Chap 5 : Basics of Hacking

How Hackers Beget Ethical Hackers?

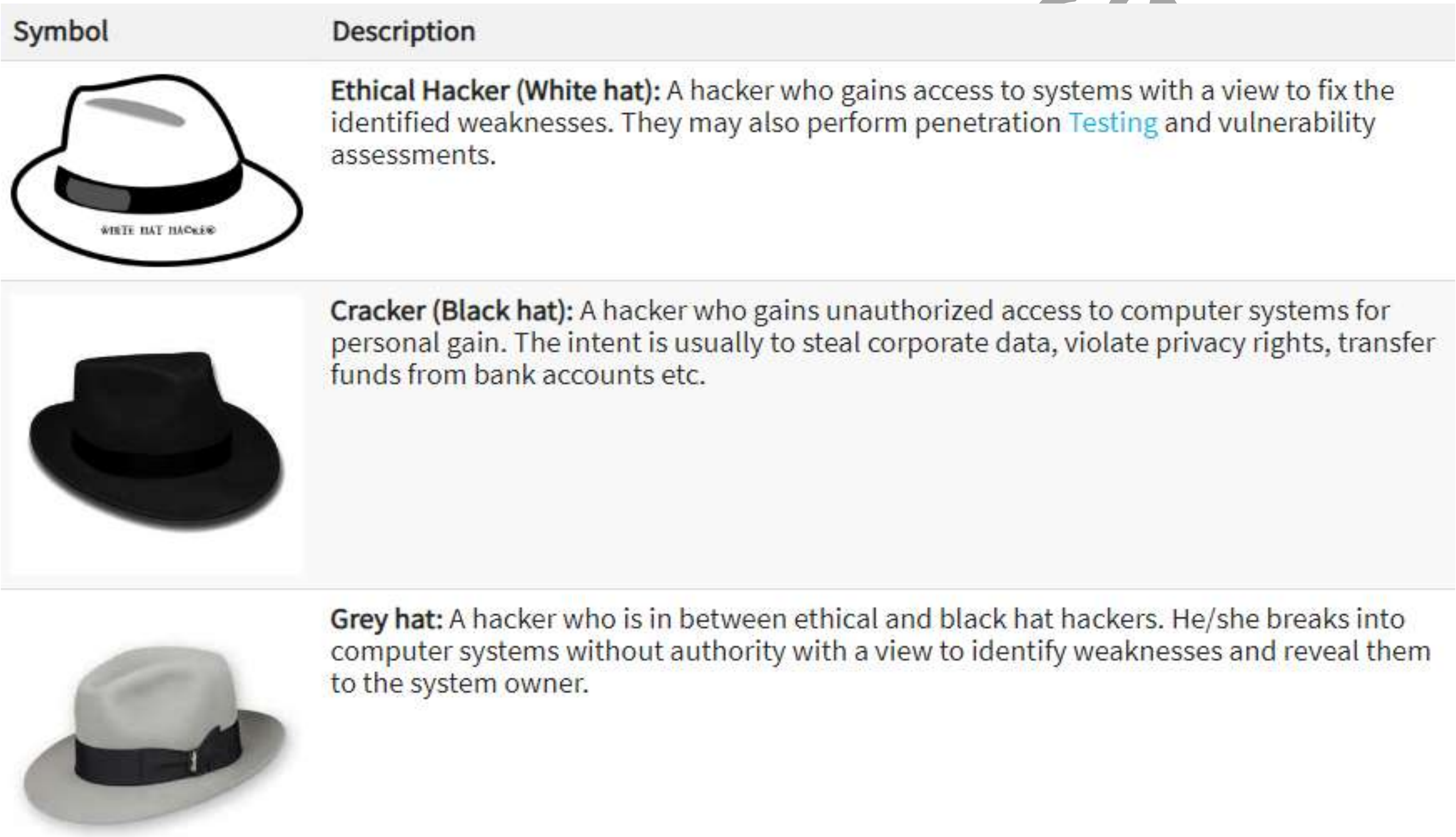
- We’ve all heard of hackers.
- Many of us have even suffered the consequences of hacker actions. So what is hacking and who are these hackers?
- Why is it important to know about them?

