

Covers all Exam Objectives for CEHv6



Includes Real-World Scenarios, Hands-On Exercises, and
Leading-Edge Exam Prep Software Featuring:

- Custom Test Engine
- Hundreds of Sample Questions
- Electronic Flashcards
- Entire Book in PDF

CEHTM

Certified Ethical Hacker

STUDY GUIDE


Exam 312-50
Exam EC0-350

Kimberly Graves



SERIOUS SKILLS.

Chapter 15. Performing a Penetration Test.....	1
Section 15.1. Defining Security Assessments.....	2
Section 15.2. Penetration Testing.....	3
Section 15.3. Pen Test Deliverables.....	8
Section 15.4. Summary.....	10
Section 15.5. Exam Essentials.....	10
Section 15.6. Review Questions.....	11
Section 15.7. Answers to Review Questions.....	15



Chapter 15

Performing a Penetration Test

CEH EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ Overview of penetration testing methodologies
- ✓ List the penetration testing steps
- ✓ Overview of the Pen-Test legal framework
- ✓ Overview of the Pen-Test deliverables
- ✓ List the automated penetration testing tools



A penetration test simulates methods that intruders use to gain unauthorized access to an organization's network and systems and to compromise them.

The purpose of a penetration test is to test the security implementations and security policy of an organization. The goal is to see if the organization has implemented security measures as specified in the security policy.

A hacker whose intent is to gain unauthorized access to an organization's network is different from a professional penetration tester. The professional tester lacks malice and intent and uses their skills to improve an organization's network security without causing a loss of service or a disruption to the business.

In this chapter, we'll look at the aspects of penetration testing (pen testing) that you must know as a CEH.

Defining Security Assessments

A *penetration tester* assesses the security posture of the organization as a whole to reveal the potential consequences of a real attacker compromising a network or application. Security assessments can be categorized as security audits, vulnerability assessments, or penetration testing. Each security assessment requires that the people conducting the assessment have different skills based on the scope of the assessment.

A *security audit* and a *vulnerability assessment* scan IP networks and hosts for known security weaknesses with tools designed to locate live systems, enumerate users, and identify operating systems and applications, looking for common security configuration mistakes and vulnerabilities.

A vulnerability or security assessment only identifies the potential vulnerabilities whereas a *pen test* tries to gain access to the network. An example of a security assessment is looking at a door and thinking if that door is unlocked it could allow someone to gain unauthorized access, whereas a pen test tries to open the door to see where it leads. A pen test is usually a better indication of the weaknesses of the network or systems but is more invasive and therefore has more potential to cause disruption to network service.

Penetration Testing

There are two types of security assessments: external and internal assessments. An *external assessment* tests and analyzes publicly available information, conducts network scanning and enumeration, and runs exploits from outside the network perimeter, usually via the Internet. An *internal assessment* is performed on the network from within the organization, with the tester acting either as an employee with some access to the network or as a black hat with no knowledge of the environment.

A black-hat penetration test usually involves a higher risk of encountering unexpected problems. The team is advised to make contingency plans in order to effectively utilize time and resources.

You can outsource your penetration test if you don't have qualified or experienced testers or if you're required to perform a specific assessment to meet audit requirements, such as the Health Insurance Portability and Accountability Act (HIPAA).

An organization employing an assessment term must specify the scope of the assessment, including what is to be tested and what is not to be tested. For example, a pen test may be a targeted test limited to the first 10 systems in a demilitarized zone (DMZ) or a comprehensive assessment uncovering as many vulnerabilities as possible. In the scope of work, a service-level agreement (SLA) should be defined to determine any actions that will be taken in the event of a serious service disruption.

Other terms for engaging an assessment team can specify a desired code of conduct, the procedures to be followed, and the interaction or lack of interaction between the organization and the testing team.

A security assessment or pen test can be performed manually with several tools, usually freeware or shareware, though the test may also include sophisticated fee-based software. A different approach is to use more expensive automated tools. Assessing the security posture of your organization using a manual test is sometimes a better option than just using an automated tool based on a standard template. The company can benefit from the expertise of an experienced professional who analyzes the information. While the automated approach may be faster and easier, something may be missed during the audit. However, a manual approach requires planning, scheduling, and diligent documentation.

The only difference between true "hacking" and pen testing is permission. It is critical that a person performing a penetration test get written consent to perform the pen testing.



