Chapter 1 – Ethical hacking

Why is learning Hacking important ?

…..to assess the security of your own information systems, find security vulnerabilities, and fix the vulnerabilities before malicious and criminal hackers have an opportunity to take advantage of them.

Who is a hacker ?

---hacker is someone who likes to tinker with software or electronic systems. Hackers enjoy exploring and learning how computer systems operate.

--- 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.

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.)

What is Ethical hacking ?

….the science of testing your computers and network for security vulnerabilities and plugging the holes you find before the bad guys get a chance to exploit them.

You can implement all the security technologies and other best practices possible, and your information systems may be secure — as far as you know. However, until you understand how hackers think and apply that knowledge to assess your systems from a hacker's-eye view, you can't get a true sense of how secure your information really is.

Ethical hacking — sometimes referred to as *penetration testing* or *white-hat hacking* — is a necessary requirement to ensure that information systems are truly secure on an ongoing basis.

Who should learn ethical hacking ?

a network administrator, information-security manager, security consultant, or someone interested in finding out more about legally and ethically hacking your own or a customer's information systems to make them more secure.

As the ethical hacker performing well-intended information-security assessments, you can detect and point out security holes that may otherwise be overlooked

An *ethical hacker* possesses the skills, mindset, and tools of a hacker but is also trustworthy. Ethical hackers perform the hacks as security tests for their systems.

Features/ Characteristics of 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.

Hacking… preys 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.

Goals as an ethical hacker should be as follows:

_ Hack your systems in a nondestructive fashion.

_ Enumerate vulnerabilities and, if necessary, prove to upper management that vulnerabilities exist.

_ Apply results to remove vulnerabilities and better secure your systems.

Non-Technical attacks

Exploits that involve manipulating people — 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.

Hackers break into buildings, computer rooms, or other areas containing critical information or property. Physical attacks can include *dumpster diving* (rummaging 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.

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 802.11b wireless configuration

Operating-system attacks

Hacking operating systems (OSs) is a preferred method of the bad guys. Oss 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 NetWare 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.

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 your computer systems.

Ethical Hacking Commandments

1. Working ethically (working with high professional morals and principles. Whether you're performing ethical hacking tests against your own systems or for someone who has hired you, everything you do as an ethical hacker must be aboveboard and must support the company's goals.)
2. Respecting privacy (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.)
3. Not crashing your systems(when people try to hack their own systems, they lend up 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. You can easily create DoS conditions on your systems when testing. Running too many tests too quickly on a system causes many system lockups.)

The Ethical Hacking Process

➢ 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. If you're testing for a customer, have a signed contract in place, stating the customer's support and authorization. Get written approval on this sponsorship.

You need a detailed plan:
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, you can test computer passwords or attempt social engineering attacks before drilling down into more detailed systems. It pays to have a contingency plan for your ethical hacking process in case something goes awry. What if you're assessing your firewall or Web application, you take 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. Do you 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 of your timing.The best approach is an unlimited attack, wherein any type of test is possible.

Don't stop with one security hole. This can lead to a false sense of security. Keep going to see what else you can discover. One of your goals may be to perform the tests without being detected. For example, you may be performing your tests on remote systems or on a remote office, and you don't want the users to be aware of what you're doing. Otherwise, the users may be on to you and be on their best behavior
Base the type of test you will perform on your organization's or customer's needs.

Selecting Tools for the hacking :
if you don't have the right tools for ethical hacking, accomplishing the task effectively is difficult.
Many security-assessment tools generate false positives and negatives (incorrectly identifying vulnerabilities).

Others may miss vulnerabilities. If you're performing tests such as social engineering or physical-security assessments, you may miss weaknesses. Many tools focus on specific tests, but no one tool can test for everything.

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 nontechie types

➢ 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.

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.

Harness as much information as possible about your organization and systems, which is what malicious hackers
do. Start with a broad view and narrow your focus:

1. Search the Internet for your organization's name, your computer and network system names, and your IP addresses.

Google is a great place to start for this.

2. Narrow your scope, targeting the specific systems you're testing.

Whether physical-security structures or Web applications, a casual assessment can turn up much information about your systems.

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

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

➢ 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. Submit a formal report to upper management or to your customer, outlining your results.

