Conversation with:

Sofia Russo
Incident Responder

Cyber Defense Incident Responder Challenge Chat Transcript

Sofia sent:
Hello, @playerone! I'm Sofia Russo; I'm an Incident Responder here at the TryCyber Inter-Agency Response Team.

Welcome to the team! I'll be your mentor while you're interning with us. 😊

Sofia sent:
I'm going to be showing you how to perform the tasks of a **Cyber Defense Incident Responder**. I usually perform my daily tasks using a workstation like the **Ubuntu 22.04 Linux** workstation you are looking at now.

Sofia sent:
The tasks you will be doing today will require you to use **Wireshark**. Wireshark can be intimidating if you have not used it before. So let me know if you want a very brief tutorial on it.

Sofia sent:
So, are you ready to get started?

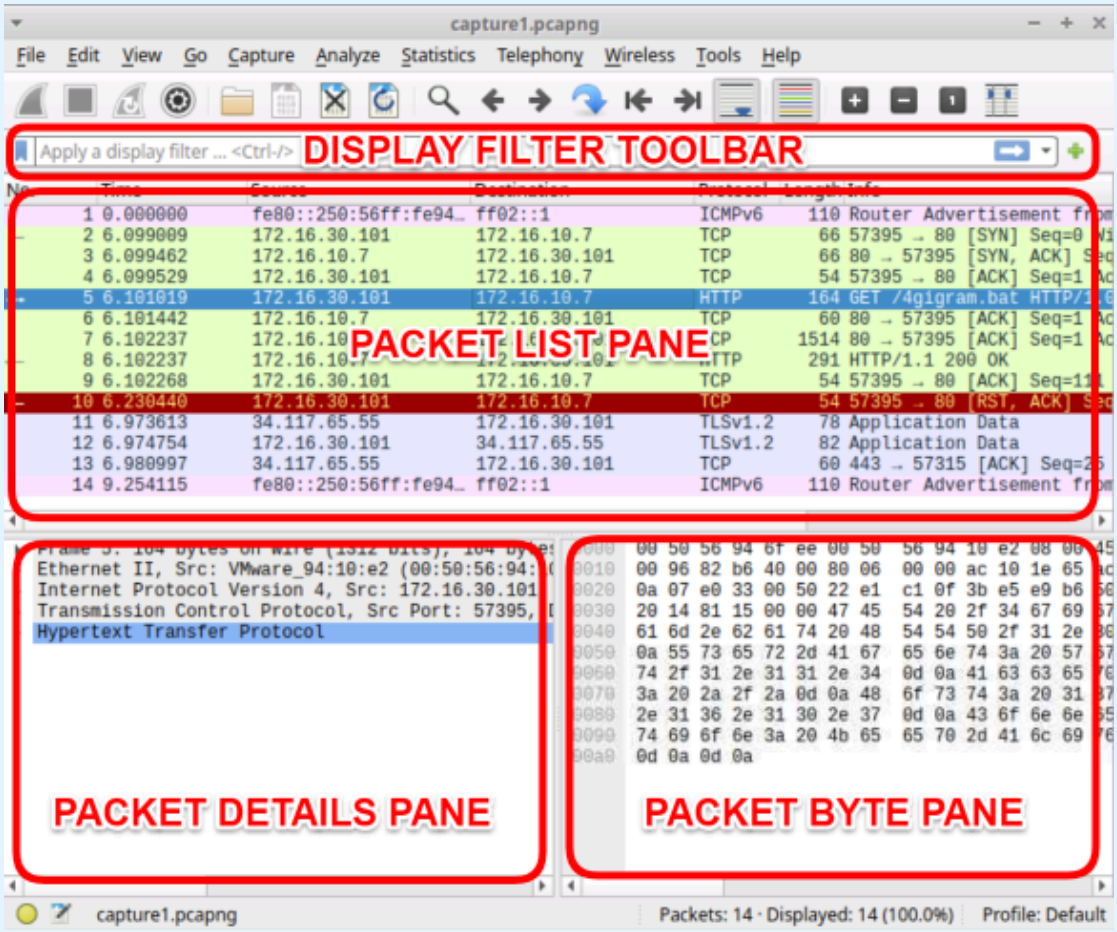
Participant sent:
Wireshark tutorial, please!

