Certifications Preparation Guide

CEH, CEH Practical, Security+, PenTest+, OSWP, OSCP, eJPT and eMAPT

By

Joas Antonio

Details

- This document was prepared to assist those who wish to obtain the certifications described in the title, I hope it will be useful!

- And count on me if you need help, my LinkedIn is this: https://www.linkedin.com/in/joas-antonio-dos-santos

CEH ANSI

Preparation

CEH - Details

- In 2003, CEH introduced the five phases of ethical hacking, the blueprint for approaching your target and succeeding at breaking in. We have continued to hone these 5 phases, updating and refining them to match the skillset ethical hackers need today:
- Reconnaissance
- Gaining Access
- Enumeration
- Maintaining Access
- Covering Your Tracks

CEH - Details

About The Exam

Number of Questions: 125

Test Duration: 4 Hours

Test Format: Multiple Choice

Test Delivery: ECC EXAM, VUE

Exam Prefix: 312-50 (ECC EXAM), 312-50 (VUE)

Passing Score:

In order to maintain the high integrity of our certification exams, EC-Council Exams are provided in multiple forms (I.e. different question banks). Each form is carefully analyzed through beta testing with an appropriate sample group under the purview of a committee of subject matter experts that ensure that each of our exams not only has academic rigor but also has real world applicability. We also have a process to determine the difficulty rating of each question. The individual rating then contributes to an overall cut score for each exam form. To ensure each form has equal assessment standards, cut scores are set on a “per exam form” basis. Depending on which exam form is challenged, cut scores can range from 60% to 85%.

CEH - Details

Course Outline

Module 01: Introduction to Ethical Hacking	Module 11: Session Hijacking
Module 02: Footprinting and Reconnaissance	Module 12: Evading IDS, Firewalls, and Honeypots
Module 03: Scanning Networks	Module 13: Hacking Web Servers
Module 04: Enumeration	Module 14: Hacking Web Applications
Module 05: Vulnerability Analysis	Module 15: SQL Injection
Module 06: System Hacking	Module 16: Hacking Wireless Networks
Module 07: Malware Threats	Module 17: Hacking Mobile Platforms
Module 08: Sniffing	Module 18: IoT Hacking
Module 09: Social Engineering	Module 19: Cloud Computing
Module 10: Denial-of-Service	Module 20: Cryptography

CEH - Details

Training Options

iLearn (Self-Study)

This solution is an asynchronous, self-study environment which delivers EC-Council's sought-after IT Security hacking training courses in a streaming video format.

iWeek (Live Online)

This solution is a live, online, instructor-led training course that you can attend with a live instructor from anywhere with an internet connection.

Master Class

This solution offers you the opportunity to learn from world-class instructors and the opportunity to collaborate with top Infosecurity professionals. MasterClass classes come with a slew of additional benefits including add-on certification training, local meet-up opportunities, and iLearn access.

Training Partner (In Person)

This solution offers in-person CEH training so that you can get the benefit of collaborating with your peers and gaining real-world skills, conveniently located at one of the hundreds of training centers authorized to teach EC-Council courses around the world.

Education Partner (In Person or Online)

This solution offers education courses through EC-Council Academia partnered institutions to benefit students enrolled in a college or university degree programs.

CEH – Preparation Tips and Tricks

1. You can choose to buy the course material or even take the course at an accredited ATC, this helps a lot;

2. You can study alone, searching for content on the internet and using ebooks and discussion centers like Reddit;

3. The simulations are very fundamental to assist in your study, I recommend going after some VCE Exam Simulator, to assist in your journey;

4. Consult professionals who have already taken the certification and ask what usually falls the most;

5. Take a look at the Blueprint of the test and see what has more weight in the answers;

6. Study attack vector concepts, for example: If you are studying SQL Injection, memorize the types of SQL Injection that exist as well;

CEH – Materials

https://www.eccouncil.org/wp-content/uploads/2021/01/CEH-Exam-Blueprint-v4.0.pdf

https://github.com/Samsar4/CEH-v10-Study-Guide

https://www.amazon.com.br/Certified-Ethical-Hacker-Study-Guide/dp/1119800285

https://www.reddit.com/r/CEH/

https://github.com/priyankgada/The-Complete-Practical-Certified-Ethical-Hacking-Course-in-Hindi

https://www.youtube.com/watch?v=27i_husVE1I&ab_channel=AllAboutTech

https://www.youtube.com/watch?v=PhVTVXqrW2s&ab_channel=NetworkChuck

CEH – Simulations

http://www.gocertify.com/quizzes/ceh/ceh1.html

https://exam.proveyourself.net/

http://www.mindcert.com/resources/

https://ceh.cagy.org/?fbclid=IwAR3x6Ox88PfQS9PEnQeXfMyz7peSUhtTl56ehJ2zRfDqqu30lhRgam-bGVY

CEH PRACTICAL

Preparation

CEH Practical – Details

The World's First Ethical Hacking Industry Readiness Assessment That Is 100% Verified, Online, Live, Proctored!

