

Table of Contents

Preface	1
<hr/>	
Chapter 1: Security Posture	7
<hr/>	
The current threat landscape	7
The credentials – authentication and authorization	11
Apps	12
Data	14
Cybersecurity challenges	15
Old techniques and broader results	15
The shift in the threat landscape	16
Enhancing your security posture	17
The Red and Blue Team	19
Assume breach	22
References	23
Summary	25
<hr/>	
Chapter 2: Incident Response Process	27
<hr/>	
Incident response process	27
Reasons to have an IR process in place	28
Creating an incident response process	30
Incident response team	33
Incident life cycle	34
Handling an incident	35
Best practices to optimize incident handling	38
Post-incident activity	38
Real-world scenario	38
Lessons learned	40
Incident response in the cloud	41
Updating your IR process to include cloud	42
References	42
Summary	43
<hr/>	
Chapter 3: Understanding the Cybersecurity Kill Chain	45
<hr/>	
External reconnaissance	45
Scanning	47
NMap	47

Metasploit	49
John the Ripper	50
THC Hydra	51
Wireshark	52
Aircrack-ng	53
Nikto	55
Kismet	56
Cain and Abel	57
Access and privilege escalation	58
Vertical privilege escalation	58
Horizontal privilege escalation	59
Exfiltration	59
Sustainment	60
Assault	61
Obfuscation	62
Threat life cycle management	63
References	66
Summary	68
Chapter 4: Reconnaissance	69
<hr/>	
External reconnaissance	70
Dumpster diving	70
Social media	71
Social engineering	72
Pretexting	73
Diversion theft	73
Phishing	74
Phone phishing (vishing)	75
Spear phishing	76
Water holing	77
Baiting	77
Quid pro quo	78
Tailgating	78
Internal reconnaissance	79
Sniffing and scanning	79
Prismdump	80
tcpdump	81
NMap	81
Wireshark	83
Scanrand	84
Cain and Abel	85
Nessus	85
Metasploit	86
Aircrack-ng	88

Wardriving	89
Conclusion of the reconnaissance chapter	89
References	90
Summary	92
Chapter 5: Compromising the System	93
<hr/>	
Analyzing current trends	94
Extortion attacks	94
Data manipulation attacks	95
IoT device attacks	97
Backdoors	97
Mobile device attacks	98
Hacking everyday devices	98
Hacking the cloud	100
Phishing	101
Exploiting a vulnerability	104
Zero-day	104
Fuzzing	105
Source code analysis	105
Types of zero-day exploits	106
Buffer overflows	107
Structured exception handler overwrites	107
Performing the steps to compromise a system	108
Deploying payloads	108
Installing and using a vulnerability scanner	108
Using Metasploit	109
Compromising operating systems	111
Compromising systems using Kon-Boot or Hiren's BootCD	111
Compromising systems using a Linux Live CD	113
Compromising systems using preinstalled applications	114
Compromising systems using Ophcrack	115
Compromising a remote system	116
Compromising web-based systems	117
SQL injection	117
Cross-site scripting	118
Broken authentication	118
DDoS attacks	119
References	120
Summary	122
Chapter 6: Chasing a User's Identity	123
<hr/>	
Identity is the new perimeter	123

Strategies for compromising a user's identity	126
Gaining access to the network	128
Harvesting credentials	128
Hacking a user's identity	130
Brute force	131
Social engineering	132
Pass the hash	140
Other methods to hack identity	142
References	142
Summary	143
Chapter 7: Lateral Movement	145
<hr/>	
Infiltration	146
Network mapping	146
Avoiding alerts	148
Performing lateral movement	149
Port scans	149
Sysinternals	150
File shares	153
Remote Desktop	154
PowerShell	155
Windows Management Instrumentation	156
Scheduled tasks	158
Token stealing	158
Pass-the-hash	159
Active Directory	159
Remote Registry	160
Breached host analysis	161
Central administrator consoles	161
Email pillaging	162
References	162
Summary	163
Chapter 8: Privilege Escalation	165
<hr/>	
Infiltration	166
Horizontal privilege escalation	166
Vertical privilege escalation	167
Avoiding alerts	167
Performing privilege escalation	168
Exploiting unpatched operating systems	169

