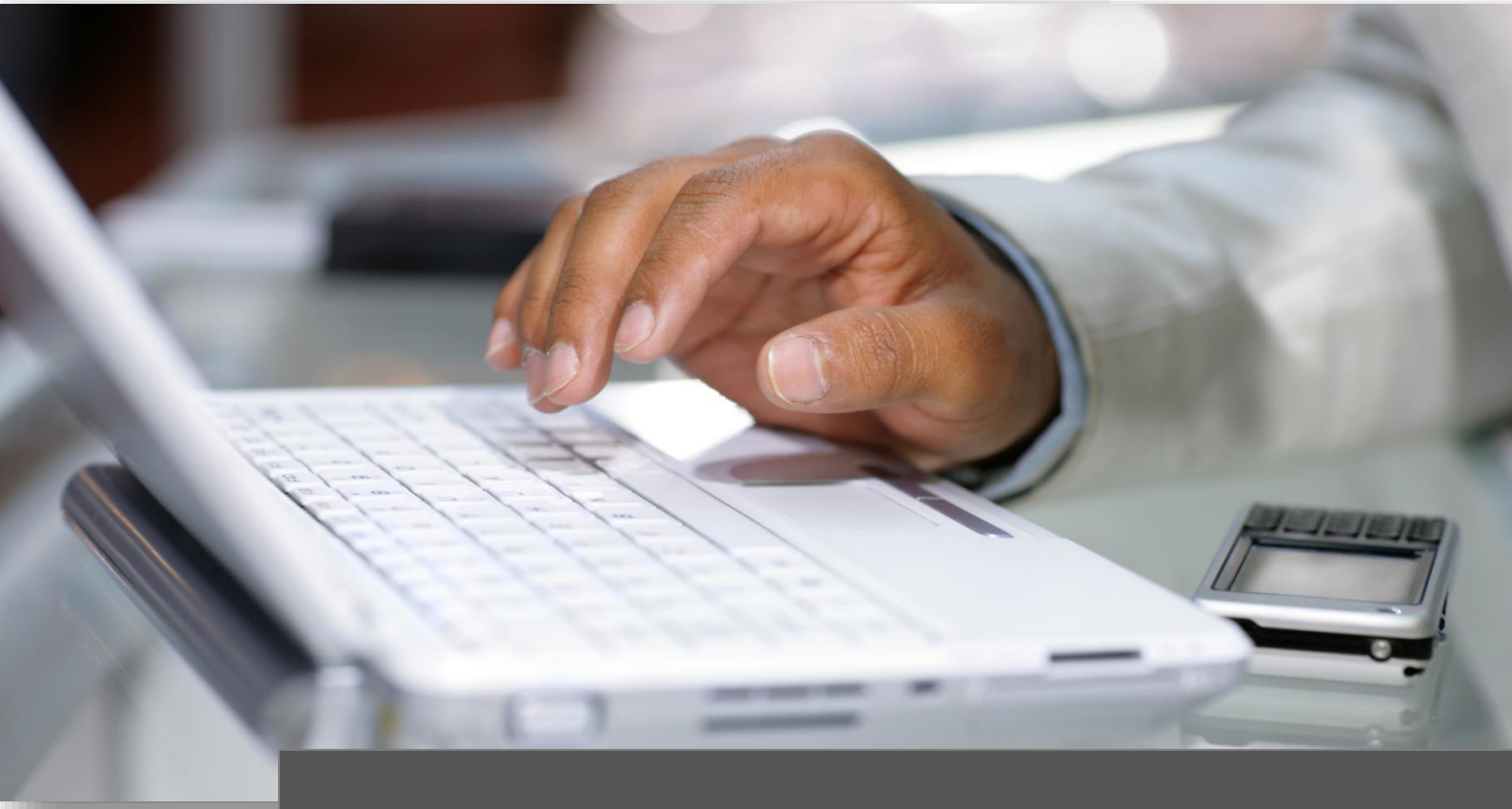
# ITKwebcollege.Security

## Advanced Trainings

Online-Trainings für Security-Consultants/Security-Experten | Stand Dezember 2023



Ausbildungsinhalte

ITKservice

# Inhaltsverzeichnis

# Security Advanced Trainings

## AD Hacking mit BloodHound

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

AD Hacking mit PowerShell
- ✓ Definition
- ✓ Gründe für BloodHound
- ✓ BloodHound in der Praxis
  - Wie sammle ich Informationen?
  - Wie nutze ich BloodHound?
  - Was gilt es zu beachten?
- ✓ Maßnahmen gegen BloodHound/Session-Enumeration

## AD Hacking mit PowerShell

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

AD Hacking mit PowerShell
- ✓ Zielsetzung
- ✓ Persönliche Meinung
- ✓ Empire Framework
- ✓ Verschleierung per Bordmittel (SED)
- ✓ Verschleierung über einfache Tools
- ✓ Verschleierung über komplexe Tools
- ✓ Auswirkungen auf Pentests

## Analyse von Logfiles und SIEM

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Analyse von Logfiles und SIEM
- ✓ Bedarfsanalyse
  - Beispiel: Website
- ✓ Kritikalität
  - Beispiel: Website
- ✓ Mindestanforderungen
  - Beispiel: Website
- ✓ Zählen reicht nicht aus?
- ✓ Automatismen schaffen
- ✓ Schnelles Security Monitoring mit OMD
- ✓ OMD CheckMK
  - Installation und Einsatz
  - Maßgeschneidert
- ✓ Logfile Analyse durch SIEM und Co
- ✓ Harte Fakten
- ✓ Dienstleistung & Services

## Anatomie und Härtung gegen Cyberangriffe

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Anatomie und Härtung gegen Cyberangriffe
- ✓ Phase 1: Angriffskanäle abseits der E-Mail
  - Physikalischer Zugriff (und Tests)
  - Datenträger (USB-Stick) und Tests
  - Manipulierte Devices
- ✓ Phase 2: Prüfungen der Resistenz
  - Firewall Prüfungen
  - Proxy Prüfungen
  - Spezielle Angriffsprotokolle
- ✓ Phase 2a: Prüfung der Möglichkeiten
  - AD Prüfung
  - Share Prüfung
  - Vulnerability Scan
  - NSM Dienstleistungen

