BlackBerry

Devel
CYBERSECURITY REDEFINED

DSOC
CERT

DFIR Y THREAT HUNTING

Antes que entren, vamos a cazarlos.

Triada de la Ciberseguridad.

(Confidencialidad, Disponibilidad e Integridad)

Cyber Kill Chain.

(7 Pasos para el desastre)

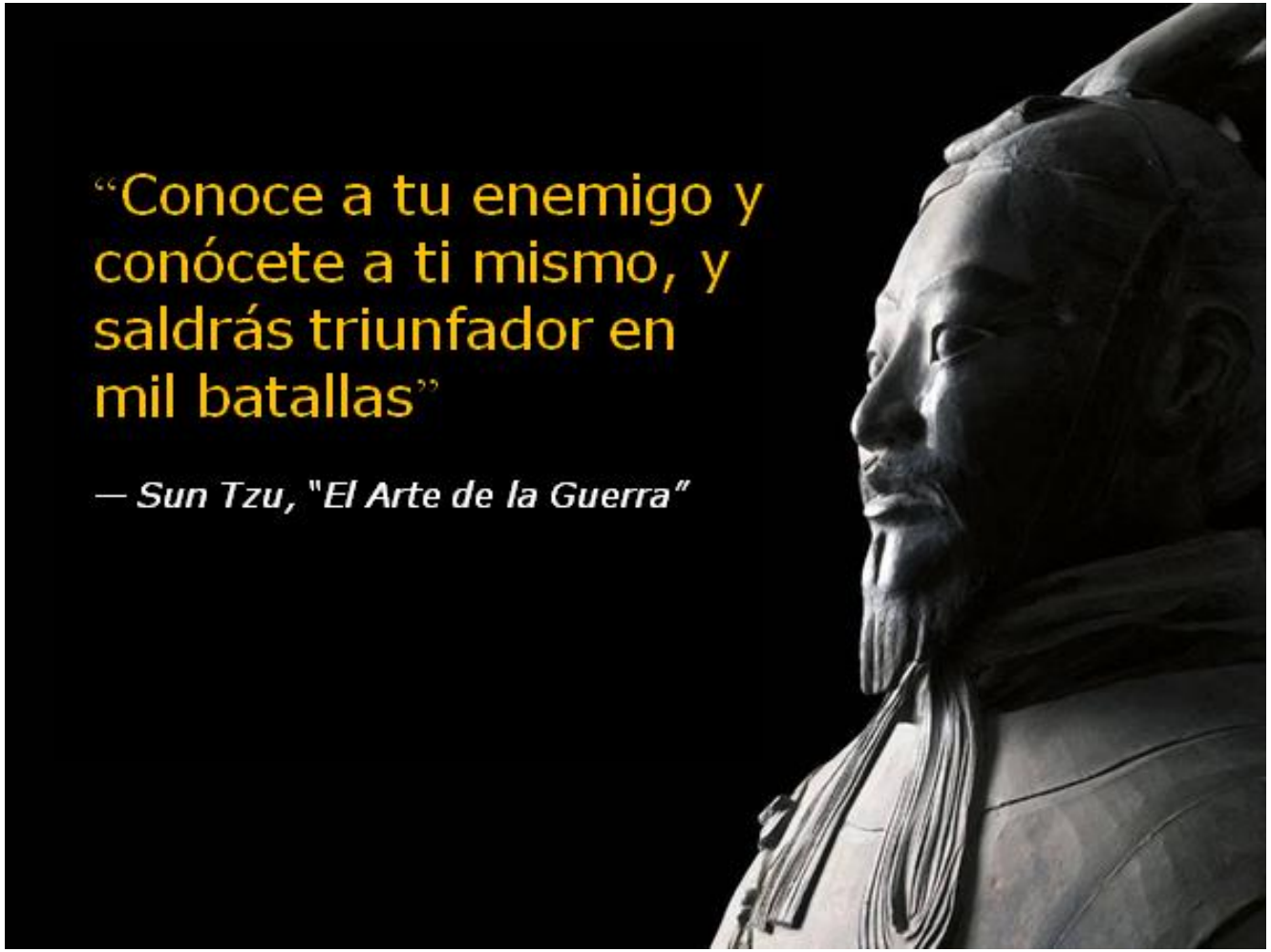
DFIR.

(Digital Forensics and Incident Response)

DFIR: Proceso de respuesta a incidente, donde se recolecta información de los equipos comprometidos para su análisis y determinar la causa raíz del incidente y llegar a la resolución dejando los equipos operativos nuevamente.

CONOCE A TU ENEMIGO.

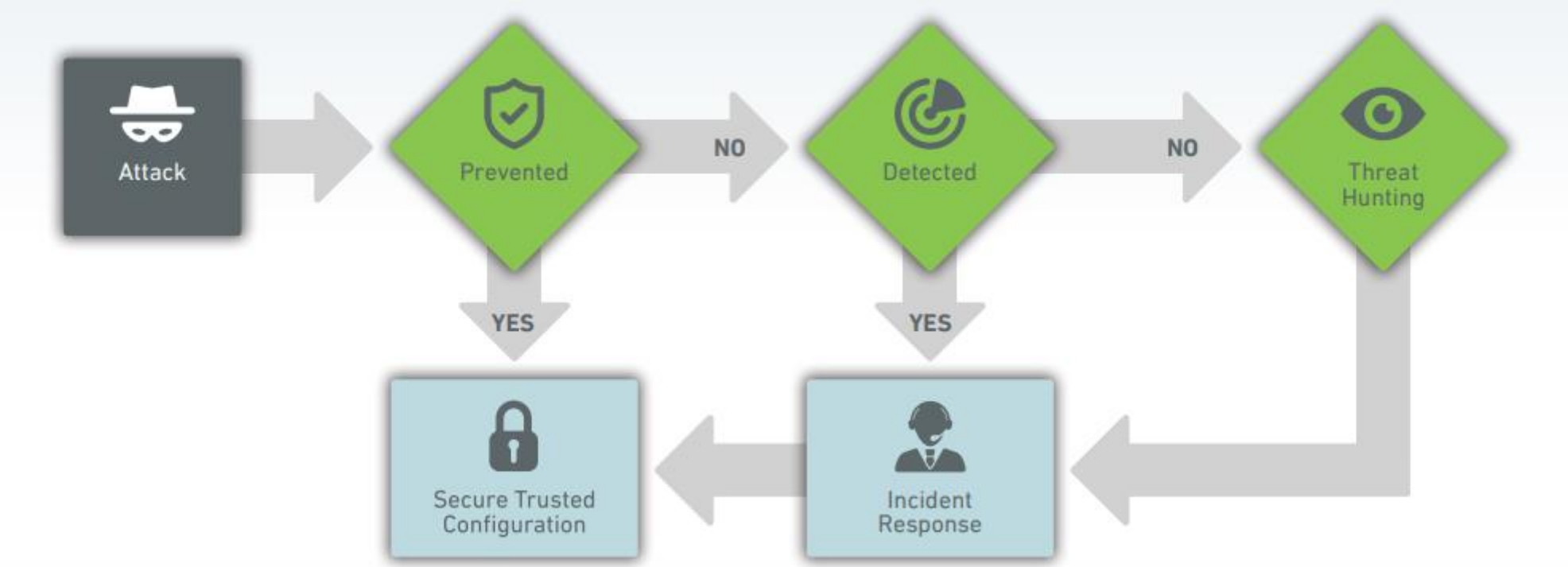
(Piensa como lo haría el atacante)



