Introduction to Incident Response

Overview: The following is the tentative outline for the 2-day TrustedSec Introduction to Incident Response.

Purpose: To provide an overview of the Incident Response process and common investigation techniques often performed during an incident. Labs and examples will consist of real-world incidents that TrustedSec commonly investigates. At the end of the course, participants will understand the basics of network and host-based investigation and know how to recognize common tactics, techniques, and procedures (TTPs) of attackers.

Audience: Beginner to intermediate-level incident responders, IT first responders.

Requirements: Students will be required to provide their own laptop that can run a virtual machine. VMWare or VirtualBox may be used. Students should be familiar with how to use a virtual machine and copying files in and out of VMs.

Demos and labs: Will be performed throughout the course. Any topic not specified below can be covered during class by request.

- What is Incident Response (IR)?
- Why is IR needed?
- Threat Landscape
    - Data Breaches
    - Threat Actor Types (Examples)
        - Organized Crime
        - Cyber Terrorists
        - Hacktivists
        - Nation State
- Incident Response Planning
    - IR Policy
    - Run books and use cases
- IR Standards
- Types of Incidents
    - Proactive vs. Reactive
        - Incident Response (Reactive)
        - Threat Hunting (Proactive)
- Attack Vector Methods (Examples)
    - Phishing
    - Web-based attacks
    - Social Engineering
    - Malicious Documents
    - Supply Chain
- Incident Response Lifecycle

    - Preparation
    - Identification
    - Containment
    - Eradication
    - Remediation
    - Lessons Learned
- IR and Forensic Best Practices
- Incident Detection
    - Network visibility vs host visibility
- Forensic Investigation
    - Order of volatility
- Live Response / Triage
- Host Analysis
    - Persistence
    - Event Logs
    - Timelines
    - Browser Forensics
    - Evidence of Execution
- Network Forensics
    - Packet analysis
    - Flow Analysis
    - Command and Control Identification
- Open Source Intelligence (OSINT)
    - IOC
        - IP Address
        - Domain
        - Malware Hash
        - Threat Actor Handle
        - Threat Actor Email Address
        - Threat Actor Attack Tool\s Used
    - Available Open Source Tools
    - Available Clearnet Reputation and Threat Intelligence Resources