Possible Solution

What date and time the infected memory image was collected?

- Plugin: imageinfo
- By defining the profile in the command, the results of the scan should appear after seconds to 1-2 minutes.
- Correct answers (either is ok):
  - Image date and time : 2021-07-22 05:49:20 UTC+0000
  - Image local date and time : 2021-07-22 07:49:20 +0200

Which plugin of Volatility generates a list of processes as a tree?

- Command: vol.py -h | grep process
- Correct answer: pstree

What is the IP address of the investigated computer?

- Plugin: netscan
- Correct answer: 192.168.240.129

What is the name and the PID of the malicious process?

- Plugin: cmdline
- Correct answer:
  - Name: gcttt.exe
  - PID: 5040

List a maximum of 5 additional executables that reside in the same path as the malicious process and that have the same execution timestamp as the malicious process.

- Plugin: mftparser
- Correct answer:
  - Newptad284.exe
  - Install.exe
  - askinstall20.exe
  - md2_2efs.exe
  - BTRSetp.exe
  - Duplicates are NEWPTA-1, ASKINS-1 and shouldn't count as correct answer.
  - Gcttt.exe doesn't qualify for "all other executable names" as specified in the task.

Dump the malicious process into a file and search the file for a suspicious ASCII URL string that most likely is hosting other malware components. What's the registrar of that domain? Record the ASCII URL and the domain name registrar.

Dumping:

- Plugin / command: procdump -p 5040

Searching:

- Command: strings executable.5040.exe | grep http
- Correct answer: http[:]//uehge4g6Gh[.]2ihsfa[.]com (or screenshot of actual URL)
- Strings encoded in Unicode will not show the desired URL, however ASCII encoded strings command will do.
- Please note that the [] brackets are here to disarm the link. Conscious candidates should know that potentially malicious links should be disarmed first. There are many ways to do this. Brackets are common practice.

Registrar:

- Approach: "whois" query on the internet
- Correct answer: NameCheap Inc.

Which of the DLLs linked to the malicious process is most likely responsible for initiating HTTP Internet connections?

- Plugin / command: impscan -p 5040 | grep -i http
- Correct Answer: WINHTTP.DLL

What is the SID of the user account under which the process was executed?

- Plugin / command: getsids | grep gcttt.exe
- Correct answer: S-1-5-21-2016556524-1009367435-3578074633-1000