THE PENTEST EXPERTS

WWW.SYSS.DE

SySS GmbH Tübingen Germany +49 (0)7071 - 40 78 56-0 schulung@syss.de

THE PENTEST EXPERTS.

HACKING & SECURITY 2020

SICHERHEIT TRAINIEREN – KOMPETENZEN AUSBAUEN

SEBASTIAN SCHREIBER
GESCHÄFTSFÜHRER

EIN WORT VORWEG

IT-Systeme und Anwendungssoftware entwickeln sich kontinuierlich weiter. Entsprechend feilen auch Hacker stetig an ihren Fertigkeiten, um neue Software und Hardware anzugreifen. Meine IT Security Consultants und ich nehmen die hieraus entstehenden Herausforderungen immer wieder aufs Neue an. Seit über 20 Jahren bauen wir unser Wissen und unsere Erfahrung stetig aus. So sind und bleiben wir ein verlässlicher Partner, der Ihnen Wissen rund um IT-Sicherheit und Hacking vermittelt und Sie vor unliebsamen Eindringlingen schützt.

Angesichts der immer größer werdenden Bedeutung des Internet of Things gibt es heutzutage weitreichende Möglichkeiten, die unterschiedlichsten Geräte miteinander zu verbinden und über das Internet zu steuern. Dies eröffnet Angreifern zahlreiche Wege, Systeme zu kompromittieren. Zu diesem Thema haben wir eine anschauliche und praxisnahe Schulung entwickelt, mit der Sie Hardware-Hacking lernen und erleben: „Hack9: Embedded Security" wird unterschiedliche Angriffsmöglichkeiten beleuchten und Ihnen Hilfestellung geben, wie Sie Ihre Embedded Devices sichern können.

Mein Team und ich freuen uns, Sie dabei zu unterstützen, Ihre IT-Sicherheit zu steigern.
Wünschen Sie darüber hinaus eine Beratung? Wir stehen Ihnen jederzeit zur Verfügung.

Herzliche Grüße, Ihr Sebastian Schreiber

P.S.: Profitieren Sie auch von unseren Newslettern „SySS Management News" und „SySS Research News", die Sie regelmäßig mit IT-Sicherheits-Know-how und Security Advisories auf dem Laufenden halten. Der nebenstehende QR-Code bringt Sie direkt zur Anmeldeseite.

Wir, die SySS GmbH, sind ein Unternehmen für IT-Sicherheit, spezialisiert auf Penetrationstests.

Seit der Gründung 1998 durch unseren Geschäftsführer Sebastian Schreiber führen wir hochwertige Sicherheitstests durch. Bei unserer Arbeit verbinden wir hohen technischen Anspruch mit der von uns entwickelten Ethik für Penetrationstester.

INHALT

HACK1/HACK2: HACKING WORKSHOP TEIL 1 & 2

Referenten: Michael Großmann, Marcel Mangold

Computermissbrauch und Cyberkriminalität bedrohen IT-Netze tagtäglich. Meist geschehen sie sehr unauffällig und werden erst bemerkt, wenn der Schadensfall schon eingetreten ist. Somit sind sie eine ernst zu nehmende Bedrohung. Damit Unternehmen ihre IT-Umgebung vor Gefahren dieser Art besser schützen können, haben wir die Workshops Hack1 und Hack2 entwickelt. Wir betrachten das Thema IT-Sicherheit aus der Perspektive eines Täters bzw. „Hackers", was dabei helfen soll, Netzwerke im eigenen Verantwortungsbereich besser abzusichern. Beide Workshops können unabhängig voneinander besucht werden, jedoch baut Workshop 2 auf Workshop 1 auf.

WORKSHOP 1

Themen

- Informationsquellen
  - Identifikation erreichbarer Systeme; Suche nach Hinweisen auf potenzielle Angriffsziele
- Standard-Sicherheitswerkzeuge und ihr Einsatz
  - Portscanner, Sniffer
- Man-in-the-Middle-Angriffe
  - Vor allem in lokalen Netzen können Man-in-the-Middle-Angriffe verwendet werden, um verschlüsselten Datenverkehr oder auch VoIP-Telefonate mitzulesen bzw. mitzuhören. Im Rahmen des Workshops werden Angriffsszenarien durchgeführt und Schutzmechanismen besprochen.
- Passwortsicherheit unter Linux, Windows und in Windows-Netzen
  - Anhand verschiedener Cracking-Techniken schätzen wir die Sicherheit ein, die eine Passwortrichtlinie bietet.
- Ausnutzen von Sicherheitslücken
  - Vorgehensweise eines Angreifers bei der Ausnutzung von Schwachstellen (Verwendung von Exploits, Trojanisierung des Zielsystems)

