

EC-Council (312-50)

CEH



**Smarter
Training**

This LearnSmart exam manual covers the most important topics you will encounter on the Certified Ethical Hacker (CEH) exam (312-50). By studying this manual, you gain familiarity with a wealth of exam-related content, including:

- Ethics and Legal Issues
- Footprinting
- Scanning
- System Hacking
- Session Hijacking
- And more!

Give yourself the competitive edge necessary to further your career as an IT professional and purchase this exam manual

Ethics and Legality

Nothing contained in this Exam Manual is intended to teach or encourage the use of security tools or methodologies for illegal or unethical purposes. Always act in a responsible manner. Make sure you have written permission from the proper individuals before you use any of the tools or techniques described in this exam manual.

What is an Exploit?

According to the Jargon Dictionary, an exploit is defined as, “a vulnerability in software that is used for breaking security.” Hackers rely on exploits to gain access to, or to escalate their privileged status on, targeted systems.

The Security Functionality Triangle

The CIA triangle or triad comprises the three fundamental pillars of security. These include:

- Confidentiality – Insures that the information is kept private and is only available to those that should have legitimate access to it. Threats to confidentiality include network sniffing and interception of passwords.
- Integrity – Insures that information and resources have not been improperly changed or altered. Threats to integrity include worms and viruses.
- Availability – Insures that the resources are available when needed by a legitimate user. Threats to availability include Denial of Service (DoS) attacks.

The Attacker’s Process

Attackers follow a fixed methodology. The steps involved in attacks are shown below and each will be discussed throughout this exam manual.

- Footprinting
- Scanning
- Enumeration
- Penetration – (Individuals that are unsuccessful at this step may opt for a Denial of Service attack)
- Escalation of Privilege
- Cover Tracks
- Backdoors

Reconnaissance

Reconnaissance is one of the most important steps of the hacking process. Before an actual vulnerability can be exploited it must be discovered. Discovery of potential vulnerabilities is aided by identification of the technologies used, operating systems installed, and services/applications that are present. Reconnaissance can broadly be classified into two categories: passive and active.

Passive Reconnaissance

This form of information gathering is the most covert as there is little to no way the target organization can discover the hacker's activity. An example of passive reconnaissance is that of scanning the help wanted ads to find out more about what types of technology and equipment the target organization uses.

Active Reconnaissance

This form of information is more overt as there is a chance that the target organization may notice the hacker's activities. An example of active reconnaissance is that of running a port scanner or using telnet to grab banners from the target organization's computers.

Types of Attacks

There are several ways in which hackers can attack your network. No matter which path of opportunity they choose, their goal is typically the same: control and use of your network and its resources.

- LAN Attack – This mode of attack is carried out over a Local Area Network
- WAN Attack – This mode of attack is attempted through remote services, i.e., via the Internet
- Physical Entry – This mode of attack is attempted through the lack of physical control of resources. Once a hacker has physical access, there is no remaining security
- Stolen Equipment – This mode of attack occurs when equipment is stolen and data, passwords, and configurations are recovered by the hacker
- Unsecured Wireless Access – This mode of attack can bypass firewalls and result in LAN access
- Dialup Attack – This mode of attack can be carried out if there are unsecured modems used by employees or routers that may have dialup capability that can be used for out-of-band management

Categories of Exploits

An exploit is the act of taking advantage of a known vulnerability. When ethical hackers discover new vulnerabilities, they usually inform the product vendor before going public with their findings. This gives the vendor some time to develop solutions before the vulnerability can be exploited. Some of the most common types of exploits involve:

- Program bugs
- Buffer overflows
- Viruses

- Worms
- Trojan Horses
- Denial of Service
- Social Engineering

Goals Attackers Try to Achieve

While the type of attack may vary, the hacker will typically follow a set methodology. This includes:

1. Reconnaissance - Passive and active
2. Gaining Access – The first phase of actual control
3. Maintaining Access – Planting back doors, cracking all of the systems' passwords, and adding accounts
4. Covering Tracks – Attempting to remove all traces of their activity, such as turning off logging and clearing the log files

Ethical Hackers and Crackers

Historically, the word **hacker** was not viewed in a negative manner. It was someone that enjoyed exploring the nuances of programs, applications, and operating systems. The term **cracker** actually refers to a "criminal hacker." This is a person that uses his skills for malicious intent.

Hacking for a Cause (Hacktivism)

These are individuals that perform criminal hacks for a cause. Regardless of their stated good intentions ("self proclaimed ethical hackers"), the act of gaining unauthorized access to someone's computer or system is nonetheless a crime.

