

Módulo	ANÁLISIS FORENSE
Nombre y apellidos	David Fernández Alejo
Fecha entrega	

Para la resolución del ejercicio se deberá responder a las siguientes preguntas **sobre esta plantilla**. Será necesario atender a los siguientes puntos:

- Contestar a las preguntas en el orden establecido.
- Limitarse a contestar a las preguntas planteadas mediante una respuesta directa que posteriormente se deberá argumentar y desarrollar con detalle así como utilizar, cuando proceda, las evidencias facilitadas para el análisis
- El ejercicio se puede resolver bien analizando los resultados de la ejecución de la herramienta WLR que se incluyen en el fichero comprimido, bien analizando el disco facilitado del equipo víctima (mediante una herramienta forense, tipo Autopsy, Caine o similar). Ambas opciones son válidas. Para la opción de análisis con herramienta forense no es necesario saber la cuenta de administrador del equipo víctima.
- Como orientación, el ejercicio debe tener una extensión comprendida entre 10 y 15 páginas.

Pregunta 1 (2 puntos):

¿Cómo, cuándo y desde dónde accedió el intruso al servidor? Indique el detalle de las evidencias (archivo, evento, etc.) de las que se deduce esta información.

Respuesta:

En primer lugar, para poder realizar un análisis de los datos , se importarán los distintos eventos al visor de eventos de Windows para poder comprobar los eventos de tipo Security y comprobar los distintos accesos al servidor.

Como se puede comprobar hay numerosos eventos:

Vista de eventos (local)

Vistas personalizadas

Registros de Windows

Registros de aplicaciones y servicios

Registros guardados

Application

HardwareEvents

Internet Explorer

Log Management Service

Security

Setup

System

Windows PowerShell

Suscripciones

Security	Número de eventos: 1,000	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	07/05/2021 15:01:08	Microsoft Windows security audit...	4634	Logoff	
Información	07/05/2021 15:01:08	Microsoft Windows security audit...	4634	Logoff	
Información	07/05/2021 15:01:08	Microsoft Windows security audit...	4634	Logoff	
Información	07/05/2021 15:01:06	Microsoft Windows security audit...	4672	Special Logon	
Información	07/05/2021 15:01:06	Microsoft Windows security audit...	4624	Logon	
Información	07/05/2021 15:01:06	Microsoft Windows security audit...	4648	Logon	
Información	07/05/2021 15:01:06	Microsoft Windows security audit...	4778	Credential Validation	
Información	07/05/2021 15:01:01	Microsoft Windows security audit...	4790	User Account Management	
Información	07/05/2021 14:54:43	Microsoft Windows security audit...	4790	User Account Management	
Información	07/05/2021 14:09:26	Microsoft Windows security audit...	4672	Special Logon	
Información	07/05/2021 14:09:26	Microsoft Windows security audit...	4624	Logon	
Información	07/05/2021 13:55:57	Microsoft Windows security audit...	4790	User Account Management	
Información	07/05/2021 13:55:56	Microsoft Windows security audit...	4790	User Account Management	
Información	07/05/2021 13:55:56	Microsoft Windows security audit...	4790	User Account Management	
Información	07/05/2021 13:45:26	Microsoft Windows security audit...	4634	Logoff	
Información	07/05/2021 13:42:26	Microsoft Windows security audit...	4624	Logon	
Información	07/05/2021 13:42:26	Microsoft Windows security audit...	4672	Special Logon	
Información	07/05/2021 13:42:24	Microsoft Windows security audit...	4672	Special Logon	
Información	07/05/2021 13:42:24	Microsoft Windows security audit...	4624	Logon	
Información	07/05/2021 13:42:24	Microsoft Windows security audit...	4624	Logon	
Información	07/05/2021 13:42:24	Microsoft Windows security audit...	4648	Logon	
Información	07/05/2021 13:42:23	Microsoft Windows security audit...	4672	Special Logon	
Información	07/05/2021 13:42:23	Microsoft Windows security audit...	4672	Special Logon	
Información	07/05/2021 13:42:23	Microsoft Windows security audit...	4672	Special Logon	
Información	07/05/2021 13:42:23	Microsoft Windows security audit...	4648	Logon	
Información	07/05/2021 13:42:23	Microsoft Windows security audit...	4778	Credential Validation	
Información	07/05/2021 13:42:23	Microsoft Windows security audit...	4790	User Account Management	
Información	07/05/2021 13:42:22	Microsoft Windows security audit...	4672	Special Logon	
Información	07/05/2021 13:42:22	Microsoft Windows security audit...	4672	Special Logon	
Información	07/05/2021 13:42:22	Microsoft Windows security audit...	4624	Logon	
Información	07/05/2021 13:42:22	Microsoft Windows security audit...	4624	Logon	
Información	07/05/2021 13:42:22	Microsoft Windows security audit...	4648	Logon	
Información	07/05/2021 13:42:20	Microsoft Windows security audit...	5061	System Integrity	

