

Table of Contents

Preface	xiii
Chapter 1: Security Posture	1
The current threat landscape	1
The credentials – authentication and authorization	5
Apps	6
Data	8
Cybersecurity challenges	9
Old techniques and broader results	9
The shift in the threat landscape	10
Enhancing your security posture	12
Cloud Security Posture Management	13
The Red and Blue Teams	14
Assume breach	17
Summary	18
References	19
Chapter 2: Incident Response Process	21
The incident response process	21
Reasons to have an IR process in place	22
Creating an incident response process	24
Incident response team	27
Incident life cycle	28
Handling an incident	28
Best practices to optimize incident handling	31
Post-incident activity	31
Real-world scenario	32
Lessons learned	33

Incident response in the cloud	34
Updating your IR process to include cloud	35
Appropriate toolset	35
IR Process from the Cloud Solution Provider (CSP) perspective	36
Summary	36
References	37
Chapter 3: What is a Cyber Strategy?	39
Introduction	39
Why do we need to build a cyber strategy?	39
How to build a cyber strategy	41
Understand the business	42
Understand threats and risks	42
Document	43
Best cyber attack strategies (Red Team)	44
External testing strategies	44
Internal testing strategies	44
Blind testing strategy	45
Targeted testing strategy	45
Best cyber defense strategies (Blue Team)	45
Defense in depth	45
Defense in breadth	47
Summary	48
Further reading	48
Chapter 4: Understanding the Cybersecurity Kill Chain	49
Introducing the Cyber Kill Chain	50
Reconnaissance	51
Weaponization	52
Privilege Escalation	52
Vertical privilege escalation	53
Horizontal privilege escalation	54
Exfiltration	54
Sustainment	57
Assault	58
Obfuscation	60
Obfuscation Techniques	61
Dynamic code obfuscation	62
Hiding Trails	62
Threat Life Cycle Management	64
Data Collection Phase	65
Discovery Phase	65
Qualification Phase	66

Investigation Phase	66
Neutralization Phase	67
Recovery Phase	67
Shared files	67
Tools used in the Cyber Kill Chain Phases	68
Nmap	68
Zenmap	69
Metasploit	70
John the Ripper	71
Hydra	72
Wireshark	73
Aircrack-ng	74
Nikto	76
Kismet	77
Airedddon	78
Deauther Board	79
Mitigations against wireless attacks	80
EvilOSX	81
Cybersecurity Kill Chain Summary	82
Lab – Hacking Wireless Network/s via Evil Twin Attack	83
The Lab Scenario	83
Step 1 – Ensure you have all required hardware and software for the "simulated attack"	84
Step 2 – Install Airedddon in Kali	84
Step 3 – Configure Airedddon	86
Step 4 – Select target	88
Step 5 – Gathering the handshake	89
Step 6 – Set the phishing page	93
Step 7 – Capturing the network credentials	94
Lab Summary	95
References	95
Further Reading	97
Chapter 5: Reconnaissance	99
External reconnaissance	100
Webshag	100
PhonelInfoga	103
Email harvester – TheHarvester	104
Web Browser Enumeration Tools	106
Penetration Testing Kit	106
Netcraft	107
Dumpster diving	107

Social media	108
Social engineering	111
Pretexting	112
Diversion theft	113
Phishing	113
Keepnet Labs	117
Water holing	120
Baiting	121
Quid pro quo	122
Tailgating	122
Internal reconnaissance	123
Airgraph-ng	124
Sniffing and scanning	125
Prismdump	126
Tcpcat	127
Nmap	127
Wireshark	128
Scanrand	130
Masscan	130
Cain and Abel	130
Nessus	131
Metasploit	132
Aircrack-ng	134
Wardriving	134
Hak5 Plunder Bug	136
CATT	137
Canary token links	138
Summary	139
LAB	140
Google Hacking:	140
Part 1: Hacking personal information	140
Part 2: Hacking Servers	149
References	152
Chapter 6: Compromising the System	155
Analyzing current trends	156
Extortion attacks	157
Data manipulation attacks	159
IoT device attacks	160
Backdoors	162
Mobile device attacks	163
Hacking everyday devices	164
Hacking the cloud	165
The appeal of cloud attacks	167
Cloud Hacking Tools	168