THREAT HUNTING.

(Proceso de caza de amenazas)

THREAT HUNTING: Es la metodología basada en la hipótesis y descubrimiento de artefactos (artifacts), actividad sospechosa en donde un método pasivo se queda corto.



THREAT HUNTING.

(6 Claves para una caza de amenazas efectiva)

1 – PROACTIVIDAD
2 – IMPULSADO POR HIPOTESIS
3 – ANALISIS RETROSPECTIVO
4 – DESCUBRIMIENTO
5 – ARTEFACTOS Y ACTIVIDAD
6 – METODOS AVANZADOS DE DETECCION

HERRAMIENTAS.

(¡Vamos a cazar amenazas!)

¿NO HAY EDR/XRD?: No hay problema, usemos SYSMON.

Sysmon

HERRAMIENTAS.

(¡Vamos a cazar amenazas!)

¿NO HAY EDR/XRD?: No hay problema, usemos SYSMON.

Event Information

Event Name	FileCreate
Low Level Category	File Created
Event Description	File create operations are logged when a file is created or overwritten.
Magnitude	
Username	N/A
Start Time	May 31, 2022, 10:35:59 AM
Account Name (custom)	N/A
Event ID (custom)	11
Filename (custom)	document3684.docx
Logon Type (custom)	N/A
Object Name Lowercase (custom)	null
Object Type (custom)	N/A
Process GUID (custom)	N/A
Process Name (custom)	quickbuck.exe

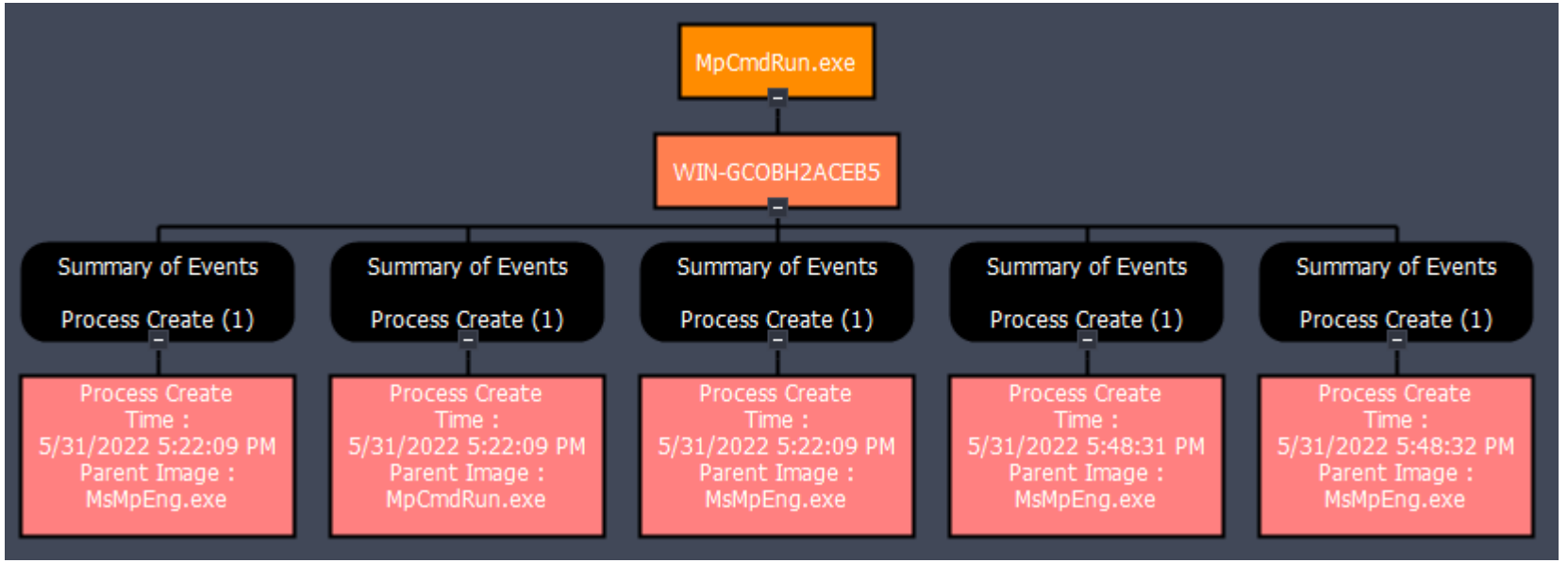
Event Information

Event Name	RegistryEvent (Value Set)
Low Level Category	Successful Registry Modification
Event Description	This Registry event type identifies Registry value modifications.
Magnitude	(5)
Username	N/A
Start Time	May 31, 2022, 9:59:59 AM
Account Name (custom)	N/A
Event ID (custom)	13
Logon Type (custom)	N/A
Object Name Lowercase (custom)	null
Object Type (custom)	N/A
Pipe Name (custom)	N/A
Process GUID (custom)	N/A
Process Name (custom)	reg.exe
Source Workstation (custom)	N/A
Target Details (custom)	C:\putty.exe
Target Object (custom)	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\calc
TargetObjectDetails (custom)	C:\putty.exe

HERRAMIENTAS.

