# WIRESHARK CHALLENGE

**1.CHALLENGE #1: WHAT THE HECK?**

**TRACE FILE**: challengescan.pcapng

**BACKGROUND**: This captured file was taken from a very large and well-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 opens on the target?

4. Which ICMP packets contain non-standard Type/Code numbers?

5. What software is used to scan the target?

**2.CHALLENGE #2**: CURSED

**TRACE FILE**: challengewhatsup.pcapng

**BACKGROUND**: Sure, Scott is one of the 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 though he’s not touching the keyword. 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 seems 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?

**3. CHALLENGE #3: FTPS ANALYSIS**

**TRACE FILES**: challengeftp1.pcapng challengeftp2.pcapng

**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 illustrates implicit FTPS?

3. Which trace illustrates explicit FTPS?

4. What IP address initiated the data connections in the trace file?

5. What port numbers are used for the data connection in each trace file?

**4.CHALLENGE #4: OUCH!**

**TRACE FILE**: challengeattack.pcapng

**BACKGROUND**: These capture files were taken from a network that was 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 antivirus/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 the file?

3. What is the name of the file that is being transferred?

**5.CHALLENGE #5: DNS TROUBLE**

**TRACE FILE**: challengednstrouble.pcapng

**BACKGROUND**: After a maintenance window on the day before, when several servers had been upgraded to a newer operating system, a lot of trouble tickets have come in. Users complain that connecting to web sites and other services takes 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 DNS 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?

**6.CHALLENGE #6: VOIP RECONSTRUCTION**

**TRACE FILES**: challengevoip.pcapng

BACKGROUND: This captured 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?

**CHALLENGE #7: BOYSCOUT**

**TRACE FILES**: challengeboyscout.pcapng

**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?