EXIN

# EXIN Ethical Hacking

FOUNDATION

Certified by EXIN

## Exam Literature

Edition 201804

Author: Hans van den Bent

Disclaimer: Although every effort has been taken to compose this publication with the utmost care, the Authors, Reviewers, Editors and Publisher cannot accept any liability for damage caused by possible errors and/or incompleteness within this publication. Any mistakes or omissions brought to the attention of the Publisher will be corrected in subsequent editions. All rights reserved.

# Content

# Preface

This white paper presents exam literature for candidates studying for the EXIN exam Ethical Hacking Foundation (EHF). For the most recent exam requirements we would like to refer to the official EXIN Preparation Guide which can be downloaded from www.exin.com.

Protection against cybercrime is a must. Companies and governments globally are facing an ever-increasing risk of cybercrime as every day cyber-attacks become more aggressive and extreme. Current annual cost from cybercrime to the global economy run into billions of dollars and this will only increase. Organizations need to take more measures to protect their assets.

Ethical Hacking is such a measure: a well-known method of duplicating the intent and actions of malicious hackers in order to locate, evaluate and resolve hardware and software vulnerabilities.

EXIN Ethical Hacking Foundation is a basic level but hands-on certification that covers a variety of hacking related topics, including network traffic analyzing, wireless network hacking, network scanning and the penetration of computer systems and websites.

Ethical Hacking ties in perfectly with Secure Programming. The software developer builds security measures into the programming phase, and then his / her colleague tests the software for resilience to cyber-attack, using ethical hacking methods. If the program's defenses do not succeed, they can be fixed before the program goes live.

*EXIN, September 2015*

# 1. Defining Ethical Hacking

In this chapter we will first look at some definitions of hacking and ethical hacking. Secondly, we will describe different type of hackers because It is important to understand the dividing line between a “normal” hacker and an ethical hacker.

## 1.1 Definitions

### To Hack (verb)

Linguistically, the verb to hack has its origin in the Anglo-Saxon language (450-1066 ad).

tó-haccian - *To hack to pieces or cut to pieces*

Modern day malicious hackers will find some recognition in this definition. They typically cause damage. The present day and popular online dictionary Yourdictionary.com provides us with the following definitions:

(slang, computing) To hack into; to gain unauthorized access to (a computer system, e.g., a website, or network) by manipulating code.

(slang, computing) By extension, to gain unauthorized access to a computer or online account belonging to (a person or organization).

(computing) To accomplish a difficult programming task.

(computing) To make a quick code change to patch a computer program, often one that is inelegant or that makes the program harder to maintain.

*(Source: Yourdictionary.com (as viewed on 8 august 2015))*

### Hacker (noun)

**Hacker** \ *ˈha-kər*\
“A person who secretly gets access to a computer system in order to get information, cause damage, etc., e.g., a person who hacks into a computer system.”

*(Source: Merriam-Webster.com (as viewed on 8 August 2015))*

### Ethical Hacker

**Ethical hacker**
“A person who hacks into a computer network in order to test or evaluate its security, rather than with malicious or criminal intent: ethical hackers are becoming a mainstay of the effort to make corporate networks more secure.”

*(Source: oxforddictionaries.com (as viewed on 8 August 2015))*

Many more definitions of an ethical hacker can be found on the internet, but the bottom line is that compared to a normal hacker an ethical hacker only operates:

- With expressed (often written) permission;
- With respect for the individual's or company's privacy.

and

- Does not leave anything open for anyone to exploit at a later time;
- Lets the customer (by written report) know of any security vulnerabilities.

For those of you who would like to study “the language of hacking” further there is a full blown Hacker dictionary available in the Webster’s New World dictionary series.

## 1.2 Types of hackers

According to Hafele (2004): “to be labeled a hacker is understood in today’s society as being a derisive term.” However, his research shows that in the past that was not always the case, and being labelled a hacker was often seen as “a badge of honor bestowed to one who exhibited a high-level of expertise in knowledge about various computer-based subjects.” Therefore, we will need to take a closer look at what types of hackers are recognized in this day and age.

