# INSTRUCTOR GUIDE

National Computer Forensics Institute

# NITRO

# Network Intrusion Responder Program

# Network Intrusions Responder Program (NITRO)

# Instructor Guide

# Table of Contents

# Introduction to the NITRO Course

**Instructor Guide Overview**

The Instructor Guide is a resource for instructors to use to teach the Network Intrusions Responder Program (NITRO) Course in a consistent manner. This Guide provides:

- Overview of each module in the course
- Outline of topics to be taught in each module
- Timeline for presentation of topics
- List of all Practical Exercises
- List of tests
- Notes section for each topic where you can add your own class notes for your presentations

**How to Use this Guide**

Use this Guide as a roadmap to all of the topics covered in NITRO. You can personalize this Guide by adding individual notes to lesson topics to enhance your class presentations.

**Introduction to NITRO**

NITRO is a course designed to train first responders to successfully respond to and process a computer crime scene in a home or business environment involving either a Windows or Unix operating system. Instruction is dynamic, flexible, and focuses on hands-on training.

NITRO training familiarizes students with:

- Legal aspects of incident response procedures
- Techniques for search and seizures
- Methods and tools necessary to successfully gather volatile information
- Evidence processing and handling
- Media imaging

**NITRO Practical Exercises**

All exercises in NITRO are hands-on activities directed by instructors.

**In this Guide**

The following table shows the contents of this Guide.

**NITRO testing Policy**

Before graduation from courses at NCFI, each student must show an acceptable level of achievement on all course objectives as demonstrated by written and performance-based tests. The minimum passing score on all comprehensive written tests is 70%. The minimum passing score of 70% is also required on all performance-based tests.

To measure a student's progress throughout a course, NCFI uses several testing methods:

- *Practical Exercises (non-graded)* – Performance-based exercise to test the student's ability to perform required tasks. During this exercise, students work with peers and are guided by and can seek assistance from instructors.
- *Written Tests* – Multiple choice and short answer questions. Required minimum passing score is 70%.
- *Graded Practical Exercise* – Performance-based exercise to test the student's ability to perform required tasks. During this exercise, students work with peers and are guided by and can seek assistance from instructors. This exercise is graded and reviewed with the students to assist them in measuring their performance. The grades are not reflected in their overall course completion.
- *Performance-based Test* – An exam in which the student must work independently to perform required tasks. This exam is graded and a passing grade of 70% is required.

- For the NITRO, the student's progress will be monitored through practical exercises, written tests, and graded performance-based tests. Tests are given at the conclusion of the course.

Students who fail a written or performance-based test are given remedial training and tested again. Students will not be given a retest within eight hours after notification of a test failure. However, students will be retested no later than 24 academic hours after notification of a test failure.

# Module 1 - Understanding Computer Hardware

**Module 1: Overview**

This module explains the procedures necessary for safe handling of computers. Students will learn the primary hardware components that power the data processing and storage functions of every computer. An understanding of MBs, CPUs, memory, and bus is essential to knowing how a computer system works.

**Module 1 Exercises**

Students disassemble and rebuild PCs.

**Module 1 Testing**

There is no testing for the content of this module.

**Module 1 Objectives**

- Practice safety procedures when handling computer equipment
- Identify major computer components
- Identify and explain MB types
- Recognize individual MB components including chipsets, jumpers and switches, power supply and connections
- Define Basic Input/Output System (BIOS)
- Recall CPU functions and memory

**In this Module**

Here are the lessons in this module:

## Lesson 1 – Safety Overview

**Lesson 1: Safety Briefing**

Explains the procedures necessary for safe handling of computers.

**Lesson 1 Learning Objectives**

- Identify the steps to take to protect yourself from injury when using a computer
- Explain how to protect computer components and stored data

**Lesson 1 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Need for Safety Procedures | • Mention jewelry, IDs and any other items that may become hooked or tangled in equipment.<br>**My Notes:** |
| Step-by-Step Safety Procedures | • Reinforce wearing the wrist strap.<br>• Stress pulling the plug before working on PC.<br>**My Notes:** |

## Lesson 2 – Overview to Computers

**Lesson 2: Overview of Computers**

Presents the key components of the computer, history of computing, and basic terminology. Computer components are identified and their roles are reviewed in relation to the computer system as a whole.

**Lesson 2 Objectives**

- Define basic computer terminology
- Explain the history of the modern computer
- Identify the basic computer components

**Lesson 2 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Introduction to Computers | • Binary – used in many forms of data transfer: Memory, CDs, fiber optic<br>• Portable computers: PDAs can be used to transfer movies and pictures without the use of a typical PC or laptop. There will be no forensic evidence on a PC if transfers occurred from PDA to PDA.<br>**My Notes:** |
| History of Computers | • Switches, gears, etc. We are still using the binary system today.<br>• Systems are getting smaller, cooler, and faster.<br>**My Notes:** |
| Basic System Components | • Quick introduction, all of these parts will be covered more in-depth in class later.<br>**My Notes:** |

## Lesson 3 – Motherboards and Components

**Lesson 3: Motherboards and Components**

This lesson explains the main functions of the motherboard (MB). It also introduces the Basic Input/Output System (BIOS) as the instruction set that controls the main functions of the computer.

**Lesson 3 Objectives**

- Define the role of the motherboard
- Identify types of motherboards
- Identify main motherboard components
- Explain BIOS and the concept of Plug and Play
- Basic functions of buses
- Identify various bus types
- Recognize various bus connectors

**Lesson 3 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Motherboard Overview | • While talking about the cases, show the mod systems (ET, Falcon, toaster). These images can be found at http://mini-itx.com.<br>• Slide shows various sections of the MB<br>• Again, each will be covered more in-depth<br><br>**My Notes:** |

**Lesson 3 Topics**, continued

| Topic | Key Points |
|---|---|
| Motherboard Components | • Ask how many still use a floppy drive. Point out that they are becoming less popular and in many cases have to be ordered as an optional device. Dell charges $12 for a 3.5 inch floppy drive. Questions that could be asked:<br>• Why are floppy drives becoming obsolete? What types of devices are replacing them?<br>• Define non-volatile and volatile storage<br>• Start disassembly before getting to motherboard and BIOS section<br>• Stress the differences between BIOS and CMOS<br>• Perhaps go to motherboard.org to lookup some of the new MB information<br>**My Notes:** |
| Bus Overview | • Several types of buses; all used to transfer information from one stop to another<br>• May get a few questions about north bridge and south bridge<br>• This is a good opportunity to diagram the buses and their relationship to CPU, RAM, PCI, etc. on the whiteboard<br>**My Notes:** |
| Bus Types | • This would be a good time to stress the idea of backward compatibility<br>**My Notes:** |

## Lesson 4 – CPU and Memory

**Lesson 4: CPU and Memory**

The computer's processor, also called the central processing unit (CPU), works in concert with memory to process software and user commands. This lesson explains the significance and functions of both CPU and memory.

**Lesson 4 Objectives**

- Explain the basic functions of the CPU
- Identify the CPU in a computer
- Recognize various types of memory

**Lesson 4 Topics**

Here are the topics to present.

| Topic | Notes |
|---|---|
| CPU Functions | • Highlight the difference between the slot and socket chips<br>• The main brain of the computer<br>**My Notes:** |
| Memory | • Compare and contrast: RAM, ROM and cache.<br>• Review the older types of RAM (SIMM, 30-72 pin)<br>• Compare the DDR and RAMBUS. Students (gamers) seem to be interested in the differences.<br>**My Notes:** |

This page intentionally left blank.

# Module 2 - Data Storage Components

**Module 2 Overview**

Understanding the vast array of data storage components is vital knowledge for processing an electronic crime scene investigation. This module introduces disk drives and various types of removable storage media.

**Module 2 Exercises**

N/A

**Module 2 Testing**

Module content will be tested at the end of Module 3.

**Module 2 Objectives**

- Explain how data is stored on a hard drive
- Identify components of the hard drive
- Understand the workings of a floppy drive
- Recognize various removable media

**In this Module**

Here are the lessons in this module:

## Lesson 1 – Hard Disk Drives

**Lesson 1: Hard Disk Drives**

Hard drives are the main storage of the computer. Drives use highly sophisticated technology to write data on platters. This lesson examines the main components of hard drives and their functions. Understanding how disk drives store information is important to knowing how to safeguard data during a crime investigation.

**Lesson 1 Objectives**

- Identify the main components of a hard drive
- Explain the process by which data is stored on and retrieved from a hard drive
- Describe the basic formatting procedures for hard drives
- Explain hard drive geometry

**Lesson 1 Topics**

Here are the topics to present.

| Topic | Notes |
|---|---|
| Hard Drive Components | • Hard drive diagram slide is useful because it shows an exploded view. A good time to pass around various hard drives.<br>**My Notes:** |
| Hard Drive Controllers/Interface (IDE,SATA, SCSI) | • IDE and EIDE controllers are a part of the drive. This has not always been the case.<br>• Stress: ATAPI – CD-ROM drives; ATA5/6 – 40 pin / 80 wire<br>**My Notes:** |
| Hard Drive Geometry | • You may want to toggle between the slide describing the components (track, sector and cylinder). Define one and then show it on the diagram.<br>• Stress the difference between a sector and a cluster.<br>**My Notes:** |

**Lesson 1 Topics**, continued

| | |
|---|---|
| Drive Preparation – Wiping | • Emphasize that low-level formatting is done at the manufacturing site because it sets up the physical geometry.<br>• For partitioning, use a real-world example such as dividing up the room into two groups by placing a wall down the center row. One side of the room uses Windows and the other uses Linux.<br>• Remind them that the primary partitions take precedence when assigning drive letters.<br>• High-level formatting prepares the drive for the particular file system: (FAT16, FAT32, NTFS)<br>**My Notes:** |
| RAID Configuration Overview | • Try using a "devils advocate" approach to this section. Start with RAID 0 and imaging and ask "OK, but what if … happens?" Then, use this statement to highlight the next version of RAID, stressing the benefits.<br>**My Notes:** |

## Lesson 2 – Floppy Drives and Removable Media

**Lesson 2: Floppy Drives and Removable Media**

This lesson examines types of floppy disk drives and a variety of removable media storage components. Understanding data storage components of a computer system is important to knowing how to safeguard information that is seized during a crime investigation.

**Lesson 2 Objectives**

- Identify the characteristics of floppy disk drive components
- Explain the characteristics of a magnetic drive
- Recognize common removable media
- Explain the characteristics of a magneto-optical drive
- Name the differences between magnetic and digital audio tapes (DAT)

**Lesson 2 Topics**

Here are the topics to present.

| Topic | Notes |
|---|---|
| Floppy Disk Drives | • Ask students where the floppy drive controller is located - Super IO Chip<br><br>**My Notes:** |
| Removable Media | • If you are running behind, this is where you can catch up. Material can be covered briefly, as most students should be familiar with high level information.<br><br>**My Notes:** |

This page intentionally left blank.

# Module 3 - Input/Output Components

**Module 3 Overview**

This module examines the various components involved in the transfer of data into and out of a computer system.

**Module 3 Testing**

**Module 3 Objectives**

- Recognize basic input devices such as the keyboard, mouse, scanner, and modem
- Explain how monitors and video display adapters work
- Identify the various input/output ports found on a PC
- Define interrupts, IRQs, direct memory access, and device drivers
- Recognize SCSI devices and connectors

**In this Module**

Here are the lessons in this module:

## Lesson 1 – Input/Output Devices and Ports

**Lesson 1: Input/Output Devices and Ports**

This lesson introduces the basic input/output devices, including the keyboard, mouse, scanner, monitor, printer, and modem. Students will gain a broader understanding of common input/output components and how they work.

