A PRACTITIONER'S FIELD GUIDE

FIRST EDITION



Cybersecurity Playbook 2027

Build ➜ Hack ➜ Investigate ➜ Secure ➜ Audit.

Rohas Nagpal

ASIAN SCHOOL OF CYBER LAWS

Contents

Preface 15
How to Use This Book 17
Who This Book Is For 19
The Labs 21

PART I **Internet Infrastructure**

1 **Linux Server Hardening** 23

BUILD · SECURE · AUDIT

1.1 What an Operating System Does 23
1.2 What Linux Is 24
1.3 Windows, macOS and Linux Compared 24
1.4 Why Linux Runs the Internet 25
1.5 Distributions 25
1.6 Ideas You Will Meet in the Lab 26
1.7 What Hardening Means 27
1.8 The Controls in the Lab 27
1.9 How the Lab Works 28
1.10 Beyond the Lab 28

2 **Domain Security Audit** 30

AUDIT · REPORT

2.1 What a Domain Is 30
2.2 How DNS Works 31
2.3 What an Attacker Learns from the Outside 31
2.4 HTTPS, TLS and Certificates 32
2.5 Why Email Is Easy to Fake 32
2.6 SPF, DKIM and DMARC 32
2.7 Protecting the Domain Itself 33
2.8 How the Lab Works 33
2.9 From Findings to Fixes 34

3 **Network Reconnaissance & Vulnerability Scanning** 35

HACK · SECURE

3.1 Addresses and Networks 36
3.2 Ports, Protocols and Services 36
3.3 Rules for Scanning a Network 37
3.4 Mapping the Network and Discovering Devices 37
3.5 Identifying Open Ports and Running Services 38
3.6 Scanning for Known Vulnerabilities 38
3.7 Separating Real Weaknesses from False Positives 39
3.8 Deciding What to Fix First 39
3.9 How the Lab Works 40
3.10 Rescanning to Verify Remediation 41

4 **Web Server Deployment & Security** 43

BUILD · HACK · SECURE

4.1 How a Website Is Served 44
4.2 Connecting a Domain and Configuring HTTPS 44
4.3 Exposed Directories and Files 45
4.4 Insecure Configurations 45
4.5 Missing Security Protections 45
4.6 Common Web Server Vulnerabilities 46
4.7 Exploiting Weaknesses in a Controlled Environment 47
4.8 How the Lab Works 47
4.9 Fixing and Verifying 47

5 **DNS Infrastructure & Attack Simulation** 49

HACK · INVESTIGATE · SECURE

5.1 How Domain Names Are Resolved 50
5.2 How DNS Infrastructure Is Configured 50
5.3 DNS Spoofing and Cache Poisoning 51
5.4 Other DNS-Based Attacks 51
5.5 Investigating Suspicious DNS Activity 52
5.6 Common DNS Misconfigurations 53
5.7 How the Lab Works 53
5.8 Recommending and Testing Controls 54

PART II **Applications & APIs**

6 **Building a Full-Stack Web Application** 56

BUILD

6.1 Frontend, Backend, Database and REST APIs 57
6.2 User Registration and Login 57
6.3 Password Reset 58
6.4 User Roles 58
6.5 Session Management and Authentication Tokens 59
6.6 File Uploads 59
6.7 Application Logging for Monitoring and Investigation 60
6.8 Deploying the Application 60

7 **Web Application Hacking** 62

HACK

7.1 Setting Up a Controlled Attack Environment 63
7.2 Attacking Authentication 63
7.3 Breaking Access Controls 63
7.4 Injection 63
7.5 Cross-Site Scripting 64
7.6 Insecure Session Handling 64
7.7 File Upload Attacks 64
7.8 Accessing Other Users' Data 64
7.9 Demonstrating Impact 65

8 **API Hacking & Security** 66

HACK · SECURE

8.1 Discovering the APIs Behind an Application 66
8.2 Broken Authentication 67
8.3 Unauthorised Access to API Endpoints 67
8.4 Insecure Object References 67
8.5 Excessive Data Exposure 67
8.6 API Abuse 68
8.7 Token Handling and Authorisation Weaknesses 68
8.8 Controls That Prevent API Attacks 68

