ProcNet Challenge

Task 1:
To which IP address and port number is the malware attempting to establish a connection ?

I checked the Sysmon logs for event ID 3 in both files and found it on the Desktop logs.

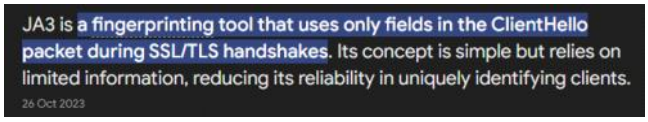
```
The description for Event ID ( 3 ) in Source ( Microsoft-Windows-Sysmon ) could not be found.
Either the component that raises this event is not installed on the computer or the installation is
corrupted.You can install or repair the component or try to change Description Server.

The following information was included with the event:
-
2023-05-22 08:19:07.389
{5080714d-1856-646b-df01-000000000a00}
6148
C:\Users\alonzo.spire\Downloads\csgo.exe
FORELA\alonzo.spire
tcp
true
false
10.10.0.79
-
50088
-
false
3.6.165.8
-
443
-
```

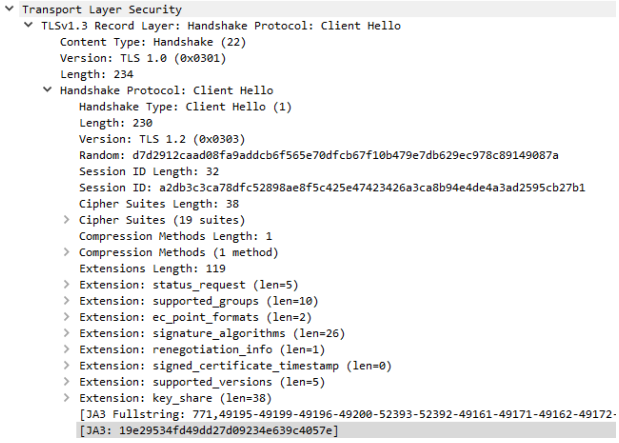
Answer: 3.6.165.8:443

Task 2:
Now that you are aware of the IP address and port number, what is the JA3 fingerprint of the C2 server ?

I checked on Google what is JA3 fingerprint



Then I searched in Wireshark for ip.addr == 3.6.165.8 && tcp.port == 443 and looked for a Client Hello packet



Answer: 19e29534fd49dd27d09234e639c4057e

Task 3:
What is the name of the C2 framework being utilized by the red team ?

I filtered in Wireshark for "ip.addr == 3.6.165.8 && http" and found a GET request to csgo.exe
Checking the TCP Stream there is "MZ" which means there is an executable

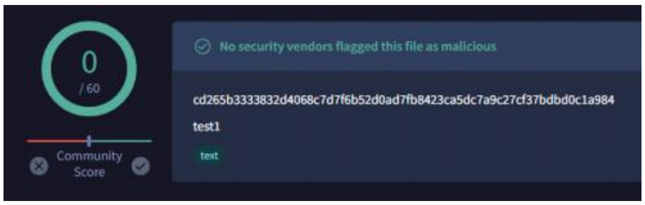
```
GET /csgo.exe HTTP/1.1
Host: 3.6.165.8:8080
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://3.6.165.8:8080/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.10.6
Date: Mon, 22 May 2023 08:19:21 GMT
Content-type: application/x-msdos-program
Content-Length: 17056768
Last-Modified: Sun, 21 May 2023 10:24:52 GMT

MZ......................@...........................................          .!..L.!This program cannot be run in DOS mode.

$.......PE..d........B........"......F....................@............................. ............`... ......................................
....@...H...........................text.....E.......F.................. ..`.rdata....]..`....]..L..............@..@.data....K...................
```

I saved as filename.exe and then took the hash and checked it on Virus Total but the file was clean without any indicators about it



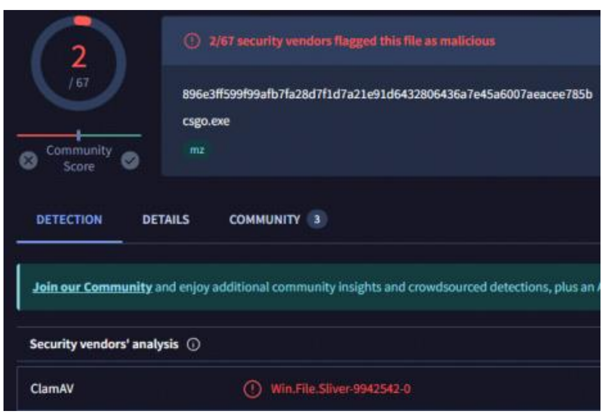
So I opened the filename.txt with Notepad and saw all the GET requests above the MZ so I deleted everything until the MZ and saved it again and took the hash again to Virus Total - BFAE4066E2177FB2E35CCA537A5119AC

```
GET /csgo.exe HTTP/1.1
Host: 3.6.165.8:8080
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://3.6.165.8:8080/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.10.6
Date: Mon, 22 May 2023 08:19:21 GMT
Content-type: application/x-msdos-program
Content-Length: 17056768
Last-Modified: Sun, 21 May 2023 10:24:52 GMT

MZ......................@...........................................  .!..L.!This program cannot be run in DOS mode.
```