### White hat hacker (or ethical hacker)

Ethical hackers are so-called “white hat hackers.” According to Wikipedia “The term white hat (originating in Internet slang) refers to an ethical computer hacker, or a computer security expert, who specializes in penetration testing and in other testing methodologies to ensure the security of an organization's information systems.”

These tests may be conducted in different ways so that the ethical hacker:

- Has full knowledge
- Has partial knowledge
- Has no knowledge of the target to be evaluated

These different perspectives are called box-testing. We will go into more detail on this topic in chapter 3.

### Black hat hacker

According to Wikipedia: “A black hat hacker is a hacker who violates computer security for little reason beyond maliciousness or for personal gain." (Moore, 2005). Black hat hackers violate networks with the aim to destroy, modify, or steal data, or to disable a network.

### Grey hat hacker

According to Wikipedia: “The term grey hat refers to a computer hacker or computer security expert whose ethical standards fall somewhere between purely altruistic and purely malicious.” At the present day there are discussions on how to handle this type of hacking and hackers. Some hackers keep entering the customer’s systems after their contract has ended. This may seem altruistic, but is still illegal. There are also recent examples of hackers performing unasked for penetration tests resulting in the finding of information security vulnerabilities in public sector systems. After publishing these results on the internet, or through the press the authorities reacted in mixed ways. How many shades of grey are there? The hackers were sometimes prosecuted, and sometimes invited to be involved in the mitigation process. In the case of public scandals like WikiLeaks we prefer to speak of Hacktivism.

### Hacktivist

According to Wikipedia: “Hacktivism is the subversive use of computers and computer networks to promote a political agenda.”

Popular forms of hacktivism:

- Websites like WikiLeaks or software extensions like those made available by RECAP (an NGO*) set up for political purposes.
- Website mirroring. Making a copy of a (government) censored website in a non-censored domain.
- Geo-bombing. Geo-tagging of YouTube content to Google Maps and/or Google Earth. Example: When people fly over a certain location, e.g., the offices of an oppressive government, they can access video messages promoting civil liberties.
- Anonymous blogging, etc.

> * ”RECAP is a joint project of the Center for Information Technology Policy at Princeton University and Free Law Project. It is one of several projects that harness the power of the web to increase government transparency.”
>
> *(Source: recapthelaw.org (as viewed on 7 August 2015))*

### Penetration tester

A basic definition of a penetration tester is: “Someone whose job it is to attack computer systems in order to find security weaknesses that can then be fixed.” *(Source: macmillandictionary.com/open-dictionary/ (as viewed on 8 august 2015))*

Penetration testing is a more specific task performed by white hat or ethical hackers. Penetration testers are certified testing professionals who work according to a strict code of ethics. A penetration test is also called a Pentest. The process of penetration testing is discussed in more detail in chapter 3 (box-testing). Penetration tests are often a component of a full security audit. EC-Council is a well-known examination board that provides technical certifications for ethical hackers and penetration testers. After achieving the CEH (certified ethical hacking) certification individuals can go one step further and aim for the ECSA/LPT (EC-Council Security Analyst & Licensed Penetration Tester) certificate.

## 1.3 A short history of (ethical) hacking

Ethical hacking may seem a recent phenomenon, but in fact the first work that can be labelled as such was done in the first half of the 1970’s. Aasha Bodhan (2012) gives us the following example:

> “In 1974, the Multics (Multiplexed Information and Computing service) operating systems were then renowned as the most secure OS available. The United States Air Force organized an ethical vulnerability analysis to test the Multics OS and found that, though the systems were better than other conventional ones, they still had vulnerabilities in hardware and software security.”

The following table gives some examples of historic events on the ethical hacking timeline.

| | |
|---|---|
| 1974 | **Ethical vulnerability analysis** to test the Multics OS (see item above) |
| | |
| 1985 | **Phrack** is an online (originally printed) **magazine** written by and for hackers. It is the oldest and longest running and was first published November 17, 1985. |
| | |
| 1995 | **First use of the term "ethical hacking" by IBM's John Patrick.** Wikipedia: "John Russell Patrick (August 5, 1945 - ). During his tenure as a vice president at IBM, he helped launch the IBM ThinkPad and the OS/2 operating system and was later an influential force behind IBM's early adoption of the Internet and World Wide Web." |
| | |
| 2003 | OWASP established. **The Open Web Application Security Project (OWASP)** is a worldwide not-for-profit charitable organization focused on improving the security of software. |
| | |
| 2013 | **PTES standard established.** The penetration testing execution standard consists of seven main sections. These cover everything related to a penetration test. |

# 2. Legal aspects of ethical hacking and hacking ethics

It is important to understand the dividing line between a “normal” hacker and an ethical hacker. Many attempts have been made to draw this line, but in the best scenario it may still seem a little bit blurred. Words like white, grey and black hat hacker demonstrate that fact.

