**1-Starting out in Cyber Sec**

**Offensive Security**

The first large area within Cyber Security is the offensive side. This area involves attacking different applications and technologies to discover vulnerabilities.

This career is for you if:

* you enjoy understanding how things work
* you are analytical
* you like thinking out of the box

The most common offensive security job role is a penetration tester. A penetration tester is an individual that is legally employed by an organisation to find vulnerabilities in their products. A penetration tester usually requires a broad range of knowledge including:

* web application security
* network security
* use of programming languages to write various scripts

More recently, cloud security has also been gaining popularity as various organisations are now shifting their infrastructure to cloud providers such as AWS and Azure.

It's also possible to have a speciality in one of these topics, however a broad knowledge is the best way to start out.

To help you build this broad knowledge set, we have a [beginner pathway](https://tryhackme.com/path/outline/beginner) that covers the aforementioned areas. Alternatively, you can go to the [Hacktivities](https://tryhackme.com/hacktivities" \t "_blank) page and search for various topics (either by broad technologies such as web/network or specific keywords if you're familiar with certain attacks and techniques that you want to learn).

Defensive Security

This is the second major area within Security. While Offensive Security involves actively finding vulnerabilities and misconfigurations within technologies, Defensive Security involves detecting and stopping these attacks.

This career track is for you if:

* you are analytical
* you enjoy problem solving

One of the careers under this track is a Security Analyst. This is an individual in an organisation who's job is to monitor various systems in the organisation and detect whether any of these systems are being attacked. To do this, you need to understand how underlying technologies work and then understand what attacks against these technologies look like. You can learn about this using this room:

* [Detect Attacks Using Splunk](https://tryhackme.com/room/splunk101)

While a Security Analyst deals with detecting attacks, an Incident Responder is usually brought in once an attack has already occurred. Their main responsibilities include understanding what actions an attacker has taken in the organisation and what the impact of their actions will be. Incident Responders also need to know how underlying technologies work and what potential attacks could be carried out against a system. They then analyse trace evidence left by an attacker. You can learn about this on this room:

* [Analyse Memory To Trace An Attackers Actions Using Volatility](https://tryhackme.com/room/volatility)

While this is a very specialist role, malware analysis is quite common when detecting and responding to attacks. Malicious actors would use malicious pieces of software in any stage of their attack cycle from gaining access to a system to maintaining persistence. If you can understand what exactly this malware is doing, you can prevent further abuse and also identify the malicious action. You can learn about this on various rooms:

* [Introduction To Malware Analysis](https://tryhackme.com/room/malmalintroductory)
* [Researching and Identifying Malware](https://tryhackme.com/room/malresearching)
* [Identifying Strings In Malicious Applications](https://tryhackme.com/room/malstrings)

