Making Sense of Cybersecurity

Kranz, Thomas

Monografía

Título: Making Sense of Cybersecurity

Editorial: New York Manning Publications Co. LLC 2022 2022

Descripción física: 1 online resource (255 pages)

Contenido: Intro -- inside front cover -- Making Sense of Cybersecurity -- Copyright -- dedication -- contents -- front matter -- foreword -- preface -- acknowledgments -- about this book -- Who should read this book -- How this book is organized: A roadmap -- liveBook discussion forum -- about the author -- about the cover illustration -- 1 Cybersecurity and hackers -- 1.1 Cybersecurity: How it has evolved -- 1.2 Why should you care about cybersecurity? -- 1.3 Who is the ideal reader for this book? -- 1.4 How does hacking-and defending-work? -- 1.5 What will you learn in this book? -- 1.6 What we won't cover -- 1.6.1 Denial-of-service attacks -- 1.6.2 Encryption -- 1.7 What tools do you need to get started? -- Summary -- 2 Cybersecurity: Everyone's problem -- 2.1 Keeping it simple -- 2.2 Impacts of a security breach -- 2.3 Objectives of a cybersecurity strategy -- 2.3.1 Applying what we've learned so far -- 2.4 Supporting our strategy: Building a patching policy -- 2.4.1 CVEs are used to coordinate all information around a specific bug, and a CVSS score is used to rate how serious it is -- 2.4.2 Building a patching policy -- 2.5 A culture of security -- 2.6 How ready are you? -- Summary -- Part 1 -- 3 Understanding hackers -- 3.1 Who are the hackers? -- 3.1.1 Black hat -- 3.1.2 Grey hat -- 3.1.3 White hat -- 3.2 Where do they come from? -- 3.2.1 Black hat hacker: Alberto Gonzalez -- 3.2.2 Grey hat hacker: Sabu and the Anonymous collective -- 3.2.3 White hat hacker: Mudge -- 3.2.4 The hacker mindset -- 3.3 What are hackers capable of? -- 3.3.1 The bad guys: Black hats -- 3.3.2 The middle ground: Grey hats -- 3.3.3 The good guys: White hats -- 3.4 Working through a real-life problem: How do hackers think? -- 3.4.1 Breaking a financial services website -- 3.4.2 Combining the hacker mindset with the OODA loop -- Summary -- 4 External attacks 4.1 How do hackers get in? -- 4.1.1 Home setup -- 4.1.2 Corporate network -- 4.2 Data injection attacks -- 4.2.1 SQLi -- 4.2.2 Cross-site scripting -- 4.3 Malware: Viruses, Trojans, and ransomware -- 4.3.1 Viruses -- 4.3.2 Trojans -- 4.3.3 Ransomware -- 4.3.4 Protection -- 4.4 Dodgy Wi-Fi -- 4.4.1 Defenses -- 4.5 Mobile phones, SMS, and 5G -- 4.5.1 Malware -- 4.5.2 IMEI cloning -- 4.5.3 SMS spoofing -- 4.5.4 Problems with 5G -- 4.5.5 Keeping safe -- Summary -- 5 Tricking our way in: Social engineering -- 5.1 The weakest link: People -- 5.2 Malicious USB -- 5.2.1 USB devices with malware -- 5.2.2 BadUSB: USB devices that attack your laptop and phone -- 5.2.3 Evil maid attacks -- 5.3 Targeted attacks: Phishing -- 5.4 Credential theft and passwords -- 5.4.1 Store passwords more securely -- 5.4.2 Make it easier to use unique, complex passwords -- 5.4.3 Stop relying on just a password to protect your accounts -- 5.5 Building access cards -- Summary -- 6 Internal attacks -- 6.1 What happens after they get in? -- 6.2 Gaining more control: Privilege escalation -- 6.3 Data theft -- 6.3.1 Advanced persistent threat -- 6.3.2 Making money from stolen financial details