In this chapter we will first look at the legal implications of hacking. Ethical hacking needs to be legal(ized) in order to avoid possible negative repercussions. Next, we will look at the ethics part of ethical hacking including some codes, and finally we will have a brief look at ethical hacking contracts.

## 2.1 The legal implications of hacking

Privacy and data security are at the heart of the ethical discussion. What are the borders that may not be crossed?

Gunarto (2003) provides us with some essential questions that result from many negative impacts on privacy and security in the past:

- What information about individuals can be revealed to others?
- What information about individuals should be kept in databases, and how secure is the information in the computer systems?
- How should one handle data piracy on the computer networks?
- Who is allowed to access the data and information?
- How can safeguards be introduced to ensure that the information can be accessed only by the right person or organizations?

Many people, for a long time, thought that the online world of the internet and computer networks and data stores of organizations and individuals were a free for all. Most people did not ask themselves the questions above and therefore developed none or low ethics concerning cyberspace. According to Gunarto (2003): “Self-protection is not sufficient to make cyberspace a safe place to conduct business. The rule of law must also be enforced.”

Let's take a look at a recent example of hacking that may have been considered ethical in some ways by the perpetrators.

**The Legal Implications of the Cardinals' Alleged Hacking**
by Nathaniel Grow - June 16, 2015

"The New York Times dropped a bombshell of a story Tuesday morning, reporting that the FBI is investigating whether front-office officials from the St. Louis Cardinals may have illegally hacked into the Houston Astros' proprietary computer network. According to the Times, government officials believe that unnamed Cardinals employees may have accessed the Astros' computers in order to retrieve the team's internal trade discussions, proprietary statistics and scouting reports. The FBI has apparently traced the source of the hacking to a house shared by some Cardinals employees."

*(Source: fangraphs.com (as viewed on 8 august 2015))*

A famous saying is "all is fair in love and war," or in sports for all that matters. Maybe this is what the perpetrators of this offence thought before they started hacking into their rival's computer systems. However, they should have done their homework before the act.

The author Nathaniel Grow further states that "The primary law implicated by the Cardinals' alleged hacking would appear to be the Computer Fraud and Abuse Act. The CFAA was originally passed back in 1984 to protect both the government and the financial industry from electronic espionage. The law was later expanded in 1996, however, to cover any unauthorized, remote access of another's computer."

This story makes it clear that hacking is not considered to be a legal activity, and not taken lightly by international law makers and police organizations like the FBI. Nathaniel Grow further states that "So any Cardinals employees involved in the alleged hacking could potentially face criminal prosecution under the CFAA."

Ever since the 1980's international legislation and directives were created to ensure the privacy and security of computer systems and their users. At the (original) publication date of this paper the following legislation existed. For practical purposes we limit ourselves to some examples from major countries and regions like Europe (EU) and the U.S.A.

| **Country / Region** | **Year** | **Legislation / Directive** | **Summary** |
|---|---|---|---|
| USA | **1980** | Privacy Protection Act | Provides protection of privacy in computerized and other documents. |
| USA | **1987** | Computer Security Act | Security of information regarding individuals. |
| UK | **1990** | UK Computer Misuse Act | See example below table. |
| USA | **1997** | Consumer Internet Privacy Protection Act | Requires prior written consent before a computer service can disclose subscriber's information. |
| USA | **1997** | Data Privacy Act | Limits the use of personally identifiable information and regulates "spamming." |
| UK | **1998** | Data Protection Act | |
| EU | **2002** | 2002/58/EU | Directive on data protection and privacy in the digital age. |
| EU | **2013** | Directive 2013/40/EU | Directive on attacks against information systems |

