

PRACTICAL HACKING TECHNIQUES AND COUNTERMEASURES

Mark D. Spivey, CISSP



Auerbach Publications
Taylor & Francis Group

Contents

- 1 Preparation 1**
 - Installing VMware Workstation 3
 - Configuring Virtual Machines 10
 - Installing a Virtual Windows 2000 Workstation 11
 - Installing VMware Tools for Windows 2000 Virtual Machines 29
 - Installing a Red Hat Version 8 Virtual Machine 35
 - Installing VMware Tools for Red Hat Virtual Machines 55
 - What Is on the CD? 60
 - Restrict Anonymous 60
 - To Restrict Anonymous 60
 - In Windows NT 60
 - For Windows XP, 2003 60
 - For Windows 2000 61
 - What Is the Difference? 61

- 2 Banner Identification 63**
 - Lab 1: Banner Identification 65
 - Lab 2: Banner Identification 67
 - Lab 3: Banner Identification 73
 - Lab 4: Operating System Identification 75
 - Detect Operating System of Target: Xprobe2* 79
 - Lab 5: Banner Identification 84
 - Lab 6: Banner Identification 84
 - Lab 7: Personal Social Engineering 86
 - Social Engineering Techniques: Dumpster Diving/Personnel*

3	Target Enumeration	87
Lab 8:	Establish a NULL Session.....	89
	<i>Establish a NULL Session: NULL Session</i>	
Lab 9:	Enumerate Target MAC Address.....	90
	<i>Enumerate MAC Address and Total NICs: GETMAC</i>	
Lab 10:	Enumerate SID from User ID	91
	<i>Enumerate the SID from the Username: USER2SID</i>	
Lab 11:	Enumerate User ID from SID	93
	<i>Enumerate the Username from the Known SID: SID2USER</i>	
Lab 12:	Enumerate User Information	96
	<i>Enumerate User Information from Target: USERDUMP</i>	
Lab 13:	Enumerate User Information	97
	<i>Exploit Data from Target Computer: USERINFO</i>	
Lab 14:	Enumerate User Information	98
	<i>Exploit User Information from Target: DUMPSEC</i>	
Lab 15:	Host/Domain Enumeration	102
	<i>Enumerate Hosts and Domains of LAN: Net Commands</i>	
Lab 16:	Target Connectivity/Route	105
	<i>Detect Target Connectivity: PingG</i>	
Lab 17:	Target Connectivity/Route	107
	<i>Connectivity/Routing Test: Pathping</i>	
Lab 18:	Operating System Identification.....	109
	<i>Identify Target Operating System: Nmap/nmapFE</i>	
Lab 19:	Operating System Identification.....	117
	<i>Identify Target Operating System: NmapNT</i>	
Lab 20:	IP/Hostname Enumeration	123
	<i>Enumerate IP or Hostname: Nslookup</i>	
Lab 21:	IP/Hostname Enumeration	124
	<i>Enumerate IP or Hostname: Nmblookup</i>	
Lab 22:	RPC Reporting.....	125
	<i>Report the RPC of Target: Rpcinfo</i>	
Lab 23:	Location/Registrant Identification	126
	<i>Gather Registration Info/Trace Visual Route: Visual Route</i>	
Lab 24:	Registrant Identification	128
	<i>Gather IP or Hostname: Sam Spade</i>	
Lab 25:	Operating System Identification.....	131
	<i>Gather OS Runtime and Registered IPs: Netcraft</i>	
Lab 26:	Operating System Identification.....	133
	<i>Scan Open Ports of Target: Sprint</i>	
Lab 27:	Default Shares	135
	<i>Disable Default Shares: Windows Operating System</i>	
Lab 28:	Host Enumeration.....	139
	<i>Scan Open Ports of Target: WinFingerprint</i>	
4	Scanning.....	145
Lab 29:	Target Scan/Share Enumeration	147
	<i>Scan Open Ports of Target: Angry IP</i>	