CEH (Practical) Credential Holders Are Proven To Be Able To:

- Demonstrate the understanding of attack vectors
- Perform network scanning to identify live and vulnerable machines in a network.
- Perform OS banner grabbing, service, and user enumeration.
- Perform system hacking, steganography, steganalysis attacks, and cover tracks.
- Identify and use viruses, computer worms, and malware to exploit systems.
- Perform packet sniffing.
- Conduct a variety of web server and web application attacks including directory traversal, parameter tampering, XSS, etc.
- Perform SQL injection attacks.
- Perform different types of cryptography attacks.
- Perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems etc.

CEH Practical – Details

What is C|EH (Practical)?

C|EH Practical is a six-hour, rigorous exam that requires you to demonstrate the application of ethical hacking techniques such as threat vector identification, network scanning, OS detection, vulnerability analysis, system hacking, web app hacking, etc. to solve a security audit challenge.

This is the next step after you have attained the highly acclaimed Certified Ethical Hacker certification.

Key Outcomes

- Mastery of Ethical Hacking skills
- Demonstrate the application of the knowledge to find solutions to real-life challenges
- Commitment to code of ethics
- Validate essential skills required in the ethical hacking domains

Exam Information

- **Number of Practical Challenges:** 20
- **Duration:** 6 hours
- **Availability:** Aspen – iLabs
- **Test Format:** iLabs Cyber Range

C|EH (Practical) Certified Professional Can

- Demonstrate the understanding of attack vectors
- Perform network scanning to identify live and vulnerable machines in a network.
- Perform OS banner grabbing, service, and user enumeration.
- Perform system hacking, steganography, steganalysis attacks, and cover tracks.
- Identify and use viruses, computer worms, and malware to exploit systems.
- Perform packet sniffing.
- Conduct a variety of web server and web application attacks including directory traversal, parameter tampering, XSS, etc.
- Perform SQL injection attacks.
- Perform different types of cryptography attacks.
- Perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems etc.

CEH Practical – Preparation

1. CEH Practical complements CEH Ansi, if you can afford it, do it one after the other;

2. You can also buy iLabs which is great for you to study, as CEH Practical comes down to almost 90% of iLabs

3. Look for test discussion groups like Reddit

4. Practice a lot over the content that the proof delivers as key details

CEH Practical – Materials

https://github.com/CyberSecurityUP/Guide-CEH-Practical-Master

https://www.reddit.com/r/CEH/comments/b1wgbs/ceh_v10_practical/

https://www.linkedin.com/pulse/my-jouney-ceh-practical-joas-antonio-dos-santos/?trk=read_related_article-card_title

https://www.linkedin.com/pulse/ceh-practical-exam-review-ali-alenezi/

https://forums.itpro.tv/topic/2604/ceh-practical/2

https://www.linkedin.com/pulse/considera%C3%A7%C3%B5es-sobre-o-exame-ceh-practical-leandro-cortiz/

https://infayer.com/archivos/65

https://medium.com/@jonaldallan/passed-ec-councils-certified-ethical-hacker-practical-20634b6f0f2

https://www.reddit.com/r/CEH/comments/c69fou/passed_ceh_practicalpost_exam_writeup/

https://www.reddit.com/r/CEH/comments/eeu3cx/ceh_practical_handson_exam_passed_with_2020_score/

https://www.reddit.com/r/CEH/comments/8wk2ve/ceh_vs_ceh_practical/

https://www.reddit.com/r/CEH/comments/dfa1y8/passed_ceh_practical/

CEH Practical – Materials

https://sysaptechnologies.com/certified-ethical-hacker-ceh-v10-practical/

https://jensoroger.wordpress.com/2019/02/09/oscp-ceh-practical/

https://khroot.com/2020/06/20/certified-ethical-hacker-practical-review/

https://github.com/Samsar4/Ethical-Hacking-Labs

https://www.reddit.com/r/CEH/comments/jg0y6u/ceh_practical/

https://www.reddit.com/r/CEH/comments/dfa1y8/passed_ceh_practical/

https://www.reddit.com/r/CEH/comments/cgualo/ceh_practical_tell_me_about_it/

https://www.reddit.com/r/CEH/comments/c69fou/passed_ceh_practicalpost_exam_writeup/

CEH Practical – Materials

https://www.reddit.com/r/CEH/comments/b1wgbs/ceh_v10_practical/
https://www.youtube.com/watch?v=ZYEo2AQdgcg
https://www.youtube.com/watch?v=MEYjyr65bJE
https://www.reddit.com/r/CEH/comments/ek0gzp/ceh_practical_passed_2020/
https://www.reddit.com/r/CEH/comments/evuztj/ceh_practical/
https://www.reddit.com/r/CEH/comments/f6t80r/can_ceh_practical_be_regarded_as_a/
https://www.reddit.com/r/CEH/comments/g6z6vn/just_passed_ceh_practical_1920/
https://medium.com/@jonathanchelmus/c-eh-practical-exam-review-42755546c82e
https://www.reddit.com/r/CEH/comments/hk6880/passing_ceh_practical/
https://www.reddit.com/r/CEH/comments/f629zk/ceh_practical_vs_ejpt_vs_ecppt/
https://www.youtube.com/watch?v=o1u69KvSFmQ&list=PLmQBbrHGk7jQbsvF3_xJp720yaUgeYCkj
https://www.youtube.com/watch?v=oYgtePf0z44