Real World Scenario

Ensure You Have Permission Before Pen Testing

About eight years ago I worked as a network administrator for an organization of some 500 users. My boss asked if I would do a security assessment of the organization's perimeter network. I told him to send me an email describing what he wanted to come out of the assessment, and within hours I was scanning my heart out.

After initial reviews, I found that the previous administrator had several "Allow All" exceptions set in the firewall. Our organization shared a connection, data, servers, and facilities with another organization that did much the same job as ours. Once I did the review and fixed a number of issues, my boss told other managers of the progress, and they decided that they wanted me to test the other organization's perimeter. I requested first thing that they make sure we had authorization to do that testing. After a day or two, my manager told me that we were good to go on the testing. Management was concerned about someone attacking the other organization and tunneling through our dedicated line to our network.

I did not get a copy of the written authorization to conduct the testing (that is, the very important "Get Out of Jail Free" card).

During the scan, I found a network—which had no firewall and mostly unpatched servers—running IIS web services, with only antivirus software for protection. The network was also running an Oracle database.

I stopped doing anything on that machine and network once I was able to login as admin on the server because doing anything further was pointless. I wrote a report and submitted it to my manager.

About a month later someone on our staff read in the newspaper that the other organization "got hacked." The office of the state attorney general became involved, and my managers and I were threatened with prosecution. Ultimately, nothing happened to me or my manager. The moral of the story: always carry your Get Out of Jail Free card, and make sure you have a signed copy. Don't ever take anyone's word for it.

Penetration Testing Steps

Penetration testing includes three phases:

- Preattack phase
- Attack phase
- Postattack phase

The *preattack phase* involves reconnaissance or data gathering. This is the first step for a pen tester. Gathering data from Whois, DNS, and network scanning can help you map a target network and provide valuable information regarding the operating system and applications running on the systems. The pen test involves locating the IP block and using Whois domain name lookup to find personnel contact information, as well as enumerating information about hosts. This information can then be used to create a detailed network diagram and identify targets. You should also test network filtering devices to look for legitimate traffic, stress-test proxy servers, and check for default installation of firewalls to ensure that default users IDs, passwords, and guest passwords have been disabled or changed and no remote login is allowed.

Next is the *attack phase*, and during this phase tools can range from exploitive to responsive. They're used by professional hackers to monitor and test the security of systems and the network. These activities include but aren't limited to the following:

Penetrating the Perimeter This activity includes looking at error reports, checking access control lists by forging responses with crafted packets, and evaluating protocol filtering rules by using various protocols such as SSH, FTP, and telnet. The tester should also test for buffer overflows, SQL injections, bad input validation, output sanitization, and DoS attacks. In addition to performing software testing, you should allocate time to test internal web applications and wireless configurations, because the insider threat is the greatest security threat today.

Acquiring the Target This set of activities is more intrusive and challenging than a vulnerability scan or audit. You can use an automated exploit tool like CORE IMPACT or attempt to access the system through legitimate information obtained from social engineering. This activity also includes testing the enforcement of the security policy, or using password cracking and privilege escalation tools to gain greater access to protected resources.

Escalating Privileges Once a user account has been acquired, the tester can attempt to give the user account more privileges or rights to systems on the network. Many hacking tools are able to exploit a vulnerability in a system and create a new user account with administrator privileges.

Executing, Implanting, and Retracting This is the final phase of testing. Your hacking skills are challenged by escalating privileges on a system or network while not disrupting business processes. *Leaving a mark* can show where you were able to gain greater access to protected resources. Many companies don't want you to leave marks or execute arbitrary code, and such limitations are identified and agreed upon prior to starting your test.

The *postattack* phase involves restoring the system to normal pretest configurations, which includes removing files, cleaning Registry entries if vulnerabilities were created, and removing shares and connections.

Finally, you analyze all the results and create two copies of the security assessment reports, one for your records and one for management. These reports include your objectives, your observations, all activities undertaken, and the results of test activities, and may recommend fixes for vulnerabilities.

Exercise 15.1 shows a framework for a comprehensive penetration test.

