The Certified Ethical Hacker (CEH) exam covers a wide range of topics related to cybersecurity and ethical hacking. Here are the core concepts and principles that you should be familiar with for each category of the exam:

1. Introduction to Ethical Hacking

   Definition of ethical hacking
   Legal and ethical considerations
   Types of hackers
   Phases of ethical hacking

2. Footprinting and Reconnaissance

   Information gathering techniques
   Footprinting through search engines, social media, and other tools
   DNS enumeration
   Network scanning
   Enumeration and vulnerability scanning

3. Scanning Networks

   Port scanning techniques
   Network mapping
   Banner grabbing
   Vulnerability scanning
   Operating system fingerprinting

4. Enumeration

   NetBIOS enumeration
   SNMP enumeration
   LDAP enumeration
   NTP enumeration
   SMTP enumeration

5. System Hacking

   Password cracking techniques
   Privilege escalation
   Trojans, backdoors, and rootkits
   File and folder permissions
   Physical security attacks

6. Malware Threats

   Types of malware
   Virus, worm, and Trojan horse
   Spyware and adware
   Rootkits
   Bots and botnets

7. Sniffing

Types of sniffing attacks
Sniffing tools and techniques
ARP poisoning
MAC flooding
DNS poisoning

8. Social Engineering

Types of social engineering attacks
Human-based attacks
Email-based attacks
Phone-based attacks
Dumpster diving
Physical social engineering attacks

9. Denial-of-Service

Types of DoS and DDoS attacks
DoS/DDoS tools and techniques
Ping of Death
SYN flood
Smurf attack

10. Session Hijacking

Session hijacking techniques
Cookie hijacking
Session fixation
Cross-site scripting
Cross-site request forgery

11. Hacking Web Servers

Web server attacks
Web server hacking tools and techniques
File inclusion attacks
SQL injection
Command injection

12. Hacking Web Applications

Web application attacks
Web application hacking tools and techniques
Cross-site scripting
SQL injection
Session hijacking

13. SQL Injection

Types of SQL injection attacks
SQL injection tools and techniques
SQL injection countermeasures
Blind SQL injection
Error-based SQL injection

14. Hacking Wireless Networks

    Types of wireless networks
    Wireless encryption and authentication
    Wireless hacking tools and techniques
    WEP cracking
    WPA/WPA2 cracking

15. Hacking Mobile Platforms

    Mobile platform vulnerabilities
    Mobile hacking tools and techniques
    Android hacking
    iOS hacking
    Mobile malware

16. IoT Hacking

    IoT security vulnerabilities
    IoT hacking tools and techniques
    Firmware attacks
    Radio frequency attacks
    IoT botnets

These are the core concepts and principles that you should know for each category of the CEH exam. However, this is not an exhaustive list, and you should also be familiar with other related topics, such as cryptography, incident response, and penetration testing.