WORKSHOP 1
Techn. Voraussetzungen: Grundkenntnisse über Betriebssysteme, Netzwerke, Linux, Windows, TCP/IP
Termine: 04.-05.02.2020 / 21.-22.04.2020 / 16.-17.06.2020 / 22.-23.09.2020 / 17.-18.11.2020 (2 Tage)
Preis: € 1500,00*

WORKSHOP 2
Techn. Voraussetzungen: Grundkenntnisse über Betriebssysteme, Netzwerke, Linux, Windows, TCP/IP
Termine: 06.-07.02.2020 / 23.-24.04.2020 / 18.-19.06.2020 / 24.-25.09.2020 / 19.-20.11.2020 (2 Tage)
Preis: € 1500,00*

WORKSHOP 2

Themen

- Metasploit Framework
  - Einführung und Umgang mit unterschiedlichen Modulen
- Sicherheit in Windows-Netzen
  - Eskalation von Benutzerrechten auf lokalen Windows-Systemen sowie im Windows-Netzwerk bis hin zur Berechtigung eines Domänenadministrators
  - Verständnis von typischen Vorgehensweisen wie Pass-the-Hash
  - Extraktion von Klartextpasswörtern und Übernahme von Benutzersitzungen
- Schwachstellenscanner
  - Funktionsweise, Konfiguration und Umgang mit einem Schwachstellenscanner
- Tunneling
  - Verwendung harmloser Protokolle zur verdeckten Übertragung von Daten
  - Umlenken von Netzwerkverkehr über kompromittierte Systeme, um Firewalls zu umgehen oder Remotezugriff zu erlangen.

* Für weitere Details: siehe Seite 20

HACK3: ANGRIFFE AUF WINDOWS-BASIERTE NETZWERKE

Referenten: Daniel Isern, Franz Jahn, Dr. Adrian Vollmer, Wolfgang Zejda

Zur technischen Organisation von Computern, Benutzern, Gruppen und weiteren Objektklassen wird in Unternehmensnetzwerken in der Regel auf einen Verzeichnisdienst zurückgegriffen. Weit verbreitet sind in Windows-basierten Netzwerken die auf dem Domänen-Vertrauensprinzip basierenden Active Directory Domain Services. Gelingt es einem Angreifer, initial von außen in das interne Netzwerk einzudringen, so kann er innerhalb dieses Verzeichnisdienstes seine Rechte meist mit überschaubarem Aufwand ausweiten. In dieser Schulung sollen ein tieferer Einblick in die Vorgehensweise von Angreifern gewährt und Gegenmaßnahmen aufgezeigt werden. Theoretische Konzepte werden erläutert und Angriffsvektoren anhand von „Hands-on-Übungen" praktisch erprobt.

Themen

- Windows-basierte Netzwerke
  - Active Directory, Domain-Controller
  - Struktur- und Trust-Ermittlung einer Active Directory-Umgebung
  - Berechtigungs- und Authentifizierungskonzepte
  - Hash-Typen in der Microsoft-Welt
  - Windows-Anmeldeprozess
- Angriffe auf Einzelsysteme und Netzwerkprotokolle
  - Ausnutzung von Schwachstellen
  - Angriffe gegen Authentisierungsmechanismen
  - Ausnutzung schwacher Dienstekonfigurationen
  - Angriffe gegen Kerberos (z. B. Golden Ticket)
  - Traffic-basierte Angriffe (NBNS, MitM)
- Rechteausweitung/Ausbreitung
  - Mangelhafter Passwortschutz
  - Ausnutzung von „Features", „Spuren"
  - Access Tokens und „gecachte" Passwörter
  - Pass-the-Hash-Angriffe
  - Security Support Provider
  - Group Policy Objects/Preferences
- Einsatz geeigneter Tools
  - Metasploit Framework
  - Portscanner wie Nmap
  - PowerShell-Tools
  - Cracking-Tools
  - Tools für spezielle Einsatzzwecke
- „Best Practice"-Schutzmaßnahmen
  - Detektionsverfahren
  - IT Security-Prinzipien
  - Konfigurationsempfehlungen

Techn. Voraussetzungen: Grundkenntnisse von Linux- und Windows-basierten Systemen und Netzen
Termine: 17.-19.03.2020 / 21.-23.07.2020 / 29.09.-01.10.2020 / 24.-26.11.2020 (3 Tage)
Preis: € 2250,00

HACK4: ANGRIFFE GEGEN VOIP-INFRASTRUKTUREN

Referenten: Michael Schmidt, Ludwig Stage

Das Protokoll VoIP ist in den letzten Jahren für Unternehmen nicht zuletzt aufgrund langfristiger Kosteneinsparungen bzw. einer einheitlichen Infrastrukturnutzung immer mehr in den Vordergrund gerückt. Mit der Einführung von VoIP beginnt oder erweitert sich auch der Wunsch nach einer strikten Trennung bestimmter Daten im Netzwerk. Diese Trennung wird in der Regel nicht physisch, sondern auf logischer Ebene via VLANs erreicht. Gelingt es einem Angreifer beispielsweise, im internen Netzwerk auf andere VLANs zuzugreifen, so ist er eventuell in der Lage, vertrauliche Gesprächsverbindungen mitzuschneiden oder die eigenen Zugriffsberechtigungen zu erweitern.

