

ITKwebcollege.Security Advanced Trainings

Online-Trainings für Security-Consultants oder Security-Experten | Stand Juli 2019



Ausbildungsinhalte

Inhaltsverzeichnis

Security Advanced Trainings	3
Analyse von Logfiles und SIEM	3
Backdoors, Angriffsmethoden und Erkennung	3
Docker für IT-Security Spezialisten	3
E-Mail Spoofing & Spearphishing	4
Emotet is back	4
Empire Framework	4
Empire Framework & Deathstar	5
Erpressungstrojaner oder Kryptotrojaner (Ransomware)	5
Früherkennung von Cyberangriffe	5
Hacker's Diary - Dedicated Malware Attack	5
Hacker's Diary - Unerkannt bleiben	6
Hacking und IT-Security	6
Handwerkszeug für Securityspezialisten	6
IDS-System: Wirksamer Schutz?	7
Infrastruktur und Demilitarisierte Zone (DMZ)	7
IT-Forensic	7
KALI2018: Web Hacking Tools im Überblick	8
Meltdown & Spectre (und) Memory Attacks	8
Meltdown/Spectre – Stand Dezember 2018	8
Malware & Viren	9
Network Security Monitoring (NSM)	9
OpenVAS – Schwachstellenscanner	9
Opfer eines Hackerangriffs	9
Pentesting 2019	10
Raspberry Pi/Hacking Devices	10
Security Onion 2018	10
Social Engineering	11
Spectre Update + Alarmstufe Rot	11
The Golden Ticket	11
Vulnerability Scanner und deren Anwendungen	12
Waffen der Hacker: SQL Injection	12
Webservice und –server	12
Wie sicher ist Festplattenverschlüsselung?	13
Wie sich Hacker im Internet verstecken	13
Weitere wichtige Informationen	14
Sie haben Fragen oder Anregungen?	14
Copyrights und Vertragsbedingungen	14
Kontaktdaten Impressum	14

Security Advanced Trainings

Analyse von Logfiles und SIEM

Unterrichtseinheit	UE 01	SAD
<ul style="list-style-type: none">✓ Analyse von Logfiles und SIEM✓ Bedarfsanalyse<ul style="list-style-type: none">▪ Beispiel: Website✓ Kritikalität<ul style="list-style-type: none">▪ Beispiel: Website✓ Mindestanforderungen<ul style="list-style-type: none">▪ Beispiel: Website✓ Zählen reicht nicht aus?✓ Automatismen schaffen✓ Schnelles Security Monitoring mit OMD✓ OMD CheckMK<ul style="list-style-type: none">▪ Installation und Einsatz▪ Maßgeschneidert✓ Logfile Analyse durch SIEM und Co✓ Harte Fakten✓ Dienstleistung & Services		

Backdoors, Angriffsmethoden und Erkennung

Unterrichtseinheit	UE 01	SAD
<ul style="list-style-type: none">Backdoors, Angriffsmethoden und Erkennung✓ Backdoor<ul style="list-style-type: none">▪ Funktionsweise▪ Implementierung✓ Häufige Backdoor/Angriff: DRIDEX✓ Analyse von DRIDEX im Detail✓ Tools zur Erkennung von Backdoors✓ TCPView zur Prozessanalyse✓ Alternative zur AV Erkennung: CyLance✓ Erkennung über NSM Systeme✓ Analyse per NSM✓ Analyse per Network Flow Auswertung✓ Kampf gegen Backdoors		

Docker für IT-Security Spezialisten

Unterrichtseinheit	UE 01	SAD
<ul style="list-style-type: none">Docker für IT-Security Spezialisten✓ Docker für IT-Sicherheitsexperten✓ Docker Basics✓ Docker lernen✓ Docker Plattformen✓ Beispiel – Nessus Essentials✓ Dockerfile für Nessus erstellen✓ Build für Docker Nessus✓ Nessus: Image starten und testen✓ Docker Volumen: Persistenz für Container✓ Beispiel – OpenVAS für Docker✓ Beispiel – Verbesserter TOR Proxy		

E-Mail Spoofing & Spearphishing

Unterrichtseinheit	UE 01	SAD
Spearphishing Angriffe per E-Mail <ul style="list-style-type: none"> ✓ Beispiel ✓ Wie Angreifer professionelle E-Mails erzeugen ✓ Professionelle E-Mails mit Atomic Studio ✓ Stichwort: Proxy Server ✓ Verifikation von E-Mail Adressen ✓ Erstellen von professionellen E-Mails 		