**Lesson 1 Objectives**

- Recognize input devices such as the keyboard, mouse, scanner, and modem
- Explain how monitors work and be familiar with video display adapters
- Identify the various input/output ports

**Lesson 1 Topics**

Here are the topics to present.

| Topic | Notes |
|---|---|
| Overview | • Going over this basic stuff is necessary to help identify computers.<br>• If you haven't shown the images of mod PCs, show them now. If they have been shown, refer back to them.<br>**My Notes:** |
| Input Devices | • The PS/2 ports are technically not keyboard and mouse ports.<br>• FireWire ports have either 4 or 6 connectors. Six connectors supply power; four connectors do not.<br>**My Notes:** |

**Lesson 1 Topics**, continued

| *Topic* | *Notes* |
|---|---|
| Output Devices | • Review the basics<br>**My Notes:** |
| Input/Output Ports | • Reiterate specifics:<br>• It's a serial port, not a com port<br>• It's a parallel port, not a printer port<br>• They are PS/2 ports, not keyboard and mouse ports<br>**My Notes:** |
| Modems | • PC works in digital, phone lines work in analog<br>• Cable modem is not a true modem; it's a basic type of router.<br>**My Notes:** |
| PC Cards | • Three main categories: Type 1 – memory, Type 2 – communication, Type 3 – storage devices<br>• Finding a PC card means they probably have a notebook or a laptop<br>**My Notes:** |

## Lesson 2 - BIOS and System Initialization

**Lesson 2: BIOS and System Initialization**

This lesson explains the main functions of the Basic Input/Output System (BIOS) as the instruction set that controls the main functions of the computer. It will delve into how the BIOS initializes hardware and starts the operating system.

**Lesson 2 Objectives**

- Define the role of the BIOS
- Understand what POST codes are
- Explain BIOS and the concept of Plug and Play
- Explain how a system boots

**Lesson 2 Topics**

Here are the topics to present.

| Topic | Notes |
|---|---|
| Motherboard Components | • Define non-volatile and volatile storage<br>• Start disassembly before getting to motherboard and BIOS section<br>• Stress the differences between BIOS and CMOS<br>• Perhaps go to motherboard.org to lookup some of the new MB information<br>**My Notes:** |

**Lesson 2 Topics**, continued

| Topic | Notes |
|---|---|
| BIOS Information | • Discuss the basics of the BIOS and how the function of the setup program<br>• Make sure you note that each different motherboard chipset may have a unique keystroke required to enter the setup, and many don't even notify the user what to press<br>• Note that passwords could be implemented to block investigators out of the BIOS and the ways around the password – refer to websites such as: labmice.techtarget.com/articles/BIOS_hack.htm<br>• Note what information to gather while in BIOS<br>**My Notes:** |
| The Boot Process | • Discuss IO.SYS and MSDOS.SYS<br>• Stress which of the files are necessary to boot a system<br>**My Notes:** |
| The Master Boot Record | • Briefly cover the MBR and how the BIOS points to this to load the operating system<br>**My Notes:** |

This page intentionally left blank.

# Module 4 - Operating Systems and Installation

**Module 4: Overview**

Windows XP Professional is one of the most popular and widely used Operating System on the market today. This lesson explains how to select a file system and install an Operating System

**Module 4: Exercises**

Students will configure their forensic workstations and install additional applications

**Module 4 Testing**

**Module 4 Objectives**

- Installing Windows XP Professional
- Compare and Contrast the FAT and NTFS File System
- Install updates on Windows XP

**In this Module**

Here are the lessons in this module:

## Lesson 1 – File System / Operating System Basics

**Lesson 1: File Systems**

This lesson provides an overview of File System / Operating System Basics, including selecting a file system.

**Lesson 1 Learning Objectives**

- Give a brief overview of file systems
- Explain how to install Windows XP Professional
- Identify how Updates are installed on Windows XP

**Lesson 1 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| File Systems | • Show advantages and disadvantages of NTFS vs. FAT<br>• Touch on how FAT can be converted to NTFS through "convert.exe"<br>• Show in what operating systems each file system can be found, where will investigators run across certain ones in the field<br>**My Notes:** |
| Operating System Installation | • Installing Windows may not be required for this course, but showcase the steps in case a student needs help on other computers.<br>**My Notes:** |
| Operating System Updates | • Show how to enable or disable automatic patching, and how to use Windows Update online and application.<br>**My Notes:** |

This page intentionally left blank.

# Module 5 - Introduction to Networks

**Module 5 Overview**

Most computers today are connected in some way to a network. To understand network components and functions, students need to recognize the common network architectures and know various access methods. This module presents basic networking concepts, architectures, and common network topologies.

**Module 5 Exercises**

**Module 5 Testing**

**Objectives**

- Explain network technologies
- Identify different network configurations including LAN, WAN, and the Internet
- Explain the OSI model and how it standardizes network communications
- Name the differences between TCP/IP and the OSI model
- Explain common ports and their uses
- Identify the six main network models
- Describe different network topologies

**In this Module**

The following table shows the contents of this module.

## Lesson 1 – Network Basics

**Lesson 1: Networks Basics**

Networks are the pathways of communication that link individual computers and network devices. This lesson explores the types of networks used today and the two primary methods of transmitting network data.

**Lesson 1 Learning Objectives**

- Define what a network is and the components that comprise one
- Identify the various types of networks
- Explain the difference between circuit-switched and packet-switched networks

**Lesson 1 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Introduction to Networks | • Purpose of: share resources<br>• IEEE 802.X, why have standards? Interoperability<br>**My Notes:** |
| Network Types | • LAN & WAN = size and equipment<br>• Internet = interconnected networks ISP (function)<br>• Differences and importance of Intranet / Extranets<br>**My Notes:** |
| Network Categories | • Circuit switched = like a telephone call or train<br>• Packet switched = like the Post Office or UPS<br>• Connection vs. Connectionless<br>**My Notes:** |

## Lesson 2 – Network Technologies

**Lesson 2: Network Technologies**

Networks send data from a sending device through network interfaces, across cables or other transmission media, to a receiving device. In this lesson, you will describe the two most common technologies used to facilitate this data transfer. Students will gain an understanding of the technological framework upon which networks are built.

**Lesson 2 Learning Objectives**

- Describe the difference between broadcast and point-to-point technologies

**Lesson 2 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Introducing Network Technologies | • Broadcast – CSMA/CD – Collisions – Multipoint<br>• Sniffing on Broadcast Networks<br>All systems can see the packets<br>• Point-to-Point – Token<br><br>**My Notes:** |

## Lesson 3 – Network Topologies

**Lesson 3: Networks Topologies**

In networking, the term topology refers to the layout identifying the location of all network components and the way data flows through the network. This lesson presents the most common network topologies: bus, ring, star, tree, and mesh.

**Lesson 3 Learning Objectives**

- Identify the main network topologies
- Explain the difference between a physical topology and the logical topology of a network

**Lesson 3 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Topologies Defined | • Physical – how the network is setup<br>• Logical – how the data flows around the network<br>• Outline on the board for clarity:<br>Stress Bus, Star, Star-wired Ring, Mesh<br>• Bus versus Star = amount of cable used<br>• Review Topology diagrams in Student Book<br>**My Notes:** |

## Lesson 4 – Network Architecture

**Lesson 4: Network Architecture**

A network's architecture refers broadly to the overall configuration of the network and includes the type, topology, hardware, speed, and specific cabling used in a given implementation. It is important for students to know the characteristics of the various network architectures. This information will be necessary in assessing a crime scene and the capabilities and properties of the target network.

**Lesson 4 Learning Objectives**

- Identify the most common network architectures

**Lesson 4 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Introduction to Network Architecture | • State basic architecture of:<br>Ethernet - Token Ring<br>FDDI - ATM<br>**My Notes:** |
| Ethernet | • Explain codes: 10baseT - 100baseT, etc.<br>• Describe cable types: coax and UTP<br>**My Notes:** |
| Token Ring | • Star-wired Ring = MAU<br>• Must have token to communicate<br>**My Notes:** |

**Lesson 4 Topics,** Continued

| Topic | Key Points |
|---|---|
| Fiber Distributed Data Interface (FDDI) | • Duel rings made of fiber<br>• Built-in failure recovery<br>**My Notes:** |
| Asynchronous Transfer Mode | • Data, sound, and video<br>• Fixed length cells<br>**My Notes:** |
| Broadband | • Refers to telecommunication methods where wide ranges of frequencies are available. Multiple frequencies can be divided up into multiple channels, which can be used to send more information within a given amount of time.<br>**My Notes:** |

## Lesson 5 – The OSI Model

**Lesson 5: The OSI Model**

This lesson describes each step in the process of transmitting information from one computer to another across the network through the Open Systems Interconnect (OSI) model. The OSI model is a conceptual model or framework of how communication is to take place and promote open networking environments.

**Lesson 5 Learning Objectives**

- Explain the main objectives of the OSI model
- Name the seven OSI layers
- Identify the functions of each OSI layer

**Lesson 5 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| OSI Model Overview | • "Conceptual" or software<br>• To-do list for communicating on a network<br>**My Notes:** |
| OSI Model Layers | • Acronyms:<br>All People Seem To Need Data Processing<br>Please Do Not Throw Sausage Pizza Away<br>• Explain in general what happens at each layer starting with the Application level<br>• The more "intelligent" a device is, the higher it is on the OSI model.<br>**My Notes:** |

Page Intentionally Left Blank

# Module 6 - Network Connectivity and Protocols

**Module 6 Overview**

Networks come in many configurations, or topologies. Students need to be able to recognize common network topologies and understand how they function. This module introduces the various network topologies and explains how networks interconnect.

**Module 6 Exercises**

- Build a Local Area Network
- Configure protocol stacks
- Compare/contrast protocols

**Module 6 Testing**

**Objectives**

- Identify network connection configurations
- Name network connection devices and their functions
- Recognize connection hardware and describe their characteristics
- Describe different network topologies

**In this Module**

The following table shows the contents of this module:

## Lesson 1 – Network Connectivity

**Lesson 1: Network Connectivity**

This lesson identifies the various physical components used to connect computers and devices within a network environment. Students will learn how computers and stand-alone devices interconnect to form a network. They will also discover how to connect clients and servers on a LAN to other networks. An introduction to wireless networks is also included.

**Lesson 1 Learning Objectives**

- Name the various types of transmission cabling used to wire a network
- Identify network interface cards and adapters
- Explain how modems work to provide remote access
- Identify the various types of wireless media

**Lesson 1 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Network Connectivity | • Explain what a NIC is<br>• Card can be ISA/PCI/USB and wireless<br><br>**My Notes:** |
| Network Transmission Media | • Characteristics – UTP is mostly used today<br>• Categories of UTP<br>• Types of fiber cables and connectors<br><br>**My Notes:** |

**Lesson 1 Topics**, continued

| | |
|---|---|
| Network Devices | • Explain the NIC to MAC relationship<br>• Show coffer.com<br>• Explain where each of the following is listed on the OSI model and why:<br>• Hubs, repeaters, bridges, switches, routers, gateways.<br>• Explain the difference between active and passive hubs, digital and analog repeaters.<br>**My Notes:** |
| Wireless Media | • Compare fixed versus mobile technologies<br>• Range of signals<br>• New wireless PC card will work in older laptops<br>• Types of transmissions (3)<br>**My Notes:** |

## Lesson 2 – Network Configuration Models

**Lesson 2: Network Configuration Models**

The network configuration models presented in this lesson include client/server network, server/server network, peer-to-peer network, server-centric network, enterprise network, and remote access service (RAS) network. Students will learn to recognize common network configurations. This information will be helpful for computer crime investigations involving networks.

**Lesson 2 Learning Objectives**

- Identify the six main network configurations
- Describe the key characteristics of each network configuration
- Explain how remote access service networks function

**Lesson 2 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Introduction to Network Models | • What's in it for me as an investigator? Knowing the model that a network is associated with will help determine the scope of a network. For instance, a server-centric or enterprise environment will have more nodes than a peer-to-peer environment.<br>**My Notes:** |

## Lesson 3 - Network Protocols

**Lesson 3: Network Protocols**

Network protocols are guidelines that define how computers transmit and receive data. These rules for transmission follow the guidelines established by the OSI model. Protocols ensure that all devices attempting to communicate on a network are following the same rules. In this lesson, students will explore commonly used protocols.

**Lesson 3 Objectives**

- Define network protocol
- Describe the characteristics of TCP/IP, IPX/SPX, NetBEUI, PPP, and PPTP

**Lesson 3 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Protocols | • Explain the definition of the word protocol. A code or a set of processes used in accomplishing a task, for example: an SOP.<br>• Relate this to networking protocols – a set of standards used to transmit information.<br>**My Notes:** |
| TCP/IP | • The protocol of the Internet<br>• Not associated with any company – considered an open source protocol<br>• Is routable<br>• Is associated with: IP addresses, subnets, gateways, DNS, etc.<br>**My Notes:** |

**Lesson 3 Topics**, continued

| Topic | Key Points |
|---|---|
| Other Protocols | • NetBEUI/NetBIOS – Created by Microsoft<br>• IPX/SPX – Created by Novell<br>• PPP – Creates a connection between an analog modem and an ISP. Once connected, TCP/IP packets can travel to and from a modem.<br>• PPTP – Non-routable packets are encapsulated into routable packets. This allows protocols like IPX/SPX to be sent over the Internet.<br>**My Notes:** |

## Lesson 4 – Wireless Networks

**Lesson 4: Wireless Networks**

This lesson presents basic information about wireless networks, including how they work, the different types of wireless networks, the components that makeup a wireless network, and security concerns. Students will gain insight on wireless networks and how these networks can be used with good and bad intentions.

