DIGITAL SECURITY AUTHORITY

NATIONAL CSIRT-CY

EUROPEAN SECURITY AND DEFENCE COLLEGE
COLLÈGE EUROPÉEN DE SÉCURITÉ ET DE DÉFENSE

INVITATION
Activity under the Cyber ETEE platform:

Course on Cybersecurity Organisational and Defensive Capabilities

Online, 18-20 January 2021
hosted by the Digital Security Authority of Cyprus *(DSA)*
Venue: Online via Webex
Time zone: Central European Time (CET)

Under the auspices of the European Security and Defence College (ESDC), the Digital Security Authority (DSA) -National CSIRT-CY of Cyprus has the great honour of organising a course dedicated to cyber challenges in the areas of information and risk management, incident handling, threat intelligence and media monitoring and response. The course will be held in Nicosia from 18 - 20 January 2021.

This course is intended to strengthen the establishment of the Cyber Education Training Exercise and Evaluation (ETEE) platform of the ESDC and widen the scope of its activities by addressing technical and tactical/operational-level training.

This course therefore aims to provide a forum for the exchange of knowledge and best practices among cyber experts on cyber topics by improving their knowledge, skills and competencies.

The course is a specialized course at technical/tactical level therefore the technical specificities of ‘’Annex A” are needed. The course will be held in English and can participate a maximum of 30 participants. Due to the current circumstances the course will take place in Virtual Form.

This training course is open to civil servants and military personnel from EU Member States and EU institutions and agencies who are currently employed in positions in which they are required to deal with cyber operational/tactical and technical issues or who are willing to discuss and update their knowledge on these issues. Participants will have the opportunity to benefit from the know-how of experts from the European institutions and the Member States.

It is therefore with great pleasure that the Digital Security Authority - National CSIRT-CY of Cyprus invites you to this course on 'Cybersecurity Organisational and Defensive Capabilities'.

DIGITAL SECURITY AUTHORITY

NATIONAL CSIRT-CY

ETCE CYBER PLATFORM

ESDC CESD

Course on Cybersecurity Organisational and Defensive Capabilities

18 – 20 January 2021

Hosted by

COMMISSIONER OF COMMUNICATIONS

DIGITAL SECURITY AUTHORITY

NATIONAL CSIRT-CY

DAY 1 Time zone : CET	Monday, 18 January 2021 Online Training
8:00 – 8:30	**Welcome address by Mr. George Michaelides, Commissioner of Communications, Cyprus** **Opening Address by** • **Dr. Marios Thoma, European Security Defence College** • **Professor Stavros Stavrou, Dean - Open University of Cyprus, Chairman - EAB.Cyber**
	SESSION 1: Forensics: Mr Nikos Doukas
8:30 – 10:25	**Fundamentals of Forensics Ethical and legal issues** **File System Analysis** – Forensics Tools and Testing – Hard drive and File system technical background – File system terminology – Phases of an investigation – Partitions and partition tables, File Systems – Boot process – Deleting and recovering files – FAT, NTFS, ext2, ext3 file systems – Media preparation and Imaging – Imaging of drives – Imaging tools – Drive Image Analysis and Tools **Registry Analysis** – Accessing the Registry – Registry Structure – Registry Keys and Structure – Registry Hives – System information and tracking user activity – Network Information from the Registry – Booting Information in the registry – Registry Information of user activity – USB and mounted devices – Registry Forensics techniques and tools – Recovering file information from the Registry
10:25 – 10:30	**Break**
10:30 – 11:00	**File System Analysis Practical Exercises** – Forensics workstation setup – Hash function and encryption cracking – USB drive examination with Python – Automated parsing of text files – Evidence extraction from binary files – Metadata file examination – Event timeline investigation – Triage of Systems **Registry Analysis Practical Exercises** – Security and Security Account Manager (SAM) Hive – System Hive – Software Hive – Boot Configuration Data (BCD) Hive **Nikos Doukas**, Professor on Informatics and Military Applications, Director of, Informatics LAB, Hellenic Military Academy, Mathematics and Engineering Sciences Section