- **Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access.**
- Example of Hacking: Using password cracking algorithm to gain access to a system
- In other words we cans ay that, **Hacking** means **using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc.**

Who is a 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.**

Types of Hackers



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.
	Cracker (Black hat): A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.
	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.

Script kiddies: A non-skilled person who gains access to computer systems using already made tools.

Hacktivist: 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.

Phreaker: A hacker who identifies and exploits weaknesses in telephones instead of computers.

Ethical Hacking

- Ethical Hacking is **identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses.**
- Ethical hackers must follow the rules listed below:
  - 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**.

Why Ethical Hacking?

- **Information** is one of the most **valuable assets of an organization**. Keeping **information secure 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.
- Ethical hacking **puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.**

- **Ethical Hackers attitude:**
  - Encompasses **formal and methodical testing, white hat hacking and vulnerability testing, which involves the same tools, tricks and techniques that criminal hacker use**, but with one major difference :
    - Ethical hacking **is performed with the target permission** in a professional setting.

- The **intent of ethical hacking is to discover vulnerabilities from malicious attacker view point to better secure system.**

- It’s a important part under **risk management program** that allows for on going security improvements.

- In Raymond dissertation, “How to Become a Hacker” , he describes the fundamentals of hacker attitude which are as follows:

- **The world is full of fascinating problems waiting to be solves:**
  - If hacker find problem fascinating and exciting then it wont even feel like hard work.

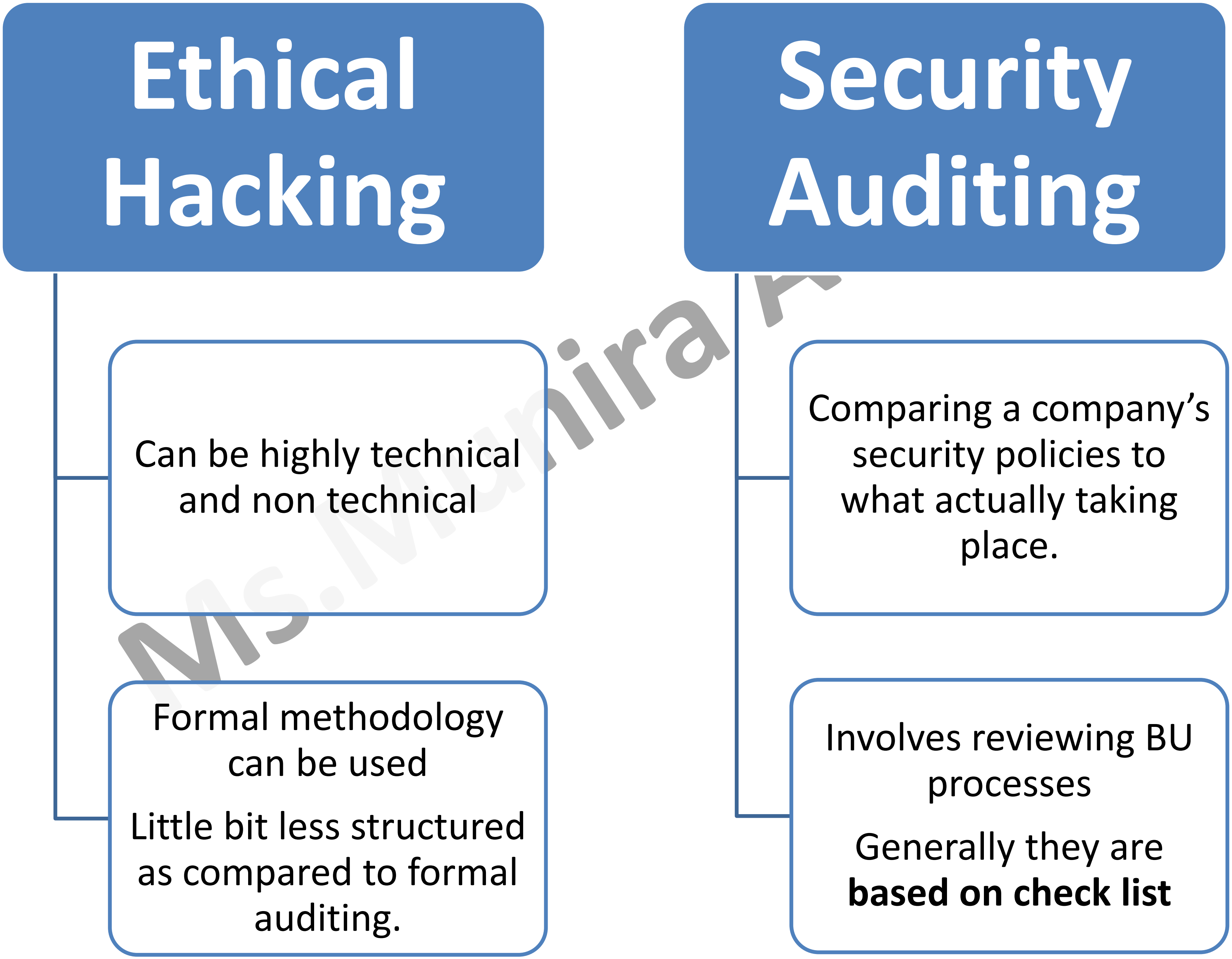
- **No problem should be ever have to solved twice:**
  - Hackers are perfectionist for clarifying the problem before they start generating ideas.
  - Its easy to jump to a solutions, but sometimes that means wrong problems are solved.
  - A little bit of accuracy on the front end of a problem solving process means one tackles the right and real problem, so one only have to do it once.