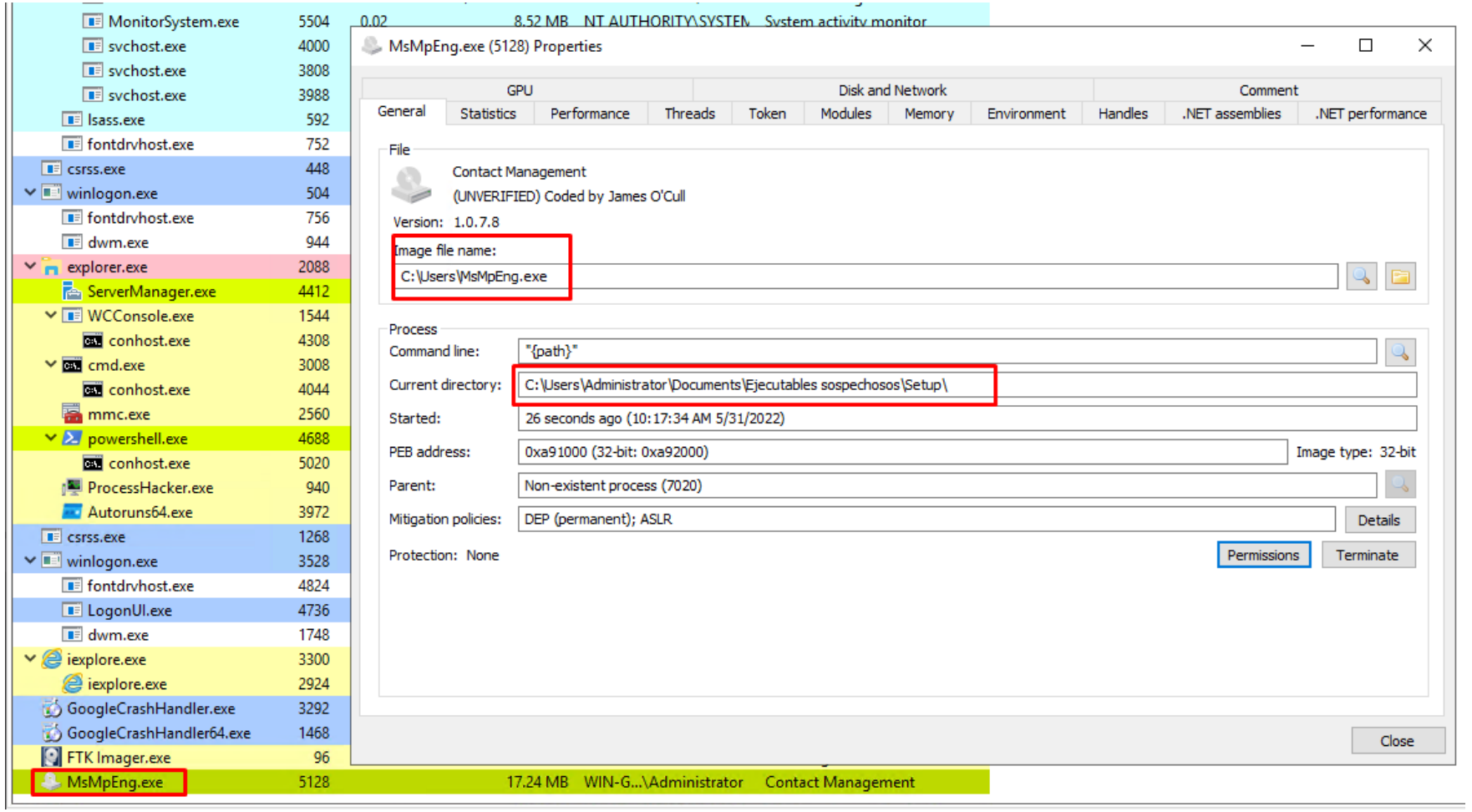
(Sysmon View)

¿NO HAY EDR/XRD?: No hay problema, usemos SYSMON.



HERRAMIENTAS.

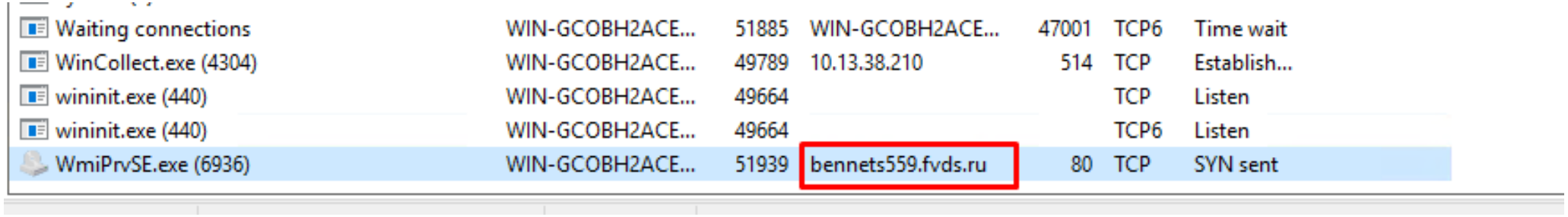
(ProcessHacker2)



HERRAMIENTAS.

(ProcessHacker2)

ProcessHacker2 también sirve para analizar conexiones generadas por procesos.



Waiting connections	WIN-GCOBH2ACE...	51885	WIN-GCOBH2ACE...	47001	TCP6	Time wait
WinCollect.exe (4304)	WIN-GCOBH2ACE...	49789	10.13.38.210	514	TCP	Establish...
wininit.exe (440)	WIN-GCOBH2ACE...	49664			TCP	Listen
wininit.exe (440)	WIN-GCOBH2ACE...	49664			TCP6	Listen
WmiPrvSE.exe (6936)	WIN-GCOBH2ACE...	51939	bennets559.fvds.ru	80	TCP	SYN sent

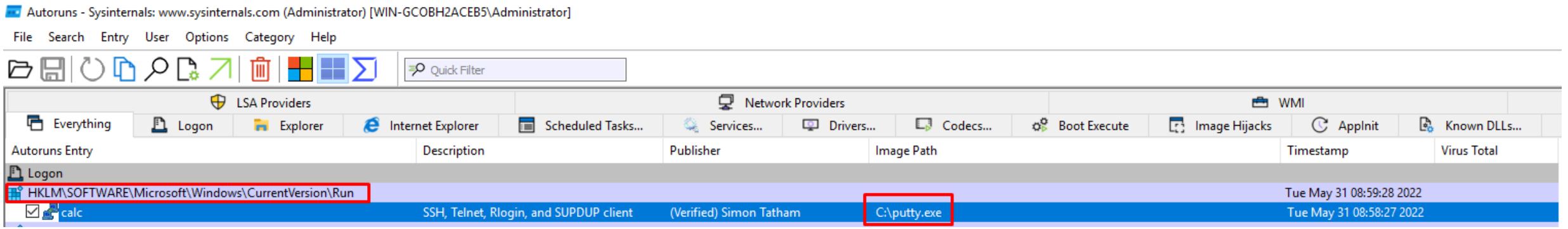
HERRAMIENTAS.

