Blue Team Handbook: Incident Response Edition

A condensed field guide for the Cyber Security Incident Responder.

By: Don Murdoch, GSE, MBA, CISSP+14
Version 2.0

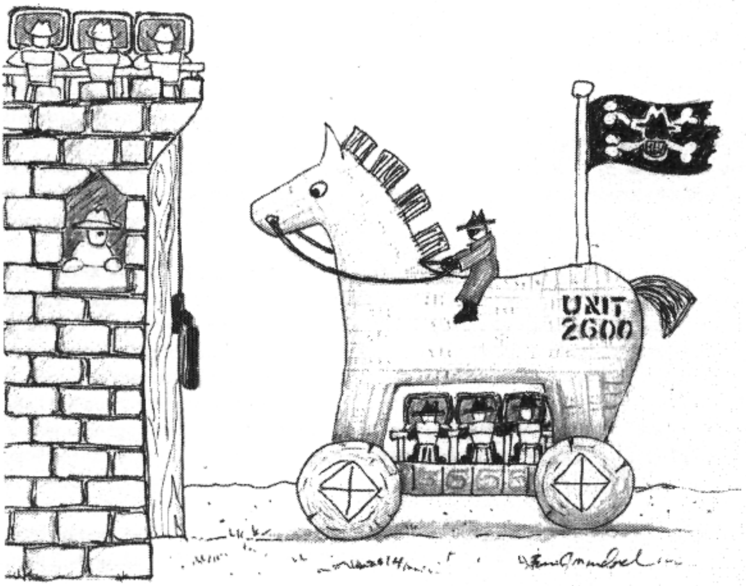

Table of Contents

1. Blue Team Handbook - Introduction....................................3
2. Some Lessons from the US Military....................................4
3. Six Steps of Incident Response..5
4. Assessing Impact of Cyber Attacks....................................16
5. Essential IR Business Process and Paperwork...................18
6. Chain of Custody and Evidence Topics (V2).......................24
7. Six Step Incident Response Template...............................26
8. Commercial Incident Response Template 28
9. Incident Response and Forensics are Partners.................31
10. The Attack Process, Tools, and IR Points 33
11. Secure Communications 39
12. Netcat and Cryptcat for the Blue Team 41
13. Nmap and Masscan Network Assessment.....................45
14. Windows Counter Loops..49
15. Simple Windows Password Guessing............................50
16. Automated Collection (Windows).................................51
17. Malware Standard Response Pattern 53
18. Windows Volatile Data Investigation............................54
19. Other Windows Artifact Investigation 69
20. Linux Volatile Data System Investigation......................70
21. Linux Artifact Investigation 74
22. SIFT Based Timeline Construction (Windows) 78
23. Linux Iptables Essentials: An Example 80
24. Firewall Assurance/Testing with HPing.........................82
25. Network Device Collection and Analysis Process 84
26. Website Investigation Techniques................................87
27. Network Traffic Analysis Techniques............................88
28. Common Malware Campaign Pattern 97
29. Suspicious Traffic Patterns...99
30. Packet Data Carving Notes...105
31. RDBMS Incident Response (V2) 106
32. Wireless Specific Topics 108
33. Using the Snort IDS (BackTrack, Kali)..........................110
34. Notes: Bootable Linux Distributions 114
35. Vulnerability Testing (OpenVAS).................................116
36. Wireshark Usage Notes..117
37. Password Assessment 119

38. Common TCP and UDP Ports 121
39. ICMP Table 125
40. Web Site References 128
41. ICMP Header 131
42. IPV4 Header 132
43. UDP Header 133
44. TCP Header 134
45. IPv6 Header 135
46. Acronyms Used in this Manual 136
47. Bibliography, Reading List, and References 138
48. Index 144

List of Tables

Table 1 Step One: Preparation 5
Table 2 Step Two: Identification 9
Table 3 Step Three: Containment 11
Table 4 Step Four: Eradication 14
Table 5 Step Five: Recovery 14
Table 6 Step Six: Lessons Learned (or Follow Up) 15
Table 7 Categorize Cyber Attack's Effects (MITRE) 17
Table 8 PenTest Authorization Letter (Skoudis) 20
Table 9 Six Step Structured Incident Response Template 26
Table 10 Commercial Structured Incident Response Template 28
Table 11 Google Search Examples 35
Table 12 Google Search Terms for Incident Response 35
Table 13 NetCat Relay Setup 43
Table 14 Masscan Examples 47
Table 15 WFT Quick Start 51
Table 16 Mandiant RedLine Quickstart 52
Table 17 Prepare Environment for Collection (Windows) 54
Table 18 Mandiant Memoryze Quick Start 55
Table 19 Volatility Example for Win2008 SP1 56
Table 20 Windows Environment Data Collection (Native) 57
Table 21 Windows Environment Data Collection (Third Party) .59
Table 22 FTK Imager Collection 60
Table 23 Supplemental System Collection (Windows) 61
Table 24 Process Explorer View of Normal Processes 62

Table 25 Windows Firewall Commands (netsh) 64
Table 26 Windows Firewall Commands (netsh advfirewall)......64
Table 27 Other Windows Artifact Investigation 69
Table 28 Prepare Environment for Collection (Linux)................70
Table 29 User Account Related Artifacts (Linux) 74
Table 30 OS Artifacts (Linux)..74
Table 31 Log Collection (Linux) 76
Table 32 File Activity Analysis (Linux) 77
Table 33 hping...82
Table 34 Hping2 Examples...82
Table 35 Hping3 Examples...83
Table 36 PCAP Timeframe Analysis (Wireshark).......................91
Table 37 PCAP Timeframe Analysis (tcpdump).........................91
Table 38 Detect MAC Address Manipulation............................92
Table 39 Fragmentation Checks..93
Table 40 Tcpdump Traffic Filter Examples................................95
Table 41 tcpdump Control Bits 95
Table 42 Malware Distribution Pattern 97
Table 43 Common Ports Found in Corporate Setting.............100
Table 44 Suspicious TCP Patterns 101
Table 45 Suspicious Traffic Volume 102
Table 46 Suspicious Broadcast Traffic.....................................102
Table 47 MAC / ARP attacks...102
Table 48 Suspicious ICMP 103
Table 49 DoS/DDoS...103
Table 50 Suspicious Brute Force 104
Table 51 File Extension Types 107
Table 52 Wireshark Wireless Display Filters...........................108
Table 53 Wireshark Wireless Capture Filters..........................108
Table 54 Wireshark Display Filters...117

List of Figures

Figure 1 Conflict Superimposed on Six Steps..............................4
Figure 2 Seven Domains of IT Infrastructure 16
Figure 3 Malware / Automated Attacker General Process........33
Figure 4 Determined Attacker General Process........................33
Figure 5 NIST 800-115 Penetration Test Process.......................34

Figure 6 Example of a Windows Disk Image with mmls 78
Figure 7 Syn/Ack Packets in Wireshark..88
Figure 8 Wireshark ICMP Type and Code Display........................94
Figure 9 Wireshark "contains" Example 117