Extra WIRESHARK Newsletter Mai 2024

Liebe Kunden und Wireshark Freunde

Dieser Wireshark Newsletter von Leutert NetServices informiert Sie unregelmässig über Neuerungen im Zusammenhang mit dem Open Source Analyzer Wireshark und weiteren Netzwerkanalyse-Produkten.

Dies ist eine Newsletter '*Extra-Ausgabe*'

Der Anlass ist die Ankündigung eines neuen Kurses mit dem Thema **Wireshark im Security-Umfeld.**

Der Kurs '**The Packet Factor**' zeigt, wie Wireshark im Bereich **Intrusion Detection and Prevention** auf Paketebene zur Erkennung von Netzwerk-Manipulationen und -Attacken eingesetzt werden kann.

Mein langjähriger Kollege **Walter Hofstetter** ist Autor und Leiter dieses Kurses und eine Koryphäe auf dem Gebiet **Netzwerk-Analyse und -Security**. Es gibt in dieser Kombination und diesem Detaillierungsgrad aktuell keinen vergleichbaren Kurs auf dem Markt.

Erfahren Sie mehr im nachfolgenden **Interview mit Walter** und unter diesem Link:

https://www.linkedin.com/pulse/unlock-secrets-network-security-packet-factor-anyweb-hofstetter-l1gwe/

Interview mit Walter Hofstetter, dem Autor des neuen Wireshark Kurses

«The Packet Factor»

Rolf Leutert

Walter Hofstetter

Rolf: Hallo Walter, wir beide sind ja Urgesteine der Netzwerkanalyse, angefangen in den 80er Jahren mit dem **Sniffer von Network General**. Den Sniffer gibt es inzwischen nicht mehr, aber wir beide sind immer noch aktiv in diesem Bereich.

Walter: Ja, der Sniffer war damals eine Sensation, er eröffnete eine komplett neue Sicht auf die Paketschicht und damit den **Beginn der Netzwerkanalyse**.

Rolf: Ich erinnere mich gut, ich war damals bei der Swissair, und wir beschafften den ersten Sniffer in Europa. Der grösste Mangel war jedoch, dass es zu der Zeit noch **keine Kurse** gab, und ohne das entsprechende Protokoll-Knowhow hatte man keine Chance zu verstehen, was da auf dem kleinen Bildschirm abging.

Walter: Dieses Bedürfnis wurde erkannt und später deshalb die **Sniffer University** gegründet. Diese bot ein breites Spektrum an Kursen zu Themen wie **Ethernet, Token Ring, FDDI, WAN, ATM, ISDN** usw**.** Wir beide waren da ja von Anfang an dabei und wurden die ersten zertifizierten Sniffer-Instruktoren in Europa.

Rolf: Das war eine spannende Zeit mit vielen Reisen, wir kamen ja weltweit als Instruktoren zum Einsatz. Später bist du dann in den **Netzwerk-Security Bereich** abgeschwenkt, wie kam es dazu?

Interview mit Walter Hofstetter, Autor von «The Packet Factor»

Walter: Ich war bei **Network General** als diese 1997 von **McAfee** übernommen und der Name auf **Network Associates** geändert wurde**.** Danach kam ich vermehrt mit der Thematik **Viren und Network Intrusion** in Kontakt und dieser Bereich faszinierte mich.

Rolf: Danach warst du ja noch bei weiteren Firmen im Security-Umfeld.

Walter: Ich arbeitete für Firmen wie **Symantec, Palo Alto Networks und Deutsche Telekom Security** immer mit Fokus auf Netzwerk Security. Auch wenn heutige Werkzeuge wie IDS/IPS (Intrusion Detection / Protection) oder Next Generation Firewalls viele Informationen in einem grafischen «User Interface» bieten, konnte mir oft erst ein Blick auf die Pakete Gewissheit verschaffen, warum und wie etwas funktioniert oder eben nicht. Meine Devise lautete schon damals **"Packets Don't Lie"** und mit Hilfe des **Sniffers** und später **Wireshark** konnte ich zahlreiche kritische Vorfälle analysieren und erklären.

Rolf: Und so entstand die Idee für diesen neuen Kurs?