CEH Practical – Materials

https://www.youtube.com/watch?v=9g5gdhoDotg&list=PLWGnVet-gN_kGHSHbWbeI0gtfYx3PnDZO

https://www.youtube.com/watch?v=LHU0OFcWSBk

https://medium.com/@mruur/ceh-practical-exam-review-918e76f831ff

https://www.youtube.com/c/XanderBilla/videos

https://www.youtube.com/watch?v=YZf5xmeaU58

https://newhorizons.com.sg/ceh-master/

https://www.iitlearning.com/certified-ethical-hacker-practical.php

https://medium.com/@anontuttuvenus/ceh-practical-exam-review-185ea4cef82a

https://www.cyberprotex.com/ceh.html

https://www.infosec4tc.com/product/ceh-master-exam1-exam2-practical/

https://www.mindmeister.com/pt/1758854211/ejpt-and-ceh-practical-guide-by-joas

Security+

Preparation

Security+ – Details

Why is it different?

- **More choose Security+** - chosen by more corporations and defense organizations than any other certification on the market to validate baseline security skills and for fulfilling the DoD 8570 compliance.
- **Security+ proves hands-on skills** – the only baseline cybersecurity certification emphasizing hands-on practical skills, ensuring the security professional is better prepared to problem solve a wider variety of today's complex issues.
- **More job roles turn to Security+ to supplement skills** – baseline cybersecurity skills are applicable across more of today's job roles to secure systems, software and hardware.
- **Security+ is aligned to the latest trends and techniques** – covering the most core technical skills in risk assessment and management, incident response, forensics, enterprise networks, hybrid/cloud operations, and security controls, ensuring high-performance on the job.

Security+ – Details

About the exam

CompTIA Security+ (SY0-501) English language exam will retire on July 31, 2021.
The new Security+ (SY0-601) is now available.

CompTIA Security+ is the first security certification a candidate should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Security+ incorporates best practices in hands-on troubleshooting, ensuring candidates have practical security problem-solving skills required to:

- **Assess** the security posture of an enterprise environment and recommend and implement appropriate security solutions
- **Monitor and secure** hybrid environments, including cloud, mobile, and IoT
- **Operate** with an awareness of applicable laws and policies, including principles of governance, risk, and compliance
- **Identify, analyze, and respond** to security events and incidents

Security+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements. Regulators and government rely on ANSI accreditation, because it provides confidence and trust in the outputs of an accredited program. Over 2.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.

Security+ – Details

What Skills Will You Learn?

Attacks, Threats and Vulnerabilities

Focusing on more threats, attacks, and vulnerabilities on the Internet from newer custom devices that must be mitigated, such as IoT and embedded devices, newer DDoS attacks, and social engineering attacks based on current events.

Architecture and Design

Includes coverage of enterprise environments and reliance on the cloud, which is growing quickly as organizations transition to hybrid networks.

Implementation

Expanded to focus on administering identity, access management, PKI, basic cryptography, wireless, and end-to-end security.

Operations and Incident Response

Covering organizational security assessment and incident response procedures, such as basic threat detection, risk mitigation techniques, security controls, and basic digital forensics.

Governance, Risk and Compliance

Expanded to support organizational risk management and compliance to regulations, such as PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST, and CCPA.

Security+ – Details

What Skills Will You Learn?

Attacks, Threats and Vulnerabilities

Focusing on more threats, attacks, and vulnerabilities on the Internet from newer custom devices that must be mitigated, such as IoT and embedded devices, newer DDoS attacks, and social engineering attacks based on current events.

Architecture and Design

Includes coverage of enterprise environments and reliance on the cloud, which is growing quickly as organizations transition to hybrid networks.

Implementation

Expanded to focus on administering identity, access management, PKI, basic cryptography, wireless, and end-to-end security.

Operations and Incident Response

Covering organizational security assessment and incident response procedures, such as basic threat detection, risk mitigation techniques, security controls, and basic digital forensics.

Governance, Risk and Compliance

Expanded to support organizational risk management and compliance to regulations, such as PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST, and CCPA.

Security+ – Simulations

https://www.examcompass.com/

http://examsforall.com/exams/comptia/

https://www.examcollection.com/

https://www.udemy.com/course/comptia-security-cert-sy0-501-practice-tests/

https://www.udemy.com/course/comptia-security-practice-exams/

https://www.udemy.com/course/security_plus_practice_exams/

Security+ – Materials

https://www.amazon.com/CompTIA-Security-Get-Certified-Ahead-ebook/dp/B09237T9ZB/ref=sr_1_11?dchild=1&keywords=comptia+security%2B+601&qid=1618858578&sr=8-11

https://www.amazon.com/CompTIA-Security-Get-Certified-Ahead/dp/1939136059/ref=sr_1_1?dchild=1&keywords=sec%2B+get+ahead&qid=1596499105&sr=8-1

https://www.amazon.com.br/CompTIA-Security-Study-Guide-SY0-601/dp/1119736250/ref=sr_1_1?__mk_pt_BR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&dchild=1&keywords=security%2B&qid=1619627370&sr=8-1

https://www.amazon.com.br/Simulados-Certifica%C3%A7%C3%A3o-CompTIA-Security-SY0-501-ebook/dp/B07FKS8HKY/ref=sr_1_4?__mk_pt_BR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&dchild=1&keywords=security%2B&qid=1619627370&sr=8-4

