Seminar: Angriffstechniken

Ihr Nutzen: Kompakt in nur drei Tagen ……

- vermitteln wir Ihnen die gängigen Sicherheitsprobleme und die Vorgehensweise potentieller Angreifer.
- vertiefen Sie das Erlernte anhand zahlreicher praktischer Übungen.
- erwerben Sie Grundlagenwissen in den verschiedenen Bereichen der Informationssicherheit.
- lernen Sie, wie Sie sich vor aktuellen Angriffstechnologien wirksam schützen können.

Zielgruppe: Die Schulung richtet sich Personen, die sich intensiv mit IT-Sicherheit beschäftigen, die für IT-Sicherheit in Unternehmen oder in Behörden verantwortlich sind oder die z.B. als Systemadministrator oder Programmierer tätig sind.

Termin: **18. bis 20. Juli 2011 in Bochum**

Preis: € 1.690.,- netto zzgl. 19 % MwSt.

Anmeldung:

Internet:	www.is-its.org
Tel:	0234 - 32 26743
E-Mail:	info@is-its.org

Ihre Ansprechpartnerin: Annette Montag

Ihre Trainer:

Dr. Christoph Wegener, zertifizierter CISA, CISM, GDDcert, CCSK und CBP, ist promovierter Physiker und seit 1999 mit der wecon.it-consulting freiberuflich in den Themen IT-Sicherheit, Datenschutz und Open Source aktiv. Er ist Autor zahlreicher Fachbeiträge, Mitglied in vielen Programmkomitees, Fachgutachter für verschiedene Verlage und engagiert sich in der Ausbildung im Bereich der IT-Sicherheit. Seit Anfang 2005 ist er auch als Projektleiter und Berater für IT-Sicherheit am Horst Görtz Institut für IT-Sicherheit tätig.

Daniel Bußmeyer ist am Horst Görtz Institut für IT-Sicherheit der Ruhr-Universität in Bochum beschäftigt und befasst sich dort unter anderem mit den Themen Secure Software Engineering, Implementierung kryptographischer Verfahren und Source Code-Analysen. Darüber hinaus hat er sich bereits vielfach mit Sicherheitsanalysen von existierenden Diensten auseinandergesetzt.

Dominik Birk studierte IT-Sicherheit (M.Sc.) an der Ruhr-Universität in Bochum und ist nun Doktorand am Horst Görtz Institut für IT-Sicherheit wo er im Bereich Cloud Security & Forensik promoviert. Des Weiteren ist er Autor zahlreicher Fachartikel zu den Themen Web-2.0 Sicherheit, Cloud Security, Identitätsdiebstahl und Social Network Privacy. Als freiberuflicher Referent ist er zudem im IT-Sicherheitsumfeld tätig.

Seminar: Angriffstechniken

Programm Tag 1: Spoofing und Cracking

09.45 **Empfang mit Kaffee und Tee**

10.00 **Einleitung in die Schulung**
- Begrüßung durch den Schulungsleiter
- Vorstellung der Teilnehmer

10.15 **Rechtliche Rahmenbedingungen**
- Strafrechtliche Aspekte
- Datenschutzrechtliche Aspekte
- Leitfaden zur Durchführung von Penetrationstests

11.30 **Kaffeepause**

11.45 **Sichere Systeme durch sichere Passworte**
- Passworte testen mit Ophcrack und John
- Sammeln von Passworten mit Cain&Abel
- Empfehlungen zur richtigen Passwortwahl

13.00 **Mittagessen**

14.00 **Manipulation von Netzwerkverkehr**
- Grundlagen von mit ARP-Spoofing und Co.
- Praktischer Einsatz von Cain&Abel und Ettercap
- Abhören von VoIP-Telefonaten

15.45 **Überblick über weitere Angriffsmöglichkeiten im Netzwerk**
- Angriffe mittels TCP RST und doppelten TCP SYN
- Überblick über die Sicherheitsproblematiken in IPv6
- Überblick zur WLAN-Sicherheit

16.30 **Kaffeepause**

16.45 **Netzwerkmapping mit Nmap**
- Möglichkeiten von Nmap
- Nmap im praktischen Einsatz

17.30 **Schwachstellentests mit Nessus und OpenVAS**
- Grundlagen und Möglichkeiten von Nessus und OpenVAS
- OpenVAS im praktischen Einsatz

18.00 **Ende des 1. Schulungstages**

Seminar: Angriffstechniken

Programm Tag 2: Metasploit und Backtrack

09.00 Probleme bei der Programmierung

- Sicherheitsproblematiken bei der Programmierung
- Wie funktioniert eine Programmausführung in der CPU?
- Was sind Bufferoverflows?
- Was sind Format-String Attacken?

10.30 Kaffeepause

10.45 Hands-on Bufferoverflows/Formatstrings

- Untersuchen eines Beispielprogramms
- Finden einer Schwachstelle (Bufferoverflow)
- Ausnutzen der gefundenen Schwachstelle durch Bufferoverflow
- Gegenmaßnahmen zu Bufferoverflows und Format-Strings

11.30 Kaffeepause

11.45 Einführung und Benutzung von Rootkits

- Was sind die Gefahren von Rootkits, wie funktionieren diese?
- Installation eines Beispiel-Rootkits
- Aufrufen und Ausnutzen der Backdoor des Rootkits

13.00 Mittagessen

14.00 Benutzung von Metasploit / Meterpreter

- Suchen und Identifizieren potentieller Schwachstellen
- Ausnutzung der Schwachstellen durch Metasploit
- Verbinden zur Metasploit-Console *Meterpreter*
- Benutzung von Meterpreter und Kompromittieren eines Systems

16.30 Kaffeepause

16.45 Vollautomatisches Ausnutzen von Sicherheitslücken mit Fasttrack

- Vollautomatisiertes
  - Scannen des Netzwerks
  - Suchen nach Sicherheitslücken
  - Auswählen eines geeigneten Exploits
  - Ausführen des ausgewählten Exploits
- Erkennen von Sicherheitslücken im eigenen System
- Schließen gefundener Sicherheitslücken

18.00 Ende des 2. Schulungstages

Seminar: Angriffstechniken

Programm Tag 3: Web Application Hacking

09.00 Einführung
- Motivation und Kurzeinführung in die Websicherheit
- Umgang mit dem VMware-Image und der Burp-Suite

10.30 Kaffeepause

10.45 Cross Site Scripting (XSS)
- Grundlagen der Webkommunikation
- Problematik mit XSS-Schwachstellen
- Praktische Übungen

11.30 Kaffeepause

11.45 Cross Site Request Forgery (CSRF)
- Grundlagen von CSRF
- Praktische Übungen

13.00 Mittagessen

14.00 Local/Remote File Inclusion (LFI/RFI)
- Grundlegende Problematik von LFI/RFI
- Praktische Übungen

15.15 SQL-Injektion (SQLi)
- Grundlegende Problematik von SQLi
- Praktische Übungen

16.30 Kaffeepause

16.45 Remote Command Execution (RCE)
- Grundlegende Problematik von RCE
- Praktische Übungen

17.15 Appendix
- Web Application Vulnerability Scanner
- Web Application Firewalls
- Forensische Untersuchungen in Web-Anwendungen
- Offene Fragerunde

18.00 Ende des 3. Schulungstages