SHADØW
SYND1CATE

CTF 101 Workshop

Authored By: Collin Montenegro (Unkn0wn)

Twitter- @_Unkn0wn1
Instagram- @collinmontenegro

Purpose

The purpose of this lab is to provide some realistic examples of possible CTF problems that you will have to solve. This lab incorporates a handful of useful tools that you gain exposure to and can leverage for future CTFs!

Background

We have been monitoring our mortal enemies, the Legion of Light (LoL), for the past couple of weeks and were able to capture some network traffic from one of their remote facilities. However, we know that they don't just blatantly transfer sensitive information over the wire without some sort of encryption of covert actions. Your job as a Shad0w Synd1cate operative is to sift through the network traffic and find anything of interest. We are hoping you can find any information regarding the Legion of Light and what they may be up to. Are you up for the challenge?

Objective 0x01

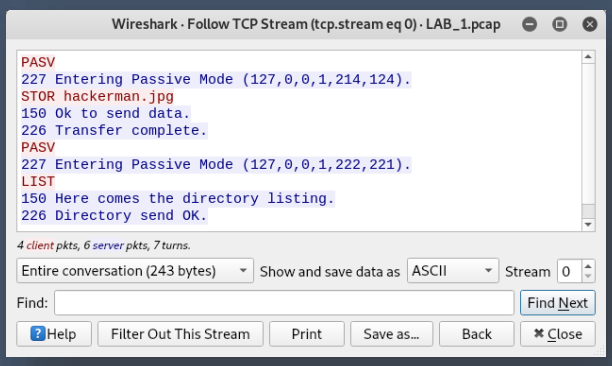
You are given a .pcap (LAB_1.pcap) of some FTP network traffic that we gathered from one of Legion of Light`s remote facilities. Legion of Light is known to use ***Steganography*** in order to covertly send messages in the clear. Your objective is to see if you can extract any data/information from the FTP traffic that could unveil any secret plans they may have against us!

What was the secret message that you uncovered from the traffic?

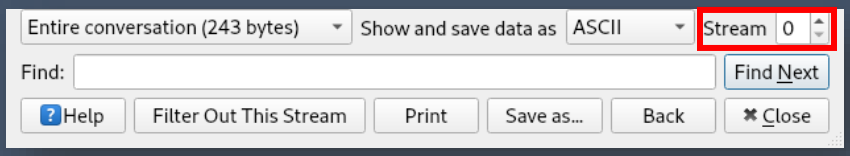
_____

Objective 0x01 - Walkthrough

1. Open the. pcap and find the beginning of the FTP traffic as seen in the "Protocol" Column. Right click on one of the FTP packets and select ***Follow > TCP Stream***. This will open up a separate window highlighting the data transferred for that specific TCP stream as seen below:



2. As you can see, this stream doesn't provide the actual data of the file that was transferred during this FTP session. Let's try a different FTP stream! To switch to the next stream, simply click on the up arrow located next to the word "Stream" within the TCP Stream window we just opened as seen below:



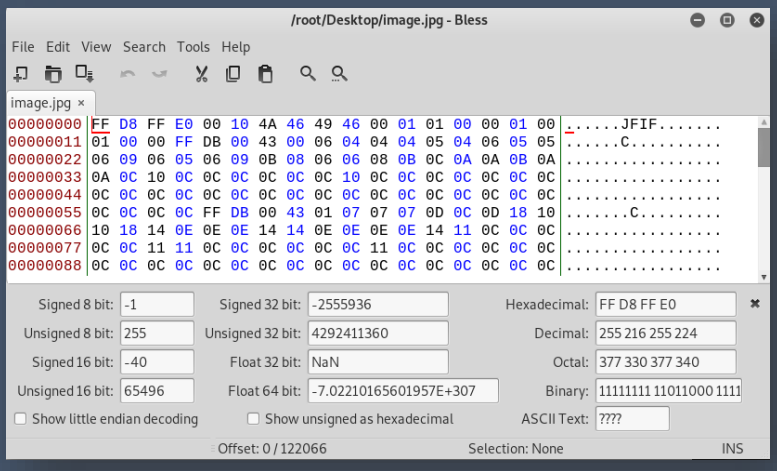
3. We are now seeing the actual data transfer stream! It appears that the file that was transferred was a .jpg image based on the file signature or "Magic Number" of ***JFIF*** that is displayed in the ASCII converted data located in the window. We now want to extract this image so we can open it up and see what it is. To do this change the "***Show and save data as***" field to ***raw*** and save it to your Desktop naming it whatever you prefer with a file extension of ***.jpg*** (Example: haxor.jpg).