Security+ – Materials

https://www.amazon.com/CompTIA-Security-Get-Certified-Ahead-ebook/dp/B09237T9ZB/ref=sr_1_11?dchild=1&keywords=comptia+security%2B+601&qid=1618858578&sr=8-11

https://www.amazon.com/CompTIA-Security-Get-Certified-Ahead/dp/1939136059/ref=sr_1_1?dchild=1&keywords=sec%2B+get+ahead&qid=1596499105&sr=8-1

https://www.amazon.com.br/CompTIA-Security-Study-Guide-SY0-601/dp/1119736250/ref=sr_1_1?__mk_pt_BR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&dchild=1&keywords=security%2B&qid=1619627370&sr=8-1

https://www.amazon.com.br/Simulados-Certifica%C3%A7%C3%A3o-CompTIA-Security-SY0-501-ebook/dp/B07FKS8HKY/ref=sr_1_4?__mk_pt_BR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&dchild=1&keywords=security%2B&qid=1619627370&sr=8-4

Security+ – Materials

https://github.com/PacktPublishing/CompTIA-Security-SY0-501-Complete-Course-and-Practice-Exam

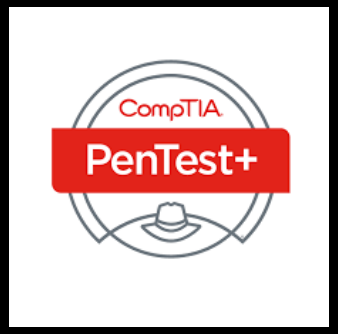
https://github.com/aaronshaf/security-plus

https://github.com/Samsar4/CompTIA-Security-SY0-501-Study-Guide

https://github.com/PacktPublishing/CompTIA-Security-SY0-501-Complete-Course-and-Practice-Exam/blob/master/CompTIA%20Security%2B%20(Study%20Notes).pdf

https://github.com/krovs/security-plus-notes

https://github.com/xChockax/CompTIA-Security-SY0-501-Certification



Pentest+

Preparation

PenTest+ – Details

Firstly, it is necessary to acquire a focus to study for certification, especially if you want to do well and take full advantage of the content. So techniques like pomodoro and learning pyramid are very good, I recommend on your journey to do this, it is valid for any certification.

- Leave the phone aside to study;
- Focus on only one module at a time;
- Make manual notes or even drawings and sketches;
- Look for practical issues that help you develop further;
- And when in doubt, review the material or look for other sources of knowledge to have a full understanding of what you are studying;

PenTest+ – Materials

In addition to the books, you can use the Exam Guide to consult what falls on the test and study through materials also available on the internet Search for pentest + exam guide filetype: pdf

https://github.com/dustypioneer/pentest_plus

https://github.com/pentestplus

https://github.com/PacktPublishing/CompTIA-Pentest-Ethical-Hacking-Course-and-Practice-Exam

https://github.com/xChockax/CompTIA-Pentest-PT0-001

https://github.com/PacktPublishing/CompTIA-PenTest-Exam-Guide-PT0-001

https://github.com/PacktPublishing/-Ethical-Hacking-and-CompTIA-PenTest-Exam-Prep-PT0-001-

https://pentestplus.github.io/

https://github.com/artiommocrenco/comptia-pentest-notes

PenTest+ – Tips

- Study a lot of attack vectors in web applications, because there are many questions related to techniques and even remedies, involving the web application security part, for example: How to prevent an SQL Injection or LFI?
- In addition, knowing about PenTest frameworks and methodologies is essential, as it involves issues involving a pentest cycle of such methodology;
- Knowing about nmap is fundamental too, there are a lot of questions about the tool and exploring all its syntaxes, at least knowing what each one is for is enough;
- Understanding of vectors of attacks aimed at Social Engineering, as you will come across many issues that bring scenarios and situations;
- Knowing a little about the fundamentals involving application security and hardening, is also interesting, since there are issues that you may need to mitigate or perform some hardening or even code review;
- Knowing the main tools used in the market is fundamental;
- Know the techniques involved in each PenTest cycle, from the collection of information to the report;
- There will be a lot of questions that can question what actions you should take, when you encounter any non-compliance and etc; I
- recommend writing down concepts, nomenclatures and jargon that falls a lot on the test, for example: SOW, NDA and etc ...

