ETHICAL HACKING
PRACTITIONER

Sample Exam

SECO INSTITUTE

Sample Exam Ethical Hacking Practitioner

SECO-Institute issues the official Ethical Hacking courseware to accredited training centres where students are trained by accredited instructors. Students can take their exams at an accredited exam centre or directly at the SECO-Institute. Attending an official certification course is not a prerequisite for taking an exam. Upon successful completion of a practitioner exam (with a passing score of 60%), students can claim their digital badge at the SECO-Institute.

This document provides a sample exam for you to familiarise yourself with the structure and topic areas of the current Ethical Hacking Practitioner examination. We strongly recommend you to test your knowledge before taking the actual assessment. The results of this test do not count towards your certification assessment.

Examination type

Computer-based

- 1 Practical exercise ('Capture the Flag') *: 30 points
- 10 Multiple choice: 3 points per question
- 5 Open questions: 8 points per question

* The Capture the Flag hacking challenge is completed during the course. Students wishing to take the exam without enrolling for the course should contact the SECO-Institute.

Time allotted for examination

120 minutes

Examination details

- Pass mark: 60% (out of 100)
- Open book/notes: no
- Electronic equipment permitted: no
- The Rules and Regulations for SECO-Institute examinations apply to this exam.

This sample exam consists of:

- 10 Multiple choice questions
- 5 Open questions

Questions

Question 1

What is a popular tool to keep track of penetration test results?

A. KeepTrack
B. KeepNote
C. TrackTrace
D. OpenVAS

Question 2

Which CVSS score suits best for an SQL Injection that can be exploited remotely?

A. CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
B. CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:L/A:N
C. CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:N/I:L/A:N
D. CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H

Question 3

Robert wants to know the IPv6 address for www.seco-institute.org. Which record is he looking for?

A. CNAME
B. PTR
C. NS
D. AAAA

Question 4

Julia wants to scan all TCP/IP ports including a service scan on the open ports and determine which operating system the target is running. Which command would be best to achieve this?

A. nmap -vv -T5 -A -p 1-65545 <target>
B. nmap -vv -T4 -A -p - <target>
C. nmap -vv -p all -sV -O <target>
D. nmap -vv -p 0-65535 --scripts=os_detect,service_ident <target>

Question 5

On which layer of the OSI model is a TCP/IP segment defined?

A. Transport layer
B. Network layer
C. Application layer
D. Network access layer

Question 6

When performing a MitM attack using Ettercap, which protocol is abused?

A. HTTPS
B. UDP/IP
C. ICMP
D. ARP

Question 7

Which of the following is an MD5 hash?

A. 6eaf15d4506262ca8e023ccb432168e9a3e8f24d
B. 6eaf15d4506262ca8e023chb432168e9a3e8f24d
C. 4424345186616ae25810d3d6658f181f
D. 4424345186616ae25810g3d6658f181f

Question 8

Peter steals John's session cookie by taking advantage of a Cross-Site Scripting vulnerability and uses this cookie in his own browser. What is this technique called?

A. Session Manipulation
B. Browser Hijacking
C. Session Hijacking
D. Man in the Middle

Question 9

You have found a way to upload files through SQL Injection, but you need to convert your 'dropper' into hexadecimal values. What command-line tool would you use for this?

A. xxd
B. nano
C. hexxer
D. md5sum

Question 10

You have found a PostgreSQL server and want to launch a brute-force attack against it by using a Metasploit module. Which module would you use?

A. exploit/scanner/postgres/postgres_login
B. auxiliary/bruteforce/pgsql/postgres_login
C. admin/brute/login/scanners/postgresql
D. auxiliary/scanner/postgres/postgres_login

Question 11

What elements does a proper penetration test report contain?

Question 12

You are writing a buffer overflow exploit and have gathered all the information you need to write the code. What elements do you put in your final exploit?

Question 13

Define the phases of a penetration test as described in the first module of the course.

Question 14

Explain what White-, Gray- and Blackbox testing is.

Question 15

In the process of finding a buffer overflow, what is fuzzing?

Answers

1. **B**
   KeepNote is used to keep track of notes during penetration testing. It is a free and open-source tool, which is included in Kali Linux by default.

2. **A**
   CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

3. **D**
   AAAA

4. **B**
   nmap -vv -T4 -A -p - <target>

5. **A**
   Transport layer

6. **D**
   ARP

7. **C**
   4424345186616ae25810d3d6658f181f

8. **C**
   Session Hijacking

9. **A**
   xxd

10. **D**
    auxiliary/scanner/postgres/postgres_login

11. An introductive text, definition of scope, management summary, findings described properly and in a reproduceable manner, often providing information towards a solution, and a conclusion. During the training, a penetration test report example was discussed.

12. The first part is often the part that fills the existing buffer until it's edge. The next part is a return pointer, followed in most cases by NOPs. Then the shellcode containing instructions is defined, often generated to exclude found bad characters.

13. The first part is the intake process, where the penetration test is defined and scope is discussed. The second phase is reconnaissance where information is gathered about the target(s).

The next step is Attack Preparation, where possible exploits are gathered. This phase is followed by the actual attack/penetration phase, in which exploits are launched against the target(s). In the end, results have to be reported.

14. With a whitebox test, the tester usually has all the information he needs, including administrative logins, a network diagram and maybe even source code. This type of test is the most effective and can cover most elements in the least amount of time, but it is also the least realistic type of test. Blackbox tests are the exact opposite. Only the target address(es) are known and no logins are provided. Greybox tests are in between black and white tests. In these tests, normal login details are often provided but there is no access to source code or network diagrams.

15. Fuzzing is used to fill input variables until the application crashes, after which the crashes can be analysed and researched to possibly create a buffer overflow exploit.

How to book your exam?

All our exams are delivered through an online examination system called ProctorU. To enrol for an exam, go to: https://www.seco-institute.org/certification-exams/how-to-book-exam/
Make sure you are fully prepared. Use the ProctorU Preparation checklist to assess whether you are ready to take the exam.

Review the examination rules at
https://www.seco-institute.org/html/filesystem/storeFolder/10/Rules-and-Regulations-for-SECO-Institute-Examinations-2017-11.pdf

Claim your title and digital badge

Upon successful completion of an exam, students can claim their **S-EHP title** at the SECO-Institute. Each certification level requires a certain number of Continuing Professional Education (CPE) hours over an annual and a three-year-period. This requirement must be met in order to retain a certification. Practitioner certifications require a minimum of 20 CPE credits yearly (60 in the three-year certification cycle).

SECO-Institute and digital badge provider Acclaim have partnered to provide certification holders with a digital badge of their SECO-Institute certification. Digital badges can be used in email signatures as well as on personal websites, social media sites such as LinkedIn and Twitter, and electronic copies of resumes. Digital badges help certification holders convey employers, potential employers and interested parties the skills they have acquired to earn and maintain a specialised certification.

Claim your title at https://www.seco-institute.org/claim-your-title

EHP-Sample_Exam-EN-v1.0