

Intensiv-Workshops „Hacking & Security“ 2012

Mit neuen Schulungen:

- **Incident Response
bei Hacking-Vorfällen**
- **Exploit Development**

The PenTest Experts.

» Wir machen Sicherheitstests.

Intensiv-Workshops „Hacking und Security“ 2012

Die SySS GmbH bietet hochwertige Schulungsmaßnahmen im Bereich IT-Security an. Diese haben weitgehend Workshop-Charakter. Jeder Workshop kann einzeln gebucht werden.

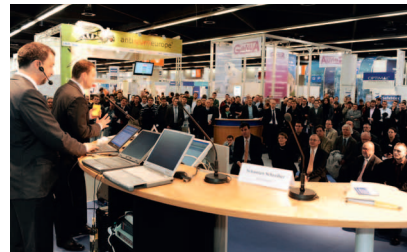
Die Zielgruppe unseres Weiterbildungsangebots sind Personen, die bereits über ein gewisses Know-how im Bereich IT/Netzwerke/Systemadministration verfügen. Grundkenntnisse darin, ebenso in Windows und Unix/Linux werden vorausgesetzt, da unsere Workshops anhand der Praxis durchgeführt werden.

Bis auf den Workshop „Rechtliche Aspekte der IT-Security“ sind die Referenten IT-Security Consultants der SySS GmbH, die großteils über eine langjährige Erfahrung im Bereich IT-Sicherheit verfügen.

Wir bieten unsere Schulungen auch auf Englisch an und wenn Sie wünschen, kommen wir gerne zu Ihnen ins Haus und halten die Schulungen bei Ihnen.



Sebastian Schreiber
Diplom-Informatiker
Geschäftsführer



Live-Hacking der SySS GmbH
(it-sa 2010, Nürnberg)

Inhaltsverzeichnis

Vorwort	3
Inhaltsverzeichnis	5
Praktische IT-Security: Hackertechniken beherrschen – Workshop 1	6
Praktische IT-Security: Hackertechniken beherrschen – Workshop 2	7
Forensik bei Computern und Smartphones	8
Incident Response bei Hacking-Vorfällen	10
WLAN-Hacking und WLAN-Security	11
Sicherheit bei Web-Applikationen	12
Exploit Development	13
IT-Recht und Datenschutz für IT-Verantwortliche	14
Planung und Durchführung von Penetrationstests ...	16
IPv6-Security	17
Anmeldung	18

Praktische IT-Security: Hacker- techniken beherrschen Teil 1 & 2

Computermissbrauch und Cyber-Kriminalität bedrohen IT-Netze tagtäglich. Meist geschehen sie sehr unauffällig und werden erst bemerkt, wenn der Schadensfall schon eingetreten ist. Somit sind sie eine ernstzunehmende Bedrohung. Damit Unternehmen ihre IT-Umgebung vor Gefahren dieser Art wappnen und besser schützen können, haben wir diese Workshops entwickelt. In ihnen betrachten wir das Thema IT-Sicherheit aus der Perspektive eines Täters bzw. „Hackers“. Sie sind für Systemverantwortliche, Administratoren und IT-Sicherheitsbeauftragte gedacht, die mit Hilfe dieser Perspektive ihr Netz bzw. ihre Organisation absichern wollen.

Beide Teile können unabhängig voneinander besucht werden, jedoch baut Workshop 2 selbstverständlich auf Workshop 1 auf.

Workshop 1 (2 Tage)

Folgende Themen werden behandelt:

- **Informationsquellen**
Wie verraten sich angreifbare oder verwundbare Systeme?
- **Standard-Sicherheitswerkzeuge und ihr Einsatz**
(Portscanner, Sniffer)
- **Man-in-the-Middle-Angriffe**
Vor allem in lokalen Netzen können MitM-Angriffe verwendet werden, um verschlüsselten Verkehr oder auch VoIP-Telefonate mitzulesen bzw. zu hören. Durchführung von Angriffsszenarien, Besprechung von Schutzmechanismen.
- **Passwortsicherheit unter Linux, Windows und in Windows-Netzen**
Anhand von verschiedenen Cracking-Techniken schätzen wir die Sicherheit ein, welche eine Passwort-Richtlinie bietet.
- **Sicherheitslücken im Netz**
Ausnutzung, Eskalierung von Rechten – dies bietet Aufschluss über die Wirksamkeit von Schutzmechanismen.