CloudTracker	173
OWASP DevSlop Tool	174
Cloud security recommendations	174
Phishing	175
Exploiting a vulnerability	178
Hot Potato	179
Zero-day	180
WhatsApp vulnerability (CVE-2019-3568)	180
Chrome zero-day vulnerability (CVE-2019-5786)	182
Windows 10 Privilege escalation	182
Windows privilege escalation vulnerability (CVE20191132)	182
Fuzzing	183
Source code analysis	184
Types of zero-day exploits	185
Buffer overflows	186
Structured exception handler overwrites	186
Performing the steps to compromise a system	187
Deploying payloads	188
Installing and using a vulnerability scanner	188
Using Metasploit	189
Compromising operating systems	192
Compromising a remote system	197
Compromising web-based systems	199
Mobile phone (iOS / Android attacks)	206
Exodus	206
SensorID	208
iPhone hack by Cellebrite	209
Man-in-the-disk	210
Spearphone (loudspeaker data capture on Android)	211
Tap n Ghost	211
Red and Blue Team Tools for Mobile Devices	212
Snoopdroid	212
Androguard	213
Frida	213
Cycrypt	214
iOS Implant Teardown	215
Lab	216
Building a Red Team PC in Windows	216
Lab 2: Hack those websites (legally!)	221
bWAPP	222
HackThis!!	222
OWASP Juice Shop Project	222
Try2Hack	222

Google Gruyere	223
Damn Vulnerable Web Application (DVWA)	224
Summary	225
References	226
Further reading	228
Chapter 7: Chasing a User's Identity	229
Identity is the new perimeter	229
Strategies for compromising a user's identity	232
Gaining access to the network	234
Harvesting credentials	234
Hacking a user's identity	236
Brute force	237
Social engineering	239
Pass the hash	245
Identity theft through mobile devices	247
Other methods for hacking an identity	247
Summary	248
References	248
Chapter 8: Lateral Movement	251
Infiltration	252
Network mapping	252
Avoiding alerts	254
Performing lateral movement	255
Think like a Hacker	257
Port scans	258
Sysinternals	259
File shares	262
Windows DCOM	264
Remote Desktop	265
PowerShell	267
Windows Management Instrumentation	269
Scheduled tasks	271
Token stealing	271
Stolen credentials	272
Removable media	272
Tainted Shared Content	273
Remote Registry	273
TeamViewer	273
Application deployment	274
Network Sniffing	274

ARP spoofing	275
AppleScript and IPC (OS X)	276
Breached host analysis	276
Central administrator consoles	276
Email pillaging	277
Active Directory	277
Admin shares	279
Pass the ticket	280
Pass the hash (PtH)	280
Winlogon	282
Lsass.exe Process	283
Security Accounts Manager (SAM) database	283
Domain Active Directory Database (NTDS.DIT):	283
Credential Manager (CredMan) store:	284
PtH Mitigation Recommendations	284
Lab	286
Hunting Malware without antivirus	286
Summary	300
References	300
Further Reading	301
Chapter 9: Privilege Escalation	303
Infiltration	304
Horizontal privilege escalation	304
Vertical Privilege Escalation	305
Avoiding alerts	306
Performing Privilege Escalation	307
Exploiting unpatched operating systems	310
Access token manipulation	311
Exploiting accessibility features	313
Application shimming	314
Bypassing user account control	319
DLL injection	321
DLL search order hijacking	323
Dylib hijacking	324
Exploration of vulnerabilities	325
Launch daemon	326
Hands-on example of Privilege Escalation on a Windows target	327
Privilege escalation techniques	329
Dumping the SAM file	330
Rooting Android	331
Using the /etc/passwd file	333

Extra window memory injection	333
Hooking	334
New services	334
Scheduled tasks	335
Windows Boot Sequence	335
Startup items	337
Startup 101	337
Sudo caching	345
Additional tools for privilege escalation	346
Oxsp Mongoose v1.7	346
Conclusion and lessons learned	347
Summary	347
Lab 1	348
Lab 2	356
Part 1 – Retrieving passwords from LSASS	356
Part 2 – Dumping Hashes with PowerSploit	361
Lab 3: HackTheBox	366
References	374
Chapter 10: Security Policy	377
Reviewing your security policy	377
Educating the end user	379
Social media security guidelines for users	380
Security awareness training	381
Policy enforcement	381
Application whitelisting	383
Hardening	386
Monitoring for compliance	391
Continuously driving security posture enhancement via security policy	395
Summary	397
References	397
Chapter 11: Network Segmentation	399
The defense in depth approach	399
Infrastructure and services	401
Documents in transit	401
Endpoints	404
Physical network segmentation	404
Discovering your network	407
Securing remote access to the network	409
Site-to-site VPN	411
Virtual network segmentation	412