- **Boredom an drudgery(more and more work) are evil:**
  - To lose touch with **innovation** is too become too repetitive.
  - Innovation requires constant and vigilant creativity.

- **Freedom is good:**
  - – Hackers need freedom to work upon their ideas.

Malicious User

- **Internal attackers**
- Users who try to **compromise computers** and sensitive information **from the inside as authorized and trusted users**
- They go for s/y they believe they can compromise **for fraudulent gains or revenge**.
  - » Malicious attackers are generally known as both hacker and malicious users
  - » They are dishonest employee, contractor, intern or other user who abuses his her trusted privileges.



Ethical Hacking

Can be highly technical and non technical

Formal methodology can be used

Little bit less structured as compared to formal auditing.

Security Auditing

Comparing a company's security policies to what actually taking place.

Involves reviewing BU processes

Generally they are **based on check list**

Policy Consideration

- 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.**

– Who’s doing the testing?

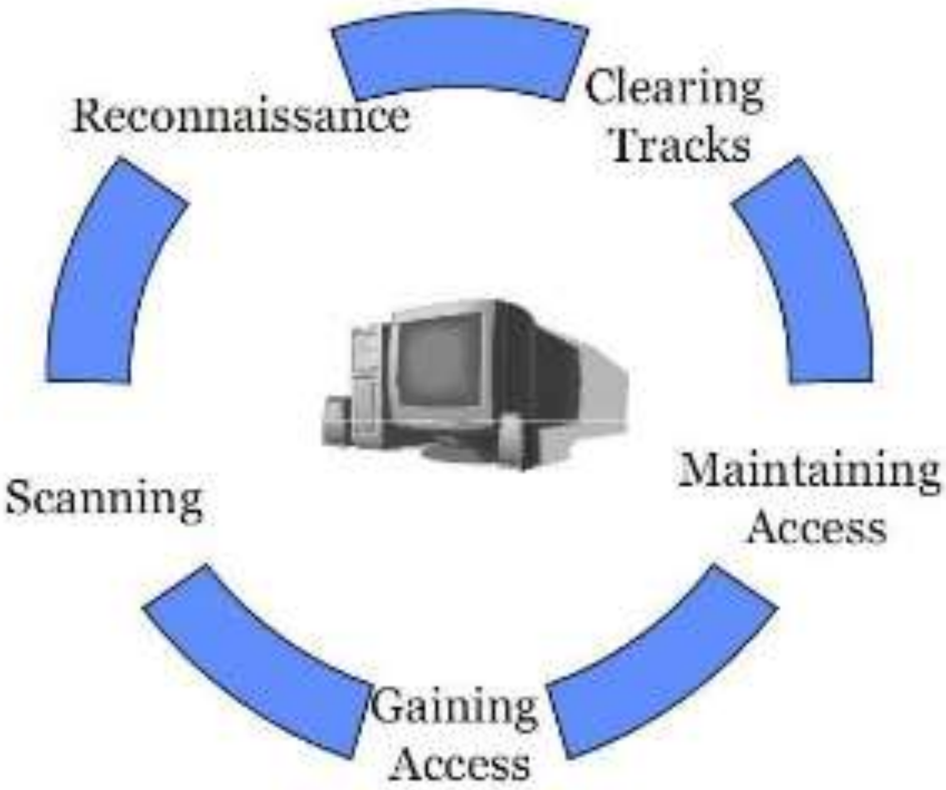
– The general type of testing that is performed?