Im Rahmen eines zweitägigen Workshops wird die Perspektive eines Angreifers eingenommen. Es werden Verfahren gezeigt, mit denen die oben genannten Ziele erreicht werden können. Der Workshop soll einen tieferen Einblick in die Vorgehensweise von Angreifern geben, damit Teilnehmer bei der Nachbereitung die Risiken im eigenen Netzwerk einschätzen und minimieren können. Theoretische Konzepte werden erläutert und erlernte Angriffsvektoren anhand von „Hands-on-Übungen" praktisch erprobt.

Themen

- Technische Grundlagen
  - Einführung in die Techniken
  - VoIP-Terminologie und -Aufbau
  - Passive und aktive Trafficanalyse
  - VLAN-Terminologie und -Aufbau
- Angriffsverfahren
  - Netzbasierte Angriffe gegen VoIP-Telefone und -Anlagen
  - Angriffe gegen Authentisierungsverfahren
  - Angriffe gegen die Vertraulichkeit von Daten
  - Bootangriffe und weitere physische Trunking-Angriffe
  - Inter-VLAN-Routing
- Schutzmaßnahmen
  - Erkennungsmöglichkeiten
  - IT Security-Prinzipien
  - Konfigurationsempfehlungen

Techn. Voraussetzungen: Grundkenntnisse in Netzwerktechnik
Termine: 24.-25.03.2020 / 15.-16.12.2020 (2 Tage)
Preis: € 1500,00

HACK5: EXPLOIT DEVELOPMENT

Referent: Matthias Deeg

Diese Schulung vermittelt die theoretischen und praktischen Grundlagen der Funktionsweise und der Entwicklung von Exploits. Dabei soll vorrangig betrachtet werden, wie Zielplattformen aufgebaut sind, welche Besonderheiten sie aufweisen, welche verschiedenen Formen der Schwachstellenanalyse existieren, welche Werkzeuge für die Exploit-Entwicklung wichtig sind (Debugger, Disassembler, Exploit Frameworks etc.) und wie diverse Schwachstellentypen ausgenutzt werden können. Ferner geht die zweitägige Schulung noch auf die Fragen ein, welche Möglichkeiten existieren, sich gegen eine Ausnutzung der gezeigten Schwachstellen durch Angreifer zu schützen, und wie Hacker solche Schutzmaßnahmen möglicherweise umgehen können.

Themen

- Besonderheiten verschiedener Zielplattformen
  - Prozessorarchitektur: x86
  - Betriebssysteme: Windows, Unix/Linux
- Verschiedene Formen der Schwachstellenanalyse
  - Statische Codeanalyse
    - » Quellcodeanalyse
    - » Analyse von Binärprogrammen (Reverse Code Engineering)
  - Dynamische Codeanalyse (Laufzeitanalyse)
    - » Verhaltensbasierte Sicherheitsanalyse
    - » Fuzzing
- Tools of the Trade: Wichtige Werkzeuge für die Exploit-Entwicklung
  - Debugger/Disassembler/Exploit-Frameworks/Assembler (x86)
  - Programmiersprache der Wahl (z.B. C/C++, Python, Perl, Ruby etc.)
- Ausnutzung verschiedener Schwachstellentypen
  - Fehler in der Hard- und Softwarearchitektur und Anwendungslogik
  - Fehler in der Datenverarbeitung, z. B.
    - » Buffer Overflow-Schwachstellen (Stack, Heap, Off-By-One)
    - » Format String-Schwachstellen
- Schutzmaßnahmen und Umgehungsmöglichkeiten
  - Stack Cookies
  - SafeSEH
  - Data Execution Prevention (DEP)
  - Address Space Layout Randomization (ASLR)

Techn. Voraussetzungen: Grundkenntnisse über Betriebssysteme und Rechnerarchitektur
Termine: 12.-13.02.2020 / 14.-15.07.2020 (2 Tage)
Preis: € 1500,00

HACK6: MOBILE DEVICE HACKING

Referenten: Philipp Buchegger, Dr. Benjamin Heß

Mobile Devices sind aus dem Unternehmensumfeld nicht mehr wegzudenken und übernehmen schon lange nicht mehr nur die Aufgabe eines Telefons. Mittlerweile ist es weit verbreitet, dass viele Arbeitnehmer auf ihren mobilen Geräten E-Mails bearbeiten, ins Internet gehen und eine große Menge an oftmals vertraulichen Unternehmensdaten bewegen. Diese Konzentration an interessanten Daten macht Mobile Devices für Angreifer sehr attraktiv.