PenTest+ – Tips

PROOF OF PROCEDURE FOR TESTING

- If the test does not have a native language, you will probably have an American proctor to supervis
- System test on the computer and the network you plan to take the exam on;
- Necessary identification (issued by the government);
- Sign an NDA (non-disclosure agreement) before the
- test; Lock browser enabled;
- Introduce your entire work environment to the inspector before the test;
- Requires a webcam (the video is recorded and the inspector is watching
- you); No disturbing noises;
- No breaks to go to the bathroom;
- No food (only drinks allowed are water in a clear glass);
- You are not allowed to leave your seat at ANY TIME during the exam;

PenTest+ – Simulated

SIMULATED

- https://issuu.com/freedumpsquestions2019/docs/comptia_pentest__pt0-001_free_dumps_questions_v9.0
- https://www.youtube.com/watch?v=s6yehzNuD5M&ab_channel=PacktVideo
- https://www.edusum.com/category/pentest-plus-simulator
- https://www.mindomo.com/en/outline/how-are-you-able-to-clear-pt0-001-exam-with-pt0-001-test-simulator-andexam-dumps
- https://www.udemy.com/course/comptia-pentest-pt0-001-practice-tests-4-exams/
- https://www.udemy.com/course/ethical-hacking-and-comptia-pentest- exam-prep-en0-001 /
- https://www.udemy.com/course/practice-comptia-pentest-exam-340-questions-pt0-001/
- These are some simulations that can help, but it does not mean that the questions presented will fall on the test

PenTest+ – Laboratories

LABORATORIES

- https://tryhackme.com/path/outline/pentestplus
- https://www.cybrary.it/catalog/practice_labs/comptia-pentest-plus/
- https://www.reddit.com/r/CompTIA/comments/eehi5y/pentest_labs/
- https://www.hackthebox.eu/
- http://vulnhub.com/

PenTest+ – Laboratories

TEST REVIEWS

- https://medium.com/@kcco.io/comptia-pentest-certification-exam-review-1a0a02883650
- https://www.tevora.com/comptia-pentest-certification-review/
- https://www.reddit.com/r/CompTIA/comments/8er30w/i_took_pentest_today_and_even_as_a_pentester_that/
- https://resources.infosecinstitute.com/topic/pentest-plus-vs-ceh/
- https://www.youtube.com/watch?v=l12oxXncQCE&ab_channel=ITCareerQuestions
- https://www.youtube.com/watch?v=nUXL39z91k4&ab_channel=Infosec
- https://medium.com/@h4unt3r/comptia-pentest-certification -review-4ce42871e39b
- https://blog.wyatttauber.com/how-i-passed-comptia-pentest-pt0-001-75471e505abd
- https://www.linkedin.com/pulse/my-comptia-pentest-study-guide-kelshallwilliams/?articleId=6652888150140088322

OSWP

Preparation

OSWP – Details

- Wireless Attacks (PEN-210) introduces students to the skills needed to audit and secure wireless devices. It's a foundational course alongside PEN-200 and would benefit those who would like to gain more skill in network security.
- In PEN-210, students will learn to identify vulnerabilities in 802.11 networks and execute organized attacks. Each student will set up a home lab to practice the techniques learned in this online, self-paced course.
- Successful completion of the course and exam confers the Offen

OSWP – Details

COURSE INFO

BENEFITS

- Be able to identify existing encryptions and vulnerabilities in 802.11 networks
- circumvent network security restrictions and recover the encryption keys in use

ABOUT THE EXAM

- The PEN-210 course and online lab prepares you for the OSWP certification
- 4-hour exam
- Learn more about the exam

WHO IS THE COURSE FOR?

This course is designed for information security professionals who want to learn wireless penetration testing. This includes:

- Security professionals and enthusiasts
- Network administrators

COURSE PREREQUISITES

All students are required to have:

- Solid understanding of TCP/IP and the OSI model as well as familiarity with Linux.
- A modern laptop or desktop that can boot and run BackTrack
- Specific Hardware is required to complete course exercises

OSWP – Details

COURSE INFO

BENEFITS

- Be able to identify existing encryptions and vulnerabilities in 802.11 networks
- circumvent network security restrictions and recover the encryption keys in use

ABOUT THE EXAM

- The PEN-210 course and online lab prepares you for the OSWP certification
- 4-hour exam
- Learn more about the exam

WHO IS THE COURSE FOR?

This course is designed for information security professionals who want to learn wireless penetration testing. This includes:

- Security professionals and enthusiasts
- Network administrators

COURSE PREREQUISITES

All students are required to have:

- Solid understanding of TCP/IP and the OSI model as well as familiarity with Linux.
- A modern laptop or desktop that can boot and run BackTrack
- Specific Hardware is required to complete course exercises

OSWP – Details Concepts

- IEEE 802.11
- Wireless Networks
- Packets and Network Interaction
- Linux Wireless Stack and Drivers
- Aircrack-ng Essentials
- Cracking WEP with Connected Clients
- Cracking WEP via a Client
- Cracking Clientless WEP Networks
- Bypassing WEP Shared Key Authentication
- Cracking WPA/WPA2 PSK with Aircrack-ng
- Cracking WPA with JTR and Aircrack-ng
- Cracking WPA with coWPAtty
- Cracking WPA with Pyrit
- Additional Aircrack-ng Tools
- Wireless Reconnaissance
- Rogue Access Points

