OT300 OT Pentesting

Kurzbeschreibung:

Penetrationstests können das Sicherheitsniveau erheblich anheben, weswegen sie in Zeiten existenzieller Bedrohungen durch Ransomware und Co. aus der IT-Welt nicht mehr wegzudenken sind. Mit der zunehmenden Vernetzung von OT-Umgebungen steigt allerdings auch in diesem Umfeld das Risiko, Opfer eines Cyberangriffs zu werden, wie die zahlreichen Zwischenfälle der vergangenen Jahre gezeigt haben.

Das Training **OT300 OT-Pentesting** vermittelt die erforderlichen Grundlagen, um im OT-Umfeld Penetrationstests durchführen zu können und somit die Sicherheit der eigenen Produktionsanlagen/OT-Umgebungen, als wichtigen Baustein der IT-Sicherheitsarchitektur, zu stärken.

Zielgruppe:

- Blue Teams / Security-Teams / Security Practitioner
- IT- und Cybersecurity-Experten
- OT-Verantwortliche
- IT-Verantwortliche mit Bezug zu OT/Produktionsanlagen/Industriesteuerung
- IT- und OT-Fachleute, die ihre Fähigkeiten im Bereich OT-Pentesting erweitern möchten

Voraussetzungen:

Um den Kursinhalten und dem Lerntempo im Workshop **OT300 OT-Pentesting** gut folgen zu können, sind folgende Kenntnisse nötig:

- Grundlegende IT- und Netzwerk-Kenntnisse
- Grundkenntnisse im Bereich IT-Security

Hilfreich, aber nicht zwingend erforderlich sind darüber hinaus:

- Handlungssicherheit im Umgang mit Linux-Betriebssystemen
- Grundkenntnisse im Bereich Netzwerk-Protokolle
- Programmier-Grundkenntnisse Python
- Erfahrung im Umgang mit Virtualisierungsumgebungen (VMware, VirtualBox, o.vglb.)
- Erfahrung hinsichtlich der Durchführung von Security Assessments im IT-Umfeld

Sonstiges:

Dauer: 5 Tage

Preis: 3950 Euro plus Mwst.

Ziele:

Die Teilnehmer des Kurses **OT300 OT Pentesting** erlangen die theoretischen wie praktischen Grundlagen zur Planung, Umsetzung, Auswertung und Dokumentation von OT-Security Assessments/Penetrationstests, können diese in ausgewählten Testszenarien anwenden und auf eigene OT-Geräte oder ganze OT-Umgebungen (eigene Produktionsanlagen) übertragen.

Inhalte/Agenda:

- **Einführung OT, OT-Security, Pentesting**
  - Besonderheiten (OT vs. IT)
  - Normen, Standards, Zertifizierungen
  - Ziele, Ausprägungen/Abgrenzungen
  - Wording
  - Methodik
- **Praktische Umsetzung der vorgestellten Methodik**
  - Passive Informationsgewinnung/OSINT
  - Aktive Informationsgewinnung
  - Systemanalyse
  - Angriffsszenarien
- **Physische Sicherheit**
  - Identifikation und Test von Schnittstellen
  - Betriebsmodi
- **Firmware**
  - Grundlagen
  - Firmwareanalyse
- **Reporting**
  - Schwachstellen bewerten und dokumentieren
- **Eigene Test-/Trainingsumgebung erstellen**
- **Capture The Flag (CTF) / Abschlussübung**
-