Para poder filtrar los eventos y ver la información de una manera mas visual, se utilizará la herramienta hayabusa, para exportar los distintos eventos a un csv.

```
PS E:\Programas\hayabusa-3.2.0-win-aarch64> .\hayabusa-3.2.0-win-aarch64.exe csv-timeline -f C:\Users\David\Desktop\Security.evtx -o C:\Users\David\Desktop\report_security_inf.csv

HAYABUSA
by Vanate Security

Verped for the modern-day digital detective-

Start time: 2022/06/20 12:12
Total event log files: 1
Total file size: 1.2 MB

Now choose:
-Which set of detection rules would you like to load? - S. All event and alert rules (9,439 rules) ( status: + [ level: Informational* )
-Include deprecated rules? (218 rules) - yes
-Include unsupported rules? (42 rules) - yes
-Include noisy rules? (12 rules) - yes
-Include system rules? (2,568 rules) - yes

Loading detection rules. Please wait.

Included rules: 26
Noisy rules: 12

Deprecated rules: 218 (0.66%)
Experimental rules: 218 (0.73%)
Stable rules: 258 (0.53%)
Test rules: 2,879 (00.26%)
Unsupported rules: 42 (0.51%)

Correlation rules: 3 (0.07%)
Correlation reference rules: 3 (0.07%)

Ignored rules: 18 (0.12%)
Enabled ignored rules: 0 (0.00%)

Hayabusa rules: 191
Sigma rules: 4,418
Total detection rules: 4,609

Creating the channel filter. Please wait.

Extra files loaded after channel filter: 1
Detection rules enabled after channel filter: 1,849

Output profile: standard

Scanning in progress. Please wait.

[00:00:00] 1 / 1 [ ] 100%

Scanning finished. Please wait while the results are being saved.

Rule Authors:

Zach Mathis (17)  Darkoverl (2)  Micah Babinski (1)

Results Summary:

Events with hits / total events: 392 / 1,000 (Data reduction: 608 events (60.80%))

Total | Unique detections: 393 | 19
Total | Unique emergency detections: 0 (0.00%) | 0 (0.00%)
Total | Unique critical detections: 0 (0.00%) | 0 (0.00%)
Total | Unique high detections: 0 (0.00%) | 0 (0.00%)
Total | Unique medium detections: 3 (0.76%) | 1 (0.76%)
Total | Unique low detections: 13 (3.31%) | 2 (0.00%)
Total | Unique informational detections: 177 (09.93%) | 14 (0.00%)

First Timestamp: 2021-05-06 16:15:21.894 +02:00
Last Timestamp: 2021-05-07 15:41:05.959 +02:00

Dates with most total detections:
Emergency: n/a, critical: n/a, high: n/a, medium: 2021-05-07 (2), low: 2021-05-07 (11), informational: 2021-05-07 (218)

Top 5 computers with most unique detections:
Emergency: n/a
Critical: n/a
High: n/a
Medium: WIN-SFBLTHXDMQ (3)
Low: WIN-SFBLTHXDMQ (1)
Informational: WIN-SFBLTHXDMQ (14)

Top emergency alerts:
n/a
n/a
n/a
n/a
n/a

Top critical alerts:
n/a
n/a
n/a
n/a
n/a

Top high alerts:
n/a
n/a
n/a
n/a
n/a

Top medium alerts:
User Password Changed (1)
Password Reset By Admin (1)
External Remote RDP Logon from Public IP (1)
n/a
n/a

Top low alerts:
Logon Failure (Unknown Reason) (10)
Logon Failure (Wrong Password) (2)
n/a
n/a
n/a

Top informational alerts:
Logon (Service) (Noisy) (110)
Proc Exec (101)
Admin Logon (34)
Logon (Interactive) (Noisy) (27)
Explicit Logon Attempt (Noisy) (24)

Saved file: C:\Users\David\Desktop\report_security_inf.csv (213.9 KB)

Elapsed time: 00:00:07.1127

Please report any issues with Hayabusa rules to: https://github.com/Vanate-Security/hayabusa-rules/issues
Please report any false positives with Sigma rules to: https://github.com/SigmaHQ/sigma/issues
Please submit new Sigma rules with pull requests to: https://github.com/SigmaHQ/sigma/pulls
```

Como se puede observar, en el reporte que nos da la herramienta nos indica el número de accesos, así como los eventos sospechosos.