OSWP – Reviews

https://www.offensive-security.com/offsec/oscp-osce-oswp-review/

https://www.linkedin.com/pulse/my-journey-oswp-joas-antonio-dos-santos/?trackingId=%2BszI2BPfT465vft5fY%2FsNA%3D%3D

https://nethemba.com/offensive-security-wireless-professional-oswp-review/

https://medium.com/@obikag/my-wifu-journey-oswp-certification-review-a1784730449c

https://www.triaxiomsecurity.com/oswp-course-review/

https://charonv.com/OSCP-OSWP-review/

https://tulpa-security.com/2016/12/10/review-oswp-offensive-security-wireless-professional/

https://ryandinho.me/2019/05/26/wifu-and-oswp-certification-review.html

OSWP – Network Device

- **Recommended Wireless Network Routers**
  - D-Link DIR-601
  - Netgear WNR1000v2
- **Recommended Wireless Cards**
  - Netgear WN111v2 USB
  - ALFA Networks AWUS036H USB 500mW
  - Tplink wn722n

  https://www.kabum.com.br/produto/12114/adaptador-wireless-tp-link-usb-150mbps-tl-wn722n?gclid=CjwKCAjwkN6EBhBNEiwADVfya-BnFi4QPDDNcnBTqpL7DWBXs85kvFf-QHpbTrogXGWk3dtCrFEDJRoCg6QQAvD_BwE

  https://www.alfa.com.tw/

OSWP – Tips and Tricks

- I recommend attending classes and reading the wireless attack material, all without exception.
- The test is random, it may drop 2 WPA and 1 WEP, be it with or without a client and so on.
- Another detail, try and do not give up, you can use other techniques within the scope, but do not think about using wifite, as you will be disqualified, but try other syntaxes of the Aircrack tools.
- And finally, be patient, I recommend you to take a print of the screens and after the end of the first challenge, write the report. But it is up to each person, this is my recommendation.

OSWP – Materials

https://drive.google.com/file/d/1oFFlw9d1l9PJ6BVUnMn1ZWnB5e3mNefg/view?usp=sharing

https://github.com/vdb-sander/OSWP

https://github.com/gh0x0st/OSWP-Expanding-Your-Reach

https://github.com/ckt29175/OSWP

https://github.com/wwong99/oswp/blob/master/summaryattacks

https://github.com/wwong99/oswp/blob/master/aircrack-ng%20Commands

OSCP

Preparation

OSCP – Details

Penetration Testing with Kali Linux (PEN-200) is the foundational course at Offensive Security. Those new to OffSec or penetration testing should start here.

This online ethical hacking course is self-paced. It introduces penetration testing tools and techniques via hands-on experience. PEN-200 trains not only the skills, but also the mindset required to be a successful penetration tester.

Students who complete the course and pass the exam earn the coveted Offensive Security Certified Professional (OSCP) certification.

OSCP – Details

BENEFITS

- Introduction into the latest hacking tools and techniques
- Training from the experts behind Kali Linux
- Learn the “Try Harder” method and mindset
- Earn the industry-leading OSCP certification

ABOUT THE EXAM

- The PEN-200 course and online lab prepares you for the OSCP certification
- 24-hour exam
- Proctored
- Learn more about the exam

WHO IS THE COURSE FOR?

- Infosec professionals transitioning into penetration testing
- Pentesters seeking an industry-leading certification
- Security professionals
- Network administrators
- Other technology professionals

COURSE PREREQUISITES

All students are required to have:

- Solid understanding of TCP/IP networking
- Reasonable Windows and Linux administration experience
- Familiarity with basic Bash and/or Python scripting

OSCP – Details

COURSE SYLLABUS

PEN-200 is a unique course that combines traditional course materials with hands-on simulations, using a virtual lab environment. The course covers the following topics. View the full syllabus.

- Penetration Testing: What You Should Know
- Getting Comfortable with Kali Linux
- Command Line Fun
- Practical Tools
- Bash Scripting
- Passive Information Gathering
- Active Information Gathering
- Vulnerability Scanning
- Web Application Attacks
- Introduction to Buffer Overflows
- Windows Buffer Overflows
- Linux Buffer Overflows
- Client-Side Attacks
- Locating Public Exploits
- Fixing Exploits
- File Transfers
- Antivirus Evasion
- Privilege Escalation
- Password Attacks
- Port Redirection and Tunneling
- Active Directory Attacks
- The Metasploit Framework

WHAT COMPETENCIES WILL YOU GAIN?

