ETHICAL HACKING
PRACTITIONER

Exam syllabus

S-EHP-2019

SECO INSTITUTE

Table of contents

Disclaimer

The SECO-Institute has made every effort to ensure that the information included in this exam syllabus were correct at the time of publication. Yet, the SECO-institute does not assume and hereby disclaims any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause.

Copyright notice

Exam Syllabus: Ethical Hacking Practitioner

The Ethical Hacking Practitioner certificate demonstrates that you have acquired intermediate-level knowledge of the most important aspects of Ethical Hacking. You are able to analyse network traffic, hack wireless networks, scan networks and penetrate computer systems and websites. You know what tools to use and how to manipulate applications into doing something they were not designed to do.

Context

The Practitioner training and certificate are intended to be an important career milestone for Ethical Hacking professionals, as they constitute the second level of a complete and extensive Certified Ethical Hacking Leader certification track. Obtaining the Ethical Hacking Practitioner certificate means that you have acquired sufficient knowledge to be able to continue with Ethical Hacking Expert and advance your career path to become a Certified Ethical Hacking Leader (CEHL). Students who already possess medium-level Ethical Hacking knowledge can decide to start their training with the Expert level of the certification track.

Target audience

This course is ideal for professionals whose work involves dealing with cybercrime or testing business systems to protect them against cyber threats. The certification is especially recommended to:

- Network and system administrators
- Penetration testers (ethical hackers)
- Security specialists

Exam information

SECO-Institute issues the official Ethical Hacking Practitioner courseware to accredited training centres where candidates are trained by accredited instructors. Candidates can take their exams at an accredited exam centre or directly with the SECO-Institute.

Examination details

- Computer-based
- Multiple choice & essay-type questions based on a case study
  - 10 MC: 3 points per question
  - 5 short essay-type questions: 8 points per question
  - 1 essay-type question based on a case study: 30 points
- Time allotted: 120 minutes
- Pass mark: 60%
- Open book/notes allowed? NO
- Electronic equipment permitted? NO

The Rules and Regulations for SECO-Institute examinations apply to this exam.

Exam requirements

The following tables list the exam requirements and exam specifications.

Ethical hacking practitioner											
Requirements	1. Introduction to Ethical Hacking (Foundation Recap) 2. Reconnaissance and Intelligence Gathering 3. Infrastructure Security 4. Web Applications 5. Systems and Applications 6. Exploiting Buffer Overflows										
Required prior Knowledge/experience	Basic technical knowledge of networks and software (e.g. operating systems, web apps, etc.).										
Learning levels	Know		Understand	x	Apply	x	Analyse, Synthesise		Create		

Exam specifications

Bloom level

2. Understanding
3. Applying

Requirements, specifications, testing levels				**Bloom level**
1.	**Introduction to Ethical Hacking (Foundation Recap)**			
	1.1	*The candidate can explain the concept of penetration testing*		2
		The candidate is able to:		
		1.1.1	*Explain how the penetration testing process works*	2
		1.1.2	*Describe the different types of penetration testing*	2
		1.1.3	*Describe different penetration testing guidelines*	2
Exam topics and terms			*Penetration testing process: scope, boundaries, legal waiver, testing phases. Blackbox, Graybox, Whitebox (code review), CVSS.*	
	1.2	*The candidate knows the basics of cybercrime legislation and hacking ethics*		2
		The candidate is able to:		
		1.2.1	*Describe legal terms and concepts relating to cybercrime*	2
		1.2.2	*Describe what legislation applies to cybercrime*	2
		1.2.3	*Explain the concept of hacking ethics*	2
Exam topics and terms			*Cybercrime, Personal identifiable information, ethics, handling vulnerabilities.*	
	1.3	*The candidate knows how to report on a penetration test*		3
		The candidate is able to:		
		1.3.1	*Describe the contents of a penetration test report*	2
		1.3.2	*Use a vulnerability scoring system*	3
Exam topics and terms			*CVSS: types of metrics, scoring, Cross-site Scripting (XSS), Attack Vector, Attack Complexity, Privileges Required User Interaction, Scope, Confidentiality Impact, Integrity Impact, Availability Impact.*	

Requirements, specifications, testing levels				Bloom level
2.	**Reconnaissance and Intelligence Gathering**			
	2.1	*The candidate can explain how intelligence gathering is performed*		2
		The candidate is able to:		
		2.1.1	*Describe the concept of Open-Source INTelligence gathering (OSINT)*	2
		2.1.2	*Explain how intelligence can be Gathered using WHOIS lookups*	2
		2.1.3	*Explain how intelligence can be Gathered using DNS lookups and enumeration*	2
Exam topics and terms			*Open Source Intelligence (OSINT): Using search operators in Google and using the GHDB, using online publicly available information, WHOIS lookups, 'whois', DNS lookups and enumeration, 'dig', DNSenum, fierce.*	
	2.2	*The candidate knows how reconnaissance is performed*		3
		The candidate is able to:		
		2.2.1	*Demonstrate how manual port scanning and automated port scanning works*	3
		2.2.2	*Explain how to read and interpret scan results*	2
		2.2.3	*Describe how to find services using service identification and fingerprinting techniques*	2
Exam topics and terms			*Reconnaissance, port scanning, Nmap, netcat, FTP, SSH, HTTP, encrypted services.*	

