

# Information Assurance Security+ Lab Series

## Table of Contents

### **Lab 1: Network Devices and Technologies - Capturing Network Traffic**

Task 1: Using <i>tcpdump</i> to Capture Network Traffic.....	pg 6 of 33
Task 2: Capturing and Analyzing Traffic with Wiresharkpg.....	pg 20 of 33
Task 3: Capturing and Analyzing Traffic with Network Minerpg.....	pg 28 of 33

### **Lab 2: Secure Network Administration Principles - Log Analysis**

Task 1: Log Analysis in Linux Using <i>Grep</i> .....	pg 8 of 29
Task 2: Log Analysis in Linux Using <i>Gawk</i> .....	pg 15 of 29
Task 3: Log Analysis in Windows Using <i>Find</i> .....	pg 22 of 29

### **Lab 3: Protocols and Default Network Ports - Transferring Data Using TCP/IP**

Task 1: Using Hyper Text Transfer Protocol (HTTP) to Transfer Files.....	pg 8 of 26
Task 2: Using Fire Transfer Protocol (FTP) to Transfer Files.....	pg 16 of 26
Task 3: Transferring Files Securely Using SCP.....	pg 24 of 26

### **Lab 4: Protocols and Default Network Ports - Connecting to a Remote System**

Task 1: Connecting to a Windows system Through the Command Line.....	pg 8 of 30
Task 2: Connecting to a Linux System Through the Command Line.....	pg 16 of 30
Task 3: Analyzing Remote Connections in Network Traffic.....	pg 24 of 30

### **Lab 5: Secure Implementation of Wireless Networking**

Task 1: Examining Plain Text Traffic.....	pg 7 of 30
Task 2: Cracking and Examining WEP Traffic.....	pg 15 of 30
Task 3: Cracking and Examining WPA Traffic.....	pg 22 of 30

### **Lab 6: Incident Response Procedures**

Task 1: Using <i>db_autopwn</i> to Attack a Remote System.....	pg 8 of 29
Task 2: Collecting Volatile Data.....	pg 15 of 29
Task 3: Viewing Network Logs.....	pg 23 of 29

### **Lab 7: Analyze and Differentiate Types of Malware**

Task 1: Using <i>Netcat</i> to Send a Reverse Shell.....	pg 7 of 24
Task 2: Using <i>Ncat</i> to Send a Reverse Shell.....	pg 15 of 24
Task 3: Sending a Bash Shell to a Windows Machine using <i>NetCat</i> .....	pg 19 of 24

### **Lab 8: Analyze and Differentiate Types of Attacks Using Window Commands**

Task 1: Viewing Network Resources.....	pg 6 of 26
Task 2: Using <i>PSEXEC</i> to Connect to a Remote System.....	pg 14 of 26
Task 3: Stopping, Starting, and Removing Services.....	pg 20 of 26

## **Lab 9: Analyze and Differentiate Types of Application Attacks**

- Task 1: Scanning the Network for Vulnerable Systems.....pg 8 of 33
- Task 2: Introduction to *Metasploit*, a Framework for Exploitation.....pg 13 of 33
- Task 3: Attacking a Remote System Utilizing *Armitage*.....pg 20 of 33
- Task 4: Post Exploitation of the Remote System.....pg 25 of 33

## **Lab 10: Mitigation and Deterrent Techniques - Anti-Forensics**

- Task 1: The Windows Event Viewer.....pg 8 of 30
- Task 2: Enabling Auditing.....pg 15 of 30
- Task 3: Clearing the Event Logs.....pg 23 of 30

## **Lab 11: Mitigation and Deterrent Techniques - Password Cracking**

- Task 1: Cracking Linux Passwords.....pg 7 of 33
- Task 2: Cracking Windows Passwords.....pg 15 of 33
- Task 3: Cracking Windows Passwords with *Cain*.....pg 27 of 33

## **Lab 12: Discovering Security Threats and Vulnerabilities**

- Task 1: Scanning the Network for Vulnerable Systems.....pg 8 of 26
- Task 2: Using *Nessus*.....pg 14 of 26
- Task 3: Introduction to *Metasploit*, a Framework for Exploration.....pg 18 of 26

## **Lab 13: Importance of Data Security - Data Theft**

- Task 1: Using *Metasploit* to Attack a Remote System.....pg 8 of 28
- Task 2: Stealing Data using FTP and HTTP.....pg 17 of 28
- Task 3: Stealing Data using *Meterpreter*.....pg 25 of 28

## **Lab 14: Importance of Data Security - Securing Data Using Encryption Software**

- Task 1: Installing *TrueCrypt*.....pg 6 of 28
- Task 2: Creating a *TrueCrypt* Container.....pg 11 of 28
- Task 3: Opening and Viewing Data within a *TrueCrypt* Container.....pg 21 of 28

## **Lab 15: Authentication, Authorization, and Access Control**

- Task 1: Adding Users, Groups, and Passwords.....pg 6 of 25
- Task 2: Symbolic Permissions.....pg 13 of 25
- Task 3: Absolute Permissions.....pg 19 of 25

## **Lab 16: General Cryptography Concepts**

- Task 1: Hiding a Picture within a Picture Using *S-Tools*.....pg 7 of 32
- Task 2: Hiding a Media File within a Picture Using *S-Tools*.....pg 18 of 32
- Task 3: Revealing Hidden Data Using *S-Tools*.....pg 27 of 32