3 Day Hands-on Training

Network Forensics *via* Packet Analysis

Course Outline

DAY 1 – SESSIONS AND LAB WORK

1. **Introduction to Protocol Analysis**

2. **The functions of a Protocol Analyser**

3. **Installing Wireshark Protocol Analyser**

Lab Work:

L3.a Installation of Protocol Analyser Tool

4. **What are Dissectors?**

4.1 Resolution Process – Dissectors
4.2 Understanding Dissectors
4.3 Dissector Tables, Use of Dissectors
4.4 List of Dissectors
4.5 The Core engine of the Analyser
4.6 Protocol identifying parameters & Protocol Structure

Lab Work:

L4.a Demonstration of Dissectors
L4.b Find the various parameters of Protocols/Applications on a Network

5. **Traffic capturing methods**

5.1 Capture to Ring Buffer
5.2 Capture Filters
5.3 Display Filters
5.4 Capture formats & conversions
5.5 Time Display Formats

Lab Work:

L5.a. Capture Traffic to/from the Hardware Address using the Ring Buffer method and Capture filter method.
L5.b Set Time Display format and trace delays in the packet transfer process.

6. Analyse ARP Traffic

6.1 Analysing ARP Traffic
6.2 ARP Overview
6.3 ARP Packet Structure
6.4 Filter on ARP Traffic

Lab Work:

L6.a Capture and Analysis of ARP packets,
L6.b ARP Padding, Layer 2 Broadcast identification,
L6.c Need for L2 broadcasting,
L6.d Encapsulation process,
L6.e Analysing ARP Payload

7. Analyse ICMP traffic

7.1 Analysing ICMP Traffic
7.2 ICMP Overview
7.3 ICMP Packet Structure
7.4 Filter on ICMP Traffic
7.5 ICMP Type numbers, Code numbers
7.6 TTL Value, TTL Expired in Transit

Lab Work:

L7.a Capture ICMP traffic and analyse the packets for Type number and Code number of the ICMP packet captured.

8. Saving / Retrieving Traces

8.1 Capturing Traffic on the cabling system
8.2 Opening Trace Files
8.3 Processing Packets based on powerful filtering system
8.4 The Changing Status Bar

Lab Work:

L8.a Capture traffic on Cabling system and save it to the Disk.
L8.b Open Existing Capture files into Packet Analyser
L8.c Filter the traffic with specific Parameters.
L8.d Understand the Status bar while capturing the packets.

---------- End of Day – 1----------

DAY 2 – SESSIONS AND LAB WORK

9. Coloring Techniques

9.a Coloring Techniques
9.b The Navigation Techniques
9.c Tracing packets based on various Characteristics
9.d Build Permanent Coloring Rules
9.e Identify a Coloring Source
9.f Mark Packets of Interest

Lab Work:

L9.a Capture / Open Trace files
L9.b Find, Mark, Save, and Colorize Packets

10. Filtering traffic using Display Filters

10.a How to configure Display Filters
10.b Filtering traffic using Display Filters
10.c Build Filters Based on Packets
10.d Display Filter Syntax

Lab Work:

L10.a Capture live packets.
L10.b Filter the traffic using display filters.
L10.c Use various display filter parameters and analyse.

11. Analysing DHCP Traffic

11.a Analysing DHCP Traffic
11.b DHCP packet structure
11.c Discover, Offer, Request and Acknowledgement packets
11.d Flooded Broadcast packet identification
11.e DHCP packet analysis
11.f The significance of <bootp> packet

Lab Work:

L11.a Capture and analyse DHCP DORA process packets,
L11.b Analyse the DHCP Error Message packet,
L11.c Leasing Parameters

12. Analyse DNS Traffic

12.a Analysing DNS Traffic
12.b DNS Overview
12.c DNS Packet Structure
12.d DNS Queries
12.e Filter on DNS Traffic
12.f The Opcode values and its meaning
12.g Analyze Normal/Problem DNS Traffic
12.h UDP 53 and TCP 53 packet parameter analysis

Lab Work:

L12.a Installation of DNS Server,
L12.b Creating zone and resource records,
L12.c Capturing the DNS Traffic,
L12.d Analyse DNS Query & Response,
L12.e Unusual DNS packets.

13. Analysing IPV4 Traffic

13.a Analysing IPv4 Traffic
13.b IPv4 Overview
13.c IPv4 Packet Structure
13.d Analyze Broadcast/Multicast Traffic
13.e Filter on IPv4 Traffic
13.f IP Protocol Preferences

Lab Work:

L13.a Capture and Analyse the Network Layer Header, Source IP & Destination IP
L13.b Time difference between request and response
L13.c IPV4 parameters

14. Analysing UDP Traffic

14.a Analysing UDP Traffic
14.b UDP Overview
14.c Watch for Service Refusals
14.d UDP Packet Structure
14.e Filter on UDP Traffic
14.f Follow UDP Streams to Reassemble Data

Lab Work:

L14.a Capture UDP Traffic
L14.b Analyse source port and destination port

---------- End of Day – 2----------

DAY 3 – SESSIONS AND LAB WORK

15. Analysing TCP Protocol

15.a TCP Overview
15.b The TCP Connection Process
15.c TCP Handshake Problem
15.d TCP Packet Structure
15.e Analysis of TCP Flags
15.f The TCP Sequencing/Acknowledgment Process
15.g Packet Loss Detection
15.h Retransmission Detection
15.i Out-of-Order Segment Detection
15.j Filter on TCP Traffic and TCP Problems
15.k Follow TCP Streams to Reassemble Data
15.l Determining the Next Sequence Numbers
15.m Understanding Packet size

Lab Work:

L15.a Capture the packets of TCP 3 way handshake and analyse Sequence numbers
L15.b Port numbers and Acknowledgement numbers
L15.c Explain each parameters in the TCP Flags.

16. Analysing HTTP

16.a Analysing HTTP Traffic
16.b HTTP Overview
16.c HTTP Packet Structure
16.d Filter on HTTP Traffic
16.e HTTP Statistics

Lab Work:

L16.a Capture and Analyse HTTP packets:
- i. Source IP,
- ii. Destination IP,
- iii. Source and Destination Port numbers
- iv. Packet fragmentation details,
- v. Size of the fragment

17. Analysing SSL Encrypted Traffic

17.a Analysing SSL-Encrypted Traffic (HTTPS)
17.b Examining SSL/HTTPS Traffic
17.c Filter on SSL

Lab Work:

L17.a Capture and analyse the SSL encrypted Traffic
L17.b Analyse SSL handshake process from the Capture.

18. Analysing File Transfer Protocol (FTP)

18.a FTP Overview
18.b FTP Packet Structure
18.c Analyze FTP Control Connections
18.d Analyze FTP Data Connections
18.e Filter on FTP Traffic

Lab Work:

L18.a Capture and analysis of FTP Traffic
L18.b Control Connections and Data connection handshakes
L18.c Identify Clear Text Password in FTP Traffic and the TCP handshake
L18.d Tear down process for FTP traffic.

---------- End of Day – 3----------

Certification

At the end of the course, candidates can take an on-line examination (50 MCQ plus Two Scenario Analysis). Those who obtain 43 correct answers in MCQ and answer both the Scenario questions correctly will be awarded

CERTIFICATE IN NETWORK FORENSICS via PACKET ANALYSIS

Exams are conducted by and Certificates are awarded by: