

The virus scanner is written in python on Linux and the scanner file is ***scan.py***. It takes two arguments. First argument is the signature file and the second argument is the directory to be scanned.

To run this scanner, unzip the files into a desired directory. The usage of the python script is shown below:

```
#python scan.py <signature_file> <directory_to_scan>
```

The zip file contains an example signature file named ***signatures***. To scan the current directory (".") recursively the following example command can be run.

Example:

```
#python scan.py signatures .
```

The signatures in the signatures file are line separated. The python script reads the file contents and splits the data based on newlines using "splitlines" method into an array of signatures.

The os.walk method is used to recursively traverse all the directories and all the files in a directory. The file is then run through a scanner written in the method ***scanvirus***. This method one by one checks the presence of signatures in the file from the signature array and prints a message if a match for the signature is found. The screenshot below shows a sample run of the Virus Scanner.

```
root@kali:~/scanner# pwd
/root/scanner
root@kali:~/scanner# ls -lrt
total 24
-rw-r--r-- 1 root root 57 Dec 16 18:09 signatures
-rw-r--r-- 1 root root 37 Dec 16 18:25 VirusFile3
drwxr-xr-x 2 root root 4096 Dec 16 18:26 subdir1
drwxr-xr-x 2 root root 4096 Dec 16 18:26 subdir2
-rw-r--r-- 1 root root 51 Dec 16 19:10 SafeFile
-rw-r--r-- 1 root root 860 Dec 16 19:11 scan.py
root@kali:~/scanner# ls -lrt subdir1/
total 4
-rw-r--r-- 1 root root 77 Dec 16 18:26 VirusFile1
root@kali:~/scanner# ls -lrt subdir2/
total 4
-rw-r--r-- 1 root root 52 Dec 16 18:26 VirusFile2
root@kali:~/scanner# cat signatures
testsig1
testsig2
testsig3
testsig4
ThisIsVirus
TestSig5
root@kali:~/scanner# cat subdir1/VirusFile1

leadinggarbagetestsig1testsThisIsVirusblankjunk
fgdfghzSomething something

root@kali:~/scanner# cat subdir2/VirusFile2

dsfdgfd
leadinggarbagetestsig2blankjunk
End

root@kali:~/scanner# cat VirusFile3

leadinggarbageThisIsVirusblankjunk

root@kali:~/scanner# cat SafeFile

This file is safe.
contains no virus signatures.

root@kali:~/scanner# python scan.py
<Usage>: python scan.py <signature_file> <directory to scan>
root@kali:~/scanner# python scan.py /root/scanner/signatures /root/scanner/
Found match for signature: 'ThisIsVirus' in File: /root/scanner/VirusFile3
Found match for signature: 'testsig1' in File: /root/scanner/subdir1/VirusFile1
Found match for signature: 'ThisIsVirus' in File: /root/scanner/subdir1/VirusFile1
Found match for signature: 'testsig2' in File: /root/scanner/subdir2/VirusFile2
root@kali:~/scanner#
```