IT Forensics for System Administrators 2

Report of Contributions

https://events.geant.org/e/1194

Contribution ID: **1** Type: **not specified**

IT Forensics for System Admins - CyberChef

Wednesday, 27 April 2022 11:00 (1 hour)

Since its first release in 2017 CyberChef - described as “The Cyber Swiss Army Knife” - has quickly become one of the go-to tools for many IT security practitioners. CyberChef is a free, browser-based, open source tool, that supports hundreds of different “cyber operations” such as encoding, encrypting, compressing, converting, analysing data, etc. It is especially useful for malware analysts as well as forensic investigators. This webinar/live demo will demonstrate many of CyberChef’s powerful capabilities as well as some of the less well known operations.

Presenter: Mr KELM, Stefan (DFN-CERT)

Contribution ID: **2** Type: **not specified**

IT Forensics - Memory Analysis Basics - First Steps

Wednesday, 4 May 2022 11:00 (1 hour)

Having obtained an image of the memory of a compromised system, what to do with it? This part of the forensic process is called analysis, and this webinar will go through the first steps of analysing a memory image, looking into processes, network and temporary filesystems as well as some operating system specific artefacts, such as the Windows registry of the Linux Bash history.

Presenter: Mr MÖLLER, Klaus (DFN-CERT)

Contribution ID: **4** Type: **not specified**

IT Forensics - Advanced Memory Analysis - Dealing with Malicious Code

Thursday, 12 May 2022 11:00 (1 hour)

Malware that is other compressed and encrypted on disk is usually unpacked and in cleartext in memory. Likewise, rootkits that conceal adversary activities can be found with relative ease in the memory image of a compromised system. This webinar will show some techniques to obtain malware that works along common ways, such as DLL injection, malicious kernel modules, or system call table manipulation. Concluding the module, ways to extract suspicious code segments for further analysis are also shown.

Presenter: Mr MÖLLER, Klaus (DFN-CERT)

Contribution ID: **5** Type: **not specified**

IT Forensics - Persistent Storage Forensics I - Basics and First Steps

Wednesday, 25 May 2022 11:00 (1 hour)

In this session, we will discuss the basic concepts of persistent storage forensics. Furthermore, some approaches with easy-to-use basic tools will be presented and demonstrated.

Presenter: Mr DUSSA, Tobias (DFN-CERT)

Contribution ID: **6** Type: **not specified**

IT Forensics - Persistent Storage Forensics II - Advanced Approaches

Monday, 30 May 2022 11:00 (1 hour)

In this session, more advanced analysis methods and tools will be discussed. Furthermore, these methods and tools will be demonstrated in practice with select case samples.

Presenter: Mr DUSSA, Tobias (DFN-CERT)