Hands-on Incident Response Workshop

How would your organisation respond to a cyber security incident?

Work through a scenario with CERT technical advisers who will provide hands-on experience of the procedures and tools used to analyse incidents, determine the impact and develop an effective remediation plan.

Determine the Tactics, Techniques and Procedures (TTPs) employed by actors and improve your readiness to meet these challenges.

Who Should Attend

The workshop is aimed at technical staff with beginner to intermediate knowledge of cyber security and incident response. Participants will utilise Windows and Linux tools to analyse memory snapshots and network packet captures.

- Security Professionals (Beginner to Intermediate level)
- Systems Administrators;
- Other IT Technical staff looking to increase knowledge and awareness.

Prerequisites

****Bring your own laptop**** A relatively powerful laptop is required as participants will run two Virtual machines. All workshop exercises will take place within these virtual machines; artefacts for the workshop will be downloadable from a Wi-Fi connection at the workshop.

Minimum System Hardware Requirements

- CPU: 64-bit Intel i5/i7 (4th generation+);
- 8Gb RAM+;
- BIOS/UEFI settings for Intel-VT enabled. Access to BIOS/UEFI password;
- Wireless 802.11 Capability;
- Sufficient disk space to run two virtual machines.

Virtual Machines

We would recommend using VMWare Workstation or VirtualBox as the hypervisor.

Please download and install these virtual machines prior to the workshop:

- The SIFT Workstation is a group of free open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings and can be downloaded from: https://digital-forensics.sans.org/community/downloads
- FLARE VM is a freely available and open sourced Windows-based security distribution designed for reverse engineers, malware analysts, incident responders and penetration testers and can be downloaded from: https://www.fireeye.com/services/freeware/flare-vm.html