1. Record Nr. UNINA9910508473403321

Autore	Dutta Nitul
Titolo	Cyber Security
Pubbl/distr/stampa	Singapore : , : Springer Singapore Pte. Limited, , 2021 ©2022
ISBN	981-16-6597-4
Descrizione fisica	1 online resource (183 pages)
Collana	Studies in Computational Intelligence Ser. ; ; v.995
Altri autori (Persone)	JadavNilesh TanwarSudeep SarmaHiren Kumar Deva PricopEmil
Soggetti	Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Contents -- About the Authors -- 1 Introduction to Cybersecurity -- 1 Introduction to Cybersecurity -- 1.1 Introduction -- 1.2 The Necessity of Cybersecurity -- 1.3 Cybersecurity and Ethics -- 2 Domains of Cybersecurity -- 3 Threats and Actors -- 3.1 Threats in Cyberspace -- 3.2 Types of Threats -- 3.3 Threat Actors and Types of Threat Actors -- 4 Recent Attacks -- 5 Awareness of Cybersecurity in Educational System -- 6 The Outline of the Book -- References -- 2 Being Hidden and Anonymous -- 1 Introduction -- 1.1 The Need for Anonymity -- 2 The Onion Router -- 3 Invisible Internet Project (IIP or I2P) -- 3.1 Working of I2P -- 4 Freenet -- 5 Java Anon Proxy (JAP) -- 6 Summary -- References -- 3 TOR-The Onion Router -- 1 Introduction -- 2 TOR-The Onion Router -- 2.1 Onion Routing -- 3 TOR Browser Installation -- 4 TOR Entities -- 5 TOR Status -- 6 TOR for Mobile-Orbot -- 7 Loopholes in TOR -- 8 What not to Use in TOR -- References -- 4 DarkNet and Hidden Services -- 1 Introduction -- 2 TOR and Its Hidden Service -- 3 Essential Concepts of TOR Hidden Services -- 4 Installation of Hidden Service in Linux -- 5 Countermeasures to Secure Your Own Hidden Service -- References -- 5 Introduction to Digital Forensics -- 1 Introduction to Forensics -- 2 Cyberforensic Process -- 3 Different Artifacts and Forensic Tools -- 3.1

Autopsy -- 3.2 DumpIt -- 3.3 Belkasoft Live RAM Capturer -- 4 Artifacts Gathering -- 4.1 Browser Artifacts -- 4.2 Registry Artifacts -- 4.3 Bulk Extractor -- 5 Network Forensics -- 5.1 ARP Cache Poisoning -- 5.2 Port Mirroring -- 5.3 Flooding -- 5.4 Dynamic Host Control Protocol (DHCP) Redirection -- 5.5 Detection of TOR Traffic in the Captured Traffic -- 6 Conclusion -- References -- 6 Intrusion Detection Systems Fundamentals -- 1 Introduction to Intrusion Detection System -- 2 Techniques to Combat Cyberthreats. 2.1 Firewall -- 2.2 Authentication -- 2.3 Authorization -- 2.4 Encryption -- 2.5 Intrusion Detection System -- 3 Network-Based Intrusion Detection System (NIDS) -- 4 Host-Based Intrusion Detection System (HIDS) -- 5 Distributed Intrusion Detection System (DIDS) -- 5.1 Signature-Based Analysis -- 5.2 Anomaly-Based Analysis -- 6 Snort-Network-Based Intrusion Detection System -- 6.1 Additional Snort Add-Ons -- 6.2 Installation of Snort in Linux -- 6.3 Snort Rules -- 6.4 Rule Header -- 6.5 Rules Options -- 7 Open-Source Host-Based Intrusion Detection System (OSSEC) -- 7.1 Installation of OSSEC in Linux -- 8 Summary -- References -- 7 Introduction to Malware Analysis -- 1 Introduction of Malware -- 2 Types of Malware -- 3 Malware Symptoms -- 4 Need of Malware Analysis and Spreading Mechanism -- 4.1 Need for Malware Analysis -- 4.2 Malware Spreading Mechanism -- 5 Malware Analysis Prerequisites -- 6 Malware Analysis Environment -- 7 Malware Detection System and Analysis -- 7.1 Malware Detection -- 7.2 Malware Analysis -- 8 Conclusion -- References -- 8 Design of a Virtual Cybersecurity Lab -- 1 Introduction of Cybersecurity -- 2 Tools for Cybersecurity -- 3 Virtualization for Cybersecurity -- 4 Installation and Configuration of VMWare Workstation -- 5 Network Modes in Virtual Machines -- 6 Cybersecurity and Various Attacks -- 7 Defense Strategies Against Various Attacks -- 8 Case Study on Website Attacks -- 9 Conclusion -- References -- 9 Importance of Cyberlaw -- 1 Introduction -- 2 Why Cyberlaw is Necessary -- 3 Global Landscape of Cyberlaw -- 4 Cybercrimes -- 4.1 Categories of Cybercrime -- 4.2 Types of Cybercrime -- 5 Conclusion -- References.