Conversation with:
Indigo Johnson
Digital Forensic Examiner

Digital Evidence Analysis Challenge Chat Transcript

Indigo sent:
Hello there, @playerone! You must be my new trainee!

I'm Indigo Johnson, I'm a Digital Forensic Examiner here at TryCyber Municipal Police Department.

Indigo sent:
I'm going to be showing you how to perform some core **Digital Evidence Analysis** tasks. You'll be helping me accomplish some of the simpler tasks I perform using the **Ubuntu 22.04 Linux** workstation you are looking at now.

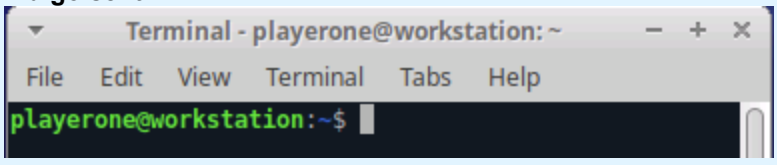
Indigo sent:
The tasks we will be doing today will be completed using the **Terminal**. It can be intimidating if you have not used it before. So let me know if you want a brief tutorial on it.

Indigo sent:
With that little summary out of the way, are you ready to get started on today's tasks? 😮

Participant sent:
Terminal tutorial, please!

Indigo sent:
The **Terminal** is primarily used to access an application called a shell. We interact with shells via a **command-line interface (CLI)** where we input and execute text-based commands on a system.

Indigo sent:
Let's open the Terminal on this system now and run a few basic commands so you get the hang of it. You can open the **Terminal** by double-clicking the icon on the desktop named **Terminal Emulator**. It should look like this once you have it open...

Indigo sent:


Participant sent:
I've opened the Terminal.

Indigo sent:
Great. Basically, you type commands into the shell within the Terminal and then hit `Enter` or `Return` on the keyboard to run the command.

Indigo sent:
To properly utilize any CLI command, you must understand its format, options, and other arguments. The **format** defines the structure and order of options and other arguments, the **options** define or modify behavior, and the **arguments** are command defined input types (e.g., files, directories, users, software packages, etc.).

Indigo sent:
Additionally, all CLI commands on this system are case-sensitive, so pay close attention to the capitalization of letters.

Indigo sent:
The basic command format is...

```
command [OPTIONS] [ARGUMENTS]
```

However, it varies a lot from command to command, and options and other arguments are not always required.

Indigo sent:
An example of a command that does not require any options or other arguments is `whoami`. If you type `whoami` into the shell and then hit `Enter` or `Return` on the keyboard, the `whoami` command will output the name of the user running the command into the Terminal. It should look like this if you run that command...

Indigo sent:

```
playerone@workstation:~$ whoami
playerone
```

Participant sent:
What's a more involved example?

Indigo sent:
I'll give you a more complex example using the `ls` command.

Indigo sent:
In this example, we will use the `ls` command to list detailed information about the entire contents of the `Templates` directory (i.e., folder) in your (playerone's) `home` directory. Our example `ls` command will use the following format...

```
ls [OPTIONS] [DIRECTORY]
```

Note that in this case, the command's argument requires the input to be a directory.

Indigo sent:
The actual command we want to run is...

```
ls -a -l /home/playerone/Templates
```

Indigo sent:
The `-a` and the `-l` are both options that modify the `ls` command's behavior, and `/home/playerone/Templates` is our argument which is a directory provided in the form of a **path**.

Indigo sent:
For this command's argument, we must provide the **path** to the directory from the root of the file system; otherwise, the system won't know which directory named `Templates` we are referring to.

Indigo sent:
And finally, when you run that command, the output should look like this...

Indigo sent:

```
playerone@workstation:~$ ls -a -l /home/playerone/Templates/
total 24
drwxr-xr-x  2 playerone playerone 4096 Jul 12 21:36  .
drwxr-x--- 14 playerone playerone 4096 Jul 12 21:36  ..
-rw-r--r--  1 playerone playerone 6859 Apr  9  2022 'OpenDocument Spreadsheet.ods'
-rw-r--r--  1 playerone playerone 7388 Apr  9  2022 'OpenDocument Text.odt'
-rw-r--r--  1 playerone playerone    0 Apr  9  2022 'Plain Text.txt'
```

Participant sent:
Got it. Any extra notes?

