Course Syllabus

Nmap: A Network Scanning Deep Dive

Instructor Name: Rob Thurston

Course Creation Date: 11/08/2018

Course Description and Goals

Course Description: *Nmap is one of the highest quality and powerful free network utilities in the cybersecurity professional's arsenal.* Though this product is extremely well documented and demonstrated in many other courses, there are very few that provide a deep-dive into all its capabilities, functionality, use cases, and features. This comprehensive course will make you an expert in Nmap and arm you with the knowledge and skills necessary to make you a better network administrator and cybersecurity professional.

Whether you are relatively new to networking, or a seasoned expert, this course will expand your knowledge and/or provide an excellent reference for using Nmap for a multitude of purposes. *Are you a network administrator?* Nmap can be your source for creating a detailed inventory of network assets. *Are you a network security admin or incident responder?* Nmap can help find the sources of almost every problem (threats, threat actors, and vulnerabilities) and help you eliminate them. *Are you a penetration tester or ethical hacker?* Nmap may be the single most important tool you can use to perform scanning, enumeration, banner grabbing, device fingerprinting and vulnerability scanning while evading firewalls and intrusion detection. *Are you studying for a certification test?* This course will provide you with detailed explanations of the most important Nmap commands and help you memorize them for test day.

Prerequisites: The student should have a fundamental understanding of the TCP/IP protocol suite, including transport layer protocols (TCP and UDP) and network layer protocols (IP and ICMP). 3-5 years of network analysis, administration, or cybersecurity experience is recommended. CompTIA Network+, Security+, or Cisco CCNA designations would be of great benefit.

Course Goals: By the end of this course, students should be able to:

- ❏ Explain why Nmap is so important for network administrators and cybersecurity professionals
- ❏ Demonstrate Nmap's ability to create a network asset inventory
- ❏ Demonstrate Nmap's vulnerability assessment capabilities
- ❏ Demonstrate Nmap's penetration testing capabilities
- ❏ Optimize Nmap's performance and customize its results
- ❏ Use Nmap without reference material from the command line or GUI

Labs Used: The student will be guided through the creation of a personal "lab" through the installation and configuration of the Nmap environment. This course will provide detailed commands and explanations that walk the student through running Nmap scans and analyzing the results. Additionally, Cybrary offers several excellent full featured lab environments through Cybrscore. If the student maintains an "Insider Pro" membership, two labs that will be recommended include:

https://www.cybrary.it/catalog/cybrscore/preliminary-scanning
https://www.cybrary.it/catalog/cybrscore/additional-scanning-options

Course Outline

Module 1 | Introduction

- Lesson 1.1: Nmap: What It Is and Why It’s Important (04:35)
- Lesson 1.2: About the Instructor (02:14)
- Lesson 1.3: Course Overview and Pre-requisites (03:08)
- Lesson 1.4: Ethics and Legality of Scanning (10:06)

Module 2 | Nmap Basics

- Lesson 2.1: Installing Nmap on Windows (07:19)
- Lesson 2.2: Installing Nmap on Linux (09:37)
- Lesson 2.3: Installing Nmap on Mac (10:13)
- Lesson 2.4: Kali Linux – A Hacker’s Best Friend (05:19)
- Lesson 2.5: Kali Linux – Lab: Running it Live (09:19)
- Lesson 2.6: Removing Nmap from Windows (08:41)
- Lesson 2.7: Removing Nmap from Linux (02:50)
- Lesson 2.8: Removing Nmap from Mac (04:06)
- Lesson 2.9: Getting Help (11:09)
- Lesson 2.10: Phases of the Nmap Scan (11:30)
- Lesson 2.11: Constructing an Nmap Scan (11:22 Mins)
- Lesson 2.12.1: Constructing an Nmap Scan - Lab Part 1 (07:42)
- Lesson 2.12.2: Constructing an Nmap Scan - Lab Part 2 (10:13)
- Lesson 2.13: Custom Scan Profiles Part 1 (08:35)
- Lesson 2.14: Custom Scan Profiles Part 2 (08:13)

Module 3 | Nmap & The TCP/IP Protocol Suite

- Lesson 3.1: IPv4 for Nmap (08:11)
- Lesson 3.2: IP, TCP, UDP, and ICMP Headers (11:26)
- Lesson 3.3.1: Nmap and Wireshark – Part 1 (10:23)
- Lesson 3.3.2: Nmap and Wireshark – Part 2 (14:00)
- Lesson 3.4: Nmap & IPv6 (05:40)

Module 4 | Network Scanning and Discovery

- Lesson 4.1: Target Specification Review+ (04:10)

Lesson 4.2.1: Target Specification Lab – Part 1 (10:49)
Lesson 4.2.2: Target Specification Lab – Part 2 (08:48)
Lesson 4.3: Scan Techniques (10:59)
Lesson 4.4: Scan Techniques Lab (15:27)
Lesson 4.5.1: Host Discovery – Part 1 (08:42)
Lesson 4.5.2: Host Discovery – Part 2 (10:20)
Lesson 4.6: TCP & UDP Port Scanning (07:48)
Lesson 4.7.1: TCP & UDP Port Scanning Lab – Part 1 (09:09)
Lesson 4.7.2: TCP & UDP Port Scanning Lab – Part 2 (10:20)
Lesson 4.8.1: Service and Application Version Detection – Part 1 (12:13)
Lesson 4.8.2: Service and Application Version Detection – Part 2 (10:15)
Lesson 4.9.1: Operating System Detection and Fingerprinting - Part 1 (09:19)
Lesson 4.9.2: Operating System Detection and Fingerprinting - Part 2 (14:14)
Lesson 4.10.1: NSE, Vulnerability Testing & Exploitation – Part 1 (5:48)
Lesson 4.10.2: NSE, Vulnerability Testing & Exploitation – Part 2 (13:20)
Lesson 4.10.3: NSE, Vulnerability Testing & Exploitation – Part 3 (10:24)
Lesson 4.11.1: Timing and Performance – Part 1 (05:39)
Lesson 4.11.2: Timing and Performance – Part 2 (07:16)