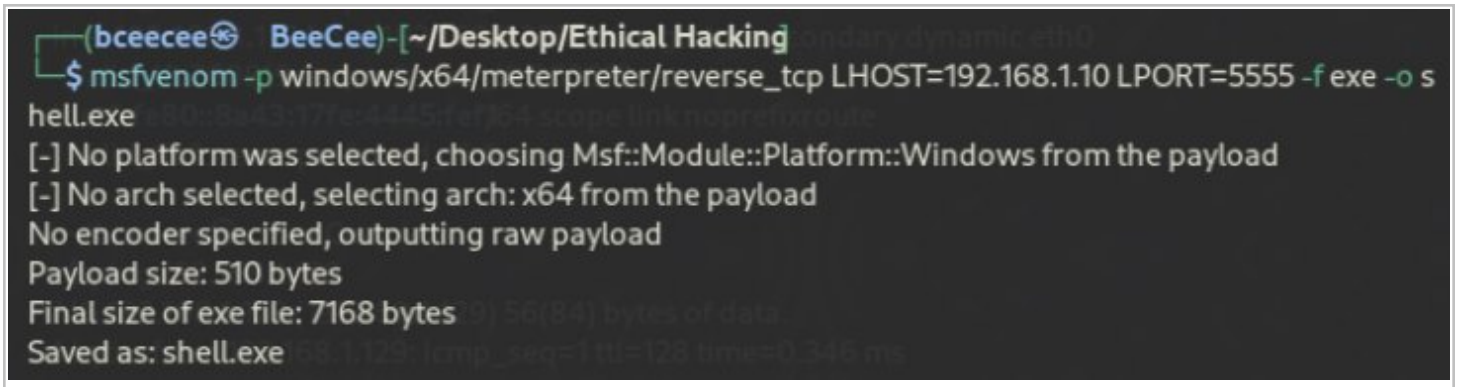
Section 10: Gaining Access (Viruses, Trojans, Payloads)

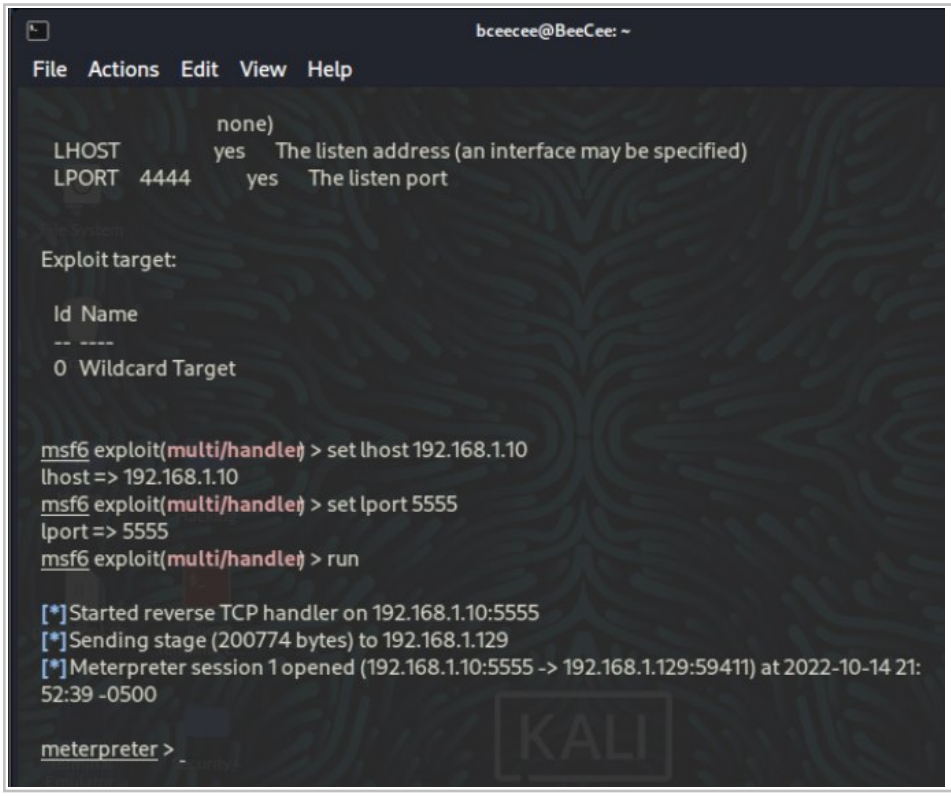
Name: BC

Choose screenshots for each lab that best illustrates your completion of the lab. Submit by clicking the box and locating the screenshot. Use a black-on-white color scheme for all Terminal sessions.

