
# Sharkfest 2013 Challenge

Download all Sharkfest 2013 Challenge trace files from
***www.wiresharktraining.com/sharkfest2013challenge.html***.



All those successfully completing the Packet Challenge will receive a “Certified Packet Whisperer” lapel pin and will be eligible for a drawing for an AirPcap Nx and Cascade Pilot Personal Edition license. Two Nx and Cascade Pilot PE licenses will be raffled off to qualified CPW entrants.

## HOW TO SUBMIT YOUR ANSWERS

Fill in your answers on the Answer Sheet (last page of this document) and return in the Challenge Answer Box at the Sharkfest 2013 Registration Desk no later than **noon Tuesday, June 18, 2013**.

# Sharkfest 2013 Challenge

## CHALLENGE #1: WHAT THE HECK?

Created by Phill Shade / Forensic Engineer / Merlion's Keep Consulting

### TRACE FILE(S)

Download this trace file from *www.wiresharktraining.com/sharkfest2013challenge.html*.

**challengescan.pcapng** (270 KB)

### BACKGROUND

This capture file was taken from a very large and long-time established network that had been considered very stable and unchanging. The network administrator has given you this file that contains what he considers "suspicious" behavior and has asked you to evaluate it.

### QUESTIONS

1. **What is the IP address of the scanning host?**
2. **What is the IP address of the target host?**
3. **Which TCP port is open on the target?**
4. **Which ICMP packets contain non-standard Type/Code numbers?**
5. **What software is used to scan the target?**

### SUBMIT YOUR ANSWERS

Fill in your answers on the Answer Sheet (last page of this document) and return in the Challenge Answer Box at the Sharkfest 2013 Registration Desk no later than **noon Tuesday, June 18, 2013**.

# Sharkfest 2013 Challenge

## CHALLENGE #2: CURSED

Created by Laura Chappell, Wireshark University

### TRACE FILE(S)

Download this trace file from *www.wiresharktraining.com/sharkfest2013challenge.html*.

**challengewhatsup.pcapng** (4.43 MB)

### BACKGROUND

Sure, Scott is one of your best friends at the company, but he's always asking for computer help. No amount of training seems to work. Today he sent you a text message to complain that his computer hard drive light is always blinking on – even when he's not touching the keyboard. With a promise of decent drinks after work, you remotely connected to his machine and started capturing traffic. Sure enough – loads of packets were flying around. Just then, Scott arrived in your office.

Hmmm… Scott is here, but his computer seemed to have a lot of network activity going on. You stopped the trace to see what happened in the background on his system.

### QUESTIONS

1. **How many different IP hosts is Scott's machine communicating with?**
2. **What is the average packets per second rate seen in this trace file?**
3. **How many HTTP POST requests did Scott's machine send?**
4. **What location information is contained in the POST to scanscout.com?**
5. **What application appears to be generating these GET/POST requests?**
6. **Find, export and reassemble load_small.png. What shape is in the image?**

### SUBMIT YOUR ANSWERS

Fill in your answers on the Answer Sheet (last page of this document) and return in the Challenge Answer Box at the Sharkfest 2013 Registration Desk no later than **noon Tuesday, June 18, 2013**.

# Sharkfest 2013 Challenge

## CHALLENGE #3: FTPS ANALYSIS

Created by Larry Greenblatt

### TRACE FILE(S)

Download this trace file from *www.wiresharktraining.com/sharkfest2013challenge.html*.

**challengeftp1.pcapng (10 KB)**
**challengeftp2.pcapng (11 KB)**

### BACKGROUND

A customer needed a secure file transfer application put in place. These two trace files illustrate the separate options they have tested – implicit FTPS and explicit FTPS.

### QUESTIONS

1. **What is the IP address of the server?**
2. **Which trace file illustrates implicit FTPS?**
3. **Which trace file illustrates explicit FTPS?**
4. **What IP address initiated the data connections in the trace files?**
5. **What port numbers are used for the data connection in each trace file?**

### SUBMIT YOUR ANSWERS

Fill in your answers on the Answer Sheet (last page of this document) and return in the Challenge Answer Box at the Sharkfest 2013 Registration Desk no later than **noon Tuesday, June 18, 2013**.

# Sharkfest 2013 Challenge

## CHALLENGE #4: OUCH!

Created by Phill Shade / Forensic Engineer / Merlion's Keep Consulting

### TRACE FILE(S)

Download this trace file from *www.wiresharktraining.com/sharkfest2013challenge.html*.

**challengeattack.pcapng** (72 KB)

### BACKGROUND

These capture files were taken from a network experiencing a "Zero-day" attack and was completely overwhelmed. It is also reported that some of the Nodes within the network appear to be unable to update their Anti-Virus/Security software. The Network Administrator has given you this file that contains what he considers "Suspicious" behavior and has asked you to help. The Administrator can tell you that 141.157.228.12 is a Server and that 10.1.1.31 is a client machine.

