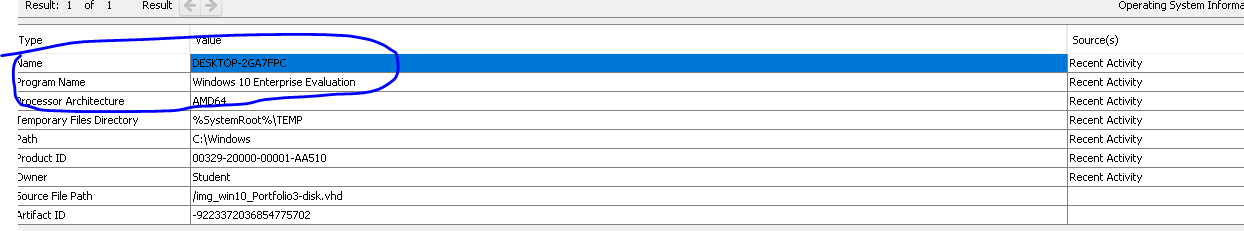
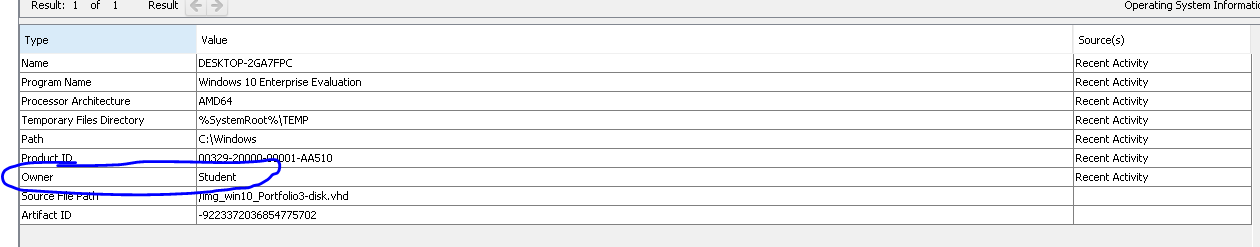
**Portfolio 4**

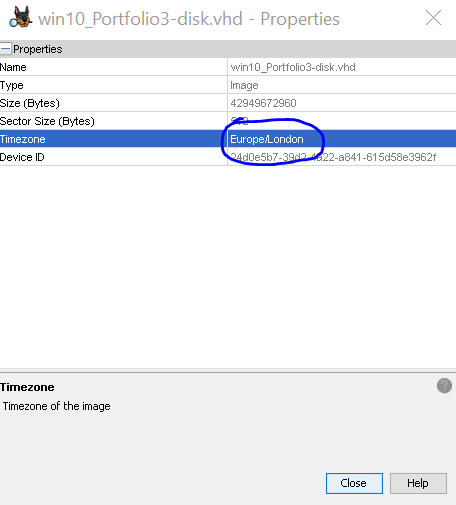
# Component 1

1) the name of the computer is DESKTOP-2GA7FPC

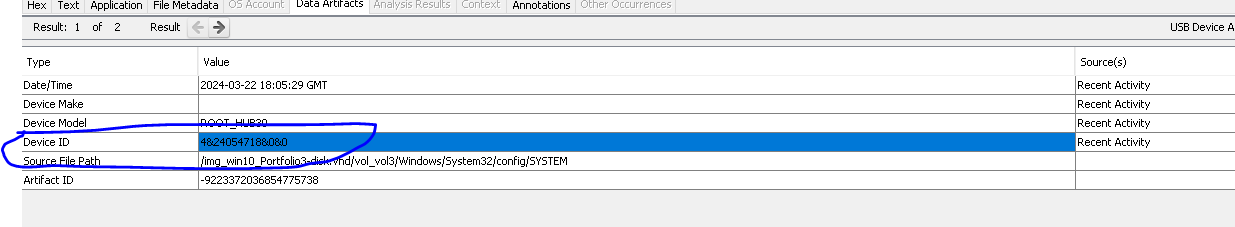


2) the owner of this device is student

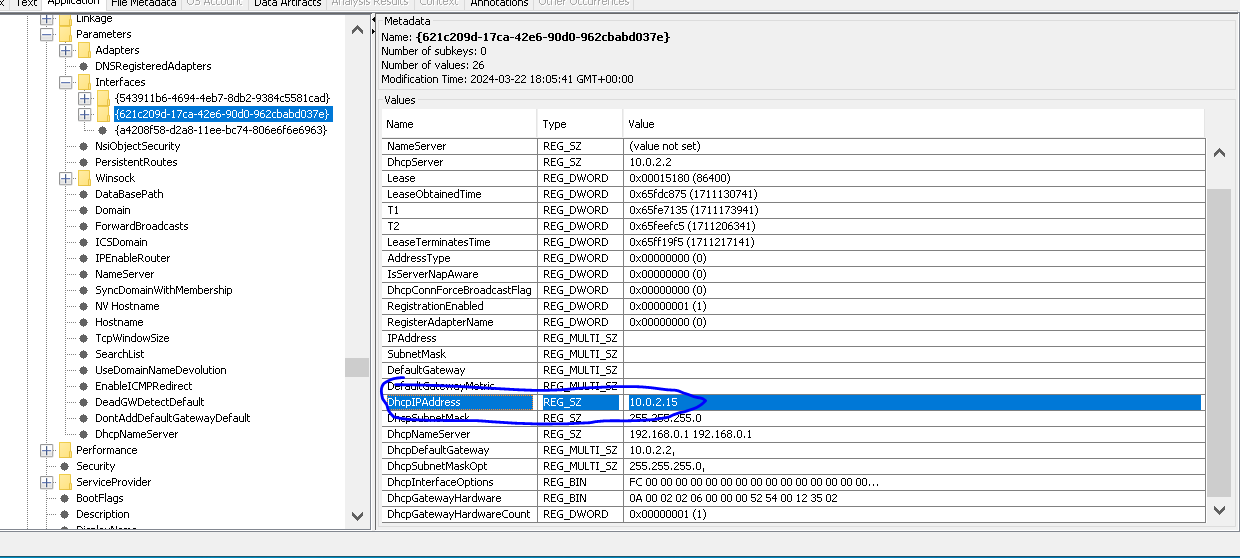


3) The time zone for this device is europe/london as you can see in the screenshot below