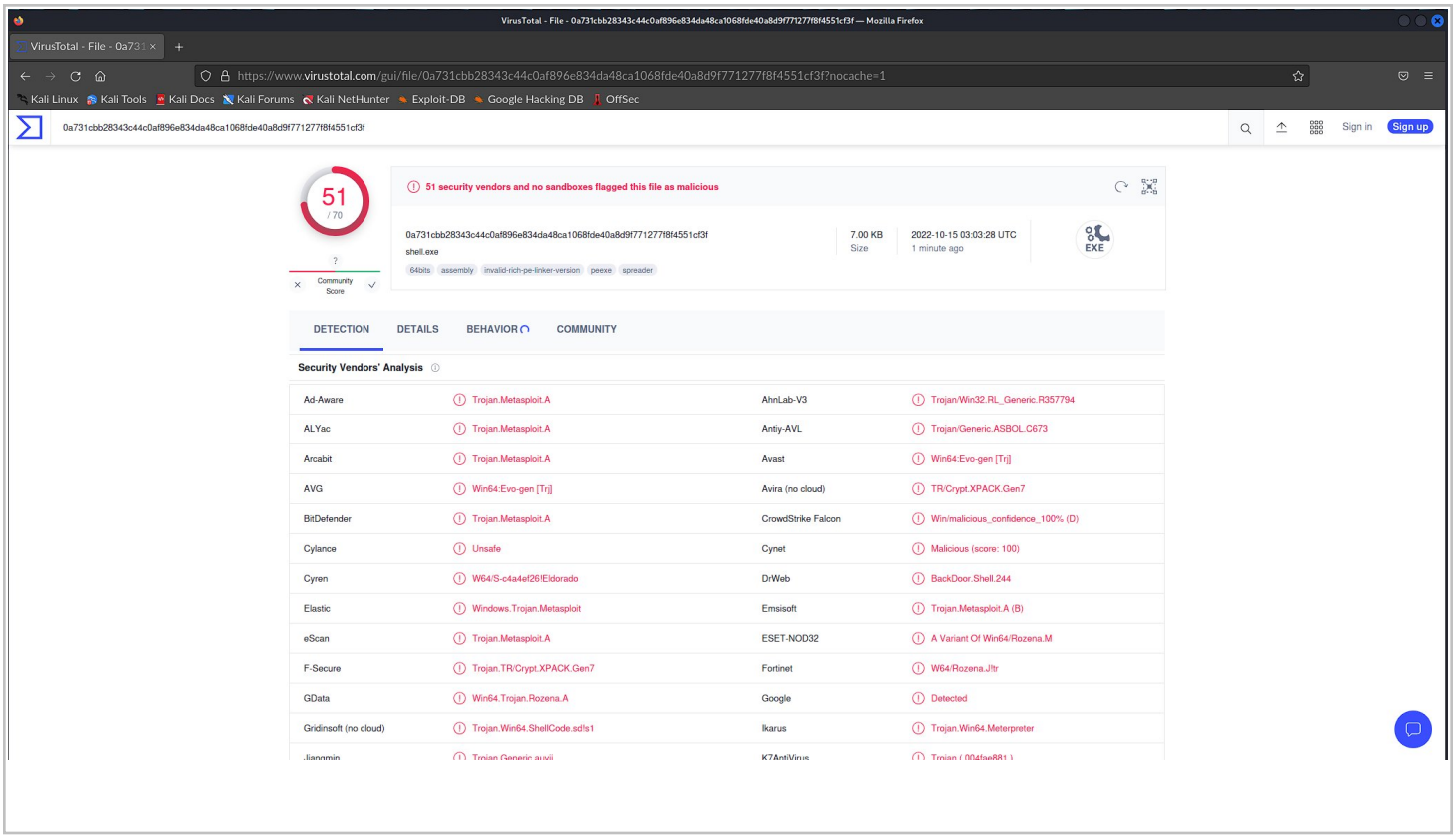
Lab 1: Create a Windows 10 payload that supports a reverse TCP Meterpreter session (81)