## Angriffsszenario basierte Bedrohungsmodellierung mit Attack-Trees (2 UE)

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|
| Angriffsszenario basierte Bedrohungsmodellierung mit Attack-Trees<br>✓ Threat Modeling<br>✓ Benefits of Threat Modeling<br>✓ Bottom-Up Approach<br>✓ Top-Down Approach<br>✓ STRIDE<br>✓ DREAD<br>✓ PASTA<br>✓ Applicability<br>✓ Attack Trees in Threat Modeling<br>✓ Customization<br>✓ Attack Tree Creation<br>✓ Risk Mitigation<br>✓ Identifying Controls<br>✓ Examples<br>✓ Comparison<br>✓ | | |

## Backdoors, Angriffsmethoden und Erkennung

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|
| Backdoors, Angriffsmethoden und Erkennung<br>✓ Backdoor<br>▪ Funktionsweise<br>▪ Implementierung<br>✓ Häufige Backdoor/Angriff: DRIDEX<br>✓ Analyse von DRIDEX im Detail<br>✓ Tools zur Erkennung von Backdoors<br>✓ TCPView zur Prozessanalyse<br>✓ Alternative zur AV Erkennung: CyLance<br>✓ Erkennung über NSM Systeme<br>✓ Analyse per NSM<br>✓ Analyse per Network Flow Auswertung<br>✓ Kampf gegen Backdoors | | |

## Balena Cloud und IT-Security am Beispiel von Nessus

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|
| Balena Cloud und IT-Security am Beispiel von Nessus<br>✓ Balena Cloud im Überblick<br>✓ Balena und Security Appliances, Gründe<br>✓ Meine NSM/Balena<br>✓ Nessus für Balena Device<br>✓ Balena App erstellen<br>✓ Download des Image File<br>✓ Image auf NUC installieren<br>✓ Device in Balena einsehen | | |

## Building Hacking Labs

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Building Hacking Labs
- ✓ Hacken ist nicht schwer… und wie soll das funktionieren?
- ✓ Die Hardware
- ✓ Die einfach oder komplexe Variante
- ✓ Vagrant
  - Automatisierte Virtualisierung
  - Einfach Beispiele
  - Ausführliche Beispiele
  - Komplexes Beispiel
- ✓ Box selbst erzeugen
- ✓ Wieso Vagrant ein Thema ist

## Command & Control Frameworks

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Command & Control Frameworks
- ✓ Command & Control – Einführung
- ✓ C2 – Statische Command & Control
- ✓ C3/C4 – Customized Command & Control

## Crashkurs BURP Suite

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Crashkurs Burp Suite
- ✓ BURP Einführung – Interception Proxy
- ✓ BURP – Alternativer Proxy
- ✓ Automatisierte Scans mit BURP Suite
- ✓ Browser orientierte Scans
- ✓ Ohne Proxy
- ✓ BURP Suite Scan nach Baumstruktur
- ✓ Berichte mit BURP Suite erzeugen
- ✓ Gefundene Schwachstellen entfernen

## Crashkurs BURP Suite (3 UE)

| Unterrichtseinheit | UE 03 | SAD |
|---|---|---|

Crashkurs Burp Suite
- ✓ Recap SSL/TLS + Zertifikate
  - Hauptfunktionen von SSL/TLS
  - SSL/TLS für E2E Transportsicherheit
  - Zertifikat für Authentizität
- ✓ Was ist ein Intercepting Proxy?
- ✓ Anwendungsgebiete
  - Sicherheitsforscher und Unternehmen
- ✓ Praxisbeispiele

## Cyber Security Check – die bessere Alternative zum Pentest

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Cyber Security Check – die bessere Alternative zum Pentest
- ✓ Pentesting – Schnee von gestern?
- ✓ Neue Ideen und deren Umsetzung
- ✓ Die Methoden im Überblick
- ✓ E-Mail
- ✓ Vulnerability Scan
- ✓ Windows AD Security
- ✓ Firewall Security
- ✓ AD Password Security
- ✓ Reporting: CyberSecurityCheck by Colors

## Dark Hacker – Wie funktioniert das?

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|
| Dark Hacker – Wie funktioniert das?<br>✓ Schritt 1 – Die sichere TOR Umgebung<br>✓ Schritt 2 – Digitale Währung<br>✓ Schritt 3 – The Dark Side<br>✓ Schritt 4 – Digital Currency Exchanger<br>✓ Schritt 5 – Waschtag<br>✓ Schritt 6 – Waffenkäufe<br>✓ Shopping Option<br>▪ VPS Server<br>▪ VPN Accounts | | |

## Docker für IT-Security Spezialisten

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|
| Docker für IT-Security Spezialisten<br>✓ Docker für IT-Sicherheitsexperten<br>✓ Docker Basics<br>✓ Docker lernen<br>✓ Docker Plattformen<br>✓ Beispiel – Nessus Essentials<br>✓ Dockerfile für Nessus erstellen<br>✓ Build für Docker Nessus<br>✓ Nessus: Image starten und testen<br>✓ Docker Volumen: Persistenz für Container<br>✓ Beispiel – OpenVAS für Docker<br>✓ Beispiel – Verbesserter TOR Proxy | | |

## Docker für IT-Security Spezialisten (3 UE)

| Unterrichtseinheit | UE 03 | SAD |
|---|---|---|
| Docker für IT-Security Spezialisten<br>✓ Einordnung<br>✓ Virtuelle Maschinen vs. Container<br>✓ Einführung Docker<br>▪ Docker Build, Registry und Images<br>▪ Docker Container<br>▪ Docker Networks<br>▪ Docker Port Mappings<br>▪ Docker Volumes und Bind Mounts<br>✓ Sicherheitsempfehlungen<br>✓ OSINT in der Praxis | | |

## Elastic Cloud SIEM im Eigenbau

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|
| Elastic Cloud SIEM im Eigenbau<br>✓ SIEM aus Elastic Cloud<br>✓ Aufbau als praktische Live Demo | | |