Dieses Seminar richtet sich an Nutzer, die Sicherheitsaspekte von mobilen Endgeräten besser verstehen wollen, beispielsweise für die Integration in die eigene Unternehmensinfrastruktur. Neben der Verwaltung der Geräte werden die kritischen Angriffspunkte beleuchtet. Ferner werden durch „Hands-on-Übungen" verschiedene Schwachstellen analysiert und aufgezeigt, deren theoretische Grundlagen zuvor erarbeitet wurden.

Themen

- Allgemeine Informationen
  - Eigenschaften von Mobile Devices
  - Verwaltung mobiler Endgeräte im Unternehmen
  - Mobile Device Management-Lösungen
- Angriffstechniken
  - Physischer Zugriff auf das Gerät
  - Hardware-Hacks
  - Mitschnitt des Datenverkehrs
  - Man-in-the-Middle-Angriffe
- Apple iOS
  - Sicherheitskonzept von iOS-Geräten
  - Angriffe auf Apps mit einem Proxy
  - Reverse Engineering von Apps
  - Laufzeitmanipulation
- Google Android
  - Sicherheitskonzept von Android
  - Angriffe auf alte und aktuelle Android-Versionen
  - Emulation eines Android-Smartphones
  - Rooting Detection und Zertifikat-Pinning
  - Angriffe auf Services, Content Provider etc.
  - Reverse Engineering von Apps
  - Laufzeitmanipulation

Techn. Voraussetzungen: Grundlagen in Linux
Termine: 18.-19.02.2020 / 26.-27.05.2020 / 13.-14.10.2020 (2 Tage)
Preis: € 1500,00

HACK7: SICHERHEIT UND EINFALLSTORE BEI WEBAPPLIKATIONEN

Referenten: Torsten Lutz, Marcel Mangold

Schwachstellen in Webapplikationen sind für Angreifer besonders attraktiv, denn diese ermöglichen es ihnen in vielen Fällen, vertrauliche Daten zu stehlen oder ins Unternehmensnetzwerk vorzudringen.
Im Rahmen dieses zweitägigen Workshops lernen die Teilnehmer, wie Hacker in Webapplikationen einbrechen und welchen Risiken diese Anwendungen ausgesetzt sein können. Die Schulung zeigt die gängigsten Angriffe in Theorie und Praxis. Ziel ist es, dass die Teilnehmer am Ende des zweiten Schulungstages selbst Angriffe auf eine eigens hierfür erstellte Webapplikation durchführen können.

Themen

- Cross-Site Scripting (XSS)
  - Angriffe auf Sitzungsinformationen, Phishing und Defacing
- Cross-Site Request Forgery (XSRF)
- SQL Injection
- OS Command Injection
- Local/Remote File Inclusion (LFI/RFI)
  - Angriffe auf Server mit eigenem Programmcode
- Sessionmanagement
  - Sessionmanagement kennenlernen
  - Durchführung von Session Hijacking
  - Cookie-Verständnis und Fehlerausnutzung
  - Passwort-Rate-Angriffe
- Cookies
  - Was bei der Generierung und Verwendung von (Session-)Cookies zu beachten ist
- Browsersicherheit
  - Same-Origin Policy
  - Cross-Origin Resource Sharing
- CAPTCHA
  - Erschweren automatisierter Angriffe und Identifikation von Schwächen bei den Schutzmaßnahmen
- Übungen
  - Festigung der Lerninhalte anhand punktueller Übungen zu allen Themen
  - Abschließende eigenständige Analyse einer vollständigen Webapplikation

Techn. Voraussetzungen: Grundkenntnisse in HTML, HTTP und SQL
Termine: 03.-04.03.2020 / 30.06.-01.07.2020 / 15.-16.09.2020 / 01.-02.12.2020 (2 Tage)
Preis: € 1500,00

HACK8: WLAN-HACKING UND WLAN-SECURITY

Referenten: Gerhard Klostermeier, Michael Schmidt

Wireless LAN ist eine äußerst attraktive Technologie. Sie ermöglicht einer Vielzahl von Geräten die kabellose Nutzung des Internets und einen schnellen, unkomplizierten Zugang zum World Wide Web. Im Zuge der Verbreitung entsprechender Geräte nehmen öffentliche Hotspots zu und die zur Verfügung stehende Bandbreite wächst stetig an. Doch wie sicher ist WLAN? Gehen die Entwicklung von WLAN und von entsprechenden Schutzmaßnahmen gegen Missbrauch Hand in Hand?

