Find Files and Directories

Importance of the Search

It is crucial to be able to find the files and folders we need. Once we have gained access to a Linux based system, it will be essential to find configuration files, scripts created by users or the administrator, and other files and folders. We do not have to manually browse through every single folder and check when modified for the last time. There are some tools we can use to make this work easier.

Which

One of the common tools is `which`. This tool returns the path to the file or link that should be executed. This allows us to determine if specific programs, like cURL, netcat, wget, python, gcc, are available on the operating system. Let us use it to search for Python in our interactive instance.

```
amit8986@htb[/htb]$ which python

/usr/bin/python
```

If the program we search for does not exist, no results will be displayed.

Find

Another handy tool is `find`. Besides the function to find files and folders, this tool also contains the function to filter the results. We can use filter parameters like the size of the file or the date. We can also specify if we only search for files or folders.

Syntax - find

Syntax - find

```
amit8986@htb[/htb]$ find <location> <options>
```

Let us look at an example of what such a command with multiple options would look like.

Syntax - find

```
amit8986@htb[/htb]$ find / -type f -name *.conf -user root -size +20k -newermt 2020-03-03 -exec ls -al {} \; 2>/dev/

-rw-r--r-- 1 root root 136392 Apr 25 20:29 /usr/src/linux-headers-5.5.0-1parrot1-amd64/include/config/auto.conf
-rw-r--r-- 1 root root 82290 Apr 25 20:29 /usr/src/linux-headers-5.5.0-1parrot1-amd64/include/config/tristate.conf
-rw-r--r-- 1 root root 95813 May  7 14:33 /usr/share/metasploit-framework/data/jtr/repeats32.conf
-rw-r--r-- 1 root root 60346 May  7 14:33 /usr/share/metasploit-framework/data/jtr/dynamic.conf
-rw-r--r-- 1 root root 96249 May  7 14:33 /usr/share/metasploit-framework/data/jtr/dumb32.conf
-rw-r--r-- 1 root root 54755 May  7 14:33 /usr/share/metasploit-framework/data/jtr/repeats16.conf
-rw-r--r-- 1 root root 22635 May  7 14:33 /usr/share/metasploit-framework/data/jtr/korelogic.conf
-rwxr-xr-x 1 root root 108534 May  7 14:33 /usr/share/metasploit-framework/data/jtr/john.conf
-rw-r--r-- 1 root root 55285 May  7 14:33 /usr/share/metasploit-framework/data/jtr/dumb16.conf
-rw-r--r-- 1 root root 21254 May  2 11:59 /usr/share/doc/sqlmap/examples/sqlmap.conf
-rw-r--r-- 1 root root 25086 Mar  4 22:04 /etc/dnsmasq.conf
-rw-r--r-- 1 root root 21254 May  2 11:59 /etc/sqlmap/sqlmap.conf
```

Now let us take a closer look at the options we used in the previous command. If we hover the mouse over the respective options, a small window will appear with an explanation. These explanations will also be found in other modules, which should help us if we are not yet familiar with one of the tools.

Option	Description
`-type f`	Hereby, we define the type of the searched object. In this case, '`f`' stands for '`file`'.
`-name *.conf`	With '`-name`', we indicate the name of the file we are looking for. The asterisk (`*`) stands for 'all' files with the '`.conf`' extension.
`-user root`	This option filters all files whose owner is the root user.
`-size +20k`	We can then filter all the located files and specify that we only want to see the files that are larger than 20 KiB.
`-newermt 2020-03-03`	With this option, we set the date. Only files newer than the specified date will be presented.
`-exec ls -al {} \;`	This option executes the specified command, using the curly brackets as placeholders for each result. The backslash escapes the next character from being interpreted by the shell because otherwise, the semicolon would terminate the command and not reach the redirection.
`2>/dev/null`	This is a `STDERR` redirection to the '`null device`', which we will come back to in the next section. This redirection ensures that no errors are displayed in the terminal. This redirection must `not` be an option of the 'find' command.

Locate

It will take much time to search through the whole system for our files and directories to perform many different searches. The command `locate` offers us a quicker way to search through the system. In contrast to the `find` command, `locate` works with a local database that contains all information about existing files and folders. We can update this database with the following command.

Syntax - find

```
amit8986@htb[/htb]$ sudo updatedb
```

If we now search for all files with the "`.conf`" extension, you will find that this search produces results much faster than using `find`.

Syntax - find

```
amit8986@htb[/htb]$ locate *.conf

/etc/GeoIP.conf
/etc/NetworkManager/NetworkManager.conf
/etc/UPower/UPower.conf
/etc/adduser.conf
<SNIP>
```

However, this tool does not have as many filter options that we can use. So it is always worth considering whether we can use the `locate` command or instead use the `find` command. It always depends on what we are looking for.

? Optional Exercise:

Try the different utilities and find everything related to the **netcat** / **nc** tool.

> VPN Servers
>
> ⚠ Warning: Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.
>
> All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.
>
> Existing PwnBox instances will automatically switch to the new VPN server.

eu-academy-1

PROTOCOL

● UDP 1337 ○ TCP 443

DOWNLOAD VPN CONNECTION FILE

Start Instance

0 / 1 spawns left

Waiting to start...

Questions

Cheat Sheet

Download VPN Connection File

Answer the question(s) below to complete this Section and earn cubes!

Target: 10.129.55.110

Life Left: 76 minutes +

SSH to 10.129.55.110 with user "htb-student" and password "HTB_@cademy_stdnt!"

+ 1 What is the name of the config file that has been created after 2020-03-03 and is smaller than 28k but larger than 25k?

Submit your answer here...

Submit

+ 1 How many files exist on the system that have the ".bak" extension?

Submit your answer here...

Submit

+ 0 Submit the full path of the "xxd" binary.

Submit your answer here...

Submit

Previous Next

Cheat Sheet

? Go to Questions

Table of Contents