(AutoRuns)

La persistencia es vital para el atacante, por eso debemos investigar y analizar **tareas programadas** y modificaciones de **llaves de registro**.

Administrator: Windows PowerShell

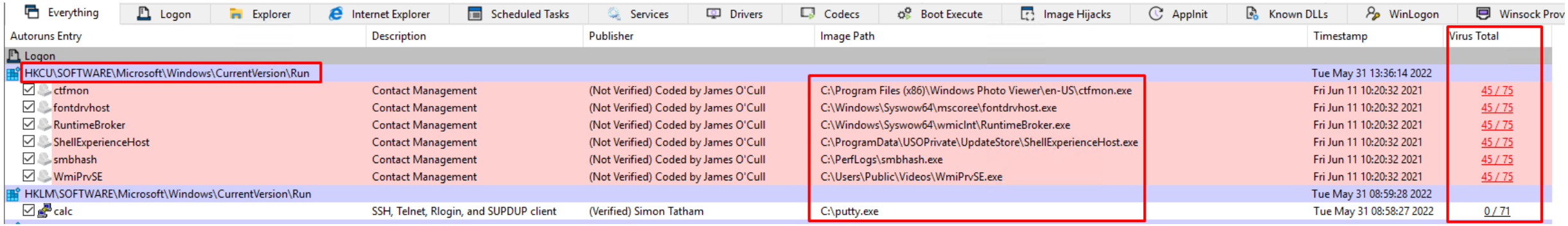
```
PS C:\Users\Administrator>
PS C:\Users\Administrator> reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v calc /t REG_SZ /d "C:\putty.exe"
The operation completed successfully.
PS C:\Users\Administrator>
```



HERRAMIENTAS.

(AutoRuns)

La persistencia es vital para el atacante, por eso debemos investigar y analizar **tareas programadas** y modificaciones de **llaves de registro**.



Everything | Logon | Explorer | Internet Explorer | Scheduled Tasks | Services | Drivers | Codecs | Boot Execute | Image Hijacks | AppInit | Known DLLs | WinLogon | Winsock Prov

Autoruns Entry	Description	Publisher	Image Path	Timestamp	Virus Total
Logon					
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Tue May 31 13:36:14 2022	
ctfmon	Contact Management	(Not Verified) Coded by James O'Cull	C:\Program Files (x86)\Windows Photo Viewer\en-US\ctfmon.exe	Fri Jun 11 10:20:32 2021	45 / 75
fontdrvhost	Contact Management	(Not Verified) Coded by James O'Cull	C:\Windows\Syswow64\mscoree\fontdrvhost.exe	Fri Jun 11 10:20:32 2021	45 / 75
RuntimeBroker	Contact Management	(Not Verified) Coded by James O'Cull	C:\Windows\Syswow64\wmicInt\RuntimeBroker.exe	Fri Jun 11 10:20:32 2021	45 / 75
ShellExperienceHost	Contact Management	(Not Verified) Coded by James O'Cull	C:\ProgramData\USOPrivate\UpdateStore\ShellExperienceHost.exe	Fri Jun 11 10:20:32 2021	45 / 75
smbhash	Contact Management	(Not Verified) Coded by James O'Cull	C:\PerfLogs\smbhash.exe	Fri Jun 11 10:20:32 2021	45 / 75
WmiPrvSE	Contact Management	(Not Verified) Coded by James O'Cull	C:\Users\Public\Videos\WmiPrvSE.exe	Fri Jun 11 10:20:32 2021	45 / 75
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Tue May 31 08:59:28 2022	
calc	SSH, Telnet, Rlogin, and SUPDUP client	(Verified) Simon Tatham	C:\putty.exe	Tue May 31 08:58:27 2022	0 / 71

Autoruns Entry	Description	Publisher	Image Path	Timestamp	Virus Total
Task Scheduler					
\GoogleUpdateTaskMachineCore{C8ADECBB-4581-4C81-95FE-88948726576A}	Mantiene actualizado el software de Goo...	(Verified) Google LLC	C:\Program Files (x86)\Google\Update\GoogleUpdate.exe	Tue May 31 09:25:09 2022	
\GoogleUpdateTaskMachineUA{9ED65573-0E37-4981-8D83-B7CEBD877B08}	Mantiene actualizado el software de Goo...	(Verified) Google LLC	C:\Program Files (x86)\Google\Update\GoogleUpdate.exe	Tue May 31 09:25:09 2022	
\MsMpEng		(Not Verified)	C:\Documents and Settings\MsMpEng.exe	Fri Jun 11 10:20:32 2021	
\RuntimeBroker		(Not Verified)	C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\RuntimeBroker.exe	Fri Jun 11 10:20:32 2021	
\smbhash		(Not Verified)	C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\en-US\smbhash.exe	Fri Jun 11 10:20:32 2021	
\Microsoft\Windows\Server Manager\CleanupOldPerfLogs	Microsoft ® Console Based Script Host	(Verified) Microsoft Windows	C:\Windows\system32\cscript.exe	Sat Sep 15 00:12:39 2018	
\Microsoft\Windows\Software Inventory Logging\Collection	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe	Sat Sep 15 00:12:15 2018	
\Microsoft\Windows\Software Inventory Logging\Configuration	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe	Sat Sep 15 00:12:15 2018	
\Microsoft\Windows\Windows Defender\Windows Defender Cache Maintenance	Periodic maintenance task.	(Verified) Microsoft Corporation	C:\Program Files\Windows Defender\MpCmdRun.exe	Sat Sep 15 00:13:24 2018	
\Microsoft\Windows\Windows Defender\Windows Defender Cleanup	Periodic cleanup task.	(Verified) Microsoft Corporation	C:\Program Files\Windows Defender\MpCmdRun.exe	Sat Sep 15 00:13:24 2018	
\Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan	Periodic scan task.	(Verified) Microsoft Corporation	C:\Program Files\Windows Defender\MpCmdRun.exe	Sat Sep 15 00:13:24 2018	
\Microsoft\Windows\Windows Defender\Windows Defender Verification	Periodic verification task.	(Verified) Microsoft Corporation	C:\Program Files\Windows Defender\MpCmdRun.exe	Sat Sep 15 00:13:24 2018	
\vm3dservice		(Not Verified)	C:\Windows\Syswow64\olepro32\vm3dservice.exe		
\WinCollect		(Not Verified)	C:\Program Files\IBM\WinCollect\bin\zlib1\WinCollect.exe	Fri Jun 11 10:20:32 2021	
\WmiPrvSE		(Not Verified)	C:\Windows\Syswow64\wbem\kerberos\WmiPrvSE.exe		

HERRAMIENTAS.