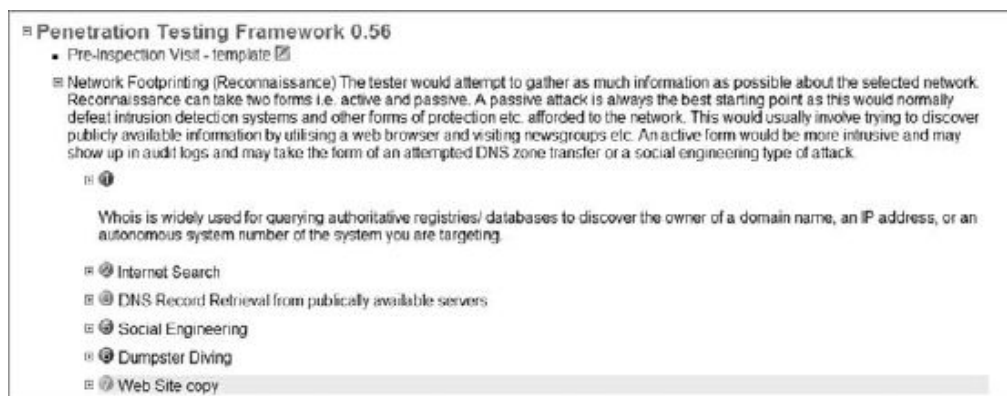
EXERCISE 15.1

Viewing a Pen Testing Framework of Tools

1. Open a web browser to www.vulnerabilityassessment.co.uk.



2. Click the Pen Test Framework link near the top.
3. Expand the Network Footprinting section and view the subheadings.



4. Continue down the major heading, expanding each of the subheadings for the pen test framework. You can use this list to locate all the tools necessary in each step of the pen testing process.

The Pen Test Legal Framework

A penetration tester must be aware of the legal ramifications of hacking a network, even in an ethical manner. We explored the laws applicable to hacking in Chapter 1. The documents that an ethical hacker performing a penetration test must have signed with the client are as follows:

- Scope of work, to identify what is to be tested
- Nondisclosure agreement, in case the tester sees confidential information
- Liability release, releasing the ethical hacker from any actions or disruption of service caused by the pen test

Automated Penetration Testing Tools

A 2006 survey of the hackers mailing list created a top-10 list of vulnerability scanning tools; more than 3,000 people responded. Fyodor (<http://insecure.org/fyodor/>), who created the list, says, “Anyone in the security field would be well advised to go over the list and investigate tools they are unfamiliar with.” The following should be considered the top pen testing tools in a hacker’s toolkit:

Nessus This freeware network vulnerability scanner has more than 11,000 plug-ins available. Nessus includes remote and local security checks, a client/server architecture with a GTK graphical interface, and an embedded scripting language for writing your own plug-ins or understanding the existing ones.

GFI LANguard This is a commercial network security scanner for Windows. GFI LANguard scans IP networks to detect what machines are running. It can determine the host operating system, what applications are running, what Windows service packs are installed, whether any security patches are missing, and more.

Retina This is a commercial vulnerability assessment scanner from eEye. Like Nessus, Retina scans all the hosts on a network and reports on any vulnerabilities found.

CORE IMPACT CORE IMPACT is an automated pen testing product that is widely considered to be the most powerful exploitation tool available (it’s also very costly). It has a large, regularly updated database of professional exploits. Among its features, it can exploit one machine and then establish an encrypted tunnel through that machine to reach and exploit other machines.

ISS Internet Scanner This is an application-level vulnerability assessment. Internet Scanner can identify more than 1,300 types of networked devices on your network, including desktops, servers, routers/switches, firewalls, security devices, and application routers.

X-Scan X-Scan is a general multithreaded plug-in-supported network vulnerability scanner. It can detect service types, remote operating system types and versions, and weak usernames and passwords.

SARA Security Auditor's Research Assistant (SARA) is a vulnerability assessment tool derived from the System Administrator Tool for Analyzing Networks (SATAN) scanner. Updates are typically released twice a month.

QualysGuard This is a web-based vulnerability scanner. Users can securely access QualysGuard through an easy-to-use web interface. It features more than 5,000 vulnerability checks, as well as an inference-based scanning engine.

SAINT Security Administrator's Integrated Network Tool (SAINT) is a commercial vulnerability assessment tool.

MBSA Microsoft Baseline Security Analyzer (MBSA) is built on the Windows Update Agent and Microsoft Update infrastructure. It ensures consistency with other Microsoft products and, on average, scans more than 3 million computers each week.

In addition to this list, you should be familiar with the following vulnerability exploitation tools:

Metasploit Framework This is an open source software product used to develop, test, and use exploit code.

Canvas Canvas is a commercial vulnerability exploitation tool. It includes more than 150 exploits.

