ETHICAL HACKING
FOUNDATION

Sample Exam

SECO INSTITUTE

Sample Exam Ethical Hacking Foundation

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 foundation 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 Data Protection Foundation 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
- 40 Multiple choice: 2,5 points per question

Time allotted for examination

- 60 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

Questions

Question 1

You have found a live system on IP-address 192.168.11.54. Which nmap command lets you determine the operating system of the target?

A. nmap -oS 192.168.11.54
B. nmap -sn 192.168.11.54
C. nmap -O 192.168.11.54
D. nmap -sL 192.168.11.54

Question 2

Using Wireshark you encounter the following text in a packet "Authorization: Basic aHR0cHdhdGNoOmY=". What are you looking at?

A. A form of authentication using a digest
B. An HTTP protocol packet with basic authentication
C. A TCP/IP packet to login to a SSH server
D. Authorization packet to login to a WEP-encrypted Wifi network

Question 3

You find a live webserver. For what purpose would you use Dirb?

A. To scan the webserver for folders and filenames that are not at glance obviously present on the webserver
B. To test the website of application for known vulnerabilities
C. To check for the presence of injection vulnerabilities on the login page
D. To act as a MitM proxy and alter packets

Question 4

What does the CONCAT function within SQL do?

A. Concatenates two string values
B. Splits the value of a string in two values
C. Changes the table and put two columns in one column
D. Returns the values of two fields as one field

Question 5

If you click the login button on a webpage, what kind of request does the browser generally send to the server?

A. An HTTP POST request
B. An HTTP GET request
C. An HTTP PUT request
D. An HTTP OPTIONS request

Question 6

An ethical hacker gets no details on the target that must be tested. What kind of test is this?

A. Blackbox testing
B. White box testing
C. Greybox testing
D. Crystalbox testing

Question 7

What piece of information do you need if you want to find known vulnerabilities, for example using ExploitDB, in a standard product?

A. The operating system the product is running on
B. Full access to the server
C. Specific productname and version
D. Access to the source code

Question 8

Using Javascript (for example in case you are testing a XSS vulnerability), how would you get to the session cookie?

A. session.cookie
B. window.cookies
C. browser.cookies
D. document.cookie

Question 9

The SSID is used as?

A. Unique identifier of a service
B. Identification of a Wifi network
C. The service identifier of the wifi network adapter
D. The identification of a laptops network card

Question 10

In which step of the hacking process is Nikto most likely to be used?

A. Attack preparation
B. Information gathering
C. Reporting
D. Attack

Question 11

What is the purpose of the Burp Suite?

A. Act as a MITM proxy
B. Scan network hosts
C. Let's you take over a browser
D. Scan websites for vulnerabilities

Question 12

Why would a developer use sanitization on the output in a web application?

A. To speed up the web page by creating cleaner content
B. To be sure validations can be done properly and correctly
C. To make sure the output can never be interpreted as code by the browser
D. To check all input sent from a client/browser

Question 13

What are examples of webshell scripts?

A. R57, Bash
B. R57, C99
C. Bash, Zsh
D. Zsh, C99

Question 14

While testing you find that the website uses a URL parameter called "id". How would you test if it is vulnerable to SQL injection?

A. Use id=-1
B. Use id=<
C. Use id='
D. Use id=;

Question 15

You use the SQLmap option --os-shell. What are you trying to find?

A. See if a shell on the database can be started
B. Get the OS password from the user the database is using
C. Dump interesting database tables
D. A writable directory to upload a shell

Question 16

Which network type is the most secure?

A. WPA2 network with client certificate
B. WPA network with 'spoofing disabled' = yes
C. WEP network with password 'dfYFgC1@3%9)h7TRDTyu&lP3s'
D. Hidden WPA2 network with Pre-Shared Key (PSK)

Question 17

Which prerequisites are best for an Ethical Hacker?

A. A hardened system with a flexible network adapter i.e. it supports spoofing
B. A laptop with a hidden MAC-address to avoid premature discovery
C. A standard Kali Linux system
D. A high-end desktop PC with a wireless network adapter

Question 18

To investigate wireless networks, which mode must be set for your network device?

A. Mode = Managed
B. Mode = Monitor
C. Mode = Master
D. Mode = Special

Question 19

Which aireplay-ng option is essential to crack a wireless WEP network password?

A. option 'wlan' allows capture of 1500+ bytes of the WLAN traffic to extract the IV (initialization vector) of the encryption key
B. option '5' allows us to generate a valid key-stream based on previously captured WLAN traffic
C. option 'c' allows capture of necessary bytes to completely extract of the password
D. option 'MAC-from-AP' cracks the PRGA (Pseudo Random Generation Algorithm) of the selected wireless network

Question 20

Which parameters does 'packetforge-ng' need to successfully inject an ARP packet in a WLAN?