### QUESTIONS

1. **What file transfer application is seen in this trace file?**
2. **What is the IP address of the host that is receiving a file?**
3. **What is the name of the file that is being transferred?**

### SUBMIT YOUR ANSWERS

Fill in your answers on the Answer Sheet (last page of this document) and return in the Challenge Answer Box at the Sharkfest 2013 Registration Desk no later than **noon Tuesday, June 18, 2013**.

# Sharkfest 2013 Challenge

## CHALLENGE #5: DNS TROUBLE

Created by Jasper Bongertz, Cassidian CyberSecurity

### TRACE FILE(S)

Download this trace file from *www.wiresharktraining.com/sharkfest2013challenge.html*.

**challengednstrouble.pcapng** (2.6 KB)

### BACKGROUND

After a maintenance window on the day before where several servers had been upgraded to a newer operating system a lot of trouble tickets come in. Users complain that connecting to web sites and other services take a long time now, especially when connecting for the first time.

A quick check on all relevant switches, routers and servers reveals no bottlenecks in CPU, memory or disk I/O, so of course the tickets are handed over to the network guys – it must be the network, right? Finally, one of the network engineers comes to you and asks you to help him with analyzing a trace he took. He suspects that there is something wrong with the DNS name resolution, but even after filtering away most of the other stuff he can't put his finger on it. Can you take a look at his trace to find out what happened and if this is a network problem at all?

### QUESTIONS

1. **What FQDN is the client attempting to resolve?**
2. **To what IP address is the first recursive DNS query sent?**
3. **To what IP address is the second recursive query sent?**
4. **The trace file includes authoritative DNS servers responsible for what top level country code domain?**
5. **What is the IP address of the host that is responsible for the long delay in resolving the host name?**

### SUBMIT YOUR ANSWERS

Fill in your answers on the Answer Sheet (last page of this document) and return in the Challenge Answer Box at the Sharkfest 2013 Registration Desk no later than **noon Tuesday, June 18, 2013**.

# Sharkfest 2013 Challenge

## CHALLENGE #6: VOIP RECONSTRUCTION

Created by Phill Shade / Forensic Engineer / Merlion's Keep Consulting

### TRACE FILE(S)

Download this trace file from *www.wiresharktraining.com/sharkfest2013challenge.html*.

**challengevoip.pcapng** (166 KB)

### BACKGROUND

This capture file was collected from a recently installed VoIP network that is experiencing performance issues and you have been asked to evaluate it and recommend corrective action.

### QUESTIONS

1. **What three UDP-based protocols are used for the VoIP call and call setup?**
2. **With what three IP addresses is 45.210.3.90 communicating?**
3. **What SIP error code is seen in this trace file?**
4. **What is the stated cause of this SIP error?**

### SUBMIT YOUR ANSWERS

Fill in your answers on the Answer Sheet (last page of this document) and return in the Challenge Answer Box at the Sharkfest 2013 Registration Desk no later than **noon Tuesday, June 18, 2013**.

# Sharkfest 2013 Challenge

## CHALLENGE #7: BOYSCOUT

Created by Alex Weber

### TRACE FILE(S)

Download this trace file from *www.wiresharktraining.com/sharkfest2013challenge.html*.

**challengeboyscout.pcap** (17 MB)

### BACKGROUND

Information leaks from all sorts of places...
Consider the name of this challenge when you view the trace file.

### QUESTIONS

1. **What is the secret message?**

### SUBMIT YOUR ANSWERS

Fill in your answers on the Answer Sheet (last page of this document) and return in the Challenge Answer Box at the Sharkfest 2013 Registration Desk no later than **noon Tuesday, June 18, 2013**.

# Sharkfest 2013 Challenge

## ANSWER SHEET

Fill in your answers on this page and turn in **just this page** in the Challenge Answer Box at the Sharkfest 2013 Registration Desk no later than noon Tuesday, June 18, 2013. Use the feedback area to make any notes or add comments about your answers, if desired.

Name: _____ Email: _____

### CHALLENGE #1: WHAT THE HECK?

Answer 1: _____

Answer 2: _____

Answer 3: _____

Answer 4: _____

Answer 5: _____

FEEDBACK/COMMENTS

### CHALLENGE #2: CURSED

Answer 1: _____

Answer 2: _____

Answer 3: _____

Answer 4: _____

Answer 5: _____

Answer 6: _____

FEEDBACK/COMMENTS

### CHALLENGE #3: FTPS ANALYSIS

Answer 1: _____

Answer 2: _____

Answer 3: _____

Answer 4: _____

Answer 5: _____

FEEDBACK/COMMENTS

# Sharkfest 2013 Challenge

## CHALLENGE #4: OUCH!

Answer 1: _____

Answer 2: _____

Answer 3: _____

FEEDBACK/COMMENTS

## CHALLENGE #5: DNS TROUBLE

Answer 1: _____

Answer 2: _____

Answer 3: _____

Answer 4: _____

Answer 5: _____

FEEDBACK/COMMENTS

## CHALLENGE #6: VOIP RECONSTRUCTION

Answer 1: _____

Answer 2: _____

Answer 3: _____

Answer 4: _____

FEEDBACK/COMMENTS

## CHALLENGE #7: BOYSCOUT

Answer 1: _____

FEEDBACK/COMMENTS