11:00 – 11:05	**Break**
	SESSION 2: Cyber Security, Attacks, Intruders Methodology and Countermeasures: Dr Nikos Bardis
11:05 – 13:05	**Part 1: Cyber Security & Attacks** – Cyber Security & Attacks – Wireless Security – Cryptography of Wireless networks – WiFi networks attacks – Attacks – Wardriving – Rogue Access Points – ad-hoc networks – MAC spoofing – Eavesdropping – Sniffer – Evil Twin – Man-in-the-Middle – Non-broadcasting network attack – Krack Attacks – Wi-Fi Protected Setup (WPS) – Denial of Service – Jamming Attack – Wi-Fi deauthentication attack
13:05 – 13:10	Break
13:10 – 13:35	**Part 3: Attacks Applications** – Wireshark- Quick User Guide-Example of Code Interception o Wireshark sniffing to: o Record sensitive data such as login codes o Interception of chat messages o Retrieve files that have been transferred over a network – Portable Device Construction for Deauthentication Attacks o Deauthentication Attack in 802.11 – Phishing-Social Engineering based on Evil Twin Attack o The experiment to be carried out is an application of the "Evil Twin Attack" technique. In essence it is a phishing – social engineering method. The attack is launched with the creation with the creation of an identical wireless network, with the same name and frequency as the victim network We will deal with – Penetration test – Vulnerability vs. Penetration Assessments – Vulnerability Assessment? – Test System vs. Production System? – Methodology of Penetration Tester – Tools: whois, traceroute, nslookup, Dig, Host, recon-ng, ech – Scanning: o ping o half syn scan, o open ports, o Services, o Version, o Operating system, o Applications Vulnerabilities – Enumeration

	– Firewalls – Exploitation – Vulnerability Assessment + Penetration Tests – Open Tools: o Kali 2 o Parrot OS Security o MSBA (Microsoft Baseline Security Analyzer) o NESSUS (Network and O.S. Vulnerability Scanner) o OPENVAS (http://www.openvas.org/) o NIKTO (WEB Vulnerability Scanner) o Netsparker (http://www.mavitunasecurity.com/communityedition/) o Fluxion o Evil Twin Attack **Summary – Conclusions** **Nikos Bardis,** Professor on Informatics and Military Applications, Hellenic Military Academy, Mathematics and Engineering Sciences Section

* * *

DAY 2 Time zone : CET	**Tuesday, 19 January 2021** Online Training
08:00 – 08:30	**Opening address by the presenter** – What we are going to discuss – Overall Goals – Required Background
	SESSION 1: Android Forensics
08:30 – 10:25	**Fundamentals of Smartphone Forensics** The sections of the lecture are supported by short practical exercises – Data storage in Android systems – Regular expressions – Password manipulation – Rooting and JTAG **Smartphone data acquisition principles** – Android phone data extraction – Physical and logical extraction – Deleted file recovery **Android data analysis** – Contacts – calls – Browser history – WiFi analysis – Social media – Messages – Applications – Application Forensic Analysis – Forensic tools for Android smartphones – Malware identification – Malware analysis – Practical **Summary – Conclusions** **Nikos Bardis,** Professor on Informatics and Military Applications, Hellenic Military Academy, Mathematics and Engineering Sciences Section **Nikos Doukas**, Professor on Informatics and Military Applications, Director of, Informatics LAB, Hellenic Military Academy, Mathematics and Engineering Sciences Section
10:25 – 10:30	Break
	SESSION 2: Introduction to Risk Management Concepts and Frameworks
10:30 – 11:30	• Context – what is risk and why is it important? • What is risk management and how does it fit in an overall organisational approach to cybersecurity? • Main risk management concepts and terminology • Relevant standards and frameworks

	• Risk Management Process
	  ○ Context Establishment
	  ○ Risk Identification
	  ○ Risk Analysis
	  ○ Risk Evaluation
	  ○ Risk Treatment
	  ○ Monitoring and Communication

	SESSION 3: Introduction to Risk Assessment Techniques

11:30 – 12:30	• Deeper dive on each part of risk assessment
	  ○ Techniques for Risk Identification
	  ○ Techniques for Risk Analysis
	  ○ Techniques for Risk Evaluation
	• Risk reporting
	• Risk treatment planning
	• Compliance to standards for information security management based on risk – benefits and dangers to keep in mind

