Table of Contents

|  |  |
| --- | --- |
| Welcome | 1 |
| Getting Started | 5 |
| Lab 1.1: Windows Cheat Sheet | 8 |
| Lab 1.2: Enterprise Wide Identification and Analysis | 28 |
| Lab 1.3: Incident Response Tabletop Exercise | 38 |
| Lab 1.4: Linux Cheat Sheet | 42 |
| Lab 2.1: OSINT with Spiderfoot | 54 |
| Lab 2.2: Wireless LAN Discovery with InSSIDer | 68 |
| Lab 2.3: Nmap | 73 |
| Lab 2.4: Nessus Scan Analysis | 84 |
| Lab 2.5: SMB Sessions | 90 |
| Lab 3.1: The Many Uses of Netcat | 104 |
| Lab 3.2: ARP and MAC Analysis | 123 |
| Lab 3.3: Responder | 131 |
| Lab 3.4: Metasploit Attack and Analysis | 138 |
| Lab 4.1: John the Ripper | 166 |
| Lab 4.2: Hashcat | 174 |
| Lab 4.3: BeEF for Browser Exploitation | 183 |
| Lab 4.4: Cross Site Scripting and SQL Injection | 193 |
| Lab 4.5: Counting Resources to Evaluate Denial of Service Attacks | 213 |
| Lab 5.1: Windows Attack Analysis with Rekall | 230 |
| Lab 5.2: Fun with Rookits | 243 |
| Lab 5.3: Shell History Analysis | 251 |
| Lab 5.4: Alternate Data Streams | 258 |
| Lab 5.5: Windows Log Editing | 267 |
| Lab 5.6: Covert Channels | 281 |
| Connecting to the Network | 287 |
| Online CTF Access | 303 |