Walter: Den Gedanken, meine jahrelange Erfahrung in einem Kurs weiterzugeben, hatte ich schon länger. Ich bin der Meinung, dass der **Faktor Paket-Analyse** den Security-Spezialisten viel zu wenig bewusst ist, deshalb auch der Name des Kurses **«The Packet Factor»**. Mit dem entsprechenden Wissen gibt es zahlreiche Möglichkeiten, Security-Probleme und Schwachstellen **auf Paket-Level** erkennen zu können.

Rolf: Was kann denn Wireshark, was ein herkömmliches **Intrusion Detection System** (IDS) nicht auch bieten kann?

Walter: Diese Systeme sind unabdingbar und erfüllen wichtige Erkennungs- und Abwehrfunktionen. Es gibt jedoch immer wieder Situationen, wo man die Ursache einer bestimmten Warnmeldung eines IDS verifizieren möchte. Im Kurs analysieren wir mit **zahlreichen Übungen** und entsprechenden Tracefiles verschiedene Angriffe auf Paketebene.

Interview mit Walter Hofstetter, Autor von «The Packet Factor»

Rolf: Ich habe deinen Pilotkurs besucht, ein geniales Training, das zeigt, wie Wireshark auch im Bereich der Netzwerksicherheit eingesetzt werden kann. Sehr spannend sind auch die Möglichkeiten, mit Wireshark die Muster verschiedener Intrusion Events und Attacken mit manipulierten Paketen erkennen zu können.

Walter: Wir verwenden im Kurs **Kali Linux** und zahlreiche weitere Tools, welche oft für Angriffe verwendet werden. Auch sogenannte **Man-in-the-Middle (MITM) Attacken** werden simuliert und analysiert.

Rolf: Dein Kurs wird ja öffentlich bei **AnyWeb Training** in Oerlikon oder als Firmenkurs angeboten, wo ich auch meine öffentlichen Wireshark Protokoll Kurse durchführe. Welche Voraussetzungen sollte nun ein Teilnehmer für **«The Packet Factor»** mitbringen?

Walter: Der Kurs richtet sich an Spezialisten im Bereich **Netzwerk-Security** mit entsprechenden Erfahrungen, aber auch an Einsteiger. Nicht unbedingt erforderlich, jedoch hilfreich sind auch Kenntnisse im Bereich **Routing / Switching**, sowie **Wireshark** und **Linux Command Line.**

Rolf: Letzte Frage - **Warum sollte ein Netzwerk-Security-Spezialist diesen Kurs besuchen?**

Walter: Ich weiss aus eigener Erfahrung, dass diese Spezialisten in ihrem Daily Business sehr eingespannt sind; die Anzahl und Vielfalt der Netzwerk-Attacken nehmen rasant zu und werden immer raffinierter. Es fehlen Zeit und Kenntnisse, den Hintergrund von IDS-Meldungen zu erkunden. Der Kurs eröffnet eine **neue Sicht und verbessert das Verständnis** für die ganze Thematik Intrusion Detection and Prevention. Dieser Kurs erweitert den Horizont ungemein, und es lohnt sich, dafür die zwei Tage Zeit zu nehmen.

Rolf: Meine Gratulation zu dem neuen Kurs. Ich wünsche dir und den Teilnehmern viel Erfolg damit.

Unsere Wireshark-Protokoll-Kurse & andere Events

- **Öffentliche Kurse in der Schweiz** → Zur Anmeldung bei AnyWeb
  Bei AnyWeb Training in Zürich
- **Öffentliche Kurse in Österreich** → Zur Anmeldung bei ARROW
  Bei Arrow ECS GmbH in Wien
- **Öffentliche Kurse in Deutschland** → Zur Anmeldung bei ALSO
  Remote Kurse bei ALSO
- **Übersicht aller öffentlicher Kurse** → Kurse Leutert NetServices

Unsere Spezialität sind Firmenkurse oder Tech-Sessions nach ihren Wünschen zu den Themen:

- **Einführung Netzwerkanalyse, Wireshark Tipps & Tricks, TCP/IP, QUIC, WLAN, VoIP und IPv6**

- YouTube Webinar (1h) **Troubleshooting WLANs mit Wireshark** aufgezeichnet durch onway.
- YouTube Webinar (1h) **Wird QUIC der Nachfolger von TCP?** aufgezeichnet durch onway.

Unser Newsletter Archiv finden sie unter: https://www.netsniffing.ch/de/wireshark-infos/newsletter

Es würde uns freuen, Sie in einem unserer Kurse begrüssen zu können.

Have fun and enjoy sniffing, Rolf Leutert