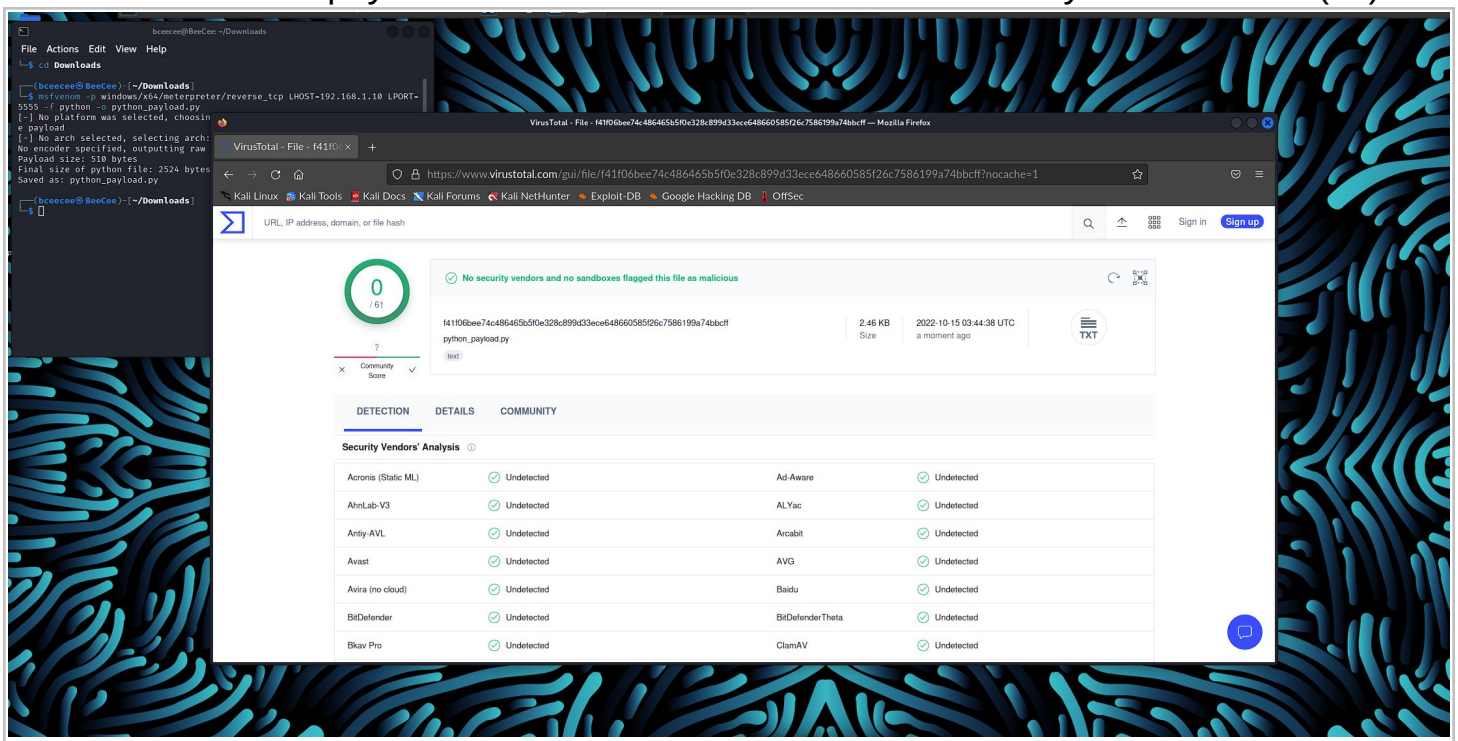
Lab 2: Tell Kali to listen for a reverse TCP connection for a Meterpreter session (81)



