**Template for the PIVOT Open Lab/Challenge Project:**

**Version 0.9**

Lab / Challenge Developers,

We have an eager audience of participants ready to try out your new lab/challenge - they just need a little info to get started. Please provide some basic details of your work by filling out this brief template.

Keep in mind that we encourage creativity and new ideas, so if your lab or challenge does not fit some of the questions below, that’s OK! Just let us know as much as possible about the special thing you’ve built. If you have any questions, please contact ????.

|  |
| --- |
| Title of Lab / Challenge: **File Carving Using Wireshark**  **The Basic Facts**  *Who?* Author’s Name: **Jeff Hanson**  Author’s Organization: **Damascus High School Academy of Information Technology**  *What?* Short description of the Lab/Challenge : **In this activity students will be taught through a video how to use Wireshark to view files transferred through HTTP. Wireshark supports carving files via HTTP, but not FTP. Students will be shown how to do both automatic and manual file carving. The students will then be challenged to use Wireshark to carve a file that was transferred via FTP.**  *Why?* Skills that can be learned from this Lab/Challenge: **Students will learn how to use Wireshark to read a packet capture file (.pcap, .pcapng) file to carve (extract) a file that was transferred via HTTP and FTP**  *Pre-Req?* Skills that are needed going into this Lab/Challenge: **Knowledge of Wireshark**  *Difficulty Level ? (circle one)* Introductory - **Moderate** - Advanced  *How long?* to Complete Instruction: **12 minute video**  to Complete Lab / Challenge: **approximately 30-45 minutes** |

|  |
| --- |
| **A little more detail**  *How does it work?*  - Type of Hands-on Lab / Challenge   * Step-by-Step Lab * Capture the Flag * **Solve the Puzzle: What file was transferred via FTP?** * Other. Please describe: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   - Scoring mechanism:   * No scoring (lab only) * **Shortest time wins** * Point-based system * Other. Please describe: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   *How many?*  - Is the Challenge / Lab for individuals or teams? **individual**  - If groups, what is the ideal team size? \_\_\_\_\_\_ people per team  - How much is "too much" - is there a maximum scale of number of participants for the challenge, given performance or other characteristics? Yes/No  Maximum number \_\_\_\_\_\_\_\_ people  *How will I learn*? - Instructional Method (check one or more)  🗹 Video   * Article / Presentation * None – the challenge explains itself * Other. Please describe: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Checklist**  *What you get:*  - Assets provided in this Lab / Challenge. (Please list all, such as pcap files, VM images, evidence files, etc.): **pcap files and a set of questions**  *What you need #1:*  **-** Infrastructure Requirements needed to run the Lab / Challenge (Please list all, including required devices such as PCs, tablets, local networking configuration, Internet connectivity, bypass of firewall or proxy restrictions, etc.): **Need computer with Wireshark, Internet access**  *What you need #2:*  **-** Assets needed in Advance for the Lab / Challenge (Please list all, such as virtual machines, operating system installs, application installations, etc.): **Need computer with Internet access to download video and files, need Wireshark to follow along and view packet capture files used in the instruction and hex editor.** |

|  |
| --- |
| **Wrapping it up**  Can you give us a longer narrative that tells us what makes the Lab / Challenge fun, interesting, and targets the development of useful information security skills?  **Students will learn how to view files that were transferred via HTTP and FTP. This is an important skill as it relates to viewing malware files transferred through various methods. Plus it will be exciting for students to learn how to carve files from individual packets.**  If you have had a chance to look at the existing challenges, can you suggest where your Lab/Challenge fits into that Roadmap or Sequence?  **This topic and challenge would fit in with the forensic analysis topic and would be considered an introduction to file carving.** |