**Example:**
The UK Computer Misuse Act (1990) covers the following computer misuse offences:

1. Unauthorized access to computer material.
2. Unauthorized access with intent to commit or facilitate commission of further offences.
3. Unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

**Hackers in chains: 13 of the biggest US prison sentences for electronic crime**
May 21, 2014 | By Caroline Wall (source: fierceitsecurity.com (as viewed on 8 august 2015))

“Last week David C. gained the dubious distinction of having the longest U.S. prison sentence ever for electronic crime.” - *Jail sentence: 20 years, Date sentenced: May 15, 2014*

## 2.2 Code of ethics

Let’s look at a definition of code of ethics first. Businessdictionary.com gives us the following definition:

Code of ethics - A written set of guidelines issued by an organization to its workers and management to help them conduct their actions in accordance with its primary values and ethical standards.
*(Source: Businessdictionary.com (as viewed on 8 august 2015))*

Although hackers are not your typical worker, Levy (1984) first suggests that a hacker’s code of ethics is on its way. In his own modest words he suggests that a “code of ethics is in the air.”

**The Hacker's Code of Ethics - Levy (1984)**

- Access to Computers - and anything which might teach you something about the way the world works - should be unlimited and total. Always yield to the Hands-On Imperative!
- All information should be free.
- Mistrust Authority - Promote Decentralization.
- Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
- You can create art and beauty on a computer.
- Computers can change your life for the better.

In these days of cybercrime this code of ethics may sound a bit optimistic or even anarchistic. Eventually not every hacker turned out to be such an idealist and legislation started to appear like for example the U.S.A. Computer Security Act in 1987. At the present day the best known codes for ethical hackers and penetration testers are provided by the International Council of Electronic Commerce Consultants (EC-Council). EC-Council is a member-supported professional organization, and best known as a professional certification body. `

**The EC-Council "Code of Ethics"** is the general code for all people involved in ethical hacking. EC-Council describes an ethical hacker as "any individual who is trained in mastering hacking technologies." The code consists of the following 17 clauses:

**Code of Ethics**

1. Privacy
2. Intellectual property
3. Disclosure
4. Areas of Expertise
5. Unauthorized Usage
6. Illegal activities
7. Authorization
8. Disclosure
9. Management
10. Knowledge Sharing
11. Confidence
12. Extreme Care
13. Malicious Activities
14. No Compromise
15. Legal Limits
16. Involvement
17. Underground communities

*The full text for each clause can be viewed at the EC-Council official website: eccouncil.org (as viewed on 8 august 2015)*

Clause *17-Underground Communities* for example describes that the individual shall not be part of any underground hacking community.

**The EC-Council Licensed Penetration Tester (LPT) Professional Code of Conduct** is aimed specifically at professional penetration testers.

The **LPT code** is divided into **four main principles:**

- Act within legal limits
- Act with honesty and integrity
- Uphold professionalism
- Maintain privacy and confidentiality

*The full description of each principle can be viewed at the EC-Council official website: eccouncil.org (as viewed on 8 august 2015)*

Having a formal contract is described in different hacking codes of ethics. We will discuss this topic in the next paragraph.

## 2.3 Legal agreements and contracts

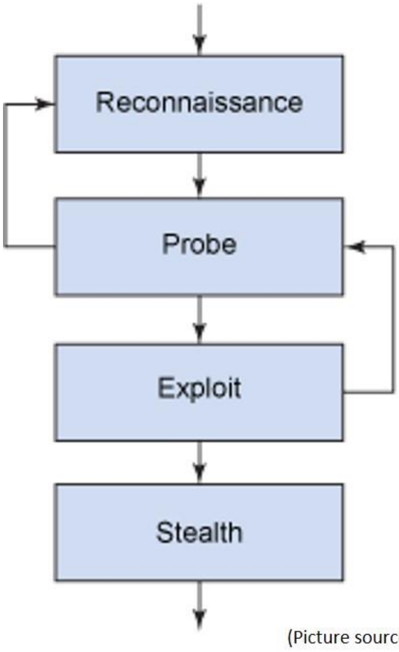
Because there is still some controversy around ethical hacking every ethical hacker should consider the legal implications of his/her work. A general advice is to put everything on paper and only work under a legally binding contract with the customer. Aspects to consider are:

- Permission from the customer and/or systems owner.
- The position of the owners whose personal data you may access via these systems. You will need to claim indemnity to cover issues like personal data that you access, third party intellectual property, etc.
- The different international, national and local legal acts, directives or regulations that may be involved.
- Authorization to hack.
- Contractual protection against liability.
- Indemnity to cover incompleteness of testing results like the vulnerabilities you do not find.
- Etc.

