SEARCH DECIPHER ALERT!

OMR 150

Network Traffic Analysis Made Easy

DATE	14-16 January 2019
TIME	8:00 a.m. – 5:00 p.m.
VENUE	Al Falaj Hotel, Muscat

Looking at who sent what, when and where!
A 03 day, practical course designed to give you a thorough understanding of Network Traffic Analysis which is essential in identifying malicious communications and troubleshooting devices and applications.

Who should Attend?

IT Executives, IT Managers, Incident Response Team Members, Information Security Analysts

What will you learn?

- How networking works at the packet level.
- Interpreting packet data at a fundamental level in hexadecimal or binary.
- Analyzing packets on the command line with tcpdump.
- Basic analysis features of Wireshark.Reducing capture files with Berkeley packet filters and Wireshark display filters.
- Interpreting common network and transport layer protocols like IP, ICMP, TCP, and UDP.
- Interpreting common application layer protocols like HTTP, DNS, SMTP, and more.
- Normal and abnormal stimulus and response patterns for common protocols.
- How common network attacks are seen by an intrusion detection systems.
- Techniques for investigating security alerts using packet data.
- How malware communicates on the network.

Participants must have working knowledge of TCP/IP and be familiar with the use of Linux commands such as cd, sudo, pwd, ls, more, less, tcpdump

For more information & registrations please contact Ed at **edd@bposllc.com**

Programme Partner

bpos GLOBAL

Supporting Partner

RCC

EGUARDIAN™ OMAN

OMR 150

Details of the course

DAY 1

A refresher or introduction to TCP/IP, depending on your background and prior knowledge.
We will cover the basics of TCP/IP communication models, theory of bits and bytes, and the use of Wireshark and tcpdump.

DAY 2

Explores Berkeley packet filters and Wireshark display filters further.
We proceed with our exploration of the TCP/IP which will give you the ability to interpret common network and transport layer protocols like IP, ICMP, TCP, and UDP. This will also give you the skills to analyze your own traffic and interpret common application layer protocols such as HTTP, DNS and SMTP not just in theory and function, but from the perspective of an attacker and defender.

DAY 3

How common networks are seen by an intrusion detection system.
This process will give you an indepth knowledge about these detection systems and how they work to identify breaches and how malware communicates on a network We will then move on to discuss various techniques available for investigation using packet data. At the end of day 3 you will be able to troubleshoot using different searching methods and even build your own alert mechanism.

** Morning and evening snacks and lunch will be provided on all 03 days*

ABOUT THE TRAINER

Trained under the Volatility Foundation & SANS Institution in the US and with over 17 years of experience in secure network design, penetration testing, incident response, forensics and malware reverse engineering, Shihan has been provided technology consulting including architectural guidance to many corporates and government sector organizations

Shihan ANNON
Principal Consultant

For more information & registrations please contact Ed at **edd@bposllc.com**

Programme Partner

bpos GLOBAL

Supporting Partner

RCC

EGUARDIAN™ OMAN