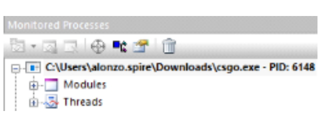
This time the file was found reported as known as "Sliver"

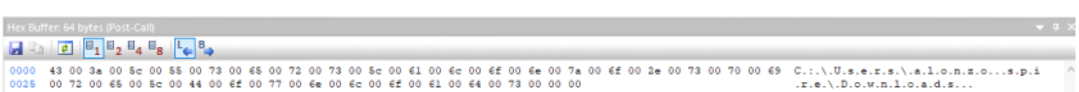


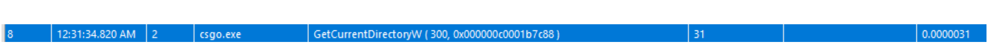
Answer: sliver

Task 4:
Which WIN32 API provided the red team with the current directory information ?

I opened the file Employee.apmx64 and at the Monitored processes I clicked on the csgo.exe and starting searching in the Summary table until I found at path directory in the Hex Buffer







The API is right to the csgo.exe

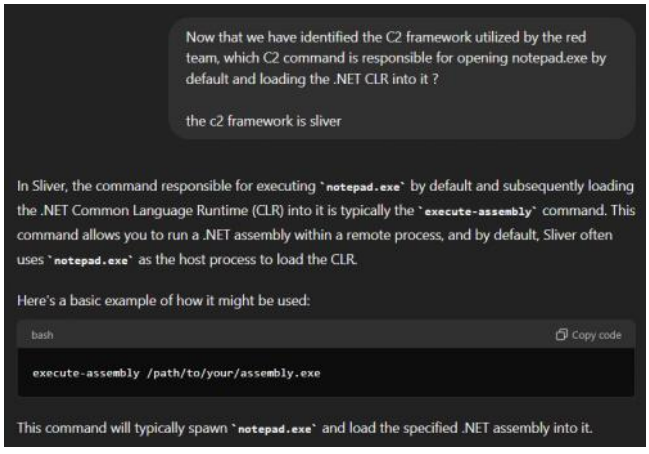
Answer: GetCurrentDirectoryW

Task 5:
Now that we have identified the C2 framework utilized by the red team, which C2 command is responsible for opening notepad.exe by default and loading the .NET CLR into it ?

I searched for "CLR" inside the notepad.exe in the Modnitored Processes and noticed a lot of "clr.dll"

1777	12:33:58.452 AM	1	clr.dll
1778	12:33:58.452 AM	1	clr.dll
1779	12:33:58.452 AM	1	clr.dll
1780	12:33:58.452 AM	1	clr.dll
1781	12:33:58.452 AM	1	clr.dll
1782	12:33:58.452 AM	1	clr.dll
1783	12:33:58.452 AM	1	clr.dll
1784	12:33:58.452 AM	1	clr.dll
1785	12:33:58.452 AM	1	clr.dll
1786	12:33:58.452 AM	1	clr.dll
1787	12:33:58.452 AM	1	clr.dll
1788	12:33:58.452 AM	1	clr.dll
1789	12:33:58.452 AM	1	clr.dll
1790	12:33:58.452 AM	1	clr.dll
1791	12:33:58.452 AM	1	clr.dll
1792	12:33:58.452 AM	1	clr.dll

Then I asked the ChatGPT



Answer: execute-assembly

Task 6:
What is the name of the module (DLL) that was loaded to gain access to Windows Vault ?