Requirements, specifications, testing levels					Bloom level
3.	**Infrastructure security**				
	3.1	*The candidate can explain how infrastructure security works*			3
		The candidate is able to:			
		3.1.1	*Explain the basic concepts of networking*		2
		3.1.2	*Explain how basic network protocols work*		2
		3.1.3	*Use tools to compromise networking connections*		3
Exam topics and terms			*TCP/IP, IPv4, IPv6, handshake, UDP, Authoritative nameservers, caching, rootservers, DNS, DNS, ARP Spoofing / Cache poisoning attack, DNSSEC, DHCP, ARP.*		
	3.2		*The candidate knows how Wi-Fi networks can be compromised*		3
			The candidate is able to:		
			3.2.1	*Explain how wireless network protocols work and how they can be cracked*	
			3.2.2	*Explain the importance of network mapping*	2
			3.2.3	*Use port scanning techniques*	3
Exam topics and terms			*Wi-Fi, WPA, WEP, Wi-Fi process, monitor mode, de-authentication, network mapping, evil access point, nmap scanning.*		
	3.3		*The candidate can scan for vulnerabilities*		3
			The candidate is able to:		
			3.3.1	*Describe different types of vulnerability scans*	2
			3.3.2	*Interpret scanner results*	3
Exam topics and terms			*Vulnerabilities, infrastructure scan, web scan, Metasploit, NMAP.*		
	3.4		*The candidate can explain the concepts of secure networking*		2
			The candidate is able to:		
			3.4.1	*Describe a secure networking architecture and its building blocks*	**2**
			3.4.2	*Explain the concept of virtual private networking (VPN)*	**2**
Exam topics and terms			*Secure networking, IPSec, OPEN VPN.*		
	3.5		*The candidate knows how cryptography works*		3
			The candidate is able to:		
			3.5.1	*Explain Basic cryptography*	2
			3.5.2	*Describe the concept of Public Key Infrastructure (PKI)*	2
			3.5.3	*Explain how Hashing works*	2
			3.5.4	*Apply cracking techniques*	3
Exam topics and terms			*Cryptography, symmetric, asymmetric, algorithms, strong keys, SSL/TLS, Uses of SSL (HTTPS, OpenVPN, Starttls), PKI, certificates, PGP, Hashing, SHA, MDH, LM hash, cracking techniques for hashes.*		

Requirements, specifications, testing levels				Bloom level
4.	**Web applications**			
	4.1	*The candidate understands how general HTTP methods are used, and how the infrastructure of web applications is constructed*		2
		The candidate is able to:		
		4.1.1	*Explain how HTTP methods work*	2
		4.1.2	*Describe the different HTTP headers*	2
		4.1.3	*Explain how the infrastructure of web applications is constructed*	2
Exam topics and terms			*HTTP, GET, POST, etc., Webapp infrastructure.*	
	4.2	*The candidate knows how to use testing guides and testing tools*		
		The candidate is able to:		
		4.2.1	*Apply testing techniques from a testing guide like OWASP*	3
		4.2.2	*Use Webapp testing tools*	3
Exam topics and terms		*OWASP, WEbapp testing tools, vulnerability testing, Cross-Site scripting*		
	4.3	*The candidate knows how 'Cross-Site scripting' vulnerabilities can be exploited and is able to attack different authentication methods*		3
		The candidate is able to:		
		4.3.1	*Explain how XSS attacks and Session Hijacking can be performed*	2
		4.3.2	*Apply attack techniques from the Browser Exploitation Framework (BeEF)*	3
		4.3.3	*Explain how different authentication methods work*	2
		4.3.4	*Apply attacking techniques to authentication methods*	3
Exam topics and terms			*XSS attacks, Session Hijacking, POC, Browser Exploitation Framework (BeEF), Authentication, HTTP auth, login forms, sessions, etc., authentication attacks.*	
	4.4	*The candidate knows how Man in the middle attacks are performed*		3
		The candidate is able to:		
		4.4.1	*Use Man in the middle proxies*	3
Exam topics and terms			*MITM proxies, vulnerability scanners (Burp Suite, OWASP Zap).*	
	4.5	*The candidate knows how to execute SQL injection attacks and upload a web shell*		3
		The candidate is able to:		
		4.5.1	*Explain how databases work, and how they are used*	2
		4.5.2	*Use SQL injections to attack databases*	3
		4.5.3	*Explain how a web shell be uploaded*	2
		4.5.4	*Explain how full access to a server can be gained using a web shell*	2
Exam topics and terms			*Database, SQL injection, SQLmap, Webshell.*	

