

Introductory Researching

Introductory Research

[Task 1] Introduction

[Task 1] 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

Let's begin.

[#1] Read the Introduction ✓

[Task 2] 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:



hiding things inside images



→ More images for hiding things inside

Report images

People also ask

How do I hide text in a picture?



How do you hide a picture in a picture?



How do I hide a batch of pictures?



How can steganography be used to hide information other than images?



Feedback

www.groovypost.com › howto › hide-text-inside-image-files ▾

How To Hide Text Inside Image Files - groovyPost

14 May 2019 - The folder should now look something like this. Hide text in image folder. Now, open a Command Prompt and use the cd.. command to ...

null-byte.wonderhowto.com › how-to › steganography-hide-secret-data-...

Steganography: How to Hide Secret Data Inside an Image or ...

11 Nov 2017 - Uploaded by Null Byte

This technique changes the last few bits in a byte to encode a message, which is especially useful in ...

Videos



How to hide any file in an image



How to hide secrets inside your image

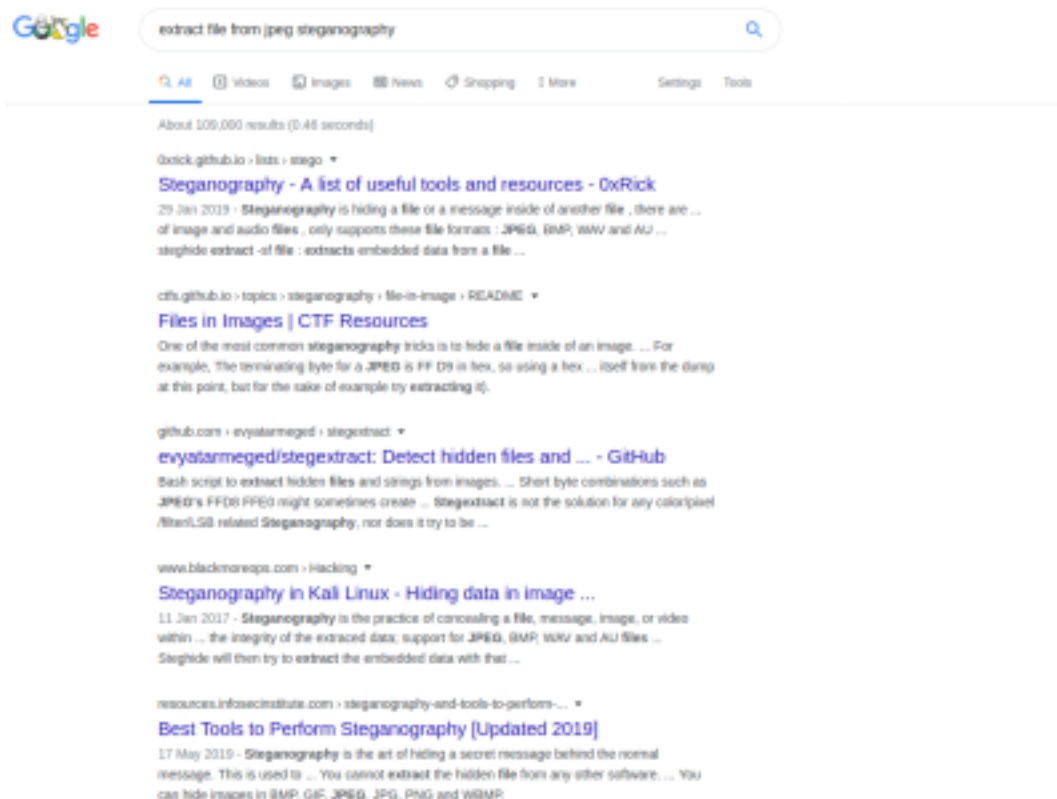


Secrets Hidden in Images (Steganography) - Computerwile

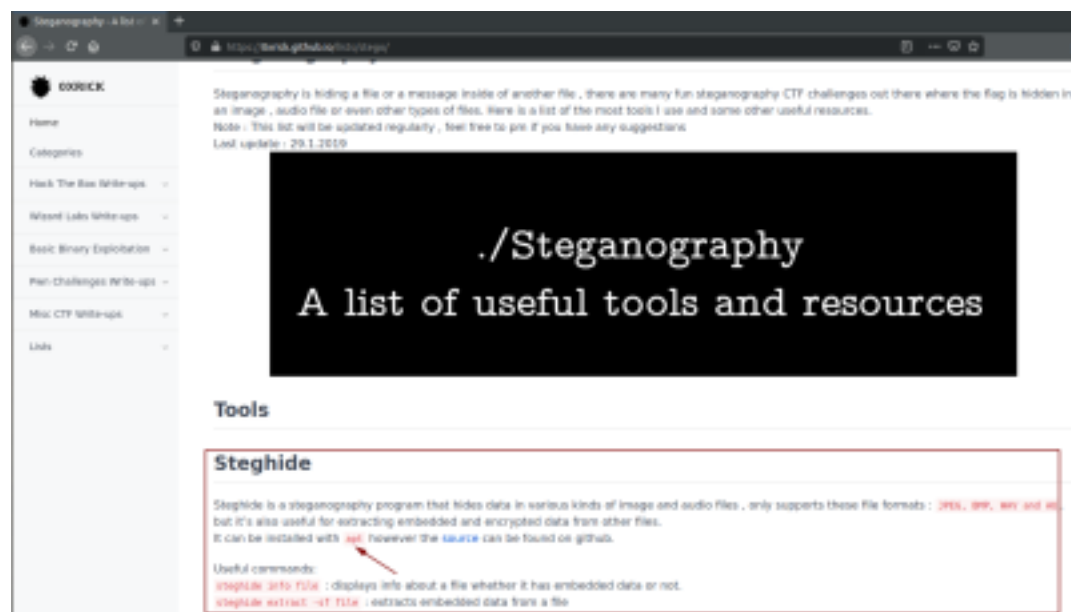


Notice that the second link down gives us the title of a technique: “Steganography”. You can then click that link and read the document, which will teach you how files are hidden inside images.

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/>):

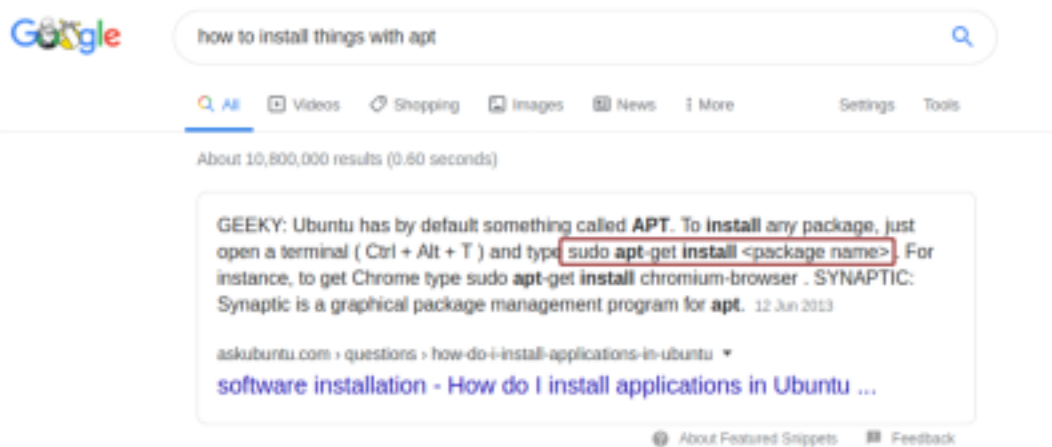