These are just some examples of areas to consider. A legal agreement or contract template should preferably be obtained from a specialized legal firm. Please consult your own legal advisor on how to proceed in this area.

# 3. Basic principles of ethical hacking

## 3.1 The generic hacking process



(Picture source: IBM.com)

**Figure 1: The generic hacking process**

**Explanation of the phases:**

1. Reconnaissance (or identification of the target);
   There are two main types of reconnaissance: Passive and Active.
   - The goal of passive reconnaissance is to gain information on the target by watching their offices and employees, entry procedures, and finding information on the Internet. Another method is called Network Sniffing which enables you to find useful information like IP addresses.
   - Active reconnaissance involves probing the network to discover individual hosts, IP addresses, and services on the network.

   The difference between non-ethical and ethical hacking is that in the first scenario you make sure that your target is not aware of your actions.

2. Probe (also known as scanning) and gain access;
   Identify vulnerabilities (touchpoints) that have the potential for exploitation. For this the hacker can use tools like: dialers, port scanners, network mappers, sweepers, and vulnerability scanners.

3. Exploit, gain and maintain access;
   Commonly used routes are the local area network (wired or wireless), local access to a PC, the Internet, or offline. Often used methods to get to own the system in hackers' terms, are: stack-based buffer overflows, Denial of Service (DoS), and session hijacking. Maintaining access can be achieved by creating backdoors or inserting rootkits, Trojans, etc.

4. Stealth, conceal your identity;
   At this stage hackers try to cover their tracks to avoid detection and subsequent prosecution. This is for example done by concealing, removing or altering system (log) files, intrusion detection alarms, etc. The concealing method is officially called Steganography (not to be confused with Stenography.) According to Wikipedia this is “the practice of concealing a file, message, image, or video within another file, message, image, or video,” and it “includes the concealment of information within computer files.”