Emotet is back

Unterrichtseinheit	UE 01	SAD
Emotet is back <ul style="list-style-type: none"> ✓ Bit Paymer <ul style="list-style-type: none"> ▪ 2017 ▪ 2018 ✓ Angriffsrekonstruktion ✓ TRICKBOT <ul style="list-style-type: none"> ▪ Kommunikation ▪ Hits ✓ Emotet vs. AV ✓ Ziel des Angreifers ✓ Angriff früh erkennen ✓ Problematik <ul style="list-style-type: none"> ▪ NSM – Port Mirroring ✓ Blocklisten 		

Empire Framework

Unterrichtseinheit	UE 01	SAD
Empire Framework <ul style="list-style-type: none"> ✓ Profitool für Domainhacker ✓ Empire Framework für Ubuntu 16.04 ✓ Installation von Empire ✓ Erste Schritte: Listener erstellen ✓ Listener von außen betrachtet ✓ Stager im Überblick ✓ Word Macro Stager als Beispiel ✓ Self Hacking ✓ Alternative zum Stager: Launcher ✓ Powershell Payload ✓ UAC Bypass gegen Up2Date Windows 10 ✓ Domain mit Empire hacken 		

Unterrichtseinheit	UE 02	SAD
Empire Framework <ul style="list-style-type: none"> ✓ Profitool für Domainhacker ✓ Empire Framework für Ubuntu 16.04 ✓ Angriffe gegen Windows Domäne ✓ Microsoft LAPS ✓ Effekt eines Angriffs ✓ Mit Verlusten muss gerechnet werden ...? ✓ Weitere sichere Domain Konfigurationen ...? ✓ Wieso Fails? 		

Empire Framework & Deathstar

Unterrichtseinheit	UE 01	SAD
Empire Framework & Deathstar ✓ Auszug Manila Hacking Days 2018 ✓ Empire Framework <ul style="list-style-type: none"> ▪ Überblick ✓ Domain Security in a Nutshell ✓ UAC-Bypass: Klassisches Szenario ✓ Memory Access ist kritisch? ✓ Ideale Lösung: Microsoft LAPS ✓ Und der Domain Administrator? ✓ Vorsicht bei Server Admin Accounts ✓ Deathstar spart Zeit: Angriff los! ✓ Testszenario ✓ Fazit: Deathstar/Empire testen		

Erpressungstrojaner oder Kryptotrojaner (Ransomware)

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

Früherkennung von Cyberangriffe

Unterrichtseinheit	UE 01	SAD
Früherkennung von Cyberangriffen ✓ Erkennen Sie Angriffe rechtzeitig oder erst nach dem Datenabfluss? ✓ Ausprägung von Cyberangriffen ✓ Scanning der Unternehmensnetzwerke ✓ Effiziente Erkennung <ul style="list-style-type: none"> ▪ Log File Analyse/SIEM ▪ Network Security Monitoring 		

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 - Unerkannt bleiben

Unterrichtseinheit	UE 01	SAD
<p>Überblick: Methoden zur Tarnung</p> <ul style="list-style-type: none"> ✓ Anonyme Netzwerke <ul style="list-style-type: none"> ▪ Öffentliche Zugänge ▪ Erkennungsmerkmale <ul style="list-style-type: none"> ▪ 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
<p>Aktuelle Angriffsszenarien</p> <ul style="list-style-type: none"> ✓ Angriffe im Überblick <ul style="list-style-type: none"> ▪ Kryptotrojaner (Ransomware) ▪ SEO Fraud ▪ Zielgerichtete Attacken ✓ Dienstleistungen im Überblick <ul style="list-style-type: none"> ▪ Penetrationstesting ▪ Forensische Analysen ▪ NSM Analysen <p>Ransomware</p> <ul style="list-style-type: none"> ✓ Ransomware 2016 ✓ Ransomware in Zahlen ✓ Sofortmaßnahmen ✓ Sofortmaßnahmen/Kalkulation ✓ Prophylaxe 	<p>SEO Fraud</p> <ul style="list-style-type: none"> ✓ 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
<p>Handwerkszeug für Securityspezialisten</p> <ul style="list-style-type: none"> ✓ Thema: Laptops ✓ Lösung zum Laptop Dilemma: APU2 <ul style="list-style-type: none"> ▪ 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
<ul style="list-style-type: none"> IDS-System ✓ Rollout der Ransomware ✓ Neue Infektion ✓ Funktionsweise ✓ Snort <ul style="list-style-type: none"> ▪ Historie ✓ Subscription Rulesets <ul style="list-style-type: none"> ▪ Überblick ▪ Vorteile ✓ Emerging Thread (ET) <ul style="list-style-type: none"> ▪ Open Rulesets ▪ Daily Updates ✓ Snort Rule Beispiele ✓ Maleware Zeus ✓ Security Onion und Snort Rules ✓ Bro <ul style="list-style-type: none"> ▪ Übersicht ▪ In der Praxis 		

