

1. Record Nr.	UNINA9910131625703321
Autore	Gregg Michael
Titolo	The network security test lab : a step-by-step guide / / Michael Gregg
Pubbl/distr/stampa	Indianapolis, Indiana : , : Wiley, , 2015 ©2015
ISBN	1-118-98713-6 1-119-18343-X 1-118-98715-2
Edizione	[1st edition]
Descrizione fisica	1 online resource (482 p.)
Disciplina	005.8
Soggetti	Computer networks - Security measures Computer security - Evaluation
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	The Network Security Test Lab; About the Author; Credits; Acknowledgments; Contents; Introduction; Chapter 1 Building a Hardware and Software Test Platform; Why Build a Lab?; Hardware Requirements; Physical Hardware; Equipment You Already Have; New Equipment Purchases; Used Equipment Purchases; Online Auctions; Thrift Stores; Company Sales; Virtual Hardware; VMware; VirtualBox; Hacker Hardware; Software Requirements; Operating Systems; Microsoft Windows; Linux; Navigating in Linux; Linux Basics; Mac OS X; Software and Applications; Learning Applications; Hacking Software; Summary; Key Terms; Exercises; Equipment Checklist; Installing VMware Workstation; Exploring Linux Operating System Options; Using VMware to Build a Windows Image; Using VMware Converter to Create a Virtual Machine; Exploring Other Operating System Options; Running Kali from VMware; Installing Tools on Your Windows Virtual Machine; Chapter 2 Passive Information Gathering; Starting at the Source; Scrutinizing Key Employees; Dumpster Diving (Electronic); Analyzing Web Page Coding; Exploiting Website Authentication Methods; Mining Job Ads and Analyzing Financial Data; Using Google to Mine Sensitive Information; Exploring Domain Ownership; WHOIS; Regional Internet Registries;

Domain Name System; Identifying Web Server Software; Web Server Location; Summary; Key Terms; Exercises; IP Address and Domain Identification; Information Gathering; Google Hacking; Banner Grabbing; Telnet; Netcat; VisualRoute; Chapter 3 Analyzing Network Traffic; Why Packet Analysis Is Important; How to Capture Network Traffic; Promiscuous Mode; Hubs and Switches; Hubbing Out and Using Taps; Switches; Capturing Network Traffic; Managed and Unmanaged Switches; ARP Cache Poisoning; Flooding; DHCP Redirection Redirection and Interception with ICMP; Preventing Packet Capture; Dynamic Address Inspection; DHCP Snooping; Preventing VLAN Hopping; Detecting Packet Capture; Wireshark; Wireshark Basics; Filtering and Decoding Traffic; Basic Data Capture-A Layer-by-Layer Review; Physical-Data-Link Layer; Network-Internet Layer; Transport-Host-Host Layer; Application Layer; Other Network Analysis Tools; Summary; Key Terms; Exercises; Fun with Packets; Packet Analysis with tcpdump; Packet Filters; Making a One-Way Data Cable; Chapter 4 Detecting Live Systems and Analyzing Results; TCP/IP Basics The Network Access Layer; The Internet Layer; The Host-to-Host Layer; Transmission Control Protocol; User Datagram Protocol; The Application Layer; Detecting Live Systems with ICMP; ICMP-Ping; Traceroute; Port Scanning; TCP and UDP Port Scanning; Advanced Port-Scanning Techniques; Idle Scan; Analyzing Port Scans; Port-Scanning Tools; Nmap; SuperScan; Other Scanning Tools; OS Fingerprinting; Passive Fingerprinting; Active Fingerprinting; How Nmap OS Fingerprinting Works; Scanning Countermeasures; Summary; Key Terms; Exercises; Understanding Wireshark; Interpreting TCP Flags; Performing an ICMP Packet Decode

Sommario/riassunto

The ultimate hands-on guide to IT security and proactive defense. The Network Security Test Lab is a hands-on, step-by-step guide to ultimate IT security implementation. Covering the full complement of malware, viruses, and other attack technologies, this essential guide walks you through the security assessment and penetration testing process, and provides the set-up guidance you need to build your own security-testing lab. You'll look inside the actual attacks to decode their methods, and learn how to run attacks in an isolated sandbox to better understand how attackers target systems, and h