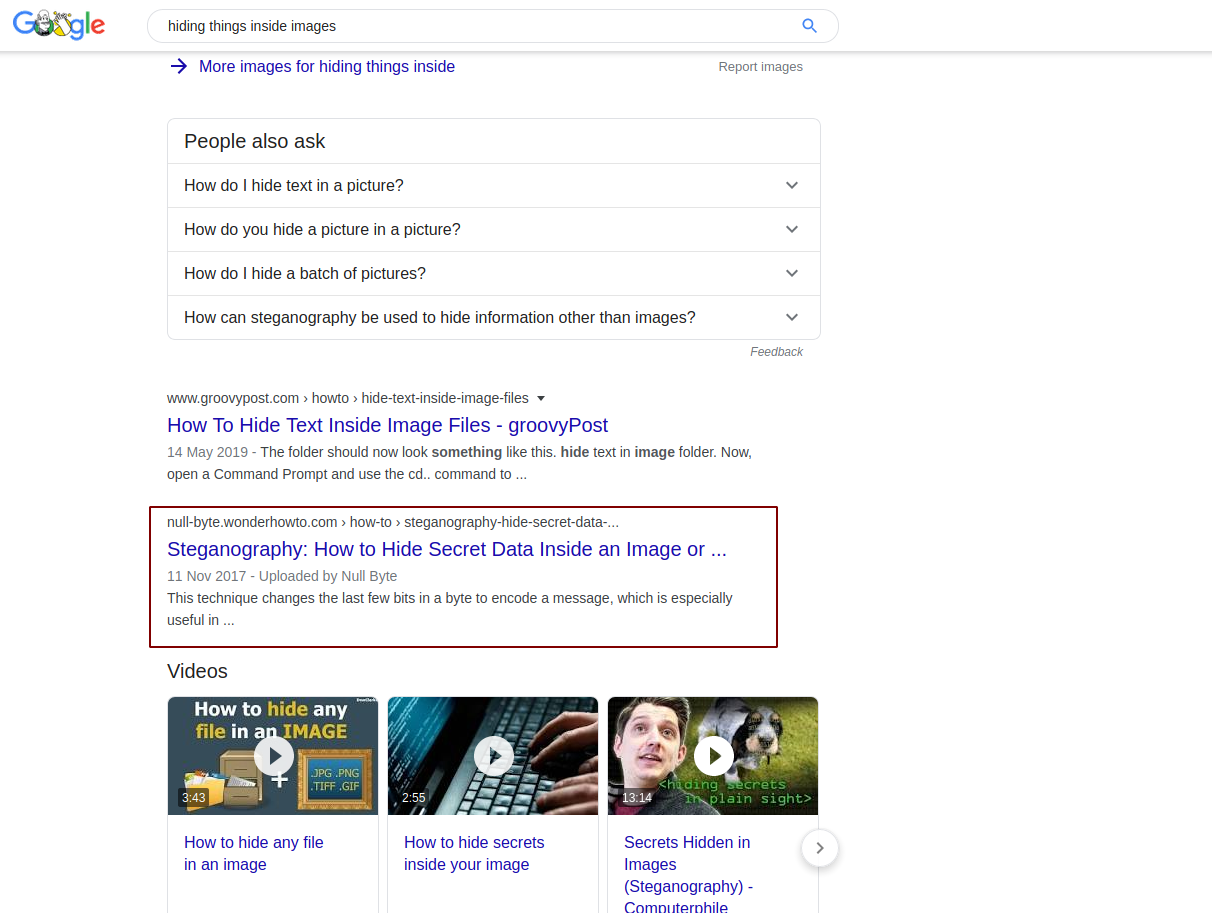
We also have a [Cyber Defence pathway](https://tryhackme.com/path/outline/blueteam) that covers a broad set of skills, tools and methodologies that would allow you to understand the fundamentals required for entry level Blue Team roles.