9 **Investigating Application Attacks** 70

INVESTIGATE · REPORT

9.1 Web Server, API, Authentication and Database Records 71
9.2 Reconstructing the Sequence of Events 71
9.3 How the Attacker Gained Access 72
9.4 Affected Accounts and Data 72
9.5 What Was Viewed, Modified or Deleted 73
9.6 How the Lab Works 73
9.7 The Incident Investigation Report 73

10 **Application Security, Auditing & Secure Deployment** 75

SECURE · AUDIT · REPORT

10.1 Fixing the Vulnerabilities Found Earlier 76
10.2 Authentication, Authorisation and Session Security 76
10.3 Input Validation and Logging 76
10.4 Securing Source Code and Dependencies 77
10.5 Securing the Deployment Pipeline 77
10.6 Securing Container Images 78
10.7 The Structured Security Audit 78
10.8 Retesting Exploited Weaknesses 78
10.9 Reporting Security Posture and Remaining Risk 79

PART III **Cloud & Containers**

11 **Cloud Infrastructure & Security** 81

BUILD · SECURE

11.1 Virtual Servers and Public and Private Networks 82
11.2 Object Storage 82
11.3 Identities and Permissions 82
11.4 Logging, Monitoring and Backups 83
11.5 DNS and Edge Security Controls 83
11.6 Excessive Permissions 83
11.7 Exposed Storage and Leaked Credentials 84
11.8 Weak Network Controls 84
11.9 Identifying, Correcting and Verifying Weaknesses 84

12 **Container Hacking & Security** 86

BUILD · HACK · SECURE

12.1 How Applications Are Containerised 87
12.2 Private Image Registries 87
12.3 Container Orchestration 87
12.4 Vulnerable Images 87
12.5 Excessive Privileges 88
12.6 Exposed Secrets 88
12.7 Insecure Configurations and Weak Access Controls 88
12.8 Exploiting, Remediating and Retesting 88

13 **Cloud Incident Investigation & Audit** 90

INVESTIGATE · AUDIT

13.1 Identity, Access, Storage, Application and Network Evidence 91
13.2 Container Records 91
13.3 Compromised Credentials 92
13.4 Unauthorised Access and Excessive Permissions 92
13.5 Suspicious Data Transfers 92
13.6 Reconstructing the Incident 93
13.7 Auditing the Environment with Cyber360 93
13.8 Reviewing and Verifying Remediation 93

PART IV **AI Systems**

14 **Building an AI Application with RAG and Tool Calling** 95

BUILD

14.1 How an AI Application Is Put Together 96
14.2 User Accounts and Document Uploads 96
14.3 The Knowledge Base 96
14.4 Retrieval-Augmented Generation 97
14.5 Connecting External APIs and Tools 97
14.6 Permissions and Credentials 98
14.7 Logging Interactions, Retrievals and Tool Executions 98

15 **AI Forensics & Security** 100

HACK · INVESTIGATE · AUDIT

15.1 How AI Applications Are Attacked 101
15.2 Prompt Injection and Data Leakage 101
15.3 Unsafe Tool and Agent Actions 101
15.4 Other AI Weaknesses 101
15.5 Investigating an AI Incident 102
15.6 Controls and Their Limits 102
15.7 Testing AI Applications Safely 103
15.8 Reporting and Remediation 103

PART V **Smart Contracts**

16 **Smart Contract Development & Deployment** 105

BUILD

16.1 Blockchains, Test Networks and Wallets 106
16.2 Tokens 106
16.3 Token Vaults 107
16.4 Escrow Systems 107
16.5 Payment Contracts 107
16.6 Access Permissions 107
16.7 How Contracts Interact with Users, Tokens and Other Contracts 108

17 **Smart Contract Hacking & Security** 110

HACK · SECURE

17.1 Why Contract Weaknesses Are Dangerous 111
17.2 Re-entrancy 111
17.3 Broken Access Control 111
17.4 The tx.origin Flaw 111
17.5 Other Common Weaknesses 112
17.6 Exploiting Safely on a Test Chain 112
17.7 Remediating and Retesting 112
17.8 Securing Contracts in Practice 112

PART VI **Investigations**

18 **Fraud, Phishing & Identity Crime** 114

INVESTIGATE · REPORT

18.1 Anatomy of a Fraud Operation 115
18.2 Phishing Emails and Spoofed Websites 115
18.3 Compromised Accounts and Stolen Identities 116
18.4 How the Offenders Approached Their Victims 116
18.5 Following the Money 116
18.6 Identifying Affected Persons and Accounts 117
18.7 Testing Competing Explanations 117
18.8 The Investigation Report 117