- Using information gathering techniques to identify and enumerate targets running various operating systems and services
- Writing basic scripts and tools to aid in the penetration testing process
- Analyzing, correcting, modifying, cross-compiling, and porting public exploit code
- Conducting remote, local privilege escalation, and client-side attacks
- Identifying and exploiting XSS, SQL injection, and file inclusion vulnerabilities in web applications
- Leveraging tunneling techniques to pivot between networks
- Creative problem solving and lateral thinking skills

SUPPORTING YOUR ONLINE JOURNEY

- 17+ hours of video
- 850-page PDF course guide
- Over 70 machines
- Active student forums
- Access to virtual lab environment

OSCP – Materials

https://www.offensive-security.com/offsec/my-philosophical-approach-to-oscp/

https://sock-raw.org/blog/oscp-review/

https://royaljay.com/security/how-i-became-an-offensive-security-certified-professional/

https://github.com/0x4D31/awesome-oscp

https://github.com/six2dez/OSCP-Human-Guide

https://github.com/cpardue/OSCP-PWK-Notes-Public

https://github.com/wwong99/pentest-notes/blob/master/oscp_resources/OSCP-Survival-Guide.md

OSCP – Materials

https://github.com/noraj/OSCP-Exam-Report-Template-Markdown

https://github.com/strongcourage/oscp

https://gist.github.com/natesubra/5117959c660296e12d3ac5df491da395

https://github.com/so87/OSCP-PwK

https://github.com/fr-ez/oscp-reference

https://github.com/strongcourage/oscp

https://gist.github.com/natesubra/5117959c660296e12d3ac5df491da395

https://github.com/whoisflynn/OSCP-Exam-Report-Template

OSCP – Materials

https://github.com/areyou1or0/OSCP

https://github.com/security-prince/PWK-OSCP-Preparation-Roadmap

https://github.com/so87/OSCP-PwK

https://github.com/xapax/oscp

https://github.com/JoaoPauloF/OSCP

https://drive.google.com/file/d/1A6-mOeX_JvLONgU0D_H6bnp9noE0VR_c/view?usp=sharing (OSCP SURVIVAL BOOK)

OSCP – Reviews

https://medium.com/cybersecpadawan/the-long-awaited-oscp-review-5a377f103a39

https://ranakhalil101.medium.com/my-oscp-journey-a-review-fa779b4339d9

https://bad-jubies.github.io/OSCP-Review/

https://www.reddit.com/r/oscp/comments/cwht67/another_oscp_exam_review/

https://hakin9.org/try-harder-my-penetration-testing-with-kali-linux-oscp-review-and-courselab-experience-my-oscp-review-by-jason-bernier/

https://steflan-security.com/my-oscp-journey/

https://buffered4ever.com/tag/oscp-review/

OSCP – Reviews

https://rana-khalil.gitbook.io/hack-the-box-oscp-preparation/

https://infosecwriteups.com/how-i-passed-oscp-with-100-points-in-12-hours-without-metasploit-in-my-first-attempt-dc8d03366f33

https://emaragkos.gr/oscp/tryhackme-oscp-preparation-path-review/

https://forum.hackthebox.eu/discussion/1655/oscp-exam-review-2019-notes-gift-inside

OSCP – Laboratories

https://www.mindmeister.com/pt/1781013629/the-best-labs-and-ctf-red-team-and-pentest

https://www.offensive-security.com/labs/

https://www.hackthebox.eu/

- OSCP LABS COURSE

https://tryhackme.com/

eJPT

Preparation

eJPT – Details

Overview

The eLearnSecurity Junior Penetration Tester (eJPT) is a 100% practical certification on penetration testing and information security essentials. By passing the exam, a cyber security professional proves to employers they are ready for a rewarding new career.

WHY eJPT?

Here are some of the ways eLearnSecurity Junior Penetration Tester certification is different from conventional certification:

- Instead of putting you through a series of multiple-choice questions, you are expected to perform an actual penetration test on a corporate network. This penetration test is modeled after a real-world scenario
- eJPT is the only practical certification that proves you have essential Penetration Testing skills

eJPT – Details

KNOWLEDGE DOMAINS

By obtaining the eJPT Gold, your skills in the following areas will be assessed and certified:

- TCP/IP
- IP routing
- LAN protocols and devices
- HTTP and web technologies
- Essential penetration testing processes and methodologies
- Basic vulnerability assessment of networks
- Basic vulnerability assessment of web applications
- Exploitation with Metasploit
- Simple web application manual exploitation
- Basic information gathering and reconnaissance
- Simple scanning and profiling the target

eJPT – Details

PREREQUISITES

The eJPT is a certification for advanced IT professionals who have just begun their journey in penetration testing. Everyone can attempt the certification exam, however here are the skills that will help you pass:

- Deep understanding of networking concepts
- Simple manual web application security assessment and exploitation
- Basic vulnerability assessment of networks
- Using Metasploit for performing simple attacks
- Web application manual exploitation through attack vectors
- Ability to perform protocol analysis of a traffic capture
- Understanding of information gathering techniques
- Understanding of the penetration testing process

eJPT – Details

eLearnSecurity's eJPT certifies that the candidate has all the prerequisites needed to enroll in INE's Penetration Testing Professional learning path.