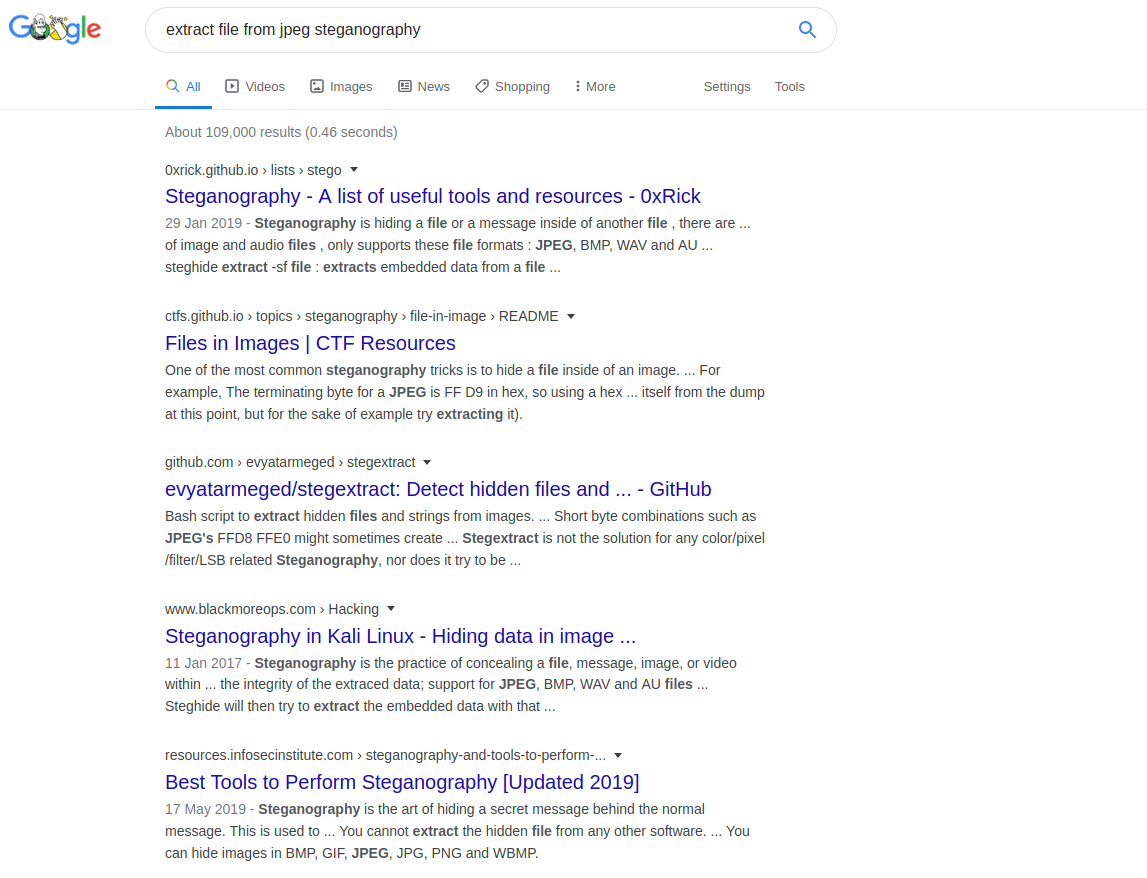
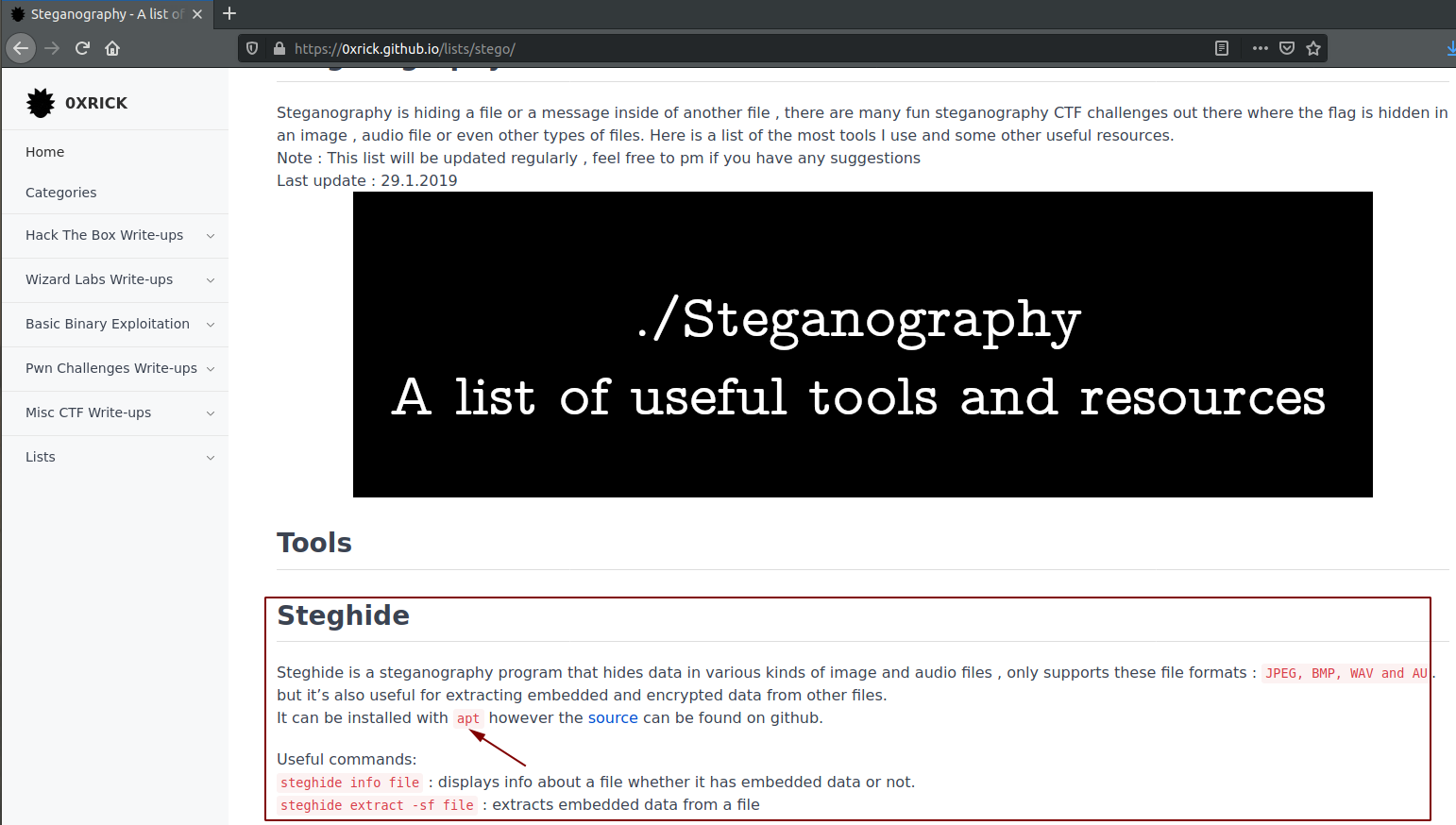