## E-Mail Spoofing & Spearphishing

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|
| Spearphishing Angriffe per E-Mail<br>✓ Beispiel<br>✓ Wie Angreifer professionelle E-Mails erzeugen<br>✓ Professionelle E-Mails mit Atomic Studio<br>✓ Stichwort: Proxy Server<br>✓ Verifikation von E-Mail Adressen<br>✓ Erstellen von professionellen E-Mails | | |

## Emotet is back

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | Emotet is back<br>✓ Bit Paymer<br>▪ 2017<br>▪ 2018<br>✓ Angriffsrekonstruktion<br>✓ TRICKBOT<br>▪ Kommunikation<br>▪ Hits<br>✓ Emotet vs. AV<br>✓ Ziel des Angreifers<br>✓ Angriff früh erkennen<br>✓ Problematik<br>▪ NSM – Port Mirroring<br>✓ Blocklisten | | |

## Empire 3 (BC Security) und CrackMapExec

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | Empire 3 (BC Security) und CrackMapExec<br>✓ Empire Framework 3<br>✓ AD Hacking Umgebung<br>✓ AD Analyse mit PingCastle<br>✓ Angriff gegen Domäne<br>✓ CrackMapExec (CME)<br>✓ Kombinationen | | |

## Empire Framework

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | Empire Framework<br>✓ Profitool für Domainhacker<br>✓ Empire Framework für Ubuntu 16.04<br>✓ Installation von Empire<br>✓ Erste Schritte: Listener erstellen<br>✓ Listener von außen betrachtet<br>✓ Stager im Überblick<br>✓ Word Macro Stager als Beispiel<br>✓ Self Hacking<br>✓ Alternative zum Stager: Launcher<br>✓ Powershell Payload<br>✓ UAC Bypass gegen Up2Date Windows 10<br>✓ Domain mit Empire hacken | | |

| | Unterrichtseinheit | UE 02 | SAD |
|---|---|---|---|
| | Empire Framework<br>✓ Profitool für Domainhacker<br>✓ Empire Framework für Ubuntu 16.04<br>✓ Angriffe gegen Windows Domäne<br>✓ Microsoft LAPS<br>✓ Effekt eines Angriffs<br>✓ Mit Verlusten muss gerechnet werden …?<br>✓ Weitere sichere Domain Konfigurationen …?<br>✓ Wieso Fails? | | |

## Empire Framework & Deathstar

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | Empire Framework & Deathstar<br>✓ Auszug Manila Hacking Days 2018<br>✓ Empire Framework<br>▪ Überblick<br>✓ Domain Security in a Nutshell<br>✓ UAC-Bypass: Klassisches Szenario<br>✓ Memory Access ist kritisch?<br>✓ Ideale Lösung: Microsoft LAPS<br>✓ Und der Domain Administrator?<br>✓ Vorsicht bei Server Admin Accounts<br>✓ Deathstar spart Zeit: Angriff los!<br>✓ Testszenario<br>✓ Fazit: Deathstar/Empire testen | | |

## Erkennung von LOG4J Sicherheitslücken

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | Erkennung von LOG4J Sicherheitslücken<br>✓ Log4J/Log4Shell<br>▪ Überblick<br>▪ Was kann passieren?<br>▪ Beschaffenheit der Sicherheitslücke<br>▪ Probleme lösen<br>✓ UPDATE<br>▪ LOG4J per Nessus prüfen<br>▪ LOG4J per Burp Suite prüfen<br>▪ LOG4J per Docusnap erkennen | | |

## Erpressungstrojaner oder Kryptotrojaner (Ransomware)

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | Ransomware<br>✓ Funktionsweise und Abwehr<br>✓ Erscheinung der Neuzeit?<br>✓ Wer ist betroffen?<br>✓ Sollte man zahlen?<br>✓ Wieso erwischt man die nicht?<br>✓ Infektionswege?<br>✓ E-Mail Infektion<br>✓ E-Mail Payload<br>✓ Webbrowser Angriffe<br>✓ Welche Exploits stecken drin<br>✓ Netzwerkanalyse Locky<br>✓ Wie funktioniert Locky?<br>✓ Welche Dateien greift Locky an?<br>✓ Abwehrmaßnahmen<br>Ransomware 2.0<br>✓ Was kommt auf uns zu? | | |

## Exchange Hack – Maßnahmen

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | Exchange Hack – Maßnahmen<br>✓ Kurze Historie des Angriffs<br>✓ Wer hat´s erfunden?<br>✓ Entry Point: Exchange, System Account<br>✓ A New Era: Geburtsstunde der AD Forensik<br>✓ Prophylaxe: NSM Sensoren einsetzen!<br>✓ Anbieter für AD Forensic/NSM Sensoren | | |

## Forensische Erfassung von RAID Laufwerken

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | Forensik und RAID-Laufwerke<br>✓ Durchführung einer RAID-Forensik<br>✓ Erfassung der einzelnen Datenträger<br>✓ E01 Image als Empfehlung<br>✓ Alle forensischen Kopien erstellt<br>✓ Wie kommt R-Studio an Platten ran<br>✓ In R-Studio einbinden<br>✓ Abschließende Forensische Kopie des Images<br>✓ Verwendung in Forensik Tools | | |

## Früherkennung von Cyberangriffe

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | Früherkennung von Cyberangriffen<br>✓ Erkennen Sie Angriffe rechtzeitig oder erst nach dem Datenabfluss?<br>✓ Ausprägung von Cyberangriffen<br>✓ Scanning der Unternehmensnetzwerke<br>✓ Effiziente Erkennung<br>▪ Log File Analyse/SIEM<br>▪ Network Security Monitoring | | |

## Graylog 5 – OpenSearch 2

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | Graylog 5 – OpenSearch 2<br>✓ Graylog5<br>✓ Docker Way<br>✓ OpenSearch – SigmaHQ<br>✓ OpenSearch – Dashboards | | |

## Hacker Kubernetes

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | Hacker Kubernetes<br>✓ Was ist Kubernetes?<br>✓ Angriffsszenario<br>✓ Damn Vulnerable Web Application (DVWA)<br>✓ Angriffsphase 1: Shell Code Injection<br>✓ Evil Genius: MSF ELF Payload per Shell<br>✓ Lösungsansatz: BASE64 Encoding<br>✓ Meterpreter Inbound: Verbindung hergestellt!<br>✓ Root Exploit?<br>✓ Kubernetes gehackt | | |

