

Third Edition

HANDS-ON INFORMATION SECURITY LAB MANUAL

Michael E. Whitman and Herbert J. Mattord



PREPARING TOMORROW'S
INFORMATION
SECURITY
PROFESSIONALS

TABLE OF Contents

CHAPTER 1: INFORMATION SECURITY PROCESS FLOWS	1
Flow 1.1 Firewalls	3
Flow 1.2 Remote Access	3
Flow 1.3 Access Controls	4
Flow 1.4 Vulnerability Assessment	5
Flow 1.5 Penetration Testing	6
Flow 1.6 Forensics and Antiforensics	7
Flow 1.7 Client Security	8
Flow 1.8 Perimeter Defense	10
Flow 1.9 Server Security	11
Flow 1.10 Intrusion Detection	12
Flow 1.11 Network Security	13
Flow 1.12 Cyber Defense	14
References	15
 CHAPTER 2: BACKGROUND AND THEORY FOR LAB EXERCISES	 17
2.1 Footprinting	18
2.2 Scanning and Enumeration	22
2.3 OS Processes and Services	25
2.4 Vulnerability Identification and Research	26
2.5 Vulnerability Validation	28
2.6 Systems Remediation and Hardening	28
2.7 Web Browser Security and Configuration	29
2.8 Data Management	30
2.9 Data Backup and Recovery	31
2.10 Access Controls	31
2.11 Host Intrusion Detection	33
2.12 Log Security Issues	34
2.13 Privacy and Anti-forensics	36
2.14 Software Firewalls	36
2.15 Linksys Firewalls Routers and Access Points	38
2.16 Network Intrusion Detection Systems	38
2.17 Network Traffic Analysis	39
2.18 Virtual Private Networks and Remote Access	41
2.19 Digital Certificates	41
2.20 Password Circumvention	43
2.21 Antivirus Defense	43
2.22 Malware Prevention and Detection	44
 CHAPTER 3: WINDOWS LABS	 47
Lab 3.1 Footprinting Using Windows	48
Lab 3.2 Scanning and Enumeration Using Windows	73
Lab 3.3 Windows OS Processes and Services	81
Lab 3.4 Vulnerability Identification and Research Using Windows	91
Lab 3.5 Vulnerability Validation Using Windows	105
Lab 3.6 System Remediation and Hardening Using Windows	113
Lab 3.7 Windows Web Browser Security and Configuration	141
Lab 3.8 Data Management Using Windows	157
Lab 3.9 Data Backup and Recovery Using Windows	171
Lab 3.10 Access Controls Using Windows	185
Lab 3.11 Host Intrusion Detection Using Windows	201
Lab 3.12 Log Security Issues Using Windows	211
Lab 3.13 Windows Privacy and Antiforensics Issues	223

Lab 3.14 Software Firewalls Using Windows	235
Lab 3.15 Linksys Firewall Routers and Access Points	251
Lab 3.16 Network Intrusion Detection Systems Using Windows	273
Lab 3.17 Network Traffic Analysis Using Windows	285
Lab 3.18 Virtual Private Networks and Remote Access Using Windows	301
Lab 3.19 Digital Certificates Using Windows	315
Lab 3.20 Password Circumvention Using Windows	323
Lab 3.21 Antivirus Using Windows	331
Lab 3.22 Malware Prevention and Detection Using Windows	347

CHAPTER 4: LINUX LABS 361

Lab 4.1 Footprinting Using Linux	362
Lab 4.2 Scanning and Enumeration Using Linux	373
Lab 4.3 Linux OS Processes and Services	383
Lab 4.4 Vulnerability Identification and Research Using Linux	395
Lab 4.5 Vulnerability Validation Using Linux	401
Lab 4.6 System Remediation and Hardening Using Linux	409
Lab 4.7 Linux Web Browser Security	419
Lab 4.8 Data Management Using Linux	427
Lab 4.9 Data Management Using Linux	433
Lab 4.10 Access Controls Using Linux	443
Lab 4.11 Host Intrusion Detection Using Linux	455
Lab 4.12 Log and Security Using Linux	461
Lab 4.13 Privacy and Antiforensics Issues Using Linux	467
Lab 4.14 Software Firewalls Using Linux	471
Lab 4.15 Linksys Firewall Routers and Access Points	483
Lab 4.16 Network Intrusion Detection Systems Using Linux	485
Lab 4.17 Network Traffic Analysis Using Linux	493
Lab 4.18 Virtual Private Networks and Remote Access Using Linux	505
Lab 4.19 Digital Certificates Using Linux	511
Lab 4.20 Password Circumvention Using Linux	523
Lab 4.21 Antivirus Using Linux	533
Lab 4.22 Malware Prevention and Detection	541

INDEX 545