Ethical Hacking:

Classification of hackers:

- **Black hat:** Individuals with extraordinary computer skills who act with malicious intent for fun, personal gain or to cause damage to people or organisations.
- **Grey hat:** Individuals who work offensively and defensively at various times
- **White hat:** Individuals with same skills and knowledge as black hats and grey hats but whose intent is to protect people and companies and enhance security. They are also known as security analysts. White hat hackers are ethical hackers.
- **Suicide hackers:** Individuals aiming to bring down critical infrastructure for a cause. Unlike black hats, suicide hackers don't try to hide their true identity. Instead, they claim responsibility for their attacks
- **Script kiddies:** Individuals with no actual skill using tools created by others to try and hack organisations
- **Cyber terrorists:** Individuals or organisations motivated by religious or political beliefs. Try to create fear via large scale disruption of computer networks. Might attack countries and organisations to promote their causes.
- **State sponsored:** Individuals employed by governments to spy on enemies, neighbour countries and dissidents. Their goal is to enhance the country’s own security and obtain secret information which would be damaging to other countries and governments and their security.
- **Hacktivists:** Individuals who wish to promote their political agenda by hacking and defacing websites. Hacktivists don’t cripple critical infrastructure.

What is ethical hacking:

- Locating weaknesses and vulnerabilities in computers and information systems emulating the intents and actions of malicious actors/hackers.
- Intent of malicious actors/hackers is to attain personal gains or cause damage. Intent of ethical hackers is to try to identify vulnerabilities and weaknesses and enhance security by mitigating those weaknesses.
- Ethical hackers or penetration testers penetrate a computer system or network with the authorisation of the organisation/owner(s). They test the security controls, networks and applications used by the employer to find flaws so they can be fixed.

Job of ethical hackers:

- Test organisations security controls
- Test all applications,databases and computer systems being utilised by the company
- Trying to emulate malicious attackers
- Figure out vulnerabilities and weaknesses in the systems
- Generate a report based on their findings
- Provide recommendations for enhancing security

Advantages of hiring ethical hackers:

- Ethical hackers can emulate actual threats
- They allow the organisation to mitigate potential risks
- Ethical hackers increase the organisations productivity by allowing teams to focus on delivering the product
- Ethical hackers can guard the reputation of the company
- Security professionals can inspire the confidence of the customers
- They provide protection for customers and clients data
- Company can advertise itself as being secure and security compliant to clients

Phases of ethical hacking:

1. **Reconnaissance:** Identify the target. Gather evidence and information about the target. Get to know the target. Gather any personal or organisational information that can be leveraged for social engineering as well. Find out email addresses, IP addresses, domains and subdomains, phone numbers etc. used by the target.
2. **Scanning:** Actively scan for live devices. Scan live devices to determine the ports and protocols being used by the systems and the services running on those systems. These ports and protocols are the entry points into systems. The flaws exist here. Enumerate the systems. Scan for vulnerabilities and create list of possible vulnerabilities which can be exploited.
3. **Gain access:** Exploit the vulnerabilities listed earlier to attack systems and gain access or embed a trojan, a virus, a key-logger, some spyware etc.
4. **Maintain access:** Retain access for an extended period of time in order to gain more information over time. Don’t rely on a single hack forever as it may not work after a period of time. Install an unauthorised backdoor.
5. **Cover tracks:** After installing the rootkit /trojan /spyware, the installed software will create directories and files. Try to erase the traces of the creation of these files. And to delete any logs that record your activity. Try to erase the traces of all of these activities.

Common types of attacks:

- **DDoS:** Distributed Denial of Service. Makes services unavailable for legitimate users.
- **Password attacks:** Attacks that try to access user accounts by cracking user passwords in order to gain unauthorised access to data.
- **MitM:** Capture data packets between victim client and target server. Attempts to intercept and analyse data packets for sensitive information.
- **E-mail attacks/phishing/social engineering:** Fake emails that persuade users to click links to malicious websites or links which download malicious files.
- **SQL injection:** Target websites and web applications with databases connected to them. Misconfigured and unsecured servers can be exploited by sending malicious queries which can dump data or expose confidential information.

- **Eavesdropping attack:** Attacker observes traffic on the system. Trojans, wire tapping etc. fall under eavesdropping attacks.

Certs:

- **Foundational knowledge:**
  - ➔ BS in CS or IT/Security field
  - ➔ Solid foundation in networks and protocols
  - ➔ Experience with and understanding of programming and scripting languages
  - ➔ A solid understanding of the architectures, operations and internal workings of Operating Systems
  - ➔ Knowledge about cloud systems, cloud services and cloud security
  - ➔ Knowledge about malware analysis and reverse engineering

- **CEH(Certified Ethical Hacker)**

- **ECSA/LPT(EC Council Certified Security Analyst /Licensed Penetration Tester)**

- **(Self note: Video doesn’t include information about other certifications such as Comptia Security+, OSCP, PNPT, eJPT etc)**