

Table of Contents

Chapter I: Why Ethical Hacking?	1
1.1 You	2
1.2 Me.....	3
1.3 Ethical Hacking	7
Chapter II: Essential Terms and Concepts	19
2.1 Types of Ethical Hackers	19
2.2 Definitions and Typology of Ethical Hacking	21
2.3 Conventional Computer-Security-Threat Model	22
2.4 Common Methods Used in Ethical Hacking	23
2.5 Other Relevant Terms	30
Chapter III: Methodology and Quantitative Studies of Ethical Hacking: Evidence-Based Decision and Policy-Making	35
3.1 Report for Public Safety Canada, 2011	35
3.2 Summary of Findings	38
3.3 GDELT Analysis Service—Event Data (with Kevin Kim)	40
3.4 Google’s BigQuery (with Richard Li).....	43
3.5 Dark-Net Analysis of Malware and Cyber-Jihad Forums	45
3.5.1 Cyber-Jihad Forums (with Adrian Agius).....	45
3.5.2 Hacking Forums (with Richard Li)	50
3.6 Observations	55
Chapter IV: Legal Cases Around the World (with Jelena Ardalic).....	57
Chapter V: Select Ethical-Hacking Incidences: Anonymous	97
Chapter VI: Select Ethical-Hacking Incidences: Chaos Computer Club, CyberBerkut, LulzSec, Iranian Cyber Army, and Others	137

Chapter VII: Online Civil Disobedience..... 195

7.1	Online Civil Disobedience in Context	196
7.2	Timeline.....	200
7.3	Case Studies	201
7.3.1	Anonymous, Operation Titstorm	202
7.3.2	German Lufthansa Protest	205
7.3.3	Twitter #TellVicEverything Campaign	206
7.4	Observations	207

Chapter VIII: Hacktivism 211

8.1	Hacktivism in Context	211
8.2	Timelines	212
8.3	Case Studies	216
8.3.1	Anonymous, Post-Christmas Charity Donations.....	216
8.3.2	Neo-Nazi Website.....	217
8.3.3	WikiLeaks, Operation Payback.....	217
8.4	Observations	219

Chapter IX: Penetration/Intrusion Testing and Vulnerability

Disclosure 223

9.1	Penetration Testing and Vulnerability Disclosure in Context	223
9.2	Timeline.....	225
9.3	Case Studies	227
9.3.1	Australian Security Expert Patrick Webster	227
9.3.2	Cisco Router	228
9.3.3	LulzSec Hacking to Incentivize Sony to Fix Known Software Bugs	230
9.3.4	Guardians of Peace, North Korea, and the Sony Pictures Hack	231
9.3.5	Vulnerability Hunter Glenn Mangham	231
9.3.6	Da Jiang Innovation	233
9.4	Observations	233

Chapter X: Counterattack/Hackback 237

10.1	Counterattack/Hackback in Context	238
10.2	Case Studies	241
10.2.1	LulzSec, MasterCard and PayPal, and Barr.....	242

10.2.2	Illegal Streaming Link Sites	243
10.2.3	Automated Counter-DDoS	244
10.3	The Legalization of Hackback	245
10.4	Observations	248

Chapter XI: Security Activism 253

11.1	Security Activism in Context.....	253
11.2	Case Studies	254
11.2.1	Spamhaus Project	254
11.2.2	Spam Fighter	254
11.2.3	Botnet Removal Communities	256
11.2.4	Cyber-Security Researcher Y	258
11.3	Observations	259

Chapter XII: Ethical-Hacking Challenges in Legal Frameworks, Investigation, Prosecution, and Sentencing 263

12.1	Criminal Landscape: Convention on Cybercrime and the Canadian Criminal Framework	264
12.2	Attribution	267
12.3	Jurisdiction.....	269
12.4	Evidence	271
12.5	Integrity, Volatility of Evidence, and the Trojan-Horse Defence	272
12.6	Damages	274
12.7	Sentencing and Dealing with Mental Disorders—Addiction and Autism Spectrum (with PhD candidate Hannah Rappaport)	274
12.8	Observations	279

Chapter XIII: Ethical Hacking, Whistle-Blowing, and Human Rights and Freedoms 287

13.1	The Canadian Charter of Human Rights and Freedoms.....	288
13.2	Whistle-Blowing and Ethical Hacking	294
13.3	Observations	295

Chapter XIV: Toward an Ethical-Hacking Framework	299
14.1 Ethical Hacking in Context	299
14.2 Encourage Legitimate Space for Virtual Protests	301
14.3 Guidelines and Policy	302
14.4 Code of Conduct for Hackback	303
14.5 Transparency of Government Engagement with Hackback	305
14.6 Security Research Exemption and Public-Interest Consideration	305
14.7 Concluding Remarks.....	306
Bibliography.....	309
Appendix: Interview Questions	357