Workshop 2 (2 Tage)

Folgende Themen werden behandelt:

- **Verwendung von Rootkits und Abwehrmaßnahmen**
- **Sicherheit in Windows-Netzen**
 - Eskalation von Benutzerrechten zum Domain-Administrator
 - Umgang mit Windows-Tokens
- **Tunneling**
Verwendung harmloser Protokolle zur verdeckten Übertragung von Daten oder Remote-Zugriff von außen
- **Professionelles Portscannen**
 - Ergebniserhalt in kürzester Zeit
 - Anwendung im lokalen Netz
(Suche nach unerwünschten Geräten)
- **Exkurs: Sicherheit von Web-Applikationen**
Das am besten gesicherte Betriebssystem kann nicht helfen, wenn eine Anwendung unsicher betrieben wird. Behandelt werden die häufigsten Sicherheitslücken wie XSS, Command- und SQL-Injection.

Forensik bei Computern und Smartphones (3 Tage)

Hackerangriffe gegen Firmennetze gehören zur Tagesordnung. Immer wieder werden Unternehmen Opfer von Eindringlingen, die sensible Daten ausspähen und diese illegal weiterverwenden.

Wenn der Ernstfall eintritt, fragen sich die Opfer, wo die Ursache dieser Angriffe zu suchen ist und wer sich dahinter verbirgt. Um hier Klarheit zu bekommen, wird der Angriff forensisch untersucht. Dies bedeutet, dass Spuren identifiziert und (gerichtsverwertbar) gesichert werden. Danach werden die Ergebnisse ausgewertet und als Beweismittel aufbereitet.

Dieser Workshop richtet sich an alle Verantwortlichen für IT. In ihm werden grundlegende Fragestellungen der IT-Forensik und angewandte Standardtechniken analysiert und erörtert. Die Workshopteilnehmer erhalten einen Überblick über forensische Werkzeuge und schärfen ihren Blick für solche Szenarien durch die neu gewonnenen Erkenntnisse.

In den letzten Jahren hat die Smartphone-Forensik eine immer größere Bedeutung erhalten. Da auf Smartphones in der Regel private und dienstliche Daten in großer Zahl abgelegt werden, haben sich diese Geräte als ergiebige Quellen forensischer Untersuchungen erwiesen. Im Unterschied zu normalen IT-Systemen ist ein Zugriff auf Smartphone-Daten meist nur eingeschränkt möglich, so dass hier spezielle Tools und Techniken zum Einsatz kommen.

Folgende Punkte werden behandelt:

- **Definition der Begriffe Forensik und IT-Forensik**
- **Auftreten von Spuren**
 - Festplatte, Hauptspeicher (Prozesse, Netzwerkverbindungen, offene Dateien, etc.)
 - Smartphone, SIM-Karte
 - Versteckte Spuren (z.B. Steganografie)
- **Sicherung von Spuren, lokal und über das Netzwerk**
- **Sicherstellung der Authentizität von Spuren, Gerichtsverwertbarkeit**
- **Forensik-Tools und Toolkits auf Boot-CDs**
- **Analyse der erhobenen Daten**
 - Werkzeuge unter Windows und Linux
 - Ursachenforschung
 - Rückschlussmöglichkeiten auf Ziele und Kenntnisstand des Täters
- **Smartphone-Forensik**
 - Grundsätzliche Fragestellungen
 - Forensik bei iOS, Android, BlackBerry OS, Windows Mobile/Phone
- **Verfassen von gerichtskonformen Berichten**
- **Projektmanagement: IT-Forensik**
 - Zusammenarbeit mit Strafverfolgungsbehörden
 - Rechtliche Situation
 - Behandlung von Sicherheitsvorfällen konform zu den BSI-Grundschutzkatalogen

Incident Response bei Hacking-Vorfällen (3 Tage)

Neu

Gegenwärtig gehört der Datenklau zur Tagesordnung. Fast täglich kann man in den Medien von Hacker-Angriffen lesen und hören, bei denen vertrauliche Daten von Dritten kopiert werden. Werden Hacker-Angriffe bemerkt, ist es wichtig, überlegt handeln zu können. Aus diesem Grund bieten wir einen Workshop an, der Systemadministratoren und IT-Verantwortlichen eine Handlungsgrundlage bieten soll, auf Hacking-Vorfälle reagieren zu können.