Themen

- Grundlagen der WLAN-Technologie
  - Standards
  - Begriffe
- Aufbau einer WLAN-Umgebung
  - Unter Linux
- WLAN-Sniffing
  - Ausspähen ungesicherter Drahtlosnetzwerke
- Sicherheitsansätze des 802.11-Standards
  - Betrachtung von Schwächen
  - SSID-/MAC-basierte Filter, WEP
- Erweiterungen des 802.11-Standards
  - WPA, WPA2
- Authentifizierung in 802.11i
  - 802.1x, EAP, PSK
- Schlüsselmanagement in 802.11i
  - Schlüsselhierarchien
  - Handshakes
- Funktionsweise der Verschlüsselungsmechanismen
  - WEP
  - TKIP
  - CCMP
- WLAN-Hacking
  - DoS-Angriffe
  - WEP-Cracking
  - Angriffe gegen WPA/WPA2-PSK
  - Angriffe gegen WPS
  - Angriffe gegen WPA2-Enterprise
  - Evil Twin-Angriffe
  - Angriffsmöglichkeiten gegen Captive Portals
  - Das Smartphone: Ein hilfreiches Werkzeug

Techn. Voraussetzungen: Grundkenntnisse in Netzwerktechnik
Termine: 02.-03.04.2020 / 10.-11.11.2020 (2 Tage)
Preis: € 1500,00

HACK9: EMBEDDED SECURITY

Referenten: Michael Großmann, Gerhard Klostermeier

Im Zeitalter von IoT-Geräten, smarten Autos oder Industriesteuerungen ist das Thema „Embedded Security" nicht mehr wegzudenken. Wenn die Beleuchtung mit dem Handy gesteuert wird, Autos mehr als 100 Computer enthalten und der reibungslose Ablauf der Produktion im Internet geprüft werden kann, tun sich auch für Angreifer viele Wege auf, ein System zu kompromittieren. Nicht zu vernachlässigen sind dabei die IT-Sicherheit der eigentlichen Hardware und die folgenden Fragestellungen: Wurden Debug-Zugänge nach der Produktion geschlossen? Kann ein Angreifer sensible Daten aus dem Speicher auslesen oder gelingt es ihm gar, eigenen Code auf dem Gerät auszuführen?
Was getan werden muss, um solchen Sicherheitsproblemen vorzubeugen, ist schnell zu erkennen, wenn man selbst einmal typische Schwachstellen ausgenutzt hat. Werden Sie daher selbst zum Angreifer und lernen anhand praxisnaher Übungen, wie Embedded Devices angegriffen und abgesichert werden.

Themen

- Allgemeines
  - Grundlagen von Embedded Security
  - Arbeiten am PCB
  - Hardwarekomponenten zuordnen
  - Datenblätter lesen und verstehen
  - Was passiert beim Booten?
  - Dateisysteme für Embedded Devices
- Typische Schnittstellen
  - UART
  - I2C/SPI
  - JTAG/SWD
- Sicheres Booten
  - Absichern von U-Boot
  - Secure Boot
- Daten sicher speichern
  - Interne/Externe Speicher
  - Hardware Security Module (HSM)
- Umgang mit diversen Tools
  - Multimeter
  - Logic Analyzer
  - JTAGulator
  - J-Link
  - Bus Pirate

Techn. Voraussetzungen: Grundlagen im Umgang mit Linux
Termine: 23.-24.06.2020 / 20.-21.10.2020 (2 Tage)
Preis: € 1500,00

SECU1: DIGITALE FORENSIK BEI COMPUTERN UND SMARTPHONES

Referent: Dr. Markus a Campo

Immer wieder sind Firmennetze Ziele für Hackerangriffe und Unternehmen Opfer von Eindringlingen, die sensible Daten ausspähen und diese illegal weiterverwenden. Um in solchen Fällen Klarheit zu erlangen, wird der Angriff forensisch untersucht. Spuren werden identifiziert und (gerichtsverwertbar) gesichert. Die Ergebnisse werden ausgewertet und als Beweismittel aufbereitet. In der Schulung werden grundlegende Fragestellungen der IT-Forensik und angewandte Standardtechniken analysiert und ausprobiert.
Da auf Smartphones sowohl private als auch dienstliche Daten in großer Zahl abgelegt werden, sind auch diese Geräte eine ergiebige Quelle forensischer Untersuchungen. Ein Zugriff auf die Daten ist meist nur eingeschränkt möglich, sodass spezielle Tools zum Einsatz kommen. Die Sicherung und Analyse von Beweismitteln wird anhand praktischer Übungen und Fallbeispielen verdeutlicht.