Pen Test Deliverables

The main deliverable at the end of a penetration test is the pen testing report. The report should include the following:

- A list of your findings, in order of highest risk
- An analysis of your findings
- A conclusion or explanation of your findings
- Remediation measures for your findings
- Log files from tools that provide supporting evidence of your findings
- An executive summary of the organization's security posture
- The name of the tester and the date testing occurred
- Any positive findings or good security implementations

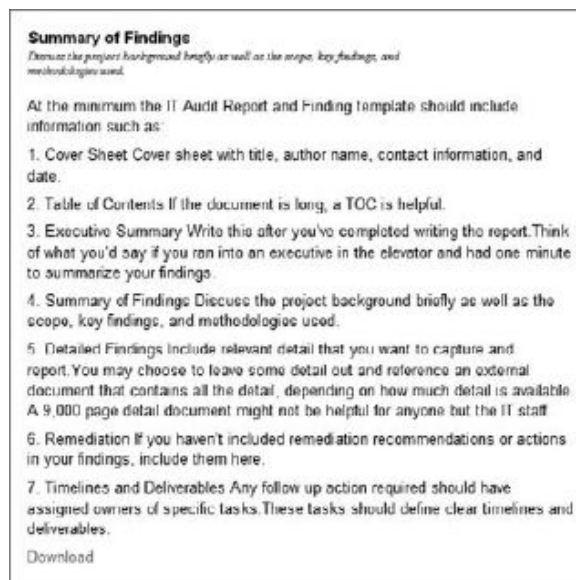
EXERCISE 15.2

Viewing a Sample Pen Testing Report Framework

1. Open a web browser to www.desktopauditing.com.
2. Click the link on the left side for IT Security Audit Report and Findings Template.

EXERCISE 15.2 (continued)

3. Scroll all the way to the bottom of the page and click the Download link.



4. Use the sample report as a template for creating your own security auditing reports.

Summary

Security auditing or pen testing is a necessary part of running a secure networking environment. It is critical that a trusted and knowledgeable individual such as a CEH test the systems, applications, and components to ensure all security findings can be addressed by the organization. The organization can use the pen testing report as a measure of how successfully they have implemented the security plan and to make improvements on the data security.

Exam Essentials

Be able to define a security assessment. A security assessment is a test that uses hacking tools to determine an organization's security posture.

Know pen testing deliverables. A pen testing report of the findings of the penetration test should include suggestions to improve security, positive findings, and log files.

Know the legal requirements of a pen test. A pen tester should have the client sign a liability release, a scope of work, and a nondisclosure agreement.

List the penetration testing steps. Preattack, attack, and postattack are the three phases of pen testing.

Know the two types of security assessments. Security assessments can be performed either internally or externally.

Review Questions

1. What is the purpose of a pen test?
 - A. To simulate methods that intruders take to gain escalated privileges
 - B. To see if you can get confidential network data
 - C. To test the security posture and policies and procedures of an organization
 - D. To get passwords
2. Security assessment categories include which of the following? (Choose all that apply.)
 - A. White-hat assessments
 - B. Vulnerability assessments
 - C. Penetration testing
 - D. Security audits
 - E. Black-hat assessments
3. What type of testing is the best option for an organization that can benefit from the experience of a security professional?
 - A. Automated testing tools
 - B. White-hat and black-hat testing
 - C. Manual testing
 - D. Automated testing
4. Which type of audit tests the security implementation and access controls in an organization?
 - A. A firewall test
 - B. A penetration test
 - C. An asset audit
 - D. A systems audit
5. What is the objective of ethical hacking from the hacker's prospective?
 - A. Determine the security posture of the organization
 - B. Find and penetrate invalid parameters
 - C. Find and steal available system resources
 - D. Leave marks on the network to prove they gained access
6. What is the first step of a pen test?
 - A. Create a map of the network by scanning.
 - B. Locate the remote access connections to the network.
 - C. Sign a scope of work, NDA, and liability release document with the client.
 - D. Perform a physical security audit to ensure the physical site is secure.

7. Which tools are *not* essential in a pen tester's toolbox?
 - A. Password crackers
 - B. Port scanning tools
 - C. Vulnerability scanning tools
 - D. Web testing tools
 - E. Database assessment tools
 - F. None of the above
8. What are not the results to be expected from a preattack passive reconnaissance phase? (Choose all that apply.)
 - A. Directory mapping
 - B. Competitive intelligence gathering
 - C. Asset classification
 - D. Acquiring the target
 - E. Product/service offerings
 - F. Executing, implanting, and retracting
 - G. Social engineering
9. Once the target has been acquired, what is the next step for a company that wants to confirm the vulnerability was exploited? (Choose all that apply.)
 - A. Use tools that will exploit a vulnerability and leave a mark.
 - B. Create a report that tells management where the vulnerability exists.
 - C. Escalate privileges on a vulnerable system.
 - D. Execute a command on a vulnerable system to communicate to another system on the network and leave a mark.
10. An assessment report for management may include which of the following? (Choose all that apply.)
 - A. Suggested fixes or corrective measures.
 - B. Names of persons responsible for security.
 - C. Extensive step by step countermeasures.
 - D. Findings of the penetration test.
11. What makes penetration testing different from hacking?
 - A. The tools in use
 - B. The location of the attack
 - C. Permission from the owner
 - D. Malicious intent