Categories of Ethical Hackers

Ethical hackers can be separated into several categories:

- White Hat Hackers – These individuals perform ethical hacking to help secure companies and organizations. Their belief is that you must examine your network in the same fashion a criminal hacker would to better understand its vulnerabilities.
- Reformed Black Hat Hackers – These individuals often claim to have changed their ways and that they can bring special insight into the ethical hacking methodology.

Skills Required for Ethical Hacking

Ethical hackers must possess an in-depth knowledge of networking, operating systems, and technologies used in the computer field. They also need good written and verbal skills because their findings must be reported to individuals that range from help desk employees to the CEO. These individuals must also understand the legal environment in which they operate. This is often referred to as the **rules of engagement**. These skills help ensure that ethical hackers are successful in their jobs.

Ethical Hacker Job Duties

Ethical Hackers typically perform penetration tests. These tests may be configured in such way that the ethical hackers have full knowledge or no knowledge of the target of evaluation.

- White Box Testing – The ethical hacker has full knowledge of the network. This type of penetration test is the cheapest of the methods listed here.
- Black Box Testing – This type of penetration test offers the ethical hacker very little initial information. It takes longer to perform, cost more money, but may uncover unknown vulnerabilities.

Security Evaluation Plan

The most important step that the ethical hacker must perform is that of obtaining a security evaluation plan. This needs to be compiled in document form and should clearly define the actions allowed during an ethical hack. This document is sometimes referred to as “rules of engagement.” It will clearly state what actions are allowed and denied. This document needs approval by the proper authorities within the organization that the security assessment is being performed on. The security assessment will be one of several common types.

Testing Types

The three most common types of tests are detailed below. These tests may require individuals on the team to attempt physical entry of the premises or manipulation of targeted employees through social engineering.

- Internal Evaluations – Performed on the internal network to determine what resources and information employees can access.
- External Evaluations – Examination of the external network; i.e., review of web, e-mail, and publicly accessible services to determine their vulnerabilities.
- Stolen Equipment Evaluations – This type of assessment is performed to determine what type of information leakage would result from equipment that was stolen or pilfered.

Ethical Hacking Report

There are three parts to the ethical hacking report. These include:

- Preparation – This part of the report outlines the what, when, who, and where of the ethical hack. What’s important here is that it is clearly stated what is and is not allowed, what the time schedule is and what resources are available to the ethical hacker. The document needs to be signed by the proper individuals and should be reviewed by the legal department.
- Findings – This portion of the report details what was found during the test.
- Conclusion – This portion of the report details what corrective actions should take place and the total cost of these activities.

Computer Crime

The United States Department of Justice defines computer crime as “any violation of criminal law that involved the knowledge of computer technology for its perpetration, investigation, or prosecution.” Statistics indicate that computers are used in the commission of a crime as much as 92% of the time. This means the computer could be used for research, e-mail, planning, or as an aid to avoid capture or detection. While there are many laws that can be applied to criminal offenses, the ones listed below focus on computer crimes.

Overview of US Federal Laws

Typically, illegal computer activity breaks federal law when one or more of the following conditions are met:

1. The illegal activity involves a computer owned by a US government department or agency
2. The activity involves national defense or other restricted government information
3. Banking, savings and loan, or other financial institutions have been accessed
4. The activity uses computers located in other states or countries
5. Interstate communication is involved

So, as you can see, it is very easy for a hacker to break federal law if he has used the Internet for any of his activities. While most computer crime is categorized under 18 U.S.C. 1029 and 1030, there are many other laws the hacker can run afoul of. These include:

18 U.S.C. 1029 Fraud and related activity in connection with access devices
18 U.S.C. 1030 Fraud and related activity in connection with computers
18 U.S.C. 1343 Fraud by wire, radio, or television
18 U.S.C. 1361 Injury to Government Property
18 U.S.C. 1362 Communication lines, stations or systems
18 U.S.C. 1831 Economic Espionage Act
18 U.S.C. 1832 Trade Secrets Act

Penalties for these laws can range from 5 to 20 years per offense. As these are federal offenses, the total amount of jail time is typically stacked. This means that two 20 year offenses would result in a 40 year jail term.

Cyber Security Enhancement Act of 2002

What is most important to know about the Cyber Security Enhancement Act of 2002 is that it specifies life sentences for hackers that endanger lives. It also allows the government to gather information, such as IP addresses, URL's, and e-mail without a warrant if they believe national security is endangered. Before 9-11, government agencies were required to obtain a warrant to access an individual's voicemail, e-mail, attachments or other electronic data. With the passage of the Cyber Security Enhancement Act, law enforcement may request the service providers (ISP's) supply this information upon demand. Groups concerned with individual freedom have complained about the passage of this law, as no search warrant is required.