I searched for vault inside the API Monitor and found the DLL name

26539	12:34:00.818 AM	1	clr.dll	WideCharToMultiByte (CP_UTF8, 0, "vaultcli.dll", 13, 0x000000867b3bdc50, 37, NULL, NULL)	13		0.0000004
26540	12:34:00.818 AM	1	clr.dll	HeapAlloc (0x0000022d8a590000, 0, 36)	0x0000022d8a6...		0.0000002
26541	12:34:00.818 AM	1	clr.dll	HeapAlloc (0x0000022d8a590000, 0, 132)	0x0000022d8a6...		0.0000003
26542	12:34:00.818 AM	1	clr.dll	WideCharToMultiByte (CP_UTF8, 0, "VaultOpenVault", -1, NULL, 0, NULL, NULL)	15		0.0000003
26543	12:34:00.818 AM	1	clr.dll	WideCharToMultiByte (CP_UTF8, 0, "VaultOpenVault", -1, 0x0000022d8a641af3, 381, NULL, NULL)	15		0.0000002
26544	12:34:00.818 AM	1	clr.dll	WideCharToMultiByte (CP_UTF8, 0, "VaultCloseVault", 16, 0x000000867b3bdba0, 46, NULL, NULL)	16		0.0000002
26545	12:34:00.818 AM	1	clr.dll	WideCharToMultiByte (CP_UTF8, 0, "vaultcli.dll", 13, 0x000000867b3bdc50, 37, NULL, NULL)	13		0.0000001
26546	12:34:00.818 AM	1	clr.dll	WideCharToMultiByte (CP_UTF8, 0, "VaultCloseVault", -1, NULL, 0, NULL, NULL)	16		0.0000003
26547	12:34:00.818 AM	1	clr.dll	WideCharToMultiByte (CP_UTF8, 0, "VaultCloseVault", -1, 0x0000022d8a641b03, 365, NULL, NULL)	16		0.0000002
26548	12:34:00.818 AM	1	clr.dll	WideCharToMultiByte (CP_UTF8, 0, "VaultFree", 10, 0x000000867b3bdbb0, 28, NULL, NULL)	10		0.0000001
26549	12:34:00.818 AM	1	clr.dll	HeapAlloc (0x0000022d8a590000, 0, 56)	0x0000022d8a6...		0.0000003
26550	12:34:00.818 AM	1	clr.dll	WideCharToMultiByte (CP_UTF8, 0, "vaultcli.dll", 13, 0x000000867b3bdc50, 37, NULL, NULL)	13		0.0000002
26551	12:34:00.818 AM	1	clr.dll	WideCharToMultiByte (CP_UTF8, 0, "VaultFree", -1, NULL, 0, NULL, NULL)	10		0.0000002
26552	12:34:00.818 AM	1	clr.dll	WideCharToMultiByte (CP_UTF8, 0, "VaultFree", -1, 0x0000022d8a641b0d, 355, NULL, NULL)	10		0.0000002

Answer: vaultcli.dll

Task 7:
After loading the mentioned module, there were a series of WIN32 APIs loaded. Which specific Win32 API is responsible for enumerating vaults ?

I keep searching for the vault like task 6 until I found the API

26948	12:34:00.866 AM	1	clr.dll	GetProcAddress (0x00007fff16860000, "VaultEnumerateVaults")	0x00007fff1687...		0.0000031
26949	12:34:00.866 AM	1	clr.dll	GetProcAddress (0x00007fff16860000, "VaultEnumerateVaultsW")	NULL	127 = The specified pr...	0.0000020

Answer: VaultEnumerateVaults

Task 8:
Which command did the attacker execute to identify domain admins ?

In the Monitored Proceesses I clicked on the net.exe and at the Summary I found some

reconnaissance commands

17	12:41:11.691 AM	1	net.exe	_wcsnicmp ("/YES", "/dom", 4)	21		0.0000010
18	12:41:11.691 AM	1	net.exe	_wcsnicmp ("/NO", "/dom", 4)	10		0.0000003
19	12:41:11.691 AM	1	net.exe	_fileno (0x00007fff30f8fa00)	0		0.0000027
20	12:41:11.691 AM	1	net.exe	_setmode (0, _O_TEXT)	_O_TEXT		0.0000032
21	12:41:11.691 AM	1	net.exe	_wcsicmp ("use", "group")	14		0.0000029
22	12:41:11.691 AM	1	net.exe	_wcsicmp ("view", "group")	15		0.0000002
23	12:41:11.691 AM	1	net.exe	_wcsicmp ("use", "domain admins")	17		0.0000003
24	12:41:11.691 AM	1	net.exe	_wcsicmp ("view", "domain admins")	18		0.0000003
25	12:41:11.691 AM	1	net.exe	wcschr ("net group "domain admins" /dom", ' ')	0x0000029595f...		0.0000003
26	12:41:11.691 AM	1	net.exe	wcscpy_s (0x0000029595f80416, 277, "\net1")	0		0.0000029
27	12:41:11.691 AM	1	net.exe	wcscat_s ("C:\WINDOWS\system32\net1", 296, " group "domain admins" /dom")	0		0.0000004

Answer: net group "domain admins" /dom

Task 9:
The red team has provided us with a hint that they utilized one of the tools from "ARMORY" for lateral movement to DC01. What is the name of the tool ?