A. -0 <MAC-from-AP> <MAC-from-PC> <destination-mask> <source-mask> <packet-file>
B. -0 <WLAN-id> <full-broadcast> <destination-MAC> <source-MAC> <packet-file>
C. -w <WLAN-id> <full-broadcast> <destination-IPaddress> <source-IPaddress> <packet-file>
D. -w <MAC-from-AP> <MAC-from-PC> <destination-IPaddress> <source-IPaddress> <packet-file>

Question 21

The aircrack-ng tool reports 'insufficient amount of packets'. What is your best option to solve this problem?

A. Use aircrack-ng with the filter option -b for the MAC address from the access point
B. Set the option for aircrack-ng to start calculating right after 40.000 packets are availabe
C. Use airmon-ng options to block ARP-traffic from other WLAN networks
D. Generate traffic, capture new packets and write them to dump*.cap files with airodump-ng

Question 22

Which command decrypts previously captured wireless traffic data?

A. airdecap -a <MAC-from-AP> -p <Password> -r capture.cap
B. airdecap -m <MAC-from-AP> -e <BSSID> -s <Password> capture.cap
C. airdecap -b <BSSID> -e <ESSID> -w <Password> capture.cap
D. airdecap -b <BSSID> -e <ESSID> -d <Password> -r capture.cap

Question 23

Which command sends a fake authentication request to a WEP access point?

A. packetforge-ng -0 -a <MAC-from-AP> -y capture.cap -i wlan0mon
B. aireplay-ng -1 3600 –q 10 -a <MAC-from-AP> wlan0mon
C. aireplay-ng -5 -b <MAC-from-AP> wlan0mon
D. packetforge-ng -0 -a <MAC-from-AP> -y capture.cap -w arp-request

Question 24

Why is Base64 encoding generally used?

A. Encoding binary data with a XOR operation and a 64-bit key
B. To prevent automatic decoding of binary data
C. Translating binary data to text that can be transmitted in e-mails and HTML data
D. It is not used anymore, since it has been replaced by Base128 (ASCII) character encoding

Question 25

Which of the following tools is best suited to map accessible hosts in a network?

A. nmap
B. network-discover
C. wireshark
D. ip-show

Question 26

What is the best explanation for the cause of vulnerability for SQL injection?

A. If a website links to a database which stores login information of user accounts
B. The database is not properly isolated from the website (e.g. in a DMZ)
C. A webpage directly transfers a search request of the user to the database
D. The database administrator did not properly restrict access to the database

Question 27

What is the best description of false positives?

A. Scanning tools sometimes raise warnings which prove to be incorrect
B. Scanning tools sometimes produce errors when processing the input
C. Scanning tools do not raise exceptions based on processing suspicious input
D. Scanning tools produce errors which cannot be verified

Question 28

Why is the MD5 hashing algorithm considered as weak?

A. An MD5 hash apparently can be decrypted to retrieve the original password
B. The MD5 algorithm is broken as a one-way cryptographic function
C. An attacker can easily generate a text with a hash equal to the given MD5 hash
D. The md5sum tool can efficiently produce the hash of any password

Question 29

John the Ripper supports multiple types of password hashes, but can only crack one type at a time. We have a file that contains NTLM hashes and we would like to crack them. How can you force John the Ripper to crack the NTLM hashes without changing the input file?

A. You can't, you will need to copy the NTLM hashes into a separate file.
B. You use the command-line option --multi-format.
C. You use the command-line option --format=nt.
D. You edit the file ~/.john/john.log.

Question 30

Which tool support brute-force attacks?

A. L0pthCrack
B. ZAP
C. r57
D. Nikto

Question 31

What is the best reason not trying brute force to find a working SSH user-ID and password?

A. This will require much more time than other methods
B. This can cause us to be blocked from the system
C. Automated brute-force attacks can lead to false positives
D. SSH sessions on port 22 cannot be accessed by brute force

Question 32

Which tool does best fit this description: "discovers vulnerabilities in web applications"?

A. Dirb
B. Vega
C. THC Hydra
D. inj3ctor

Question 33

Structured Query Language (SQL) is used in ANSI relational database management systems and consists of the following special purpose languages:

A. Data query language, Data definition language, Database control language
B. Data definition language, Data control language, Data manipulation language
C. Object structuring language, Data definition language, Stored procedure language
D. Data specification language, Structured relation language, Database management language

Question 34

Which sqlmap option provides you the information that the database is vulnerable to SQL injection?

A. sqlmap -h “http://webapplication-URL”
B. sqlmap -u “http://webapplication-URL” --passwords
C. sqlmap -u “http://webapplication-URL”
D. sqlmap -p “http://webapplication-URL” --time-test

Question 35

If you turn off the safe mode in the R57 shell, which option becomes available?

A. You can execute commands directly on the server
B. You can edit, create and delete files on the server
C. You can launch a brute-force attack against the FTP server
D. You can send files from the server to your email (this leaves traces!)

Question 36

If a server is vulnerable to Local File Inclusion (LFI), how can it be exploited?

A. Request the server to display his local files
B. Include new content on websites
C. Session cookies can be altered and sent to the server
D. Put malicious scripts inside unvalidated parameters and then passed through

Question 37

What is the most common risk of downloading and using shell code for File Inclusion?