Indigo sent:
The Terminal and shells are incredibly powerful and versatile tools. Not all commands and programs follow the general structure I've provided you with here. Unfortunately, we only have time to cover the basics, but I do have a few last things I'd like to mention.

Indigo sent:
Some commands will not print visual output to the Terminal in normal operation, such as the `cp` command, which is used to copy files and directories.

Indigo sent:
Many commands can use multiple arguments, handle multiple input types for arguments (e.g., file and/or directory paths), or have options that will have their own arguments.

Indigo sent:
Some options can, or must be, written in a long-form format (e.g., `ls --all [DIRECTORY]` is the same as `ls -a [DIRECTORY]`).

Indigo sent:
Options without arguments can often be provided together and in any order (e.g., `ls -la [DIRECTORY]` is the same as `ls -a -l [DIRECTORY]`).

Indigo sent:
And last, but certainly not least, you can almost always reference a command's format, options, and other arguments using the command `man [COMMAND]` (e.g., `man cp`) to view the provided command's manual page in the Terminal.

Indigo sent:
Hopefully that was not too much information! I know it seems like a lot, but it gets easier the more you use it. For today's tasks, I'll be sure to provide you with more details for any commands and programs you'll need.

Participant sent:
Sounds good! I'm ready to get started!

Indigo sent:
Great! Let's get started! 👍

Indigo sent:
We just got in some new digital evidence for a recent cybercrime case that involved a *social engineering attack* where someone left CDs infected with **malicious software** around a few parking lots looking for curious victims.

Indigo sent:
Today, you are going to be helping me **scan** that new digital evidence for malicious software. A common Digital Evidence Analysis task.

Indigo sent:
The digital evidence we have today are digital copies of some CDs, **ISO (i.e., the file system written to a CD-ROM) images**, that we think could be involved with this case and might contain **malicious software**.

Indigo sent:
I've gone ahead and **read-only mounted** copies of the two ISOs on the Ubuntu Linux workstation in front of you. Mounting the ISO as read-only enables us to access and view the contents of the ISO image without the ability to modify or write. Any modifications we make to the ISO image could result in the evidence being challenged or even deemed inadmissible in court. Therefore, it is important to mount the ISO image in read-only so that any findings will be deemed sound and admissible in court.

Indigo sent:
We will use **ClamAV**, **an anti-virus scanning software**, to scan all the files within these two ISOs. If any file is **identified as suspicious** by ClamAV, we will **make a copy** of the suspicious file within the `Artifacts` folder on your desktop (which is at the path `/home/playerone/Desktop/Artifacts/`) for a specialist to review later.

Participant sent:
Sounds good to me. Where do we start?

Indigo sent:
Glad you asked! First, let's make sure the **first ISO image**, `drive1.iso`, is mounted.

Indigo sent:
As I mentioned earlier, both ISO images should already be mounted, but it will be good for you to confirm that and see what **directories** they are mounted to. To do this, you will want to run the following command in the Terminal...

```
mount -l -t iso9660
```

Indigo sent:
That `mount` command includes the `-l` option to output a list of current system mounts but also includes a `-t` option with the argument `iso9660` to limit the list to only mounts with the ISO type. The output of that command should look like this...

Indigo sent:

```
playerone@workstation:~$ mount -l -t iso9660
/home/playerone/Desktop/Materials/drive1.iso on /mnt/drive1 type iso9660 (ro,rel
atime,nojoliet,check=s,map=n,blocksize=2048,uid=1000,gid=1000,iocharset=utf8) [C
DROM]
/home/playerone/Desktop/Materials/drive2.iso on /mnt/drive2 type iso9660 (ro,rel
atime,nojoliet,check=s,map=n,blocksize=2048,uid=1000,gid=1000,iocharset=utf8) [C
DROM]
```

Participant sent:
Got it.

Indigo sent:
If your output matches my screenshot, you are seeing two mount entries for the two ISO images we need to scan. The first ISO image we need to scan is `drive1.iso`, which is mounted at the `/mnt/drive1` directory on the workstation, as shown by the output of that `mount` command.

Indigo sent:
Once we've scanned the contents of the ISO image, if the virus scanner identifies any files as suspicious, we will make a copy of the suspicious file using the `cp` command and place it in the `Artifacts` folder on the desktop. The format of that `cp` command would be `cp [SOURCE] [DESTINATION]`.