Lab 30: Target Scan/Penetration	151
<i>Scan Open Ports/Penetration Testing: LANguard</i>	
Lab 31: Target Scan through Firewall	153
<i>Scan Open Ports of Target: Fscan</i>	
Lab 32: Passive Network Discovery	154
<i>Passively Identify Target Information on the LAN: Passifist</i>	
Lab 33: Network Discovery	158
<i>Identify Target Information: LanSpy</i>	
Lab 34: Open Ports/Services	161
<i>Scan Open Ports/Services of Target: Netcat</i>	
Lab 35: Port Scan/Service Identification	163
<i>Scan Open Ports of Target: SuperScan</i>	
Lab 36: Port Scanner	166
<i>Identify Ports Open: Strobe</i>	
Lab 37: Anonymous FTP Locator	169
<i>Locate Anonymous FTP Servers: FTPScanner</i>	
Lab 38: CGI Vulnerability Scanner	171
<i>Identify CGI Vulnerabilities: TCS CGI Scanner</i>	
Lab 39: Shared Resources Locator	178
<i>Identify Open Shared Resources: Hydra</i>	
Lab 40: Locate Wingate Proxy Servers	187
<i>Locate Wingate Proxy Servers: WGateScan/ADM Gates</i>	
5 Sniffing Traffic	193
Lab 41: Packet Capture — Sniffer	195
<i>Exploit Data from Network Traffic: Ethereal</i>	
To Install Ethereal on a Red Hat Linux Computer	196
To Install Ethereal on Microsoft Windows	206
Lab 42: Packet Capture — Sniffer	213
<i>Exploit Data from Network Traffic: Ngrep</i>	
For Linux	213
For Windows	219
Lab 43: Packet Capture — Sniffer	223
<i>Exploit Data from Network Traffic: TcpDump</i>	
Lab 44: Packet Capture — Sniffer	230
<i>Exploit Data from Network Traffic: WinDump</i>	
Lab 45: Packet Capture — Sniffer	234
<i>Monitor IP Network Traffic Flow: IPDump2</i>	
For Linux	234
For Windows	237
Lab 46: Password Capture — Sniffer	240
<i>Exploit Passwords and Sniff the Network: ZxSniffer</i>	
Lab 47: Exploit Data from Target Computer — Sniffit	249
6 Spoofing	261
Lab 48: Spoofing IP Addresses	263
<i>Send Packets via False IP Address: RafaleX</i>	
Lab 49: Spoofing MAC Addresses	268
<i>Send Packets via a False MAC Address: SMAC</i>	

Lab 50: Spoofing MAC Addresses	277
<i>Send Packets via a False MAC Address: Linux</i>	
Lab 51: Packet Injection/Capture/Trace.....	284
<i>Send Packets via a False IP/MAC Address: Packet</i>	
Lab 52: Spoof MAC Address	295
<i>Altering the MAC Address: VMware Workstation</i>	
7 Brute Force	299
Lab 53: Brute-Force FTP Server.....	301
<i>Crack an FTP Password: NETWOX/NETWAG</i>	
Lab 54: Retrieve Password Hashes	309
<i>Extract Password Hashes: FGDump</i>	
Lab 55: Crack Password Hashes	313
<i>Crack and Capture Password Hashes: LC5</i>	
Lab 56: Overwrite Administrator Password.....	325
<i>Change the Administrator Password: CHNTPW</i>	
Lab 57: Brute-Force Passwords.....	337
<i>Brute-Force Passwords for a Hashed File: John the Ripper</i>	
Lab 58: Brute-Force FTP Password.....	346
<i>Brute-Force an FTP Password Connection: BruteFTP</i>	
Lab 59: Brute-Force Terminal Server	354
<i>Brute-Force Terminal Server Passwords: TSGrinder II</i>	
8 Vulnerability Scanning	357
Lab 60: Vulnerability Scanner	359
<i>Perform Vulnerability Assessment: SAINT</i>	
Lab 61: SNMP Walk.....	379
<i>Exploit Data via SNMP Walk: NETWOX/NETWAG</i>	
Lab 62: Brute-Force Community Strings	386
<i>Exploit the SNMP Community Strings: Solar Winds</i>	
Lab 63: Target Assessment	392
<i>Assessment of Target Security: Retina</i>	
Lab 64: Target Assessment	397
<i>Assessment of Target Security: X-Scan</i>	
Lab 65: Vulnerability Scanner	402
<i>Perform Vulnerability Assessment: SARA</i>	
Lab 66: Web Server Target Assessment.....	414
<i>Assessment of Web Server Security: N-Stealth</i>	
Lab 67: Vulnerability Scanner	421
<i>Exploit Data from Target Computer: Pluto</i>	
Lab 68: Vulnerability Assessment.....	429
<i>Perform Vulnerability Assessment: Metasploit</i>	
On Windows.....	429
On Linux	441
Lab 69: Web Server Target Assessment.....	451
<i>Assessment of Web Server Security: Nikto</i>	
Lab 70: Vulnerability Scanner	455
<i>Assessment of Target Security: Shadow Scanner</i>	