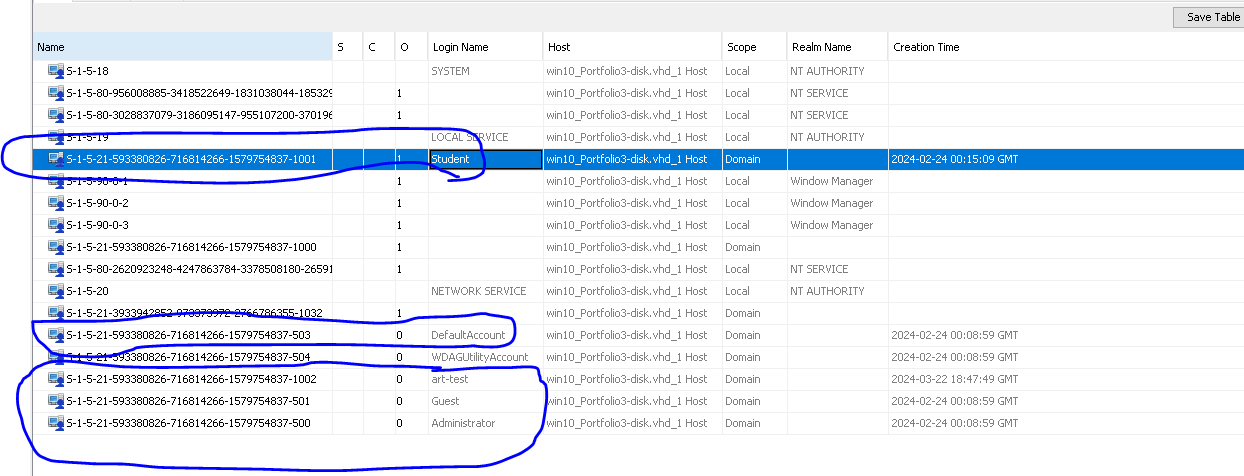
4) the device id is 4&24054718&0&0



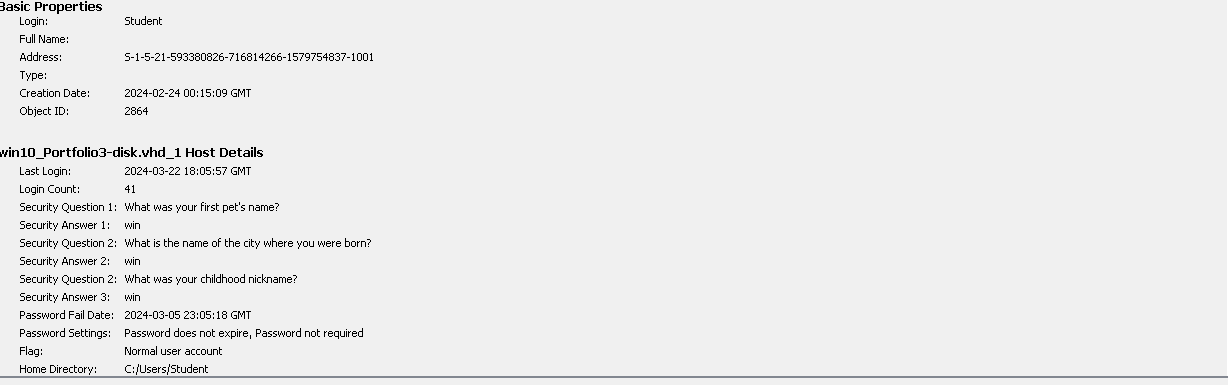
5) the DHCP IP address is 10.0.2.15