## Hacker’s Diary – Breakouts aus dem Firmennetzwerk

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Breakouts aus dem Firmennetzwerk
- ✓ Wieso sollte man die Outbound-FW abhärten?
- ✓ Methoden für den Breakout Test
- ✓ Outbound per NMAP prüfen
- ✓ Reverse Scan im Überblick
- ✓ Reverse Scan:
  - ✓ Funktionsweise
  - ✓ Ergebnisse auswerten
  - ✓ Sinn
- ✓ ICMP Breakout Check

Breakouts aus dem Firmennetzwerk
- ✓ ICMP Tool: HANS
  - ✓ HANS einsetzen
- ✓ DNS Breakout Check
- ✓ DNS Breakout Tool: iodine
  - ✓ Iodine einsetzen
- ✓ TOR Breakout Check
- ✓ TOR Breakout Tool: TOR
  - ✓ TOR einsetzen
- ✓ Breakout Tests?

## Hacker’s Diary - Dedicated Malware Attack

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Gezielte Malware-Angriffe gegen Unternehmen
Information Gathering
Livedemo
- ✓ Angriffsmethode finden
- ✓ Dark Net Analyse der Ziele
- ✓ Informationssammlung
- ✓ Malware als Baukasten
- ✓ Dark Services
- ✓ Auslieferung der Malware

Gegenmaßnahmen

## Hacker’s Diary - Professioneller TOR Gateway

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Professioneller TOR Gateway
- ✓ Dark Gate – Professioneller TOR Gateway
- ✓ Kochtopf für den Dark Gate
- ✓ Argumente für ESXi/NUC
- ✓ TOR Gatway assemblieren
- ✓ Whonix Gateway einbauen
- ✓ Whonix Gateway komprimieren
- ✓ pfSense
- ✓ Dark Gate wird Super Dark Gate
  - Master Edition Gate

## Hacker’s Diary - Unerkannt bleiben

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Überblick: Methoden zur Tarnung
- ✓ Anonyme Netzwerke
  - Öffentliche Zugänge
  - Erkennungsmerkmale
    - MAC Adressen tarnen
    - Videoüberwachung in Deutschland
    - Augenzeugen
  - Hidden Services
    - Proxy Server
    - VPN Anbieter
  - Anonyme Betriebssysteme
  - Spezial: TOR-KALI-Master Unit

## Hacking und IT-Security

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Aktuelle Angriffsszenarien
- ✓ Angriffe im Überblick
  - Kryptotrojaner (Ransomware)
  - SEO Fraud
  - Zielgerichtete Attacken
- ✓ Dienstleistungen im Überblick
  - Penetrationtesting
  - Forensische Analysen
  - NSM Analysen

Ransomware
- ✓ Ransomware 2016
- ✓ Ransomware in Zahlen
- ✓ Sofortmaßnahmen
- ✓ Sofortmaßnahmen/Kalkulation
- ✓ Prophylaxe

SEO Fraud
- ✓ SEO Fraud 2016
- ✓ Blind Phishing Angriffe
- ✓ E-Mail Interception Angriffe
- ✓ E-Mail/Telefon Angriffe
- ✓ Gegenmaßnahmen

Zielgerichtete Attacken
- ✓ Sofortmaßnahme

Dienstleistungen im Überblick

## Handwerkszeug für Securityspezialisten

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Handwerkszeug für Securityspezialisten
- ✓ Thema: Laptops
- ✓ Lösung zum Laptop Dilemma: APU2
  - APU2 Board
  - APU2 Installation
  - APU 2 Baukasten
- ✓ Ubuntu per VMware Workstation installieren
- ✓ FREE ESXi
- ✓ Szenarien und Installation
- ✓ OpenVAS für Ubuntu 16.04
- ✓ Nessus für Ubuntu 16.04
- ✓ Empire Framework für Ubuntu 16.04
- ✓ CrackMapExec für Ubuntu 16.04
- ✓ NMap für Ubuntu 16.04

## IDS-System: Wirksamer Schutz?

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

IDS-System
- ✓ Rollout der Ransomware
- ✓ Neue Infektion
- ✓ Funktionsweise
- ✓ Snort
  - Historie
- ✓ Subscription Rulesets
  - Überblick
  - Vorteile
- ✓ Emerging Thread (ET)
  - Open Rulesets
  - Daily Updates
- ✓ Snort Rule Beispiele
- ✓ Maleware Zeus
- ✓ Security Onion und Snort Rules
- ✓ Bro
  - Übersicht
  - In der Praxis

## Infrastruktur und Demilitarisierte Zone (DMZ)

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Wie Sie ein Unternehmen besser absichern
Angriffspunkte im Überblick
- ✓ Mitarbeiter
- ✓ Webserver
- ✓ IT-Infrastruktur
- ✓ DMZ

Infrastruktur im Überblick
- ✓ Häufig homogen gewachsen
- ✓ IT folgt Anforderung des Unternehmens
- ✓ Altlasten im Unternehmen
- ✓ Häufig keine Klassifikation von Sub-Netzen
- ✓ Analysen von Netzwerkströmen nur im Störfall

Maßnahmen
- ✓ Organisatorische Maßnahmen
- ✓ Technische Maßnahmen

Schutzbedarf nach Bereich
- ✓ Arbeitsplatz
- ✓ Server
- ✓ Domaincontroller

Nessus Schwachstellenscanner
Greenbone Security Manager (GSM)
Web Security Scanner Netsparker Professional
Erfassung von offenen Diensten
Sonderrolle
- ✓ DMZ

## IT-Forensic

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

IT Forensic
- ✓ Geschichte der Computer Forensic
- ✓ Erfolge der Computer Forensic
- ✓ Unterstützende Gesetze
- ✓ Forensic im Internet
- ✓ Forensic Tools
  - OSForensics
  - Volatility
  - DEFT Linux
- ✓ Beispiel Projekt
  - CFREDS
- ✓ Umsetzung in Phase
- ✓ Forensische Analyse
- ✓ Forensische Berichterstattung