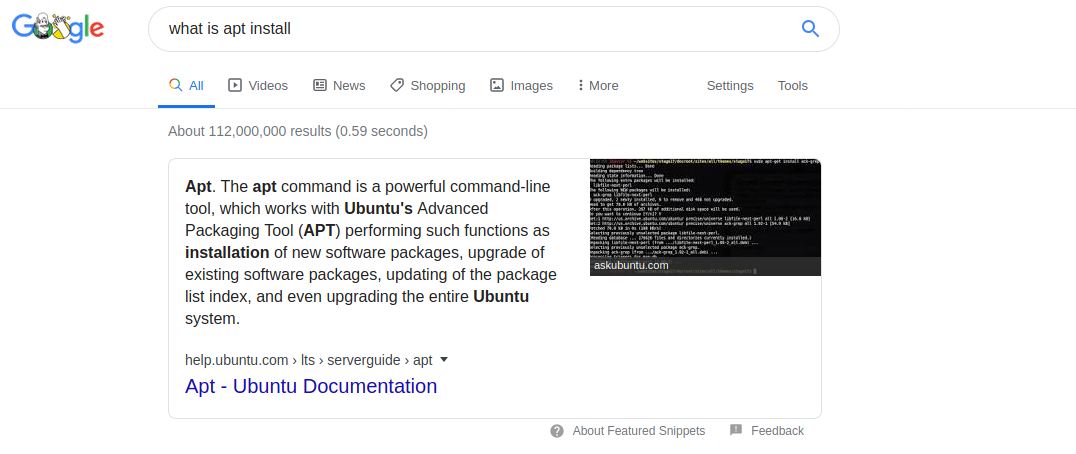
**3-Introductory Researching**

