

## 360 Penetration Testing Course

Varighed: 5 Days    Kursus Kode: 360PTC    Leveringsmetode: Company event (Firmakursus)

---

### Beskrivelse:

**You will enjoy it!** This course teaches infrastructure security concepts, including the techniques how to attack and how to respond with an appropriate countermeasure implementation.

This 3 day course will be presented by Paula Januszkiewics. Paula Januszkiewicz is IT Security Auditor and Penetration Tester, Enterprise Security MVP, trainer (MCT) and Microsoft Security Trusted Advisor. She is also a top speaker at many international conferences (incl. TechEd North America, TechEd Middle East and TechEd Europe, RSA China, Cybercrime Forum and other) and writes articles on Windows Security. The trainings she conducts usually cover Security, Windows operating system topics and Virtualization. Paula is passionate about sharing her knowledge with others. She conducted many IT security audits and penetration tests – these are her everyday tasks.

We go far beyond simply presenting how to 'break into operating systems'. This course has been developed around professional penetration testing and security awareness in the business and IT fields. To make sure that all participants will gain the necessary infrastructure security knowledge this class has intensive hands-on format. All labs are constantly updated and have 3 levels of difficulty and can be easily adjustable to the overall level of the group. Every exercise is supported with the lab instructions and multiple tools, traditional and specialized.

### Firmakursus

Med et firmakursus bliver jeres it-kompetenceudvikling målrettet jeres behov. Det betyder, at vi hjælper med at finde og sammensætte det helt rigtige kursusindhold og den helt rigtige form. Kurset kan afvikles hos os eller kunden, standard eller virtuelt.

---

### Målgruppe:

Security Analysts, Risk Managers, Security Officers, System Managers, Architects, Penetration Testers.

---

### Agenda:

- |                                           |                                              |
|-------------------------------------------|----------------------------------------------|
| ■ Students will learn how to:             | ■                                            |
| ■ Identify security profile of the target | ■ Figure out protection opportunities        |
| ■                                         | ■                                            |
| ■ Perform the testing activities          | ■ Optimize security controls to reduce risks |
- 

### Forudsætninger:

- Sound knowledge of TCP/IP
  - Operating systems architecture (windows, Linux)
-

## Indhold:

- Operating System Services Security Overview
- Operating System Internal Security
- Databases Security
- Google Hacking
- HTTP Request Building
- Reconnaissance and Target Profiling
- Information Leakage and Error Handling
- Session Manipulation
- Tampering with Communication (Wired and Wireless)
- Exploiting a Lack of Access Controls
- Malicious Files Execution
- Legal Issues
- Methods described in the training are demonstrated during live penetration tests and IT security audits. Our real live experience has allowed to work out the applicable testing methodology that requires a solid understanding of the security profile of the target. We are proud to say that this course is equally important for those who

- Operating System Services Security Overview
- Operating System Internal Security
- Databases Security
- Google Hacking
- HTTP Request Building
- Reconnaissance and Target Profiling
- Information Leakage and Error Handling
- Session Manipulation
- Tampering with Communication (Wired and Wireless)
- Exploiting a Lack of Access Controls
- Malicious Files Execution
- Legal Issues
- Methods described in the training are demonstrated during live penetration tests and IT security audits. Our real live experience has allowed to work out the applicable testing methodology that requires a solid understanding of the security profile of the target. We are proud to say that this course is equally important for those who

- Operating System Services Security Overview
- Operating System Internal Security
- Databases Security
- Google Hacking
- HTTP Request Building
- Reconnaissance and Target Profiling
- Information Leakage and Error Handling
- Session Manipulation
- Tampering with Communication (Wired and Wireless)

- Operating System Services Security Overview
- Operating System Internal Security
- Databases Security
- Google Hacking
- HTTP Request Building
- Reconnaissance and Target Profiling
- Information Leakage and Error Handling
- Session Manipulation
- Tampering with Communication (Wired and Wireless)
- Exploiting a Lack of Access Controls
- Malicious Files Execution
- Legal Issues
- Methods described in the training are demonstrated during live penetration tests and IT security audits. Our real live experience has allowed to work out the applicable testing methodology that requires a solid understanding of the security profile of the target. We are proud to say that this course is equally important for those who

- Operating System Services Security Overview
- Operating System Internal Security
- Databases Security
- Google Hacking
- HTTP Request Building
- Reconnaissance and Target Profiling
- Information Leakage and Error Handling
- Session Manipulation
- Tampering with Communication (Wired and Wireless)
- Exploiting a Lack of Access Controls
- Malicious Files Execution
- Legal Issues
- Methods described in the training are demonstrated during live penetration tests and IT security audits. Our real live experience has allowed to work out the applicable testing methodology that requires a solid understanding of the security profile of the target. We are proud to say that this course is equally important for those who