I completed this task with a dirty way.

I told ChatGPT to give me the tools name of the Armory of Sliver C 2 framework and he leads me to an article
https://bishopfox.com/blog/passing-the-osep-exam-using-sliver

Armory Goodness

If you haven't done this yet, I suggest you install all (or some) of the armory extensions. The armory helps Sliver shine, and I constantly used them during my labs, practice tests, and final exam. You can do so with **`armory install all`** and give it a minute or so.

```
sliver (AMUSED_GEMSBOK) > armory install all

? Install 20 aliases and 106 extensions? Yes
[*] Installing alias 'Sharp Hound 3' (v0.0.2) ... done!
[*] Installing alias 'sqlrecon' (v0.0.2) ... done!
[*] Installing alias 'SharpHound v4' (v0.0.1) ... done!
[*] Installing alias 'SharpChrome' (v0.0.2) ... done!
[*] Installing alias 'SharpRDP' (v0.0.1) ... done!
[*] Installing alias 'SharpView' (v0.0.1) ... done!
[*] Installing alias 'KrbRelayUp' (v0.0.1) ... done!
[*] Installing alias 'SharPersist' (v0.0.2) ... done!
[*] Installing alias 'SharpDPAPI' (v0.0.2) ... done!
[*] Installing alias 'sharpsh' (v0.0.1) ... done!
[*] Installing alias 'NoPowerShell' (v0.0.1) ... done!
[*] Installing alias 'Sharp SMBExec' (v0.0.3) ... done!
[*] Installing alias 'Certify' (v0.0.3) ... done!
[*] Installing alias 'SharpUp' (v0.0.1) ... done!
[*] Installing alias 'Sharp WMI' (v0.0.2) ... done!
[*] Installing alias 'Seatbelt' (v0.0.4) ... done!
[*] Installing alias 'Rubeus' (v0.0.22) ... done!
[*] Installing alias 'SharpSecDump' (v0.0.1) ... done!
[*] Installing alias 'SharpLAPS' (v0.0.1) ... done!
[*] Installing alias 'SharpMapExec' (v0.0.1) ... done!
[*] Installing extension 'credman' (v1.0.7) ... done!
```

Then I looked for a tool which ends with "I"

Answer: sharpwmi

Task 10:
Which command was executed by the red team to extract/dump the contents of NTDS.DIT ?

I investigated the Sysmon logs and searched for event ID 1 of the DC01 and looked for any NTDS activity and found a cmd command line.

Description ×

```
The description for Event ID ( 1 ) in Source ( Microsoft-Windows-Sysmon ) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You
can install or repair the component or try to change Description Server.

The following information was included with the event:
-
2023-05-22 07:55:26.448
{524bc579-1fee-646b-5701-000000000900}
6800
C:\Windows\System32\conhost.exe
10.0.14393.0 (rs1_release.160715-1616)
Console Window Host
Microsoft® Windows® Operating System
Microsoft Corporation
CONHOST.EXE
\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
C:\Windows
NT AUTHORITY\SYSTEM
{524bc579-15c0-646a-e703-000000000000}
0x3e7
0
System
SHA1=00667A0F0C0D5E9DA697E9FF54ECDDD449259354,MD5
=D752C96401E2540A443C599154FC6FA9,SHA256=
046F7A1B4DE67562547ED9A180A72F481FC41E803DE49A96D7D7C731964D53A0,IMPHASH=
2C980A4DA7C717CC670CB9E1D2C4D733
{524bc579-1fee-646b-5601-000000000900}
7332
C:\Windows\System32\cmd.exe
cmd /c ntdsutil "ac in ntds" ifm "cr fu %TEMP%\H00i0Z000.dat" q q
NT AUTHORITY\SYSTEM
```

Answer: cmd /c ntdsutil "ac in ntds" ifm "cr fu %TEMP%\H00i0Z000.dat" q q

Task 11:
The red team has obtained the aforementioned dump by compressing it into a ZIP file. Which specific Win32 API is responsible for retrieving the full path of the file to be downloaded?

I searched inside the DC01.apmx file for NTDS in the fifa24.exe

11515	1:04:27.591 AM	5	fifa24.exe	GetFullPathNameW ("ntds.zip", 100, 0x000000c000076000, NULL)	38	0.0000065

Answer: GetFullPathNameW