## IT-Security Box im Eigenbau – Vorstellung und Business Potential

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

IT-Security Box im Eigenbau – Vorstellung und Business Potential
- ✓ IT-Security Box aus Business
- ✓ Die „Hardware“
- ✓ Funktionen
- ✓ Vulnerability Scan
- ✓ NSM Sensor
- ✓ AD Testsysteme
- ✓ Firewall Checkup Device
- ✓ (Security) Monitoring System
- ✓ Security Onion Sensor
- ✓ Web Security Box

## IT-Security: Firewall, Proxy, AV-Testing

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

IT-Security: Firewall, Proxy, AV-Testing
- ✓ Simulation eines Cyberangriffes
- ✓ Auffällige Elemente
- ✓ Payloads erstellen
- ✓ Fortgeschrittene Payloads erstellen
- ✓ Verschleierte Payloads
- ✓ Kommerzielle Frameworks

## KALI2018: Web Hacking Tools im Überblick

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

IT-Security Box im Eigenbau – Vorstellung und Business Potential

- ✓ IT-Security Box aus Business
- ✓ Die „Hardware“
- ✓ Funktionen
- ✓ Vulnerability Scan
- ✓ NSM Sensor
- ✓ AD Testsysteme
- ✓ Firewall Checkup Device
- ✓ (Security) Monitoring System
- ✓ Security Onion Sensor
- ✓ Web Security Box

## KALI2018: Web Hacking Tools im Überblick

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

KALI2018

- ✓ KALI Linux 2018 Edition
- ✓ Grundsätzliches: KALI vs. Windows
- ✓ DAMN VULNERABLY WEB APPLICATION (DVWA)
- ✓ KALIs Web Security Scanner
  - OWASP ZAP
  - BURP Suite
- ✓ Effektive Web Angriffe mit KALI
- ✓ Effektives Verstecken von Web Angriffen

## KALI 2019 im Überblick

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

KALI Linux 2019.4

- ✓ Besonderheiten
- ✓ Neuerungen
- ✓ Pentest nach Kategorie
- ✓ Information Gathering
- ✓ Vulnerability Management
- ✓ Installationsanleitung für OpenVAS
- ✓ Nessus Essentials für KALI Linux
- ✓ Docker für KALI Linux

## Malware & Viren

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Ursprung, Funktion & Bekämpfung

- ✓ Kurze Historie der Malware
- ✓ Quellen moderner Malware
  - Verbreitungskanal: E-Mail
  - Verbreitungskanal: Exploit Kit
- ✓ Angebote für Malware
  - Darknet Börsen: AlphaBay Market
- ✓ Funktionen moderner Malware
  - Ransomware
  - Keylogger
  - Trojans
- ✓ Abwehrverfahren im Überblick
  - Anti Maleware Lösungen
  - Network Security Monitoring
  - Generelle Abwehrmethoden

Ursprung, Funktion & Bekämpfung

- ✓ Viren 2016: Symantec IS Treat Report
- ✓ Exploit Kit Analyse mit NSM
- ✓ Malware im Internet
- ✓ Erkennungsquote von Malware
- ✓ Malware Tarnverfahren
- ✓ Effekte moderner Malware
- ✓ Tspion – Keylogger im Kleinstformat
- ✓ Analyse von Tspion über Malwr.com

## Meltdown & Spectre (und) Memory Attacks

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Meltdown/Spectre/Memory Attacks

- ✓ Meltdown
  - Angriff
  - Beschreibung
  - Vorführung
  - Bedrohungspotential
- ✓ Spectre
  - Angriff
  - Beschreibung
  - Angriffsmethoden
  - Bedrohungspotential
- ✓ Chance für Dienstleister

## Meltdown/Spectre – Stand Dezember 2018

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Meltdown/Spectre

- ✓ Was ist eigentlich Meltdown?
  - Kurz und bündig
  - Ausführlich
- ✓ Was ist eigentlich Spectre?
  - Kurz und bündig
  - Ausführlich
- ✓ Bisherige Varianten
- ✓ Neue Varianten
- ✓ Spectre-NG im Überblick
- ✓ NetSpectre
- ✓ Foreshadow
- ✓ Meltdown/Spectre prüfen
- ✓ Gegenmaßnahmen

## Memory Analysen & Empire 4

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Memory Analysen & Empire 4

- ✓ Voraussetzung für Memory Analysen
- ✓ VMware Workstation als Virtualisierer
- ✓ POSIX Tools für Windows
- ✓ Windows Logon
- ✓ Spickzettel Syntax
- ✓ Empire Framework 4

## Network Security Monitoring (NSM)

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Security Onion

- ✓ Historie
- ✓ Primäre Tools in Security Onion
- ✓ Snort
- ✓ Xplico/Netminer
- ✓ Sguil/Squert
- ✓ ELSA/Bro
- ✓ Argus/RA

Snort

- ✓ Historie
- ✓ Emerging Thread (ET) Rules für Snort
- ✓ Emerging Thread (ET) Daily Updates
- ✓ Snort Rule Beispiel: Malware Zeus (Community)
- ✓ Snort Rules und Alerts

Sguil

- ✓ Übersicht
- ✓ Herzstück der Security Onion
- ✓ Passive Real-time Asset Detection System (PRADS)
- ✓ Schlüsselfunktionen
- ✓ Mächtiges Werkzeug

SQUERT

- ✓ NIDS/HIDS Event Konsole

Bro

- ✓ Übersicht

## Neue Anforderungen an Pentests 2021+

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|

Neue Anforderungen an Pentests 2021+
- ✓ Neue Anforderungen?
- ✓ E-Mail Security
- ✓ SPF als Fallstrick?
- ✓ SPF Check für Partner?
- ✓ Markieren von EXTERNEN E-Mails
- ✓ Windows AD Security
- ✓ Firewall Security
- ✓ Proxys & C2
- ✓ Password Security AD
- ✓ Security Audits als Konzept?