Top emergency alerts:	Top critical alerts:
n/a	n/a
n/a	n/a
n/a	n/a
n/a	n/a
n/a	n/a
Top high alerts:	Top medium alerts:
n/a	User Password Changed (1)
n/a	Password Reset By Admin (1)
n/a	External Remote RDP Logon from Public IP (1)
n/a	n/a
n/a	n/a
Top low alerts:	Top informational alerts:
Logon Failure (Unknown Reason) (10)	Logon (Service) (Noisy) (110)
Logon Failure (Wrong Password) (2)	Proc Exec (101)
n/a	Admin Logon (34)
n/a	Logon (Interactive) (Noisy) (27)
n/a	Explicit Logon Attempt (Noisy) (24)

Posteriormente, se filtrará por los eventos 4624 que son los inicios de sesión, que además tengan un id 2 (interactivo, acceso local) y 10 (acceso remoto, por ejemplo, RDP).

1	Timestamp	Subfente	Level	Computer	Channel	EventID	RecordID	Details	ExtraFields	RuleID
143	07/05/2021 13:42	Logon (RemoteInteractive (RDP)) "Credits in memory"	info	WIN-SF01TM2DHI	Sec	4624	815	Type 30 REMOTE INTERACTIVE : TglUser: Administrator ; SrcComp: WIN-SF01TM2DHI ; SrcIP: 129 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
144	06/05/2021 16:39	Logon (Interactive) "Credits in memory"	info	WIN-SF01TM2DHI	Sec	4624	295	Type 2 INTERACTIVE : TglUser: Administrator ; SrcComp: WIN-SF01TM2DHI ; SrcIP: 127.0.0.1 ; U AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
147	06/05/2021 16:21	Logon (Interactive) "Credits in memory"	info	WIN-SF01TM2DHI	Sec	4624	360	Type 2 INTERACTIVE : TglUser: Administrator ; SrcComp: WIN-SF01TM2DHI ; SrcIP: 127.0.0.1 ; U AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
148	06/05/2021 16:30	Logon (Interactive) "Credits in memory"	info	WIN-SF01TM2DHI	Sec	4624	474	Type 2 INTERACTIVE : TglUser: Administrator ; SrcComp: WIN-SF01TM2DHI ; SrcIP: 127.0.0.1 ; U AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
149	06/05/2021 17:32	Logon (Interactive) "Credits in memory"	info	WIN-SF01TM2DHI	Sec	4624	507	Type 2 INTERACTIVE : TglUser: Administrator ; SrcComp: WIN-SF01TM2DHI ; SrcIP: 127.0.0.1 ; U AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
150	07/05/2021 10:00	Logon (Interactive) "Credits in memory"	info	WIN-SF01TM2DHI	Sec	4624	639	Type 2 INTERACTIVE : TglUser: Administrator ; SrcComp: WIN-SF01TM2DHI ; SrcIP: 127.0.0.1 ; U AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
151	07/05/2021 10:29	Logon (Interactive) "Credits in memory"	info	WIN-SF01TM2DHI	Sec	4624	709	Type 2 INTERACTIVE : TglUser: Administrator ; SrcComp: WIN-SF01TM2DHI ; SrcIP: 127.0.0.1 ; U AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
152	07/05/2021 11:14	Logon (Interactive) "Credits in memory"	info	WIN-SF01TM2DHI	Sec	4624	775	Type 2 INTERACTIVE : TglUser: Administrator ; SrcComp: WIN-SF01TM2DHI ; SrcIP: 127.0.0.1 ; U AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
153	07/05/2021 11:23	Logon (Interactive) "Credits in memory"	info	WIN-SF01TM2DHI	Sec	4624	832	Type 2 INTERACTIVE : TglUser: Administrator ; SrcComp: WIN-SF01TM2DHI ; SrcIP: 127.0.0.1 ; U AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
154	07/05/2021 11:40	Logon (Interactive) "Credits in memory"	info	WIN-SF01TM2DHI	Sec	4624	894	Type 2 INTERACTIVE : TglUser: Administrator ; SrcComp: WIN-SF01TM2DHI ; SrcIP: 127.0.0.1 ; U AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
155	07/05/2021 10:10	Logon (Interactive) "Credits in memory"	info	WIN-SF01TM2DHI	Sec	4624	896	Type 2 INTERACTIVE : TglUser: Administrator ; SrcComp: WIN-SF01TM2DHI ; SrcIP: 127.0.0.1 ; U AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
156	06/05/2021 16:35	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	56	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
157	06/05/2021 16:35	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	157	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
158	06/05/2021 16:35	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	128	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
159	06/05/2021 16:35	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	127	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
160	06/05/2021 16:30	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	321	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
161	06/05/2021 16:29	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	320	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