Themen

- IT-Forensik und Incident Response
- Behandlung von Sicherheitsvorfällen
- Sicherung von Beweisen, lokal und über das Netzwerk
- Sicherstellung der Authentizität von Beweisen, Gerichtsverwertbarkeit
- Forensik-Tools und -Toolkits
- Analyse der erhobenen Daten
  - Werkzeuge unter Windows und Linux
  - Suche nach versteckten Spuren
  - Ermittlung von Ursachen, Schäden und Angriffsszenarien
  - Rückschlussmöglichkeiten auf Ziele und Kenntnisstand des Täters
- Smartphone-Forensik
  - Grundsätzliche Fragestellungen sowie Forensik bei iOS, Android, BlackBerry, Windows Phone
  - Spezielle Werkzeuge für die Smartphone-Forensik
- Verfassen von gerichtskonformen Berichten
- Projektmanagement: IT-Forensik
  - Zusammenarbeit mit Strafverfolgungsbehörden, rechtliche Situation

Techn. Voraussetzungen: Grundkenntnisse über Netzwerke unter Windows, Linux oder Unix
Termine: 05.-07.05.2020 / 03.-05.11.2020 (3 Tage)
Preis: € 2250,00

SECU2: INCIDENT RESPONSE

Referenten: Joscha Hänel, Jürgen Steinel, Dr. Klaus Tichmann

Alle Welt redet von „Cyberwar", Industriespionage und Datenklau. Werden Angriffe bemerkt, ist es wichtig, überlegt und organisiert zu handeln. Der angebotene Workshop bietet eine Handlungsgrundlage, um adäquat auf IT-Sicherheitsvorfälle reagieren zu können.

Themen

- Grundsätzlicher Ablauf Incident Response
  - 5-Phasen-Modell
  - Was geht nur intern? Was ist auslagerbar?
  - Dos and Don'ts (Unbekannte Tools, „Blaming" etc.)
- Vorbereitung: Incident Readiness
  - Grundsätzliche Tools
  - Personelle Vorbereitung
    - » „Know your tools, know your procedures"
  - Organisatorische Vorbereitung
  - Technische Vorbereitung
  - Analyse des bestehenden Netzwerks
    - » „Baselining", Struktur etc.
- Angriffserkennung
  - Arbeitsweise von Hackern
  - Anti-Forensik-Maßnahmen und was man dennoch sieht
  - Warnungen von Dritten
  - IPS, SIEM etc.
- Angriffsanalyse
  - Logdateien und Protokolle
  - Sicherheitstests und Malware-Analyse
  - Identifikation des Angriffsvektors
  - Forensische Untersuchungen vs. Triage: Abwägung individueller Analysemethoden
- Abwehrmaßnahmen und Aufräumen
  - Die Wichtigkeit des Menschen beim Schutz von Systemen
  - Konzentration auf Bordmittel
  - Grenzen von IPS, SIEM, AV und Firewall
- „Lessons Learned" und organisatorische Strukturen
- Angriffsmuster und Analyse beispielhafter Angriffe
  - „Kenne Deinen Feind"
  - Phishing und klassische Internetkriminalität
  - Ausforschung und gezielte Angriffe
  - OpSec und das Zusammenspiel von IT- und anderer Sicherheit
  - Analyse beispielhafter Angriffe

Techn. Voraussetzungen: Grundlegende Netzwerk-, Forensik- und Linux-Kenntnisse
Termine: 10.-12.03.2020 / 07.-09.07.2020 / 27.-29.10.2020 (3 Tage)
Preis: € 2250,00

SECU3: IPV6-SECURITY

Referent: Marcel Mangold

Die Tage des Internetprotokolls in der Version 4 (IPv4) werden bald gezählt sein. Daher setzen viele Bereiche schon heute das Internetprotokoll in der Version 6 (IPv6) ein. Aktuelle Betriebssysteme unterstützen dieses Protokoll meist schon von sich aus, ohne dass eine Interaktion des Benutzers notwendig wird. Dieser Umstand birgt die Gefahr, dass hier Sicherheitslücken entstehen können, derer sich IT-Sicherheitsbeauftragte oft nicht bewusst sind. Dennoch sollte der Datenverkehr mit IPv6 in gleicher Weise gesichert werden wie der mit IPv4.

Themen

- Einführung in IPv6
  - Einführung in die Adresstypen
  - Übersicht über die Hilfsprotokolle
  - Teredo
  - Routing und Router Advertisements
  - DNS
- Firewalls und IPv6
  - Unfreiwillige Löcher im Sicherheitssystem durch IPv6
- Schwächen im internen Netzwerk
  - Denial-of-Service-Angriffe
  - Man-in-the-Middle-Angriffe
  - Routing-Angriffe
- Schwächen in Sicherheitsmechanismen
  - Umgehung durch Fragmentierung
- (Remote) Host Discovery
- Sicherheitsmaßnahmen
  - Secure Neighbor Discovery

Techn. Voraussetzungen: Grundkenntnisse zu IPv4
Termine: 28.04.2020 / 08.12.2020 (1 Tag)
Preis: € 750,00

