Sale!

Nmap for Hackers (W59)

~~$249.00~~ **$199.00**

Add to cart

Get the access to all our courses via Subscription

Subscribe

CATEGORY: COURSES

f   🐦   G   in   ⊛

DESCRIPTION   **REVIEWS (0)**

This course is designed to equip you with relevant skills to be able to analyze computer systems and network resources using the Network Mapper Tool, generally referred to as Nmap. It is an essential tool necessary for scanning and enumeration of computer networks during a penetration testing service. A comprehensive understanding of the techniques involved in using this tool will make your job easier and faster. My desire is that at the end of the course you see the relevance that Nmap carries in the Information Technology space.

Why you?	Why now?	Why this course?

Who is this course for:

- Network Administrators
- Penetration Testers/Ethical Hackers
- Network Security Auditors
- Security Engineers (Network/System)
- Digital Forensics Analysts
- Information Security Analysts
- System Administrators
- IT Managers
- SOC Managers

Course benefits:

Tools	Skills	Scope

What tools will you use?

- Kali-Linux
- Virtual Box

- Nmap
- Zenmap

Course general information:

<table>
<tr><td>How this works</td><td>Lab Setup</td><td>Prerequisites</td></tr>
</table>

DURATION: 18 hours

CPE POINTS: On completion, you get a certificate granting you 18 CPE points.

LAUNCH DATE: October 14th 2021 (weekly publishing schedule)

Course format:

- Self-paced
- Pre-recorded
- Accessible even after you finish the course
- No preset deadlines
- Materials are video, labs, and text
- All videos captioned

YOUR INSTRUCTOR:

Hanniel H. Jafaru is a Cyber Security/IT Consultant, Instructor & Writer with over 14 years of experience. He is the Director of Studies at HICS Academy, formerly known as Ham Institute of Cyber Security and MD/CEO of Ham Network Ltd. He is a member of Cyber Security Experts Association of Nigeria (CSEAN), ASIS International, Association for Computing Machinery (ACM) & International Consortium of Minority Cybersecurity Professionals (ICMCP). His professional area of specialization is Information Security, Ethical Hacking & Digital Forensics.

COURSE SYLLABUS

Module 1

Introduction to Nmap

This module is going to give us a basic understanding of Nmap, why it is important and what it can be used for. We are going to teach how to install the required tools for the course on both a Windows operating system and a Linux operating system. It is important that you understand the concept of this tool to be able to integrate its use in subsequent modules.

<table>
<tr><td>Topics</td><td>Assignment</td></tr>
</table>

- Understanding Nmap
- History and Future of Nmap
- Nmap & Legal Implication
- Installing Nmap - Windows OS, Linux Distributions
- Nmap Scan Phases

Module 2

Working with Nmap

In this module, you will learn about the different parameters, techniques and switches used to engage Nmap in achieving results for analysis. This is required for Nmap basic usage. It is important to understand this module to be able to comprehend the Nmap Script Engine which will be covered in the next module.

Topics	Assignment

- Target & Host Discovery
- Port Scanning Techniques
- Service Version Detection
- OS Detection
- Evading Firewall & Intrusion Detection System

Module 3

Advance Scanning - Nmap Script Engine

This module will introduce the Nmap Script Engine, which enables you to implement different scripts available in Nmap. It contains scripts that will be used to detect vulnerabilities, engage in brute-forcing, and detect other services, etc.

Topics	Assignment

- Introduction to Nmap Script Engine
- Default Nmap Script Engine
- Enumeration & Discovery with NSE
- Vulnerability & Malware Detection with NSE
- Brute Forcing with NSE
- Exploiting with .nse

Module 4

Working with Zenmap

This module is designed for you to explore the Graphics User Interface of Nmap, which is Zenmap. All we have learnt in the previous model will be put into practice via the GUI. Also, we will be able to practice different use cases of both Nmap and Zenmap.

Topics	Assignment

- Introduction to Zenmap
- Scanning with Zenmap
- Interpreting Zenmap Results
- Nmap Use Case 1
- Nmap Use Case 2
- Zenmap Use Case 3

Final exam

Final exam:

Interpreting Results Practical Assignment

- Interpreting Results Practical Assignment

QUESTIONS?

If you have any questions, please contact our eLearning Manager Marta at marta.strzelec@hakin9.org.

OUR BRANDS

eForensics Magazine

PenTest magazine

OUR PRODUCTS

Magazines

Online Courses

Subscription

COMPANY

About Us

Become an Instructor

Write for us

Partners

Blog

SUPPORT

Contact Us

FAQs

MORE

Privacy Policy

Terms and conditions