The candidate will receive a real-world engagement within INE's Virtual Lab environment. You will need an Internet connection and VPN software in order to carry out this exam.

eJPT – Materials

https://github.com/d3m0n4l3x/eJPT

https://github.com/cocomelonc/ejpt

https://github.com/fdicarlo/eJPT

https://github.com/anontuttuvenus/eJPT

https://github.com/umkhan23/eJPT-Prep

https://github.com/hunterluker/eJPT-notes

https://github.com/tr0nucf/My-Tools/blob/master/eJPT%20Notes.txt

https://infosecwriteups.com/ultimate-guide-to-pass-ejpt-in-the-first-attempt-by-mayur-parmar-75effc877394

https://refabr1k.gitbook.io/oscp/elearnsecurity-ejpt/untitled

eJPT – Materials

https://kentosec.com/2019/08/04/how-to-pass-the-ejpt/

https://www.rehanbari.com/cyber-security/week-4-ejpt-review/

https://infosecwriteups.com/ultimate-guide-to-pass-ejpt-in-the-first-attempt-by-mayur-parmar-75effc877394

https://joasantonio108.medium.com/my-journey-to-pass-ejpt-elearnsecurity-7de5cd532dd9

https://www.mindmeister.com/pt/1758854211/ejpt-and-ceh-practical-guide-by-joas

eJPT – Reviews

https://forum.hackthebox.eu/discussion/4196/ejpt-review

https://www.youtube.com/watch?v=sXdPtEo8hk0&ab_channel=ITProTV

https://www.youtube.com/watch?v=vP5VaxrM_O0&ab_channel=JonGood

https://www.youtube.com/watch?v=E_xbHTPwhIQ&ab_channel=NetworkChuck

https://www.reddit.com/r/netsecstudents/comments/eux4fh/elearnsecurity_junior_penetration_tester_ejpt/

https://community.elearnsecurity.com/topic/7948-ejpt-earnedreviewtips/

https://kentosec.com/2019/08/04/elearnsecurity-junior-penetration-tester-ejpt-course-review/

https://jorenjacob.com/2019/05/27/ejpt-certificate-review/

eJPT – Laboratories

- Practice a lot in laboratories like Hack The Box and Try Hack Me, which will be very easy for you to pass the test.
- Mainly because she has questions that you answer by doing a pentest, which is actually more enumeration than intrusion

eMAPT

Preparation

eMAPT – Details

Overview

The eLearnSecurity Mobile Application Penetration Tester (eMAPT) certification is issued to cyber security experts that display advanced mobile application security knowledge through a scenario-based exam.

WHY eMAPT?

Here are some ways the eLearnSecurity Mobile Application Penetration Tester certification is different from conventional certifications:

- Ensures that you have a strong understanding of theoretical aspects behind mobile application security.
- Tests a candidate's ability to identify and exploit vulnerable mobile applications through a 100% practical exam.
- Not only must you try different methodologies to conduct a thorough penetration test, you are also asked to write a complete working exploit.
- Only individuals who provide proof of their findings in addition to writing a working exploit are awarded the eMAPT Certification.

eMAPT – Details

KNOWLEDGE DOMAINS

By obtaining the eMAPT, your skills in the following areas will be assessed and certified:

- Information Gathering
- Reverse engineering Android applications
- Exploit Android vulnerabilities
- Applied security principles
- Logic flaws
- Exploit development for Android environments
- Encryption and cryptography
- Identify vulnerable implementations

eMAPT – Details

PREREQUISITES

eMAPT is a certification for individuals with a complex understanding of mobile application vulnerabilities and exploits. Everyone can attempt the certification exam; however, here are the advised skills to possess for a successful outcome:

- Letters of engagement and the basics related to a penetration testing engagement
- Android applications architecture, security mechanisms and components
- Vulnerability assessments of mobile applications
- Performing Android application reverse engineering and algorithm analysis
- Encryption/decryption algorithms
- Performing manual exploitation

eMAPT – Details

THE EXAM

eLearnSecurity's eMAPT is the only certification for mobile security experts that evaluates your practical abilities through a real world engagement.

eLearnSecurity's eMAPT is a hands-on challenge. Students will receive a real-world scenario of two Android applications to analyze and pentest. The final deliverable is a working and reproducible proof of concept that is reviewed by INE's course instructors.

eMAPT – Materials

https://rzepsky.medium.com/mobile-application-security-and-penetration-testing-maspt-course-elearnsecurity-mobile-ee61a7fe28d0

https://brcyrr.medium.com/recommendations-review-of-emapt-819e72a27f06

https://www.youtube.com/watch?v=e7PcuZOD8bs

https://community.elearnsecurity.com/topic/3885-emapt-passed/

https://medium.com/swlh/android-mobile-penetration-testing-lab-dfb8ceb4efbd

eMAPT – Materials and Labs

https://pentestlab.blog/category/mobile-pentesting/

https://infosecwriteups.com/android-pentesting-lab-4a6fe1a1d2e0

https://github.com/tanprathan/MobileApp-Pentest-Cheatsheet

https://appsec-labs.com/mobile_pentesting/

https://www.hackingarticles.in/android-pentest-lab-setup-adb-command-cheatsheet/

https://github.com/OWASP/owasp-mstg/blob/master/Document/0x04b-Mobile-App-Security-Testing.md

https://www.youtube.com/watch?v=dslIFMeIq4k&ab_channel=Hacoder

https://owasp.org/www-project-mobile-security-testing-guide/

https://github.com/OWASP/owasp-mstg

eMAPT – Tips and Tricks

I recommend getting to know a little about Mobile development, mainly in Java;

I recommend acquiring fundamental knowledge in architecture of Mobile Android and IOS applications;

And finally, mobile attack vectors;