A. The shell code must be unescaped first to verify the code
B. The shell can trigger a Denial of Service attack by crashing the system
C. The shell code can be encrypted, to avoid code inspection
D. The shell can notify its creator that it is available on the system

Question 38

Why do developers allow File Inclusions on a web server?

A. Developers shouldn't use it, because it provides an extensive attack vector
B. Because (Web)applications receive and use input in many different forms
C. File inclusions are handy for developers, for example for reusing code
D. Developers can easily get shell access to repair production systems

Question 39

Which Linux command should be used to configure wireless devices?

A. ifconfig
B. iw
C. iwconfig
D. ipconfig

Question 40

Dirb finds a directory 'Phpmyadmin'. What is this directory most likely used for?

A. Phpmyadmin is a php-based interface for managing MySQL databases
B. Phpmyadmin is a tool to create webpages using the PHP script language
C. Phpmyadmin is the directory for the admin of the web server
D. Phpmyadmin is the directory to store restricted files on the web server

Answers

Question	Answer	Explanation
1	C	The correct nmap option is -O. The other options change the output (-o), skip DNS resolution(-n) or lists all hosts present (-L).
2	B	The correct answer is HTTP with basic authentication.
3	A	Scanning for folders and files on a webserver is the function of Dirb. For the others you should use other testing tools, like Nikto.
4	A	Within SQL the CONCAT function concatenates two string values
5	A	With normal forms in HTML the browser will send a HTTP POST request.
6	A	With no details on the target, this is blackbox testing.
7	C	You need the product name and version to find known vulnerabilities specific to that version of the product
8	D	The correct javascript DOM property is document.cookie
9	B	The answer is Wifi network identification
10	A	Nikto is mostly used in attack preparation. Nikto is too visible for information gathering and will give information on vulnerabilities that can be tested or used in the attack/verification phase.
11	A	Burp is a proxy and can be used for MITM attacks
12	C	Sanitation is used to make sure that output won't be interpreted as code
13	B	Examples are R57 and C99. The others are Linux shells
14	C	The correct test is by using the '
15	D	The correct answer is testing for writable directories to upload a webshell to.
16	A	When legitimate clients have a certificate, which matches the server certificate, this is the most secure option
17	C	A standard Kali Linux system has extensive tooling to support Ethical Hacking (e.g. Metasploit)
18	B	With Monitor mode your wireless network card can capture all traffic. With this mode, you can identify networks, devices, encryption (WEP, WPA, WPA2, ...) and the radio channels used.
19	B	Cracking the password requires sufficient packets from the router to discover the Initialisation Vector (IV). With aireplay-ng -5, we capture approximately 1500 bytes of network traffic to generate a valid key-stream
20	A	Options needed: -0: create ARP packet; -a : AP MAC address; -h: PC MAC address; -k: target IP mask (= broadcast); -l: source IP mask (= broadcast); -y: .xor file previously created; -w; write output to file
21	D	If a 'sufficient' amount of packets has not yet been reached, aircrack-ng will try again on the next expected threshold (5000 in this example)
22	C	The correct airdecap switches are: -b <MAC- address AP> -e <ESSID> -w <Password> capture.cap
23	B	aireplay-ng -1 3600 –q 10 -a <MAC-from-AP> wlan0mon
24	C	Base64 encoding is used to transfer binary data as human readable text

25	A	Nmap is the correct answer. Wireshark only intercepts random traffic and the other tools do not exist
26	C	An SQL injection is caused by unsanitized input of the user, which enables the user to run SQL queries on the database.
27	A	A false positive is a warning that later proves to be incorrect
28	C	The MD5 algorithm produces only 16-byte hashes, thus generating a 'collision' using brute-force is feasable with current computing power.
29	C	You could copy the hashes into a separate file, but that is awkward and the question asked to not do that. You can force the hash format with the --format option.
30	A	Only L0pthCrack is a tool that can brute-force passwords
31	B	Brute-force is very 'noisy' and may cause our further attempts to be blocked
32	B	Vega is a vulnerability scanner that automatically tests all web-pages provided by the web server
33	B	SQL = Data definition language, Data control language, Data manipulation language
34	C	The command: sqlmap -u "http://webapplication-URL" identifies the given URL for SQL Injection vulnerabilities
35	A	With safe mode turned off, you can execute commands directly on the server
36	A	With LFI, attackers can view server files, e.g. /etc/passwd
37	D	The creator can have a malicious intent to provide the shell code
38	C	By using file inclusions, developers can reuse (code) files on the server
39	B	iw, the rest is deprecated; ipconfig is a Windows command
40	A	Phpmyadmin is a commonly used php-based interface for managing MySQL databases

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

Digital badges

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.

SECO-Institute doesn't issue certification titles for Foundation courses. However, upon successful completion of your Foundation exam, you can claim your digital badge free of charge at the SECO-Institute.

https://www.seco-institute.org/claim-your-foundation-badge

EHF-Sample Exam-v1.3