(AutoRuns)

Direcctorios a investigar:

- C:\Users\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp

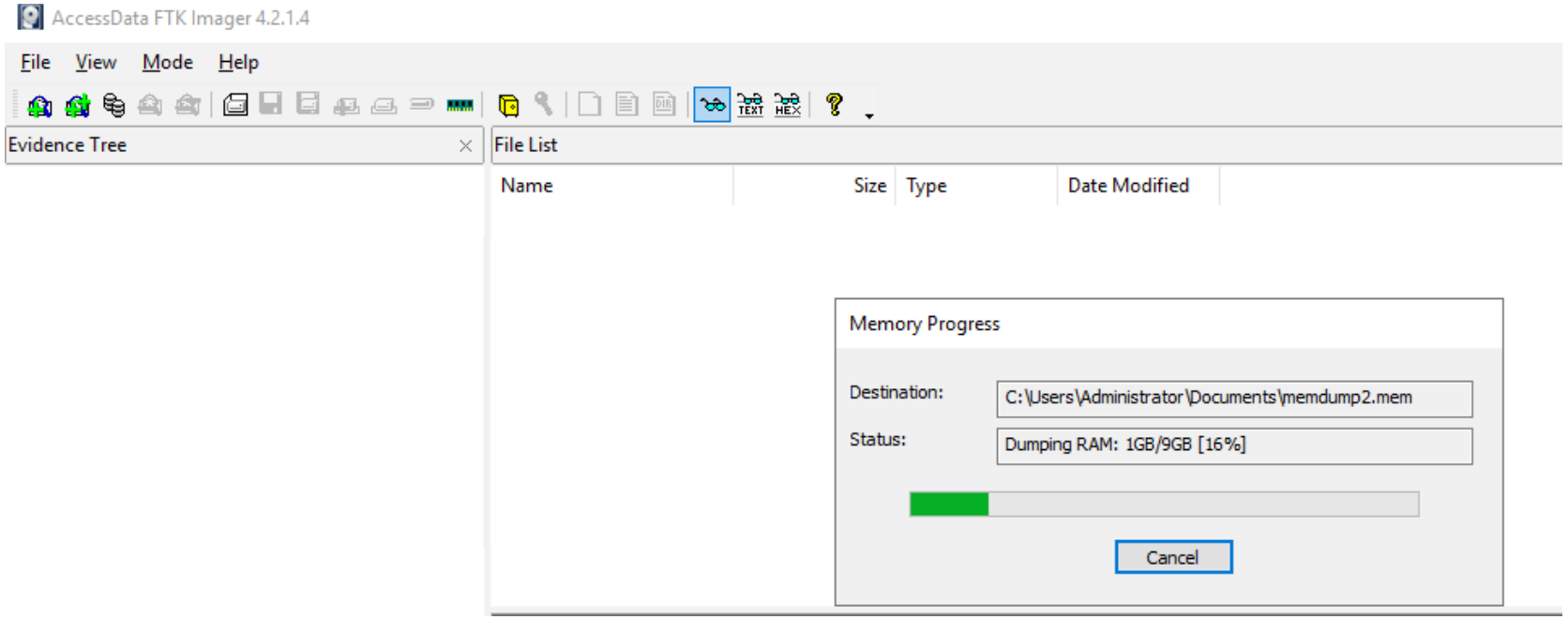
Llaves de registro a investigar:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices Once
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices Once
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices

HERRAMIENTAS.

(FTK Imager)

Un análisis de lo que hay en memoria es muy útil para encontrar artifacts o elementos que determinen un falso positivo o verdadero positivo. Para ello se necesita sacar un volcado de memoria del equipo en sospechas.



HERRAMIENTAS.

(VolatilityV3 y Redline)

Una vez se tenga el volcado de memoria se puede analizar con herramientas especializadas como **Volatilityv2 o v3** y **Redline**.