– How often the testing takes place?

Legality of Ethical Hacking

- **Ethical Hacking is legal if the hacker follows the rules .**
- 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.

Hacking Phases



Reconnaissance

- Is the **preparation phase**. It seeks **to gather information about the target**.
- There’s two kind of reconnaissance; **active** and **passive**.

  Active reconnaissance permits **direct interaction** by any mean with the target. **Passive reconnaissance** does **not permit any direct interaction** with the target.

Scanning

- Scanning is the **pre-attack phase**, it’s done on the basis of information gathered during recon phase.
- This phase includes the **usage of port scanners, net mappers, and many other tools**. Information extracted by the attacker during this phase are live machine, OS detail

Gaining access

- Gaining access is **the point where the attacker obtains access to the system or the application.**
- The attacker can then, **escalate privileges to gain a complete control of the system.**

Maintaining access

- Maintaining access is the retention the system’s owner.

Cleaning tracks

- Clearing tracks are hiding its malicious acts to prevent being uncovered.

Understanding the dangers your system face

- Non technical attacks
- N/w infrastructure attack
- OS attack
- Application and other specialized attacks

Non technical attacks

- Attacks that involves **manipulating people or end users and even your self** are the greatest vulnerabilities.
- Exploitation of trusting nature of human beings to gain information for malicious purpose.

- Other common and effective attacks are physical:
  - Hacker **breaks into bldg. or other areas containing critical information or property**.
  - Also include dumpster diving(searching through trash cans and dumpsters for intellectual property, password, n/w diagram and other information.

This entails combing through someone else's trash to find treasures—or in the tech world, discarded sensitive information that could be used in an illegal manner. Information that should be securely discarded includes, but is not limited to:

1 Passwords

2 Access codes

3 Organizational charts

4 Calendars

5 Network/application diagrams

6 Credit card receipts

7 Expense reports

8 Phone numbers

9 Printed emails

10 Names

N/w infrastructure attack

- This attack can be easy, because many n/w can be reached from anywhere in the world via internet.
- Eg:
  - **Flooding** a n/w with too many request, creating **DOS** for legitimate request
  - **Installing n/w analyzer** on a n/w and capturing every packet that travels across it, revealing confidential information in clear text.
  - **Exploiting transport mechanism** such as TCP/IP

OS attack Hacking

- OS preferred as a method of bad guy hacker.
- Attackers prefer attacking systems like windows and Linux because they are widely used and better known for their vulnerabilities.
- Eg:
  - Breaking file system security
  - Attacking built in authentication system
  - Cracking password and encryption mechanism.

Application and other specialized attacks

- Virus , Worms , Trojan and spyware.
- Spam & Email server.
- HTTP and SMTP applications are frequently attacked.(to get full access to the following programs via internet)

Obeying the Ethical Hacking Commandments

- Working ethically
- Respecting privacy
- Not crashing your systems

Working ethically

- The word ethical in this context can be defined as **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 above board and must support the company's goals**.
- **No hidden agendas are allowed!** **Trustworthiness** is the ultimate tenet. **The misuse of information is absolutely forbidden.** That's what the bad guys do.