Infrastruktur und Demilitarisierte Zone (DMZ)

Unterrichtseinheit	UE 01	SAD
<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> IT Forensic ✓ Geschichte der Computer Forensic ✓ Erfolge der Computer Forensic ✓ Unterstützende Gesetze ✓ Forensic im Internet ✓ Forensic Tools <ul style="list-style-type: none"> ▪ OSForensics ▪ Volatility ▪ DEFT Linux ✓ Beispiel Projekt <ul style="list-style-type: none"> ▪ CFREDS ✓ Umsetzung in Phase ✓ Forensische Analyse ✓ Forensische Berichterstattung 		

KALI2018: Web Hacking Tools im Überblick

Unterrichtseinheit	UE 01	SAD
<p>KALI2018</p> <ul style="list-style-type: none">✓ KALI Linux 2018 Edition✓ Grundsätzliches: KALI vs. Windows✓ DAMN VULNERABLY WEB APPLICATION (DVWA)✓ KALIs Web Security Scanner<ul style="list-style-type: none">▪ OWASP ZAP▪ BURP Suite✓ Effektive Web Angriffe mit KALI✓ Effektives Verstecken von Web Angriffen		

Meltdown & Spectre (und) Memory Attacks

Unterrichtseinheit	UE 01	SAD
<p>Meltdown/Spectre/Memory Attacks</p> <ul style="list-style-type: none">✓ Meltdown<ul style="list-style-type: none">▪ Angriff▪ Beschreibung▪ Vorführung▪ Bedrohungspotential✓ Spectre<ul style="list-style-type: none">▪ Angriff▪ Beschreibung▪ Angriffsmethoden▪ Bedrohungspotential✓ Chance für Dienstleister		

Meltdown/Spectre – Stand Dezember 2018

Unterrichtseinheit	UE 01	SAD
<p>Meltdown/Spectre</p> <ul style="list-style-type: none">✓ Was ist eigentlich Meltdown?<ul style="list-style-type: none">▪ Kurz und bündig▪ Ausführlich✓ Was ist eigentlich Spectre?<ul style="list-style-type: none">▪ Kurz und bündig▪ Ausführlich✓ Bisherige Varianten✓ Neue Varianten✓ Spectre-NG im Überblick✓ NetSpectre✓ Foreshadow✓ Meltdown/Spectre prüfen✓ Gegenmaßnahmen		

Malware & Viren

Unterrichtseinheit	UE 01	SAD
<p>Ursprung, Funktion & Bekämpfung</p> <ul style="list-style-type: none"> ✓ Kurze Historie der Malware ✓ Quellen moderner Malware <ul style="list-style-type: none"> ▪ Verbreitungskanal: E-Mail ▪ Verbreitungskanal: Exploit Kit ✓ Angebote für Malware <ul style="list-style-type: none"> ▪ Darknet Börsen: AlphaBay Market ✓ Funktionen moderner Malware <ul style="list-style-type: none"> ▪ Ransomware ▪ Keylogger ▪ Trojans ✓ Abwehrverfahren im Überblick <ul style="list-style-type: none"> ▪ Anti Malware Lösungen ▪ Network Security Monitoring ▪ Generelle Abwehrmethoden 	<p>Ursprung, Funktion & Bekämpfung</p> <ul style="list-style-type: none"> ✓ 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 	

Network Security Monitoring (NSM)

Unterrichtseinheit	UE 01	SAD
<p>Security Onion</p> <ul style="list-style-type: none"> ✓ Historie ✓ Primäre Tools in Security Onion ✓ Snort ✓ Xplico/Netminer ✓ Sguil/Squert ✓ ELSA/Bro ✓ Argus/RA <p>Snort</p> <ul style="list-style-type: none"> ✓ Historie ✓ Emerging Thread (ET) Rules für Snort ✓ Emerging Thread (ET) Daily Updates ✓ Snort Rule Beispiel: Malware Zeus (Community) ✓ Snort Rules und Alerts 	<p>Sguil</p> <ul style="list-style-type: none"> ✓ Übersicht ✓ Herzstück der Security Onion ✓ Passive Real-time Asset Detection System (PRADS) ✓ Schlüsselfunktionen ✓ Mächtiges Werkzeug <p>SQUERT</p> <ul style="list-style-type: none"> ✓ NIDS/HIDS Event Konsole <p>Bro</p> <ul style="list-style-type: none"> ✓ Übersicht 	