Lab 3: Determine how many AV programs will detect the payload created in the lab above (82)



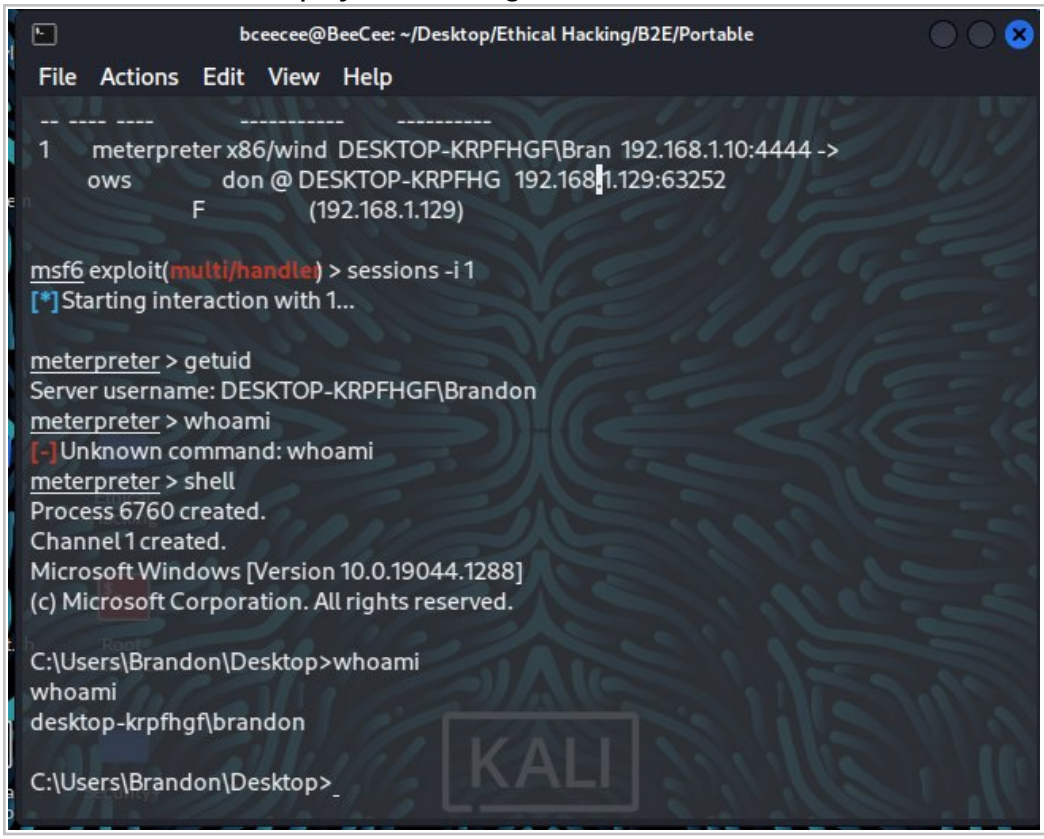
Lab 4: Create a new payload to attack Windows 10 that is least likely to be detected (83)



Before beginning the next lab, install wine (runs Windows programs inside Linux) by executing the following commands as root:
dpkg --add-architecture i386 && apt-get update && apt-get install wine32
Note: You may first need to download and install the bare metal full version of Kali from kali.org.

Lab 5: Install Veil (84)

Lab 6: Create a PS payload using Veil to attack 64-bit Windows 10. Run in msfconsole (84)



Lab 7: Make a payload less detectable. Show before and after MD5SUMs below (87)

```
┌──(kali㉿bracker)-[~/Desktop]
└─$ md5sum shel.exe
ecb85ee71d9587d6f698ff76e5352320  shel.exe

┌──(kali㉿bracker)-[~/Desktop]
└─$ hexeditor shel.exe

┌──(kali㉿bracker)-[~/Desktop]
└─$ md5sum shel.exe
a6856072f9198b2000f70429db2fc415  shel.exe

┌──(kali㉿bracker)-[~/Desktop]
└─$
```

Download WinRar from www.win-rar.com and install on Windows 10 before starting next lab.

Lab 8: Create a payload that opens an image (88)