INTRUSION ANALYSIS WITH THE STORM UNVEILED

WHO SHOULD ATTEND?

IT Admins who are interested in cybersecurity, Ethical Hackers, Pen Testers.

WORKSHOP OVERVIEW

Intrusion Analysis:

The foundation of all hacking and security work is TCP/IP traffic. In this workshop you will learn the foundation of TCP/IP, you will be introduced to what normal traffic looks like, then you will review traffic for signs of an attack. The process of protocol analysis will be covered to assist you in identifying the attacks and what the risk is to the network. The workshop will provide you practice with basic, advanced and web attack analysis techniques.

SESSION ONE: TECHNICAL INTRODUCTION TO THE STORM

- Hardware Assembly and Chipsets
- Imav ging Techniques
- Linux ARM Distro options
- Management of Modules and Meta Packages
- Industry tips and best practices

LAB: Backing up and restoring the Storm image

SESSION TWO: INTRODUCTION TO INTRUSION ANALYSIS

- Analyzing network traffic
- Examining the data at the packet level
- Control flags of TCP
- Identifying the characteristics of network connections

LAB: Analyzing Packets

- Advanced Protocol analysis
- Using protocol analyzers
  - tcpdump
  - dsniff
  - Wireshark
  - Etherape
  - Ettercap

LAB: Protocol Analysis I

- Wireshark Tricks
  - Leveraging the filter capabilities
  - Working within the GUI
  - Low level analysis
  - Following session communication
  - Customizing the interface
  - Using the statistics features within the tool
  - Text-based Wireshark
  - Packet decomposition

LAB: Protocol Analysis II

SESSION THREE: CAPTURING TRAFFIC ON THE "WIRE" AND IMPLEMENTING NETWORK FORENSICS

- Layer by layer forensics
- Collecting data
  - Raw protocol analysis
    - Tcpdump
    - Windump
  - Full protocol analysis
    - Wireshark
      - Working with filters
      - Session re-assembly

LAB TCP/IP analysis – (CHFI Module 7 – Network Forensics

- Colasoft
- Hping

LAB: Crafting Packets

SESSION FOUR: INTRUSION ANALYSIS OF NETWORK TRAFFIC ON WINDOWS AND LINUX

- Identifying normal vs abnormal traffic
- Determining cause of abnormal traffic
  - Passive fingerprinting characteristics
- Recognizing common patterns of network attacks
- Identifying the OS from the network traffic
  - Error
    - Nuances of the TCP/IP stack

LAB : Analyzing basic attacks

- Components of a sophisticated attack
  - Deception techniques
  - Protocol camouflage
  - Encryption and tunnels
- Components of advanced attacks
  - Protocol encapsulation
    - More than one layer 7
  - Web attacks
    - Services
    - SQL
    - XSS
    - Access controls

LAB : Analysis of Web Attacks