SECU4: IT-RECHT UND DATENSCHUTZ FÜR IT-VERANTWORTLICHE

Referent: Horst Speichert

IT-Verantwortliche müssen täglich Entscheidungen treffen, ohne sich der rechtlichen Tragweite bewusst zu sein. Oft riskieren sie dabei Rechtsverstöße, Bußgelder oder stehen gar „mit einem Bein im Gefängnis". In dieser Schulung erwarten Sie topaktuelle Themen wie die DSGVO und das neue BDSG, außerdem steht die E-Privacy-Verordnung vor der Tür. Zuvor: Wie reagieren Sie auf den Brexit? Welche Lösungen für den US-Datentransfer gibt es? Was sind die rechtlichen Anforderungen an ein IT-Sicherheits- und Löschkonzept? Wie bewältigen Sie ein Softwarelizenz-Audit? Wie gestalten Sie sichere Nutzungsbedingungen?

Der Referent ist Spezialist für IT-Recht und Datenschutz, Lehrbeauftragter für Informationsrecht an der Universität Stuttgart und Autor des Fachbuchs „Praxis des IT-Rechts".

Themen

- Datenschutzgrundverordnung (DSGVO)
  - Fit für die praktische Umsetzung?
- E-Privacy-Verordnung
  - Der neue Internet-Datenschutz
- Auswirkungen Brexit, globale Datenströme, rechtssichere Cloud-Verträge
- Der neue Arbeitnehmerdatenschutz (neues BDSG)
- IT-Sicherheits- und Löschkonzept
  - ISMS-Standards, IT-Compliance
- Soziale Netze wie Facebook, WhatsApp etc.
  - Tracking, Standards
- Softwarelizenz-Audit
  - Gebrauchtsoftware
- WLAN-Gesetz, mobile Geräte
  - Nutzungsrichtlinien gestalten
- Mitarbeiterkontrolle
  - Private Nutzung, E-Mail-Archivierung
- Digitalisierte Arbeitswelten
- Big Data, Industrie 4.0
- Richtlinien, Dokumentation von IT-Sicherheit, Betriebsvereinbarungen
- Haftungsrisiken für IT-Verantwortliche
  - Vermeidungsstrategie

Techn. Voraussetzungen: Grundkenntnisse und gute Allgemeinbildung im Bereich IT

Termine: 27.05.2020 / 14.10.2020 (1 Tag)

Preis: € 750,00

SECU5: PLANUNG UND DURCHFÜHRUNG VON PENETRATIONSTESTS

Referent: Sebastian Schreiber

Eine unsichere IT-Landschaft kann den Betrieb oder sogar den Fortbestand von Unternehmen erheblich gefährden. Meist reißen kleine, unscheinbare Fehler gefährliche Löcher in IT-Netze. Voraussetzung für die Behebung dieser Fehler ist es, die Lücken zu identifizieren. IT-Infrastrukturen und Applikationen können hochwertig und robust konzipiert sein und dennoch Schwachstellen aufweisen. Um diesen auf die Spur zu kommen, eignet sich der Penetrationstest hervorragend als Kontrollinstrument. Denn nur auf diese Weise können IT-Netze von außen und innen effektiv auf Sicherheitslücken hin untersucht werden. Die Durchführung solcher simulierter Hacker-Attacken ist aber alles andere als einfach und wird im Workshop diskutiert.

Themen

- Der Penetrationstest
  - Warum Penetrationstests?
    » Definition/Motivation/Besonderheiten
  - Ethische Aspekte
  - Penetrationstests im Licht des neuen IT-Sicherheitsgesetzes
  - Neueste Trends/Penetrationstests der Zukunft
- Angriffsszenarien und Gestaltungsmöglichkeiten
  - Prüfgegenstand (Perimeter, LAN, WLAN, Webapplikation etc.)
  - Einmalig oder kontinuierlich?
  - Blackbox- oder Whitebox-Test?
  - Aggressiv oder vorsichtig?
- Steuerung von Penetrationstestserien
  - Projektmanagement: PPMO
  - Kosten-/Nutzenverhältnis und Budgetoptimierung
  - Metriken und Standards
  - Umfang der Serien: vier Tests pro Jahr oder mehr?
  - Anlassbezogene/turnusmäßige Tests
  - Testtiefe/Testfrequenz
  - Sourcing: Anzahl/Strategie/Benchmarking
  - Agile Umgebungen
- 80/20: Der Pentest-Servicekatalog
  - Red Teaming
- Reporting
  - Ticketsysteme
  - Metrik
  - Projektübergreifendes Reporting
- Schwachstellenmanagement/Re-Tests
- 10 praktische Tipps von Sebastian Schreiber

Termine: 11.02.2020 / 28.07.2020 / 12.11.2020 (1 Tag)