The very first tool there looks to be useful. It can be used to extract embedded data from JPEG files -- exactly what we need it to do!

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:

```
~$ sudo apt-get install steghide
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  efibootmgr libfwup1
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  steghide
0 to upgrade, 1 to newly install, 0 to remove and 17 not to upgrade.
Need to get 139 kB of archives.
After this operation, 468 kB of additional disk space will be used.
Get:1 http://gb.archive.ubuntu.com/ubuntu bionic/universe amd64 steghide amd64 0.5.1-12 [139 kB]
Fetched 139 kB in 4s (34.1 kB/s)
Selecting previously unselected package steghide.
(Reading database ... 292217 files and directories currently installed.)
Preparing to unpack .../steghide_0.5.1-12_amd64.deb ...
Unpacking steghide (0.5.1-12) ...
Setting up steghide (0.5.1-12) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
```

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?

Useful commands:

`steghide info file` : displays info about a file whether it has embedded data or not.

`steghide extract -sf file` : extracts embedded data from a file

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.

Now it's your turn. See if you can answer the following questions using your research skills. The first three questions have appropriate search queries in the hints:

[# 1] In the Burp Suite Program that ships with Kali Linux, what mode would you use to manually send a request (often repeating a captured request numerous times)?

repeater ✓

[#2] What hash format are modern Windows login passwords stored in?