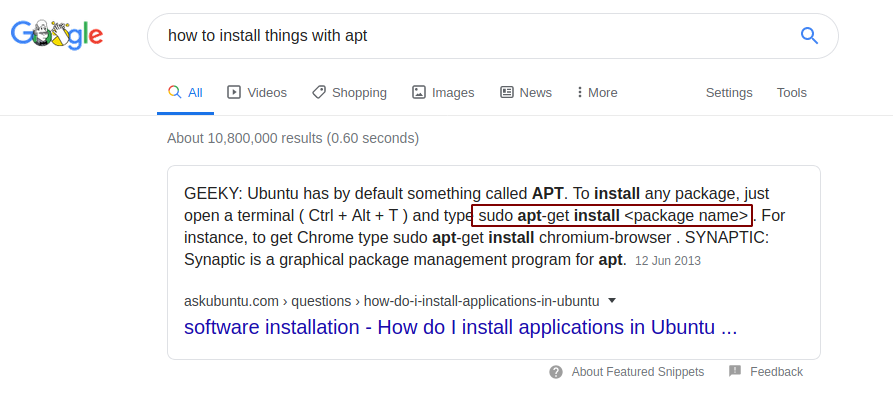
Introduction

Without a doubt, the ability to research effectively is *the* most important quality for a hacker to have. By its very nature, hacking requires a *vast* knowledge base — because how are you supposed to break into something if you don't know how it works? The thing is: no one knows everything. Everyone (professional or amateur, experienced or totally new to the subject) will encounter problems which they don't automatically know how to solve. This is where research comes in, as, in the real world, you can't ever expect to simply be handed the answers to your questions.  
  
As your experience level increases, you will find that the things you're researching scale in their difficulty accordingly; however, in the field of information security, there will never come a point where you don't need to look things up.  
  
This room will serve as a brief overview of some of the most important resources available to you, and will hopefully aid you in the process of building a research methodology that works for you.  
  
We will be looking at the following topics:  
• An example of a research question  
• Vulnerability Searching tools  
• Linux Manual Pages  
  
Example Research Question

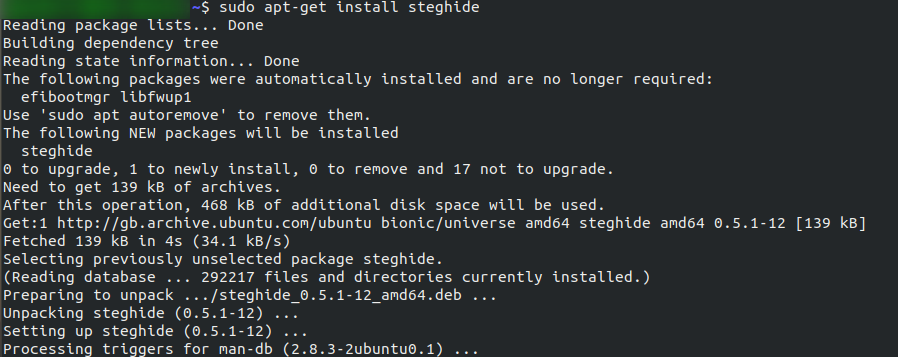
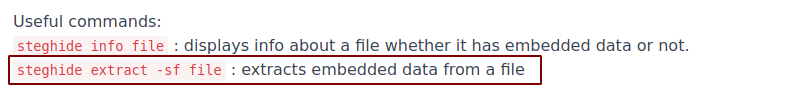
We'll begin by looking at a typical research question: the kind that you're likely to find when working through a CTF on TryHackMe.  
  
Let's say you've downloaded a JPEG image from a remote server. You suspect that there's something hidden inside it, but how can you get it out?  
How about we start by searching for “hiding things inside images” in Google:

  
  
Notice that the second link down gives us the title of a technique: “Steganography”. You can then click that link and read the document, which will teach you *how* files are hidden inside images.  
  
