NDE - Network Defence Essentials

Kestus: 19 academic hours

E-õpe

Vaata kõiki toimumiskuupäevi

EC-Council's Essentials Series is the first MOOC certification course series covering essential skills in network defense, ethical hacking, and digital forensics.

The Essentials Series' Massive Open Online Courses (MOOCs) contain eCourseware and video instruction, which is being offered free, with optional paid upgrades to course labs, exam prep, course assessments, and exam vouchers leading to certifications across each of the three Essentials Series courses.

Who Should Attend These Courses?

EC-Council's Essentials Series programs and certifications build and validate candidates' skills for their cybersecurity future. It is ideal for IT professionals who are seeking to foray into the exciting world of cybersecurity. Cybersecurity enthusiasts and students will readily find the program interesting, challenging, and useful.

Designed by the Experts

The Essentials Series was designed by industry experts to provide an unbiased approach to learning and exploring industry best practices. It empowers individuals to:
Gain foundational knowledge in cybersecurity
Practice essentials skills such as how to defend networks and investigate them
Challenge industry recognized exams and earn cybersecurity credentials to build and further your career

Network Defense Essentials is a first-of-its-kind MOOC certification that provides foundational knowledge and skills in network security with add-on labs for handson experience. The course includes 12 modules and optional upgrades to lab ranges covering fundamental network security concepts, including IoT, cryptography, and PKI

Modules: What You Will Learn

01 Network Security Fundamentals

- Fundamentals of Network Security
- Network security protocols that govern the flow of data

02 Identification, Authentication, and Authorization

- Access control principles, terminologies, and models
- Identity and access management (IAM)

03 Network Security Controls: Administrative Controls

- Regulatory frameworks, laws, and acts
- Security policies, and how to conduct security and awareness training

04 Network Security Controls: Physical Controls

- Importance of physical security and physical security controls
- Physical security policies and procedures
- Best practices to strengthen workplace security
- Environmental controls

05 Network Security Controls: Technical Controls

- Types of bastion hosts and their role in network security
- IDS/IPS types and their role in network defense
- Types of honeypots and virtual private networks (VPNs)
- Security incident and event management (SIEM)

06 Virtualization and Cloud Computing

- Key concepts of virtualization and OS virtualization security
- Cloud computing fundamentals and cloud deployment models
- Cloud security best practices

07 Wireless Network Security

- Fundamentals of wireless networks and encryption mechanisms
- Wireless network authentication methods
- Implementing wireless network security measures

08 Mobile Device Security

- Mobile device connection methods and management
- Mobile use approaches in enterprises
- Security risks and guidelines associated with enterprise mobiile usage policies
- Implement various enterprise-level mobile security management solutions
- Best practices on mobile platforms

09 IoT Device Security

- IoT devices, application areas, and communication models
- How security works in IoT-enabled environments

10 Cryptography and PKI

- Cryptographic tools, security techniques, and algorithms
- Public key infrastructure (PKI) to authenticate users and devices in the digital world

11 Data Security

- Data security and its importance
- Security controls for data encryption
- Perform data backup and retention
- Implement data loss prevention concepts

12 Network Traffic Monitoring

- Network traffic monitoring concepts
- Traffic signatures for normal and suspicious network traffic
- Perform network monitoring to detect suspicious traffic

Length: 19 academic hours

Tools You Will Learn and Use

Docker Bench for security, AWS, Miradore MDM, HashCalc, MD5 calculator, HashMyFiles, VeraCrypt, Data Recovery Wizard, and Wireshark

e-Learning resources including eBook and videos are available to all learners, free of charge. Unlock powerful add-ons, including cloud labs that provide intensive skills training and practice, official EC-Council certification exams, exam preps and certification of completion.

Exam Information

Certification : Network Defence Essentials

Exam Length : 2 Hours

Exam Format : MCQ

No. of Questions: 75

Free Courseware: The Essentials series comes with free learning resources such as eCourseware, lab tutorials, and video lectures that are easy to download and read on any device.

Lab Range (Paid): Practical hands-on learning in a simulated environment gives candidates a competitive edge to hone their skills. Each course in the Essentials Series includes 12 modules with learning exercises and lab ranges that provide a basic to intermediate knowledge of network defense, ethical hacking, and digital forensics.

Certification (Paid): Each Essentials course comes with an onsite or remote certification exam. Following a successful exam attempt, the course-specific certification credential will have a validity period of three years from the date of the successful exam attempt.

If you would like to buy the paid extras to the course, please contact us via e-mail info@koolitus.ee

Paid extras:
iLabs – 102€ (85€+km)
Exam preparation – 66€ (55€+km)
Exam voucher – 102€ (85€+km)
PRS Exam voucher – 156€ (130€+km)
iLabs + Exam preparation + Exam voucher – 216€ (180€+km)
iLabs + Exam preparation + RPS Exam voucher – 300€ (250€+km)
E-book vital source add-on – 36€ (30€+km)

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.