1. Record Nr. UNINA9910790622803321

Autore	Mowbray Thomas J
Titolo	Cybersecurity : managing systems, conducting testing, and investigating intrusions / / Thomas J. Mowbray
Pubbl/distr/stampa	Hoboken, New Jersey : , : Wiley, , [2014] ©2014
ISBN	1-118-84965-5 1-118-69704-9
Edizione	[1st edition]
Descrizione fisica	1 online resource (362 p.)
Disciplina	004.56
Soggetti	Computer networks - Security measures Internet - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cover; About the Author; Acknowledgments; Contents; Introduction; Part I: Cyber Network; Chapter 1: Executive Summary; Why Start with Antipatterns?; Security Architecture; Antipattern: Signature-Based Malware Detection versus Polymorphic Threats; Refactored Solution: Reputational-, Behavioral-, and Entropy-Based Malware Detection; Antipattern: Document-Driven Certification and Accreditation; Antipattern: Proliferating IA Standards with No Proven Benefits; Antipattern: Policy-Driven Security Certifications Do Not Address the Threat; Refactored Solution: Security Training Roadmap; Summary AssignmentsChapter 2: The Problems: Cyber Antipatterns; Antipatterns Concept; Forces in Cyber Antipatterns; Cyber Antipattern Templates; Cybersecurity Antipattern Catalog; Summary; Assignments; Chapter 3: Enterprise Security Using the Zachman Framework; What Is Architecture? Why Do We Need It?; Enterprises Are Complex and Changing; The Zachman Framework for Enterprise Architecture; Primitive Models versus Composite Models; How Does the Zachman Framework Help with Cybersecurity?; Everyone Has Their Own Specifications; The Goldmine Is in Row 2; Frameworks for Row 3 Architectural Problem Solving PatternsSummary; Assignments; Part II: Cyber Network Security Hands-On; Chapter 4: Network Administration for Security Professionals; Managing Administrator and Root Accounts;

Installing Hardware; Re-Imaging Operating Systems; Burning and Copying CDs and DVDs; Installing System Protection / Anti-Malware; Setting Up Networks; Installing Applications and Archiving; Customizing System Management Controls and Settings; Managing Remote Login; Managing User Administration; Managing Services; Mounting Disks; Moving Data Between Systems on Networks
Converting Text Files Between OSesMaking Backup Disks; Formatting Disks; Configuring Firewalls; Converting and Migrating VMs; Additional Network Administration Knowledge; Summary; Assignments; Chapter 5: Customizing BackTrack; Creating and Running BackTrack Images; Customizing BackTrack with VM; Updating and Upgrading BackTrack and Pen Test Tools; Adding Windows to BackTrack with VMware; Licensing Challenges for Network Administrators; Summary; Assignments; Chapter 6: Protocol Analysis and; Networking Theory and Practice; Frequently Encountered Network Protocols; Network Programming: Bash
Network Programming: Windows Command-Line Interface (CLI)Python Programming: Accelerated Network Scanning; Summary; Assignments; Chapter 7: Reconnaissance, Vulnerability Assessment, and Cyber Testing; Types of Cybersecurity Evaluations; Understanding the Cybersecurity Testing Methodology; Summary; Assignments; Chapter 8: Penetration Testing; Forms of Cyber Attacks; Network Penetration; Commercial Pen Testing Tools; Using Netcat to Create Connections and Move Data and Binaries; Using Netcat to Create Relays and Pivots Using SQL Injection and Cross-Site Techniques to Perform Web Application and Database Attacks

Sommario/riassunto

A must-have, hands-on guide for working in the cybersecurity profession Cybersecurity involves preventative methods to protect information from attacks. It requires a thorough understanding of potential threats, such as viruses and other malicious code, as well as system vulnerability and security architecture. This essential book addresses cybersecurity strategies that include identity management, risk management, and incident management, and also serves as a detailed guide for anyone looking to enter the security profession. Doubling as the text for a cybersecurity course, it is