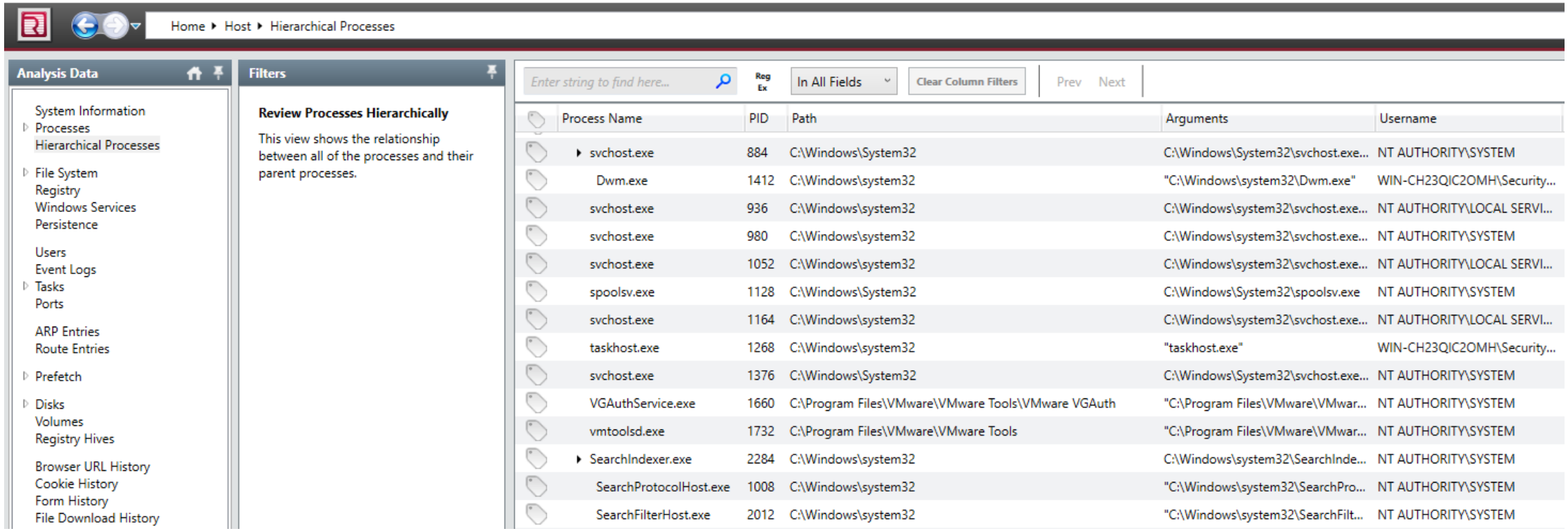
```
C:\Users\Administrator\Downloads\volatility3-1.0.0>.\vol.py -f "memdump2.mem" windows.pslist
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xe10b4965d080  123     -       N/A     False   2022-05-31 14:14:58.000000      N/A     Disabled
88      4       Registry        0xe10b496af080  4       -       N/A     False   2022-05-31 14:14:53.000000      N/A     Disabled
264     4       smss.exe        0xe10b4c259280  2       -       N/A     False   2022-05-31 14:14:58.000000      N/A     Disabled
364     356     csrss.exe       0xe10b4c5eb140  10      -       0       False   2022-05-31 14:15:01.000000      N/A     Disabled
440     356     wininit.exe     0xe10b4c6ba080  1       -       0       False   2022-05-31 14:15:01.000000      N/A     Disabled
448     432     csrss.exe       0xe10b4c6bf140  11      -       1       False   2022-05-31 14:15:01.000000      N/A     Disabled
504     432     winlogon.exe    0xe10b4c7020c0  5       -       1       False   2022-05-31 14:15:01.000000      N/A     Disabled
576     440     services.exe    0xe10b4c5e2380  7       -       0       False   2022-05-31 14:15:02.000000      N/A     Disabled
592     440     lsass.exe       0xe10b4c6b9080  6       -       0       False   2022-05-31 14:15:02.000000      N/A     Disabled
700     576     svchost.exe     0xe10b4d4db080  1       -       0       False   2022-05-31 14:15:03.000000      N/A     Disabled
732     576     svchost.exe     0xe10b4d4d6080  10      -       0       False   2022-05-31 14:15:03.000000      N/A     Disabled
752     440     fontdrvhost.ex  0xe10b4c735080  5       -       0       False   2022-05-31 14:15:03.000000      N/A     Disabled
756     504     fontdrvhost.ex  0xe10b4c734080  5       -       1       False   2022-05-31 14:15:03.000000      N/A     Disabled
844     576     svchost.exe     0xe10b4d55e080  9       -       0       False   2022-05-31 14:15:03.000000      N/A     Disabled
880     576     svchost.exe     0xe10b4d557080  4       -       0       False   2022-05-31 14:15:03.000000      N/A     Disabled
916     576     sppsvc.exe      0xe10b4d551080  0       -       0       False   2022-05-31 14:15:03.000000      2022-05-31 15:22:40.000000      Disabled
944     504     dwm.exe 0xe10b4d616080  15      -       1       False   2022-05-31 14:15:04.000000      N/A     Disabled
984     576     svchost.exe     0xe10b4d614080  1       -       0       False   2022-05-31 14:15:04.000000      N/A     Disabled
296     576     svchost.exe     0xe10b4d623080  2       -       0       False   2022-05-31 14:15:04.000000      N/A     Disabled
1060    576     svchost.exe     0xe10b4d50b080  5       -       0       False   2022-05-31 14:15:09.000000      N/A     Disabled
1112    576     svchost.exe     0xe10b496792c0  4       -       0       False   2022-05-31 14:15:09.000000      N/A     Disabled
1120    576     svchost.exe     0xe10b4c5212c0  9       -       0       False   2022-05-31 14:15:09.000000      N/A     Disabled
1196    576     svchost.exe     0xe10b4c51f680  3       -       0       False   2022-05-31 14:15:09.000000      N/A     Disabled
1224    576     svchost.exe     0xe10b49716440  5       -       0       False   2022-05-31 14:15:09.000000      N/A     Disabled
1300    576     svchost.exe     0xe10b496d8080  6       -       0       False   2022-05-31 14:15:10.000000      N/A     Disabled
1392    576     svchost.exe     0xe10b49799080  7       -       0       False   2022-05-31 14:15:10.000000      N/A     Disabled
```

HERRAMIENTAS.

(VolatilityV3 y Redline)

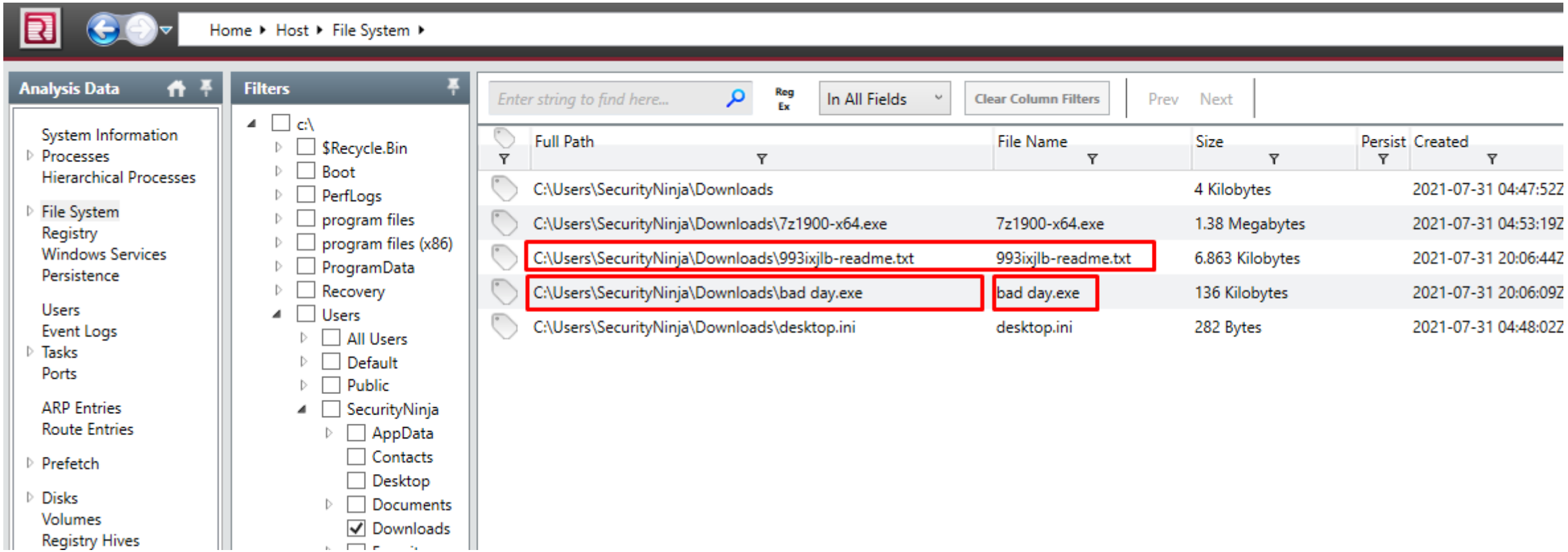
Una vez se tenga el volcado de memoria se puede analizar con herramientas especializadas como **Volatilityv2 o v3** y **RedLine**.