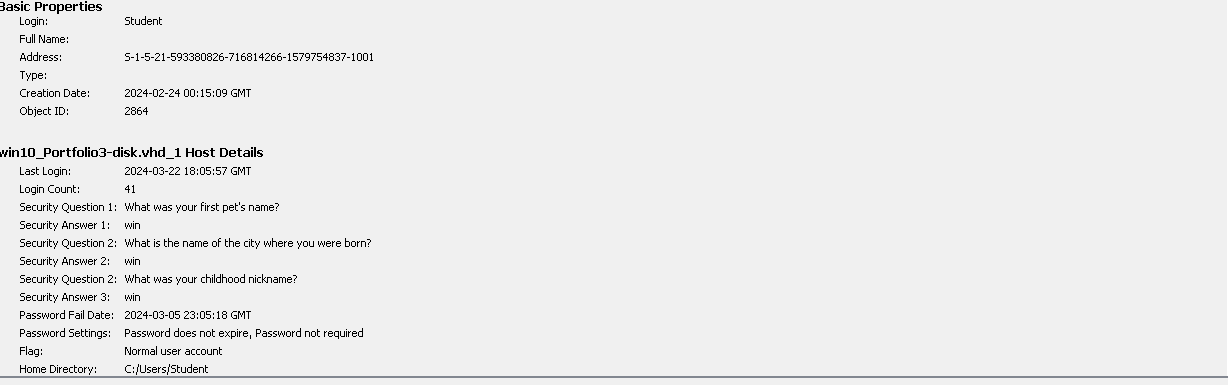


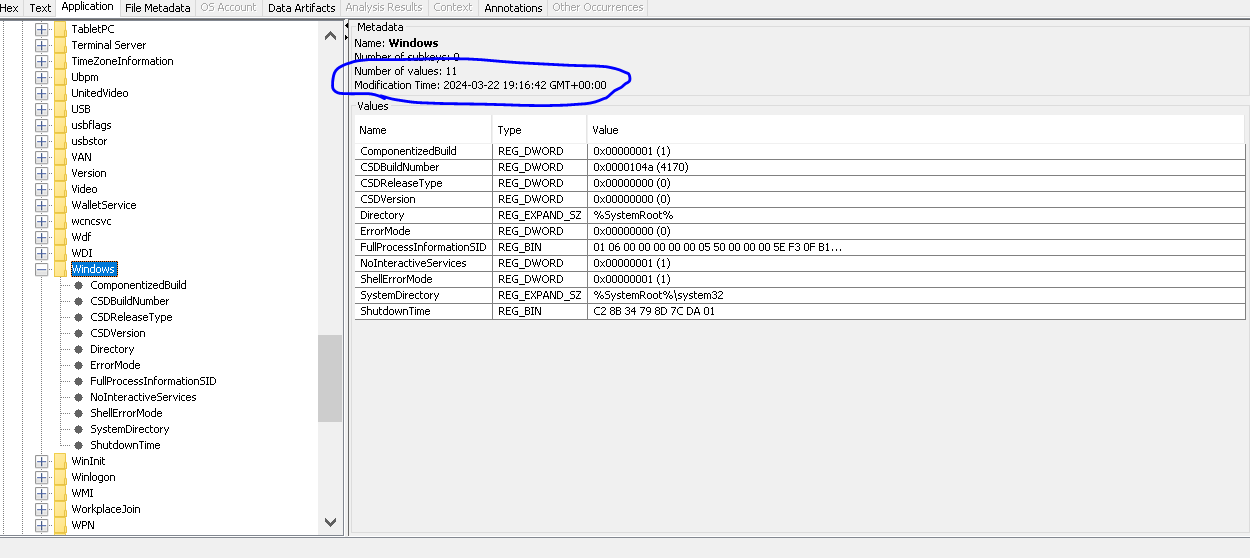
6) out of the 17 accounts there are only 5 user ones which have been circled