19 **Malware & Ransomware** 119

INVESTIGATE · REPORT

19.1 Endpoint, System, Network and Authentication Evidence 120
19.2 The Initial Compromise 120
19.3 Execution and Persistence 121
19.4 Lateral Movement 121
19.5 Data Theft and Encryption 121
19.6 Ransom Communications 121
19.7 Indicators and the Limits of the Evidence 122
19.8 Findings for Containment and Recovery 122

20 **Data Breach, Insider Threat & IP Theft** 124

INVESTIGATE · REPORT

20.1 Access, Activity, Transfer and Media Records 125
20.2 What Was Accessed, Copied, Modified or Disclosed 125
20.3 External Attacker, Insider or Compromised Account? 126
20.4 Reconstructing the Incident 126
20.5 Evidentiary Gaps 126
20.6 Assessing Impact 127
20.7 Documenting Defensible Findings 127

PART VII **Digital Evidence**

21 **Evidence Collection & Preservation** 129

INVESTIGATE · REPORT

21.1 Processing the Scene 130
21.2 Identifying Relevant Items 130
21.3 Safety and Legal Authority 130
21.4 Preserving Traditional and Digital Evidence 131
21.5 Calculating and Verifying Hashes 131
21.6 Chain of Custody 131
21.7 Contamination and Evidence Loss 132
21.8 The Evidence Collection Record 132

22 **IoT Seizure & Forensic Analysis** 134

INVESTIGATE

22.1 The Smart Environment 135
22.2 Mapping Devices and Their Relationships 135
22.3 Isolating and Preserving Devices 135
22.4 Device, Network, Application and Cloud Records 135
22.5 Correlating Events Across Different Clocks 136
22.6 Gaps and Conflicting Data 136
22.7 Why Association Does Not Prove Identity 136

23 **Drone Forensics** 138

INVESTIGATE · REPORT

23.1 Physical and Battery Safety 139
23.2 Network Isolation and Volatile Evidence 139
23.3 Aircraft Storage, Flight Logs and Controller Data 139
23.4 Mobile Applications, Media and Cloud Records 139
23.5 Remote ID Observations 140
23.6 Acquisition Limitations 140
23.7 Reconstructing the Flight Path 140
23.8 Validating Timestamps and GPS Records 140
23.9 The Drone Forensic Evidence Pack 141

24 **Vehicle Infotainment & Telematics Forensics** 142

INVESTIGATE · REPORT

24.1 Physical, Airbag, Electrical and High-Voltage Risks 143
24.2 Infotainment, Telematics and Navigation Records 143
24.3 Paired Devices, Key Fobs and Connected Services 143
24.4 Preserving and Acquiring the Evidence 144
24.5 Reconstructing Journeys and Device Interactions 144
24.6 Correlating with External Evidence 144
24.7 Attribution Limitations 145
24.8 The Vehicle Forensic Report 145

25 **Forensic Reporting & Expert Evidence** 147

REPORT

25.1 Organising Evidence and Exhibits 148
25.2 Facts, Assumptions, Allegations and Inferences 148
25.3 Methodology and Limitations 148
25.4 Supporting Every Material Conclusion 149
25.5 Structuring the Forensic Report 149
25.6 Presenting Evidence in Legal Proceedings 149
25.7 Direct and Cross-Examination 150
25.8 Staying Within Your Expertise 150

PART VIII **The Cyber360 Framework**

26 **Introducing Cyber360** 152

BUILD · HACK · INVESTIGATE · SECURE · AUDIT

26.1 Build, Hack, Investigate, Secure, Audit, Repeat 152
26.2 What an AI Agent Is 153
26.3 The Six Components of a Cyber360 Agent 153
26.4 The Chief Cyber360 Officer 154
26.5 The Specialist Agents and Their Six Categories 155
26.6 Skills, Checklists and the Standards Catalog 155
26.7 Shared Infrastructure 156

27 **Build Agents** 158

BUILD

27.1 **B1** Threat Modelling 159
27.2 **B2** Security Architecture & Requirements 160
27.3 **B3** Privacy & Data Protection Engineering 161
27.4 **B4** Secure Code Review & Remediation 162