12:30 – 13:00	• Presentation of short homework exercises based on the delivered material • Discussion and Q&As **Summary – Conclusions** **Costas Efthymiou,** Technical Officer, Digital Security Authority

* * *

DAY 3 Time zone : CET	Wednesday, 20 January 2021 Online Training
08:00 – 08:30	**Opening address by the presenter** • What we are going to discuss • Overall Goals • Required Background
	SESSION 1: Virtual Machine Setup
08:30 – 09:00	**How to create a Malware Analysis lab** – Download VirtualBox, Flare VM – Step by step how to setup critical features in each VM – How to create a share folder between Host
09:00 – 09:05	Break
	SESSION 2: Assembly language for x86 Processors
09:05 – 11:30	**Part 1: Malware Analysis** – Basic Techniques – Virtual Machine Setup tips – Architecture of Microprocessors – Data Representation – Endianness (Big-Endian and Little-Endian Order) **Part 2: x86 Processor Architecture** – General-Purpose Architecture – EFLAGS Register – Instruction Pointer **Part 3: Assembly Language Fundamentals** – Operand Types – Basic Instructions – Transfer Instructions – Stack Operations – Defining and Using Procedures **Part 4: Reverse Engineering Mindset** – Debugger's Interface – How to run an executable in the debugger – Basic steps to follow in the debugger – Using the registers and the stack

11:30 – 11:35	Break
11:35 – 12:05	– **Labs** **Summary – Conclusions** – References & Further Reading – Conclusion **Christos Pachoulides**, Analyst, National CSIRT-CY

* * *

DIGITAL SECURITY AUTHORITY

NATIONAL CSIRT-CY

Annex A

Technical Specificities

Software Tools

For the practical exercises you might find it useful to download and configure in advance the following software tools:

1. A virtual machine (e.g. VirtualBox, VMWare) with Kali Linux. There exist virtual machine files with Kali Linux pre-installed, but you may also choose to download each component separately. Download files, documentation and configuration guidelines are available from a variety of sources, such as:

    - The official Kali Linux page: https://www.kali.org/
    - The OSBoxes page: https://www.osboxes.org/kali-linux/

2. A virtual machine (e.g. VirtualBox, VMWare) with Ubuntu Linux. One can also select between preinstalled virtual machine files and customized installations. Possible sources include:

    - The OSBoxes page: https://www.osboxes.org/ubuntu/
    - Linux Images: https://www.linuxvmimages.com/

3. Another useful platform is the SIFT workstation:

    - Digital Forensics page: https://digital-forensics.sans.org/community/downloads

4. The base installation of the VMWare player may be downloaded from https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html

5. The Sleuth kit & Autopsy offer a selection of tools that you may use for the practical part of the course, but are useful for anyone experimenting with computer forensic analysis

    - The Sleuth kit & Autopsy Open Source Digital Forensics Tools: http://www.sleuthkit.org/

6. For the Android forensics, Android Studio offers a useful toolset

    - https://developer.android.com/studio

- https://developer.android.com/studio/#command-tools

7. OS Kali Linux or a virtual machine (e.g. VirtualBox, VMWare) with Kali Linux. There exist virtual machine files with Kali Linux pre-installed, but you may also choose to download each component separately. Download files, documentation and configuration guidelines are available from a variety of sources, such as:
    - The official Kali Linux page: https://www.kali.org/
    - The OSBoxes page: https://www.osboxes.org/kali-linux/
8. A virtual machine (e.g. VirtualBox, VMWare) with OS PARROT
    - The official OS Parrot page: https://www.parrotsec.org/
9. Security tools:
    1. FLUXION,
    2. nmap,
    3. ettercap,
    4. wireshark,
    5. MetaSploit,
    6. sqlmap,
    7. airmon-ng,
    8. airodump-ng,
    9. aireplay-ng,
    10. aircrack-ng,
    11. Aqlmap,
    12. nikto,
    13. burp suite

Depending on your interests regarding the material presented in the course you might also use additional software tools. You will be guided for their download and installation during the course.