**Lesson 4 Objectives**

- Explain what a wireless network is and how it works
- Explain the 802.11 standard
- Explain the difference between infrastructure and ad-hoc modes
- Discuss security concerns of implementing wireless networks

**Lesson 4 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| What is a Wireless Network? | • Explain that 802.11b and g are compatible, but "a" devices will not communicate with either of the other classifications. Explain why (frequency).<br>• Address the security risks related to Hotspots<br>• Explain the significance of the WiFi and Centrino symbols<br>**My Notes:** |
| Types of Wireless Networks | • Adhoc – used for temporarily swapping files<br>• Infrastructure – typical wireless environment where a WAP is used to connect wireless devices to a wired network<br>**My Notes:** |

**Lesson 4 Topics**, continued

| Topic | Key Points |
|---|---|
| Hardware Components | • Stress that the wireless-NIC could be integrated into the motherboard<br>**My Notes:** |
| Security Concerns | • Compare WEP and WPA<br>• SSID and MAC filtering – easy to implement, but rarely turned on. Routers are "wide open" when they are initially turned on. This is by design (IEEE specs).<br>**My Notes:** |
| Vulnerabilities | • Overlapping signals and Accidental Association are related – one can cause the other.<br>• Bluejacking – from a social aspect<br>• Man-in-the-Middle – Starbucks example<br>• War driving video is about 20 minutes long<br>**My Notes:** |

This page intentionally left blank.

# Module 7 - IP Addresses and Subnets

**Module 7: Overview**

This module explains Internet Protocol (IP) addresses and how they are constructed. Students will learn about IP addressing and the classes of networks in IP addressing schemes. They will also learn about subnets and the IP addressing schemes for subnet masks.

**Module 7 Exercises**

Subnetting exercise in Lesson 3

**Module 7 Testing**

**Module 7 Objectives**

- Explain IP addresses and how they are constructed
- Name the classes of IP addresses and their characteristics
- Describe Domain Name Service functions
- Define subnetting
- Explain how subnet masking is used
- Name the types of firewalls used today and their characteristics

**In this Module**

The following table shows the contents of this module:

## Lesson 1 – IP Addresses

**Lesson 1: IP Addresses**

In a TCP/IP network, IP addressing is essential to the physical routing of network communications. Every device on a LAN must have a unique IP address. Each address is essential for internetworking over WANs. Students will learn the importance of IP addressing and know the three classes of IP addresses. They will also explore the concepts of domain name service (DNS).

**Lesson 1 Learning Objectives**

- Define IP addresses
- Identify the various classes of IP addresses
- Explain the functions of DNS and Classless Inter-Domain Routing (CIDR)

**Lesson 1 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| IP Address Basics | • Show them their IP, subnets, and MAC addresses with ipconfig /all<br>• Demonstrate converting from binary to decimal on the board. Stress that they will not have to perform this on the test.<br>**My Notes:** |
| IP Address Classes | • Another way to identify the class – the first two bits:<br>Class A – the 1st 2 bits – 00<br>Class B – the 1st 2 bits – 10<br>Class C – the 1st 2 bits – 11<br>**My Notes:** |

**Lesson 1 Topics**, continued

| Topic | Key Points |
|---|---|
| More about IP Addresses | • Stress the benefits of:<br>CIDR – better use of IP addresses<br>DNS – web versus IP address<br>DHCP – easier to manage IP addresses, better use of IP addresses<br>**My Notes:** |

## Lesson 2 - Ports

**Lesson 2: Ports**

This lesson presents information about network ports, what they are, and how they are used, misused, and managed.

**Lesson 2 Objectives**

- Discuss the definition of a port
- Discuss how ports are used in network administration
- Discuss how hackers can identify open ports and what this means to network security

**Lesson 2 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Overview of Ports | • Use an analogy to describe ports as a tunnel or a private phone line. If it's closed, the packet cannot get through.<br>**My Notes:** |
| How Ports are Used | • Used for communication, monitoring traffic flow and security/control.<br>**My Notes:** |
| Configuring TCP/IP | • Use steps in book to manually break up class into different IP address segments.<br>• Based on class structure and setup, IP addresses may be changed for the course.<br>**My Notes:** |

## Lesson 3 - Subnets

**Lesson 3: Subnets**

Networks can be logically divided into sub-networks (subnets) to enhance efficiency and security. This lesson introduces subnetting and the use of subnet masks.

**Lesson 3 Objectives**

- Define subnetting and explain its benefits
- Explain the value of subnet masks
- Identify the components of a subnet mask

**Lesson 3 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Subnet Overview | • Stress that this is *not* on the test<br>• Identify the benefits<br>**My Notes:** |
| Subnet Masks | • Demonstrate with a ipconfig command<br>• Walk through the process, but going too deep could cause confusion<br>• **Exercise:** Practice Subnetting<br>  • Have each student ensure they can see everyone else in their Network Neighborhood<br>  • Logically assign each team into a different subnet – reboot if necessary<br>  • Have students check again to see which computers they can see in Network Neighborhood<br>  • To mix things up, try pinging before/after subnetting.<br>**My Notes:** |

**Lesson 3 Topics**, continued

| Topic | Key Points |
|---|---|
| Virtual LAN | • Another way of subnetting a network<br>• Based on the port on the switch<br>• Easy to look at the GUI setup and make changes<br>• Can be done via MAC address and via switch software – needs to be updated if the NIC changes. Easy to move one computer from one office to another.<br>**My Notes:** |

## Lesson 4 – Network Security

**Lesson 4: Network Security**

Network security, an essential component for network management, strives to protect network resources through layered defenses. These defenses generally contain encryption, anti-virus software, firewalls, and Intrusion Detection System (IDS) devices. This lesson focuses on the network security methods available today.

**Lesson 4 Objectives**

- Explain the various firewall architectures
- Name the types of firewalls used today and their characteristics
- Explain data encryption
- Define the security methods of IDS
- Identify various types of network logs

**Lesson 4 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Data Encryption | • Use whiteboard to demonstrate that Asymmetric and Symmetric Public key is given out to anyone, Private key is not<br>**My Notes:** |
| Anti-virus Software | • Signatures have to be updated<br>**My Notes:** |

**Lesson 4 Topics**, continued

| | |
|---|---|
| Firewalls | • Compare to firewall in car<br>• Can be hardware and software<br>• Stress that they typically log only failed attempts<br>• Stateful Inspection: looks into the packet<br>• Packet-Filtering: Is it incoming and is it part of a requested traffic flow?<br>• Block command<br>• Circuit-Level: much more complex<br>• Three node connection:<br>You ----- Firewall ----- Website<br>• Attackers connect to firewall versus you<br>• Client Software needs to be reprogrammed:<br>Proprietary software may need to be changed to work with this type of firewall. Could be very expensive.<br>• Application Gateway – usually run as software on client:<br>Slower than others, vulnerable to OS bugs<br>Hole in XP = hole in firewall<br>**My Notes:** |
| IDS | • SNORT – open source – downloadable<br>• Host-based vs. Network-based.<br>**My Notes:** |

**Lesson 4 Topics**, Continued

| Topic | Key Points |
|---|---|
| Logs | • Always a potential source of evidence<br>**My Notes:** |
| Network Security Summary | • Explain how IDS, firewalls, etc., can work in partnership<br>•<br>**My Notes:** |

This page intentionally left blank.

# Module 8 - Common Network Crimes

**Overview**

Like physical crimes, network based crimes can be placed into categories. In this module we will look at some of the most commonly perpetrated crimes involving use of network communications and discuss characteristics of each.

**Objectives**

- Describe each of the crimes
- Be able to discuss the methodologies of each crime
- Describe the traditional responses to these crimes.

**In this Module**

Here are the lessons in this module:

## Lesson 1 – E-Mail Scams

**Lesson 1: E-Mail Scams**

Today's criminals use the Internet and know a majority of victims do not look closely at E-mail. As a result E-mail scams are quite prevalent.

**Lesson 1 Learning Objectives**

- Describe E-mail Scams
- Explain how E-Mail Scams are perpetrated
- Describe how investigators typically respond to these attacks

**Lesson 1 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Overview | • Define Scam - a dishonest act or fraud<br>• Simple leap for scammers from surface-<br>• mail to e-mail<br>• Works because people do not closely<br>• inspect mail<br>• Logos and other items to give impression<br>• of respectability<br>**My Notes:** |

**Lesson 1 Topics**, continued

| Topic | Key Points |
|---|---|
| Attack Methodologies | • The Nigerian, or 419 Scam<br>• Foreign Nation<br>• Government connected source<br>• Large sums of money<br>• Money Access<br>• Advance Fee<br>• Where 419 comes from<br>• Phishing<br>• Legitimate looking E-mail in an attempt to<br>• gain financial or personal information<br>• E-Bay/PayPal<br>• Banks<br>• Cross Site Scripting<br>• Spam<br>• Unsolicited advertisement or bulk E-mail<br>•<br>**My Notes:** |
| Investigative Response | • Capture<br>• Preservation<br>• Warrants<br>• Reporting<br>• Education<br>**My Notes:** |

## Lesson 2 – On-line Fraud

**Lesson 2: On-line Fraud**

The Internet is a busy place for business. Because of this there are numerous ways in which a victim can be defrauded in the world of E-Commerce

**Lesson 2 Learning Objectives**

- Describe some of the common online fraud techniques
- Discuss the methodologies used in these cases
- Describe some of the responses to these attacks

**Lesson 2 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Overview | • Online Fraud is any form of trickery or deceptive gain that is practiced on the Internet<br>• Common attack vectors include:<br>• Price to good to be true<br>• Short time to decide<br>• Fine print<br>• Hijacked sites<br>• Box-of-rocks<br>• Stall tactics<br>**My Notes:** |
| Attack Methodologies | • Bogus web sites<br>• Auctions<br>• Bogus Charities<br>**My Notes:** |
| Investigative Response | • Capture<br>• Preservation<br>• Warrants<br>• Reporting<br>• Education<br>**My Notes:** |

## Lesson 3 – Identity Theft

**Lesson 3: Identity Theft**

In 2007 there were an estimated 8.4 million reported cases of identity theft in the U.S. That number is down from the reported 10.1 million in 2003. Even with the decline the identity theft problem is ever present in society today

**Lesson 3 Learning Objectives**

- Describe some of the common online identity theft techniques
- Discuss the methodologies used in these cases
- Describe some of the responses to these attacks

**Lesson 3 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Overview | • Numerous ways in which a criminal or<br>• attacker can gain enough information to assume some else's identity<br>• Search Engines<br>• Public information sites<br>• Group sites<br>• Commercial sites<br>• Membership sites<br>**My Notes:** |
| Attack Methodologies | • Name<br>• Phone<br>• Social Security Number<br>• Address<br>• License Plate<br>**My Notes:** |

**Lesson 3 Topics**, continued

| Topic | Key Points |
|---|---|
| Investigative Response | • Capture<br>• Preservation<br>• Warrants<br>• Reporting<br>• Education<br>**My Notes:** |

## Lesson 4 – Social Threats

**Lesson 4: Social Threats**

The Internet has created a layer of perceived anonymity for criminals. This has led to an increase in social threats perpetrated on the Internet.

**Lesson 4 Learning Objectives**

- Describe some of the common online social threats
- Discuss the methodologies used in these cases
- Describe some of the responses to these attacks

**Lesson 4 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Predators | • Communicate with other people on the Internet without them being able to know the "real person"<br>• Ability to lead victims to thinking predator is different than what victim thinks<br>**My Notes:** |
| Stalkers | • Will look for those who meet their victim criteria online and then begin the stalking process<br>• Use available information to choose victims<br>• May not be known to victim<br>**My Notes:** |
| Cyberbullying | • Usually always in reference to children<br>• When children use the Internet to bully, harass, embarrass, or demean another child it is considered cyberbullying<br>• Cyberbullying has led to murder and suicide.<br>**My Notes:** |

**Lesson 4 Topics,** Continued

| Topic | Key Points |
|---|---|
| Attack Methodologies | • E-mail<br>• Chat<br>• Texting<br>• Impersonation<br>**My Notes:** |
| Investigative Response | • Capture<br>• Preservation<br>• Warrants<br>• Reporting<br>• Education<br>**My Notes:** |

## Lesson 5 – Internal Threats

**Lesson 5: Internal Threats**

Without a doubt, the greatest network threat is the internal threat. Persons with knowledge of the internal workings of a system or company have the greatest capability for potential damage.