OpenVAS – Schwachstellenscanner

Unterrichtseinheit	UE 01	SAD
<ul style="list-style-type: none"> ✓ Überblick ✓ Installation unter KALLI Linux ✓ Community Edition ✓ Ein erster Scan per Wizard ✓ Scans im Detail Konfigurieren ✓ Wiederkehrende Scans festlegen ✓ Simple Target: Metasploitable v2 ✓ Metasploitable – Auswertung der Ergebnisse 		

Opfer eines Hackerangriffs

Unterrichtseinheit	UE 01	SAD
<p>Erkennung des Angriffes</p> <ul style="list-style-type: none"> ✓ Abfluss von Unternehmensdaten ✓ Forderungen/Erpressung ✓ Technische Erkennung ✓ Technische Auffälligkeiten/Anomalien <p>Abfluss von Unternehmensinformationen</p> <p>Forderung und Erpressung</p> <p>Technische Erkennung</p> <ul style="list-style-type: none"> ✓ Analyse über Security Devices <p>Technische Auffälligkeiten/Anomalien</p> <ul style="list-style-type: none"> ✓ Ungewöhnliches Anwendungs-/PC-Verhalten 	<p>Wie tief ist der Angreifer eingedrungen</p> <ul style="list-style-type: none"> ✓ Initial Analyse ✓ Erstanalyse <p>Lassen sich die Angreifer lokalisieren</p> <ul style="list-style-type: none"> ✓ Grundsätzliches <p>Welche Systeme sind betroffen</p> <ul style="list-style-type: none"> ✓ Grundsätzliches Vorgehen <p>Fließen Unternehmensinformationen ab</p>	

Pentesting 2019

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

Raspberry Pi/Hacking Devices

Unterrichtseinheit	UE 01	SAD
✓ Raspberry Pi und Hacking Devices ✓ Hacker im Taschenformat gefällig? ✓ Zwerge und Riesen ✓ Aufgaben einer Hacking Device ✓ Störung des Betriebsablaufs ✓ Aufbau einer einfachen Hacking Device ✓ Bestückung eines Raspberry Pi 3 ✓ Betriebssysteme für Raspberry Pi Hacking <ul style="list-style-type: none"> ▪ Basis OS ▪ KALI Linux ✓ Special: Raspberry Pi ohne Steckdose ✓ KALI Linux auf Raspberry installieren ✓ KALI Linux vorbereiten ✓ Konfigurationsdetails ✓ RASPI-CONFIG im Überblick ✓ Raspberry Pi vorbereiten ✓ Zugriff auf das Unternehmensnetzwerk ✓ Vorsicht: Für die echten Hacker		

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		

Social Engineering

Unterrichtseinheit	UE 01	SAD
<ul style="list-style-type: none"> ✓ Meltdown & Spectre ✓ Pre-Meltdown Bemühungen ✓ Das Ergebnis: Meltdown & Spectre ✓ Was ist eigentlich Meltdown? <ul style="list-style-type: none"> ✓ Kurz & bündig ✓ Ausführlich ✓ Was ist eigentlich Spectre? <ul style="list-style-type: none"> ✓ 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
<ul style="list-style-type: none"> ✓ Was ist Social Engineering? ✓ Grundsätzliche Arten des Social Engineering <ul style="list-style-type: none"> ✓ Human Based <ul style="list-style-type: none"> ▪ Impersonation ▪ Posing as important User ▪ Being a third party ▪ Desktop Support ▪ Shoulder Surfing ▪ Dumpster Diving ✓ Computer Based <ul style="list-style-type: none"> ▪ Phishing ▪ Spear Phishing ▪ Baiting <ul style="list-style-type: none"> • Special USB Hacking • Website Beispiel ✓ Online Scam 		

The Golden Ticket

Unterrichtseinheit	UE 01	SAD
<ul style="list-style-type: none"> ✓ 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 		