Respecting privacy

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

- Involve others in your process. This is a **“watch the watcher”** system that can **build trust and support your ethical hacking projects**.

Not crashing your systems

- One of the biggest mistakes people make **when trying to hack their own systems is inadvertently crashing the systems they're trying to keep running.**
- **Poor planning** is the main cause of this mistake.
- These testers either have not read the **documentation or misunderstand** the usage and power of the **security tools** and **techniques** at their disposal.

- **Running too many tests too quickly can cause system lockups, data corruption, reboots, and more.**
- Many vulnerability scanners can control how many tests are performed on a system at the same time.

Ethical Hacking Process

- Formulating your plan
- Selecting tools
- Executing the plan
- Evaluating results
- Moving on

Formulating your plan

- A well-defined scope includes the following information:
  - Specific systems to be tested
  - Risks involved
  - Dates the tests will be performed and your overall timeline
  - Knowledge of the systems you have before you start testing
  - Actions you will take when a major vulnerability is discovered
  - The specific deliverables

Specific systems to be tested

- When selecting systems to test, **start with the most critical systems and processes** or **the ones you suspect are the most vulnerable.**
- For instance, you can **test server OS passwords**, an **Internet-facing Web application**, or attempt some attacks before drilling down into all your systems.

Risks involved

- **Have a contingency plan** for your ethical hacking process **in case something goes wrong**.
- What if you're **assessing your firewall or Web application and you take it down**? This can **cause system unavailability, which can reduce system performance or employee productivity.**
- Even worse, it might cause loss of data integrity, loss of data itself.
- It'll most certainly **tick off a person** or **two and make you look bad.**

Dates the tests will be performed and your overall timeline

- Determining when the tests are performed is something that you must think long and hard about.
  - Do you perform tests 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**
  - where any type of test is possible at any time of day

Knowledge of the systems you have before you start testing

- You don’t need extensive knowledge of the systems you’re testing — just a basic understanding.
- This basic understanding helps protect you and the tested systems.

- Understanding the systems you’re testing shouldn’t be difficult if you’re hacking your own in-house systems.
- If you’re testing a client’s systems, you may have to **dig deeper.**

Actions you will take when a major vulnerability is discovered

- Don’t stop after you find one security hole. Keep going to see what else you can discover.

- If you haven’t found any vulnerability, you haven’t looked hard enough.
- If you uncover something big, you do need to share that information with the key players as soon as possible to plug the hole before it’s exploited.

The specific deliverables

- This **includes vulnerability scanner reports** and a higher-level report outlining the important vulnerabilities to address, **along with countermeasures to implement.**

Selecting tools

- Make sure you're using the right tool for the task:
  - To crack passwords, you need cracking tools, such as Proactive Password Auditor.

  A general port scanner, such as SuperScan or Nmap, won't work for cracking passwords and rooting out detailed vulnerabilities.

  - For an in-depth analysis of a Web application, a Web application assessment tool (such as N-Stalker or WebInspect) is more appropriate than a network analyzer (such as Wireshark).

- Whichever tools you use, familiarize yourself with them before you start using them.
- Here are ways to do that:

✓ Read the readme and/or online help files and FAQs.

✓ Study the user's guides.

✓ Use the tools in a lab or test environment.

✓ Consider formal classroom training from the security tool vendor or another third-party training provider, if available.

- Look for these characteristics in tools for ethical hacking:

✓ Adequate documentation

✓ Detailed reports on the discovered vulnerabilities, including how they might be exploited and fixed

✓ General industry acceptance

✓ Availability of updates and support

✓ High-level reports that can be presented to managers or nontechnical types

Executing the plan

- Be careful when you’re performing your ethical hacking tests.
- A hacker in your network or a seemingly benign employee looking over your shoulder might watch what’s going on and use this information against you or your business.

- Making sure that no hackers are on your systems before you start isn’t practical. Be sure you keep everything as quiet and private as possible.

- 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.