NTLM ✓

[#3] What are automated tasks called in Linux?

cron jobs ✓

[#4] What number base could you use as a shorthand for base 2 (binary)?

base 16 ✓

[#5] If a password hash starts with \$6\$, what format is it (Unix variant)?

sha512crypt ✓

[Task 3] Vulnerability Searching

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
- NVD
- CVE Mitre

MVD 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 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!

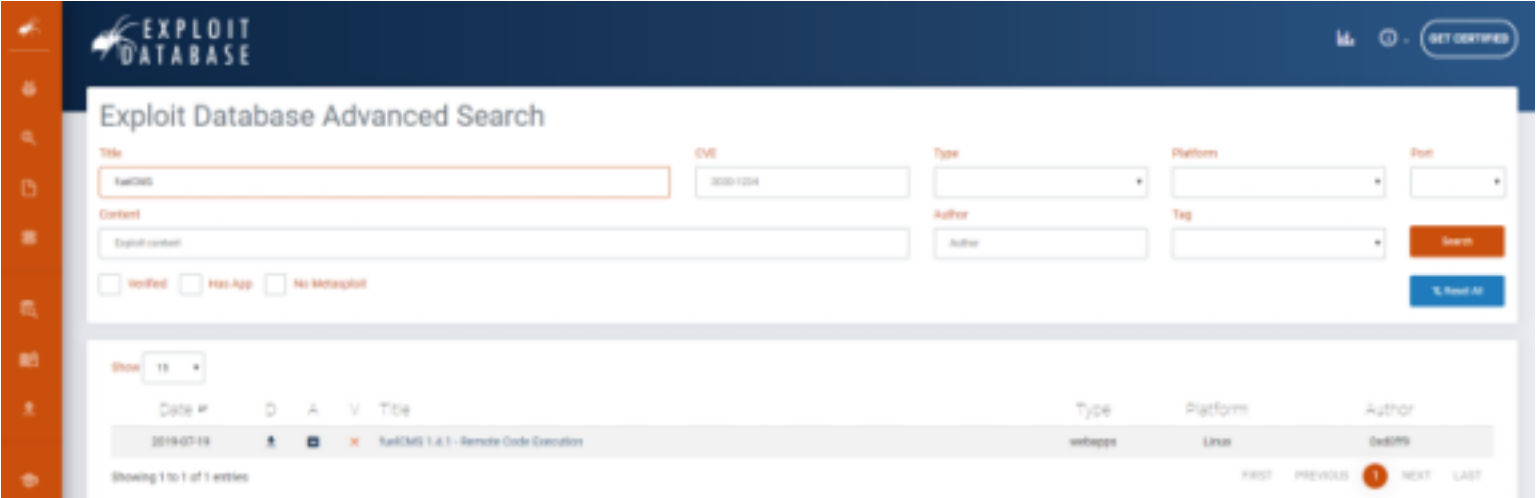
Let's take an example. Say we're playing a CTF and we come across a website:



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 I find that it's quicker -- however, you are welcome to use the website) I'm using the command searchsploit fuelcms 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:

fuelCMS 1.4.1 - Remote Code Execution

EDB-ID: 47138	CVE: 2019-16793	Author: 0x00FF0	Type: WEBAPI	Platform: Linux	Date: 2019-07-10	Become a Certified Penetration Tester Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). All new content for 2019. GET CERTIFIED
EDB Verified: ✗		Exploit:  / 		Vulnerable App: 		

Pay particular attention to the CVE numbers; you'll need them for the questions!
The format will be like so: CVE-YEAR-NUMBER

[#1] What is the CVE for the 2020 Cross-Site Scripting (XSS) vulnerability found in WPForms?

CVE-2020-10385 ✓

[#2] There was a Local Privilege Escalation vulnerability found in the *Debian* version of Apache Tomcat, back in 2016. What's the CVE for this vulnerability?

CVE-2016-1240 ✓

[#3] What is the very first CVE found in the VLC media player?

CVE-2007-0017 ✓

[#4] If I wanted to exploit a 2020 buffer overflow in the sudo program, which CVE would I use?

CVE-2019-18634 ✓

[Task 4] Manual Pages

If you haven't already worked in Linux, I would highly recommend taking a look at the Learn Linux room. 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 an 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:

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, I highly recommend CMNatic's Google Dorking room to learn some advanced Google tricks!

[# 1] Research complete!

no answer needed