Virtuelt kursus
5 dage **DKK 24.999**
Nr. 90466 A ekskl. moms

Dato	Sted
26-08-2024	Virtuelt kursus
04-11-2024	Virtuelt kursus

Masterclass: Forensics and Incident Handling [FOR]

I dag er det vigtigt at være konstant forberedt og opdateret, så du ikke bliver overhalet af hackerne. På kurset får du de nødvendige færdigheder for at kunne finde, indsamle og opbevare data på en korrekt måde, analysere dem og lære så meget om hændelsen som muligt. Undervisningen foregår på engelsk med live underviser.

Vær på forkant med hackerne

Forensics og Incident Handling er i konstant udvikling og vigtige emner inden for cybersikkerhed. Dette intense og praktiske kursus dækker den generelle tilgang til dataefterforskning og hændelseshåndtering, netværksefterforskning, vigtige aspekter af interne funktioner i Windows, analyse af hukommelse og storage, opdagelse af tegn på kompromittering og den korrekte måde at rapportere på.

Deltagerprofil

Kurset er for dig, der er IT-fagperson, specialist i dataefterforskning og hændelseshåndtering, sikkerhedskonsulent, Enterprise-administrator, infrastrukturarkitekt, sikkerhedsmedarbejder, systemtekniker, netværksadministrator, eller dig der har ansvar for at implementere netværks- og perimetersikkerhed.

Udbytte

- Lær, hvordan du finder, indsamler og opbevarer data på den mest hensigtsmæssige måde

Teknologisk Institut
kurser@teknologisk.dk
+45 72 20 30 00

- Lær at analysere, håndtere og rapportere hændelser på en hensigtsmæssig måde
- Lær, hvordan du kan lære fra disse hændelser, så du undgår, at de gentager sig

Det får du på arrangementet

- Øvelser og inddragelse
- Kursusbevis
- Erfaren underviser
- Maks. 12 deltagere
- Casearbejde
- Materiale på engelsk
- Undervisning på engelsk

Indhold

Module 1: Introduction to Incident Handling

- Types and Examples of Cybersecurity Incidents
- Signs of an Incident
- Incident Prioritization
- Incident Response and Handling Steps
- Procedures and Preparation

Module 2: Securing Monitoring Operations

- Industry Best Practices
- Detecting Malware via DNS logs
- Configuration Change Management
- Leveraging Proxy and Firewall Data
- Monitoring Critical Windows Events
- Detecting Malware via Windows Event Logs

Module 3: Network Forensics and Monitoring

- Types and approaches to network monitoring
- Network evidence acquisition
- Network protocols and Logs
- LAB: Detecting Data Thievery
- LAB: Detecting WebShells
- Gathering data from network security appliances
- Detecting intrusion patterns and attack indicators
- Data correlation
- Hunting malware in network traffic
- Encoding and Encryption

Module 4: Windows Internals

- Introduction to Windows Internals
- Fooling Windows Task Manager
- Processes and threads
- PID and TID
- Information gathering from the running operating system
- Obtaining Volatile Data
- A deep dive to Autoruns
- Effective permissions auditing
- PowerShell get NTFS permissions
- Obtaining permissions information with AccessChck
- Unnecessary and malicious services

Teknologisk Institut
kurser@teknologisk.dk
+45 72 20 30 00

- Detecting unnecessary services with PowerShell

Module 5: Memory Dumping and Analysis

- Introduction to memory dumping and analysis
- Creating memory dump - Belkasoft RAM Capturer and DumpIt
- Utilizing Volatility to analyze Windows memory image
- Analyzing Stuxnet memory dump with Volatility
- Automatic memory analysis with Volatile

Module 6: Indicators of compromise

- Yara rules language
- Malware detonation
- Introduction to reverse engineering

Module 7: Storage Acquisition and Analysis

- Introduction to storage acquisition and analysis
- Drive Acquisition
- Mounting Forensic Disk Images
- Introduction to NTFS File System
- Windows File System Analysis
- Autopsy with other filesystems
- Building timelines

Module 8: Reporting – Digital Evidence

- This module covers the restrictions and important details about digital evidence gathering. Moreover, a proper structure of digital evidence report will be introduced

Eksempler på værktøjer, software og eksempler brugt undervejs på kurset

- Belkasoft RAM Capturer
- Wireshark
- Volatility
- The Sleuth Kit® (TSK)
- Autopsy
- DumpIt
- DC3DD
- Arsenal Image Mounter
- Reclaim Me
- ReFS Images
- SysInternals Toolkit -
- ShadowCopyView
- RegRipper
- Rifiuti2
- Registry Explorer/RECmd
- FullEventLogView
- EVTXtract
- Loki IOC Scanner
- Yara
- LECmd
- LinkParser
- PECmd
- SkypeLogViewer
- SQLiteBrowser
- NetWork Miner
- StuxNet Memory Dump

Teknologisk Institut
kurser@teknologisk.dk
+45 72 20 30 00

Form

Kurset er virtuelt med live underviser.

Før du deltager i det virtuelle kursus, vil vi altid forsøge at arrangere en testsession på 15 - 20 minutter en uges tid før for at sikre, at du er i stand til at deltage i masterclassen. Herunder finder du kravene til at oprette forbindelse til det virtuelle kursus:

- En computer med en stabil internetforbindelse (skal helst køre Windows eller Mac OS).
- Tilladelser til udgående RDP-forbindelser til eksterne servere (til vores laboratoriemiljø) – port 3389
- Et headset (hovedtelefoner og mikrofon)
- Webcam (indbygget eller tilsluttet)
- En ekstra skærm er nyttig, men ikke påkrævet

Materiale

Du får adgang til unikke redigeringsværktøjer, virtuelt lab miljø, praktiske opgaver, præsentationsslides med noter i løbet af kurset.

Alle labs forbliver online i yderligere 3 uger, så du kan øve endnu mere, efter kurset er afsluttet.

Alle øvelser er baseret på Windows Server 2016 og 2019, Windows 10 og Kali Linux.

CPE Point (Continuing Professional Education)

Det er muligt at optjene CPE points ved gennemførelse af dette kursus.

UNDERVISER

Paula Januszkiewicz

Paula er verdenskendt som sikkerhedsekspert. Paula elsker at lave penetrationstests, IT-sikkerhedsevalueringer, og hendes motto er: "Harden em all!" Hun er Enterprise Security MVP og -underviser (MCT), og så er hun Microsoft Security Trusted Advisor.

Har du faglige spørgsmål så kontakt

Malene Kjærsgaard
+45 72202523
mch@teknologisk.dk