

Hacking Training

Lernen Sie Praktiken von Hackern kennen, um sich wirkungsvoll gegen künftige Angriffe zu schützen und potentielle Sicherheitslücken in Ihren Systemen zu schließen!

Als einziger weltweit autorisierter Trainingspartner von NotSoSecure bieten wir Ihnen sehr praxisbezogene Hacking Trainings an, die teilweise direkt auf der Black Hat Konferenz vorgestellt und durchgeführt werden.

Die Trainingsprogramme führen wir regelmäßig in unseren weltweiten Schulungszentren oder individuell auf Sie zugeschnitten direkt bei Ihnen vor Ort durch. Gerne steht Ihnen unser einzigartiger Pool an Security-Experten auch für Ihre Consulting-Projekte zur Verfügung.

75%

75% reales Hacking und praktisches Training in unserem Advanced "Hack-Lab"



Entwickelt von erfahrenen Penetrationstestern, die regelmäßig auf internationalen Konferenzen wie Black Hat, AppSec, OWASP, Defcon u.a. vertreten sind



Kontinuierlich aktualisierte Kursinhalte und Abdeckung aktuellster Exploits

The Art of Hacking (TAOH)



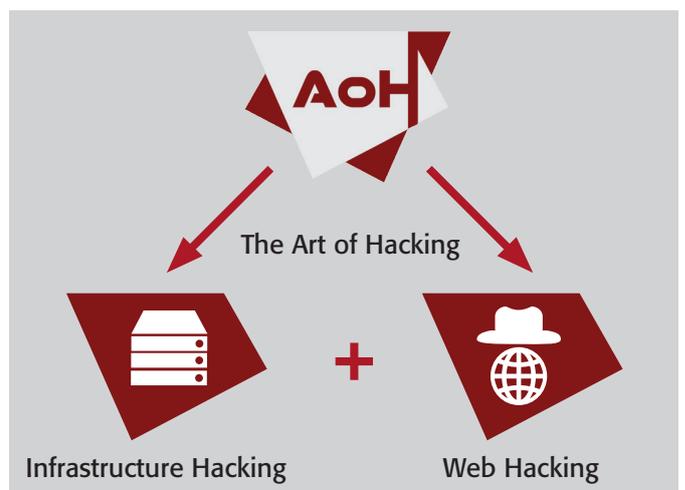
ID TAOH Preis 3.990,00 EUR (zzgl. MwSt.) **Dauer** 5 Tage

Kursinhalt

- Infrastructure Basics
 - TCP/IP Basics
 - The Art of Port Scanning
 - Target Enumeration
 - Brute-Forcing
 - Metasploit Basics
 - Password Cracking
- Hacking Unix, Databases and Applications
 - Hacking Recent Unix Vulnerabilities
 - Hacking Databases
 - Hacking Application Servers
 - Hacking Third Party Applications (WordPress, Joomla, Drupal)
- Hacking Windows
 - Windows Enumeration
 - Hacking Recent Windows Vulnerabilities.
 - Hacking Third party Software (Browser, PDF, Java)
 - Post Exploitation: Dumping Secrets
 - Hacking Windows Domains
- Information Gathering, Profiling and Cross-Site Scripting
 - Understanding HTTP protocol
 - Identifying the Attack Surface
 - Username Enumeration
 - Information Disclosure
 - Issues with SSL/TLS
 - Cross Site Scripting
 - Cross-Site Request Forgery
- Injection, Flaws, Files and Hacks
 - SQL Injection
 - XXE Attacks
 - OS Code Injection
 - Local/Remote File include
 - Cryptographic weakness
 - Business Logic Flaws
 - Insecure File Uploads



Optimale Vorbereitung auf die IEEE Computer Society's Cyber Security Global Competency Certification!



Termine Deutschland		München	23.10.-27.10.17
Düsseldorf	E 16.01.-20.01.17	Berlin	20.11.-24.11.17
Hamburg	20.02.-24.02.17	Frankfurt	E 18.12.-22.12.17
Stuttgart	20.03.-24.03.17	Termine Österreich	
Berlin	24.04.-28.04.17	Wien	29.05.-02.06.17
München	E 29.05.-02.06.17	Wien	27.11.-01.12.17
Frankfurt	26.06.-30.06.17	Termine Schweiz	
Münster	24.07.-28.07.17	Zürich	03.04.-07.04.17
Düsseldorf	21.08.-25.08.17	Zürich	11.09.-15.09.17
Hamburg	E 25.09.-29.09.17	E Training auf Englisch	

Infrastructure Hacking (ISH)