When you've finished your ethical hacking tests, you still need to implement your analysis and recommendations to make sure your systems are secure. New security vulnerabilities continually appear. Information systems constantly change and become more complex. New hacker exploits and security vulnerabilities are regularly uncovered

Chapter 2
Cracking the Hacker Mindset

Knowing what hackers want helps you understand how they work. Understanding how they work helps you look at your information systems in a whole new way.
Its important to know who's actually doing the hacking, and what their motivations and methods are so you're better prepared for your ethical hacking tests.

Hackers can be classified by both their abilities and 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. Hackers are adventurous and innovative thinkers, and are always thinking about exploiting computer vulnerabilities.
Hackers and the act of hacking drive the advancement of security technology. After all, hackers don't create security holes; they expose and exploit existing holes in applications. Unfortunately, security technology advances don't ward off all hacker attacks, because hackers constantly search for new holes and weaknesses.

Who hacks ??
Script kiddies: These are computer novices who take advantage of the hacker tools and documentation available for free on the Internet but don't have any knowledge of what's going on behind the scenes. They know just enough to cause you headaches but typically are very sloppy in their actions, leaving all sorts of digital fingerprints behind. Even though
these guys are the stereotypical hackers that you hear about in the news media, they often need minimal skills to carry out their attacks.
_ **Intermediate hackers:** These halfway hackers usually know just enough to cause serious problems. They know about computers and networks, and often use well-known exploits. Some want to be experts; given enough time and effort, they can be.
_ **Elite hackers:** These are skilled hacking experts. These are the people who write many of the hacker tools, including the scripts and other programs that the script kiddies use. These folks write such malware as viruses and worms. They can break into systems and cover their tracks. They can even make it look like someone else hacked the systems. Elite hackers are often very secretive and share information with their "subordinates" only when they are deemed worthy. Typically, for lowerranked hackers to be considered worthy, they must possess some unique information or prove themselves through a high-profile hack. These hackers are your worst enemies in information security. Okay, maybe they're not as bad as untrained end users, but that's another issue. Fortunately, elite hackers are not as plentiful as script kiddies.

Cyberterrorists 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 these threats so seriously that many mandate information-security controls in such industries as the power industry to protect essential systems against these attacks.

Why Hackers Hack ?

Hacking is a casual hobby for some hackers — they just hack 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 cyberoutlaws. Defeating an entity or possessing knowledge makes them feel better about themselves. The knowledge that malicious hackers gain and the elevated ego that comes with that knowledge are like an addiction and a way of life.

Some ***common hacker motives are revenge, basic bragging rights, curiosity, boredom, challenge, vandalism, theft for financial gain, sabotage, blackmail, extortion, and corporate espionage.***

Hacking continues to get easier for several reasons:
_ Increasing use of networks and Internet connectivity
_ Anonymity provided by computer systems working over the Internet
_ Increasing number and availability of hacking tools
_ Computer-savvy children
_ Unlikelihood that hackers are investigated or prosecuted if caught

Hacking styles vary widely:
_ **Some hackers prepare far in advance of a large attack.** They gather small bits of information and methodically carry out their hacks. These hackers are more difficult to track.
_ **Other hackers — usually, the inexperienced script kiddies — act before they think things through.** For example, such hackers may try to telnet directly into an organization's router without hiding their identities. Other hackers may try to launch a DoS attack against a Microsoft Exchange e-mail server without first determining what version of Exchange is running or what patches are installed. These are the guys who usually get caught.

Whatever approach they take, most malicious hackers prey on ignorance. They know the following aspects of real-world security:
_ The majority of systems that hackers want to attack aren't managed properly. The computer systems aren't properly patched, hardened, and monitored as they should be. Hackers often can attack by flying below the average radar of the firewalls, IDSs, and authentication systems. Most network and security administrators simply can't keep up with the
deluge of new vulnerabilities.
_ 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 their systems.
Time is a hacker's friend — and it always seems to be on the hacker's side. By attacking through computers rather than in person, hackers have more control over when they can carry out their attacks.
_ Hack attacks can be carried out slowly, making them hard to detect. _ They're frequently carried out after typical business hours — often, in the middle of the night. Defenses are often weaker at night — with less physical security and less intrusion monitoring — when the typical network
administrator (or security guard) is sleeping.