12. What documents should be signed prior to beginning a pen test? (Choose two.)
- A. Liability release
 - B. Nondisclosure agreement
 - C. Hold harmless agreement
 - D. Contract agreement
13. What is another name for a pen test?
- A. Compliance audit
 - B. Network audit
 - C. Security audit
 - D. Validation audit
14. What is the first part of the pen testing report?
- A. Findings
 - B. Remediation
 - C. Compliance
 - D. Executive summary
15. What is a type of security assessment in which the test is performed as if the tester were an employee working from within the organization?
- A. Internal assessment
 - B. Black hat testing
 - C. Full-knowledge test
 - D. Organization audit
16. Which type of test involves a higher risk of encountering unexpected problems?
- A. White-hat test
 - B. Black-hat test
 - C. Grey-hat test
 - D. Internal assessment
17. What is one reason to outsource a pen test?
- A. Specific audit requirements
 - B. Less risky
 - C. More findings
 - D. Effective countermeasures
18. In which phase of a pen test is scanning performed?
- A. Preattack phase
 - B. Information gathering phase
 - C. Attack phase
 - D. Fingerprinting phase

19. Which component of a pen testing scope of work defines actions to be taken in the event of a serious service disruption?
- A. Service requirements
 - B. Service-level agreement (SLA)
 - C. Minimum performance levels
 - D. Failback plan
20. Which automated pen testing tool can identify networked devices on the network, including desktops, servers, routers/switches, firewalls, security devices, and application routers?
- A. ISS Internet Scanner
 - B. Core Impact
 - C. Retina
 - D. Nessus

Answers to Review Questions

1. C. A penetration test is designed to test the overall security posture of an organization and to see if it responds according to the security policies.
2. B, C, D. Security assessments can consist of security audits, vulnerability assessments, or penetration testing.
3. C. Manual testing is best, because knowledgeable security professionals can plan, test designs, and do diligent documentation to capture test results.
4. B. A penetration test produces a report of findings on the security posture of an organization.
5. A. An ethical hacker is trying to determine the security posture of the organization.
6. C. The first step of a pen test should always be to have the client sign a scope of work, NDA, and liability release document.
7. F. All these tools must be used to discover vulnerabilities in an effective security assessment.
8. D, F. Acquiring the target and executing, implanting, and retracting are part of the active reconnaissance preattack phase.
9. A, D. The next step after target acquisition is to use tools that will exploit a vulnerability and leave a mark or execute a command on a vulnerable system to communicate to another system on the network and leave a mark.
10. A, D. An assessment will include findings of the penetration test and may also include corrective suggestions to fix the vulnerability.
11. C. Permission from the owner is the difference in hacking and pen testing.
12. A, B. A pen tester should have the client sign a liability release, a scope of work, and a non-disclosure agreement prior to beginning the test.
13. C. Security audits are another name for pen tests.
14. D. An executive summary should be the first part of a pen testing report.
15. A. An *internal assessment* is performed on the network from within the organization, with the tester acting as an employee with some access to the network.
16. B. A black-hat penetration test usually involves a higher risk of encountering unexpected problems. The team is advised to make contingency plans in order to effectively utilize time and resources.
17. A. You can outsource your penetration test if you don't have qualified or experienced testers or if you're required to perform a specific assessment to meet audit requirements such as HIPAA.

- 18. A. Gathering data from Whois, DNS, and network scanning can help you map a target network and provide valuable information regarding the operating system and applications running on the systems during the preattack phase.
- 19. B. In the scope of work, a service-level agreement (SLA) should be defined to determine any actions that will be taken in the event of a serious service disruption.
- 20. A. ISS Internet Scanner is an application-level vulnerability assessment. Internet Scanner can identify more than 1,300 types of networked devices on the network, including desktops, servers, routers/switches, firewalls, security devices, and application routers.