

1. Record Nr.	UNINA9910716765903321
Autore	Wang Bin
Titolo	Demystifying power system oscillations - recent and ongoing efforts // Bin Wang
Pubbl/distr/stampa	Golden, CO : , : National Renewable Energy Laboratory, , [May 2021]
Descrizione fisica	1 online resource (17 pages) : color illustrations, color maps
Collana	NREL/PR ; ; 5C00-79994
Soggetti	Oscillations Nonlinear oscillations
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"2021 Joint Synchronized Information Subcommittee (JSIS) Meeting." "May 13, 2021."

2. Record Nr.	UNINA9910814576203321
Autore	Messier Ric
Titolo	Network forensics // Ric Messier
Pubbl/distr/stampa	Indianapolis, Indiana : , : Wiley, , 2017 2017
ISBN	1-119-32917-5 1-119-32919-1 1-119-32918-3
Descrizione fisica	1 online resource
Collana	THEi Wiley ebooks.
Disciplina	005.8
Soggetti	Computer networks - Security measures Internet - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Introduction xxi 1 Introduction to Network Forensics 1 What Is Forensics? 3 Handling Evidence 4 Cryptographic Hashes 5 Chain of Custody 8 Incident Response 8 The Need for Network Forensic Practitioners 10 Summary 11 References 12 2 Networking Basics 13 Protocols 14 Open Systems Interconnection (OSI) Model 16 TCP/IP Protocol Suite 18 Protocol Data Units 19 Request for Comments 20 Internet Registries 23 Internet Protocol and Addressing 25 Internet Protocol Addresses 28 Internet Control Message Protocol (ICMP) 31 Internet Protocol Version 6 (IPv6) 31 Transmission Control Protocol (TCP) 33 Connection-Oriented Transport 36 User Datagram Protocol (UDP) 38 Connectionless Transport 39 Ports 40 Domain Name System 42 Support Protocols (DHCP) 46 Support Protocols (ARP) 48 Summary 49 References 51 3 Host-Side Artifacts 53 Services 54 Connections 60 Tools 62 netstat 63 nbstat 66 ifconfig g/ipconfig g 68 Sysinternals 69 ntop 73 Task Manager/Resource Monitor 75 ARP 77 /proc Filesystem 78 Summary 79 4 Packet Capture and Analysis 81 Capturing Packets 82 Tcpdump/Tshark 84 Wireshark 89 Taps 91 Port Spanning 93 ARP Spoofing 94 Passive Scanning 96 Packet Analysis with Wireshark 98 Packet Decoding 98 Filtering 101 Statistics 102 Following Streams 105 Gathering Files 106 Network Miner 108 Summary 110 5 Attack Types

113 Denial of Service Attacks 114 SYN Floods 115 Malformed Packets
118 UDP Floods 122 Amplification Attacks 124 Distributed Attacks
126 Backscatter 128 Vulnerability Exploits 130 Insider Threats 132
Evasion 134 Application Attacks 136 Summary 140 6 Location
Awareness 143 Time Zones 144 Using whois 147 Traceroute 150
Geolocation 153 Location-Based Services 156 WiFi Positioning 157
Summary 158 7 Preparing for Attacks 159 NetFlow 160 Logging 165
Syslog 166 Windows Event Logs 171 Firewall Logs 173 Router and
Switch Logs 177 Log Servers and Monitors 178 Antivirus 180 Incident
Response Preparation 181 Google Rapid Response 182 Commercial
Offerings 182 Security Information and Event Management 183
Summary 185 8 Intrusion Detection Systems 187 Detection Styles 188
Signature-Based 188 Heuristic 189 Host-Based versus Network-Based
190 Snort 191 Suricata and Sagan 201 Bro 203 Tripwire 205 OSSEC 206
Architecture 206 Alerting 207 Summary 208 9 Using Firewall and
Application Logs 211 Syslog 212 Centralized Logging 216 Reading Log
Messages 220 LogWatch 222 Event Viewer 224 Querying Event Logs
227 Clearing Event Logs 231 Firewall Logs 233 Proxy Logs 236 Web
Application Firewall Logs 238 Common Log Format 240 Summary 243
10 Correlating Attacks 245 Time Synchronization 246 Time Zones 246
Network Time Protocol 247 Packet Capture Times 249 Log Aggregation
and Management 251 Windows Event Forwarding 251 Syslog 252 Log
Management Offerings 254 Timelines 257 Plaso 258 PacketTotal 259
Wireshark 261 Security Information and Event Management 262
Summary 263 11 Network Scanning 265 Port Scanning 266 Operating
System Analysis 271 Scripts 273 Banner Grabbing 275 Ping Sweeps 278
Vulnerability Scanning 280 Port Knocking 285 Tunneling 286 Passive
Data Gathering 287 Summary 289 12 Final Considerations 291
Encryption 292 Keys 293 Symmetric 294 Asymmetric 295 Hybrid 296
SSL/TLS 297 Cloud Computing 306 Infrastructure as a Service 306
Storage as a Service 309 Software as a Service 310 Other Factors 311
The Onion Router (TOR) 314 Summary 317 Index 319.

Sommario/riassunto

Intensively hands-on training for real-world network forensics
Network Forensics provides a uniquely practical guide for IT and law enforcement professionals seeking a deeper understanding of cybersecurity. This book is hands-on all the way--by dissecting packets, you gain fundamental knowledge that only comes from experience. Real packet captures and log files demonstrate network traffic investigation, and the learn-by-doing approach relates the essential skills that traditional forensics investigators may not have. From network packet analysis to host artifacts to log analysis and beyond, this book emphasizes the critical techniques that bring evidence to light. Network forensics is a growing field, and is becoming increasingly central to law enforcement as cybercrime becomes more and more sophisticated. This book provides an unprecedented level of hands-on training to give investigators the skills they need. Investigate packet captures to examine network communications
Locate host-based artifacts and analyze network logs
Understand intrusion detection systems--and let them do the legwork
Have the right architecture and systems in place ahead of an incident
Network data is always changing, and is never saved in one place; an investigator must understand how to examine data over time, which involves specialized skills that go above and beyond memory, mobile, or data forensics. Whether you're preparing for a security certification or just seeking deeper training for a law enforcement or IT role, you can only learn so much from concept; to thoroughly understand something, you need to do it. Network Forensics provides intensive hands-on practice with direct translation to real-world application.

3. Record Nr.	UNIORUON00188281
Autore	Berànek, Jíí
Titolo	Absolutismus a konstitucionalismus v echách doby Velké francouzské revoluce / Jirí Beránek
Pubbl/distr/stampa	Praha, : Academia, 1989
ISBN	80-200-0101-8
Descrizione fisica	139 p. ; 21 cm.
Disciplina	943.71
Lingua di pubblicazione	Ceco
Formato	Materiale a stampa
Livello bibliografico	Monografia