Indigo sent:
For example, IF the scanner identified the file named `recipe` at the root of `drive1.iso` as suspicious, then we would use the following `cp` command to make a copy and put it in the `Artifacts` folder...

```
cp /mnt/drive1/recipe /home/playerone/Desktop/Artifacts/
```

Indigo sent:
The `cp` command does not output anything when it completes successfully. You can check that the copy occurred by running the following `ls` command...

```
ls /home/playerone/Desktop/Artifacts/
```

Which would all look like this in the Terminal...

Indigo sent:

```
playerone@workstation:~$ cp /mnt/drive1/recipe /home/playerone/Deskto
p/Artifacts/
playerone@workstation:~$ ls /home/playerone/Desktop/Artifacts/
recipe
```

Participant sent:
How do we use the scanner?

Indigo sent:
We will need to use the ClamAV scanner utility `clamscan` to **recursively scan** the contents of `drive1.iso`, which are mounted at the `/mnt/drive1` directory. And by we, I mean you this time. 😅

Indigo sent:
The `clamscan` command format to do this will be...

```
clamscan [OPTIONS] [DIRECTORY]
```

Indigo sent:
If you are not familiar with how to use the `clamscan` command/utility to do this, you could search something like 'clamscan recursive scan' using a search engine on the web (e.g., Google, Bing, DuckDuckGo) or pull up the manual page for the `clamscan` command/utility with the command `man clamscan` to help you look up what to do. Professionals must do this all the time, so get used to looking things up! 😎

Indigo sent:
If you do need to look it up on the web, be sure to do it from your computer and not the workstation. This workstation is not connected to the internet. 🚫

Indigo sent:
Oh, and don't worry if your `clamscan` command takes a while to complete or the output says the virus database is outdated. I promise it is up to today's tasks.

Indigo sent:
Anyway! I believe in you! Let me know when you've finished or if you need more help.

Participant sent:
I would like some help.

Indigo sent:
Of course!

Indigo sent:
The `clamscan` command you need to run in the Terminal to recursively scan the contents of `drive1.iso` mounted at the `/mnt/drive1` directory is...

```
clamscan -r /mnt/drive1
```

Indigo sent:
The `-r` option of the clamscan command indicates we want to scan recursively. If we don't use this flag, it will only scan the files within the directory provided as an argument. Then, we need to provide the root directory of `drive1.iso` which is mounted at `/mnt/drive1`.

Indigo sent:
The scan output should look like this...

Indigo sent:

```
playerone@workstation:~$ clamscan -r /mnt/drive1
LibClamAV Warning: **********************************
LibClamAV Warning: ***  The virus database is older t
LibClamAV Warning: ***   Please update it as soon as
LibClamAV Warning: **********************************
/mnt/drive1/hedgehog/hedge.jpg: OK
/mnt/drive1/hedgehog/hog.jpg: OK
/mnt/drive1/important/coldsoup.mp3: OK
/mnt/drive1/important/fake.xls: OK
/mnt/drive1/important/listen: OK
/mnt/drive1/important/temp.per: Eicar-Signature FOUND
/mnt/drive1/itsalie.jpe: OK
/mnt/drive1/plans/shopping: OK
/mnt/drive1/plans/trips: OK
/mnt/drive1/recipe: OK

----------- SCAN SUMMARY -----------
Known viruses: 8669399
Engine version: 0.103.8
Scanned directories: 5
Scanned files: 10
Infected files: 1
```

Indigo sent:
This output indicates that it has flagged the file named `temp.per` within the directory named `important` as suspicious. So now we need to create a copy of that file within the `Artifacts` folder using the following command...

```
cp /mnt/drive1/important/temp.per /home/playerone/Desktop/Artifacts/
```

Indigo sent:
Once you've finished, let me know so we can move on.

Participant sent:
Done!

Indigo sent:
Alright, onto your last task for the day. I'm sure you can guess what it is.

Indigo sent:
Now, I need you to do the same thing you just did for `drive1.iso` for `drive2.iso`. So, **scan** `drive2.iso`, mounted at `/mnt/drive2`, for **suspicious files** using `clamscan`.

Indigo sent:
And just like last time, if the scanner identifies anything as suspicious, you need to **make a copy** of the suspicious file within the `Artifacts` **folder** on the Desktop.

Indigo sent:
Oh shoot... this took a bit longer than I thought. I am running late for a meeting! 😳

I'll have to leave this to you! Good luck!