162	06/05/2021 16:30	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	411	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
163	06/05/2021 16:30	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	410	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
164	06/05/2021 17:31	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	527	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
165	06/05/2021 17:31	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	526	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
166	07/05/2021 9:59	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	605	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
167	07/05/2021 9:59	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	604	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
168	07/05/2021 10:29	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	680	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
169	07/05/2021 10:29	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	681	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
170	07/05/2021 11:13	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	742	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
171	07/05/2021 11:13	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	743	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
172	07/05/2021 11:23	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	802	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
173	07/05/2021 11:23	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	803	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
174	07/05/2021 11:40	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	894	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
175	07/05/2021 11:40	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	895	Type 2 INTERACTIVE : TglUser: DWM 1 ; SrcComp: ; SrcIP: ; LID: 0x1284 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
176	07/05/2021 12:50	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	965	Type 2 INTERACTIVE : TglUser: Administrator ; SrcComp: WIN-SF01TM2DHI ; SrcIP: ; LID: 0x206 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
177	07/05/2021 12:50	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	966	Type 2 INTERACTIVE : TglUser: Administrator ; SrcComp: WIN-SF01TM2DHI ; SrcIP: ; LID: 0x206 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
178	07/05/2021 12:50	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	967	Type 2 INTERACTIVE : TglUser: Administrator ; SrcComp: WIN-SF01TM2DHI ; SrcIP: ; LID: 0x206 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
179	07/05/2021 13:42	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	968	Type 2 INTERACTIVE : TglUser: DWM 2 ; SrcComp: ; SrcIP: ; LID: 0x206 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
180	07/05/2021 13:42	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	969	Type 2 INTERACTIVE : TglUser: DWM 2 ; SrcComp: ; SrcIP: ; LID: 0x206 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
181	07/05/2021 13:42	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	969	Type 2 INTERACTIVE : TglUser: DWM 2 ; SrcComp: ; SrcIP: ; LID: 0x206 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
182	07/05/2021 13:42	Logon (Interactive) (Ntlogon)	info	WIN-SF01TM2DHI	Sec	4624	969	Type 2 INTERACTIVE : TglUser: DWM 2 ; SrcComp: ; SrcIP: ; LID: 0x206 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		
384	07/05/2021 13:42	External Remote RDP Logon from Public IP	med	WIN-SF01TM2DHI	Sec	4624	975	Type 30 REMOTE INTERACTIVE : TglUser: Administrator ; SrcComp: WIN-SF01TM2DHI ; SrcIP: 129.205.96.3 ; LID: 0x27638 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000		

Como se puede observar hay numerosos accesos de este tipo al servidor, pero según el enunciado de la práctica, se indica: "... se cree que pudo haber sido un trabajador descontento del departamento de informática. Este trabajador podría conocer la dirección IP privada del servidor y conectarse a él.". Es por ello por lo que el acceso de 13:42:23 sería el acceso vía IP pública desde la IP remota indicada en el evento.