## OpenVAS – Schwachstellenscanner

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|

- ✓ Überblick
- ✓ Installation unter KALLI Linux
- ✓ Community Edition
- ✓ Ein erster Scan per Wizard
- ✓ Scans im Detail Konfigurieren
- ✓ Wiederkehrende Scans festlegem
- ✓ Simple Target: Metasploitable v2
- ✓ Metasploitable – Auswertung der Ergebnisse

## Opfer eines Hackerangriffs

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|

Erkennung des Angriffes
- ✓ Abfluss von Unternehmensdaten
- ✓ Forderungen/Erpressung
- ✓ Technische Erkennung
- ✓ Technische Auffälligkeiten/Anomalien

Abfluss von Unternehmensinformationen

Forderung und Erpressung

Technische Erkennung
- ✓ Analyse über Security Devices

Technische Auffälligkeiten/Anomalien
- ✓ Ungewöhnliches Anwendungs-/PC-Verhalten

Wie tief ist der Angreifer eingedrungen
- ✓ Initial Analyse
- ✓ Erstanalyse

Lassen sich die Angreifer lokalisieren
- ✓ Grundsätzliches

Welche Systeme sind betroffen
- ✓ Grundsätzliches Vorgehen

Fließen Unternehmensinformationen ab

## OSINT im Überblick

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|

OSINT im Überblick
- ✓ Was ist OSINT
- ✓ Ziele von OSINT Operationen
- ✓ Informationsquellen
- ✓ Kurze Historie
- ✓ Wie macht man OSINT?
- ✓ Buscador – letzte Version 2019

OSINT im Überblick
- ✓ Vorgehensweise
- ✓ Einfacher Ansatz: Google Hacking
- ✓ Username lokalisieren
- ✓ E-Mail-Adressen finden
- ✓ Übergreifende Tools

## OSINT im Überblick (3 UE)

| | Unterrichtseinheit | UE 03 | SAD |
|---|---|---|---|

OSINT im Überblick
- ✓ Definition
  - Daten vs. Information
  - Begrifflichkeit
- ✓ Gründe und Absichten
- ✓ Maßnahmen gegen OSINT
- ✓ OSINT in der Praxis

## OSINT in der IT-Security

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|
| OSINT in der IT-Security<br>✓ Spiderfoot Treffer<br>✓ OSINT Klassisch<br>✓ OSINT Framework | | |

## Pentesting 2019

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|
| Pentesting 2019<br>✓ Pentesting von der Stange<br>✓ Wie sieht ein „typischer“ Pentest aus?<br>✓ Wovor will sich der Kunde schützen?<br>✓ Wieso dann der Vulnerability Scan?<br>✓ Phase 1: Vulnerability Scan?<br>✓ Phase 1: Kritikalität<br>✓ Phase 1: Vulnerability Beschiß?<br>✓ Zeitaufwand: Berichte schreiben<br>✓ Exploiting: Machen wir nicht!<br>Live-Demos<br>✓ Angriffscheck per E-Mail<br>✓ Check der Angreifbarkeit (E-Mail)<br>✓ Firewall- INTERN -> EXTERN<br>✓ Domain Security Checks | | |

## Pentest mit NSM aufwerten

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|
| Pentest mit NSM aufwerten<br>✓ Alleinstellungsmerkmal<br>✓ Network Security Monitoring (NSM)<br>✓ Anforderungen an NSM-Pentest-Systeme<br>✓ Ideale Hardware: APU4<br>✓ Vorbereitungen<br>✓ NSM Komponenten für APU4<br>✓ Shortcuts für die Installation<br>✓ Probe aufs Example | | |

## Pentest Server in der Cloud erstellen

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|
| Pentest Server in der Cloud erstellen<br>✓ MS Exchange Sicherheitslücke<br>✓ Pentest Server in der Cloud – die Vorteile<br>✓ Welches Betriebssystem?<br>✓ Pentest Server: Windows 10<br>✓ Tools<br>▪ Nessus<br>▪ TOR<br>▪ Proxifier<br>▪ TOR Browser<br>▪ BurpSuite<br>▪ ScrapeBox<br>KALI Linux | | |

## Professioneller TOR Gateway

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|
| Professioneller TOR Gateway<br>✓ Dark Gate – Professioneller TOR Gateway<br>✓ Kochtopf für den Dark Gate<br>✓ Argumente für ESXi/NUC<br>✓ TOR Gatway assemblieren<br>✓ Whonix Gateway einbauen<br>✓ Whonix Gateway komprimieren<br>✓ pfSense | | |

| | |
|---|---|
| | ✓ Dark Gate wird Super Dark Gate<br>✓ Master Edition Gate |

## ProxMox für den Aufbau einer IT Security Service Infrastruktur

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | ProxMox für den Aufbau einer IT Security Service Infrastruktur<br>✓ Wie funktioniert ProxMox | | |

## ProxMox Single IP als IT Security Node

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | ProxMox Single IP als IT Security Node<br>✓ Installation des ProxMox Server<br>✓ Firewall Freischaltung für ProxMox Cluster<br>✓ Welche IT-Security Appliances machen Sinn<br>✓ Web/Vulnerability Maschine<br>✓ NSM Cluster<br>✓ Cloud Lab | | |

## Raspberry Pi/Hacking Devices

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | ✓ Raspberry Pi und Hacking Devices<br>✓ Hacker im Taschenformat gefällig?<br>✓ Zwerge und Riesen<br>✓ Aufgaben einer Hacking Device<br>✓ Störung des Betriebsablaufs<br>✓ Aufbau einer einfachen Hacking Device<br>✓ Bestückung eines Raspberry Pi 3<br>✓ Betriebssysteme für Raspberry Pi Hacking<br>▪ Basis OS<br>▪ KALI Linux<br>✓ Special: Raspberry Pi ohne Steckdose<br>✓ KALI Linux auf Raspberry installieren<br>✓ KALI Linux vorbereiten<br>✓ Konfigurationsdetails<br>✓ RASPI-CONFIG im Überblick<br>✓ Raspberry Pi vorbereiten<br>✓ Zugriff auf das Unternehmensnetzwerk<br>✓ Vorsicht: Für die echten Hacker | | |

