|  |  |
| --- | --- |
| Diagram  Description automatically generated  Attack scenario challenges  A series of questions to challenge your knowledge | Abstract  Within this document you will find a series of questions that correspond to specific attack scenarios that were made available during the Microsoft Defender Masterclass event series.  Mark Thomas  Microsoft Defender Masterclass I – a partner event created by James Graham |

# Scenario 1

1. **Has the device been fully remediated?**

Within the evidence tab we can see that the following files were remidated

1 Point

1. **What Evidence has been collected?**

1 Point

1. **What permission does Zach have on the device?**

1 Point

1. **How was pooler-cpuminder-2.5.1-win32.zip downloaded?**

2 Point

1. **What URLs were used to download?**

1 Point for each

1. **How was the CoinMiner executed?**

1 Point

1. **How was the CoinMiner able to execute on the device?**

5 Points

1. **How could this have been prevented?**

2 Points

1. **Advanced Hunting: How can we see if any other processes accessed sourceforge?**

5 Points

1. **Advanced Hunting: How can we see what users have disabled Real-time protection using the registry?**

5 Points

# Scenario 2

1. **What device does the incident start with?**

1 Point

1. **What is PowerShell running in the first Suspicious PowerShell Alert?**

2 Points

1. **On which machines does cleanup.ps1 exist?**

1 Point

1. **How was the suspicious service registered on device trn-w2k12-1?**

1 Point

1. **What is the impact of the WDigest configuration change?**

2 Points

1. **Advanced Hunting: Find all machines where HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\SecurityProviders\Wdigest\UseLogonCredential was changed from 0 to 1**

5 Points

1. **What users have logged into trn-w2k12-1? BONUS Advanced Hunting: Did any other users log on to the device within 30 minutes of Wdigest registry change?**

1 Point (5 Points with AH)

1. **What URL did PowerShell make a suspicious network connection to on trn-w2k12-1 and what tool was executed?**

2 Points

1. **What devices have Suspicious Task Scheduler activity and what processes were involved?**

2 Points

1. **What executable does the suspicious scheduled tasks run?**

1 Point

1. **In the device timeline what key actions does the file browserhelp.exe perform?**

3 Points

1. **Advanced Hunting: Find PowerShell events that could involve a download.**

5 Points

1. **How could we stop the attack from its conclusion?**

3 Points

**Total points =**

**Out of 54**