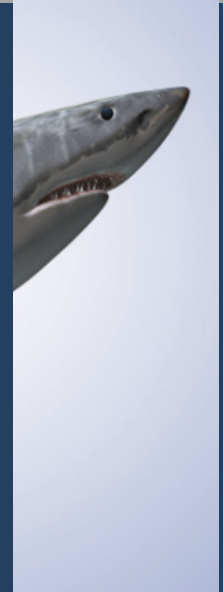


Core 2

Shark and Shark University™



Copyright 2009 Protocol Analysis Institute, Inc.




SHARK
UNIVERSITY

Table of Contents

Recommended Prerequisite Course

Core 1: Analyzing TCP/IP Networks with Wireshark™

About the Course Author/Wireshark Founder

Course Logistics

Course Content

Course Appendices/Supplements

Using the Trace File Log Book

Section 1: Analysis Overview

Analysis Tasks

Wired v. Wireless Analysis

Capturing Traffic

Opening Trace Files

Processing Packets

Resources for Analysts

Data Flow Overview

Analyzing Hubbed Networks

Analyzing Switched Networks

Hubbing Out

- Analyzer Agents

- Port Spanning/Mirroring

- Lab 1: Switched or Not Switched?

 - Trace File: trace01.pcap

Analyzing Routed Networks

Analyzing WAN Links

Analyzing Full-Duplex Links

Analyzing Wireless Networks

Dual Captures

Capturing in Stealth Mode

- Lab 2: One-Way Communications

 - Trace File: trace02.pcap

Section 2: Normal Network Communications

When Everything Goes Right

The Multi-Step Resolution Process

Port Number Resolution

Name Resolution

Location Resolution

Local – MAC Address Resolution

Remote – Route Resolution

Remote – MAC Address Resolution for a Gateway

Building the Packet

Lab 3: Normal DNS Communications [*GROUP LAB*]

Trace File: trace03.pcap

Lab 4: Normal DHCP Communications [*GROUP LAB*]

Trace File: trace04.pcap

Lab 5: Normal TCP Communications [*GROUP LAB*]

Trace File: trace05.pcap

Lab 6: Normal HTTP Communications [*GROUP LAB*]

Trace File: trace06.pcap

Lab 7: Normal FTP Communications [*GROUP LAB*]

Trace File: trace07.pcap

Lab 8: Normal POP Communications [*GROUP LAB*]

Trace File: trace08.pcap

Lab 9: Normal SMTP Communications [*GROUP LAB*]

Trace File: trace09.pcap

Lab 10: HTTP-HTCIA

Trace File: trace10.pcap

Lab 11: SMTP Connect

Trace File: trace11.pcap

Section 3: Causes of Performance Problems

Where Network Faults Occur

Time is of the Essence

Lab 12: DNS Errors

Trace File: trace12.pcap

Section 4: Wireshark Functions for Troubleshooting

Pre-Defined Coloring Rules

Basic IO Graphs

Advanced IO Graphs

Lab 13: IO Graphing

Trace File: trace13.pcap

Delta Time Value

Lab 14: Identifying Delays

Trace File: trace14.pcap

Expert System

Lab 15: FTP Expert Information

Trace File: trace13.pcap (originally used in Lab 13)

Look Who's Talking

Follow the Stream

Graph Bandwidth Use, Round Trip Time and TCP Performance

Throughput Graph

Round Trip Time (RTT) Graph

TCP Time/Sequence Graph

Flow Graphing

VoIP Graphing and Playback

Statistics (Various)

Section 5: Latency Issues

The Five Primary Points in Calculating Latency

Plotting High Latency Times

Lab 16: Slow HTTP File Download

Trace File: trace14.pcap (used in Lab 14) and trace16.pcap

Free Latency Calculators

Use the frame.time_delta Filter

Lab 17: Identifying Delays

Trace File: trace13.pcap

Section 6: Packet Loss and Retransmissions

Packet Loss and Recovery – UDP v. TCP

Previous Segment Lost Events

Duplicate ACKs

TCP Retransmission and Fast Retransmissions

Out-of-Order Segments

Selective ACKs

Lab 18: Packet Loss and Recovery

Trace File: trace18.pcap

Section 7: Misconfigurations and Redirections

Visible Misconfigurations

Lab 19: Mad User

Trace File: trace19.pcap

Don't Forget the Time!