Preis: € 750,00

ANMELDUNG 2020

Hack1: Hacking Workshop 1	☐ 04.-05.02.	☐ 21.-22.04.	☐ 16.-17.06.	☐ 22.-23.09.	☐ 17.-18.11.
Hack2: Hacking Workshop 2	☐ 06.-07.02.	☐ 23.-24.04.	☐ 18.-19.06.	☐ 24.-25.09.	☐ 19.-20.11
Hack3: Angriffe auf Windows-basierte Netzwerke	☐ 17.-19.03.	☐ 21.-23.07.	☐ 29.09.-01.10.	☐ 24.-26.11.	
Hack4: Angriffe gegen VoIP-Infrastrukturen	☐ 24.-25.03.	☐ 15.-16.12.			
Hack5: Exploit Development	☐ 12.-13.02.	☐ 14.-15.07.			
Hack6: Mobile Device Hacking	☐ 18.-19.02.	☐ 26.-27.05.	☐ 13.-14.10.		
Hack7: Sicherheit und Einfallstore bei Webapplikationen	☐ 03.-04.03.	☐ 30.06.-01.07.	☐ 15.-16.09.	☐ 01.-02.12.	
Hack8: WLAN-Hacking und WLAN-Security	☐ 02.-03.04.	☐ 10.-11.11.			
Hack9: Embedded Security	☐ 23.-24.06.	☐ 20.-21.10.			
Secu1: Digitale Forensik bei Computern und Smartphones	☐ 05.-07.05.	☐ 03.-05.11.			
Secu2: Incident Response	☐ 10.-12.03.	☐ 07.-09.07.	☐ 27.-29.10.		
Secu3: IPv6-Security	☐ 28.04.	☐ 08.12.			
Secu4: IT-Recht und Datenschutz für IT-Verantwortliche	☐ 27.05.	☐ 14.10.			
Secu5: Planung und Durchführung von Penetrationstests	☐ 11.02.	☐ 28.07.	☐ 12.11.		

Die Workshops finden in Tübingen statt. Die Preise der jeweiligen Workshops setzen sich aus der Anzahl der Workshoptage mal Tagespreis von € 750,00 zzgl. MwSt. zusammen. Im Preis enthalten sind eine ausführliche Schulung, professionelle Referenten, komplettes Equipment und Verpflegung. Bei einer Buchung von fünf oder mehr Schulungstagen gewähren wir Ihnen einen einmaligen Rabatt in Höhe von 10 % auf das gebuchte Kontingent, egal ob Sie als einzelner Teilnehmer mehrere Kursmodule besuchen oder sich mehrere Mitarbeiter Ihrer Firma zu einem Kurs anmelden. Bei Fragen hierzu stehen wir Ihnen jederzeit zur Verfügung.

Bitte senden Sie Ihre Anmeldung per Fax, E-Mail oder Post an uns zurück:
SySS GmbH, Schaffhausenstraße 77, 72072 Tübingen, Fax: +49 (0)7071 - 40 78 56-19, E-Mail: schulung@syss.de

Name

Firma

Straße

PLZ, Ort

E-Mail

Rechnungsadresse (wenn abweichend)

Telefon

Umsatzsteuernummer
(falls Firmensitz des Auftraggebers außerhalb Deutschland)

Fax

Sonstiges

☐ Ich benötige einen Parkplatz

Ich akzeptiere die umseitigen Teilnahmebedingungen

Datum

Unterschrift

TEILNAHMEBEDINGUNGEN

1. Bitte beachten Sie das VERBOT DER WEITERGABE VON HACKERTOOLS.
   Der Auftraggeber verpflichtet sich, Codes und Software, die z. H. seiner Mitarbeiter von der SySS GmbH zugänglich gemacht werden, nur zur Sicherung seiner eigenen Betriebssysteme einzusetzen; die Bestimmungen der §§ 202 a-c StGB sind ihm bekannt (siehe Anlage).
2. Eine kostenfreie Stornierung (nur schriftlich) ist 4 Wochen vor Schulungsbeginn möglich. Bei Stornierungen 2 Wochen vor Schulungsbeginn fallen 50 % der Gebühr zzgl. MwSt. an, danach die volle Gebühr. Bei Rücktritt ist die Benennung eines Ersatzteilnehmers ohne Zusatzkosten möglich.
3. Die SySS GmbH behält sich vor, die Schulung bei einer zu geringen Teilnehmerzahl bis 10 Tage vor Schulungsbeginn kostenfrei abzusagen.
4. Der Rechnungsbetrag ist ohne Abzüge innerhalb von 14 Tagen nach Rechnungsdatum zahlbar; es gelten unsere AGB.

GESETZESTEXT ZU DEN SOGENANNTEN „HACKERTOOLS“

§ 202a Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202b Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er
   a. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§202a Abs. 2) ermöglichen, oder
   b. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

SCHULUNG

TRAINING FÜR MEHR SICHERHEIT