**Lesson 5 Learning Objectives**

- Describe some of the common internal threats
- Discuss the methodologies used in these cases
- Describe some of the responses to these attacks

**Lesson 5 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Overview | • Greatest threat to network<br>• Insider has working knowledge of network<br>• Has access<br>• Greatest ability for potential damage<br>**My Notes:** |
| Attack Methodologies | • Inappropriate Usage<br>• Embezzlement<br>• Extortion<br>• Espionage<br>• Sabotage<br>**My Notes:** |
| Investigative Response | • Capture<br>• Preservation<br>• Warrants<br>• Reporting<br>• Education<br>**My Notes:** |

## Lesson 6 – Malicious Code

**Lesson 6: Malicious Code**

Malicious Code is the generic term for a collection of attacks that use any type of script or program designed to exploit security vulnerabilities. Worms, Trojans, Viruses, Backdoors are all examples of malicious code.

**Lesson 6 Learning Objectives**

- Describe some of the common malicious code threats
- Discuss the methodologies used in these cases
- Describe some of the responses to these attacks

**Lesson 6 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Malicious Code Attacks | • Viruses<br>• Trojans<br>• Worms<br>• Spyware<br>• Adware<br>• Rootkits<br>**My Notes:** |
| Investigative Responses | • Capture<br>• Preservation<br>• Warrants<br>• Reporting<br>• Education<br>**My Notes:** |

## Lesson 7 – Denial of Service Attacks

**Lesson 7: Denial of Service Attacks**

For some attackers, simply making a resource un-available is the satisfaction of the attack. The Denial of Service attack is the goal of these criminals.

**Lesson 7 Learning Objectives**

- Describe some of the common Denial of Service threats
- Discuss the methodologies used in these cases
- Describe some of the responses to these attacks

**Lesson 7 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| DOS Attack | • Flooding target computer with more information than it can handle, causing a system crash or reset.<br>• Interfering with communications channel in a way that others can't access system.<br>• Starting a number of processes on target system in a way that all available resources are used and system can no longer respond to requests.<br>• Changing access codes so that normal users of the system can no longer access the system.<br>**My Notes:** |
| DDOS Attack | • When multiple systems attack a target system.<br>• Multiple systems are usually other compromised systems over which attacker has control.<br>**My Notes:** |

**Lesson 7 Topics,** Continued

| Topic | Key Points |
|---|---|
| Investigative Response | • Capture<br>• Preservation<br>• Warrants<br>• Reporting<br>• Education<br>**My Notes:** |

## Lesson 8 - Extortion

**Lesson 8: Extortion**

Creating a sense of fear in a victim and then asking for money to make the fear stop is the goal of an extortionist. The Internet has allowed this old-school criminal activity to continue in a modern mode.

**Lesson 8 Learning Objectives**

- Describe some of the common extortion threats
- Discuss the methodologies used in these cases
- Describe some of the responses to these attacks

**Lesson 8 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Extortion on the Internet | • Usually e-mail threat against person, relative or property<br>• Direct threats<br>• Threats against tangible or non-tangible data<br>• Threats against a web entity<br>• Protection<br>**My Notes:** |
| Investigative Response | • Capture<br>• Preservation<br>• Warrants<br>• Reporting<br>• Education<br>**My Notes:** |

# Lesson 9 – Network Attacks

**Lesson 9: Network Attacks**

These types of attacks involve targeting the equipment and systems that comprise an entire network.

**Lesson 9 Learning Objectives**

- Describe some of the common Network Attacks
- Discuss the methodologies used in these cases
- Describe some of the responses to these attacks

**Lesson 9 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Network vs. System Level Attacks | • Routers.<br>• Domain Name Servers<br>• Firewalls<br>• Intrusion Detection Systems.<br>• Wireless networking equipment<br>• Access control systems<br>**My Notes:** |
| Investigative Responses | • Capture<br>• Preservation<br>• Warrants<br>• Reporting<br>• Education<br>**My Notes:** |

## Lesson 10 - Terrorism

**Lesson 10: Terrorism**

Historical accounts vary but it is generally agreed that terrorism has been on the Internet years before the attacks of September 11th. Any time that the Internet is used by a person or group to intimidate and instill fear in others, it is called terrorism.

**Lesson 10 Learning Objectives**

- Describe some of the common Terrorist Attacks
- Discuss the methodologies used in these cases
- Describe some of the responses to these attacks

**Lesson 10 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Internet Terrorist Methodologies | • Terrorism<br>• Fear<br>• Intimidation:<br>• Psychological warfare<br>• Propaganda<br>• Fund-raising<br>• Message center for coordinating activities<br>• Launch network attacks<br>• Data mining<br>• Denial of Service attacks against enemies<br>• Site defacements of web sites counter to their cause<br>• Spam e-mail attacks against enemies<br>• Phishing attacks for banking information to help fund activities<br>**My Notes:** |
| Investigative Response | • Capture<br>• Preservation<br>• Warrants<br>• Reporting<br>• Education<br>**My Notes:** |

# Module 9 - Phases of an Intrusion

**Module 9 Overview**

In order to understand how network intrusions happen you need the understanding of the phases which occur as the attacker plans and then executes the intrusion. This module illustrates those phases in depth.

**Module 9 Exercises**

None, other than the procedures in the manual.

**Module 9 Testing**

This module is not tested.

**Module 9 Objectives**

- Define network intrusions.
- Understand the phases of an intrusion
- Understand the information that an attacker can gather offline
- Understand the goals, strategies and techniques employed by the attacker.
- Know attacker profiles

**In this Module**

The following table shows the contents of this module.

## Lesson 1 – Defining an Intrusion

**Lesson 1: Defining an Intrusion**

Technically complex network intrusions can be difficult to identify. To do so you need to understand how intruders conduct these attacks.

**Lesson 1 Learning Objectives**

- Define Network Intrusion
- Discuss the vulnerabilities attackers look for in a target

**Lesson 1 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Intrusions | • Explain the definition of Intrusion, Vulnerability, Exploit and Threats or Threat Agents.<br>• Explain the goals of the intrusion and how they can be combined in several ways.<br>• Explain the types of intruders and their profiles.<br>• Touch on how insiders are the largest threat to any system.<br>• Describe the phases of an intrusion. Mention how once the attack has succeed the phases will start again from the inside and propagate throughout the internal network.<br>**My Notes:** |

## Lesson 2 - Reconnaissance

**Lesson 2: Reconnaissance**

In this lesson, the topic of how an attacker will do research on the system and resources to better understand the target.

**Lesson 2 Learning Objectives**

- Explain the purposes and methods of reconnaissance.
- Explain the difference between direct and indirect methods
- Describe some specific tools and techniques used

**Lesson 2 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Goals | • Discuss the information gathering mindset and methodologies.<br>• Describe the types of data that are searched for and used.<br>**My Notes:** |
| Direct vs. Indirect | • Describe how direct actions can be logged by the target, but indirect actions are not.<br>**My Notes:** |
| General Web Browsing | • Explain how site administrators will inadvertently leave information on a site that can be used by attackers.<br>**My Notes:** |
| Public Records | • Discuss the amounts of information that is available from public data repositories.<br>**My Notes:** |

**Lesson 2 Topics**, continued

| Topic | Key Points |
|---|---|
| DNS & Whois | • Show how the information in a DNS entry can be a wealth of information to an attacker.<br>**My Notes:** |
| The Wayback Machine | • Show how the archive site can display information that has been removed from a site but is still available from an archive copy.<br>**My Notes:** |
| Other sources | • Cover the other misc sources of information that may be available to attackers.<br>**My Notes:** |
| Target site Examination | • Discuss how the source code and information on all the pages of a target site can be examined freely.<br>•<br>**My Notes:** |

**Lesson 2 Topics**, continued

| Topic | Key Points |
|---|---|
| Attack vectors | • Show how any way into a system that has been discovered is a possible vector.<br>• Modems, faxes, telephone systems and any other in-route is a possible target of opportunity.<br>• Wireless is a popular attack vector because of the many weaknesses in that area.<br>**My Notes:** |
| Identification Live Host information | • Any information that is in a packet of data coming from the host is used.<br>• Probing these areas will potentially give information to the attacker.<br>• Any open port or protocol will be discovered and probed.<br>• Banners and other identifiers will be gathered and used to determine versions and known weaknesses.<br>**My Notes:** |
| Vulnerability scans | • The same scanning tools that system administrators use to harden a system are used by the attackers<br>**My Notes:** |

## Lesson 3 – Network Attacks

**Lesson 3: Network Attacks**

In this lesson, we look at the attack phase of an intrusion

**Lesson 3 Learning Objectives**

- Explain the goals of the attack
- List the major strategies used in an attack
- Understand some of the techniques an attacker can use to damage the functionality of a system or network

**Lesson 3 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Goals | • Discuss how the attacker wants to gain a foothold and advance his presence on the target<br>**My Notes:** |
| Authentication and Guessing | • Discuss how authentication attacking works.<br>• Talk about the many types of guessing and cracking tools there are.<br>• Note that there are all types of value metrics used to generate an attack.<br>• Credential discovery and reset techniques should be covered<br>**My Notes:** |

**Lesson 3 Topics** Here are the topics to present.

| Topic | Key Points |
|---|---|
| Identification Live Host information | • Any information that is in a packet of data coming from the host is used.<br>• Probing these areas will potentially give information to the attacker.<br>• Any open port or protocol will be discovered and probed.<br>• Banners and other identifiers will be gathered and used to determine versions and known weaknesses.<br>**My Notes:** |
| Input attacks | • Discuss how using too much input or incorrect input the system can be brought to a stop or exploited<br>• SQL injection attacks are popular and effective. Describe them<br>• Directory traversal is another popular attack type.<br>**My Notes:** |

## Lesson 4 - Entrenchment

**Lesson 4: Entrenchment**

In this lesson, we look at the entrenchment phase of an intrusion

**Lesson 4 Learning Objectives**

- Explain the goals of entrenchment
- List the major strategies used
- Understand some of the techniques an attacker can use to hide traces of unauthorized activity

**Lesson 4 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Goals | • Discuss how the attacker wants to preserve his presence on the exploited system.<br>**My Notes:** |
| Log Cleaning | • Explain how the attacker will remove traces of his presence on the system.<br>**My Notes:** |
| Automatic execution | • The attacker will setup programs to run on system startup to ensure his continued access.<br>**My Notes:** |

**Lesson 4 Topics**, continued

| Topic | Key Points |
|---|---|
| Hooking | • Discuss how the attacker will attach programs to other programs to hide his work.<br>•<br>**My Notes:** |
| File types and naming conventions | • Show how the attacker will change file extensions and names to obfuscate his use of known attacker tools.<br>•<br>**My Notes:** |
| Remote connections and Backdoors | • Explain how the attacker will use remote connectivity and backdoor programs to make use of the system easier.<br>•<br>**My Notes:** |

## Lesson 5 – Infiltration and Extraction

**Lesson 5: Infiltration and Extraction**

In this lesson, we look at the infiltration and extraction phase of an intrusion

**Lesson 5 Learning Objectives**

- Explain the purpose and methods of inflitration
- Explain the importance of trust relationships
- Determine the data types targeted by attackers and how these types are extracted.

**Lesson 5 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Sniffers | • Describe how once the attacker is on the system he uses it as a springboard to repeat the phases of an intrusion on other nearby systems.<br>• Show how sniffing of the target network is beneficial to the attacker.<br>**My Notes:** |
| Trust Relationships | • Explain how dangerous these relationships are once the attacker is on the network.<br>**My Notes:** |
| Data Extraction | • Discuss the types of data the attacker is interested in and how it is typically transferred.<br>**My Notes:** |

This page intentionally left blank.

# Module 10 - Report Writing

**Module 10 Overview**

Investigations require comprehensive reporting that documents actions and summarizes findings. The best reports are clear, concise, and accurate and report only information relevant to the facts of the case.