2. Narrow your scope, targeting the specific systems you’re testing. Whether you’re assessing physical security structures or Web applications, a **casual assessment** can turn up a lot of information about your systems.

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

4. Perform the attacks and exploit any vulnerabilities you find, if that’s what you choose to do.

Evaluating results

- Assess your results to see what you’ve uncovered, assuming that the vulnerabilities haven’t been made obvious before now.
- This is where knowledge counts.
- Your skill at evaluating the results and correlating the specific vulnerabilities discovered will get better with practice.
- You’ll end up knowing your systems much better than anyone else. This makes the evaluation process much simpler moving forward.

- **Submit a formal report to upper management or to your client, outlining your results and any recommendations you wish to share.**
- Keep these parties in the loop to show that your efforts and their money are well spent.

Cracking Hacker Mindset

- Knowing what hackers and malicious users wants helps to understand **how they work.**

Thinking Like the bad guys

- **Evading an intrusion prevention system:**
  - By changing MAC and 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, which might be made obvious by, for instance that the fact that office blinds are opened and curtains are pulled shut .

- **By passing web access controls**
  - By changing a malicious sites URL to its dotted decimal IP address equivalent and then converting it to hexadecimal for use in 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 wireless evil twin**
  - Near to local Wifi hotspot to capture entire n/w information and for easy manipulation

- **Using an overly trusting colleagues user ID and password**
  - To gain access to sensitive information that is very difficult to obtain

- **Unplugging the power cord or Ethernet connection to a networked security camera**

Who breaks into computer system

- Hacker skill level fall into three general categories:
  - Script Kiddies

    Beginners who take advantages of hacking tools, vulnerability scanners and documentation available free on the internet
  - Criminal Hackers

    These are skilled criminal experts and those who write some of the hacking tools, including the scripts and other programs that the script kiddies and ethical hacker used.

- **Advanced Hackers**
  - Nameless
  - Very secretive and share information with their subordinates only when they are deemed worthy.
  - They prove themselves via high profile hack.
  - These are some of the worst enemies in information security

- **Security researches:**
  - Highly technical and known as IT Professionals
  - Who not only monitor and crack computer, n/w, and application vulnerability but also write tools and other code to exploit them.

- **Hacktivist**
  - To distribute political and social messages through their work

- **Cyber terrorist:**
  - Attack govt computers or public utility infrastructure , such as air traffic control towers.
  - They crash critical system or steal classified govt information.

- **Hackers for hire**
  - – they are for money

Why do they do It

- Hobby- just want to know what they can break and what they cant.
- To promote individualism or at least the decentralization of information
- They don’t think about the choices that they are making today. Most of them say they don’t harm or profit through their bad deeds , a belief that justify their work.

- Some common motives are
  - Revenge
  - Curiosity
  - Boredom
  - Challenges
  - Theft for financial gain
  - Black mail
  - Extortion

  Simply just “against the man”

Hacking in the name of liberty

- Many hackers fight for civil liberties and want to be left alone but at the same time they love interfering in the business of others and controlling them in any way possible.

- Many hackers call themselves civil libertarians and claim to support the personal privacy and freedom.
- But 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 willing to go to great lengths to get their own right back.

Planning and Performing attacks

- Attacks styles may vary:
  - Some hackers prepare far in advance of an attack
  - Other hackers usually they are inexperienced script kiddies – act before they think through the consequences.
  - Malicious users are all over the map

- Although the hacker underground is a community, 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.**

Attckers know the following aspects of real-world security:

- **The majority of computer systems aren’t managed properly.**
- **Most network and security administrators simply can’t keep up with the invention of new vulnerabilities and attack methods.**
- **Information systems grow more complex every year.**

- 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.

- f you **want 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
  - (IN)SECURE Magazine
  - Hackin9
  - PHRACK

Maintaining Anonymity

- Smart hackers want to remain as low key as possible.
- They remain anonymous by using one of the following resources:
  - Open Wireless Network
  - Public computers at libraries ,school , local mall etc.
  - Borrowed or stolen desktop and VPN accounts
  - Anonymous email accounts.
  - Infected computers
  - Workstations or servers on the victims own network