CAk
Cyber Akademie

Termine

16.05 - 18.05.2017

19. 09 - 21.09.2017

in Berlin

Cyber Defence Simulation Training

Weitere Informationen unter: www.cyber-akademie.de

Cyber Defence Simulation Training

In dem einmaligen Schulungskonzept werden typische IT-Angriffe im Kontext von „echten“ Unternehmensnetzwerken simuliert. Jeder Teilnehmer erhält Zugriff auf eine eigene IT-Infrastruktur unter Nutzung von gängigen Standardprodukten, wie sie auch tagtäglich in Unternehmen zum Einsatz kommt:

- Windows Domain Infrastruktur mit diversen Windows Clients
- Windows und Linux Serversysteme
- Antiviren-Lösungen
- Web-Application Firewalls
- Sonstige IT-Monitoring und SIEM Lösungen.

Trainingsvoraussetzungen

Für eine erfolgreiche Teilnahme ist von jedem Teilnehmer ein Laptop mit folgendem Setup mitzubringen:

- Windows-Umgebung mit Internet Explorer / Edge Browser (keine VM)
- Firefox Browser installiert
- WLAN- und Ethernet-Netzwerkschnittstelle
- Java 8 installiert
- Lokale Administratorrechte
- Adapter zum Anschluss eines HDMI-Monitorkabels

Zielsetzung

Ziel ist es, das die Teilnehmer verschiedenste moderne Angriffe auf Unternehmensnetzwerke unter Anleitung verstehen, erkennen und ggf. abwehren.

- Angreifer-Logik im Gesamtkontext „Unternehmensnetzwerk“
- Grenzen von Sicherheitsprodukten korrekt einschätzen.
- Härtungsmaßnahmen im Unternehmensnetzwerk korrekt priorisieren.

ZIELGRUPPE

↗ System- und Netzwerk-Administrator / Operations Engineer, IT-Security Manager / Entscheider, Berater in IT-Security Kundenprojekten., Angehende IT-Forensikmitarbeiter /, Angehende Secure Operations Center (SoC) Mitarbeiter / Leiter

TERMINE UND ORTE

↗ 19.09 - 21.09.2017, Berlin

↗ 16.05. - 18.05.2017, Berlin

PREIS

↗ 3.200,– Euro zzgl. MwSt.

Seminarablauf

Das Training ist in 9 Kapitel und 20 Szenarien aufgegliedert.

Kapitel 1: Awareness / Bedrohungslage
Kapitel 2: Einführung - Kennenlernen der Trainingsumgebung
Kapitel 3: „Reconnaissance “ und die Limitierung von kommerziellen Security-Tools
Kapitel 4: Man-In-The-Middle - Lesen und Manipulieren von Netzwerkverkehr
Kapitel 5: Applikations-Sicherheit und tool-basierte Angriffs-Detektion (WAF)
Kapitel 6: Windows Domain Sicherheit
Kapitel 7: Krypto Trojaner auf Gruppenlaufwerken
Kapitel 8: Social Engineering mit bösartigen Anhängen
Kapitel 9: Anti-Virus (AV) Bypasses – Die Limitierungen von AV-Produkten

Vor jedem Kapitel erfolgt eine detaillierte theoretische Einführung in das Thema. Anschließend wird das erlernte in typischen Red-VS-Blue Szenarien durch die Teilnehmer praktisch geübt.

Themenüberblick 1. Tag:

09:00 - 12:00 Uhr: 1. Awareness / Bedrohungslage

12:00 - 13:00 Uhr: Mittagspause

13:00 - 15:00 Uhr: 2. Einführung
- Kennenlernen der Trainingsumgebung
- Security Tool Einführung
  - Exploit Net API
  - Exploit vsftpd

15:00 - 17:00 Uhr: 3. „Reconnaissance“ und die Limitierung von kommerziellen Security-Tools
- High Noise Scans
- Low Noise Scans

Themenüberblick 2. Tag:

09:00 - 12:00 Uhr: 4. Man-In-The-Middle: Lesen und Manipulieren von Netzwerkverkehr
- ARP Spoofing 1 „Request
- ARP Spoofing 2 „Response
- SSL/TLS - MitM Attacks
- SSL Strip V2 5

