

Post Exploitation in Windows using dir Command

January 16, 2018 By Raj Chandel

In this article, we will learn how to use Windows Command Line Command “**dir**”. We will also learn to extract files, get information about Number of files of a particular extension and much more using the Metasploit framework.

dir Command: It displays a list of a directory’s files and subdirectories.

Syntax

`dir [<Drive>:] [<Path>] [<FileName>] [/p] [/q] [/a [[:] <Attributes>]] [/s] [/b]`

1. **/p**: Displays one screen of the listing at a time.
2. **/q**: Displays file ownership information.
3. **/s**: Lists every occurrence of the specified file name within the specified directory and all subdirectories.
4. **/b**: Displays a bare list of directories and files, with no additional information.
5. **/a**: Attributes (Additional Options).

It is usually attached with options such as

- **/ad**: Directories
- **/ah**: Hidden files
- **/as**: System files
- **/a-attribute**: Not (It is used when opposite of the attribute is to be obtained)

Now to use dir for Post Exploitation, we will need an Administrator Privileged shell. This can be found here.

We will use different combinations of the attributes and parameters to extract data from the victim’s system.

Find Directories using a search string

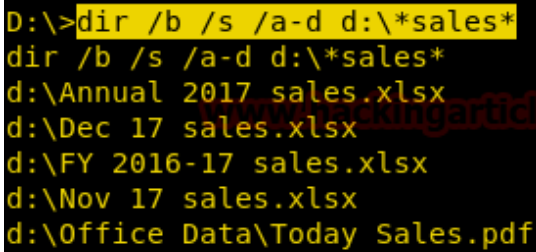
Here, we are using the following options with dir command:

- **/b** to get a bare search,
- **/s** to get a verbose result,
- **/ad** to get the list of directories,

Containing string ***sales*** in their name.

Syntax: `dir /b /s /ad [directory]*string*`

```
dir /b /s /a-d d:\*sales*
```



```
D:\>dir /b /s /a-d d:\*sales*
dir /b /s /a-d d:\*sales*
d:\Annual 2017 sales.xlsx
d:\Dec 17 sales.xlsx
d:\FY 2016-17 sales.xlsx
d:\Nov 17 sales.xlsx
d:\Office Data\Today Sales.pdf
```

Find the Number of Files/Directories in a Directory

If we need the Number of files, i.e. no. of files we have to add find command by piping [|] it with dir.

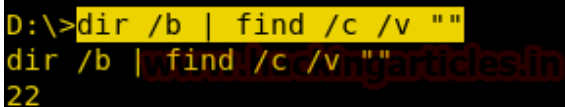
```
dir /b | find /c /v ""
```

Here [/b] to get a bare search and [/c] switch tells the find tool to Number how many lines contain our search terms, and [/v] switch will show any lines that don't contain the string of words which we have specified in this case "".

As a file name can be nothing (""), so it will Number all the file names.

Here, we are using

Above command return number of files in the Directory, we are currently in. In my case, it returns 22, which means the victim has **22 files** in his D:\ directory.



```
D:\>dir /b | find /c /v ""
dir /b | find /c /v ""
22
```

Find the Number of files

Here, we are using

```
dir /b /s /a-d d:\*sales* | find /c /v ""
```

[/ad] is for Directories.

[-] is used as NOT so [/a-d] is for not directories i.e. files

Also, find /c /v "" is used to get the Number. From given below image we can observe here it found **5 files** inside the sales folder.

```
D:\>dir /b /s /a-d d:\*sales* | find /c /v ""
dir /b /s /a-d d:\*sales* | find /c /v ""
5
```

Find the Number of Directories

Syntax: dir /b /s /ad [directory]*string* | find /c /v ""

```
dir /b /s /ad d:\*sales* | find /c /v ""
```

Here we need to get the Number of directories named *sales* It can be anything mentioned in *string*.

[/ad] is for Directories

Here **find /c /v ""** is used to get a Number and from given below image we can observe here it found **5 subdirectories** inside sales folder.

```
D:\>dir /b /s /ad d:\*sales* | find /c /v ""
dir /b /s /ad d:\*sales* | find /c /v ""
5
```

Find Files of a Particular Extension

In the given example, I searched for .xlsx files which are MS-Excel Files, but we can use it for an extension file like pdf, png, exe, docs etc.

Syntax: dir /b /s [directory]*extension*

```
dir /b /s d:\*.xlsx*
```

From given below image we can read the name of **excel files** inside D: drive.

```
D:\>dir /b /s d:\*.xlsx*
dir /b /s d:\*.xlsx*
d:\Annual 2017 sales.xlsx
d:\Dec 17 sales.xlsx
d:\FY 2016-17 sales.xlsx
d:\Nov 17 sales.xlsx
```

Find the Number of Files of a particular Extension

If we add find /c /v "" we will get the Number of files of a particular extension as shown below.

```
dir /b /s d:\*.xlsx* | find /c /v ""
```

From given below image we can observe here it found **4 excel files** inside D: drive.



```
D:\>dir /b /s d:\*.xlsx* | find /c /v ""
dir /b /s d:\*.xlsx* | find /c /v ""
4
```

Find the Number of Hidden Files/Directories

To get hidden files we will use the attribute [/ah].

And when combined with find /c /v "", we will get the Number of the hidden files/directories in the given directory as shown below.

Syntax: dir /b /ah [directory] | find /c /v ""

```
dir /b /ah d:\ | find /c /v ""
```

From given below image we can observe here it found **3 hidden files** inside D: drive.



```
D:\>dir /b /ah d:\ | find /c /v ""
dir /b /ah d:\ | find /c /v ""
3
```

Find the Hidden Files/Directories in a Directory

To view the Hidden Files in the given directory we will use attribute [/ah] with [/b] to get a bare result of the hidden files.

Syntax: dir /b /ah [directory]

```
dir /b /ah d:\
```

From given below image we can read the name of **hidden files** inside D: drive.



```
D:\>dir /b /ah d:\
dir /b /ah d:\
$RECYCLE.BIN
Kali
System Volume Information
```

Find the System Files Stored in a Directory

To get the System Files we will use another attribute which is [/as], combined with [/b] it will give the names of the system files stored in the given directory.

```
dir /b /as d:\
```

From given below image we can read the name of **system files** inside D: drive.



```
D:\>dir /b /as d:\
dir /b /as d:\
$RECYCLE.BIN
System Volume Information
```