## 3.2 The generic ethical hacking process

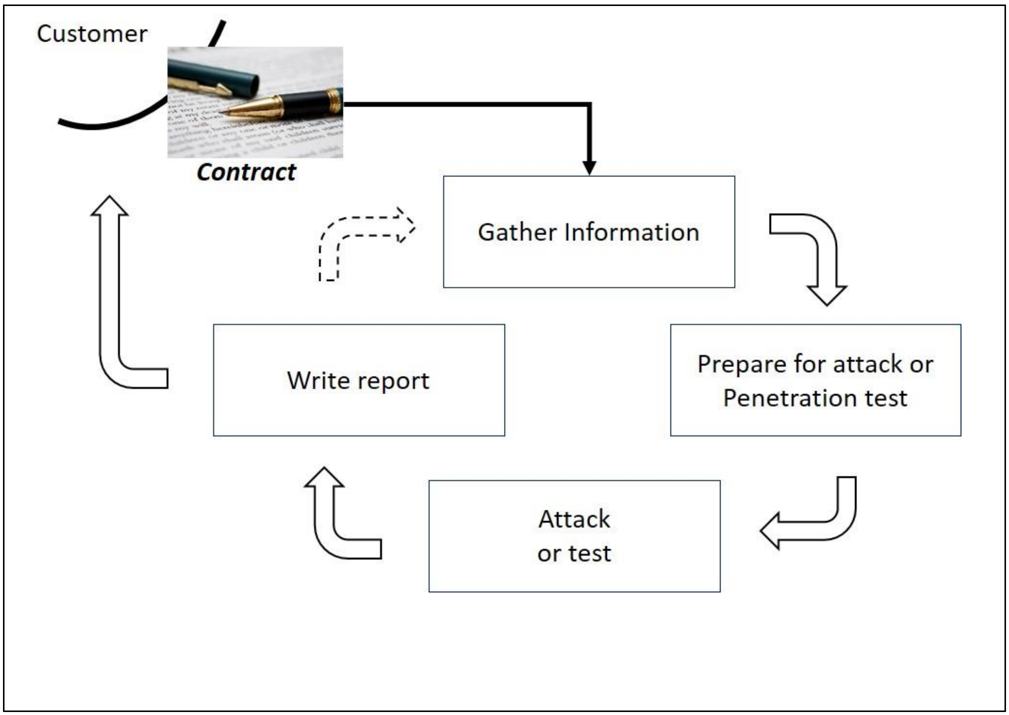


**Figure 2: The generic ethical hacking process (picture source: EXIN)**

The generic ethical hacking (or penetration testing) process consists of four main steps:

1. Information gathering; Including identifying target IP range of addresses, identifying ports/service and scan for vulnerabilities.
2. Attack preparation; Investigate gathered information, correlate results with plan.
3. Attack execution; Exploit vulnerabilities using different tools.
4. Report writing; Document findings and report to customer.

*How this process technically works, including how to use tools, is discussed in detail by Georgia Weidman (2014) in her book “Penetration Testing: A Hands-On Introduction to Hacking”. This book forms the main exam literature for the EXIN Ethical Hacking Foundation exam. Details about the exam can be obtained from exin.com.*

## 3.3 Types of testing: White, Black and Grey Box

Before going through the phases of testing (or ethical hacking process) you need to formulate a plan and discuss this with the customer. This is very important because approval for ethical hacking is an essential element. The first part of this is that you:

- Obtain sponsorship of the project and getting your plan signed off by a proper authority inside the organization.
- If working for an external customer you also need to get a signed contract.

In ethical hacking terms, in this pre-phase you obtain your “Get Out of Jail Free card.” You will need this if it becomes unclear who hired you for the job, or, heaven forbid, the authorities knock on your door.

Next you have to determine how much knowledge of the systems you need to have, or will be provided with before you start testing. This will determine whether you will perform a:

- Black Box test; meaning NO knowledge
- White Box test; meaning full knowledge
- Grey Box test; meaning limited knowledge. The information is typically distributed to you during the testing process by a ‘white’ insider who decides what specific parts need testing or what extra tests need to be done based on the results.

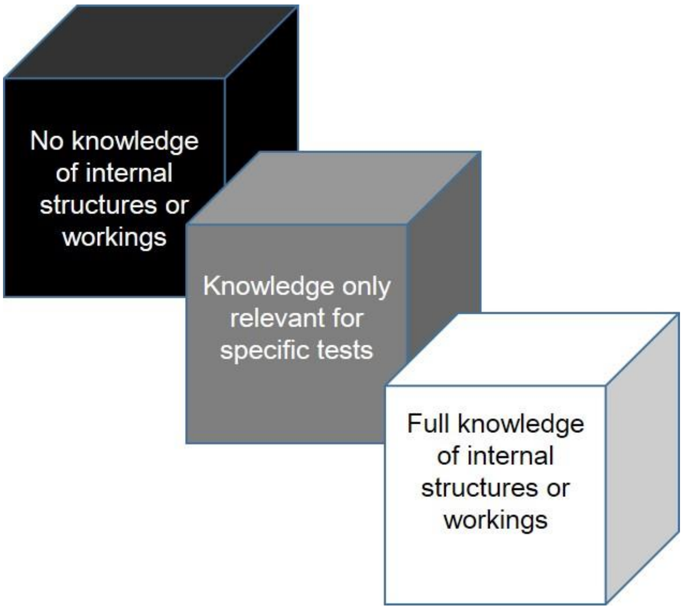

No knowledge of internal structures or workings
Knowledge only relevant for specific tests
Full knowledge of internal structures or workings

**Figure 3: Black, grey and white Box testing (picture source: EXIN)**

Other elements of the plan can be, but should not be restricted to:

- Systems to be tested (vulnerability candidates).
- Risk analysis; you need to determine the risks involved and create a contingency plan just in case things go wrong.
- Follow up actions for when vulnerabilities are detected.
- Specific deliveries for the project.
- Time frame for testing (during production hours or not, time allowed for the project, etc.).