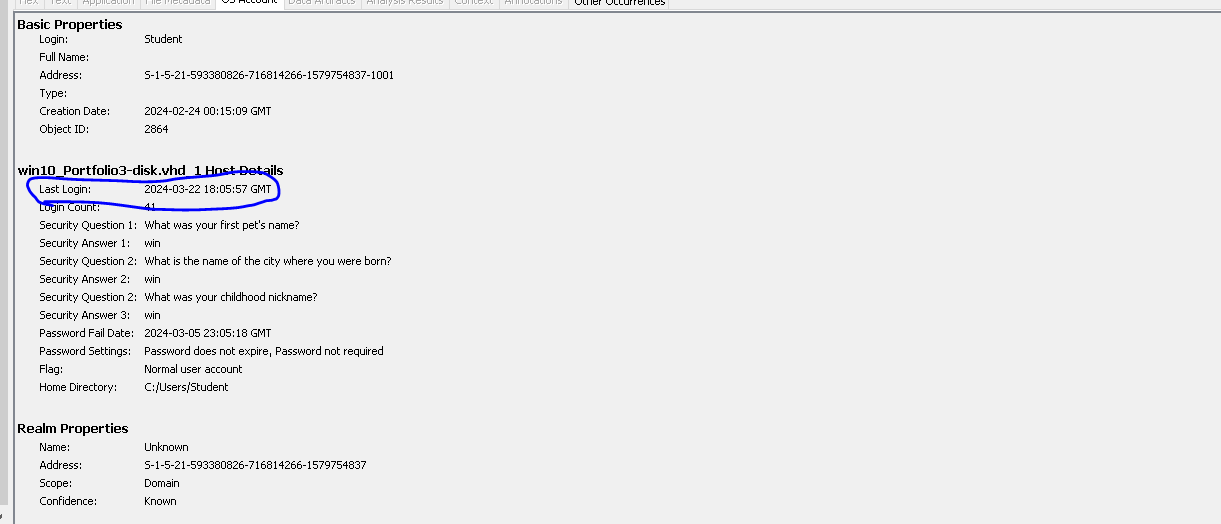
7) the last user to log in was student



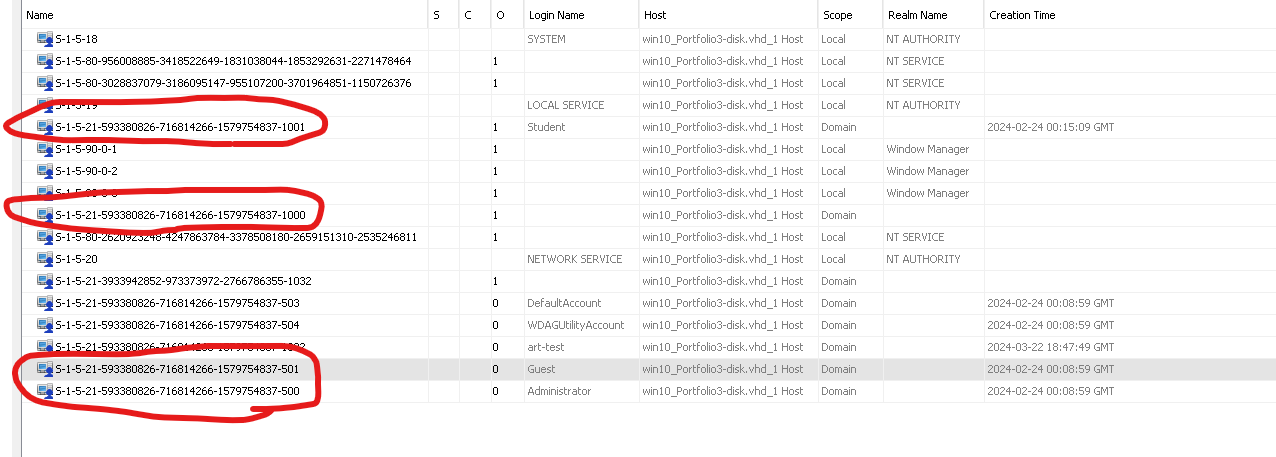
8) The account which had the most logins was Student with 41 logins to 0 on all the other accounts

9) Here is the last recorded shutdown of the computer 

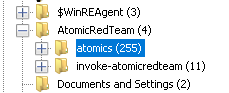
10) student was the only user logged in on the 22nd march 2024

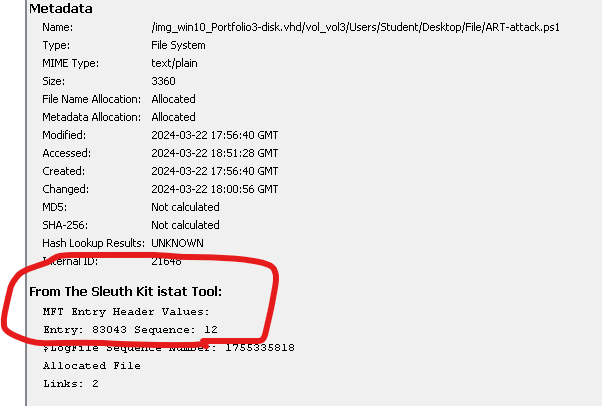


11) there was only 1 account created on the 22nd march which was art-test

12) the account with the code –500 is an administrator account, there are other possible admin accounts but you can’t find them using autopsy 

13) there are 252 + 9 different files under atomic red team. Its –2 for each folder because 2 of those files are [current folder] and [parent folder]



