Review: Quiz 03 - Windows Event Log Analysis (Digital Forensics 152361)

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

1

In Windows, what events can occur when using the Command Prompt to execute the **ping abc.com** command? Be aware that the administrator may have configured a GPO to log the PowerShell service, set up an Advanced Audit Policy, and enabled the Sysmon service on the Windows computer (Choose all that apply) *

☑ Event ID (4688) A new process has been created ✓

□ Event ID (12) RegistryEvent (Object create and delete)

☑ Event ID (22) DNS Query ✓

□ Event ID (4624) An account was successfully logged on

☑ Event ID (1) Process creation ✓

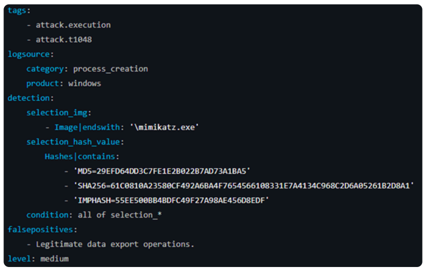
□ Event ID (4104) Powershell Execute a Remote Command

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

2

The following Sigma rules define how to detect **mimikatz** tools running on a user's computer based on Sysmon logs. What are some ways to bypass these detection rules? (Choose all that apply) *



```
tags:
    - attack.execution
    - attack.t1048
logsource:
    category: process_creation
    product: windows
detection:
    selection_img:
        - Image|endswith: '\mimikatz.exe'
    selection_hash_value:
        Hashes|contains:
            - 'MD5=29EFD64DD3C7FE1E2B022B7AD73A1BA5'
            - 'SHA256=61C0810A23580CF492A6BA4F7654566108331E7A4134C968C2D6A05261B2D8A1'
            - 'IMPHASH=55EE500BB4BDFC49F27A98AE456D8EDF'
    condition: all of selection_*
falsepositives:
    - Legitimate data export operations.
level: medium
```

☑ Execute a tool named **mimikazt.exe**, which has been stripped down to remove some features compared to the original source code ✓

□ Execute the tool named **mimikatz.exe** with the IMPHASH hash **55EE500BB4BDFC49F27A98AE456D8EDF** in the Windows Command Prompt

☑ Execute the tool named **mimidump.exe** with the MD5 hash **29EFD64DD3C7FE1E2B022B7AD73A1BA5** in the Windows Command Prompt ✓

□ All the answers are correct

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

3

Which of the following describes the reason why a penetration tester would run the command **sdelete mimikatz.*** on a Windows server that the tester compromised? *

○ To remove hash-cracking registry entries

○ To remove the tester-created Mimikatz account

● To remove tools from the server ✓

○ To remove a reverse shell from the system

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

4

A penetration tester has extracted password hashes from the lsass.exe memory process. Which of the following should the tester perform **NEXT** to **pass the hash** and provide persistence with the newly acquired credentials? *

○ Use Patator to pass the hash and Responder for persistence.

○ Use Hashcat to pass the hash and Empire for persistence.

○ Use a bind shell to pass the hash and WMI for persistence.

● Use Mimikatz to pass the hash and PsExec for persistence ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

5

An organization experienced a security breach that allowed an attacker to send fraudulent wire transfers from a hardened PC exclusively to the attacker's bank through remote connections. A security analyst is creating a timeline of events and has found a different PC on the network containing malware. Upon reviewing the command history, the analyst finds the following: **PS>.\mimikatz.exe "sekurlsa::pth /user:localadmin /domain:corp-domain.com /ntlm:B4B9B02E1F29A3CF193EAB28C8D617D3F327** Which of the following best describes how the attacker gained access to the hardened PC? *

○ The attacker created fileless malware that was hosted by the banking platform.

● The attacker performed a pass-the-hash attack using a shared support account. ✓

○ The attacker utilized living-off-the-land binaries to evade endpoint detection and response software.

○ The attacker socially engineered the accountant into performing bad transfers

✗ **Incorrect** 0/0.5 Points

0 / 0.5 pts
Auto-graded

6

A company's help desk received several AV alerts indicating Mimikatz attempted to run on the remote systems Several users also reported that the new company flash drives they picked up in the break room only have 512KB of storage Which of the following is most likely the cause? *

○ The GPO prevents the use of flash drives, which triggers a false positive AV indication and restricts the drives to only 512KB of storage

○ The new flash drives need a driver that is being blocked by the AV software because the flash drives are not on the application's allow list, temporarily restricting the drives to 512KB of storage. ✓

○ The new flash drives are incorrectly partitioned, and the systems are automatically trying to use an unapproved application to repartition the drives.