Lab 71: Internet Vulnerability Scanner	468
<i>Assessment of Target Security: Cerberus</i>	
Lab 72: WHAX — Auto Exploit Reverse Shell	474
<i>Automatically Exploit the Target: AutoScan</i>	
Lab 73: Unique Fake Lock Screen XP	491
<i>Grab the Administrator Password: Fake Lock Screen XP</i>	
Lab 74: Bypassing Microsoft Serial Numbers	499
<i>Bypassing Serial Number Protection: RockXP/Custom Script</i>	
Lab 75: Vulnerability Exploit	507
<i>Assessment of Target Security: Web Hack Control Center</i>	
9 Wireless	511
Lab 76: Locate Unsecured Wireless	513
<i>Locate Unsecured Wireless: NetStumbler/Mini-Stumbler</i>	
Lab 77: Trojan	519
<i>Unauthorized Access and Control: Back Orifice</i>	
On the Target Computer	519
On the Attacker's Computer	528
Lab 78: Trojan	534
<i>Unauthorized Access and Control: NetBus</i>	
On the Target (Server)	534
On the Attacker's Computer	540
Lab 79: ICMP Tunnel Backdoor	545
<i>Bidirectional Spoofed ICMP Tunnel: Sneaky-Sneaky</i>	
On the Target (Server)	545
On the Attacker's Machine	548
Lab 80: Hiding Tools on the Target	553
<i>Hiding Files on the Target: CP</i>	
Scenario: Hiding Netcat inside the Calculator Application	553
To Verify	555
Lab 81: Capturing Switched Network Traffic	556
<i>Intercept/Exploit Traffic: Ettercap</i>	
Lab 82: Password Capture	573
<i>Capture Passwords Traversing the Network: Dsniff</i>	
Lab 83: Data Manipulation	574
<i>Manipulate the Live Data Stream: Achilles</i>	
Lab 84: Covert Reverse Telnet Session	588
<i>Create a Reverse Telnet Session: Netcat</i>	
Lab 85: Covert Channel — Reverse Shell	596
<i>Exploit Data from Target Computer: Reverse Shell</i>	
10 Redirection	603
Lab 86: PortMapper	605
<i>Traffic Redirection: PortMapper</i>	
Lab 87: Executing Applications — Elitewrap	618
<i>Executing Hidden Applications: Elitewrap</i>	
Lab 88: TCP Relay — Bypass Firewalls	627
<i>Traffic Redirection: Fpipe</i>	

Lab 89: Remote Execution	633
<i>Remote Execution on Target: PsExec</i>	
Lab 90: TCP Relay — Bypass Firewalls	638
<i>Traffic Redirection: NETWOX/NETWAG</i>	
11 Denial-of-Service (DoS).....	643
Lab 91: Denial-of-Service — Land Attack	645
<i>DoS Land Attack: Land Attack</i>	
Lab 92: Denial-of-Service — Smurf Attack	650
<i>DoS Smurf Attack: Smurf Attack</i>	
Lab 93: Denial-of-Service — SYN Attack	655
<i>DoS Land Attack: SYN Attack</i>	
Lab 94: Denial-of-Service — UDP Flood	660
<i>DoS UDP Flood Attack: UDP Flood Attack</i>	
Lab 95: Denial-of-Service — Trash2.c	665
<i>Create Denial-of-Service Traffic: Trash2.c</i>	
Appendix A: References	671
Appendix B: Tool Syntax.....	675
Index.....	725