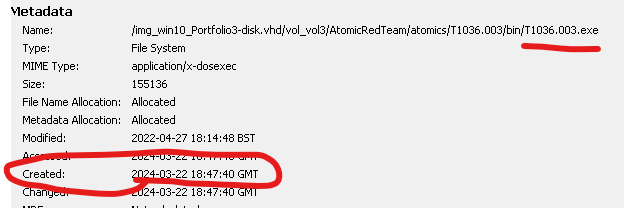
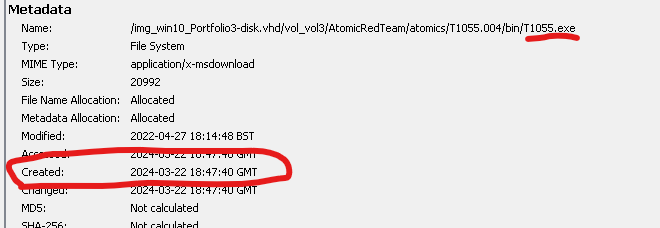
14) the MFT entry number for the ART-attacks.ps1 file is 

15) I navigated to system/controlset001/services/bam/state/usersettings and there I found the user with the RID 1001 and here are the .exe files ran with the last modification time shown too

A screenshot of a computer

Description automatically generated

16) T1055.exe and T1036.003.exe was created 22nd March 2024 as you can see in the ss below



17) there were 802 .exe files ran on 22nd march. I used the timeline tool to filter for run programs on the 22nd march only A screenshot of a computer

Description automatically generated

18) there were 149 .dll files created on march 22nd I extracted all the .dll files created on march 22nd into excel and counted all the rows -1 for the heading A screenshot of a computer

Description automatically generated

19) there were 11 .bat files created on march 22ndA screenshot of a computer

Description automatically generated

20) notepad was opened on 22nd march as you can see it was accessed multiple times throughout that dateA screenshot of a computer

Description automatically generated

21) the malicious file ART-attack.ps1 was last accessed on 22nd march at 18:51:28 and was accessed by the user Student

A screenshot of a computer

Description automatically generated

22) There is evidence that the Sysmon.exe file was executed on march 22ndA screenshot of a computer

Description automatically generated

23) there is even evidence that AdFind was installed and executed I searched for terms related to AdFind and found over 100 files relating to it along with different descriptions of tests you can do using AdFind

A screenshot of a computer

Description automatically generated

24) in the screen shot below it shows all the times powershell was used on march 22nd and what commands were usedA screenshot of a computer

Description automatically generated

25) the size of AtomicService.exe is 8063 KB in the prefetch files, there is another file called atomicservice.exe with a different size but it isn’t located in the windows/prefetch however that files size is 4096 KB

A screenshot of a computer

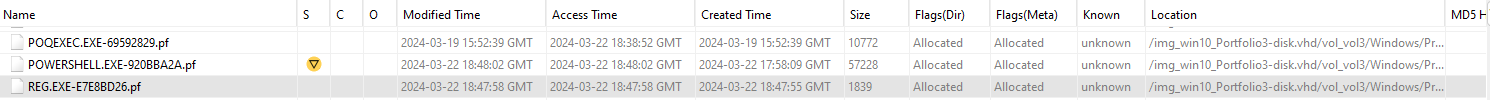
Description automatically generated

26) the timeline is from earliest to latest (top = earliest)

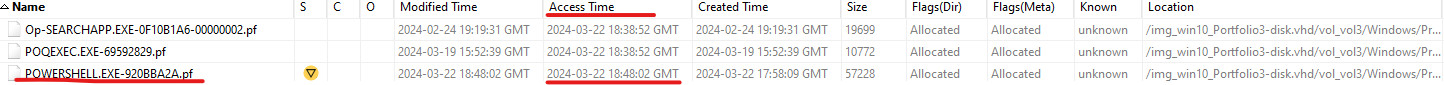
Net.exe last accessed on 18:47:50 on march 22nd



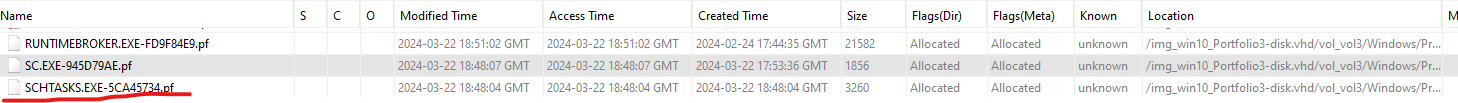
Reg.exe last accessed on 18:47:58 on march 22nd



