1. Record Nr. UNINA9910818992203321

Autore	Hosmer Chet
Titolo	Python passive network mapping : P2NMAP / / Chet Hosmer ; technical editor Gary C. Kessler
Pubbl/distr/stampa	Waltham, Massachusetts : , : Syngress, , 2015 ©2015
ISBN	0-12-802742-8 0-12-802721-5
Edizione	[1st edition]
Descrizione fisica	1 online resource (162 p.)
Disciplina	005.8
Soggetti	Computer networks - Security measures Python (Computer program language) Peer-to-peer architecture (Computer networks)
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 at the end of each chapters and index.
Nota di contenuto	Cover; Title Page; Copyright Page; Dedication; Contents; Biography; Preface; Intended Audience; Prerequisites; Reading this Book; Supported Platforms; Download Software; Comments, Questions and Contributions; Acknowledgments; Chapter 1 - Introduction; Conventions Used in This Text; So What is a Ping Anyway?; What is Python Passive Network Mapping or P2NMAP?; Why Does This Method Cast a Larger Net?; How Can Active Network Mapping Actually Hurt You?; Organization of the Book; Review; Summary Questions; References; Chapter 2 - What You DON'T Know About Your Network What's Running on Your Network Might Surprise YouBig vs. Little; We Care About What's Running on Our Systems; Why Do We Care?; A Quick Demonstration; How to Do This in Python?; Sample Program Output; OS Fingerprinting; OS Fingerprinting Using TCP/IP Default Header Values; OS Fingerprinting Using Open Port Patterns; What Open Ports or Services Don't You Know About?; How is This Useful?; Who's Touching Your Network?; Review; Summary Questions; Additional Resources; Chapter 3 - Capturing Network Packets Using Python; Setting up a Python Passive Network Mapping Environment

Switch Configuration for Packet Capture Computing Resources; Storing Captured Data; Storing the Captured Packets - Python Dictionaries; IP Observation Dictionary Class; OS Observation Dictionary Class; The Art of the Silent Capture; Python Source Code; Command Line Entry and Execution of P2NMAP-Capture.py; Review; Summary Questions; Additional Resource; Chapter 4 - Packet Capture Analysis; Packet Capture Analysis; Setting up Options for Analysis; Loading an Observation File; Direct Program Output; Specifying the Host Lookup Option; Specifying the Country Lookup Option; Performing Analysis Printing Observations All Printing the Observed Servers; Printing the Observed Clients; Printing the Observed Server to Client Connections; Printing a Histogram of Observations; Final P2NMAP-Analysis Script Complete Source Code; Review; Summary Questions; Additional Resource; Chapter 5 - PCAP Extractor and OS Fingerprinting; PCAP Extraction; Review of P2NMAP-Capture; Utilizing the dptk Package; P2NMAP-PCAP-Extractor.py Script; Executing P2NMAP-PCAP-Extractor; Passive OS Fingerprinting; OS Fingerprinting Truth Table; Truth Table Python Class; P2NMAP-OS-Fingerprint Script
Executing P2NMAP-OS-FingerprintReview; Summary Questions; Additional Resources; Chapter 6 - Future Considerations and Challenge Problems; Author Observations; Author Predictions; Challenge Problems; More Information; Subject Index

Sommario/riassunto

Python Passive Network Mapping: P2NMAP is the first book to reveal a revolutionary and open source method for exposing nefarious network activity. The ""Heartbleed"" vulnerability has revealed significant weaknesses within enterprise environments related to the lack of a definitive mapping of network assets. In Python Passive Network Mapping, Chet Hosmer shows you how to effectively and definitively passively map networks. Active or probing methods to network mapping have traditionally been used, but they have many drawbacks - they can disrupt operations, crash systems, and - most important