**Objectives**

- Discuss the importance of writing an organized, clear, concise and accurate report
- Write an organized, clear, concise, and accurate report
- Discuss the appropriate interviewing techniques for conducting investigations in a highly technical environment

**In this Module**

The following table shows the contents of this module:

## Lesson 1 – General Report Writing Techniques

**Lesson 1: General Report Writing Techniques**

Forensic reports involving the analysis of digital evidence should address the same basic information. No matter how well an investigator conducts analysis, it is of little value if results cannot be reported in an organized, clear, complete and concise manner.

**Lesson 1 Learning Objectives**

- Discusses the purpose and need for forensic analysis
- Explains what physical and/or logical evidence was analyzed
- Defines programs, terms, and their relevance
- Explains findings in an orderly manner
- Associates relevant evidence with users

**Lesson 1 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| The Forensic Report | • Culmination of a process often involving intensive and painstaking work<br>• Should reflect the time, effort and professionalism involved in building the case and acquiring the information<br>• Should be well organized, include only relevant information, and be free of grammatical, punctuation and spelling errors<br>• Recipient should be able to read it one time and have a very clear understanding of the message you are trying to convey<br>• Consider the report a reflection of your professionalism and develop it as such<br>**My Notes:** |

**Lesson 1 Topics** Here are the topics to present.

| Topic | Key Points |
|---|---|
| Examiner Notes | • Documentation that is created during the analysis process provides basis for examiner to report results of case<br>• Should be preserved and may be discoverable in court<br>• Foundation on which many digital media-related cases are built<br>• Should present a clear timeline of the actions taken and the results of those actions<br>• Provide a repeatable roadmap of your examination<br>• Number, date, and initial all note pages<br>• Ensure that you can accurately testify to actions taken during the examination<br>**My Notes:** |

**Lesson 1 Topics**, Continued

| Topic | Key Points |
|---|---|
| Forensic Reporting | • Should contain all relevant evidence found during examination<br>• Clearly identify persons related to examination including you, requestor, suspects, and other pertinent individuals<br>• Provide details about purpose for forensic analysis<br>• Describe physical and/or logical evidence analyzed<br>• Define related programs, terms and their relevance<br>• Clearly and concisely explain items of evidentiary value found on suspect media as a result of analysis<br>• Identify location and relevance of items of evidentiary value as relating to reason for analysis and/or investigation<br>• Report heading<br>• Support requested, reason or purpose for analysis<br>• Summary of findings<br>• Digital media analyzed<br>• Analysis/Suspect Software Listings<br>• Glossary of Technical Terms<br>• Detail of Findings<br>• Items Provided<br>**My Notes:** |

**Lesson 1 Topics**, Continued

| | |
|---|---|
| Title Page | • Provides an overview of the case<br>• Report Header<br>• Support Requested<br>• Current Case Status<br>• Summary of Findings<br>• Title (To:)<br>• From<br>• Subject<br>• Support Requested or Purpose for Analysis<br>• Status<br>• Summary of Findings<br>• Footer<br>**My Notes:** |
| Items Analyzed | • Describes in detail analyzed physical and/or logical evidence<br>• Always include original *and* verified hash values of all evidence items<br>• Physical Items:<br>• Manufacturer<br>• Model, serial, and part number (when possible)<br>• Item description<br>• Any specific markings<br>• Logical Items:<br>• List the image files<br>• Original file name and include any hash or other validation mechanism<br>**My Notes:** |

**Lesson 1 Topics**, Continued

| Topic | Key Points |
|---|---|
| Relevant Software | • Identifies software found on evidence media relevant to case as well as identity of forensic software used to perform analysis<br>• Analysis Software<br>• List all software applications used during the forensic examination<br>• Version and brief description of software's functionality or use<br>• Suspect Software<br>• Software name and version<br>• Full path to where application located on suspect media<br>• Brief description of program functionality and how it relates to Request for Analysis and/or investigation<br>• Be prepared to further explain items in this listing during prosecution<br>**My Notes:** |
| Glossary | • Defines technical terms, document formats, and procedure details referenced in report that may not be readily understood by average non-technical reader<br>**My Notes:** |

**Lesson 1 Topics**, Continued

| Topic | Key Points |
|---|---|
| Details of Findings | • Provides detailed information about any items of evidentiary value found on suspect media during forensic examination<br>• Should be thorough, concise, only contain details relevant to request for analysis and/or investigation<br>• Should *not* contain information about processes executed that did not produce relevant information, unless negative result is relevant<br>• Discuss organization<br>• Discuss use of hyperlinks<br>**My Notes:** |
| Items provided | • Details *all* of physical items returned to requestor with report<br>• Should include all items specified in Items Analyzed section<br>**My Notes:** |
| Reporting scenario | • Discuss example and how it incorporates information discussed in lesson<br>**My Notes:** |

## Lesson 2 – Cyber Case Interviewing Techniques

**Lesson 2: Cyber Case Interviewing Techniques**

Interviews are an essential element of developing information that is relevant to a criminal investigation. When conducting a cyber crime investigation, investigators must prepare for the interview, develop rapport with interview subjects, ask questions that generate corroborative information and leads, and terminate the interview in a way that leaves the door open for further questions.

**Lesson 2 Learning Objectives**

- Develop a plan to conduct interviews in a cyber investigation
- Explain the psychology and culture of the technology world and
- ways to apply that knowledge to the interview process
- Ask questions that will provide you with information that will assist the investigation

**Lesson 2 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Cyber Crime Interviews | • Investigator must obtain information from all people who are involved with the incident.<br>• Interview of a suspect may assist in revealing true scope of investigation and provide information needed to ensure conviction of a suspect<br>• Integral part of any investigation, victims, witnesses, and perpetrators all have pieces of puzzle that investigator is trying to put back together<br>• Investigator must skillfully navigate human landscape to develop leads, confirm events, and obtain complete picture of crime<br>• Accusatory versus Non-Accusatory Interviews<br>**My Notes:** |

**Lesson 2 Topics**, continued

| Topic | Key Points |
|---|---|
| Interview Process | • Planning/Research<br>• Opening/Rapport<br>• General Questioning<br>• Detailed Questioning<br>• Interview Termination<br>• Interview Psychology<br>• Investigator Initiated Contact<br>• Organization Initiated Contact<br>• Witness and Victims<br>• Issues to Address During Interviews<br>• Suspects<br>**My Notes:** |

This page intentionally left blank.

# Module 11 - Legal Issues

**Overview**

No matter how solid a case may be or incriminating the evidence, all computer crime investigations must be conducted in way that adheres to established legal principles. If legal standards are not met the case could be jeopardized and even dismissed, thus allowing a perpetrator to walk free.

**Purpose of this Module**

The purpose of this module is to familiarize students with some of the basic legal issues that must be considered when conducting an investigation involving digital data.

**Objectives**

After successfully completing this module, you will be able to:

- Understand some of the legal issues involved in a digital investigation
- Employ practices during an investigation that that will pass legal challenge

**In this Module**

The following table shows the contents of this module:

## Lesson 1 – Search Warrants

**Lesson 1: Search Warrants**

Searches of an individual or a location require a search warrant or a valid exception under the 4th Amendment to the U.S. Constitution

**Lesson 1 Learning Objectives**

- Understand how the 4th amendment of the United States Constitution is interpreted by the Courts
- Recognize situations in which the investigators may search or seize without a warrant
- Discuss the types of consent and their requirements

**Lesson 1 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Search Warrants | • 4th Amendment Overview<br>• What is an unreasonable search<br>• Probable Cause<br>• Affidavit<br>• Items to be Seized<br>• USDOJ-CCIPS<br>• Warrant Execution<br>**My Notes:** |
| Search Warrant Exceptions | • Consent<br>• Stop and Frisk<br>• Search Incident to Arrest<br>• Immediate threat to life or serious bodily injury<br>• Immediate threat of the destruction of evidence<br>• Fresh pursuit<br>• Plain view<br>• Vehicle searches<br>• Custodial searches<br>• Border searches<br>**My Notes:** |

**Lesson 1 Topics,** Continued

| Topic | Key Points |
|---|---|
| Consent Searches | • Voluntary Consent<br>• Informed Consent<br>• Withholding Consent<br>• Withdrawing Consent<br>• 3rd Party Consent<br>**My Notes:** |
| Stop and Frisk Searches | • May not seem applicable to digital investigations<br>• If cell phone, PDA or other digital device found during search you may request consent to browse text messages<br>**My Notes:** |
| Search Incident to Arrest | • Again, may not seem applicable to digital investigations<br>• If cell phone, PDA or other digital device found during search you may request consent to browse text messages<br>**My Notes:** |

## Lesson 2 – Internet Service Providers

**Lesson 2: ISP's**

Many crimes involve the use of commercial and private networks and communications facilities. These records are usually maintained by entities often referred to as Internet Service Providers (ISPs). ISPs often maintain records of accounts, billing, transactions, and content of the communications and data that travel over their networks.

During an investigation, you will need to gather this pertinent information from ISPs. It is imperative that an investigator understands the proper way to request these records, so they are admissible as evidence in a criminal proceeding.

**Lesson 2 Objectives**

- Explain which laws apply to a given authority and know where to find those laws
- Describe the search authorities for gathering records
- Prepare requests for records

**Lesson 2 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Legal Framework | • ECPA<br>• Consent<br>• Express Consent<br>• Written Consent<br>• 3rd Party Consent<br>**My Notes:** |
| Preservation letters | • 18 USC § 2703(f)<br>• Time Limitations<br>• Limitations (Snapshot at time of receipt)<br>• One renewal for additional 90 days<br>•<br>**My Notes:** |

**Lesson 2 Topics**, Continued

| | |
|---|---|
| Subpoenas | • Business Records<br>• Testimony<br>• Subscriber Records<br>•<br>**My Notes:** |
| ”D” Order | • 18 U.S.C. § 2703(d)<br>• Transactional Records<br>• Content<br>• Reasonable Grounds and Relevant<br>**My Notes:** |

This page intentionally left blank.

# Module 12 - Fundamentals of Log Analysis

**Module 12 Overview**

The analysis of computer network intrusions is a difficult task. The Scientific Method provides a general framework that can be used to effectively guide the investigation.

**Module 12 Exercises**

None, other than the procedures in the manual.

**Module 12 Testing**

This module is not tested.

**Module 12 Objectives**

- Describe the main steps of the Scientific Method
- Explain how the Scientific Method can be applied to digital forensic analysis
- Use the initial observations in a case to determine the most likely location of additional, related artifacts
- Apply the analysis techniques learned in the previous modules to analyze log files that contain evidence of an intrusion

**In this Module**

The following table shows the contents of this module.

## Lesson 1 – The Scientific Method and Intrusion Analysis

**Lesson 1: The Scientific Method and Intrusion Analysis**

The Scientific Method is used as a guide for investigating any problem, including a network intrusion. It is a simple but effective process by which you generate a hypothesis based upon observed events, then design and select analysis tasks to help you evaluate that hypothesis.

**Lesson 1 Learning Objectives**

- Define the Scientific Method
- Explain how the Scientific Method can guide an intrusion investigation.

**Lesson 1 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| The Scientific Method | • *Observation*: Observing one or more events or sets of events. Observation establishes the facts surrounding these events to identify their cause and consequences.<br>• *Hypothesis:* A hypothesis is generated that explains the observed events, including their root cause, interrelationship, and consequences.<br>• *Prediction*: Predictions are made as to the possible nature and location of artifacts in the evidence that will either support or contradict the hypothesis.<br>• *Evaluation*: Performing procedures that test for the presence of artifacts that support, falsify, or modify the hypothesis.<br>• *Conclusion*: Formation of a conclusion, based upon the results of tests performed during the Evaluation step.. |
| | **My Notes:** |

## Lesson 2 – Observing Intrusion Activity and Forming a Hypothesis

**Lesson 2: Observing Intrusion-related Activity and Forming a Hypothesis**

The first step of the Scientific Method applied to an intrusion is to identify the current set of observations and form a hypothesis based upon those observations.