28 **Forensics Agents** 163

INVESTIGATE

28.1 **F1** Evidence Acquisition & Chain of Custody 164
28.2 **F2** Disk, Host & Browser Forensics 165
28.3 **F3** Memory Forensics 166
28.4 **F4** Mobile Device Forensics 167
28.5 **F5** Network Forensics 168
28.6 **F6** Log & Timeline Forensics 169
28.7 **F7** Email & Messaging Forensics 170
28.8 **F8** Cloud & SaaS Forensics 171
28.9 **F9** Database Forensics 172
28.10 **F10** Multimedia & Deepfake Analysis 173

29 **Investigation & Response Agents** 174

INVESTIGATE

29.1 **Inv1** Cyber Incident Investigation 175
29.2 **Inv2** Malware Analysis 176
29.3 **Inv3** Ransomware & Extortion Investigation 177
29.4 **Inv4** Phishing & Business Email Compromise 178
29.5 **Inv5** Account Takeover Investigation 179
29.6 **Inv6** Data Breach Investigation 180
29.7 **Inv7** Insider Threat Investigation 181
29.8 **Inv8** Online Fraud & Scam Investigation 182
29.9 **Inv9** OSINT & Social Media Investigation 183
29.10 **Inv10** Threat Intelligence & Digital Risk 184
29.11 **Inv11** Cryptocurrency Investigation 185
29.12 **Inv12** Incident Response & Crisis Coordination 186

30 **Security Agents** 187

SECURE

30.1 **S1** Network & Perimeter Security 188
30.2 **S2** Linux, Unix & Virtualisation Security 189
30.3 **S3** Windows & Active Directory Security 190
30.4 **S4** Endpoint & Device Management Security 191
30.5 **S5** Identity & Access Security 192
30.6 **S6** Web Application Security 193
30.7 **S7** API Security 194
30.8 **S8** Mobile Application Security 195
30.9 **S9** Database Security 196
30.10 **S10** Cloud Security 197
30.11 **S11** TLS & Cryptography Security 198
30.12 **S12** Container & Kubernetes Security 199
30.13 **S13** SaaS & Collaboration Security 200
30.14 **S14** Software Supply Chain & CI/CD Security 201
30.15 **S15** AI, ML &ic Security 202
30.16 **S16** OT, ICS & IoT Security 203
30.17 **S17** Smart Contract & Web3 Security 204
30.18 **S18** Email & Domain Security 205
30.19 **S19** Asset, Vulnerability & Exposure Management 206
30.20 **S20** SOC, Detection Engineering & Threat Hunting 207
30.21 **S21** Business Continuity, Backup & Recovery 208
30.22 **S22** Data Security & Loss Prevention 209

31 **Hacking & Adversary Testing Agents** 210

HACK

31.1 **H1** Reconnaissance 211
31.2 **H2** Penetration Testing & Attack-Path Validation 212
31.3 **H3** Identity & Credential Attack Testing 213
31.4 **H4** Wireless & RF Security Testing 214
31.5 **H5** Social Engineering & Security Awareness 215
31.6 **H6** Red Team & Purple Team Exercises 216

32 **Governance, Audit & Assurance Agents** 217

AUDIT

32.1 **A1** Cyber Governance & Third-Party Risk 218
32.2 **A2** Security Controls Audit & Compliance Assessment 219
32.3 **A3** ISO/IEC 27001 & ISMS Audit 220
32.4 **A4** PCI DSS Assessment 221
32.5 **A5** SOC 2 Readiness & Evidence Assessment 222
32.6 **A6** AI Governance & Management-System Assurance 223

PART IX **Going Full 360**

33 **The Capstone Assessment** 224

BUILD · HACK · INVESTIGATE · SECURE · AUDIT · REPORT

33.1 The Brief: Code, Applications, Infrastructure, Logs and Evidence 224
33.2 Assessing the Environment 225
33.3 Identifying and Validating Vulnerabilities 225
33.4 Authorised Hacking 225
33.5 Investigating Simulated Incidents 225
33.6 Securing Systems and Verifying Fixes 226
33.7 Performing the Structured Security Audit 226
33.8 Writing the Final Report 226
33.9 How the Work Is Assessed 226

APPENDICES

Glossary 228