Hacking Extrem

Die größtmögliche Sicherheit kann nur dann erreicht werden, wenn man die Methoden und Vorgehensweise der Angreifer kennt und ihre Denkweise und Motive nachvollziehen kann.

Häufig werden Sicherheitsmechanismen lediglich aus der Sicht eines Administrators oder Netzwerkspezialisten geplant und aufgebaut. Die Betrachtungsweise eines Angreifers unterscheidet sich in der Regel jedoch grundlegend davon. Nicht zuletzt deshalb kommt es immer wieder zu erfolgreichen Angriffen auf Firmennetze. Dieses Intensivtraining vermittelt die Vorgehensweise von Angreifern jenseits von Web-Applikationen. Beginnend mit der Informationsgewinnung geht es in zahlreichen Schritten über Linux-Server und Windows-Clients bis in die Domäne. Es wird auf
bekannte und weniger bekannte Angriffstechniken eingegangen – von den grundlegenden Klassikern bis hin zur Umgehung aktueller
Schutzmechanismen, von konzeptionellen Problemen bis hin zu Vorgängen in der Hardware. In zahlreichen Demonstrationen werden Beispiele aus der Praxis beleuchtet.

Die Trainer führen selbst regelmäßig Sicherheitsüberprüfungen durch und geben eigene Praxiserfahrung sowie Insider-Wissen aus der „Szene“ ungefiltert weiter.

Behandelte Betriebssysteme: Linux/Unix-Umfeld und Windows

Zielgruppe: Administratoren, Netzwerkspezialisten, Sicherheitsverantwortliche und Mitarbeiter auf Management-Ebene, die sich nicht scheuen, (Un-)Sicherheit auch durch die Brille des Angreifers zu betrachten, und dabei sehr tief in eine technische Welt eintauchen möchten.

Voraussetzung: Kenntnisse der grundlegenden Vorgänge der Benutzung und Administration von Windows- und Linux-Systemen. Kenntnisse des TCP/IP-Stacks und der Funktionsweise gängiger Protokolle sind von Vorteil.

Beginn:
Dienstag, 4. Juli 2023, 09:00 Uhr

Ende:
Freitag, 7. Juli 2023, 18:00 Uhr

Veranstaltungsort:
Hamburg
Deutschland

Website & Anmeldung:
Email nadine.eimuellner@cirosec.de

http://www.cirosec.de/trainings/hacking-extrem