Im Workshop soll behandelt werden, wie Notfallplanungen umgesetzt und welche Vorkehrungsmaßnahmen getroffen werden können, um die Möglichkeit von Angriffen einzudämmen. Ferner wird der Workshop darauf eingehen, welche Tätigkeiten nach dem ersten Verdachtsmoment eines Angriffs am besten durchgeführt werden sollten.

Der Workshop ist eine Reaktion auf die momentane Häufung von Hacking-Vorfällen (Stand August 2011) und befindet sich daher noch in der Entwicklung. Aus diesem Grund kann hier noch keine konkrete Inhaltsangabe abgedruckt werden.

Sollten Sie jedoch Fragen zu den Inhalten der Schulung haben, dann scheuen Sie sich nicht, mit dem Referenten, Herrn Stefan Arbeiter, über E-Mail in Kontakt zu treten: stefan.arbeiter@syss.de

WLAN-Hacking und WLAN-Security (2 Tage)

Wireless LAN ist eine äußerst attraktive Technologie. Öffentliche HotSpots nehmen zu, und auch die zur Verfügung stehende Bandbreite wächst ständig.

Folgende Themen werden behandelt:

- **Grundlagen der WLAN-Technologie**
 - Standards
 - Begriffe
- **Aufbau einer WLAN-Umgebung**
Unter Linux (Adhoc, Infrastruktur)
- **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, 802.11i)
- **Authentifizierung in 802.11i**
 - 802.1x
 - EAP
- **Schlüsselmanagement in 802.11i**
 - Schlüsselhierarchien
 - Handshaking
- **Funktionsweise der Verschlüsselungsmechanismen**
 - WEP
 - TKIP
 - CCMP
- **WLAN-Hacking**
 - DoS-Angriffe
 - WEP-Cracking
 - Angriffe gegen WPA/WPA2-PSK
 - Session Hijacking & Man-in-the-Middle-Angriffe
- **Angriffe gegen Captive Portals**

let's warchalk..!	
KEY	SYMBOL
OPEN MODE	ssid bandwidth
CLOSED MODE	ssid
WEP MODE	ssid access control bandwidth

blackballjones.com/warchalking

Sicherheit bei Web-Applikationen (2 Tage)

Für Hacker sind Web-Applikationen heutzutage das Einfallstor Nummer 1. Oftmals finden sie Schwachstellen, die ihnen ermöglichen, sensible Daten zu entwenden und weiter in das System bis hin zum Unternehmensnetzwerk vorzudringen.

Dieser zweitägige Workshop richtet sich an Web-Developer und Mitarbeiter im IT-Bereich, die Web-Applikationen programmieren, bzw. zu betreuen haben. Im Rahmen der Fortbildungsmaßnahme lernen die Teilnehmer, wie Hacker in Web-Applikationen einbrechen und welchen Gefahren so manche Anwendungen ausgesetzt sind.

Der Workshop stellt die gängigsten Angriffe zunächst in der Theorie dar und geht anschließend mit Übungen darauf ein, wie sie in der Praxis umgesetzt werden können. Ziel des Workshops ist es, dass die Teilnehmer am Ende des zweiten Schulungstages selbst Angriffe auf eine eigens für den Workshop erstellte Web-Applikation durchführen können.