Hackers- maintaining anonymity

Hackers often remain anonymous by using one of the following techniques:
_ Borrowed or stolen dial-up accounts from friends or previous employers
_ Public computers at libraries, schools, or kiosks at the local mall
_ Internet proxy servers or anonymizer services
_ Anonymous or disposable e-mail accounts from free e-mail services
_ Open e-mail relays
_ Unsecured computers — also called *zombies* — at other organizations
_ Workstations or servers on the victim's own network
If hackers use enough steppingstones for their attacks, they are hard to trace.

Chapter 3- Developing Your Ethical Hacking Plan

As an ethical hacker, you must plan your ethical hacking efforts before you start. A detailed plan doesn't mean that your testing must be elaborate. It just means that you're very clear and concise on what's to be done. Even if you're just testing a single Web application or workgroup of computers, it's critical to establish your goals, define and document the scope of what you'll be testing, determine your testing standards, and gather and familiarize yourself with the proper tools for the task.

1- Getting Your Plan Approved

Getting approval for ethical hacking is critical. First, obtain project sponsorship. This approval can come from your manager, an executive, a customer, or yourself (if you're the boss). Otherwise, your testing may be canceled suddenly, or someone can deny authorizing the tests. There can even be legal consequences for unauthorized hacking. Always make sure that what you're doing is known and visible — at least to the decision-makers

2- Establishing your goals

The main goal of ethical hacking is to find vulnerabilities in your systems so you can make them more secure.

__**Define more specific goals.** Align these goals with your business objectives.

_ **Create a specific schedule with start and end dates.** These dates are critical components of your overall plan.

Document everything, and involve upper management in this process.

The following questions can start the ball rolling:

_ Does ethical hacking support the mission of the business and its IT and security departments?

_ What business goals are met by performing ethical hacking?

These goals may include the following:

- Prepping for the internationally accepted security framework of ISO 17799 or a security seal such as SysTrust or WebTrust
- Meeting federal regulations
- Improving the company's image

_ How will ethical hacking improve security, IT, and the general business?

_ What information are you protecting?

This could be intellectual property, confidential customer information, or private employee information.

_ How much money, time, and effort are you and your organization willing to spend on ethical hacking?

_ What specific deliverables will there be?

Deliverables can include anything from high-level executive reports to detailed technical reports and write-ups on what you tested along with the outcomes of your tests. You can deliver specific information that is gleaned during your testing, such as passwords and other confidential information.

_ What specific outcomes do you want?

Desired outcomes include the justification for hiring or outsourcing security personnel, increasing your security budget, or enhancing security systems.

After you know your goals, document the steps to get there. For example, if one goal is to develop a competitive advantage to keep existing customers and attract new ones, determine the answers to these questions:

_ When will you start your ethical hacking?

_ Will your ethical hacking be blind, in which you know nothing about the systems you're testing, or a knowledge-based attack, in which you're given specific information about the systems you're testing such as IP addresses, hostnames, and even usernames and passwords?

_ Will this testing be technical in nature or involve physical security assessments or even social engineering?

_ Will you be part of a larger ethical hacking team, often called a *tiger team* or *red team?*

_ Will you notify your customers of what you're doing? If so, how?
Customer notification is a critical issue. Many customers appreciate that you're taking steps to protect their information. Approach the testing in a positive way. Don't say, "We're breaking into our systems to see what information of yours is vulnerable to hackers." Instead, you can say that you're assessing the overall security of your systems so the information is as secure as possible from the bad guys.
_ How will you notify customers that the organization is taking steps to enhance the security of their information?
_ What measurements can ensure that these efforts are paying off?

3- Determining what systems to hack

You may decide which systems to test based on a high-level risk analysis, answering questions such as:
_ What are your most critical systems? Which systems, if hacked, would cause the most trouble or the greatest losses?
_ Which systems appear to be most vulnerable to attack?
_ Which systems are not documented, are rarely administered, or are the ones you know the least about?