Sofia sent:
Wireshark is an open-source **packet analyzer**. It is an incredibly versatile and powerful tool that is commonly used for network analysis, debugging, and troubleshooting.

Sofia sent:
However, we will use only a small subset of Wireshark's features today. We will mostly use it to review previously captured network traffic and export any files we find interesting. As such, I'm only going to go over Wireshark's main user interface so you can confidently navigate it for today's tasks.

Sofia sent:
Here is a screenshot of Wireshark's main user interface that I've annotated...

Sofia sent:



Sofia sent:
While I've highlighted and named all the main parts of the user interface, we will only be using the **Display Filter Toolbar** and **Packet List Pane** today.

Sofia sent:
The **Packet List Pane** is a scrollable, sortable, and color-coded pane of all the packets in a packet capture. The **Display Filter Toolbar** allows us to filter what packets in the packet capture are displayed in the Packet List Pane.

Participant sent:
This looks complicated...

Sofia sent:
Well, I won't lie to you; packet analyzers and networking can be complicated. 😅

Sofia sent:
But for what we are doing today, we will be barely scratching the surface of all the information you see in that screenshot. So, if it looks like a bunch of alien text to you, that's fine! Trust me, that is how everyone feels when they are just starting.

Sofia sent:
Today, we will only be looking at small packet captures and filtering for the type of network traffic you are most likely to be familiar with, HTTP traffic, or more plainly, the type of network traffic that occurs when you visit a website.

Sofia sent:
And don't worry! I'll walk you through what I want you to do today step-by-step and give you all the details you'll need once we get into the tasks.

Participant sent:
Thanks! I'm ready to get started!

Sofia sent:
Great!

Sofia sent:
To give you some background on what I want your help with today, we have an incident response team that is on-site at an organization that has recently experienced a cyber-attack. And while you and I can't be on-site today, we can remotely assist the on-site team by helping them **collect intrusion artifacts** from **packet captures** they sent us.

Sofia sent:
Cyber Defense Incident Responders are very commonly tasked with collecting intrusion artifacts, such as malware samples and malicious scripts. Intrusion artifacts are some of the primary clues we use to try and figure out what happened when a cyber-attack occurs.

Sofia sent:
Thankfully, the organization that was attacked had some devices collecting network traffic. Otherwise, we would not have these packet captures, and it would be even more difficult to figure out what happened on their network.

Participant sent:
Good to know. How do we get started?

Sofia sent:
Well, I've taken the liberty of sifting through all of the packet captures the on-site team sent us already, and I picked two short, simple captures for you to work with today.

Sofia sent:
Each packet capture has one intrusion artifact in it, and for your tasks today, I'd like you to **extract those intrusion artifacts** for me.

Sofia sent:
I promise it is easier than it sounds!

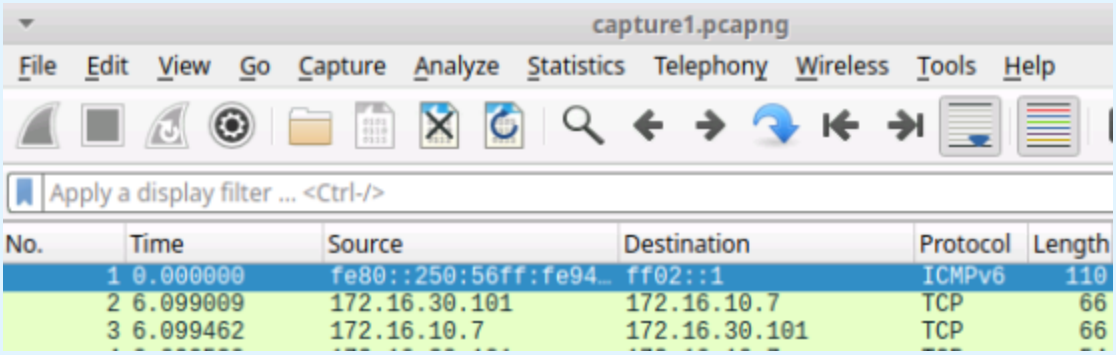
Sofia sent:
You can find the **two packet captures** in the `Materials` **folder** on the Desktop of this Ubuntu Linux workstation. The packet capture files are named `capture1.pcapng` and `capture2.pcapng`.

