AnyWeb Training
Cisco Certified Learning Center

Kursdetails

Garantierte Durchführung | Geplante Durchführung | Auf Anfrage | Ausgebucht, Warteliste möglich

The Packet Factor
TPF

Überblick

In der Welt der Cybersicherheit ist das Erkennen bösartiger Aktivitäten oft auf Analysen an der Perimeter-Firewall, auf Intrusion-Detection-Systeme oder auf Endpunkt-Sicherheitslösungen fokussiert. Es erfolgt aber kaum ein Angriff, der nicht das Netzwerk als Einfallstor oder Transportmedium benutzt und entsprechende Spuren hinterlässt. Genau hier setzt unser Kurs "The Packet Factor" an: Wir bieten umfassende Kenntnisse und praktische Fähigkeiten, um Netzwerkdaten aus sicherheitstechnischer Sicht zu bewerten und zu analysieren.

Die theoretischen Erläuterungen werden mit praktischen Übungen ergänzt, um ein fundiertes Verständnis für die Analyse von Netzwerkpaketen und Sicherheitsmethoden zu erlangen.

Neben dem bekannten Werkzeug für die Paketanalyse, Wireshark, werden während dieses Kurses auch eine Vielzahl weiterer Open-Source-Tools eingesetzt. Diese Tools spielen eine entscheidende Rolle bei der Auswertung von Daten und der Simulation von Sicherheitsangriffen. Dabei werden auch Angriffsbeispiele aus der Perspektive des Angreifers präsentiert, um die resultierenden Spuren im Netzwerk besser zu verstehen.

Der Kurs wird auf Deutsch gehalten, die Unterlagen werden in englischer Sprache bereitgestellt.

Dauer	2 Tage
Kursstart/Status	Auf Anfrage 08:30-12:00 / 13:00-16:30
Kursort	Zürich
Kosten	CHF 2220.00 Lunch und Pausenverpflegungen inklusive.
Sprache	Deutsch
Dokumentation	Es wird immer die aktuellste Version geschult. Ein Kurs- und ein Übungsbuch (PDF in Englisch) sowie PCAP(ng)-Dateien werden elektronisch zur Verfügung gestellt.

Voraussetzungen

Für die Kursteilnahme empfehlen wir Kenntnisse wie folgt:

- Grundlegendes Verständnis von Netzwerken
- Basiswissen zu den üblichen Internetprotokollen. Dies beinhaltet ein Verständnis der wichtigsten Protokolle wie IP, TCP / UDP für die Datenübertragung, sowie DNS und HTTP als grundlegende Protokolle für die World-Wide-Web-Dienste
- Neugier und die Bereitschaft, sich mit neuen Technologien und Konzepten zu befassen.

Mit den im Kurs zur Verfügung gestellten PCAP(ng)-Dateien und dem umfangreichen Kursbuch können die Teilnehmer die Übungen und Analysen auch nach Abschluss des Kurses jederzeit eigenständig wiederholen und vertiefen.

Zielgruppe

Dieser Kurs richtet sich an Network Engineers, die ihr Verständnis für Sicherheitsaspekte in Netzwerken vertiefen möchten. Er ist jedoch auch für Security Engineers von Interesse, die normalerweise auf Endpunktsicherheit spezialisiert sind und ihren Horizont erweitern möchten, um die Netzwerksicherheit besser zu verstehen.

Kontakt

AnyWeb Training
Hofwiesenstrasse 350
CH-8050 Zürich-Oerlikon

training@anyweb.ch
Tel +41 58 219 1104
Fax +41 58 219 1100

AnyWeb Training
Cisco Certified Learning Center

Kursdetails

Garantierte Durchführung | Geplante Durchführung | Auf Anfrage | Ausgebucht, Warteliste möglich

Kursinhalt

- Intro: Analyse von Netzwerkpaketen und ihre Relevanz für die Security
- Methoden zur Erfassung von Netzwerkpaketen
- Werkzeuge zur Analyse und Manipulation von Netzwerktrace-Daten
- Protokollfelder und ihre Bedeutung in der Cybersicherheit
- Verschlüsselungsprotokolle wie SSL/TLS und ihre Herausforderungen
- Techniken zur Entschlüsselung und Analyse verschlüsselter Netzwerkdaten
- Erkundung von Wireshark als Hauptwerkzeug zur Paketanalyse
- Filterausdrücke und Suchmethoden zur Mustererkennung
- Arbeiten mit Indikatoren für Kompromittierungen (IoCs in Wireshark)
- Wireshark LUA Plugins:
  - Investigators Pack, Wireshark Forensic Toolkit und MISP-Integration
- Analyse des Netzwerkverkehrs zur Identifizierung bösartigen Verhaltens
- Beispiele für Sicherheitsangriffe und ihre Netzwerkspuren
- Analysieren verschiedener Methoden zur Datenexfiltration
- Die Rolle der künstlichen Intelligenz in der Netzwerk- und Securityanalyse
- Best Practices zur Filterung und Profilverwaltung
- Tipps und Tricks.

Laborübungen

- Lab-Einrichtung
- PCAP(ng) Tools (Werkzeuge zur Paketerfassung)
- "Review" Internetprotokolle
- Erweiterte Filter
- Integration von "Threat Intelligence"
- Identifizierung verschiedener Netzwerk-Scans
- Analyse von Exploit- und Extraktionsverkehr
- Anwendungsfälle für künstliche Intelligenz
- "Von SSL Errors, Malware und Datenextraktion".

Zertifizierung

Keine.

Kontakt

AnyWeb Training
Hofwiesenstrasse 350
CH-8050 Zürich-Oerlikon

training@anyweb.ch
Tel +41 58 219 1104
Fax +41 58 219 1100