## Security Logs nach ELK

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | ✓ Sicherheit und Konsolen<br>✓ Zentrale Container für Logsammlungen<br>✓ ElasticSearch in kurzen Worten<br>✓ Komponenten zu ElasticSearch<br>✓ Beats im Überblick<br>✓ ElasticSearch im Eigenbau<br>✓ ElasticSearch für Ubuntu 18.04<br>✓ Filebeat für Ubuntu 18.04 einrichten<br>✓ Auditbeat für Ubuntu 18.04 einrichten<br>✓ Suricata für Ubuntu 18.04 einrichten<br>✓ Adaption für ElasticCloud<br>✓ Variationsmöglichkeiten<br>✓ Graylog<br>✓ Suricata & Zeek<br>✓ ELK, Graylog, Suricata, Zeek? | | |

## Security mit transparenten Brücken

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Security mit transparenten Brücken
- ✓ Transparente Brücken im Einsatz
- ✓ Wie funktioniert eine transparente Brücke?
- ✓ OpenBSD Filter mit Trans.Bridge
- ✓ Aufbau der transparenten Brück (OpenBSD)
- ✓ pfSense als transparente Firewall
- ✓ Konfiguration der transparenten Firewall
- ✓ Fleißaufgaben für pfSense/Trans.Firewall
- ✓ Security Onion mit Trans.Bridge
- ✓ Security Onion Setup: Portmirror als Bridge!
- ✓ Security Onion für Fortgeschrittene
- ✓ NACKered Script für 802.1X Bypass

## Security Onion 1

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Security Onion 1
- ✓ Business mit Security Onion 1
- ✓ Pricing für SIEM/NSM-Services
- ✓ Master Server Installation
- ✓ Hetzner Cloud Service einrichten
- ✓ Installation Security Onion 1 auf Masterserver
- ✓ Integration von Security Onion 1 Nodes
- ✓ Installation & Konfiguration des Sensors
- ✓ System Live im Einsatz

## Security Onion 2

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Security Onion 2
- ✓ Enthaltene Tools
- ✓ Security Onion 2 im Einsatz

## Security Onion 2018

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Security Onion 2018
- ✓ NSM System
- ✓ Grundfunktionen / Tools
- ✓ Einsatzgebiete
- ✓ Einrichtung der Security Onion
- ✓ Testalarm für Security Onion
- ✓ NSM Konsolen im Überblick
- ✓ Live System im Überblick
- ✓ Dienstleistung NSM

## Security Onion 2020

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Security Onion 2020
- ✓ Security Onion – NSM basierte Distribution
  - ✓ Standard Installation
  - ✓ Server Sensor Installation

## SIEM aufbauen mit Elastic Cloud

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

SIEM aufbauen mit Elastic Cloud

- ✓ Neuerungen seit Elastic
- ✓ Aufbau des SIEM mit Elastic 8.4
- ✓ Elastic Agent unter Windows installieren
- ✓ Endpoint Security
  - ✓ Konfigurieren

## Social Engineering

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

Meltdown & Spectre

- ✓ Pre-Meltdown Bemühungen
- ✓ Das Ergebnis: Meltdown & Spectre
- ✓ Was ist eigentlich Meltdown?
  - ✓ Kurz & bündig
  - ✓ Ausführlich
- ✓ Was ist eigentlich Spectre?
  - ✓ Kurz & bündig
  - ✓ Ausführlich
- ✓ Viel wichtiger: Sind Sie eigentlich geschützt?
- ✓ Patches für Microsoft Windows
- ✓ Welche Lücken beseitigt der Windows Patch?
- ✓ Welche Lücken bleiben trotz Patch?
- ✓ Patches für Windows 7 und Windows 8?
- ✓ Wird Windows Server automatisch geschützt?
- ✓ Schnellanleitung Windows
- ✓ Patchstand
- ✓ Wachsamkeit

## Spectre Update + Alarmstufe Rot

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

- ✓ Was ist Social Engineering?
- ✓ Grundsätzliche Arten des Social Engineering
  - ✓ Human Based
    - Impersonation
    - Posing as important User
    - Being a third party
    - Desktop Support
    - Shoulder Surfing
    - Dumpster Diving
  - ✓ Computer Based
    - Phishing
    - Spear Phishing
    - Baiting
      - Special USB Hacking
      - Website Beispiel
  - ✓ Online Scam

## The Golden Ticket

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

### The Golden Ticket

- ✓ Aufbau der Testumgebung
- ✓ Eine der gefährlichsten Angriffsmethoden
- ✓ Etwas Hexa notwendig
- ✓ Technische Durchschüsse gegen DCs?
- ✓ Indirekte Angriffe sind möglich
- ✓ Ergebnisse
- ✓ Effekt: Ticket Granting Tickets
- ✓ Ergebnis: Uneingeschränkte Zugriffsrechte
- ✓ Gegenmaßnahmen
- ✓ Erkennung von Golden Ticket Angriffen

## Tracking the Hackers mit OSINT

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

### Tracking the Hackers mit OSINT

- ✓ OSINT – ein mächtiges Werkzeug
- ✓ Plattform: Spiderfoot HX
- ✓ Jagd nach Leak Informationen
- ✓ OSINT Framework – Zentraler Sprungpunkt
- ✓ Doppel Leaks – interessante Einblicke
- ✓ OSINT – eine mächtige Waffe

## UAC-Angriffe gegen Windows 10 & Brute Ratel C4 Framework

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

### UAC-Angriffe gegen Windows 10 & Brute Ratel C4 Framework

- ✓ Brute Ratel C4 Framework
- ✓ Aufbau von Brute Ratel
- ✓ Erstellung von Individual-Malware
- ✓ Übernahme einer W10EE
- ✓ UAC deaktivieren
- ✓ Übernahme des User-Admins
- ✓ Fortgeschrittene Malware

## Vulnerability Scanner und deren Anwendungen

| Unterrichtseinheit | UE 01 | SAD |
|---|---|---|

### Vulnerability Scanner und deren Anwendungen

- ✓ Was ist eine Schwachstelle?
- ✓ Aufspüren einer Schwachstelle
- ✓ Vulnerability Scanner Grundfunktionen
- ✓ Verfügbare Scanner
  - ✓ Open Source
    - OpenVAS
  - ✓ Kommerzielle
    - Tenable Nessus
    - Rapid7 Nexpose
    - Qualys
    - Goolge: Vulnerability Scanner
    - Metasploitable

