Week 6 – Capture the Flag

Lab Answer Sheet

|  |
| --- |
| Full Names & PicoCTF UserIDs Lab Section#: 101-A |
| Hatice Senliler & hbs45 |
| Shanielle Hall & shani4255 |
| Cole Jackson & cwj36 |

**Record answers to the questions posed in the lab directions below.**

1.a.iii:

**→ We decided that all members would enter the info in real-time.**

1.b.iv:

**→ We reviewed each other’s documents and commented on any improvements I needed to make. - Shanielle**

**→ We switched our laptops and talked about the missing parts of the summary. - Hatice**

**1.c.iii: Our team’s strengths are communication, collaboration, and finishing on time efficiently. To improve our team, we can write our summary as we tackle the challenges.**

**1.d: Our team’s goals are to be more specific with summaries, and to attempt higher-level challenges.**

**2.b:** Document team efforts on the following pages. There are different pages for key categories.

**3.b:** For each of the categories on the following pages, copy and paste the template below and record detailed notes of your activities for challenges in each of the categories. Record all of your efforts, even if you do not successfully solve a problem.

**We attempted some medium challenges today, but while we were not able to solve any of them, we still learned about ssh and the commands used in tux. We were able to be more specific with our summaries, and we felt satisfied with the amount of challenges we completed today.**

***Your grade for this is based on your teamwork and the quality of your documentation, not the number of challenges you solve.***

**Challenge: SOAP**

**Category:** Web Exploration

**Points:** 0

**Started: 11:18** *(list date & time)*

**Ended: 11:29** *(list date & time)*

**Status:** **Surrendered** *Solved / Surrendered)*

**Summary: Cole found the hint about XML and we started to look for the XML external entity Injection in the developer tools of the web. Later we found the file in the js folder. Even though we had the file from the hint, we were able to figure out how to move forward. We couldn’t find the flag in the file and we were unable to run the file.**

**Challenge: vault-door-training**

**Category:** Reverse Engineering

**Points:**

**Started: 11:30** *(list date & time)*

**Ended: 11:32** *(list date & time)*

**Status:** Solved *Solved / Surrendered)*

**Summary: We downloaded the javascript file and searched through the file for the flag. Shanielle found the flag at the end of the Javascript file. There wasn’t much information to search through.**

**Challenge:** Trickster

**Category:** Web Exploitation

**Points:** 0

**Started: 11:36** *(list date & time)*

**Ended: 11:46** *(list date & time)*

**Status:** Surrender *Solved / Surrendered)*

**Summary: We could not find the flag after 10 minutes, so we surrendered. There was a linked website that had a place to upload images. It said that it only took pngs, but when Shanielle tried uploading a png it did nothing. We couldn’t find anything by inspecting the page either. So we just gave up.**

**Challenge:** Super SSH

**Category:** General Skills

**Points:** 1

**Started: 11: 47** *(list date & time)*

**Ended: 12:00** *(list date & time)*

**Status:** Solved *Solved / Surrendered)*

**Summary: We all tried to enter ssh** [**ctf-player@titan.picoctf.net**](mailto:ctf-player@titan.picoctf.net) **but in some cases, it didn’t work then Shanielle found out that we needed to add -p 51436 at the end of the line. Then we were able to log in with the password. Then we saw the flag in the terminal and it was solved.**

**Challenge:** First Grep

**Category:** General Skils

**Points:** 1

**Started: 12:02** *(list date & time)*

**Ended: 12: 04** *(list date & time)*

**Status:** Solved *Solved / Surrendered)*

**Summary: After reading through the instructions, we decided to search through the file using the ctrl+f function. Shanielle suggested the search bar which made our job easy without tiring ourselves.**

**Challenge:** scan surprise

**Category:** Forensics

**Points:**

**Started: 12:08** *(list date & time)*

**Ended: 12:10** *(list date & time)*

**Status:** Solved *Solved / Surrendered)*

**Summary: The file was compressed, so first we unzipped the file. This led to a QR code. We scanned the QR code and Shanielle realized the URL of the QR was the flag.**

**Challenge:** CanYouSee

**Category:** Forensics

**Points:** 1

**Started: 12:13** *(list date & time)*

**Ended: 12:20** *(list date & time)*

**Status:** Solved *Solved / Surrendered)*

**Summary: We downloaded the image but we weren’t able to find anything. However, after researching, we found out that we were supposed to decode the URL that was in the metadata. We then found the flag and submitted it.**