**Lesson 2 Learning Objectives**

- Describe common intrusion-related observations
- Form a hypothesis
- Describe common incident classifications

**Lesson 2 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Common Observations | • Discuss how network intrusion investigations should normally begin with one or more specific observations. These observations guide the formation of a hypothesis as to what may have occurred.<br>**My Notes:** |
| Common Primary Observations | Many different events can spark an intrusion investigation. Some examples include:<br>• Antivirus alerts<br>• IDS/IPS alerts<br>• System/applications errors<br>• Abnormal authentication patterns<br>• Access control list violations<br>• Generic unusual activity<br>**My Notes:** |

**Lesson 2 Topics**, continued

| Topic | Key Points |
|---|---|
| Supplementary Observations | • The incident responder should make supplementary observations before creating a hypothesis. Examples of this data are:<br>• Network diagrams<br>• Device documentation<br>• Contact information<br>**My Notes:** |
| Common Observation Attributes | • Observations made during network intrusions will have attributes that should be recorded. These attributes include, but are not limited to the following<br>• Date/Time<br>• IP Addresses<br>• Port Numbers<br>• Accounts and aliases<br>• Host names and aliases<br>• Files<br>• General description.<br>**My Notes:** |
| Recording Observations | • Observations can be recorded in many different forms including written notes, office documents, and databases. You should use the approved and tested method used by your organization. This course uses a spreadsheet template for recording this data.<br>**My Notes:** |

**Lesson 2 Topics**, continued

| Topic | Key Points |
|---|---|
| Hypothesis Formation | • This hypothesis should include a statement regarding each of the following<br>  • What/How<br>  • Where<br>  • Who<br>  • Why<br>**My Notes:** |
| Multiple Hypothesis | • Cover the concept of breaking a large hypothesis into smaller sections and proving each in turn.<br>**My Notes:** |
| Incident Classifications | • Discuss the various classifications that incidents fall into including:<br>• Denial of Service (DOS)<br>• Malicious Code<br>• Unauthorized Access<br>• Inappropriate Usage<br>• Suspicious Activity<br>• Multiple Components<br>•<br>**My Notes:** |

## Lesson 3 – Predicting the Nature & Location of Intrusion Artifacts

**Lesson 3: Predicting the Nature and Location of Intrusion Artifacts**

The purpose of this lesson is to teach you how to determine potential locations of artifacts related to your hypothesis.

**Lesson 3 Learning Objectives**

- Determine the applications and network traffic types that were involved in observed events
- Determine the flow of network traffic related to observed events
- Predict artifact location based upon the network architecture, probably traffic flow and related applications

**Lesson 3 Topics**,

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Finding Intrusion Artifacts | • Discuss the plan and mapping of artifacts to make the evaluation of facts easier.<br>**My Notes:** |
| Relating Observed Events to Applications | • You need to correlate all observed events to the applications involved. This will help you to locate potential artifacts.<br>**My Notes:** |

**Lesson 3 Topics**, Here are the topics to present.

| Topic | Key Points |
|---|---|
| Identification Live Host information | • Any information that is in a packet of data coming from the host is used.<br>• Probing these areas will potentially give information to the attacker.<br>• Any open port or protocol will be discovered and probed.<br>• Banners and other identifiers will be gathered and used to determine versions and known weaknesses.<br>**My Notes:** |
| Network Traffic Flow and Intrusion Artifacts | • One simple way to identify devices that may contain relevant data is to locate all devices that related traffic may have passed through<br>**My Notes:** |
| Predicting Artifact Location | • Discuss prediction of artifacts on:<br>• Devices<br>• File<br>• Directories<br>**My Notes:** |

## Lesson 4 – Using Log Analysis to Evaluate and Intrusion Hypothesis

**Lesson 4: Using Log Analysis to Evaluate an Intrusion Hypothesis**

The purpose of this lesson is to describe how log analysis techniques are used to evaluate an intrusion hypothesis.

**Lesson 4 Learning Objectives**

- Determine the format of log files
- Use search, filter, and extraction techniques to evaluate a hypothesis
- Record findings and keep track of new leads

**Lesson 4 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Hypothesis Evaluation | • Discuss how a hypothesis is evaluated using digital forensic data acquisition and analysis techniques<br>**My Notes:** |
| Procedure Selection | • Explain how there are multiple methods of searching and filtering log files.<br>**My Notes:** |

**Lesson 4 Topics**, continued

| Topic | Key Points |
|---|---|
| Acquiring Log Files | • Log files may be provided directly to you by an incident responder or network administrator who collected them from the original source media.<br>• You may obtain a physical or logical image of the original storage media containing the log files, and then extract the logs from that image.<br>• You may logically copy log files from the source system or device.<br>**My Notes:** |
| Previewing Log Formats | • Before analyzing collected logs, you should first preview the format of those logs to ensure that you know how to read them properly and use the correct methods for searching them.<br>**My Notes:** |
| Determining File Type | • The first step in previewing log format is to determine the file type.<br>**My Notes:** |
| Determining Data Format within a Log | • Once you know the file type for each log, you should identify the format of the data within. For network traffic capture logs, this is relatively uniform. Text logs will vary.<br>**My Notes:** |

**Lesson 4 Topics**, Continued

| Topic | Key Points |
|---|---|
| Search/Extraction Criteria | • Describe the general goal will be to search for and extract log entries, or portions of log entries that support or contradict your hypothesis.<br>**My Notes:** |
| Correlation: Timeline Unification | • The main task of correlation is the establishment of a unified timeline.<br>**My Notes:** |
| Correlation: Event Verification | • Verify events by checking each log entry for another recording of the same event from other sources.<br>**My Notes:** |
| Correlation: Using Event Verification to Synchronize Times | • The dates/times for events verified against multiple sources can also be compared to see if there is a time skew between the data sources.<br>**My Notes:** |
| Lead Tracking | • In addition to your investigative notes, leads should be recorded in your Attribute List spreadsheet along with other relevant data.<br>**My Notes:** |

This page intentionally left blank.

# Module 13 - Log Sources

**Overview**

Knowing where the logs of interest reside on a system is a key piece of information when starting a network investigation. This module will show you some of the typical locations of logs for select applications and systems.

**Objectives**

- Describe the storage locations of typical log files
- Be able to discuss some of the log file formats
- Be able to recognize IDS logs and their contents.

**In this Module**

Here are the lessons in this module:

## Lesson 1 – Windows Log Sources

**Lesson 1: Windows Log Sources**

This lesson will cover the most common logs found in a Windows environment.

**Lesson 1 Learning Objectives**

- Know where Windows Logs are stored
- Understand naming conventions of log files
- Know some of the file formats for these files

**Lesson 1 Topics** Here are the topics to present.

| Topic | Key Points |
|---|---|
| Windows Logs | • **Mail** - Outlook or Outlook Express as a mail client<br>• Default log files in Windows 2000, Server 2003 and XP inside each user's profile<br>• Outlook's MAPI accounts, found at: C:\Documents and Settings*username*\Local Settings\Temp\Opmlog.log<br>• If user established Hotmail account in Outlook, events logged in: C:\Documents and Settings*username*\Local Settings\Temp\Outlook Logging\Hotmail\http0.log.<br><br>• **Microsoft SQL Databases** - stores its log files in C:\MSSQL\LOG<br>• ERRORLOG<br>• SQLAGENT.OUT<br>• SQLDump9999.txt/SQLDump9999.mdmp<br><br>• **MySQL** - free, open source database application that is also popular on many Windows systems<br>• Default location for installation of MySQL C:\Program Files\MySQL\MySQL Server X.X<br>• Cover subdirectories under this<br>•<br>• **Microsoft Access -** Errors in Windows Event log<br>•<br>**My Notes:** |

**Lesson 1 Topics**, Continued

| Topic | Key Points |
|---|---|
| Windows Logs, Continued | • Internet Information Server (IIS)<br>• Service used by Windows based servers to host web, FTP, and e-mail services<br>• Depending on version, logs found in different locations<br>• IIS versions 4 and 5, on Windows NT 4.0 and Windows 2000, log files stored in: C:\winnt\system32\logfiles<br>• IIS version 6 and 7, on Windows XP and newer systems, log files stored in: C:\windows\system32\logfiles<br>• Log file names will be named "W3SVC"<br>• FTP and DNS messages mingled in same file if services active<br><br>• System Logs<br>• Application, Security and System<br>• Use Event Viewer to view<br>• Logs can be exported<br>•<br>• Directory Services<br>• Events will be in Event Viewer in Directory Services<br><br>• Remote Logs<br>**My Notes:** |

## Lesson 2 - Linux Log Sources

**Lesson 2: Linux Log Sources**

This lesson will cover the common and most used logs found in a Linux environment.

**Lesson 2 Learning Objectives**

- Know where Linux Logs are stored
- Understand naming conventions of log files
- Know some of the file formats for these files

**Lesson 2 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Linux Logs | • Mail Logs<br>• Mail services provided by sendmail processes<br>• Logs for these services can usually be found in the file: /var/log/maillog<br><br>• Databases<br>• MySQL most popular database program in Linux<br>• Logs typically be found in /var/log/mysqld.log file<br><br>• Services<br>• Show the log files here, bringing up live examples on a demo session.<br><br>• Directory Management<br>• Third party add-on tools provide service<br>• Seek documentation for specific AD tool and determine location of logs for each<br>**My Notes:** |

**Lesson 2 Topics**, Continued

| Topic | Key Points |
|---|---|
| Linux Logs, Continued | • System Logs<br>• Most Linux system log entries are located in /var/log/message file<br><br>• Remote Logs<br><br>**My Notes:** |

## Lesson 3 - Solaris Log Sources

**Lesson 3: Solaris Log Sources**

This lesson will cover the common and most used logs found in a Solaris environment.

**Lesson 3 Learning Objectives**

- Know where Solaris Logs are stored
- Understand naming conventions of log files
- Know some of the file formats for these files

**Lesson 3 Topics** Here are the topics to present.

| Topic | Key Points |
|---|---|
| Solaris Logs | • Mail<br>• May find file in /etc directory called syslog.conf, and it may have the location of sendmail logs listed inside<br><br>• Databases<br>• Logs in default locations of either /usr/local/mysql/data or /opt/mysql/mysql/data.<br><br>• Services<br>• Most services put log messages in /var/adm/messages log file, general catch all file for log entries in Solaris<br><br>• Directory Management<br>• Third party add-on tools available providing this service<br>• Seek documentation for specific AD tool<br><br>• System<br>• System log files will be located in /var directory in Solaris<br>• Usually several nested directories of log files under /var directory<br>• Cannot open files in use<br><br>• Remote Logs<br>• Search for pipes and hard links to mounted volumes in order to discover whether logs are being stored remotely on Solaris |
| | **My Notes:** |

## Lesson 4 – Log Searching

**Lesson 4: Log Searching**

This lesson will cover several ways to manually search through a log file.

**Lesson 4 Learning Objectives**

- Know how to use the findstr command
- Know how to use Grep/Egrep
- Understand the basics of regular expressions

**Lesson 4 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Log Searching | • Flexibility is most important feature for any tool used<br>• Variety of log files require search for different types of values<br><br>• **GREP** / **EGREP** **-** Primary applications used for searching and filtering text logs<br>• Many advanced functions only work in egrep, not in grep, so egrep is standard<br>• Regular expressions are most common method for defining search parameters, used in many other popular applications, such as PERL, Snort, and EnCase<br>• Typically found in just Unix, Linux, and OS X environments<br>• Versions available for the Windows<br><br>• FINDSTR<br>• Windows equivalent of Grep<br>**My Notes:** |

**Lesson 4 Topics,** Continued

| Topic | Key Points |
|---|---|
| Regular Expressions | • Patterns used for executing searches and filters<br>• Combining literal text and special characters, called *metacharacters,* to create a pattern<br>• Provide examples of items that use set patterns:<br>• IP addresses<br>• Dates and time<br>• Phone numbers<br>• URLs<br>• Credit card numbers<br>• Social Security numbers<br><br>• **Literal Character Searches -** Simplest type of regular expression<br>• Grep is much more powerful than what is presented here, but keep information very light unless the class is technically advanced. If so, bring up "* . ^", metacharacters as an introduction.<br><br>**My Notes:** |

## Lesson 5 – IDS Logs

**Lesson 5: IDS Logs**

This lesson will cover Intrusion Detection System logs

**Lesson 5 Learning Objectives**

- Understand the importance of IDS logs
- Understand how Snort is used

**Lesson 5 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| IDS Logs | • Intrusion Detection Systems prolific, found in many networked environments<br>• Most logs generated are binary rather than text files<br>• May have to use proprietary program to view or convert the file to text<br>• Some IDS save logs in libpcap format, you can use packet sniffer tools like Wireshark to open, view and export these files as needed<br><br>• Snort<br>• Popular IDS and intrusion reporting tool<br>• Allows administrators to flag alerts on both live traffic and traffic captured with packet sniffer<br>• Will generate a text log displaying all alerts of suspicious traffic it encountered<br>• Requires complex set of steps to configure properly, configuration will change with each type of log or capture<br>• By default, all of Snort's log files on a Linux, Unix, or OS X system will be found in: /var/log/snort<br>**My Notes:** |

This page intentionally left blank.