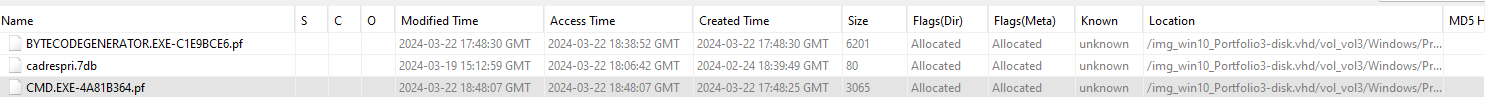
powershell.exe last accessed 18:48:02 on march 22nd



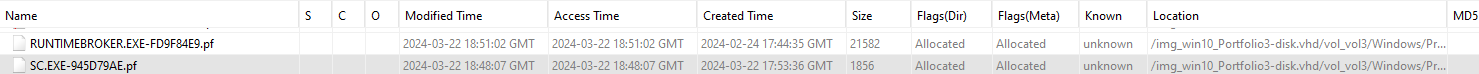
Schtasks.exe last accessed on 18:48:04 on march 22nd



Cmd.exe last accessed on 18:48:07 on march 22nd



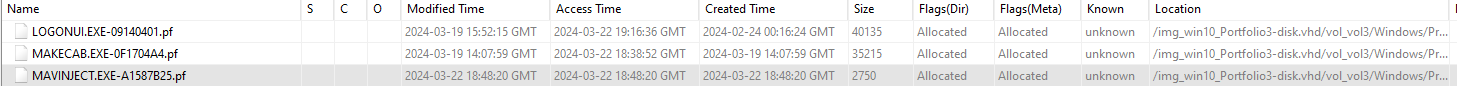
Sc.exe last accessed on 18:48:07 on march 22nd



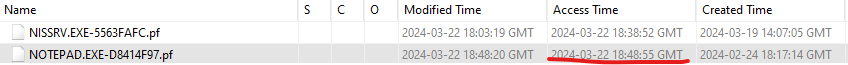
Atomicservice.exe last accessed on 18:48:17 on march 22nd



Manvinject.exe last accessed on 18:48:20 on march 22nd



Notepad.exe last accessed on 18:48:55 on march 22nd



27) to navigate to the file blow I had to go to NTUSER.DAT/SOFTWARE/Microsoft/Windows/Run however there is no AtomicService.exe file its called AtomicRedTeam.exe here the AtomicService.exe file is located in AtomicRedTeam/atomics/T1543.003/bin and isn’t inside the NTUSER.DAT hive

A screenshot of a computer

Description automatically generated

28) the suspicious file in the startup folder is batstartup.bat its suspicious because there should only be 1 file In here along with the extracted text having the T1547 name in it which relates to the atomic red team. Furthermore it is created at the same time as the atomic red team was run meaning it is probably from there and is malicious

A screenshot of a computer

Description automatically generated

29) I found 1 file for each on log on and on start up which seemed suspicious as their name related to the atomic red team

A screenshot of a computer

Description automatically generated

30) The PID for notepad.exe is 916 as seen in the screenshot below



# WOW FACTOR

The malware found on this device is Atomic Red Team (ART) which can run scripts and commands using powershell to perform attacks, it can also exploit its way to gain higher privileges to further attack a system.

For the wow factor I chose to analyse the shell bags in autopsy, shell bags can be used to create a timeline of events for when the user accessed certain folders and it records them going from folder to folder.

A screenshot of a computer

Description automatically generated

For example in this screen shot is shows the user accessed control panel and may have changed some particular settings relating to the network and security of the device to potentially weaken it making it easier to compromise with malicious software.

A screenshot of a computer program

Description automatically generated

In this screenshot is shows the computer had potentially an external device in it, relating to the D drive being accessed. Furthermore in this screenshot you can see the user navigating to user/student/document for something in particular then accessing the program files along with windows security. They then accessed the windows logs of the computer