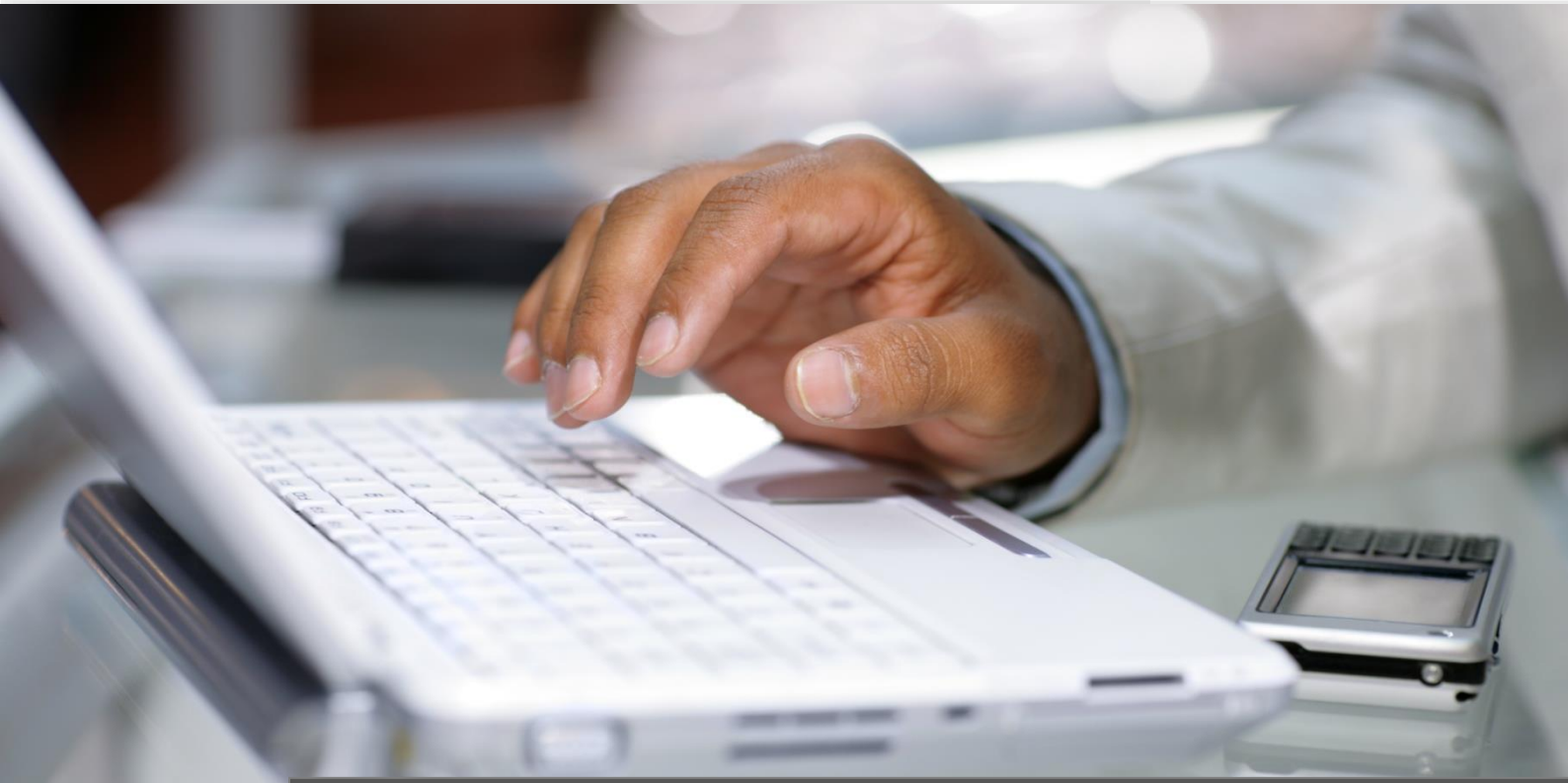
ITKwebcollege.Security

Advanced Trainings

Online-Trainings für Security-Consultants/Security-Experten | Stand März 2022



Ausbildungsinhalte

ITKservice

Inhaltsverzeichnis

Security Advanced Trainings

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		

Backdoors, Angriffsmethoden und Erkennung

Unterrichtseinheit	UE 01	SAD

Backdoors, Angriffsmethoden und Erkennung
- ✓ Backdoor
  - 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