# Module 14 - Log Analysis

**Overview**

Log data must not only be found, but properly formatted and assembled into reports. Log entries can be used directly as items of evidence, or assembled into other forms of data, such as statistics, charts, graphs, and other representations.

**Objectives**

- Generate statistics from log data
- Format log data into report-friendly formats
- Form visual charts and graphs with log data

**In this Module**

Here are the lessons in this module:

## Lesson 1 – Binary Traffic Analysis

**Lesson 1: Binary Traffic Analysis**

Binary logs require different filtering and searching techniques than those that are used with text logs. Due to the size of binary logs and their required processing power, it is often more efficient to filter binary network captures with command line tools

**Lesson 1 Learning Objectives**

- Describe the types of criteria that can be used to filter binary logs
- Convert binary logs to text files
- Understand how to filter and search binary logs with Wireshark

**Lesson 1 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Introduction to Wireshark | • Powerful, open source protocol analyzer, can be used to view full network traffic capture logs<br>• Open a variety of binary log formats<br>• Act as a sniffer<br>• Translate, or decode, known protocols within a binary log to human readable format<br>• Display highly detailed information on a frame-by-frame basis<br>• Search through a capture log for frames that match specific criteria<br>• Automatically reconstruct TCP sessions<br><br>• Walk through procedure for importing logs<br>• Walk through procedure for viewing binary logs<br>**My Notes:** |

**Lesson 1 Topics**, continued

| Topic | Key Points |
|---|---|
| Converting Binary Logs to Text Format | • Discuss binary vs. text and converting binary to text<br>**My Notes:** |
| Filtering and Searching in Wireshark | • Discuss filtering in Wireshark<br>• Capture filters<br>• Display filters<br>• Color filters<br>• Find menu<br>**My Notes:** |

**Lesson 1 Topics,** Continued

| Topic | Key Points |
|---|---|
| Filtering and Searching in Wireshark, continued | • Walk through procedure for setting up a capture filter<br>• Walk through procedure for creating a display filter<br>• Discuss creating a display filter for a keyword<br>• Discuss creating display filter for a hex value<br>• Discuss directly entering display filter expressions<br>• Review syntax of display filters<br>• Discuss altering and combining expressions<br>**My Notes:** |
| Colorizing Data Using Filters in Wireshark | • Walk through procedure for creating a color filter<br>• Walk through procedure for searching in Wireshark<br>**My Notes:** |
| Generating Statistics with Wireshark | • Discuss Statistics Menu<br>• Discuss Endpoints List<br>• Discuss Protocol Hierarchy Statistics<br>• Discuss Conversations List<br>• Discuss HTTP Requests Stats Tree<br>**My Notes:** |

**Lesson 1 Topics**, Continued

| Topic | Key Points |
|---|---|
| Exporting Data from Wireshark | • Discuss Exporting Statistics from Wireshark<br>**My Notes:** |

## Lesson 2 – Manual Log Analysis

**Lesson 2: Manual Log Analysis**

For those times when automated tools for log analysis are not readily available, we will now look at ways to manually examine and search log files for evidentiary information.

**Lesson 2 Learning Objectives**

- Understand how to build keyword lists for searching
- Know how to execute simple searches using EGREP
- Understand the basic concept of correlation of data.

**Lesson 2 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Filtering and Searching Text Logs | • Identify all log entries with a specific value or range of values<br>• Modify view of one or more log files based upon existence of an arbitrarily defined parameter<br>• Flexibility is important feature of tools<br>• Will encounter wide variety of log files that require search for different types of values<br>**My Notes:** |
| Regular Expressions | • Discuss GREP / EGREP<br>• Regular expressions common method for defining search parameters, used in applications, such as PERL, Snort, and EnCase<br>**My Notes:** |

**Lesson 2 Topics** Here are the topics to present.

| Topic | Key Points |
|---|---|
| Deciding What to Search For | • Keywords<br>• Rarely will a 'shotgun' or broad focused search turn up useable data<br>• Decide on keywords that might be available in logs and possibly locate artifacts of intrusion<br>• Sample keywords for intrusion:<br>o "Error" or "err"<br>o "Overflow"<br>o "Password" or "Pass"<br>o "Admin"<br>o "Unauthorized"<br>o IP addresses of interest<br>**My Notes:** |
| Example Log | • Walkthrough and discuss example log is text<br>**My Notes:** |

## Lesson 3 – Automated Log Analysis Tools

**Lesson 3: Automated Log Analysis Tools**

There are not many automated tools that allow you to search log files. Most require complex programming and setup prior to use. We will now look at one of the better tools on the market – Sawmill.

**Lesson 3 Learning Objectives**

- Install and configure the Sawmill program.
- Describe the function and use of the Sawmill program

**Lesson 3 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| What is Sawmill? | • Sawmill is a tool that will assist analyst in parsing network text logs and organizing logs into an easy-to-read report<br>• Can process various text logs generated by a variety of network security devices<br>• Converts text log to a cross-linked report that allows analyst to customize report according to output requirements<br>• Can be purchased and downloaded from http://www.sawmill.net<br>**My Notes:** |
| Installing Sawmill | • Walkthrough procedure for installing and configuring<br>**My Notes:** |

**Lesson 3 Topics**, continued

| Topic | Key Points |
|---|---|
| Network Log Analysis Using Sawmill | • Discuss The Administrative Interface<br>• Walkthrough procedure for creating a report profile<br>• Discuss the Report Environment<br>• Discuss the Report Header<br>• Discuss the Report Toolbar<br>• Discuss Report Menu<br>• Discuss Zoom To Filters<br>• Discuss Final Output Report (Log Detail)<br>• Discuss Single Page Summary<br><br>**My Notes:** |

This page intentionally left blank.

# Module 15 - Live Data Collection and Analysis

**Module 15 Overview**

Collecting live data from a system can uncover critically valuable information for an investigation due to the fact that volatile data is lost once the system is shut down. This module will guide you through using LiveWire tools to collect and analyze the volatile data on a remote system.

**Module 15 Exercises**

This module contains exercises in this manual to be walked through with the instructor As well as those for the students to go through themselves.

- XP-Pro-LiveWire-CookBook – Walkthrough in book
- Carly Sizemore – Practical and test to help prepare for final
- Alt tools Cookbook – Walkthrough and test
- Alt tools Carly Sizemore – Walkthrough and test
- Final Practicals – Set of three practical and tests

**Module 15 Testing**

This module is tested. The testing will include investigating 3 VMware images wish LiveWire along with multiple choice questions. A question pool of 30 questions per image has been provided for the instructor to create tests from as they see fit.

**Module 15 Objectives**

- Properly prepare for a live digital investigation.
- Use live digital investigation tools introduced in this module.

**In this Module**

The following table shows the contents of this module.

# Module 15 Exercise Configuration Details

| Module 15 Exercise Details | |
|---|---|
| VM Image: | XP-Pro-LiveWire-CookBook |
| VM Snapshots: | Anarchy CookBook – truecrypt |
| Description: | This virtual machine will be used throughout this module. Each exercise builds off of the previous exercises. The VM should be run at the specified snapshot to load the artifacts into memory that will be discovered by the students.<br><br>This Virtual Machine has the Anarchy CookBook Chapter 2 – Credit Card Fraud opened in open office. This document is stored in a truecrypt volume. |

| Summary of Artifacts to be Discovered During This Module | |
|---|---|
| Running processes: | truecrypt, open office writer |
| Document Open: | M:\anarchycookbook – credit card fraud.doc |
| TrueCrypt Volume: | My Documents\sweet-success.avi |
| Suspect images: | Located in My Pictures |
| Recent Documents: | shows files from M:\ and My Documents |

| Target VMWare Configurations | |
|---|---|
| **Computer Name:** | HellRaiser |
| **Operating System:** | Windows XP SP2 |
| **IP Address:** | 10.15.4.210 |
| **Subnet Mask:** | 255.255.255.0 |
| **Administrator U/N:** | Admin |
| **Administrator P/W:** | password |
| **Target U/N:** | Student |
| **Target P/W** | password |
| **TrueCrypt Volume:** | My Documents\sweet-success.avi |
| **TrueCrypt Volume P/W:** | anarchy |

## Lesson 1 – Data Collection

**Lesson 1: Data Collection**

When collecting data for any investigation it's vital that the data collection is conducted correctly.

**Lesson 1 Learning Objectives**

- Discuss locating physical devices in a network environment
- Discuss collecting data for forensically clean media

**Lesson 1: VMware Setup**

Throughout this module, each student will have his/her own VMware image loaded and running on the server. Each group of 4 students will be assigned a number 1 through 4 that will correspond with the last number of the IP address for the target machine. IP address 10.15.4.211 will be the target machine for student 1, IP address 10.15.4.212 will be the target machine for student 2. etc. Therefore, there will be 4 different VMware images for each exercise that is outlined in this instructor guide.

Cookbook VMware image – Load the snapshot named "Anarchy CookBook - truecrypt".

To load the correct image for the exercise in the book:

Open the Windows XP Pro CookBook VMware image.
On the task bar select VM > Snapshot > Anarchy CookBook - truecrypt".

**NOTE:** This snapshot will be used throughout this module for students to extract investigative information.

The more students that are hitting the same machine, the slower it will respond. Therefore, some actions should be expected to take longer than others depending on the number of users extracting data simultaneously.

**Lesson 1 Topics** Here are the topics to present.

| Topic | Key Points |
|---|---|
| Locating Physical Devices | • Explain that there is a difference in logical and physical topologies.<br>• Explain that logical topologies are used to show the flow of data over a network.<br>• Explain that physical topologies are used to show how devices are physically connected to other network components.<br>• Explain that a tone generator can be used to help trace network cables.<br>• Network/systems administrator may be a point of contact to interview but his answers must be verified.<br>• Explain that all findings should be recorded.<br>**My Notes:** |
| Attaching Storage Equipment | • .Explain that captured evidence may be extremely large.<br>• The investigator must ensure that there is enough hard drive space necessary to store the data on.<br>• Investigations require that evidence is stored on forensically clean media.<br>• Storage media should be wiped and verified before use.<br>• Review wiping guidelines section<br>**My Notes:** |

## Lesson 2 – Introduction to LiveWire

**Lesson 2: Introduction to LiveWire**

In this lesson, the students will be introduced to LiveWire. The software will be correctly installed and configured.

**Lesson 2 Learning Objectives**

- Explain the basic concepts of live digital investigations
- Successfully install, update, and setup LiveWire.
- Successfully install and update LiveDiscover

**Lesson 2 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Live Digital Investigations | • Live digital investigations are performed on systems that are currently active with running processes.<br>• Live systems are constantly changing.<br>• Live investigations allow the investigator to capture, view, and monitor the current system activities in real time.<br>• LiveWire requires an administrative account to retrieve data from the system.<br>• LiveWire uses Connect-Act-Disconnect.<br>• Be aware of the possibility that a knowledgeable user could become aware of the system being investigated.<br>• Discuss workstation requirements<br>**My Notes:** |
| LiveWire Installation | • Walk through installing LiveWire onto the workstation.<br>**My Notes:** |

**Lesson 2 Topics** Here are the topics to present.

| Topic | Key Points |
|---|---|
| LiveDiscover Installation | • Walk through installing LiveDiscover onto the workstation.<br>**My Notes:** |
| Updating LiveWire | • Walk through installing updating LiveWire.<br>**My Notes:** |
| Updating LiveDiscover | • Walk through updating LiveDiscover.<br>**My Notes:** |
| LiveWire Initial Setup | • Walk through the initial setup of LiveWire to prepare the system for investigations.<br>• The default LiveWire Administrator account password must be changed.<br>• Passwords require number and digits.<br>• An investigator account must be created to perform investigations.<br>**My Notes:** |

## Lesson 3 - LiveDiscover

**Lesson 3: LiveDiscover**

In this lesson, we will talk about finding the devices on the network so they can be examined.