Der Workshop behandelt die folgenden Themen detailliert:

- **Cross-Site Scripting (XSS)**
Angriffe auf Sitzungsinformationen, Phishing und Defacing
- **Cross-Site Request Forgery (CSRF)**
Wie Angreifer Applikationsnutzer dazu bringen, das zu tun, was sie wollen
- **SQL-Injection / Blind SQL-Injection**
Unberechtigtes Auslesen von Daten aus einer Datenbank
- **OS Command Injection**
Einschleusen von eigenen Betriebssystem-Kommandos in eine Web-Applikation
- **Local / Remote File Inclusion (LFI/RFI), Path Traversal**
Wie Hacker eigenen Programmcode auf dem angegriffenen Server ausführen können
- **Session-Hijacking**
Übernahme fremder Sitzungen mit Hilfe von Cross-Site Scripting-Angriffen
- **Sicherheit beim Session-Management**

Grundkenntnisse in HTML, HTTP und SQL werden vorausgesetzt.

Exploit Development (2 Tage)

Dieser Workshop vermittelt die theoretischen und praktischen Grundlagen für die Funktionsweise und die Entwicklung von Exploits. Dabei soll vorrangig betrachtet werden, wie Ziellattformen 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 Schwachstellen-Typen ausgenutzt werden können. Ferner geht der zweitägige Workshop noch auf die Frage ein, welche Möglichkeiten es gibt, sich gegen eine Ausnutzung der eigenen Schwachstellen durch Angreifer zu schützen und wie Hacker solche Schutzmaßnahmen umgehen können.

Der Workshop wird folgende Themen detailliert behandeln:

- **Besonderheiten verschiedener Ziellattformen**
 - Prozessorarchitekturen: x86, ARM, PowerPC, MIPS
 - Betriebssysteme: Windows, Unix/Linux, Mac OS
- **Verschiedene Formen der Schwachstellenanalyse**
 - Statische Codeanalysen
 - Laufzeitanalysen
- **Tools of the Trade:**
Wichtige Werkzeuge für die Exploit-Entwicklung
 - Debugger
 - Disassembler
 - Exploit-Framework
- **Ausnutzen verschiedener Schwachstellentypen**
 - Fehler in der Hard- und Softwarearchitektur
 - Fehler in der Anwendungslogik
 - Buffer Overflow-Schwachstellen
 - Format String-Schwachstellen
- **Schutzmaßnahmen und Möglichkeiten, diese zu umgehen:**
 - Stack Cookies
 - SafeSEH
 - Data Execution Prevention (DEP)
 - Address Space Layout Randomization (ASLR)

IT-Recht und Datenschutz für IT-Verantwortliche (1 Tag)

Administratoren und IT-Sicherheitsverantwortliche müssen täglich Entscheidungen treffen, ohne sich der rechtlichen Tragweite bewusst zu sein. Oft stehen sie „mit einem Bein im Gefängnis“. Ein ausgereiftes Sicherheitskonzept besteht aus der erfolgreichen Synchronisation von technischen und juristisch-organisatorischen Komponenten.

Das Seminar klärt über die aktuelle Rechtslage im weiten Feld der IT-Compliance, Informationssicherheit und Datenschutz auf, hilft kritische Situationen richtig einzuschätzen und zeigt die Lösungswege eines ganzheitlichen Sicherheitskonzeptes auf.

Der Referent, Rechtsanwalt Horst Speichert, ist Spezialist für IT-Recht und Datenschutz, Lehrbeauftragter für Informationsrecht an der Universität Stuttgart und Autor des Fachbuches „Praxis des IT-Rechts“ (2. Auflage, Vieweg-Verlag).

Die Schulung wird folgende Themen behandeln:

- **Datenschutz**
 - Das neue Arbeitnehmerdatenschutzgesetz, Novellierung des BDSG
 - Auftrags-DV, Cloud-Computing, Auslandsdienstleister
 - Private Nutzung, Fernmeldegeheimnis, datenschutzkonforme Kontrolle
 - Vermeidung von Datenschutzskandalen, legaler Datenabgleich, Mitarbeiterscreening
 - Big Brother Admin – Monitoring der Internet- und E-Mail-Nutzung
 - Gestaltung in der Betriebsvereinbarung
- **Haftung und Organisation**
Umgang mit Social Media, Social Media Guidelines entwickeln
 - Organisationspflichten und Haftungsprävention
 - Strafverfolgungsmaßnahmen und Auskunftspflichten
 - Abwehr von Abmahnungen
 - Illegale Inhalte wie mp3, Raubkopien und Pornografie
 - Persönliche Haftung des Admin, Vorstandshaftung
- **Hacking und Penetration**
 - Rechtliche Einordnung, Hackerstrafrecht
 - Strafbarkeit von Hacker-Tools nach § 202c StGB
- **Archivierung und DMS**
 - Gesetzliche Archivierungspflichten, insbesondere E-Mail-Archivierung
 - Rechtssicheres DMS, Trennung privater und dienstlicher Inhalte
 - Digitale Steuerprüfung, GDPdU-Compliance, elektronische Rechnung
 - Beweissicherheit, Vorratsdatenspeicherpflicht
- **Sicherheitssysteme und Contentfilter**
 - Datenschutzkonformer Einsatz der Filtersysteme
 - AV, URL-Filter, SSL-Decryption, Data Loss Prevention etc.
 - Webanalyse-Tools, IP-Adressen als personenbezogene Daten
- **Risikomanagement und IT-Compliance**
 - KonTraG, anerkannte Standards und Rechtsvorteile
 - Notwendige Sicherheits- und Benutzerrichtlinien

Planung und Durchführung von Penetrationstests (1 Tag)

IT-Security ist in aller Munde. Die Tatsache, dass eine unsichere IT-Landschaft den Betrieb oder sogar den Fortbestand von Unternehmen gefährden kann, wird immer offensichtlicher. Meist reißen kleine, unscheinbare Fehler gefährliche Löcher in IT-Netze. Voraussetzung für das Beheben dieser Fehler ist, diese kennenzulernen.

IT-Infrastrukturen und Applikationen können hochwertig und robust konzipiert sein und dennoch Lücken aufweisen. Um Schwachstellen auf die Spur zu kommen, eignet sich der Penetrationstest hervorragend als Kontrollinstrument. Denn auf diese Weise können IT-Netze von außen und innen auf Schwachstellen hin untersucht werden.

Die Durchführung solcher simulierter Hacker-Attacken ist aber alles andere als einfach und wird im Workshop diskutiert:

- **Warum Penetrationstests?**
- **Gegenstand der Prüfungen**
(Perimeter, LAN, WLAN, Web-Applikationen, ...)
- **Gestaltungsmöglichkeiten:**
 - Angekündigt / unangekündigt?
 - Einmalig oder als Prozess?
 - Blackbox- oder Whitebox-Test?
 - Durch einen externen Experten oder intern?
 - Aggressive oder vorsichtige Vorgehensweise?
- **Kosten-/Nutzenverhältnis**
- **Vorgehensweise**
- **Projektmanagement**
- **Nachverfolgung von Schwachstellen**
- **Politische Folgen innerhalb des Unternehmens**
- **Ethische Aspekte**

IPv6-Security (1 Tag)

Die Tage des Internet Protokolls in der Version 4 (IPv4) sind bald gezählt. Daher setzen viele Bereiche schon heute das Internet Protokoll 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, von denen IT-Sicherheitsbeauftragte oft nichts wissen, da sie sich dessen nicht bewusst sind. Dennoch sollte der IPv6-Datenverkehr in gleicher Weise gesichert werden wie der IPv4-Datenverkehr.

Dieser Workshop richtet sich an System-Administratoren und IT-Sicherheitsbeauftragte, die sich zum Thema IPv6 und der Sicherheit dieses Protokolls fortbilden möchten. Grundkenntnisse zu IPv6 sollten vorhanden sein.

- **Kurze Einführung in IPv6**
- **Firewalls und IPv6**
Unfreiwillige Löcher im Sicherheitssystem durch IPv6
- **Schwächen im internen Netzwerk**
 - Denial of Service-Angriffe
 - Man-in-the-Middle-Angriffe
 - Routing-Angriffe
- **Sicherheitsmaßnahmen**
 - IPSec
 - Secure Neighbour Discovery

ANMELDUNG

Intensiv-Workshops „Hacking und Security“ 2012

Die Workshops finden in den Schulungsräumen unseres Bürogebäudes in Tübingen statt. Einen Workshop-Tag bieten wir zum Preis von € 600,00 zzgl. MwSt. an.

