Hello Everyone! In this video you will learn about Hacking, a very important activity towards the security of cyber assets of any organization. You will also learn, how ethical hackers are different from malicious hackers, focused areas of ethical hackers and the advantages of ethical hacking.

Hacking refers to the misuse of devices like computers, smartphones, tablets, and networks to cause damage or to corrupt systems, gather information about users, steal data and documents, or disrupt data-related activity.
The person who performs the hacking activity is called a Hacker. He is a person who finds and exploits weaknesses in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

There could be various positive and negative intentions behind performing hacking activities. Here is a list of some probable reasons why hackers or Ethical hackier indulge in hacking activities. They can do it just for fun, to Show-off their skills, steal important information from the target, Damage the target system, disturb privacy, Money extortion, check the security of computers, or break policy compliance.

Some possible attacks through which hacker tries to compromise the victim's machine are

- Organizational attacks
- Social Engineering attacks
- Automated attacks

- Accidental Breaches types of attacks
- Viruses, Trojan horses, and worms based attacks
- Denial of Service attacks

A hacker performs the following activities while hacking your systems. The first activity or phase is Reconnaissance during which the attacker gathers information about a target using active or passive means. The tools that are widely used in this process are NMAP, Hoping, Maltego, and Google Dorks. After knowing the target system, the hacker performs scanning to actively probe a target machine or network for vulnerabilities that can be exploited. The tools used in this process are Nessus, Nexpose, and NMAP. After scanning the vulnerability is located and an exploit is attempted to enter the system. Metasploit is one of the tools, used during this phase. Once the access is gained, the hacker tries to maintain this access by installing some backdoors in order to enter the system whenever he needs to access it. After maintaining access, the hacker clears the evidence of compromise by deleting logs of all the activities that take place during the hacking process.

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 that Ethical hacking is legal.

Ethical hacking activities are very much important for organizations. Ethical hackers find out the weaknesses of the systems by performing penetration testing and strengthen them by putting or suggesting adequate preventive measures for avoiding any possible security breaches. They can help organizations in recovering lost information and keep the systems running.

Ethical Hackers Are Independent computer security Professionals breaking into computer systems with prior permission. They do not have any intention to damage the target systems or steal any information. Rather they evaluate the target system's security and report back to owners about the bugs found.

Ethical hackers focus on almost all areas of any organization. Such as user machines, Websites, Networks, and Email services belonging to the organization.

Ethical hackers use the same tools and techniques as used by hackers to get into these areas for checking security and strengthening it.

Let's see the difference between **Ethical Hackers and Malicious Hackers.** Ethical Hackers, Work towards improving the security of the organization by doing penetration testing, Develop most of the security software tools for security, Frequently check and update security software, Suggest using programs like pop up blocker, firewall and ad blocker while Malicious hackers , Steal valuable information from the organization or individuals, Steal money through illegitimate transactions ,Try to download copyrighted music and videos for free, Access restricted networking spaces.

An ethical hacker strives to ensure that any vulnerability or sensitive information that could damage the reputation or finances of an organization or its clients does not fall into the wrong hands. The ethical hackers perform penetration testing to ensure the immunity of the system against dumpster diving, social media based attacks, evading intrusion detection, vulnerability scanning etc. Ensuring the timely installation of patches is also one responsibility.

Thank you.