Study Guide

Certified Ethical Hacking®

# Checklist of Exam Objectives: Areas to Study

## Discuss information security and ethical hacking

## Review of current security trends

## Review cyber kill chain methodology and concepts (tactics, techniques, and procedures (TTPs))

## Discuss adversary behavioral identification

1. Discuss indicators of compromise and their categories (IOCs)
2. Discuss hacking concepts, types, and phases
3. Discuss ethical hacking concepts and scope
4. Review information security controls
5. Discuss information security laws and standards

# Exam Essentials: What you need to know

#### Types of Hackers - Blackhat, Whitehat, Grayhat, Script-Kiddies, State Sponsored, Suicide Hackers

#### Types of Attacks- Active, Passive, Insider, Close-in, and Distribution

#### Steps in a Cyber Kill Chain - Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Action on objective

## 

# Important Terminology

#### Reconnaissance --Identifying information about the target before attacking.

#### Penetration Test -- A method of evaluating the security of a network or computer system by simulating an attack by a malicious hacker without harming and with the owner's written consent.

#### Ethical Hacker -- A security professional who legally attempts to break into a computer system or network to find its vulnerabilities.

#### Ethical Hack --A type of hack done to help a company or individual identify potential threats on the organization’s IT infrastructure or network.

#### Footprinting -- Identifying the size and scope of the target network.

#### Rootkit -- A collection of software tools that gives a threat actor remote access to and control over a computer or other system.

#### Enumeration -- A technique used to extract user names, machine names, network resources, shares, and services from a target.

#### Scanning -- Collects more information using complex and aggressive reconnaissance techniques.

#### Encryption — The process of rendering sensitive data unreadable through substitution and transposition using a mathematical function (algorithm)

#### Confidentiality — the protection of sensitive data from unauthorized disclosure

#### Integrity — The measure of accuracy or precision of an entity or process

#### Availability — the measure of the criticality of an entity and the value of the entity to supporting a business process

#### Non-repudiation — The ability to link actions to an individual entity

#### Threat — Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

#### Attack — Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

#### Vulnerability — Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

#### Risk Acceptance — The level of risk within the limits set by the risk owner

#### Information Security Risk — The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.

#### Incident — an adverse event with the potential to affect business mission

#### Social Engineering — the manipulation of a person to induce them to do something they should not do

#### Compliance — Proven adherence to standards

# Self-Assessment Questions: Test your Understanding

1. When is it OK to test someone's system?
   1. If you suspect the system has been compromised
   2. If you suspect the system is of high value
   3. When you’ve been given permission or invited to
   4. When you’ve detected a system has a vulnerability
2. What is the purpose of ethical hacking?
   1. To test your security skills
   2. To look for patches and upgrades
   3. To gain an advantage over your competition
   4. To identify security issues before attacks identify them
3. While testing you accidentally come across a vulnerability on a network outside the scope of the engagement. What do you do?
   1. Notify your employer immediately
   2. See how far you can dig into the network
   3. Review the IDS logs to find the misconfiguration
   4. Add the vulnerability to your work of discovery and go back to your assignment
4. What’s the purpose of “Covering Your Tracks”?
   1. Determine the size of the scope
   2. Clean up after a Pen-Test
   3. To hide activity
   4. To hide tools in a rootkit
5. Which type of hacker does their work for good?
   1. Blackhat
   2. Whitehat
   3. Greyhat
   4. Redhat
6. What describes a collection of software tools that allows an attacker remote access to a target?
   1. SIEM
   2. Rootkit
   3. Social engineering kit
   4. GDRP
7. The main purpose of DMCA is to do what?
   1. Protect the transmission of the credit card processing
   2. Create a framework for “Purpose limitations”
   3. Guidance for security control systems
   4. Stop the circumvention of technology protections
8. Which Act protects the public and investors by increasing the accuracy and reliability of corporate disclosures?
   1. SOX
   2. DMCA
   3. GDPR
   4. DPA
9. Which law requires all providers, plans and employees to have a standard national number?
   1. GDPR
   2. DPA
   3. HIPPA
   4. FISMA
10. Which phase of hacking comes after Reconnaissance?
    1. Gaining access
    2. Clearing tracks
    3. Maintaining access
    4. Scanning
11. Why type of hacker is described as one that will hack without worries of legal consequences
    1. Gray Hat
    2. Black Hat
    3. Suicide Hacker
    4. Script Kiddie
12. Which type of attack is described as “difficult to detect”
    1. Active
    2. Insider
    3. Close-in
    4. Passive
    5. Distribution
13. The 2021 SolarWinds attack where attackers were able to infect software that then was sold to customers is an example of what type of attack?
    1. Insider
    2. Passive
    3. Active
    4. Distributed
    5. Close-in
14. In the Cyber Kill Chain methodology, which phase do attackers establish a channel to communicate and pass data back and forth?
    1. Weaponization
    2. Delivery
    3. C&C
    4. Actions on Objectives
15. TTP is short for what?
    1. Tactical TCP Protocol
    2. Techniques Termination Processes
    3. The Threat Procedures
    4. Tactics Techniques Procedures

# Answers to Self-Assessment Questions:

1. C- When you’ve been given permission or invited to
2. D -To identify security issues before attacks identify them
3. A - Notify your employer immediately
4. When attackers begin exploiting a vulnerability on the day it is discovered, it is known as a zero-day attack.
5. B - Whitehat
6. B – Rootkit
7. D - Stop the circumvention of technology protections
8. A- SOX
9. C- HIPPA
10. D - Scanning
11. C - Suicide Hacker
12. D - Passive
13. C - Distributed
14. C - C&C
15. D - Tactics Techniques Procedures