HERRAMIENTAS.

(VolatilityV3 y Redline)

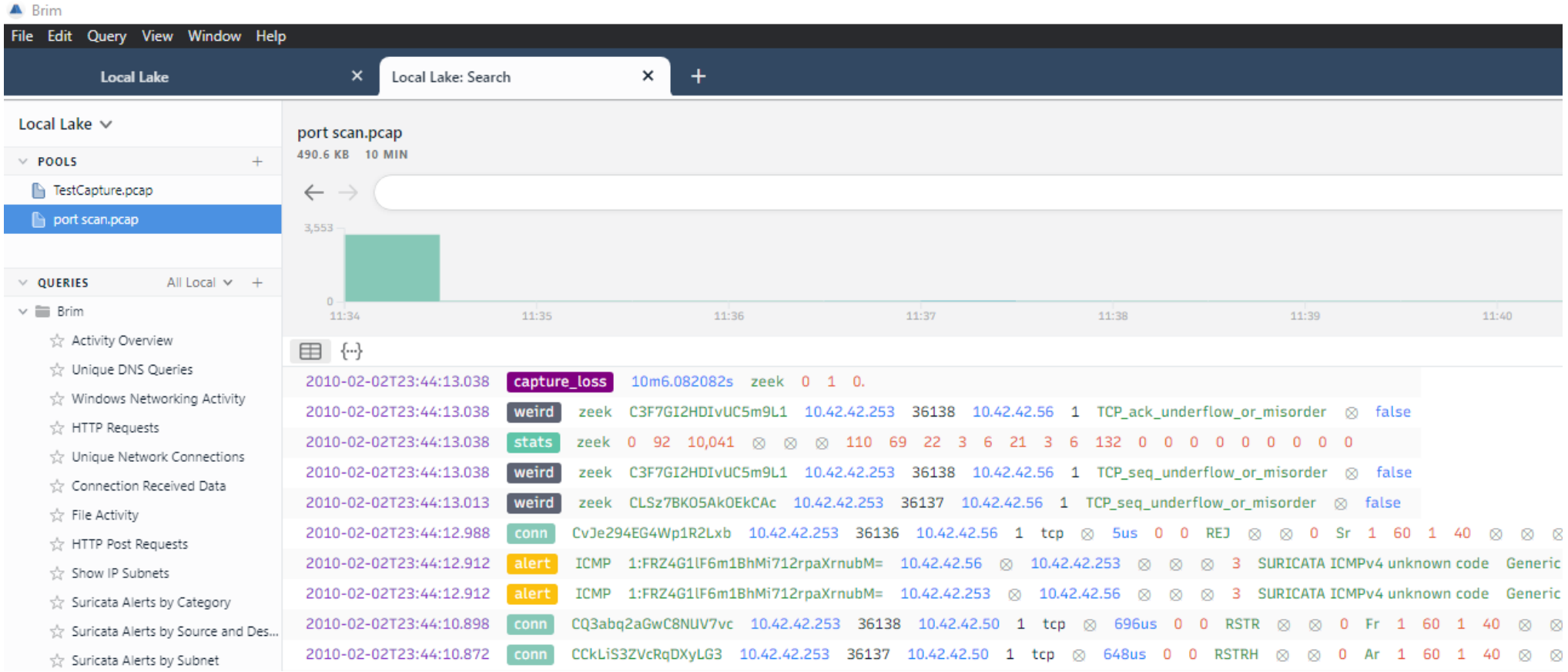
Una vez se tenga el volcado de memoria se puede analizar con herramientas especializadas como **Volatilityv2 o v3** y **RedLine**.



HERRAMIENTAS.

(Wireshark y Brim)

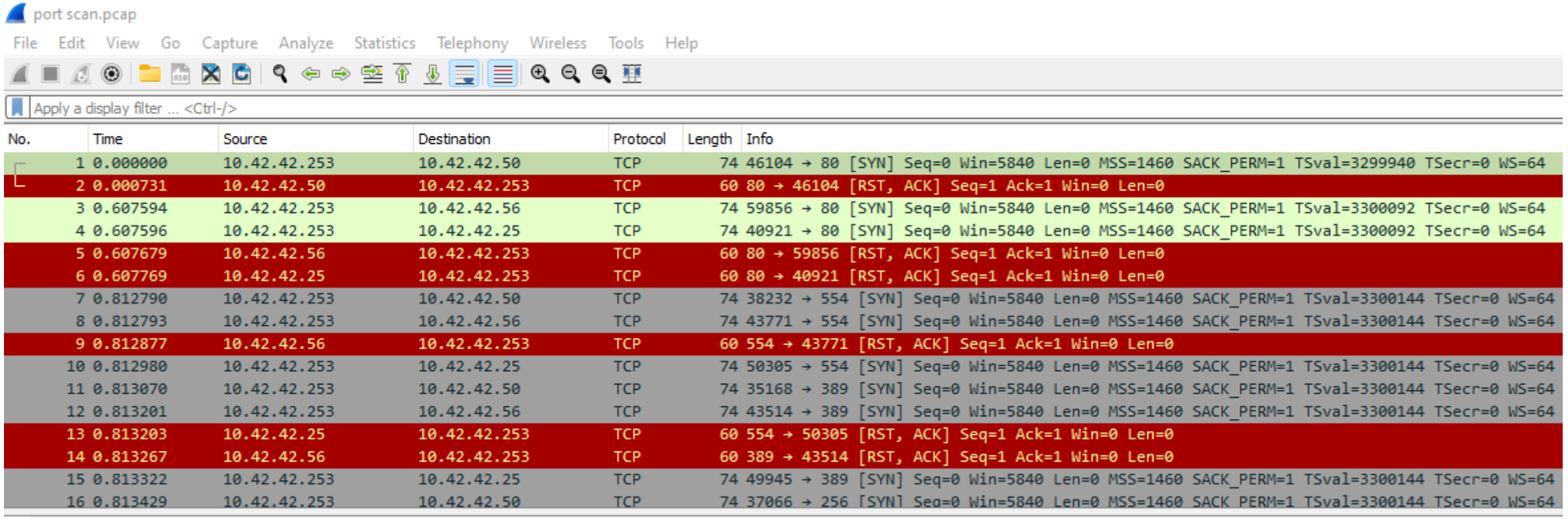
Analizar tráfico de red sospechoso es parte vital de las labores de investigación y threat hunting.