Zero trust network	415
Planning zero trust network adoption	416
Hybrid cloud network security	417
Cloud network visibility	419
Summary	422
References	423
Chapter 12: Active Sensors	425
Detection capabilities	425
Indicators of compromise	427
Intrusion detection systems	429
Intrusion prevention system	432
Rule-based detection	432
Anomaly-based detection	433
Behavior analytics on-premises	433
Device placement	437
Behavior analytics in a hybrid cloud	437
Azure Security Center	438
Analytics for PaaS workloads	442
Summary	444
References	444
Chapter 13: Threat Intelligence	445
Introduction to threat intelligence	445
Open source tools for threat intelligence	450
Free threat intelligence feeds	455
Microsoft threat intelligence	460
Azure Sentinel	460
Leveraging threat intelligence to investigate suspicious activity	463
Summary	466
References	467
Chapter 14: Investigating an Incident	469
Scoping the issue	469
Key artifacts	470
Investigating a compromised system on-premises	476
Investigating a compromised system in a hybrid cloud	479
Integrating Azure Security Center with your SIEM for Investigation	487
Proactive investigation (threat hunting)	491
Lessons learned	493
Summary	494
References	494

Chapter 15: Recovery Process	495
Disaster recovery plan	496
The disaster recovery planning process	496
Forming a disaster recovery team	497
Performing risk assessment	497
Prioritizing processes and operations	498
Determining recovery strategies	499
Collecting data	499
Creating the DR plan	499
Testing the plan	499
Obtaining approval	500
Maintaining the plan	500
Challenges	501
Contingency planning	501
IT contingency planning process	502
Development of the contingency planning policy	502
Conducting business impact analysis	503
Identifying the preventive controls	504
Business continuity vs Disaster recovery	505
Developing recovery strategies	506
Live recovery	509
Plan maintenance	510
Cyber Incident Recovery Examples from the field	511
Risk management tools	512
RiskNAV	512
IT Risk Management App	513
Best practices for recovery planning	514
Disaster recovery best practices	515
On-Premises	515
On the cloud	516
Hybrid	516
Cyber-resilient recommendations	517
Summary	518
Resources for DR Planning	519
References	519
Further Reading:	520
Chapter 16: Vulnerability Management	521
Creating a vulnerability management strategy	521
Asset inventory	522
Information management	523
Risk assessment	524
Scope	525
Collecting data	526
Analysis of policies and procedures	526
Vulnerability analysis	526

Threat analysis	527
Analysis of acceptable risks	528
Vulnerability assessment	528
Reporting and remediation tracking	530
Response planning	532
Vulnerability management tools	533
Asset inventory tools	533
Peregrine tools	533
LANDesk Management Suite	534
StillSecure	534
McAfee's Enterprise	535
Information management tools	536
Risk assessment tools	537
Vulnerability assessment tools	537
Reporting and remediation tracking tools	538
Response planning tools	539
Implementation of vulnerability management	539
Best practices for vulnerability management	541
Vulnerability management tools	543
Intruder	543
Patch Manager Plus	544
InsightVM	545
Azure Threat & Vulnerability Management	546
Implementing vulnerability management with Nessus	547
OpenVAS	554
Qualys	555
Acunetix	556
LABS	557
Lab 1: Performing an online vulnerability scan with Acunetix	557
Lab 2: Network security scan with GFI LanGuard	567
Summary	571
References	572
Chapter 17: Log Analysis	575
Data correlation	575
Operating system logs	577
Windows logs	577
Linux logs	579
Firewall logs	581
Web server logs	582
Amazon Web Services (AWS) logs	584
Accessing AWS logs from Azure Sentinel	586

Azure Activity logs	587
Accessing Azure Activity logs from Azure Sentinel	588
Summary	590
References	591
Other Books You May Enjoy	593
Index	597