Requirements, specifications, testing levels				Bloom level
5.	**Systems and applications**			
	5.1	*The candidate can use a penetration testing framework*		3
		The candidate is able to:		
		5.1.1	*Explain how to install, update, and start the Metasploit framework*	2
		5.1.2	*Describe how the different auxiliary modules of Metasploit work*	2
		5.1.3	*Use the different auxiliary modules of Metasploit*	3
Exam topics and terms			*Penetration testing framework (Metasploit), vulnerabilities.*	
	5.2	*The candidate understands how client-side attacks can be executed*		2
		The candidate is able to:		
		5.2.1	*Explain how Malicious file-type payloads are created*	2
		5.2.2	*Apply how a drive-by download exploit is created*	2
		5.2.3	*Explain the concepts of pivoting and lateral movement*	2
Exam topics and terms			*Client-side attacks (CSA), cross-site scripting (XSS), file format exploit, browser plugin.*	

Requirements, specifications, testing levels				Bloom level
6.	**Exploiting buffer overflows**			
	6.1	*The candidate knows how to exploit buffer overflows*		3
		The candidate is able to:		
		6.1.1	*Explain how a computer memory stack works*	2
		6.1.2	*Describe how buffer overflows can occur*	2
		6.1.3	*Explain the concept of fuzzing*	2
		6.1.4	*Apply techniques to develop a buffer overflow*	3
		6.1.5	*Describe the countermeasures against buffer overflows*	2
Exam topics and terms			*Exploit development: fuzzing, exploiting. Advanced buffer overflows, Payloads, Malicious executables, Privilege escalation, stack canaries, DEP, X-flags, address space layout randomisation (ASLR).*	

Literature

A	SECO-Institute course materials; Version: EN-2018-01A June 2018
Optional/ additional	
B	Weidman, G. (2014). Penetration testing -A Hands-On Introduction to Hacking; No Starch Press, US. ISBN: 9781593275648.

Exam-literature matrix

Exam requirement	Exam specification	Literature (A, B)	Chapter reference(s)
1	1.1	A	Module 1/section: Penetration testing
	1.2	A	Module 1/sections: • Laws concerning Cyberspace • Ethics
	1.3	A	Module 1/section: Reporting
2	2.1	A	Module 2/section: Intelligence gathering
	2.2	A	Module 2/section: Reconnaissance
3	3.1	A	Module 3/sections: • Networking Basics -TCP/IP • Networking Basics -Protocols
	3.2	A	Module 3/sections: • Wireless Networking (Wi-Fi) • Wireless Networking - Cracking a WPA-PSK Key • Port Scanning and Network Mapping
	3.3	A	Module 3/section: Vulnerability Scanning
	3.4	A	Module 3/section: Secure Networking
	3.5	A	Module 3/section: Cryptography
4	4.1	A	Module 4/section: Understanding HTTP
	4.2	A	Module 4/sections: • OWASP • Web Application Testing

Exam requirement	Exam specification	Literature (A, B)	Chapter reference(s)
	4.3	A	Module 4/section: • Cross-Site Scripting (XSS) • Authentication
	4.4	A	Module 4/section: HTTP MitM Proxies
	4.5	**A**	Module 4/section: SQL Injections
5	5.1	A	Module 5/section: Metasploit
	5.2	A	Module 5/section: Client-Side Attacks
6	6.1	A	Module 6/sections: • The Stack • Example Code Execution Flow • Stack Overflows • Fuzzing • Developing Buffer Overflows • Buffer Overflow Countermeasures

How to book your exam

All our exams are delivered through an online examination system called ProcterU. To enrol for an exam, go to: https://go.proctoru.com/ Make sure you are fully prepared. Use the ProctorU Preparation checklist to assess whether you are ready to take the exam.

If you are a new user, select Test Taker. Select "SECO-Institute" as the institution and fill in all the necessary information. See the instructions for more information. Once you have scheduled your exam, you will be asked to pay the exam fee. If you have an exam voucher, please fill in the access code.

Our online examination system allows you to book and take exams at your convenience. It is up to you to decide where and when you will be tested.

System requirements

To ensure the quality and security of the examination, you will have to meet specific requirements regarding your computer configuration, your exam environment and your behaviour during the exam. Click here to see the requirements.

The exam will be taken with special proctor software. To enable webcam and audio recording during the exam, you have to install software that monitors your activities.

Your exam will be recorded through your webcam and microphone. After you have completed the exam, the recordings will be checked by multiple proctors to see whether you comply with all the requirements.

Results

If no non-conformities are detected by the proctors, you will receive the final result by email one month after you complete the test. The email will also contain information on how to claim your certificate and digital badge as well as how to use your title.

Certification Title

Upon successful completion of an exam, candidates can claim their **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).

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.

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