## Vulnerability Scanning as a Service (Business Idee)

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | Vulnerability Scanning as a Service (Business Idee)<br>✓ GVM + CheckMK<br>✓ Schwachstellenscanner suchen<br>✓ GVM im Überblick<br>✓ GVM nach CheckMK<br>✓ CheckMK<br>✓ Implementierung (Beta) | | |

## Waffen der Hacker: SQL Injection

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | ✓ SQL Injection (SQLi) Erkennen und Abwehren<br>✓ SQL Injection<br>▪ Gefahren<br>▪ Grundlagen<br>✓ Betroffene Programmiersprachen<br>✓ SQL Injection in der Praxis<br>✓ Angriffstool: SQLMAP<br>✓ Erfolgreiche Angriffe<br>✓ Log goes SIEM?<br>✓ Streams vs. SQL Injection<br>✓ Einfachere Abwehrmethoden<br>✓ Effizienteste Abwehr: Gute Programmierung | | |

## Webservice und –server

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | Angriffe gegen Webanwendungen<br>Immunisierung gegen Strafverfolgung<br>Angreifertypen (Web Attacken)<br>Abhärtung gegen Angriffe<br>Grundregeln<br>✓ Szenario 1<br>Schlechtes Beispiel<br>✓ Szenario 2<br>Gutes Beispiel<br>Abhärtung gegen Angriffe: Hardening<br>Abhärtung von Apache Webserver<br>Überprüfung der SSL/TLS Einstellung<br>OWASP<br>✓ All About Web Security<br>✓ A1 – SQL Injection im Detail & Tools<br>✓ A3 – Cross Site Scripting<br>Universelle Web Security Scanner<br>Spitze des Eisbergs | | |

## Wie funktioniert ein RAT?

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | ✓ Remote Access Toolkit (RAT)<br>✓ Erkennung von RATs<br>✓ Häufig im Einsatz: Trickbot<br>✓ RATs im Internet finden<br>✓ Pylris RAT im Einsatz<br>✓ Pylris im Praxiseinsatz<br>✓ The perfect RAT?<br>✓ Wie findet man RATs? | | |

## Wie sicher ist Festplattenverschlüsselung?

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | ✓ Bitlocker und Co.<br>✓ Der Bootprozess<br>▪ Größte Schwachstellen<br>▪ Secure Boot<br>▪ Normale Boot Prozess<br>▪ Fazit<br>✓ Was hat das mit Bitlocker und Co. zu tun?<br>✓ Wie lässt sich Bitlocker angreifen?<br>✓ Angriffsszenario<br>✓ Kommerzielle Tools für Key Extraaktion<br>✓ Master Key im Einsatz<br>✓ Wie kriegt man Bitlocker sicher?<br>✓ Welche Verschlüsseler sind angreifbar?<br>✓ Veracrypt | | |

## Wie sich Hacker im Internet verstecken

| | Unterrichtseinheit | UE 01 | DSB |
|---|---|---|---|
| | ✓ Hacker ohne Spuren<br>✓ Zugang zum Internet<br>✓ Anonyme Internetzugänge<br>✓ Internetzugänge: Sagen und Legenden<br>✓ Anonymität durch Verschleierung<br>✓ Channel<br>▪ VPN<br>▪ Proxy Server<br>▪ Tunneling mit Spezialprotokollen<br>✓ TOR-Netzwerk<br>▪ Funktionsweise<br>▪ Verbindungsaufbau<br>▪ Datenübertragung<br>▪ Facts<br>✓ Tor-Wächter: Entry Guards<br>✓ Tor-Exit-Nodes<br>✓ Wo legen Hacker Daten ab? | | |

## Windows Event Logs

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | ✓ Grundsätzliches<br>✓ Qual der Wahl<br>✓ Lösungsansatz: GRAYLOG<br>✓ Installation<br>✓ Business Chance<br>✓ Andere Logs<br>✓ WinLogBeat Installation: Windows<br>✓ Konfiguration & Start<br>✓ Alternative: Cloud ELK Stacks<br>✓ Informationen und Demos | | |

## ZERO DAY: Log4J/Log4Shell

| | Unterrichtseinheit | UE 01 | SAD |
|---|---|---|---|
| | ✓ Überblick<br>✓ Was kann passieren?<br>✓ Beschaffenheit der Sicherheitslücke<br>✓ Problematik<br>✓ Manuel Testen<br>✓ Patchen<br>✓ Erkennung<br>✓ Maßnahmen | | |

# Weitere wichtige Informationen

## Sie haben Fragen oder Anregungen?

Falls Sie Fragen, Wünsche oder Anregungen zu dieser oder zu anderen Ausbildungen haben, stehen wir Ihnen montags bis donnerstags in der Zeit von 08:00 – 17:00 Uhr und freitags von 08:00 – 13:00 Uhr sehr gerne zur Verfügung.

Sie erreichen uns unter:

Telefon: 09526 95 000 60
E-Mail: info@ITKservice.NET

Ihre Ansprechpartner für das ITKwebcollege.SECURITY

Christoph Holzheid
Anne Hirschlein
Sylvia Sonntag
Thomas Wölfel

## Copyrights und Vertragsbedingungen



## Kontaktdaten | Impressum

ITKservice GmbH & Co. KG
Fuchsstädter Weg 2
97491 Aidhausen

Telefon: 09526 95 000 60
Telefax: 09526 95 000 63

www: ITKservice.NET
E-Mail: info@ITKservice.NET

Sitz der Gesellschaft: Aidhausen | Amtsgericht Bamberg, HRA 11009, Ust-Id: DE 262 344 410 | Vertreten durch: Thomas Wölfel (GF).

Bildnachweise: Alle in diesem Dokument dargestellten Bilder wurden von der ITKservice GmbH & Co. KG bei ccvision.de lizensiert.
Redaktion: ITKservice GmbH & Co. KG | Copyright © 2017 ITKservice GmbH & Co. KG.