

Intermediate Security: Live System Analysis

Introduction.....	1
Live Response: Collecting Volatile Data.....	2
Drawbacks.....	2
Advantages.....	2
Locard's Exchange Principle.....	2
Order of Volatility.....	2
Knowing What Data to Collect.....	3
Current Network Configuration.....	3
Exercise 1.....	6
Logged On Users	7
Exercise 2.....	11
Network Connections.....	12
Exercise 3.....	14
Process Information	15
TList.....	16
TaskList.....	20
PsList.....	21
ListDLLs.....	24
Handle.exe	25
Exercise 4.....	26
Process-to-Port Mapping	27
External Port Scanning to Identify Open Ports.....	29
Packet Sniffing for Port Traffic	30
Process Memory.....	31
Detecting Network Adapters in Promiscuous Mode	31
Exercise 5.....	32
Creating Microsoft Batch Files.....	33
Useful Batch File DOS Commands	33
Exercise 6.....	37
Clipboard Contents	38
Service & Driver Information.....	39
Command History.....	40
Mapped Drives.....	40

Shares	41
Exercise 7	42
Redirection	43
Redirection	43
Redirect and Append Output	43
Pipe	44
Exercise 8	45
The Registry	46
Registry Startup Locations	53
Registry Protected Storage Area	57
System Restore Points	58
Windows Memory Analysis	59
Memory Dumps	59
Configuring Memory Dumps in Windows XP	60
Exercise 9	63
Basic Forensic Drive Analysis	64
Disk Images	64
Creating a Drive Image	64
Generating Memory Dumps with Third Party Utilities	65
Analysis of Dump Files	67
Exercise 10	68
Live Response: Collecting Nonvolatile Data	69
Deleted E-Mail	69
Deleted Files	69
Exercise 11	72
Locating Information on Remote Devices	73
Appendix A: Solutions to Exercises	88