-- 6.3.3 Making money from ID theft -- 6.4 Insider threats -- 6.5 "Blast radius": Limiting the damage -- 6.5.1 AI, machine learning, behavioral analysis, and snake oil -- 6.6 Building your castle: Defense in depth -- 6.6.1 Perimeter security: Build a wall -- 6.6.2 Zero trust: The attackers are everywhere -- Summary -- 7 The Dark Web: Where is stolen data traded? -- 7.1 What is the Dark Web? -- 7.1.1 TOR -- 7.1.2 I2P -- 7.1.3 Freenet -- 7.2 How to access the Dark Web -- 7.2.1 Precautions -- 7.3 How is the Dark Web used? -- 7.3.1 Illegal weapons -- 7.3.2 Illegal drugs -- 7.3.3 Hackers for hire -- 7.3.4 Hacktivism -- 7.3.5 Evading censorship -- 7.3.6 Making money from stolen data -- 7.3.7 Bitcoin Summary -- Part 2 -- 8 Understanding risk -- 8.1 Issues vs. vulnerabilities vs. threats vs. risks -- 8.2 How likely is a hack? -- 8.3 How bad will it be? -- 8.3.1 Common Vulnerability Scoring System -- 8.3.2 CVE Vector -- 8.3.3 Making things personal -- 8.4 A simple model to measure risk -- 8.5 How do I measure and communicate this? -- 8.5.1 Page 1: Our security matrix -- 8.5.2 Page 2: Our vulnerabilities -- 8.5.3 Page 3: Our security roadmap -- 8.5.4 Page 4: Information and actions -- Summary -- 9 Testing your systems -- 9.1 How are vulnerabilities discovered? -- 9.1.1 An attacker has exploited a vulnerability -- 9.1.2 A stranger has found what they think is a vulnerability -- 9.1.3 A vendor has released a security advisory -- 9.2 Vulnerability management -- 9.2.1 Vulnerability life cycle management -- 9.2.2 Vulnerability scanning workflow -- 9.3 Break your own stuff: Penetration testing -- 9.3.1 Defining the scope -- 9.3.2 Carrying out the test -- 9.3.3 The report -- 9.4 Getting expert help: Bug bounties -- 9.5 Breaking in: Physical penetration testing -- 9.5.1 Why is physical penetration testing not carried out? -- 9.5.2 Why does physical penetration testing matter? -- 9.5.3 What should a physical penetration test cover? -- 9.6 Red teams and blue teams -- 9.6.1 Red team -- 9.6.2 Blue team -- 9.6.3 Other "colors of the rainbow" teams -- 9.6.4 Keeping your staff -- Summary -- 10 Inside the security operations center -- 10.1 Know what's happening: Logging and monitoring -- 10.1.1 Logging -- 10.1.2 Monitoring -- 10.2 Dealing with attacks: Incident response -- 10.3 Keeping track of everything: Security and Information Event Management -- 10.4 Gaining intelligence: Data feeds -- Summary -- 11 Protecting the people -- 11.1 Don't play the blame game -- 11.2 MFA -- 11.3 Protecting from ransomware 11.3.1 Make sure everyone has antimalware software installed -- 11.3.2 Make it easy to install legitimate software -- 11.3.3 Backups -- 11.4 Education and support -- 11.4.1 Regular email newsletters -- 11.4.2 Lunchtime talks -- 11.4.3 Security concierge or security champion -- 11.4.4 Live exercises -- Summary -- 12 After the hack -- 12.1 Responding to a breach -- 12.1.1 Asset ownership -- 12.1.2 Business continuity process -- 12.1.3 Data/system restore -- 12.1.4 PR/media communications -- 12.1.5 Internal notification /communication groups -- 12.1.6 Customer communications policy -- 12.1.7 Cyber insurance policies -- 12.1.8 Legal team involvement/advice -- 12.1.9 Law enforcement engagement policy -- 12.1.10 Country-specific data controller communications -- 12.2 Where to get help? -- 12.2.1 Cyber insurance providers -- 12.2.2 Legal teams -- 12.2.3 Law enforcement agencies -- 12.2.4 Country-specific data controller organizations -- 12.2.5 Hosting providers -- 12.3 What to do next? -- 12.4 Lessons learned -- Summary -- index -- inside back cover

ISBN: 1-63835-626-2

Materia: Computer security Computer networks- Security measures

Enlace a formato físico adicional: 1-61729-800-X

Baratz Innovación Documental

- Gran Vía, 59 28013 Madrid
- (+34) 91 456 03 60
- informa@baratz.es