HERRAMIENTAS.

(Wireshark y Brim)

Analizar tráfico de red sospechoso es parte vital de las labores de investigación y **Threat Hunting**.

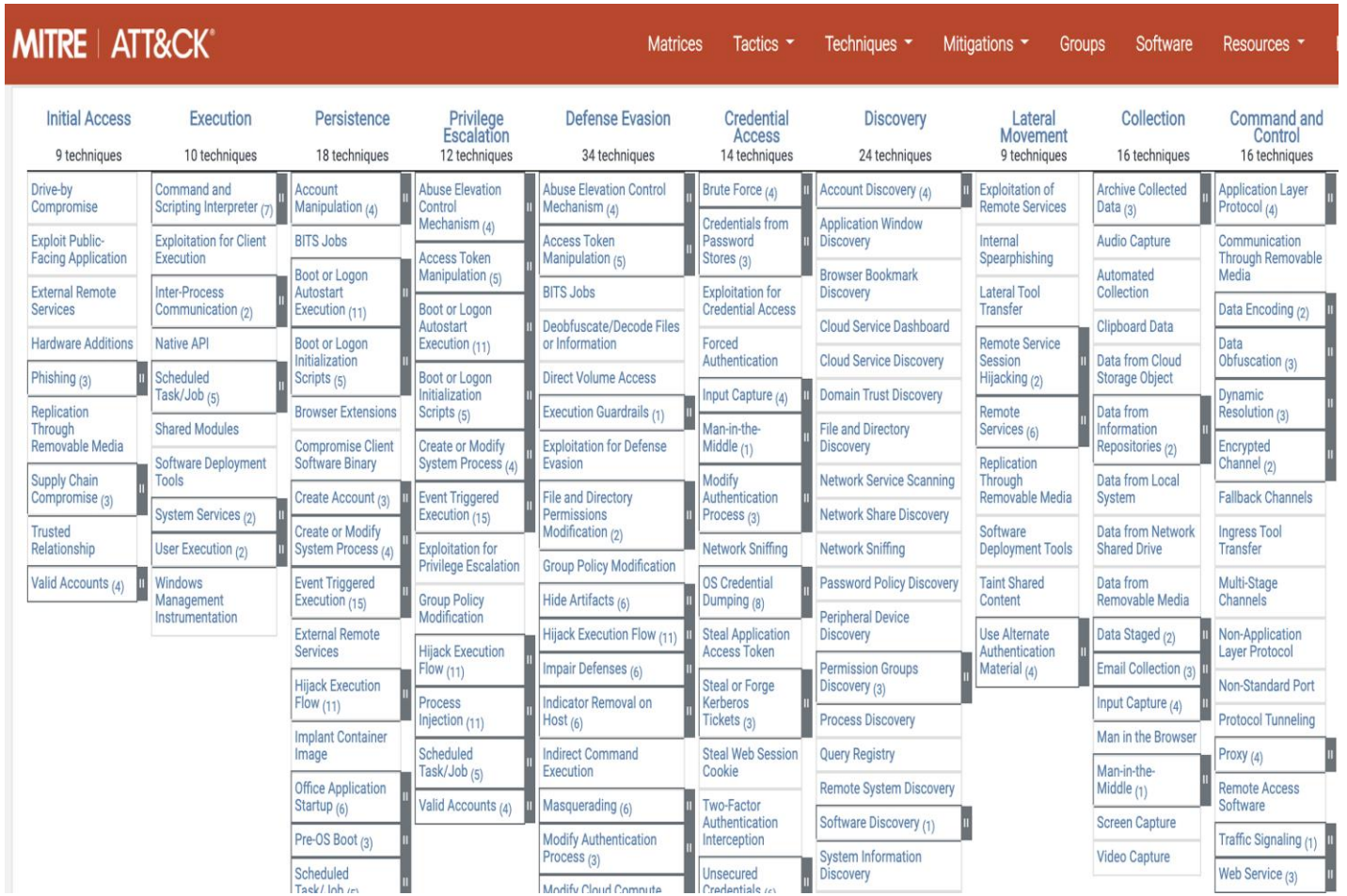


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.42.42.253	10.42.42.50	TCP	74	46104 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3299940 TSecr=0 WS=64
2	0.000731	10.42.42.50	10.42.42.253	TCP	60	80 → 46104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3	0.607594	10.42.42.253	10.42.42.56	TCP	74	59856 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3300092 TSecr=0 WS=64
4	0.607596	10.42.42.253	10.42.42.25	TCP	74	40921 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3300092 TSecr=0 WS=64
5	0.607679	10.42.42.56	10.42.42.253	TCP	60	80 → 59856 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	0.607769	10.42.42.25	10.42.42.253	TCP	60	80 → 40921 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	0.812790	10.42.42.253	10.42.42.50	TCP	74	38232 → 554 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3300144 TSecr=0 WS=64
8	0.812793	10.42.42.253	10.42.42.56	TCP	74	43771 → 554 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3300144 TSecr=0 WS=64
9	0.812877	10.42.42.56	10.42.42.253	TCP	60	554 → 43771 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10	0.812980	10.42.42.253	10.42.42.25	TCP	74	50305 → 554 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3300144 TSecr=0 WS=64
11	0.813070	10.42.42.253	10.42.42.50	TCP	74	35168 → 389 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3300144 TSecr=0 WS=64
12	0.813201	10.42.42.253	10.42.42.56	TCP	74	43514 → 389 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3300144 TSecr=0 WS=64
13	0.813203	10.42.42.25	10.42.42.253	TCP	60	554 → 50305 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14	0.813267	10.42.42.56	10.42.42.253	TCP	60	389 → 43514 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	0.813322	10.42.42.253	10.42.42.25	TCP	74	49945 → 389 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3300144 TSecr=0 WS=64
16	0.813429	10.42.42.253	10.42.42.50	TCP	74	37066 → 256 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3300144 TSecr=0 WS=64

MITRE ATT&CK.

(Framework para tácticas y técnicas)

El conocimiento es poder, y para ello necesitamos documentarnos de la mayor cantidad de recursos, la matriz de MITRE ATT&CK nos brinda las tácticas y técnicas usadas por los adversarios.



Devel
CYBERSECURITY REDEFINED

¡MUCHÍSIMAS GRACIAS!

BlackBerry