### Black box testing

*(Also known as: Dark Box, Closed box, Opaque box testing)*

In penetration testing, black-box testing refers to a methodology where an ethical hacker has no knowledge of the system being attacked. The goal of a black-box penetration test is to simulate external hacking or a cyber-warfare attack.
According to Hafele (2004) “a very useful framework developed for this attack method is described by Paul Midian.” According to Paul Midian there are five basic phases to the Black Box test: the initial reconnaissance, service determination, enumeration, gaining access, and privilege escalation. Let’s go into a little bit more detail (source: Hafele (2004).

**Phase 1: initial reconnaissance (also known as foot printing)**
The goal of this phase is to investigate the target organization by means of publically available information, e.g., the company’s web site, ‘who is’ registers in order to obtain main IP addresses, chamber of commerce transcripts, trade magazines, publications, etc.

**Phase 2: service determination (also known as scanning)**
The goal of this phase is to derive information about the various listening services and ports that are currently operational on the client’s network. In this way the tester can determine the type of operating system that the client is using. (Different operating systems have unique characteristics in that they will listen on specific TCP ports for service traffic which is particular to that OS.

**Phase 3: enumeration**
The goal of this phase is to determine vital information about key resources like:

- Network resources and shares.
- Users and groups; in order to determine whether or not there are default user or administrator accounts operating on the network.
- Applications and banners; for example, banner grabbing is a technique that helps to determine what type of device the tester is dealing with and/or what type of software is running on it.

**Phase 4: attack and gaining access**
The goal of this phase is to establish a foothold into the customer’s network. The information retrieved in the first three phases form the input for this phase. Very often old administrator accounts are not deleted, and the older they are the weaker the passwords may be to be exploited by the tester.

**Phase 5: privilege escalation and maintaining access**
The goal of this phase is to attempt to gain administrative or root level privileges on the customer’s system. These privileges may vary from one specific item on the network or full control. Because the test is done in a proper white hat way the scope will be predetermined by the customer. A tester can use password cracking tools to achieve this goal. A non-ethical hacker would, at this stage, also create backdoors enabling others to enter the system.

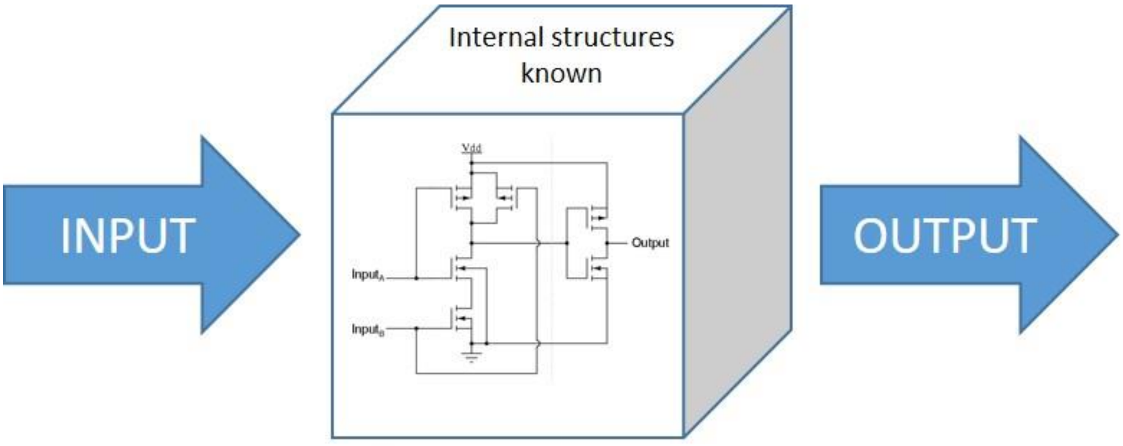
Examples of testing techniques that may be used for Black Box tests are: Equivalence partitioning, Boundary value analysis, Error Guessing, etc.

