

1 . What does the strip command do?

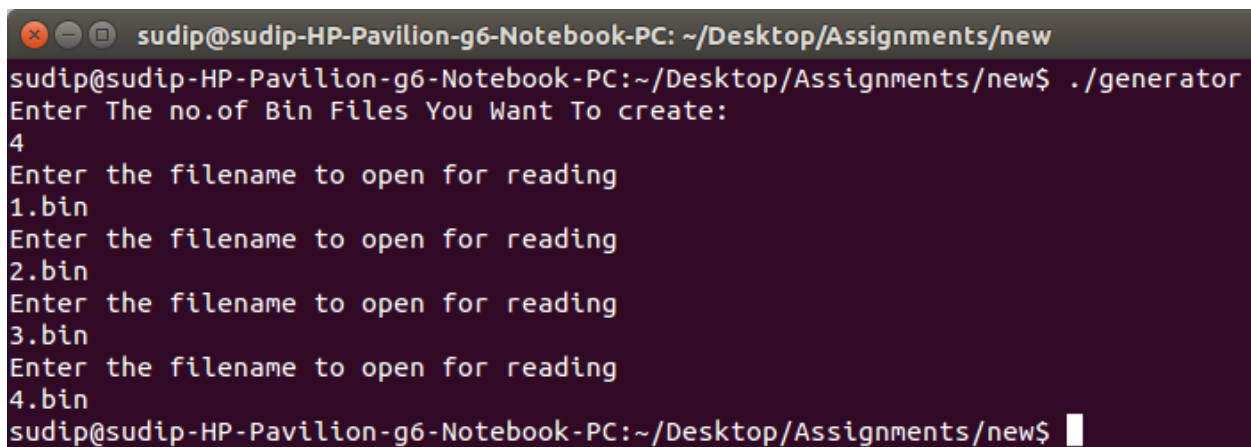
Ans: Running the strip command on an executable is the most common program protection method. In its default operation, the strip command removes the symbol table and any debugging information from an executable. It is also used to make the program lightweight and so that the program uses the bare minimum libraries and whatever is not required is. It also to some extent prevents reverse engineering.

Q11.

There is a Difference in dump and ghex and hexdump output, only dumping the file as is , will make it appear randomized and hapazard , we can see the DEADBEEFDEAD hex values in it, Ghex we can directly see it and same is the case with hexdump.

## Screenshots

### .bin File Generator.



```
sudip@sudip-HP-Pavilion-g6-Notebook-PC: ~/Desktop/Assignments/new
sudip@sudip-HP-Pavilion-g6-Notebook-PC:~/Desktop/Assignments/new$ ./generator
Enter The no.of Bin Files You Want To create:
4
Enter the filename to open for reading
1.bin
Enter the filename to open for reading
2.bin
Enter the filename to open for reading
3.bin
Enter the filename to open for reading
4.bin
sudip@sudip-HP-Pavilion-g6-Notebook-PC:~/Desktop/Assignments/new$
```

# Scanner Program

```
3;J
sudip@sudip-HP-Pavilion-g6-Notebook-PC:~/Desktop/Assignments/new$ ./Scanner
Found 4 .bin files
First match: 1.bin
0
Main Database Created
Main Database Created
Main Database Created
Main Database Created
Press Q to exit
1
You Entered 1
1
Scanning
Scanning
Scanning
Scanning
Scanning
Scanning
Scanning
Scanning
Scanning
Press Q to exit
You Entered
1
1
Scanning
1.bin
Alert!The File Has Been Infected
Scanning
Scanning
2.bin
Alert!The File Has Been Infected
Scanning
Scanning
3.bin
Alert!The File Has Been Infected
Scanning
Scanning
4.bin
Alert!The File Has Been Infected
```

# Virus Program

```
sudip@sudip-HP-Pavilion-g6-Notebook-PC:~/Desktop/Assignments/new$ ./Virus
Found 4 .bin files
1.bin
2.bin
3.bin
4.bin
Press 1 to Check the File Signature of Virus
1
58 CC 69 AC 8D 7F 00 00 | 58 CC 69 AC 8D 7F 00 00 | X.i....X.i....
00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | .....
40 00 00 00 00 00 00 00 | 68 01 00 00 00 00 00 00 | @.....h.....
00 00 00 00 40 00 38 00 | 03 00 40 00 05 00 04 00 | ...@.8...@....
01 00 00 00 05 00 00 00 | 00 00 00 00 00 00 00 00 | .....
00 00 40 00 00 00 00 00 | 00 00 40 00 00 00 00 00 | ..@.....@....
32 01 00 00 00 00 00 00 | 32 01 00 00 00 00 00 00 | 2.....2.....
00 00 20 00 00 00 00 00 | 01 00 00 00 06 00 00 00 | .. .....
34 01 00 00 00 00 00 00 | 34 01 60 00 00 00 00 00 | 4.....4.`....
34 01 60 00 00 00 00 00 | 09 00 00 00 00 00 00 00 | 4.`.....
09 00 00 00 00 00 00 00 | 00 00 20 00 00 00 00 00 | .....
04 00 00 00 04 00 00 00 | E8 00 00 00 00 00 00 00 | .....
E8 00 40 00 00 00 00 00 | E8 00 40 00 00 00 00 00 | ..@.....@....
24 00 00 00 00 00 00 00 | 24 00 00 00 00 00 00 00 | $......$......
04 00 00 00 00 00 00 00 | 04 00 00 00 14 00 00 00 | .....
03 00 00 00 47 4E 55 00 | 13 40 4B BF E3 DC 8F 3C | ....GNU...@K...<
C9 C9 8E 3E 53 8A 9A FC | 46 41 E2 3E 00 00 00 00 | ...>S...FA.>...
BA 09 00 00 00 B9 34 01 | 60 00 BB 01 00 00 00 B8 | .....4.`.....
04 00 00 00 CD 80 BB 00 | 00 00 00 B8 01 00 00 00 | .....
CD 80 00 00 42 55 53 54 | 45 44 0A 00 2E 73 68 73 | ...BUSTED...shs
74 72 74 61 62 00 2E 6E | 6F 74 65 2E 67 6E 75 2E | trtab..note.gnu.
62 75 69 6C 64 2D 69 64 | 00 2E 74 65 78 74 00 2E | build-id..text..
64 61 74 61 00 00 00 00 | 00 00 00 00 00 00 00 00 | data.....
00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | .....
00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | .....
00 00 00 00 00 00 0B 00 | 00 00 07 00 00 00 02 00 | .....
00 00 00 00 00 00 E8 00 | 40 00 00 00 00 00 E8 00 | .....@.....
00 00 00 00 00 00 24 00 | 00 00 00 00 00 00 00 00 | .....$......
00 00 00 00 00 00 04 00 | 00 00 00 00 00 00 00 00 | .....
00 00 00 00 00 00 1E 00 | 00 00 01 00 00 00 06 00 | .....
00 00 00 00 00 00 10 01 | 40 00 00 00 00 00 10 01 | .....@.....
00 00 00 00 00 00 22 00 | 00 00 00 00 00 00 00 00 | ....."......
```