Sofia sent:
When it comes time to extract the intrusion artifact out of a packet capture, be sure to put it in the `Quarantine` **folder**, which is also on the Desktop.

Sofia sent:
Okay, that's enough talk. Let's open the first packet capture! You can do that by opening the `Materials` folder and **double-clicking** on `capture1.pcapng`. That will automatically open the packet capture in Wireshark.

Sofia sent:
It should look something like this...

Sofia sent:



Sofia sent:
Let me know when you've got it open.

Participant sent:
I've got it open!

Sofia sent:
Okay, let me briefly explain what you are seeing in the packet list pane (the colorful pane in the center).

Sofia sent:
There are 14 packets in this packet capture. Each packet is listed in a separate row in the packet list pane. If you look at the packet capture `Time`, you will notice that all of the packets were captured within roughly 9 seconds.

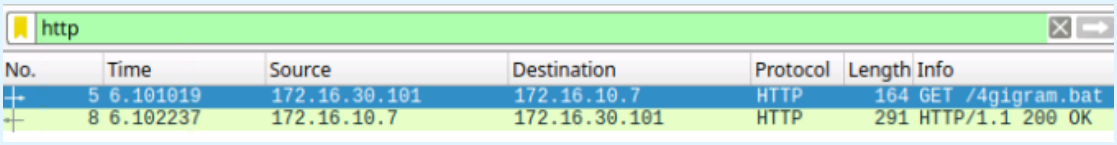
Sofia sent:
This capture mostly contains a **TCP/HTTP exchange** between a client (at the IP address `172.16.30.101`) and a web server (at the IP address `172.16.10.7`) hosting a malicious script. This exchange is color-coded green (rows 1-9 in the packet list pane). I happen to know this web server is hosting a malicious script based on other details I have from the on-site team.

Sofia sent:
To filter this down and make this exchange even simpler to look at, let's apply a display filter via the display filter toolbar, the text box near the top of the application.

Sofia sent:
Let's apply a display filter limiting it to just `http` packets. To do that, select the display filter toolbar, type in `http`, and hit `Enter` or `Return` on your keyboard.

Sofia sent:
Now you should have something that looks like this...

Sofia sent:



Participant sent:
I see the filtered results.

Sofia sent:
Okay, now that we've removed the noise, we can concentrate on the critical exchange here.

Sofia sent:
Look at the `Info` section of that first packet, `GET /4gigram.bat`. This is the client making an HTTP GET request to the server for the malicious script, `4gigram.bat`, I mentioned earlier. Then, in the `Info` section of the second packet, we see the server responding OK, confirming the download.

Sofia sent:
This is one example of how malicious scripts and malware can move around in a network. There are numerous and far more sneaky ways than this though, so don't think it is always this easy to find!

Sofia sent:
Anyway, now that we've reviewed this packet capture, let's use Wireshark's ability to **export objects** out of packet captures to extract the malicious `4gigram.bat` script.

Sofia sent:
To do this, select `File` at the top left of the application, then in the drop-down menu select `Export Objects > HTTP...`.

Sofia sent:
Then you should see a new window pop up that contains a list of all the HTTP objects in the packet capture, select the malicious `4gigram.bat` script, and then click the `Save` button in the bottom right corner.

Sofia sent:
Be sure to save it to the `Quarantine` folder on the Desktop! That is where the specialist who will examine the intrusion artifacts will expect it to be.

Participant sent:
Done. What's next!

Sofia sent:
Nice! One down and one to go!

Sofia sent:
Uhh... okay, I've just been requested to be on-site ASAP. That's usually not good. ☠️

Sofia sent:
Well... you will have to **extract the intrusion artifact** out of the last **packet capture** on your own.

Sofia sent:
I'll give you all the critical details before I go, though!

Sofia sent:
You basically just need to repeat the same process we did on `capture1.pcapng` on `capture2.pcapng`. In `capture2.pcapng`, the intrusion artifact is a **PowerShell script**, or **PS1 file**, and it was also transferred using HTTP, so you can even use the same display filter to find it.

Sofia sent:
Once you find the intrusion artifact, just extract it from the packet capture using the same export objects process and save it to the `Quarantine` **folder** on the Desktop.

Sofia sent:
Thanks for all your help today! Good Luck!