Review: Quiz 04 - Windows Threat Hunting (Digital Forensics 152361)

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

1

Which part of the **Windows Registry** contains the user's password file? *

● HKEY_LOCAL_MACHINE ✓

○ HKEY_CURRENT_CONFIGURATION

○ HKEY_USER

○ HKEY_CURRENT_USER

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

2

Hackers can gain access to Windows Registry and manipulate user passwords, DNS settings, access rights or others features that they may need in order to accomplish their objectives. One simple method for loading an application at startup is to add an entry (Key) to the following Registry Hive *

○ HKEY_LOCAL_MACHINE\hardware\windows\start

○ HKEY_LOCAL_USERS\Software\Microsoft\old\Version\Load

○ HKEY_CURRENT_USER\Microsoft\Default

● HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\Run ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

3

Which of the following options will help users to enable or disable the last access time on a system running Windows 10 OS? *

○ wmic service

○ reg.exe

● fsutil ✓

○ devcon

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

4

Microsoft Security IDs are available in Windows Registry Editor. The path to locate IDs in Windows 7 is ________ *

● HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList ✓

○ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProfileList

○ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegList

○ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Regedit

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

5

Which of the following commands shows you all of the network services running on Windows-based servers? *

● net start ✓

○ net session

○ net use

○ net config

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

6

You have been given the task of investigating web attacks on a Windows-based server. Which of the following commands will you use to look at the sessions the machine has opened with other systems? *

○ net session

○ net config

○ net share

● net use ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

7

Which of the following Windows-based tools displays who is logged onto a computer, either locally or remotely? *

○ Tokenmon

● PSLoggedon ✓

○ TCPView

○ Process Monitor

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

8

Alice, a network administrator, suspects unusual network services running on a windows system. Which of the following commands should he use to verify unusual network services started on a Windows system? *

○ net serv

○ netmgr

○ lusrmgr

● net start ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

9

Pagefile.sys is a virtual memory file used to expand the physical memory of a computer. Select the registry path for the page file? *

● HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management ✓

○ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\System Management

○ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Device Management

○ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

10

Which of the following registry hive gives the configuration information about which application was used to open various files on the system? *

● HKEY_CLASSES_ROOT ✓

○ HKEY_CURRENT_CONFIG

○ HKEY_LOCAL_MACHINE

○ HKEY_USERS

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

11

An incident response analyst is investigating the root cause of a recent malware outbreak. Initial binary analysis indicates that this malware disables host security services and performs cleanup routines on its infected hosts, including deletion of initial dropper and removal of event log entries and prefetch files from the host. Which of the following data sources would most likely reveal evidence of the root cause? (Choose all that apply) *

□ Creation time of dropper

☑ Registry artifacts ✓

□ EDR data

□ Prefetch files

☑ File system metadata ✓

□ Sysmon event log

□ Option 2

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

12

When investigating a Windows System, it is important to view the contents of the page or swap file because ________ *

○ Windows stores all of the systems configuration information in this file

○ This is file that windows use to communicate directly with Registry

● A Large volume of data can exist within the swap file of which the computer user has no knowledge ✓

○ This is the file that windows use to store the history of the last 100 commands that were run from the command line

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

13

A forensics investigator is searching for the hard drive of a computer for files that were recently moved to the Recycle Bin. He searches for files in **C:\RECYCLED** using a command line tool but does not find anything. What is the reason for this? *

○ He should search in C:\Windows\System32\RECYCLED folder

○ The Recycle Bin does not exist on the hard drive

● The files are hidden, and he must use switch to view them ✓

○ Only FAT system contains RECYCLED folder and not NTFS

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

14

A technician suspects a rootkit has been installed and needs to be removed. Which of the following would **BEST** resolve the issue? *

○ Application updates

○ Anti-malware software

● Operating System reinstallation ✓

○ File restores

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

15

Select the data that a virtual memory would store in a Windows-based system? *

○ Information or metadata of the files

○ Documents and other files

○ Application data

● Running processes ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

16

During a penetration test, a tester runs a phishing campaign and receives a shell from an internal PC running Windows 10 Operating Sysstem. The tester wants to perform credential harvesting with **Mimikatz**. Which of the following registry changes would allow for credential caching in memory? *

○ reg add HKLM\System\ControlSet002\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 0

○ reg add HKCU\System\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1

○ reg add HKLM\Software\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1

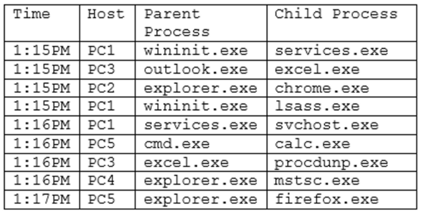
● reg add HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1 ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

17

A security analyst is reviewing system logs while threat hunting. Which of the following hosts should be investigated first? *



Time	Host	Parent Process	Child Process
1:15PM	PC1	wininit.exe	services.exe
1:15PM	PC3	outlook.exe	excel.exe
1:15PM	PC2	explorer.exe	chrome.exe
1:15PM	PC1	wininit.exe	lsass.exe
1:16PM	PC1	services.exe	svchost.exe
1:16PM	PC5	cmd.exe	calc.exe
1:16PM	PC3	excel.exe	procdunp.exe
1:16PM	PC4	explorer.exe	mstsc.exe
1:17PM	PC5	explorer.exe	firefox.exe

○ PC1

○ PC2

● PC3 ✓

○ PC4

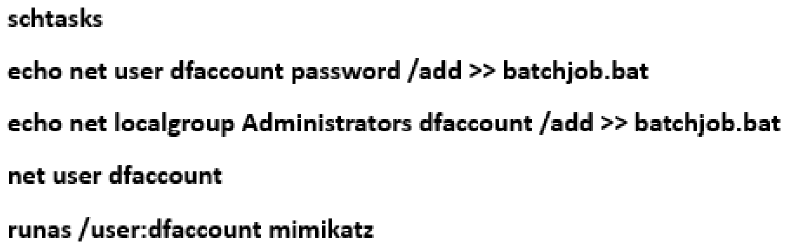
○ PC5

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

18

A penetration tester ran the following commands on a Windows server. Which of the following should the tester do AFTER deliver the final report?
*



```
schtasks
echo net user dfaccount password /add >> batchjob.bat
echo net localgroup Administrators dfaccount /add >> batchjob.bat
net user dfaccount
runas /user:dfaccount mimikatz
```

○ Delete the scheduled batch job.

○ Close the reverse shell connection.

○ Downgrade the svsaccount permissions.

● Remove the tester-created credentials ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

19

The investigator wants to examine changes made to the system’s registry by the suspect program. Which of the following tools can help the investigator? *

○ TRIPWIRE

○ RAM Capturer

● Regshot ✓

○ What’s Running

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

20

Alice is working as a computer forensics investigator for a consulting firm in Israel. He is called to seize a computer at a local school purportedly used as a botnet server. Alice thoroughly scans the computer and finds nothing that would lead him to think the computer was a botnet server. Alice decides to scan the virtual memory of the computer to possibly find something he had missed. What information will the virtual memory scan produce? *

○ It contains the times and dates of when the system was last patched

○ It is not necessary to scan the virtual memory of a computer

○ It contains the times and dates of all the system files

● Hidden running processes ✓