ID ISH Preis 2.490,00 EUR (zzgl. MwSt.) **Dauer** 3 Tage

Termine Deutschland		München		E 15.05.-17.05.17		München		16.10.-18.10.17		Wien		27.11.-29.11.17	
Düsseldorf	E 09.01.-11.01.17	Frankfurt	12.06.-14.06.17	Berlin	13.11.-15.11.17	Termin Schweiz	Zürich	27.03.-29.03.17	Zürich	04.09.-06.09.17	E Training auf Englisch		
Hamburg	13.02.-15.02.17	Münster	17.07.-19.07.17	Frankfurt	E 11.12.-13.12.17	Termin Österreich	Wien	29.05.-31.05.17					
Stuttgart	13.03.-15.03.17	Düsseldorf	14.08.-16.08.17										
Berlin	10.04.-12.04.17	Hamburg	E 18.09.-20.09.17										

Web Hacking (WH)



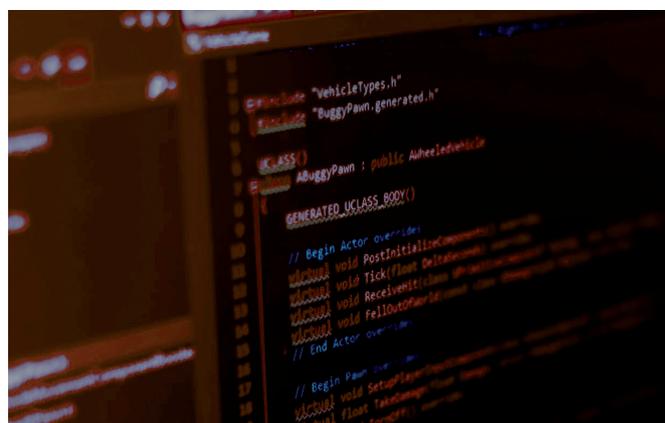
ID WH Preis 1.990,00 EUR (zzgl. MwSt.) **Dauer** 2 Tage

Termine Deutschland		München		E 18.05.-19.05.17		München		19.10.-20.10.17		Wien		30.11.-01.12.17	
Düsseldorf	E 12.01.-13.01.17	Frankfurt	19.06.-20.06.17	Berlin	16.11.-17.11.17	Termin Schweiz	Zürich	30.03.-31.03.17	Zürich	07.09.-08.09.17	E Training auf Englisch		
Hamburg	16.02.-17.02.17	Münster	20.07.-21.07.17	Frankfurt	E 14.12.-15.12.17	Termin Österreich	Wien	01.06.-02.06.17					
Stuttgart	16.03.-17.03.17	Düsseldorf	17.08.-18.08.17										
Berlin	18.04.-19.04.17	Hamburg	E 21.09.-22.09.17										

Weitere Hacking Trainings

- Advanced Infrastructure Hacking (AWH) – 5 Tage
- Advanced Web Hacking (AWH) – 3 Tage
- AppSec for Developers (ASD) – 2 Tage
- Advanced Mobile Exploitation (AME) – 3 Tage
- Offensive IoT Exploitation (OIE) – 2 Tage
- Xtreme Exploitation (XE) – 2 Tage
- PowerShell for Penetration Testers (PPTF) – 2 Tage

Weitere Informationen unter www.flane.de/notsosecure



Penetrationstests

Wie sicher sind Ihre IT-Systeme?

Gerne stehen Ihnen unsere Security-Experten auch für einen Penetrationstest zur Verfügung. Wir analysieren für Sie die Sicherheit Ihrer Systeme aus der Perspektive von hochspezialisierten Angreifern und suchen in enger Abstimmung mit Ihnen nach Sicherheitslücken und Schwachstellen. Unsere Penetrationstests basieren auf exklusivem Know-how erfahrener Pentester, die regelmäßig auf internationalen Konferenzen wie Black Hat, AppSec, OWASP, Defcon u.a. vertreten sind. Erfahren Sie, wie Sie kriminellen Angriffen auf Ihre IT-Systeme vorbeugen und potentielle Sicherheitslücken schließen.

Testmodule

Wir bieten Ihnen unterschiedliche Tests an, die Sie auch kombinieren können:

- **Infrastruktur:** Prüfung ausgewählter Teile oder der gesamten IT-Infrastruktur (z.B. Server, Router, Switches, Firewalls, VPN)
- **Wireless:** Prüfung Ihrer WLAN-Infrastruktur (Access Points, WLAN Router)
- **Clients:** Prüfung der Anfälligkeit Ihrer Clients für zielgerichtete Angriffe aus dem Internet
- **Web:** Prüfung von Webshops, Internetportalen und Webauftritten
- **Mobile Apps:** Detaillierter Sicherheitstest der von Ihnen oder Ihren Kunden eingesetzten mobilen Apps sowie Mobile-Device-Management-Lösungen

- ✓ Maßgeschneiderte und individuelle Beratung zur Prävention gegen digitale Angriffe und zum optimalen Schutz Ihrer Unternehmensdaten
- ✓ Ableitung ergänzender Sicherheitsmaßnahmen
- ✓ Expertise durch exklusives und fundiertes Know-how von Black Hat Experten
- ✓ Blackbox, Whitebox und Greybox Tests
- ✓ Berücksichtigung von Industriestandards wie OWASP Top 10 oder PCI-DSS
- ✓ Erfüllung gesetzlicher Vorschriften