Ok, so we know how it's done, let's try searching for a way to extract files using steganography:

  
  
Already virtually every link is pointing to something useful. The first link contains a collection of useful tools, the second is more instructions on how to perform steganography in the first place. Realistically any of these links could prove useful, but let's take a look at that first one (<https://0xrick.github.io/lists/stego/>):  
  
  
  
The very first tool there looks to be useful. It can be used to extract embedded data from JPEG files -- exactly what we need it to do! This page also tells you that steghide can be installed using something called “apt”.  
Let's search that up next!  
  
  
  
Great -- so apt is a package manager that lets us install tools on Linux distributions like Ubuntu (or Kali!).  
How can we install packages using apt? Let's search it!



Perfect -- right at the top of the page we're given instructions. We know that our package is called steghide, so we can go ahead and install that:

  
  
Now, let's switch back to that collection of steganography tools we were looking at before. Did you notice that there were instructions on how to use steghide right there?  
  
  
  
There we go! That's how we can extract an image from a file. Our research has paid off and we can now go and complete the task.

Notice the methodology here. We started with nothing, but gradually built up a picture of what we needed to do. We had a question (How can I extract data from this image). We searched for an answer to that question, then continued to query each of the answers we were given until we had a full understanding of the topic. This is a really good way to conduct research: Start with a question; get an initial understanding of the topic; then look into more advanced aspects as needed.

Vulnerability Researching

Often in hacking you'll come across software that might be open to exploitation. For example, Content Management Systems (such as Wordpress, FuelCMS, Ghost, etc) are frequently used to make setting up a website easier, and many of these are vulnerable to various attacks. So where would we look if we wanted to exploit specific software?

The answer to that question lies in websites such as:

* [ExploitDB](https://www.exploit-db.com/)
* [NVD](https://nvd.nist.gov/vuln/search)
* [CVE Mitre](https://cve.mitre.org/)

NVD keeps track of CVEs (**C**ommon **V**ulnerabilities and **E**xposures) -- whether or not there is an exploit publicly available -- so it's a really good place to look if you're researching vulnerabilities in a specific piece of software. CVEs take the form: CVE-YEAR-IDNUMBER  
(*Hint Hint: It's going to be really useful in the questions!)*

[ExploitDB](https://www.exploit-db.com/) tends to be very useful for hackers, as it often actually contains exploits that can be downloaded and used straight out of the box. It tends to be one of the first stops when you encounter software in a CTF or pentest.

If you're inclined towards the CLI on Linux, Kali comes pre-installed with a tool called "searchsploit" which allows you to search ExploitDB from your own machine. This is offline, and works using a downloaded version of the database, meaning that you already have all of the exploits already on your Kali Linux!

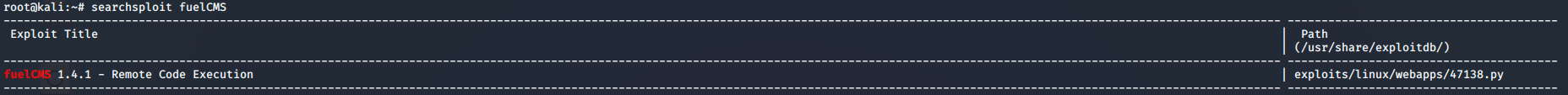
Let's take an example. Say we're playing a CTF and we come across a website:



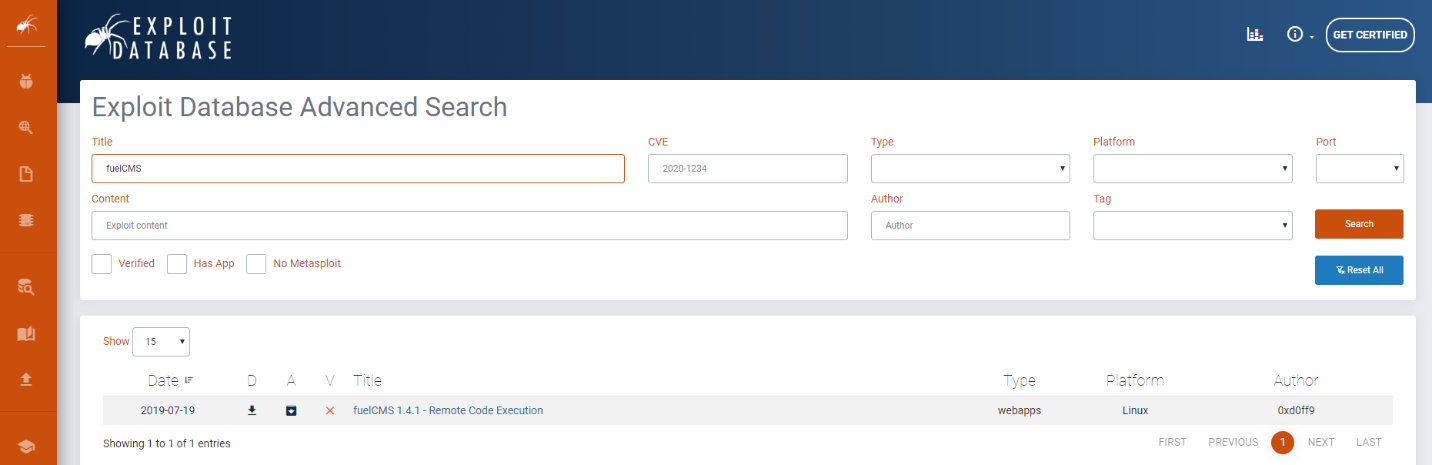
Well, this is quite obviously FuelCMS. Usually it won't be *this* obvious, but hey, we'll work with what we've got!

We know the software, so let's search for it in ExploitDB.  
(*Note: I'm going to use the CLI tool in Kali, as it tends to be quicker from a workflow perspective -- however, you are welcome to use the website)*

I'm using the command **searchsploit fuel cms** to search for exploits:



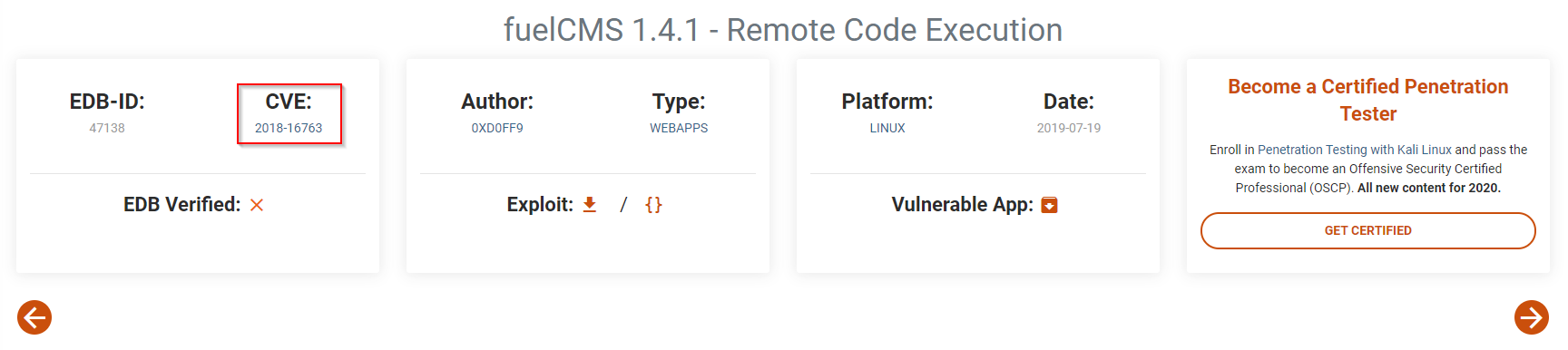
If you prefer doing things in the website, here are the results from there:



Success! We've got an exploit that we can now use against the website!

Actually using the exploit is outwith the scope of this room, but you can see the process.