## White Box testing

*(Also known as: clear box, glass box, transparent box, or structural testing)*

In white box testing the testing team has much more knowledge of the customer's environment. The main characteristic is that the tester can look 'inside' the software.
White box testing can be applied at the unit, integration and system levels of the software testing process. A unit test is performed to ensure that the software code is working as intended. The goal of an integration test is to make sure that all interactions of each interface perform according to its design. A system test is performed to ensure the correct working of the complete integrated system.
A prerequisite for white box testing is a deep knowledge of the source code. This knowledge is needed in order to be able to create test cases. The creating process of test cases consists of three basic steps:

1. Input (preparation); requirements, functional specifications, detailed designing of documents, source code, security specifications.
2. Processing (build and execute test cases); this involves risk analysis, test plans, execution of the test cases and communication of provisional results.
3. Output (reporting); this involves preparing final reports that encompass all preparations and results.



Picture source: EXIN

**Figure 4: The White Box testing process.**

Examples of testing techniques that may be used for white box tests are: Control flow testing, Data flow testing, Path testing, Statement coverage, Decision coverage (or branch) testing, etc.

## Grey Box testing

Hafele (2004) calls this type of testing an "essentially hybrid attack model that incorporates elements of both the Black Box and the White Box methods." In Grey Box testing the tester applies limited (pre-determined) knowledge of the internal structure, e.g., logic, data flow, programming, execution flow etc. for doing functional testing which in essence is a Black Box technique. In this scenario there typically is a cooperation between a black hat outsider and a white hat insider feeding information to the outsider. Management is responsible for determining what information may be shared.

Grey Box testing is useful to simulate malicious hacking attacks and test real-time countermeasures performed by white hat insiders. A drawback of grey hat testing is that the attack team easily gets the information that they are looking for, but are therefore not forced to scrutinize the network, so vulnerabilities may be overlooked. An example of a Grey Box testing technique is regression testing (implies rerunning of the test cases if new changes are made).

# Appendix A: Literature and references

*This list of publications and URLs have formed the input for and/or are referred to in this publication. A listing of the official exam literature for the EXIN Ethical Hacking Foundation can be found in the official EXIN Preparation Guide for the EXIN Ethical Hacking Foundation exam that can be downloaded from EXIN.com. This document also contains a list of basic terms with which candidates should be familiar.*

**BCS Security Forum Strategic Panel (2008),** "ETHICAL HACKING – an oxymoron or an accepted industry term?"; *Version 1.2.*

**Aasha Bodhan (2012),** article: "Ethical hacking: bad in a good way."
*Engineering and Technology Magazine, vol. 7, issue 12*

**EC-Council,** "LPT Professional Code of Conduct v1.0"; *eccouncil.org.*

**Hary Gunarto ( 2003),** paper: "Ethical Issues in Cyberspace and IT Society"; *Ritsumeikan Asia Pacific University.*

**David M. Hafele (2004),** "shades-ethical-hacking-black-white-gray-1390"; *SANS institute white paper.*

**Steven Levy (1984),** "Hackers: Heroes of the Computer Revolution"; *Anchor Press/Doubleday, Garden City, NY, 458 pp.*

**Paul Midian (2002),** paper: "Perspectives on Penetration Testing — Black Box vs. White Box"; *Network Security Journal 11/2002;*

**C. C. Palmer (2001),** "Ethical Hacking"; *IBM systems journal, Vol 40, No 3.*

**Georgia Weidman (2014),** "Penetration Testing: A Hands-On Introduction to Hacking"; *ISBN-13: 978-1593275648*

## URLs

### Ethics

http://www.eccouncil.org/Support/code-of-ethics

### Testing and hacking

http://www.pentest-standard.org/
http://hack-o-crack.blogspot.nl/2010/12/five-stages-of-ethical-hacking.html

### Legislation

http://www.legislation.gov.uk/ukpga/1990/18/contents
http://www.legislation.gov.uk/ukpga/1998/29/contents
http://db.eurocrim.org/db/en/vorgang/252/
http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm
https://www.fbi.gov/about-us/investigate/cyber
http://www.justice.gov/criminal-ccips

# Appendix B: List of figures

## Contact EXIN

www.exin.com

EXIN

YOUR ICT COMPETENCE PARTNER