Lab 20: Ugly Searches

Trace File: trace20.pcap

Section 8: Dealing with Congestion

TCP Receive Windows

Shattered Windows

Lab 21: TCP Window Issues

Trace File: trace21.pcap

Flooded Out

Lab 22: Open the Flood Gates

Trace File: trace22.pcap

Dual Capture Techniques

Lab 23: Command-Line Tools

Trace File: Not required.

Section 9: Network Baselines

Your First Task When You Leave Class

Section 10: Additional Troubleshooting Labs

Lab 24: Slow Browsing

Trace File: trace24.pcap

Lab 25: DHCP Slow

Trace File: trace25.pcap

Lab 26: Bad FTP

Trace File: trace26.pcap

Lab 27: FTP Fail

Trace File: trace27.pcap

Lab 28: POST no Bills

Trace File: trace28.pcap

Lab 29: Poisoned

Trace File: trace29.pcap

Lab 30: Client Frustrated

Trace File: trace30.pcap

Section 11: Setting Up Your Security Lab

Network Forensics and Security

Obtaining Evidence Using a Honeypot

Lab 31: Blaster Traffic

Trace File: trace31.pcap

Section 12: Unusual Network Communications

- Vulnerabilities in the TCP/IP Resolution Processes
 - Port Resolution Vulnerabilities
 - Name Resolution Process Vulnerabilities
 - MAC (Media Access Control) Address Resolution
- Route Resolution
- Spotting Unacceptable Traffic
 - Lab 32: Reconnaissance Underway
 - Trace File: trace32a.pcap and trace32b.pcap

Section 13: Reconnaissance Processes

- Port Scans
 - TCP Scan Responses
 - UDP Scan Responses
- Mutant Scans
- IP Scans
 - Lab 33: IP Scan
 - Trace File: trace33.pcap
- Application Mapping
- OS Fingerprinting
 - Lab 34: Unusual Scan
 - Trace File: trace34.pcap

Section 14: Analyzing ICMP Traffic

- ICMP Types and Codes
- ICMP Discovery
 - Lab 35: ICMP Traceroute
 - Trace File: trace35.pcap
- Route Redirection
 - Lab 36: ICMP Redirection
 - Trace File: trace36.pcap
- Dynamic Router Discovery
- Service Refusal
- OS Fingerprinting
 - Lab 37: Unusual ICMP Traffic
 - Trace File: trace37.pcap
 - Lab 38: ICMP Everywhere
 - Trace File: trace38.pcap

Section 15: TCP Security

TCP Segment Splicing

TCP Fake Resets

Lab 39: Reassembling TCP Splices

Trace File: trace39.pcap

Section 16: Address Spoofing

MAC Address Spoofing

IP Address Spoofing

Lab 40: Spoofed Addresses

Trace File: trace40.pcap

Section 17: Building Firewall ACL Rules

Overview of ACL Rule Types

Lab 41: Building Firewall Rules

Trace File: trace41.pcap

Section 18: Signatures of Attacks

Signature Locations

Header Signatures

Sequencing Signatures

Payload Signatures

Lab 42: Finding a Known Signature

Trace File: trace42a.pcap and trace42b.pcap

Obtaining Signatures

Attacks and Exploits

Lab 43: Analyze a Bot-Infected System

Trace File: trace43.pcap

Password Cracks

Brute Force

Dictionary

Lab 44: Analyze a Password Crack Attempt

Trace File: trace44.pcap

Denial of Service Attacks

Host-Targeted Attack

Network-Targeted Attack

Command-Line Tools

Lab 45: Network Flood

Trace File: trace45.pcap

Redirections

ARP-Based Redirection

ICMP-Based Redirection

Lab 46: Man-in-the-Middle Poison

Trace File: trace46.pcap

Section 19: Additional Security Labs

Lab 47: Covert FTP Connection

Trace File: trace47.pcap

Lab 48: Dueling Honeypots

Trace File: trace48.pcap

Lab 49: Worm-Infected System

Trace File: trace49.pcap

Lab 50: Hidden Data

Trace File: trace50.pcap

Lab 51: Checking for Poisoner

Trace File: trace51.pcap

Lab 52: Cleartext Passwords

Trace File: trace52.pcap

Lab 53: Decrypt SSL Traffic with an RSA Key

Trace File: trace53.cap