If you click on the title you'll be given a bit more of an explanation about the exploit:



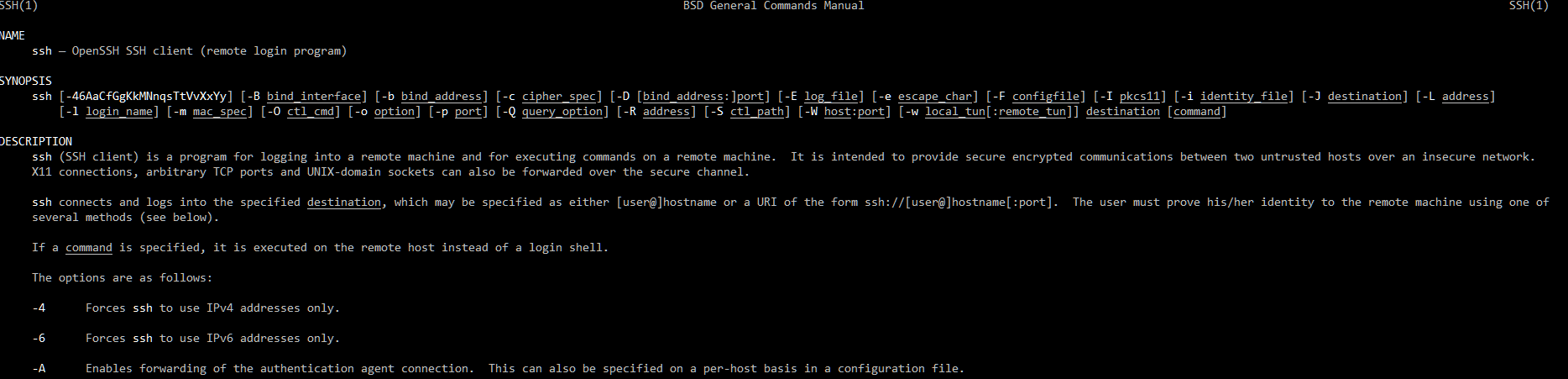
**Manual Pages**

If you haven't already worked in Linux, take a look at the [Linux Fundamentals](https://tryhackme.com/module/linux-fundamentals) module. Linux (usually Kali Linux) is without a doubt the most ubiquitous operating system used in hacking, so it pays to be familiar with it!

One of the many useful features of Linux is the inbuilt **man** command, which gives you access to the manual pages for most tools directly inside your terminal. Occasionally you'll find a tool that doesn't have a manual entry; however, this is rare. Generally speaking, when you don't know how to use a tool, **man** should be your first port of call.

Let's give this a shot!

Say we want to connect to a remote computer using SSH, but we don't know the syntax. We can try **man ssh** to get the manual page for SSH:



Awesome!

We can see in the description that the syntax for using SSH is <user>@<host>:



We can also use the man pages to look for special switches in programs that make the program do other things. An example of this would be that (from our very first example) steghide can be used to both extract and embed files inside an image, based on the switches that you give it.

For example, if you wanted to display the version number for SSH, you would scroll down in the **man** page until you found an appropriate switch:



Then use it:



Another way to find that switch would have been to search the **man** page for the correct switch using grep:



**Final Thoughts**

You may have been told in school that there are good sources and bad sources of information. That may be true when it comes to essays and referencing information; however, it's my pleasure to state that it does not apply here. Any information can potentially be useful -- so feel free to use blogs, wikipedia, or anything else that contains what you're looking for! Blogs especially can often be very valuable for learning when it comes to information security, as many security researchers keep a blog.

Having completed this room, you hopefully now have established the basis of a methodology to tackle research questions that you come across by yourself. The vast majority of rooms on TryHackMe can be solved purely using knowledge found on Google, so please take the opportunity to improve your skills by Googling any problems you come across!

As a follow-up to this room, complete CMNatic's [Google Dorking](https://tryhackme.com/room/googledorking) room to learn some advanced Google tricks!