

# **Security Auditing with NMAP**

**Author**

**Dr. Padmavathi Ganapathi**

**Dean-School of Physical Sciences and Computational Sciences**

**Professor**

**Department of Computer Science**

**Avinashilingam Institute for Home Science and Higher Education for Women**

**(Deemed to be University)**

**Coimbatore-641043**

**Tamil Nadu**

**INDIA.**

**Co-author**

**Dr. D. Nethra Pingala Suthishni**

**Assistant Professor**

**Department of Information Technology**

**Avinashilingam Institute for Home Science and Higher Education for Women**

**(Deemed to be University)**

**Coimbatore-641043**

**Tamil Nadu**

**INDIA.**

**Author (s)**

**Padmavathi Ganapathi <sup>a\*</sup>, D. Nethra Pingala Suthishni <sup>b</sup>**

<sup>a</sup> Dean - School of Physical Sciences and Computational Sciences, Professor - Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women (Deemed to be University), Coimbatore, Tamilnadu, India.

<sup>b</sup> Assistant Professor, Department of Information Technology, Avinashilingam Institute for Home Science and Higher Education for Women (Deemed to be University), Coimbatore, Tamilnadu, India.

**First Edition 2023**

**ISBN:**

@Copyright (2023): Authors. The licensee is the Publisher (Notion Press).

## Preface

Cyber Security is a major concern today. Integration of IT and digitization of all sectors mainly depend on critical IT infrastructure. A review of such infrastructures is mandatory to maintain safety and security. Security Auditing provides a comprehensive analysis and review of the IT infrastructures established in an organization. The audit detects vulnerabilities and threats, displaying weak links, and high-risk practices. It is a primary method for examining compliance and to evaluate something (a company, system, product, etc.) against a specific standard to validate that the exact needs are met. An audit ensures a 360-degree in-depth analysis of an organization's security postures.

This book titled "Security Auditing with NMAP" is primarily intends to provide a comprehensive view about the process of security auditing, importance, need, types, auditing standards and procedures for auditing. The main objective of this book is to analyse various security risks in a network and perform auditing methods that help to protect critical data, identify security loopholes, create new security policies and track the effectiveness of security strategies. This book further focuses on an open-source utility tool for network discovery and security auditing, called NMAP. NMAP is one of the important tools in Kali Linux platform for information security tasks. It uses IP packets to determine the hosts available on a network and their services, operating systems and versions, types of packet filters, firewalls and so on. This book facilitates the user to audit the network with various commands and allows a large number of scanning techniques, such as UDP, TCP connect (), TCP SYN (half-open), and FTP. It also offers a wide variety of scan types, including Proxy (bounce attack), ICMP (ping sweep), FIN, ACK sweep, SYN sweep, IP Protocol, and Null scan. It is a useful learning material for students and working professionals who would like to start their career in cyber security audit domain.

**PADMAVATHI GANAPATHI**

Dean-School of Physical Sciences and Computational Sciences  
Professor - Department of Computer Science  
Avinashilingam Institute for Home Science and Higher Education for Women  
(Deemed to be University)  
Coimbatore-641043.

## **Acknowledgement**

The authors would like to thank the authorities of Avinashilingam Institute for Home Science and Higher Education for Women (Deemed to be University) for their support and encouragement for bringing out a study material useful to the students, research scholars and other cyber security professionals. This book is an outcome of the project sanctioned by DST-CURIE-AI, the Department of Science and Technology Scheme for Women Institution. The authors acknowledge Centre for Cyber Intelligence – a project under Centre for Machine learning and Intelligence, sponsored by DST.

## INDEX

CHAPTER NO.	TABLE OF CONTENTS
<b>1</b>	<b>Cyber Security</b>
1.1	Introduction to Cyber Security
1.2	Legal Requirements on Cyber Security
1.3	Importance of Cyber Security
1.4	Need for Cyber Security
1.5	Types of Cyber Security
1.6	Cyber Crime
1.7	Cyber Criminals
1.8	Cyber Risks
1.9	Cyber Security Tools
1.10	Common Tools of Cyber Security in 2021
1.11	Key Elements of Cyber Security
1.12	Why Cyber Security is Important?
1.13	Conclusion
	Exercise
<b>2</b>	<b>Cyber Security Audit</b>
2.1	Introduction
2.2	National Institute of Standards and Technology (NIST)
2.3	Auditing a Network
2.4	Importance of Cyber Security Audit
2.5	Security Risks
2.6	Audit for Information Security
2.7	Auditing Standards
2.8	Auditing Plan
2.9	Conceptual Security Framework
2.10	Security Assessment
2.11	System Policies
2.12	User Survey
2.13	Conclusion

	Exercise
<b>3</b>	<b>Security Audit - Types and Methodology</b>
3.1	Introduction
3.2	Basics of Security Auditing
3.3	Types of Security Audit
3.4	Managing a Successful Audit
3.5	IT Security Audit Types
3.6	Cyber Risks
3.7	Vulnerability
3.8	Conclusion
	Exercise
<b>4</b>	<b>Security Auditing Tools</b>
4.1	Introduction
4.2	Kali Linux 2021.2
4.3	Kali Linux Features
4.4	Kali Linux Installation
4.5	Download Kali Linux ISO Image
4.6	Configuration of Virtual Machine Settings
4.7	Install and Set Up Kali Linux
4.8	Kali Linux Commands: An Overview
4.9	Kali Linux Tools
4.10	Conclusion
	Exercise
<b>5</b>	<b>NMAP - The Network Mapper</b>
5.1	Introduction
5.2	An Overview of Port Scanning
5.3	NMAP Commands
5.4	Demonstration of Kali Linux NMAP
	Exercise

\*\*\*\*\*