1. Record Nr. UNINA9910131512403321

Autore	Monte Matthew
Titolo	Network attacks & exploitation : a framework / / Matthew Monte
Pubbl/distr/stampa	Indianapolis, Indiana : , : Wiley, , 2015 ©2015
ISBN	1-118-98723-3 1-119-18344-8 1-118-98708-X
Edizione	[1st edition]
Descrizione fisica	1 online resource (219 p.)
Disciplina	658.478
Soggetti	Business enterprises - Computer networks - Security measures Computer security Computer crimes - Prevention Corporations - 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; Title Page; Copyright; Contents; Introduction; Chapter 1 Computer Network Exploitation; Operations; Operational Objectives; Strategic Collection; Directed Collection; Non-Kinetic Computer Network Attack (CNA); Strategic Access; Positional Access; CNE Revisited; A Framework for Computer Network Exploitation; First Principles; Principles; Themes; Summary; Chapter 2 The Attacker; Principle of Humanity; Life Cycle of an Operation; Stage 1: Targeting; Stage 2: Initial Access; Stage 3: Persistence; Stage 4: Expansion; Stage 5: Exfiltration; Stage 6: Detection; Principle of Access Inbound AccessOutbound Access; Bidirectional Access; No Outside Access; Access Summary; Principle of Economy; Time; Targeting Capabilities; Exploitation Expertise; Networking Expertise; Software Development Expertise; Operational Expertise; Operational Analysis Expertise; Technical Resources; Economy Summary; Attacker Structure; Summary; Chapter 3 The Defender; Principle of Humanity; Humanity and Network Layout; Humanity and Security Policy; Principle of Access; The Defensive Life Cycle; Principle of Economy; The Helpful Defender; Summary; Chapter 4 Asymmetries; False Asymmetries

Advantage AttackerMotivation; Initiative; Focus; Effect of Failure; Knowledge of Technology; Analysis of Opponent; Tailored Software; Rate of Change; Advantage Defender; Network Awareness; Network Posture; Advantage Indeterminate; Time; Efficiency; Summary; Chapter 5 Attacker Frictions; Mistakes; Complexity; Flawed Attack Tools; Upgrades and Updates; Other Attackers; The Security Community; Bad Luck; Summary; Chapter 6 Defender Frictions; Mistakes; Flawed Software; Inertia; The Security Community; Complexity; Users; Bad Luck; Summary; Chapter 7 Offensive Strategy; Principle 1: Knowledge Measuring KnowledgePrinciple 2: Awareness; Measuring Awareness; Principle 3: Innovation; Measuring Innovation; Defensive Innovation; Principle 4: Precaution; Measuring Precaution; Principle 5: Operational Security; Minimizing Exposure; Minimizing Recognition; Controlling Reaction; Measuring Operational Security; Principle 6: Program Security; Attacker Liabilities; Program Security Costs; Measuring Program Security; Crafting an Offensive Strategy; Modular Frameworks; A Note on Tactical Decisions; Summary; Chapter 8 Defensive Strategy; Failed Tactics; Antivirus and Signature-Based Detection
Password PoliciesUser Training; Crafting a Defensive Strategy; Cloud-Based Security; Summary; Chapter 9 Offensive Case Studies; Stuxnet; Access; Economy; Humanity; Knowledge; Awareness; Precaution; Innovation; Operational Security; Program Security; Stuxnet Summary; Flame; Gauss; Dragonfly; Red October; APT1; Axiom; Summary; Epilogue; Appendix Attack Tools; Antivirus Defeats; Audio/Webcam Recording; Backdoor; Bootkit; Collection Tools; Exploits; Fuzzer; Hardware-based Trojan; Implant; Keystroke Logger; Network Capture; Network Survey; Network Tunnel; Password Dumpers and Crackers; Packer
Persistence Mechanism

Sommario/riassunto

Incorporate offense and defense for a more effective network security strategy Network Attacks and Exploitation provides a clear, comprehensive roadmap for developing a complete offensive and defensive strategy to engage in or thwart hacking and computer espionage. Written by an expert in both government and corporate vulnerability and security operations, this guide helps you understand the principles of the space and look beyond the individual technologies of the moment to develop durable comprehensive solutions. Numerous real-world examples illustrate the offensive and defensive concepts at