- Operating System Services Security Overview
- Operating System Internal Security
- Databases Security
- Google Hacking
- HTTP Request Building
- Reconnaissance and Target Profiling
- Information Leakage and Error Handling
- Session Manipulation

- Operating System Services Security Overview
- Operating System Internal Security
- Databases Security
- Google Hacking
- HTTP Request Building
- Reconnaissance and Target Profiling
- Information Leakage and Error Handling
- Session Manipulation
- Tampering with Communication (Wired and Wireless)
- Exploiting a Lack of Access Controls
- Malicious Files Execution
- Legal Issues
- Methods described in the training are demonstrated during live penetration tests and IT security audits. Our real live experience has allowed to work out the applicable testing methodology that requires a solid understanding of the security profile of the target. We are proud to say that this course is equally important for those who

- Operating System Services Security Overview
- Operating System Internal Security
- Databases Security
- Google Hacking
- HTTP Request Building
- Reconnaissance and Target Profiling
- Information Leakage and Error Handling
- Session Manipulation
- Tampering with Communication (Wired and Wireless)
- Exploiting a Lack of Access Controls
- Malicious Files Execution
- Legal Issues
- Methods described in the training are demonstrated during live penetration tests and IT security audits. Our real live experience has allowed to work out the applicable testing methodology that requires a solid understanding of the security profile of the target. We are proud to say that this course is equally important for those who

Let us infect you with technology PASSION!

- Exploiting a Lack of Access Controls
- Malicious Files Execution
- Legal Issues
- Methods described in the training are demonstrated during live penetration tests and IT security audits. Our real live experience has allowed to work out the applicable testing methodology that requires a solid understanding of the security profile of the target. We are proud to say that this course is equally important for those who

- Operating System Services Security Overview
- Operating System Internal Security
- Databases Security
- Google Hacking
- HTTP Request Building
- Reconnaissance and Target Profiling
- Information Leakage and Error Handling
- Session Manipulation
- Tampering with Communication (Wired and Wireless)
- Exploiting a Lack of Access Controls
- Malicious Files Execution
- Legal Issues
- Methods described in the training are demonstrated during live penetration tests and IT security audits. Our real live experience has allowed to work out the applicable testing methodology that requires a solid understanding of the security profile of the target. We are proud to say that this course is equally important for those who

- Operating System Services Security Overview
- Operating System Internal Security
- Databases Security
- Google Hacking
- HTTP Request Building
- Reconnaissance and Target Profiling
- Information Leakage and Error Handling
- Session Manipulation
- Tampering with Communication (Wired and Wireless)
- Exploiting a Lack of Access Controls
- Malicious Files Execution
- Legal Issues
- Methods described in the training are demonstrated during live penetration tests and IT security audits. Our real live experience has allowed to work out the applicable testing methodology that requires a solid understanding of the security profile of the target. We are proud to say that this course is equally important for those who

- Tampering with Communication (Wired and Wireless)
- Exploiting a Lack of Access Controls
- Malicious Files Execution
- Legal Issues
- Methods described in the training are demonstrated during live penetration tests and IT security audits. Our real live experience has allowed to work out the applicable testing methodology that requires a solid understanding of the security profile of the target. We are proud to say that this course is equally important for those who

- Operating System Services Security Overview
- Operating System Internal Security
- Databases Security
- Google Hacking
- HTTP Request Building
- Reconnaissance and Target Profiling
- Information Leakage and Error Handling
- Session Manipulation
- Tampering with Communication (Wired and Wireless)
- Exploiting a Lack of Access Controls
- Malicious Files Execution
- Legal Issues
- Methods described in the training are demonstrated during live penetration tests and IT security audits. Our real live experience has allowed to work out the applicable testing methodology that requires a solid understanding of the security profile of the target. We are proud to say that this course is equally important for those who

- Operating System Services Security Overview
- Operating System Internal Security
- Databases Security
- Google Hacking
- HTTP Request Building
- Reconnaissance and Target Profiling
- Information Leakage and Error Handling
- Session Manipulation
- Tampering with Communication (Wired and Wireless)
- Exploiting a Lack of Access Controls
- Malicious Files Execution
- Legal Issues
- Methods described in the training are demonstrated during live penetration tests and IT security audits. Our real live experience has allowed to work out the applicable testing methodology that requires a solid understanding of the security profile of the target. We are proud to say that this course is equally

## Flere Informationer:

For yderligere informationer eller booking af kursus, kontakt os på tlf.nr.: 44 88 18 00

[training@globalknowledge.dk](mailto:training@globalknowledge.dk)

[www.globalknowledge.com/da-dk/](http://www.globalknowledge.com/da-dk/)

Global Knowledge, Stamholmen 110, 2650 Hvidovre