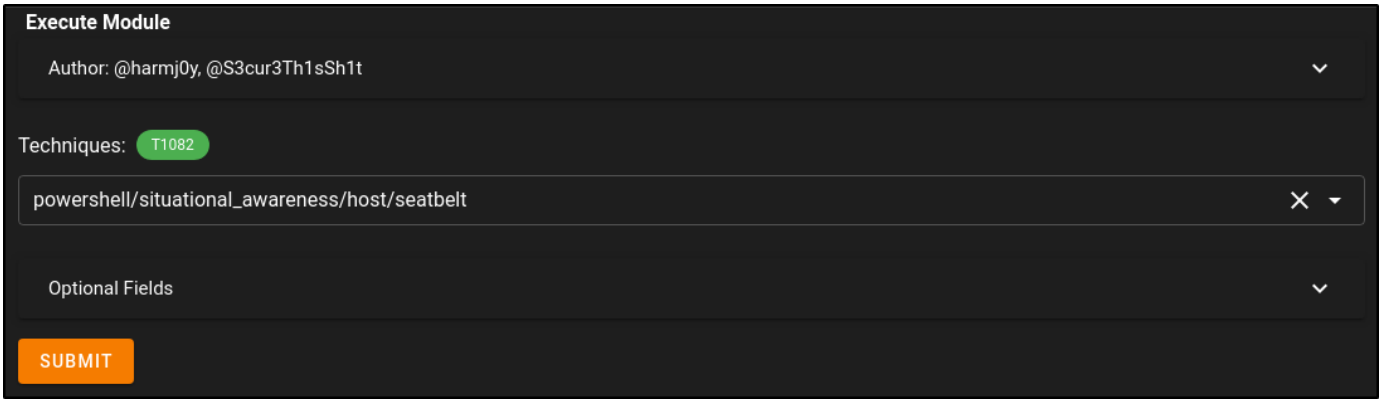
18

You have a c2 agent responding back from THROWBACK-PROD, now we need to elevate our privileges in order to dump hashes and passwords with mimikatz.
Your team has suggested to run an enumeration script like winPEAS or seatbelt to enumerate what services and privileges may be misconfigured on the device and can be exploited to escalate privileges.

Loading and Executing the Module
Note: The purpose of this task is to show you how to load and execute tasks using Starkiller. In order for Seatbelt (and the Privilege Escalation) to work properly, you should run Seatbelt over an RDP Session using the pre-compiled binary that can be found here: https://github.com/r3motecontrol/Ghostpack-CompiledBinaries

We can use use the seatbelt module within Starkiller to help enumerate the device and find potential attack vectors.

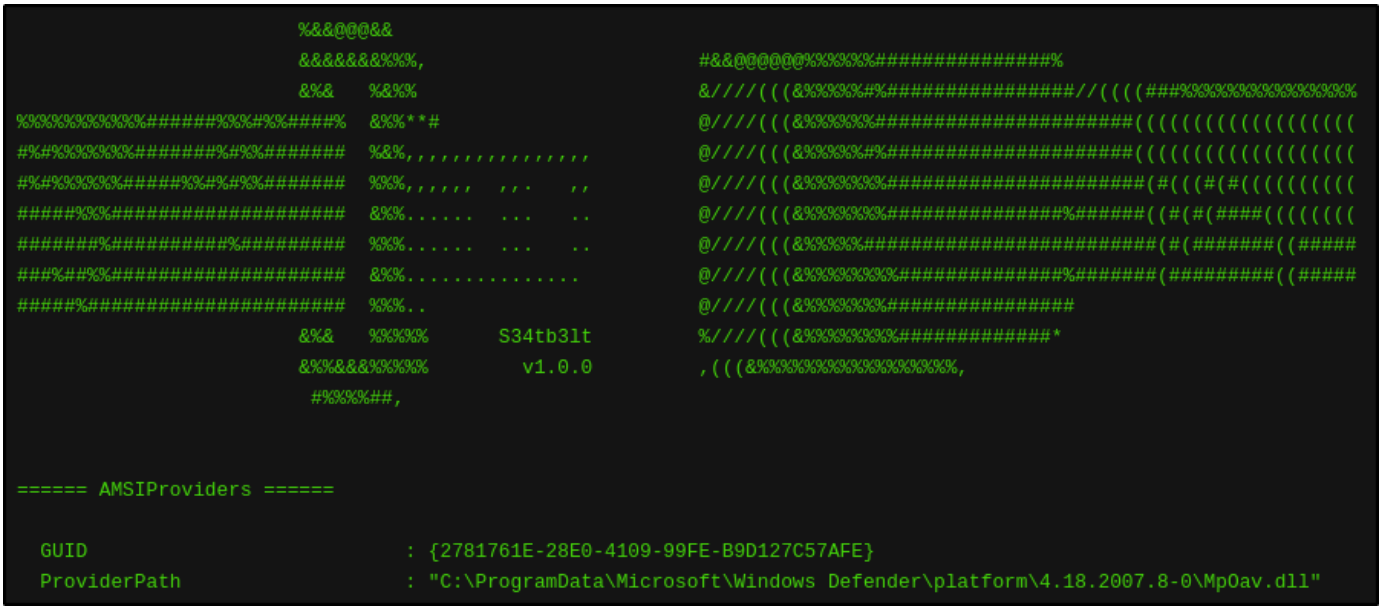
1.) The module for seatbelt is powershell/situational_awareness/host/seatbelt



Loading the seatbelt module in Starkiller

This particular modules has no field that needs to be set so we can simply submit the module and execute it.

2.) Press Submit



Enumerating the device with seatbelt

Now that seatbelt has run its safety checks we can look through the output and see if there is anything immediately obvious.

Searching Seatbelt Output

From seatbelt we can see that there may be a user account that has credentials stored within the credentials manager. We can abuse this feature to use saved creds to run a file with the accounts privileges.

```
====== CredEnum ======

  Target             : localadmin.pass
  UserName           :
  Password           :
  CredentialType     : DomainPassword
  PersistenceType    : Enterprise
  LastWriteTime      : 8/25/2020 2:52:57 AM

====== CredGuard ======
```

Found user within seatbelt

```
====== WindowsVault ======


  Vault GUID     : 4bf4c4                        04ddb28
  Vault Type     : Web Credentials

ERROR: Exception: VAULT_ELEMENT_TYPE 'ByteArray' is currently unimplemented
ERROR: Exception: VAULT_ELEMENT_TYPE 'ByteArray' is currently unimplemented

  Vault GUID     : 77bc5                          f3b29
  Vault Type     : Windows Credentials
```

Enumerating the Windows Credential Manager

Exploiting Credentials Manager

Since we know that there are saved credentials within the credentials manager from seatbelt we can utilize the windows 'runas' to run a file as an elevated user and escalate privileges.

Note: You will need an rdp session on the device in order to successfully run this command and escalate privileges.

1.) runas /savecred /user: /profile "cmd.exe"

```
C:\Users\       >runas /savecred /user:              /profile cmd.exe
Attempting to start cmd.exe as user "THROWBACK-PROD\             " ...

C:\Users\       >_
```

Executing runas to execute cmd.exe as a local admin

SUCCESSS! If executed properly the device will open a new command prompt that now has elevated privileges. In order to continue using Starkiller you will need to reupload launcher.bat or multi/launcher to get an elevated agent on the machine.

Now that you have elevated privileges you can look for the root flag and move onto post exploitation attacks.

Answer the questions below

What user was found from seatbelt?

Correct Answer

Submit flag for THROWBACK-PROD in Task 4

Question Done