CPENT - Certified Penetration Testing Professional

Kestus: 40 academic hours

Veebikoolitus

Vaata kõiki toimumiskuupäevi

EC-Council's Certified Penetration Tester (CPENT) program teaches you how to perform an effective penetration test in an enterprise network environment that must be attacked, exploited, evaded, and defended.

Years of research indicate that the majority of Pen Testing candidates have gaps in their skills when it comes to multiple disciplines. The metrics also prove when the targets are not located on the same or a directly connected and reachable segment, very few can perform as well as they do when it is direct and on a flat network.

If you have only been working in flat networks, **CPENT's live practice range will teach you** to take your skills to the next level by teaching you **how to pen test IoT systems, OT systems, how to write your own exploits, build your own tools, conduct advanced binaries exploitation, double pivot to access hidden networks, and also customize scripts/exploits to get into the innermost segments of the network.**

Target audience:

- Ethical Hackers
- Penetration Testers
- Network server administrators
- Firewall Administrators
- Security Testers
- Security Engineers
- System Administrators
- Security Analysts
- Risk Assessment professionals
- Information Security Consultants

As a result of the training participants will be able to:

- Accomplish Advanced Window Attacks
- Attack IoT Systems
- Write Exploits: Advanced Binaries Exploitation
- Bypass a Filtered Network
- Pentest Operational Technology (OT)
- Access Hidden Networks with Pivoting
- Accomplish Double Pivoting
- Perform Privilege Escalation
- Evade Defense Mechanisms
- Attack Automation with Scripts
- Build Your Armory: Weaponize Your Exploits
- Write Professional Reports

2 Certs, One Exam - CPENT & LPT Master

You have the potential to earn two certifications with one exam. If you score above 90% on the CPENT live range exam, not only will you earn the CPENT certification, but you will also earn the Licensed Penetration Tester (LPT) Master Credential!

Exam features:

- Choose your challenge! Either two 12-hour sessions or a single 24-hour exam!
- EC-Council specialists proctor the entire exam; cheating is not an option.
- Score at least 70% and become a CPENT.
- Score at least 90% and earn the highly regarded LPT (Master) designation!

Prerequisites to the course (recommended):

Extensive knowledge of penetration testing across multiple disciplines extending from windows, IoTs, inline defenses to automation, operational technology, and advanced skills in binary exploitation. The certification tests the knowledge of the tester not only on automated tools but manual testing skills as well.

- Advanced knowledge in Networking Protocols
- Knowledge in Kali or ParrotOS and common Penetration Testing Tools
- Knowledge in Exploiting Windows and Linux Hosts
- Knowledge in Privilege Escalation in Linux and Windows
- Knowledge in Wireless Penetration Testing

- Knowledge in Web Application Penetration Testing

Training Principles:

The CPENT range consists of entire network segments that replicate an enterprise network — this is not a computer game simulation; this is an accurate representation of an enterprise network that will present the latest challenges to the pen tester. The benefit of hands-on learning in a live cyber range is that candidates will encounter multiple layers of network segmentation, and the CPENT course will teach candidates how to navigate these layers so that once access is gained in one segment, a candidate will know the latest pivoting techniques required to reach the next. However, that won't be enough on its own as the targets and segments are progressive in nature, so once you get into one machine and or segment, the next one will challenge you even more.

The prerequisite for issuing the certificate is full participation in training.

Length: 40 academic hours

What Makes The Certified Penetration Testing Professional (CPENT) Unique?

Advanced Windows Attacks / Attacking IOT Systems/ Writing Exploits: Advanced Binary Exploitation/ Bypassing a Filtered Network/ Pentesting Operational Technology (OT)/ Access Hidden Networks with Pivoting/ Double Pivoting/ Privilege Escalation/ Evading Defense Mechanisms/ Attack Automation with Scripts/ Weaponize Your Exploits/ Write Professional Reports/

The training topics and description:

CPENT certification consists of 14 modules and tests the abilities of a penetration tester in almost all the vectors of cybersecurity, some of which have been introduced for the first time in any penetration certification.

Module 01: Introduction to Penetration Testing and Methodologies
Module 02: Penetration Testing Scoping and Engagement Methodology
Module 03: Open Source Intelligence (OSINT) Methodology
Module 04: Social Engineering Penetration Testing Methodology
Module 05: Network Penetration Testing Methodology –External
Module 06: Network Penetration Testing Methodology –Internal
Module 07: Network Penetration Testing Methodology -Perimeter Devices
Module 08: Web Application Penetration Testing Methodology
Module 09: Wireless Penetration Testing Methodology
Module 10: IoT Penetration Testing Methodology
Module 11: OT/SCADA Penetration Testing Methodology
Module 12: Cloud Penetration Testing Methodology
Module 13: Binary Analysis and Exploitation
Module 14: Report Writing and Post Testing Actions

Appendix A: Penetration Testing Essential Concepts
Appendix B: Fuzzing
Appendix C: Mastering Metasploit Framework
Appendix D: PowerShell Scripting
Appendix E: Bash Environment and Scripting
Appendix F: Python Environment and Scripting
Appendix G: Perl Environment and Scripting
Appendix H: Ruby Environment and Scripting
Appendix I: Active Directory Pen Testing
Appendix J: Database Penetration Testing Methodology
Appendix K: Mobile Device Penetration Testing Methodology

The training price also includes:

study materials;
a trainer's consultation on the topics learned by e-mail after the training;
exam voucher;
certificate.

You can participate in the training with the Unemployment Insurance Fund training card.

See you at the training!

LISAINFO

Osalemise tingimused
Registreerudes e-poe, e-kirja või telefoni teel, saadame Teile arve ja täpsema info osalemise kohta.
Üksteist päeva enne koolitust saadame Teile e-kirjaga meenutuse osalemise infoga.

Koolitusel osalemine on nimeline, kuid saate osalejat tasuta muuta kuni koolituse alguseni.

Koolituse eest tasumine toimub arvel viidatud arveldusarvele. Arve saadetakse maksja aadressile e-postiga. Arve tuleb tasuda enne koolituse algust arvel märgitud maksetähtajaks.

Kui Te ei saa mingil põhjusel osaleda, palun andke sellest kindlasti teada e-posti aadressil info@koolitus.ee või telefonil 618 1727 . Kui teatate koolitusel mitteosalemisest kuni 10 tööpäeva enne algust, pakume mõnd muud samaväärset koolitust või tagastame 100% tasutud koolituse maksumusest. Mitteosalemisest vähemalt 5 tööpäeva varem teatades, tagastame 50%. Muul juhul kuulub arve tasumisele. Raha tagastame ette antud summas juhul, kui pole tehtud koolituse korraldamisega seotud kulutusi (ostetud õppematerjale jms). Koolitusele mitteilmumisel, sellest mitteteatamisel või koolituse poolelijätmisel õppetasu ei tagastata.

IT Koolitusel on õigus koolitusgrupi mitte täitumisel koolituse toimumine edasi lükata või koolitus ära jätta. Koolitusele registreerunuid teavitatakse kursuse edasi lükkumisest või ära jätmisest telefoni või e-posti teel. Koolituse ära jäämisel korraldajatest tulenevatel põhjustel makstakse õppetasu tagasi. .

IT Koolitus on Eesti Töötukassa koolituskaardi koostööpartner. Tutvuge koolituskaardi infoga SIIN.
Täpsema info saamiseks võtke meiega ühendust telefonil 618 1727 või info@koolitus.ee.