Access token manipulation	170
Exploiting accessibility features	171
Application shimming	172
Bypassing user account control	177
DLL injection	178
DLL search order hijacking	179
Dylib hijacking	180
Exploration of vulnerabilities	181
Launch daemon	182
Hands-on example of privilege escalation on a Windows 8 target	182
Conclusion and lessons learned	184
References	184
Summary	185
Chapter 9: Security Policy	187
<hr/>	
Reviewing your security policy	187
Educating the end user	189
Social media security guidelines for users	190
Security awareness training	191
Policy enforcement	191
Application whitelisting	194
Hardening	195
Monitoring for compliance	200
References	204
Summary	204
Chapter 10: Network Segmentation	207
<hr/>	
Defense in depth approach	207
Infrastructure and services	209
Documents in transit	209
Endpoints	212
Physical network segmentation	212
Discovering your network	215
Securing remote access to the network	217
Site-to-site VPN	219
Virtual network segmentation	220
Hybrid cloud network security	222
References	225
Summary	225
Chapter 11: Active Sensors	227

Detection capabilities	228
Indicators of compromise	229
Intrusion detection systems	232
Intrusion prevention system	234
Rule-based detection	235
Anomaly-based detection	236
Behavior analytics on-premises	236
Device placement	240
Behavior analytics in a hybrid cloud	240
Azure Security Center	241
References	246
Summary	247
Chapter 12: Threat Intelligence	249
<hr/>	
Introduction to threat intelligence	249
Open source tools for threat intelligence	253
Microsoft threat intelligence	258
Azure Security Center	259
Leveraging threat intelligence to investigate suspicious activity	261
References	265
Summary	266
Chapter 13: Investigating an Incident	267
<hr/>	
Scoping the issue	267
Key artifacts	268
Investigating a compromised system on-premises	274
Investigating a compromised system in a hybrid cloud	279
Search and you shall find it	287
Lessons learned	288
References	288
Summary	289
Chapter 14: Recovery Process	291
<hr/>	
Disaster recovery plan	292
The disaster recovery planning process	292
Forming a disaster recovery team	293
Performing risk assessment	294
Prioritizing processes and operations	294
Determining recovery strategies	294
Collecting data	295
Creating the disaster recovery plan	295
Testing the plan	295

Obtaining approval	295
Maintaining the plan	296
Challenges	296
Live recovery	297
Contingency planning	298
IT contingency planning process	299
Development of the contingency planning policy	300
Conducting business impact analysis	300
Identifying the critical IT resources	301
Identifying disruption impacts	301
Developing recovery priorities	301
Identifying the preventive controls	302
Developing recovery strategies	302
Backups	302
Alternative sites	303
Equipment replacement	305
Plan testing, training, and exercising	305
Plan maintenance	306
Best practices for recovery	306
References	306
Summary	307
Chapter 15: Vulnerability Management	309
Creating a vulnerability management strategy	310
Asset inventory	310
Information management	311
Risk assessment	312
Scope	312
Collecting data	313
Analysis of policies and procedures	313
Vulnerability analysis	313
Threat analysis	314
Analysis of acceptable risks	314
Vulnerability assessment	315
Reporting and remediation tracking	316
Response planning	317
Vulnerability management tools	318
Asset inventory tools	318
Peregrine tools	319
LANDesk Management Suite	319
StillSecure	320
Foundstone's Enterprise	320
Information management tools	321
Risk assessment tools	322

Vulnerability assessment tools	323
Reporting and remediation tracking tools	324
Response planning tools	324
Implementation of vulnerability management	325
Best practices for vulnerability management	327
Implementing vulnerability management with Nessus	329
Flexera (Secunia) Personal Software Inspector	339
Conclusion	342
References	342
Summary	343
Chapter 16: Log Analysis	345
<hr/>	
Data correlation	345
Operating system logs	347
Windows logs	347
Linux logs	350
Firewall logs	351
Web server logs	353
References	354
Summary	354
Other Books You May Enjoy	357
<hr/>	
Index	361
<hr/>	