Hello Everyone! Now that you have understood the importance of ethical hacking and ethical hackers, you must know, what the skills required to become an ethical hacker
In this video, you will learn about the skills required to become an ethical hacker and will also learn about some courses and certifications which are essential to becoming a certified ethical hacker.

An ethical hacker must know about working of a **computer, Hardware Basics, programming skills, database management systems, operating systems, networking etc.**

An ethical hacker must be a computer systems expert and have a strong understanding of operating systems, and their working and security features like operating systems from Microsoft, which are the most commonly used operating systems by individuals and organizations.
Similarly, the Linux distributions like Ubuntu, CentOS, and Fedora are also required to be known as they are being used by most of the cyber security tools and are used by hackers to perform penetration testing.
They must also be aware of the security features provided by these systems such as windows defender firewalls, and open-source Linux firewalls such as IP tables, Pfsense, etc.

Apart from the Operating systems and their features, an ethical hacker must also be aware of routers, their configurations, various network protocols such as IP, TCP,

DNS, ARP, DHCP, HTTPS, etc., and different types of computers like workstations, servers, mainframes, etc.

There is a list of courses and certifications you might choose to pursue to become an ethical hacker−

- Obtain a bachelor's degree in Computer Science or A+ Certificate to gain an understanding of the most common hardware and software technologies.
- Get into a programmer's role for a few years and then switch to get a tech support position.
- Proceed to get network certifications like Network+ or CCNA and then security certifications like Security+, CISSP, or TICSA.
- It is recommended that you get some work experience as a Network Engineer and System Administrator to understand networks and systems inside out.
- Keep going through various books, tutorials and papers to understand various computer security aspects and take them as a challenge to secure your network and computer systems as network security engineer.

- Study courses which cover creating Trojan horses, backdoors, viruses, and worms, denial of service (DoS) attacks, SQL injection, buffer overflow, session hijacking, and system hacking.
- Master the art of penetration testing, foot printing and reconnaissance, and social engineering.
- Finally go for a Certified Ethical Hacker (CEH) Certification.

- GIAC (Global Information Assurance Certification) and Offensive Security Certified Professional (OSCP) are additional IT security certifications that will add a lot of value to your profile.

Thank You…