● The GPO blocking the flash drives is being bypassed by a malicious flash drive that is attempting to harvest plaintext credentials from memory.

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

7

Alice, a penetration tester, has received basic account credentials and logged into a Windows system. To escalate his privilege, from which of the following places is he using Mimikatz to pull credentials? *

● LSASS ✓

○ SAM database

○ Active Directory

○ Registry

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

8

A systems administrator is changing the password policy within an enterprise environment and wants this update implemented on all systems as quickly as possible. Which of the following operating system security measures will the administrator most likely use? *

○ Deploying PowerShell scripts

● Pushing GPO update ✓

○ Enabling PAP

○ Updating EDR profiles

○ Option 2

✗ **Incorrect** 0/0.5 Points

0 / 0.5 pts
Auto-graded

9

Question *

○ What is the capacity of Recycle bin in a system running on Windows 10?

○ 7.99GB

○ 3.99GB

○ Unlimited ✓

● 10% of the partition space

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

10

Which of the following is a database in which information about every file and directory on an NT File System (NTFS) volume is stored? *

○ Volume Boot Record

○ Master Boot Record

○ GUID Partition Table

● Master File Table ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

11

In the Windows Security Event Log, what does an event ID of **4625** and an error code of **0xC0000072** imply? *

○ Logon Failure – Unknown username or bad password

○ Logon Failure – User not allowed to logon at this computer

● Logon Failure – Account currently disabled ✓

○ Logon Failure – User logon from unauthorized workstation

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

12

What is one method of bypassing a system **BIOS** password? *

○ Removing the processor

● Removing the CMOS battery ✓

○ Remove all the system memory

○ Login to Windows and disable the BIOS password

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

13

A security analyst for a large chemical company was given credentials from a threat intelligence resources organization for internal users, which contain **usernames** and **valid passwords** for company accounts.
Which of the following is the first action the analyst should take as part of security operations monitoring? *

○ Run scheduled antivirus scans on all employees' machines to look for malicious processes.

○ Reimage the machines of all users within the group in case of a malware infection.

○ Change all the user passwords to ensure the malicious actors cannot use them.

● Search the event logs for event identifiers that indicate Mimikatz was used ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

14

Which list contains the most recent actions performed by a Windows User? *

● MRU (Most Recently Used) ✓

○ Activity

○ Recents

○ Windows Error Log

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

15

Windows identifies which application to open a file with by examining which of the following? *

● The file extension ✓

○ The file attributes

○ The file signature at the end of the file

○ The file signature at the beginning of the file

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

16

The command **rd /s /q C:\$Recycle.bin** is executed on a Windows machine to ___? *

○ Disable the Recycle Bin

○ Restore the files deleted from the Recycle Bin

● Repair the Recycle Bin ✓

○ Empty the Recycle Bin

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

17

What is the maximum size of the security log file after running the following command? **wevtutil sl Security /ms:1572864000** *

○ 150 MB

○ 1 GB

● 1.5 GB ✓

○ 15 GB

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

18

Windows Sysmon allows the recording of more information for IT security monitoring and threat detection, such as Event ID 1 (Process Creation) and Event ID 6 (Driver Loaded). However, why does it not completely replace Windows Advanced Audit Policy? (Choose all that apply) *

□ Windows Sysmon has a different log format and structure compared to Windows Event Logs.

☑ In Windows Sysmon, there are no events that log server logon information, such as Event 4624 in the Advanced Audit Policy ✓

□ Sysmon service log files are extremely large

☑ The Sysmon service may be incompatible with some software components on the server, such as antivirus (AV) and endpoint detection and response (EDR) solutions, potentially causing server crashes ✓

☑ Installing additional third-party software, such as Sysmon, on a server can increase risk if the Sysmon application contains vulnerabilities that allow for privilege escalation ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

19

Which of the following statements is incorrect when preserving digital evidence? *

○ Verify if the monitor is in on, off, or in sleep mode

● Turn on the computer and extract Windows event viewer log files ✓

○ Remove the plug from the power router or modem

○ Document the actions and changes that you observe in the monitor, computer, printer, or in other peripherals

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

20

Which of the following tools allows analysis of Windows Event Logs? (Choose all that apply) *

□ Wireshark

☑ Hayabusa ✓

☑ APT-Hunter ✓

☑ Event Viewer ✓

□ mimikatzt