12:00 - 13:00 Uhr: Mittagspause

Seminarablauf

13:00 - 15:00 Uhr: 5. Applikations-Sicherheit und tool-basierte Anriffs-Detektion (WAF)
- XSS Schwachstellen
- SQLi Schwachstellen

15:00 - 17:00 Uhr: 5. Applikations-Sicherheit und tool-basierte Anriffs-Detektion (WAF)
- Shell / RCE Schwachstellen
- Upload Schwachstellen

Themenüberblick 3. Tag:

09:00 - 12:00 Uhr: 6. Windows Domain Sicherheit
- Lokale NTLM Recovery und Passwort-Cracking
- Laterale bösartige Bewegung in einer Windows Umgebung
  - NTLM Hash Abuse Teil 1
  - NTLM Hash Abuse Teil 2

12:00 - 13:00 Uhr: Mittagspause

13:00 - 15:00 Uhr: 7. Krypto Trojaner auf Gruppenlaufwerken

8. Social Enginnering mit bösartigen Anhängen

15:00 - 17:00 Uhr: 9. Anti-Virus (AV) Bypasses - Die Limitierungen von AV-Produkten
- Einfacher AV-Bypass
- Komplexer AV-Bypass

Referent

Andreas Falkenberg, arbeitet seit vielen Jahren als professioneller White-Hat Hacker. In vielen internationalen Projekten in Europa, Asien und den USA kann er auf ein breites Erfahrungsspektrum, beginnend mit der Überprüfung von einfachen Webseiten bis hin zu Audits für Core-Banking Applikationen, zurückgreifen. Andreas Falkenberg hat den Master in IT-Sicherheit/Informationstechnik an der Ruhr-Universität Bochum erfolgreich abgeschlossen. Neben diversen Talks auf Veranstaltungen gibt Herr Falkenberg regelmäßig Expertenschulungen im Bereich Cyber-Security; unter anderem ab dem Jahr 2017 auch für die Bundeswehr.

Anmeldung

Fax-Anmeldung an: +49(0)228-97097-78

Online-Anmeldung unter: www.cyber-akademie.de

Ja, ich nehme am Seminar „Cyber Defence Simulation Training “

☐ vom 16.05.2017 - 18.05.2017 in Berlin ☐ vom 19.09.2017 - 21.09.2017 in Berlin

zum Preis von jeweils 3.200,- Euro zzgl. MwSt. teil.

Firma/Behörde*: _____

Abteilung*: _____

Funktion*: _____

Vorname*: _____ Name*: _____

Straße*: _____

PLZ*: _____ Ort*: _____

Personalisierte Email*: _____

Ort/Datum/Unterschrift: _____

Freiwillige Angaben

Titel / Dienstrang: _____

Telefon: _____ Fax: _____

Die mit* gekennzeichneten Felder sind für eine Anmeldung unbedingt erforderlich.

Ansprechpartnerin für organisatorische Fragen: Julia Kravcov, Veranstaltungsmanagement
Tel.: +49(0)228-97097-55, Fax: +49(0)228-97097-78, E-Mail: julia.kravcov@cyber-akademie.de

Eine Anmeldung mit diesem Formular oder unter www.cyber-akademie.de ist Voraussetzung für die Teilnahme. Die Teilnahmegebühr versteht sich zzgl. gesetzlicher Mehrwertsteuer und beinhaltet Mittagessen, Erfrischungs- und Pausengetränke und die Dokumentation/Tagungsunterlagen. Die Teilnehmerzahl ist begrenzt. Zusagen erfolgen deswegen in der Reihenfolge der Anmeldungen. Nach Eingang Ihrer Anmeldung erhalten Sie eine Anmeldebestätigung per E-Mail und eine Rechnung per Post. Bei Stornierung der Anmeldung bis zwei Wochen vor Veranstaltungsbeginn wird eine Bearbeitungsgebühr in Höhe von 100,– Euro zzgl. MwSt. erhoben. Danach oder bei Nichterscheinen des Teilnehmers wird die gesamte Tagungsgebühr berechnet. Selbstverständlich ist eine Vertretung
des angemeldeten Teilnehmers möglich. Mit dieser Anmeldung erkläre ich mich mit den Allgemeinen Geschäftsbedingungen des Veranstalter einverstanden: siehe unter: **www.cyber-akademie.de** .