4. Now that we have it saved, let's open it up! Ahhh we are faced with none other than our friend Elliot Alderson (Mr. Robot), but nothing of use. Remember we mentioned that Legion of Light tends to leverage steganography in order to transfer messages in plain sight. Maybe there is something embedded inside the image. Let's try and use a stego tool to see if we can extract something, but first lets take a look at the data to see if there is any useful information just sitting in plain ASCII. To do this you can use multiple tools/commands. Let's first try using ***Bless*** hex editor to view the image data. To do this, run the following commands:

 # Cd /root/Desktop

 # Bless <name of jpeg>.jpg

You should now see the following appear:



If you scroll through the data window you will see ASCII converted text. Do you see anything of interest there? Yes! It looks like the LoL stored a password inside the image data. This might come in handy when we attempt to extract any potential embedded files using our next tool, steghide!

Note: If you don't want to use Bless to view the ASCII output of the image data, you can also simply use the ***strings*** command which will also output all possible human readable data that may be embedded.

5. So we didn't see anything particularly interesting outside of the password listed, but there must be more to this! Let's see if there is anything embedded within the image by running a steganography tool called steghide. To do this, run the following command:

   # steghide extract -sf <name of jpg>.jpg

   When you run the above, we are prompted to type in a password…let's try and use the password we found sitting in the data.

   Voila! We were right, there was a hidden text file embedded in the image! Good thing we found this, we need to go inform our Shad0w Synd1cate members that a potential attack is near!

Objective 0x02

While monitoring other LoL network traffic, we managed to extract a .rar file of interest using methods done in the previous objective. But of course, LoL attempts to do their due diligence and they encrypted the .rar file. Your objective is to find a way to open up this .rar and see what may be inside!

What is the repeating phrase found inside the .rar file?

_____

Objective 0x02 - Walkthrough

1. As we know, the password to unlock the .rar file could be anything! Instead of manually typing in different passwords in an attempt to brute force it, let's use a password cracking tool such as ***John The Ripper***! The first thing we will need to do is attempt to extract the password hash for this .rar file. For this we will use one of John The Ripper's modules called ***rar2john***. To do this, run the following command:

   # rar2john /root/Desktop/Lab_2/LOL_Manifesto.rar > /root/Desktop/rar.hash

2. Now that we have the hash of the .rar file stored the rar.hash file, lets use John The Ripper's bruteforcing capability to attempt hundreds and thousands of passwords to see if it can find a match for the hash. To do this, run the following

   # john --wordlist= /usr/share/john/password.lst /root/Desktop/rar.hash

   The above command may take about a minute as it attempts hundreds of password attempts against the hash. After a short time, you are greeted by the password!

3. Now that we have the password, let's open up the .rar and see what is inside. Simply double click on the .rar file and select a folder to extract the files to. Once you do that, enter in the password.

Great job! You managed to crack the .rar and we found their manifesto inside! Wow….they really don't like us do they? :P

Conclusion

Great work fellow Shad0w Synd1cate operative! With your help, we were able to warn our fellow Shad0w members of an upcoming attack. We also managed to see LoL's manifesto that outlined how much they truly hate us!

While going through these objectives, you learned some valuable skills that can be used in different CTF events. Of course, these are just a few of the many tools out there, but these tools are definitely ones you will want to be comfortable with since they come in handy!