Der Preis umfasst einen ausführlichen Workshop, einen professionellen Referenten, einen komplett eingerichteten Arbeitsplatz und die Verpflegung.

Bei der Buchung von mindestens 5 Schulungstagen gewähren wir einen Rabatt in Höhe von 10% (dieser ist nicht teilnehmerbezogen).

Bei Fragen hierzu stehen wir Ihnen jederzeit zur Verfügung.

Zeitraum	IT-Security I	IT-Security II	IT-Recht
KW 9	<input type="checkbox"/> 27. - 28.02.12	<input type="checkbox"/> 29.02. - 01.03.12	-
KW 16	<input type="checkbox"/> 16. - 17.04.12	<input type="checkbox"/> 18. - 19.04.12	-
KW 19	<input type="checkbox"/> 07. - 08.05.12	<input type="checkbox"/> 09. - 10.05.12	-
KW 25	<input type="checkbox"/> 18. - 19.06.12	<input type="checkbox"/> 20. - 21.06.12 ³	<input type="checkbox"/> 22.06.12 ³
KW 37	<input type="checkbox"/> 10. - 11.09.12 ⁴	<input type="checkbox"/> 12. - 13.09.12 ⁴	-
KW 43	<input type="checkbox"/> 22. - 23.10.12 ⁵	<input type="checkbox"/> 24. - 25.10.12 ⁵	-
KW 48	<input type="checkbox"/> 26. - 27.11.12	<input type="checkbox"/> 28. - 29.11.12	<input type="checkbox"/> 30.11.12

Zeitraum	Web-App	Penetrationstests	Exploits
KW 11	<input type="checkbox"/> 13. - 14.03.12 ¹	-	-
KW 12	-	<input type="checkbox"/> 19.03.12	<input type="checkbox"/> 22. - 23.03.12
KW 18	<input type="checkbox"/> 02. - 03.05.12	-	-
KW 38	<input type="checkbox"/> 18. - 19.09.12	<input type="checkbox"/> 21.09.12	-
KW 45	-	<input type="checkbox"/> 09.11.12	<input type="checkbox"/> 07. - 08.11.12
KW 49	<input type="checkbox"/> 05. - 06.12.12	-	-

Zeitraum	IT-Forensik	IPv6	WLAN
KW 17	<input type="checkbox"/> 24. - 26.04.12	-	-
KW 24	-	<input type="checkbox"/> 11.06.12	<input type="checkbox"/> 13. - 14.06.12
KW 46	<input type="checkbox"/> 13. - 15.11.12	-	-
KW 50	-	<input type="checkbox"/> 10.12.12	<input type="checkbox"/> 12. - 13.12.12

Zeitraum	Incident Response
KW 13	<input type="checkbox"/> 27. - 29.03.12 ²
KW 39	<input type="checkbox"/> 25. - 27.09.12

Bitte senden Sie Ihre Anmeldung per Fax, E-Mail oder Post an uns zurück:

SySS GmbH
Wohlboldstraße 8
72072 Tübingen

Fax: 07071 - 407856-19

E-Mail: Info@SySS.de

Name

Firma

Straße

PLZ, Ort

Telefon

Fax

E-Mail

Rechnungsadresse

(wenn abweichend)

Sonstiges

Ich akzeptiere die Teilnahmebedingungen (siehe www.SySS.de)

Datum

Unterschrift

¹ Osterferien in Hamburg

² Osterferien in Bremen und Niedersachsen, am 29.03. ist Osterferienbeginn in Rheinland-Pfalz

³ Sommerferien in Berlin, Brandenburg und Hamburg

⁴ Sommerferien in Bayern

⁵ Herbstferien in Bremen, Hessen, Niedersachsen, Saarland, Sachsen und Thüringen



SySS GmbH
Wohlboldstraße 8
72072 Tübingen

Tel.: +49 - (0) 70 71 - 40 78 56 - 0
Fax: +49 - (0) 70 71 - 40 78 56 - 19

E-Mail: Info@SySS.de
<http://www.SySS.de>