**Lesson 3 Learning Objectives**

- Describe important functions of LiveDiscover
- Effectively scan a network for devices
- Effectively identify devices found on the network

**Lesson 3 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| LiveDiscover Network Scanning | • LiveDiscover will be used to find XP SP2 at IP 10.15.4.210<br>• Data from LiveDiscover can be used with LiveWire to perform analyses.<br>• LiveDiscover can quickly scan ranges of IP addresses.<br>• Data is stored in a database.<br>• Discuss the different tabs available.<br>• Perform a scan to find the system that will be investigated in later exercises.<br>**My Notes:** |

## Lesson 4 – Volatile Data Analysis

**Lesson 4: Volatile Data Analysis**

In this lesson, we will perform the initial inquiry of the suspect system to retrieve begin the volatile data analysis.

**Lesson 4 Learning Objectives**

- Conduct an initial inquiry.
- View the current open files on the system.
- View the current network connections and configurations.
- Image RAM over the network.

**Lesson 4 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| LiveWire Initial Inquiry | • Walk through the initial inquiry as in the book.<br>• IP 10.4.15.210<br>• Username: Admin<br>• Password: password<br>• Make the point that live systems are constantly changing and the investigator must be aware of this.<br>• Initial inquiries and other actives may impact the performance of the suspect system.<br>• Point out that data should always be saved to forensically clean media, but these lessons will use the default local directory for instructional purposes only.<br>• Discuss that the information used to perform the investigation was discovered during the LiveDiscover section. |
| | **My Notes:** |

**Lesson 4 Topics**, continued

| Topic | Key Points |
|---|---|
| System State | • Go over the exercise in the student book.<br>• View the initial inquiry information and discuss how this information can be important to the investigation.<br>• Acquire the physical RAM<br>• Many factors impact the speed of the RAM imaging process.<br>**My Notes:** |

**Lesson 4 Topics**, continued

| | |
|---|---|
| Current User Activity | • Walk through the exercise.<br>• Discuss the processes found.<br>• Notice that truecrypt is also running.<br>• Discuss the search capabilities.<br>• Discuss that LiveWire does not save the file with its extension.<br>• Discuss changing the file name does not change the hash value of the file.<br>**My Notes:** |
| Active Network State | • Walk through the exercises.<br>• Discuss the importance of open ports.<br>• Explain what the "$" on the shares mean.<br>**My Notes:** |

## Lesson 5 – Evidence Collection

**Lesson 5: Evidence Collection**

In this lesson, we look at collecting physical and logical data from the target machine.

**Lesson 5 Learning Objectives**

- Determine the status of the file system
- Generate a disk image
- Collect file evidence from the remote target

**Lesson 5: VMware Notes**

**NOTE:** This lesson discusses imaging physical and logical images of the target machine. It is at the discretion of the instructor whether or not the students will take the time to image a physical or logical partition. It may be recommended to only image the logical truecrypt volume instead of the entire volume, due to the amount of time required to complete that task.

If a student accidently starts the process of creating a whole disk image or the entire logical C:\ partition, then the system will drastically slow down. To stop the creation process, that student should reboot their computer and the VMware image should be reverted back to the original snapshot state.

**Lesson 5 Topics** Here are the topics to present.

| Topic | Key Points |
|---|---|
| File System status | • Walk through the exercise.<br>• Discuss the purpose of gathering disk information<br>• Discuss gathering data about files stored on the target system<br>**My Notes:** |
| Physical vs. Logical | • Walk through the exercise.<br>• Discuss physical and logical images.<br>• Discuss physical images capture all data on the drive; free space, deleted, etc.<br>• Explain benefits of physical imaging over logical imaging.<br>• Explain the benefits of logical imaging over physical imaging.<br>**My Notes:** |
| Collection and Preservation | • Walk through the exercise.<br>• Explain why investigators should correctly preserve evidence.<br>• Students should be able to find the anarchy documents on the VMware image.<br>**My Notes:** |

**Lesson 5 Topics**, continued

| | |
|---|---|
| Hashing | • Walk through the exercise.<br>• Discuss MD5 hashing – 128-bit<br>• Discuss SHA-1 hashes<br>• MD5 is currently accepted but SHA-1 may soon be preferred.<br>• Many investigators run both MD5 and SHA-1 hashing during investigations.<br>• Hashing is a one-way algorithm.<br>**My Notes:** |

## Lesson 6 – Malicious Code Analysis

**Lesson 6: Malicious Code Analysis**

In this lesson, we look how LiveWire can be used to discover malware categorized programs on the target system.

**Lesson 6: Learning Objectives**

- Describe the malware search functions on LiveWire
- Conduct a malware analysis of a target system

**Lesson 6 Topics**

Here are the topics to present.

| Topic | Key Points |
|---|---|
| Malicious Program Search | • Walk through the exercise.<br>• Discuss some of the different categories that malicious code could be put into.<br>• Discuss the possibility of searching different locations on the target system.<br>• The malicious code search may take some time depending on many factors.<br>• Review the malware scan report.<br>• Make sure not to confuse the option under Data Analysis with the option under Acquire Disk Data.<br>**My Notes:** |

# Module 15 Exercise Configuration Details

| Module 15 Carly Sizemore Exercise Details | |
|---|---|
| **VM Image:** | Carly Sizemore |
| **VM Snapshots:** | 1. Carly Sizemore – Conf Special |
| **Description:** | **This exercise is includes a paper handout with questions for the students to answer during their investigation of the system.**<br><br>This virtual machine will be used for the students to walk through the exercise on their own, with the assistance of the Instructor when needed. Once students have completed the exercise, the instructor will walk through the examination to demonstrate finding the correct answers to the question sheet. The VM should be run at the specified snapshot to load the artifacts into memory that will be discovered by the students.<br><br>This Virtual Machine has the Conf Special document opened in open office. This document will be used to search for answers to the handout questionnaire.<br><br>The instructor can choose to demonstrate the investigation for the students on a schedule best suited for them. Ex. The instructor may choose to conduct the demo at different levels of the system examination, such as after the LiveDiscover portion. |

| Summary of Artifacts to be Discovered During This Module | |
|---|---|
| **Running processes:** | IM programs, antivirus, open office |
| **Document Open:** | My Documents\Conf special.odt |
| **Browse images:** | Located in My Pictures |

| Target VMware Configurations | |
|---|---|
| **Computer Name:** | Csizemore |
| **Operating System:** | Windows XP SP2 |
| **IP Address:** | 10.15.4.233 |
| **Subnet Mask:** | 255.255.255.0 |
| **Administrator U/N:** | Administrator |
| **Administrator P/W:** | password |
| **Target U/N:** | Carly |
| **Target P/W** | none |

## Lesson 7 – Alternate Data Collection Tools

**Lesson 7: Alternate Data Collection Tools**

In this lesson, we look at other tools that may be used to collect information. These tools are included on the LiveWire CD. The Helix Live CD is introduced.

**NOTE:** These tools do get updated and newer versions of the PSTools can be downloaded from Microsoft.com

**Lesson 7: Learning Objectives**

- Describe functions of alternate tools
- Describe the functions of the helix live CD

**Lesson 7 Topics** Here are the topics to present.

| Topic | Key Points |
|---|---|
| Windows Forensic Toolkit | • Walk through using the commands in the student book.<br>• Explain that these tools are retrieving information from a remote machine.<br>• Discuss how this information may be useful in an investigation.<br>• Explain how this information could be redirected out to at text file with the ">" option.<br>• Also mention ">>" to append data to a file.<br><br>**My Notes:** |
| Helix | • Explain that Helix is a custom version of Linux.<br>• Discuss the two modes of Helix (Windows mode and Linux mode).<br><br>**My Notes:** |

**Lesson 7 Topics**, continued

| Topic | Key Points |
|---|---|
| Helix – Windows Mode | • Walk through starting helix on a live system.<br>• Point out that the live systems are constantly changing and helix will affect the system. This is a publicly accepted fact in the industry. The investigator must be able to speak to that fact if necessary in court.<br>• Go over the different screen in Helix.<br>• Note the Quick Launch in the menu bar.<br>• Note the Triangle buttons between the left and right page. It changes pages for the different tabs.<br>• Discuss the ability to use netcat to send forensic images over a network to another system.<br>• Therefore, two helix disks could be used. One system to collect the data, and the other to store the data.<br>• Discuss the other tools available on the CD.<br>**My Notes:** |

**Lesson 7 Topics**, continued

| Topic | Key Points |
|---|---|
| Helix – Linux Mode | • Boot the computer to the Helix CD.<br>• Discuss that Helix is configured to not change any data on the host machine.<br>• Access times will not be altered if a file is viewed.<br>• Helix will mount devices with only read access.<br>• It is possible to mount devices with read/write access and must be done through the command line.<br>• Briefly discuss some of the forensic tools included on the Helix CD.<br>• Discuss some of the benefits of using the Helix CD.<br><br>**My Notes:** |

# Module 15 - Alternate Tools Practical Exercise Configuration Details

| Module 15 – Alternate Tools Practical Exercise Details | |
|---|---|
| **VM Image:** | Windows XP Pro - CookBook |
| **VM Snapshots:** | 2. Anarchy CookBook – truecrypt |
| **Description:** | **This exercise is includes a paper handout with questions for the students to answer during their investigation of the system.**<br><br>This virtual machine will be used for the students to walk through the alternate tools exercise on their own and in a group, with the assistance of the Instructor when needed. This exercise is includes a paper handout with questions for the students to answer during their investigation of the system. The VM should be run at the specified snapshot to load the artifacts into memory that will be discovered by the students. This snapshot is the same as previous exercise. This will allow the students to compare their finding discovered using LiveWire.<br><br>This Virtual Machine has the Conf Special document opened in open office. This document will be used to search for answers to the handout questionnaire.<br><br>The instructor can choose to demonstrate the investigation for the students on a schedule best suited for them. Ex. The instructor may choose to conduct the demo at different after they have completed the individual portion, then allowing the students to continue on to the group section. |

| Summary of Artifacts to be Discovered During This Module | |
|---|---|
| **Running processes:** | truecrypt, open office writer |
| **Document Open:** | M:\anarchycookbook – credit card fraud.doc |
| **TrueCrypt Volume:** | My Documents\sweet-success.avi |
| **Suspect images:** | Located in My Pictures |
| **Recent Documents:** | shows files from M:\ and My Documents |

| Target VMWare Configurations | |
|---|---|
| **Computer Name:** | HellRaiser |
| **Operating System:** | Windows XP SP2 |
| **IP Address:** | 10.15.4.210 |
| **Subnet Mask:** | 255.255.255.0 |
| **Administrator U/N:** | Admin |
| **Administrator P/W:** | password |
| **Target U/N:** | Student |
| **Target P/W** | password |
| **TrueCrypt Volume:** | My Documents\sweet-success.avi |
| **TrueCrypt Volume P/W:** | anarchy |

# Module 15 - Alternate Tools Practical Exercise Configuration Details

| Module 15 – Alternate Tools Practical Exercise Details | |
|---|---|
| VM Image: | Carly Sizemore |
| VM Snapshots: | 3. Carly Sizemore – Conf Special |
| Description: | **This exercise is includes a paper handout with questions for the students to answer during their investigation of the system.**<br><br>This virtual machine will be used for the students to walk through the alternate tools exercise on their own and in a group, with the assistance of the Instructor when needed. This exercise is includes a paper handout with questions for the students to answer during their investigation of the system. The VM should be run at the specified snapshot to load the artifacts into memory that will be discovered by the students. This snapshot is the same as previous exercise. This will allow the students to compare their finding discovered using LiveWire.<br><br>This Virtual Machine has the Conf Special document opened in open office. This document will be used to search for answers to the handout questionnaire.<br><br>The instructor can choose to demonstrate the investigation for the students on a schedule best suited for them. Ex. The instructor may choose to conduct the demo at different after they have completed the individual portion, then allowing the students to continue on to the group section. |

| Summary of Artifacts to be Discovered During This Module | |
|---|---|
| Running processes: | IM programs, antivirus, open office |
| Document Open: | My Documents\Conf special.doc |
| Browse images: | Located in My Pictures |

| Target VMware Configurations | |
|---|---|
| **Computer Name:** | Csizemore |
| **Operating System:** | Windows XP SP2 |
| **IP Address:** | 10.15.4.233 |
| **Subnet Mask:** | 255.255.255.0 |
| **Administrator U/N:** | Administrator |
| **Administrator P/W:** | password |
| **Target U/N:** | Carly |
| **Target P/W** | none |

This page intentionally left blank.