Balena Cloud und IT-Security am Beispiel von Nessus

Unterrichtseinheit	UE 01	SAD

Balena Cloud und IT-Security am Beispiel von Nessus
- ✓ Balena Cloud im Überblick
- ✓ Balena und Security Appliances, Gründe
- ✓ Meine NSM/Balena
- ✓ Nessus für Balena Device
- ✓ Balena App erstellen
- ✓ Download des Image File
- ✓ Image auf NUC installieren
- ✓ 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		

Dark Hacker – Wie funktioniert das?

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

Docker für IT-Security Spezialisten

Unterrichtseinheit	UE 01	SAD
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		

Elastic Cloud SIEM im Eigenbau

Unterrichtseinheit	UE 01	SAD
Elastic Cloud SIEM im Eigenbau ✓ SIEM aus Elastic Cloud ✓ Aufbau als praktische Live Demo		

E-Mail Spoofing & Spearphishing

Unterrichtseinheit	UE 01	SAD
Spearphishing Angriffe per E-Mail ✓ 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
- ✓ Bit Paymer
  - 2017
  - 2018
- ✓ Angriffsrekonstruktion
- ✓ TRICKBOT
  - Kommunikation
  - Hits
- ✓ Emotet vs. AV
- ✓ Ziel des Angreifers
- ✓ Angriff früh erkennen
- ✓ Problematik
  - NSM – Port Mirroring
- ✓ Blocklisten

Empire 3 (BC Security) und CrackMapExec

Unterrichtseinheit	UE 01	SAD

Empire 3 (BC Security) und CrackMapExec
- ✓ Empire Framework 3
- ✓ AD Hacking Umgebung
- ✓ AD Analyse mit PingCastle
- ✓ Angriff gegen Domäne
- ✓ CrackMapExec (CME)
- ✓ Kombinationen

Empire Framework

Unterrichtseinheit	UE 01	SAD

Empire Framework
- ✓ 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
- ✓ 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 ▪ 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		

Erkennung von LOG4J Sicherheitslücken

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

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?		

Exchange Hack – Maßnahmen

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

Forensische Erfassung von RAID Laufwerken

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

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 ▪ Log File Analyse/SIEM ▪ Network Security Monitoring		

Früherkennung von Cyberangriffe

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

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

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
- ✓ Angriffscheck per E-Mail
- ✓ Check der Angreifbarkeit (E-Mail)
- ✓ Firewall- INTERN -> EXTERN
- ✓ Domain Security Checks

Pentest mit NSM aufwerten

Unterrichtseinheit	UE 01	SAD

Pentest mit NSM aufwerten
- ✓ Alleinstellungsmerkmal
- ✓ Network Security Monitoring (NSM)
- ✓ Anforderungen an NSM-Pentest-Systeme
- ✓ Ideale Hardware: APU4
- ✓ Vorbereitungen
- ✓ NSM Komponenten für APU4
- ✓ Shortcuts für die Installation
- ✓ Probe aufs Example

Pentest Server in der Cloud erstellen

Unterrichtseinheit	UE 01	SAD

Pentest Server in der Cloud erstellen
- ✓ MS Exchange Sicherheitslücke
- ✓ Pentest Server in der Cloud – die Vorteile
- ✓ Welches Betriebssystem?
- ✓ Pentest Server: Windows 10
- ✓ Tools
  - Nessus
  - TOR
  - Proxifier
  - TOR Browser
  - BurpSuite
  - ScrapeBox

  KALI Linux

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

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 ▪ 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 Logs nach ELK

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

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		

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		

Waffen der Hacker: SQL Injection

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

Wie funktioniert ein RAT?

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

Wie sicher ist Festplattenverschlüsselung?

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

Windows Event Logs

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

ZERO DAY: Log4J/Log4Shell

	Unterrichtseinheit	UE 01	SAD
	✓ Überblick ✓ Was kann passieren? ✓ Beschaffenheit der Sicherheitslücke ✓ Problematik ✓ Manuel Testen ✓ Patchen ✓ Erkennung ✓ 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.ADMIN

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.