Vulnerability Scanner und deren Anwendungen

Unterrichtseinheit	UE 01	SAD
<p>Vulnerability Scanner und deren Anwendungen</p> <ul style="list-style-type: none"> ✓ Was ist eine Schwachstelle? ✓ Aufspüren einer Schwachstelle ✓ Vulnerability Scanner Grundfunktionen ✓ Verfügbare Scanner <ul style="list-style-type: none"> ✓ Open Source <ul style="list-style-type: none"> • OpenVAS ✓ Kommerzielle <ul style="list-style-type: none"> • Tenable Nessus • Rapid7 Nexpose • Qualys • Goolge: Vulnerability Scanner • Metasploitable 		

Waffen der Hacker: SQL Injection

Unterrichtseinheit	UE 01	SAD
<ul style="list-style-type: none"> ✓ SQL Injection (SQLi) Erkennen und Abwehren <ul style="list-style-type: none"> ✓ SQL Injection <ul style="list-style-type: none"> ▪ Gefahren ▪ Grundlagen ✓ Betroffene Programmiersprachen ✓ SQL Injection in der Praxis ✓ Angriffstool: SQLMAP ✓ Erfolgreiche Angriffe ✓ Log goes SIEM? ✓ Streams vs. SQL Injection ✓ Einfachere Abwehrmethoden ✓ Effizienteste Abwehr: Gute Programmierung 		

Webservice und -server

Unterrichtseinheit	UE 01	SAD
<p>Angriffe gegen Webanwendungen</p> <p>Immunsisierung gegen Strafverfolgung</p> <p>Angriffertypen (Web Attacken)</p> <p>Abhärtung gegen Angriffe</p> <p>Grundregeln</p> <ul style="list-style-type: none"> ✓ Szenario 1 <p>Schlechtes Beispiel</p> <ul style="list-style-type: none"> ✓ Szenario 2 <p>Gutes Beispiel</p> <p>Abhärtung gegen Angriffe: Hardening</p>	<p>Abhärtung von Apache Webserver</p> <p>Überprüfung der SSL/TLS Einstellung</p> <p>OWASP</p> <ul style="list-style-type: none"> ✓ All About Web Security ✓ A1 – SQL Injection im Detail & Tools ✓ A3 – Cross Site Scripting <p>Universelle Web Security Scanner</p> <p>Spitze des Eisbergs</p>	

Wie sicher ist Festplattenverschlüsselung?

Unterrichtseinheit	UE 01	SAD
<ul style="list-style-type: none">✓ Bitlocker und Co.✓ Der Bootprozess<ul style="list-style-type: none">▪ Größte Schwachstellen▪ Secure Boot▪ Normale Boot Prozess▪ Fazit✓ Was hat das mit Bitlocker und Co. zu tun?✓ Wie lässt sich Bitlocker angreifen?✓ Angriffsszenario✓ Kommerzielle Tools für Key Extraaktion✓ Master Key im Einsatz✓ Wie kriegt man Bitlocker sicher?✓ Welche Verschlüsseler sind angreifbar?✓ Veracrypt		

Wie sich Hacker im Internet verstecken

Unterrichtseinheit	UE 01	DSB
<ul style="list-style-type: none">✓ Hacker ohne Spuren✓ Zugang zum Internet✓ Anonyme Internetzugänge✓ Internetzugänge: Sagen und Legenden✓ Anonymität durch Verschleierung✓ Channel<ul style="list-style-type: none">▪ VPN▪ Proxy Server▪ Tunneling mit Spezialprotokollen✓ TOR-Netzwerk<ul style="list-style-type: none">▪ Funktionsweise▪ Verbindungsaufbau▪ Datenübertragung<ul style="list-style-type: none">▪ Facts✓ Tor-Wächter: Entry Guards✓ Tor-Exit-Nodes✓ Wo legen Hacker Daten ab?		

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 – 15:00 Uhr sehr gerne zur Verfügung.

Sie erreichen uns unter:

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

Ihre Ansprechpartner für das ITKwebcollege.ADMIN

Christoph Holzheid
Anne Hirschlein
Sylvia Sonntag
Thomas Wölfel



Copyrights und Vertragsbedingungen

Das Copyright © aller Trainings, inkl. aller Aufzeichnungen und Unterlagen obliegt der ITKservice GmbH & Co. KG. Die Nutzung aller ITKwebcollege-Leistungen ist nur für den Vertragspartner und nur für den internen Gebrauch gestattet. Eine Weitergabe der Leistungen an Dritte ist nicht zulässig.

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 lizenziert.

Redaktion: ITKservice GmbH & Co. KG | Copyright © 2017 ITKservice GmbH & Co. KG.