UNDERSTANDING PURPOSE OF ETHICAL HACKING

- Ethical hackers are usually security professionals or network penetration testers who use their hacking skills and toolsets for **defensive and protective purposes.**
- T**est their network** and systems security for vulnerabilities using the **same tools** that a hacker might use to compromise the network.
- Any computer professional can learn the skills of ethical hacking.

•The term **cracker** describes a hacker who uses their **hacking skills and toolset for destructive or offensive purposes** such as disseminating viruses or performing denial-of service
•(DoS) attacks to compromise or bring down systems and networks.
•No longer just looking for fun, these hackers are sometimes **paid to damage corporate reputations** or steal or reveal credit card information, while slowing business processes and compromising the integrity of the organization.

HACKER TYPES

- **White Hat:** hacking skills for **defensive purposes**. locate weaknesses **and implement countermeasures**. White hats are those who hack with **permission from the data owner**. It is critical to get permission prior to beginning any hacking activity. This is what makes a security professional a white hat versus a **malicious hacker who cannot be trusted.**

- **Black:** Having gained **unauthorized access**, black-hat hackers
destroy vital data, deny legitimate users service, and just cause problems for their targets. Black-hat hackers and crackers can easily be differentiated from white-hat hackers because their actions are malicious.

- **Grey Hat:** work offensively or defensively, depending on the situation.
may just be interested in hacking tools and technologies and are not malicious black hats. Gray hats are **self-proclaimed ethical hackers**, who are interested in hacker tools mostly from a **curiosity standpoint**. They may want to highlight security problems in a system or educate victims so they secure their systems properly. difference between white hats and gray hats is that ***permission word***

Color of the Hat…

The 6 Different Types of Hackers

Black Hat Hackers: Bad hackers who use cyber attacks to gain money or to achieve another agenda.

These hackers penetrate systems without permission to exploit known or zero-day vulnerabilities.

White Hat Hackers: Ethical hackers who protect your systems from black hat hackers.

Penetrate the system with the owner's permission to find and fix security vulnerabilities and mitigate cyberattacks.

Grey Hat Hackers: Hackers who cruise the line between being good and bad. Penetrate systems without permission but typically don't cause harm.

Draw attention to vulnerabilities and often offer a solution to patch them by charging fees.

Red Hat Hackers: Hackers who use cyber attacks to attack black hat hackers.

Their intentions are noble, but these hackers often take unethical or illegal routes to take down bad hackers.

Blue Hat Hackers: Hackers who seek to take personal revenge, or outside security professionals that companies hire to test new software & other products to find vulnerabilities prior to release.

Green Hat Hackers: Newbie hackers who are learning to hack.

They're often not aware of the consequences of their actions & cause unintentional damage without knowing how to fix it.

WHAT DO ETHICAL HACKERS DO

- They do the same as cracker.
- they're trying to determine **what an intruder can see on a targeted network** and what the hacker can do with that information.
- **Pen Test:** This process of testing the security of a system or network is known as a ***penetration test.***
- doing this doesn't usually involve a mysterious leap of hackerly brilliance, but rather persistence and the **dogged repetition of a handful of fairly well-known tricks** that exploit common weaknesses in the security of target systems.
- A pen test is no more than just performing those same steps with the same tools used by a malicious hacker to see what data could be exposed using **hacking tools and techniques**.
- When hired, an ethical hacker asks the organization **what is to be protected, from whom, and what resources the company** is willing to expend in order to gain protection.
- A **penetration test plan** can then be built around the data that needs to be protected and potential risks. **Documenting the results** of various tests is critical in producing the end product of the **pen test: pen test report**.
- Taking **screenshots of potentially valuable information** or **saving log files** is critical to presenting the findings to a client in a pen test report.
- The pen test report is a compilation of all the **potential risks** in a computer or system.

GOALS ATTACKERS TRY TO ACHIEVE

- Breach computer system security
- Security consists of.
  - Confidentiality
  - Authenticity
  - Integrity
  - Availability
- **Perform DOS**: hacker attacks the ***Availability elements of systems and network.*** main purpose is to use up system resources or bandwidth.
- A flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to legitimate users of the system
- **Information Theft:** stealing passwords or other data as it travels in clear text across trusted networks, is a ***Confidentiality attack, because it allows someone other than the intended recipient to gain access to the data.***
  This theft isn't limited to data on network servers. Laptops, disks, and backup tapes are all at risk. **Company owned devices** r loaded with confidential information and can give a hacker information about the security measures in place at an organization.

GOALS ATTACKERS TRY TO ACHIEVE…

- ***Bit-flipping :*** *are considered* ***integrity attacks*** *because the data may have been* tampered with in transit or at rest on computer systems;

- System admins are unable to verify the data is **as the sender intended it**. A bit-flipping attack is an attack on a **cryptographic cipher**: the attacker changes the cipher text in such a way as to result in a **predictable change of the plain text**, although the attacker doesn't learn the plain text itself.

- This type of attack isn't directed against the cipher but against a message or series of messages. In the extreme, this can become a DoS attack against all messages on a particular channel using that cipher. The attack is especially dangerous when the attacker knows the format of the message.

- When bit-flipping attack is applied to **digital signatures** attacker may be able to change a promissory note stating "I owe you $10.00" into one stating "I owe you $10,000."

GOALS ATTACKERS TRY TO ACHIEVE…

- ***MAC address spoofing*** *:*
- *is an* ***authentication attack*** *because it allows an* ***unauthorized*** **device to connect to the network when** Media Access Control (MAC) filtering is in place, such as on a wireless network.
- By spoofing the MAC address of a legitimate wireless station, an intruder can take on that station's identity and use the network.