The following list includes systems and applications that you may consider performing your hacking tests on:
_ Routers
_ Firewalls
_ Network infrastructure as a whole
_ Wireless access points and bridges
_ Web, application, and database servers
_ E-mail and file/print servers
_ Workstations, laptops, and tablet PCs
_ Mobile devices (such as PDAs and cell phones) that store confidential information
_ Client and server operating systems
_ Client and server applications, such as e-mail or other in-house systems

- ➢ Start with the most vulnerable systems, and consider the following factors:

_ Where the computer or application resides on the network
_ Which operating system and application(s) it runs
_ The amount or type of critical information stored on it
(Another factor to help you decide where to start is to assess the systems that have the greatest visibility. For example, focusing on a database or file server that stores customer or other critical information may make more sense — at least initially — than concentrating on a firewall or Web server that hosts marketing information about the company.)

Creating Testing Standards

To prevent mishaps, develop and document testing standards. These standards should include:

_ When the tests are performed, along with the overall timeline
_ What tests are performed
_ How the tests are performed, and from where
_ How much knowledge of the systems you acquire in advance
_ What you do when a major vulnerability is discovered

Timing

Make sure that the tests you're performing minimize disruption to business processes, information systems, and people. You want to avoid situations like miscommunicating the timing of tests and causing a DoS attack against a high-traffic e-commerce site in the middle of the day, or forcing yourself or others to perform password-cracking tests in the middle of the night.

Notify any Internet Service Providers (ISP) or Application Service Providers (ASPs) involved before performing any tests across the Internet. Thus, ISPs and ASPs will be aware of the testing going on, which will minimize the chance that they will block your traffic if they suspect malicious behavior that shows up on their firewalls or Intrusion Detection Systems (IDSs).
The timeline should include specific short-term dates and times of each test, the start and end dates, and any specific milestones in between. Gantt charts or graphs can be used for display.
This timeline will keep things simple and provide a reference during testing.

(2) Specific Tests

Either perform a general *penetration test*, or perform specific tests, such as cracking passwords or war-dialing into a network. Or you might be performing a social-engineering test or assessing the Windows operating systems on the network.
(**War dialing** refers **to** the use of various kinds of technology **to** automatically dial many phone numbers, usually **in** order **to** find weak spots in an IT security)

(3) Sometimes, you may know the general tests that you're performing, but if you're using automated tools, it may be next to impossible to understand completely every test you're performing. This is especially true if the software you're using receives real-time vulnerability-testing updates from the vendor every time you run it. The potential for frequent updates underscores the importance of reading the documentation and readme files that come with the tools you're using.

(4)Blind versus knowledge assessments
It may be good to have some knowledge of the systems you're testing, but it's not required. However, a basic understanding of the systems you're hacking can protect you and others. Obtaining this knowledge shouldn't be difficult if you're hacking your own in-house systems. If you're hacking a customer's systems, you may have to dig a little deeper into how the systems work so you know what's what.
a customer ask for a fully blind assessment. The best approach is to plan on *unlimited* attacks, wherein any test is possible.
Consider whether the tests should be undetected. This isn't required. A false sense of vigilance can be created if too many insiders know about your testing which can end up negating the hard work you're putting into this.

(3)Location

The tests you're performing dictate where you must run them from. Your goal is to hack your systems from locations where malicious hackers can access the systems. You can't predict whether you'll be attacked by a hacker from outside or inside your network, so cover all your bases. Combine external (public Internet) tests and internal (private network) tests.
You can perform some tests, such as password cracking and network-infrastructure assessments, from the comfort of your office — inside the network. But it may be better to have a true outsider perform other tests on routers, firewalls, and public Web applications.
For your external hacks that require network connectivity, you may have to go off-site (a good excuse to work from home) or use an external proxy server. Better yet, if you can assign an available public IP address to your computer, plug into the network on the outside of the firewall for a hacker's-eye view of your systems.

Characteristics in the tools you select for ethical hacking:

_ Adequate documentation.
_ Detailed reports on the vulnerabilities, including how they may be exploited and fixed.
_ Updates and support when needed.
_ High-level reports that can be presented to managers or other nontechie types.

Know the limitations of your tools and of yourself. Many security-assessment tools generate false positives — alerting to a vulnerability when it doesn't really exist. Some even generate false negatives, which means they miss the vulnerabilities altogether. Likewise, if you're performing social-engineering tests or physical-security assessments, it's only human to miss specific vulnerabilities.