable so that users can create their custom security scanners using it.

✓ **Medusa** is one of the best online brute-force, speedy, parallel password crackers ethical hacking tool. This tool is also widely used for ethical hacking.

✓ **NetStumbler** is used to detect wireless networks on the Windows platform.

✓ **SQLMap** automates the process of detecting and exploiting SQL Injection weaknesses. It is open source and cross platform. It supports the following

database engines.

Recover MS Access passwords

Uncover password field

Sniffing networks

Cracking encrypted passwords using dictionary attacks, brute-force, and cryptanalysis attacks.

✓ **Nessus** can be used to perform:

+ Remote vulnerability scanner

+ Password dictionary attacks

+ Denial of service attacks.

It is closed source, cross platform and free for personal use.

References

• <https://www.dynamicchiropractic.com/mpacms/dc/article.php?id=D18078>)

• Hacking For Dummies, 5th Edition By Kevin Beaver

http://cdn.ttgtmedia.com/searchNetworking/downloads/hacking_for_dummies

http://wiki.cas.mcmaster.ca/index.php/Ethical_Hacking

• <https://www.dummies.com/programming/networking/what-is-a-malicious->

<https://www.guru99.com/what-is-hacking-an-introduction.html#2>

• http://cdn.ttgtmedia.com/searchNetworking/downloads/hacking_for_dummies.pdf

2600-The Hacker Quarterly magazine (www.2600.com)

• (IN)SECURE Magazine (www.net-security.org/insecuremag.php)

• Hackin9 (<http://hakin9.org>)

user/

PHRACK (www.phrack.org/archives/)

• <https://learning.oreilly.com/library/view/hacking-for-dummies/>

[9781118380956/06_9781118380956-ch02.html](https://learning.oreilly.com/library/view/hacking-for-dummies/9781118380956/06_9781118380956-ch02.html)

• <https://www.quora.com/What-knowledge-is-required-to-become-an-ethical-hacker>

Sample Multiple Choice Questions:

(1

)Ethical Hacking is also known as

a. Black Hat hacking

b. White hat hacking

c. Encrypting

d. None of these

2) Tool(s) used by ethical hackers

a.

Scanner

b. Decoder

c. Proxy

d. All of these

3) Vulnerability scanning in Ethical hacking finds_

a. Strengths

b. Weakness

c. a&b

d. None of these

4) Ethical hacking will allow to

all the massive security breaches.

remove

b. measure
reject

d.

None of these

5) Sequential steps hackers use are:

A) Maintaining Access

B) Reconnaissance

C) Scanning

D) Gaining Access

a.

B, C, D, A

b. B, A, C, D

c. A, B, C, D

d. D, C, B, A

Maharashtra State Board of Technical Education