07/05/2021 13:42	External Remote RDP Logon from Public IP	med	WIN-SF01TM2DHI	Sec	4624	975	Type 30 - REMOTE INTERACTIVE : TglUser: Administrator ; SrcComp: WIN-SF01TM2DHI ; SrcIP: 129.205.96.3 ; LID: 0x27638 AuthenticationPackageName: Negotiate ; ElevatedToken: YES ; ImpersonationLevel: IMPERSONATION; WinAuthz: 000-0000-0000-0000-000000000000
Se inició sesión correctamente en una cuenta.							
Firmante:							
Id. de seguridad:		SYSTEM					
Nombre de cuenta:		WIN-SF01TM2DHI\$					
Dominio de cuenta:		WORKGROUP					
Id. de inicio de sesión:		0x3E7					
Información de inicio de sesión:							
Tipo de inicio de sesión:		10					
Modo de administrador restringido:		No					
Cuenta virtual:		No					
Token elevado:		Sí					
Nivel de suplantación:							
Suplantación							
Nuevo inicio de sesión:							
Id. de seguridad:		S-1-5-21-1046813697-208363348-2122892913-500					
Nombre de cuenta:		Administrator					
Dominio de cuenta:		WIN-SF01TM2DHI					
Id. de inicio de sesión:		0x276318					
Inicio de sesión vinculado:		0x0					
Nombre de cuenta de red:		-					
Dominio de cuenta de red:		-					
GUID de inicio de sesión:		{00000000-0000-0000-0000-000000000000}					
Información de proceso:							
Id. de proceso:		0x3f0					
Nombre de proceso:		C:\Windows\System32\svchost.exe					
Información de red:							
Nombre de estación de trabajo:		WIN-SF01TM2DHI					
Dirección de red de origen:		129.205.96.3					
Puerto de origen:		0					
Nombre de registro: Seguridad							
Origen:		Microsoft Windows security		Registrado:		07/05/2021 13:42:23	
Id. del:		4624		Categoría de tarea:		Logon	
Nivel:		Información		Palabras clave:		Auditoría correcta	
Usuario:		No disponible		Equipo:		WIN-SF01TM2DHI	
Código de operación: Información							

Este es el evento asociado al acceso vía RDP del usuario Administrador desde la ip 129.205.96.3.

Este acceso es el primero vía RDP con la IP pública del servidor, sin embargo, se puede constatar que dicho usuario había accedido previamente, ya que cómo se puede comprobar en el NTSUSERDAT (para visualizar dicha información se ha utilizado la herramienta RegRipper), se lanzó un Netscan previo a dicho acceso:

Fri May 7 11:44:00 2021 Z

{6D809377-6AF0-444B-8957-A3773F02200E}\SoftPerfect Network Scanner\netscan.exe (1)

Además, según los reportes del archivo "LasActivityView.html", después del acceso registrado a las 16:21:42 del 06/05/2021, se realizan las siguientes acciones:

[illegible]

Como se puede comprobar, se instalan varios Softwares, entre ellos Wireshark, y se desinstala Npcap para posteriormente reiniciar el servidor.

Además, como se puede observar se descarga el zip “2.2.0 20200918 Zerologon encrypted.zip”.

Por lo tanto, se puede constatar, que el usuario sospechoso accedió de forma local al servidor para instalar una serie de herramientas, para posteriormente, loguearse via RDP desde la ip 129.205.96.3 como se indica en los eventos del sistema.

Pregunta 2 (3 puntos):

¿Qué acciones fueron realizadas por el intruso a partir de su acceso? Indique el detalle de las evidencias (archivo, evento, etc.) de las que se deduce esta información.

Respuesta:

Como se ha indicado en la pregunta anterior, las acciones realizadas por el intruso son varias:

En primer lugar, presuntamente, instaló Wireshark y desinstaló Npcap:

[illegible]

Hay varios accesos del usuario Administrador, por lo que no se puede saber si está acción fue realizada por el usuario sospechoso o fue parte del mantenimiento del servidor.

Posteriormente según el archivo "LasActivityView.html", se realizaron las siguientes acciones:

```

7/8/2015 15:48:18 [*****] msiexec /? %1 %2 %3 %4 %5 %6 %7 %8 %9 %10 %11 %12 %13 %14 %15 %16 %17 %18 %19 %20 %21 %22 %23 %24 %25 %26 %27 %28 %29 %30 %31 %32 %33 %34 %35 %36 %37 %38 %39 %40 %41 %42 %43 %44 %45 %46 %47 %48 %49 %50 %51 %52 %53 %54 %55 %56 %57 %58 %59 %60 %61 %62 %63 %64 %65 %66 %67 %68 %69 %70 %71 %72 %73 %74 %75 %76 %77 %78 %79 %80 %81 %82 %83 %84 %85 %86 %87 %88 %89 %90 %91 %92 %93 %94 %95 %96 %97 %98 %99 %100 %101 %102 %103 %104 %105 %106 %107 %108 %109 %110 %111 %112 %113 %114 %115 %116 %117 %118 %119 %120 %121 %122 %123 %124 %125 %126 %127 %128 %129 %130 %131 %132 %133 %134 %135 %136 %137 %138 %139 %140 %141 %142 %143 %144 %145 %146 %147 %148 %149 %150 %151 %152 %153 %154 %155 %156 %157 %158 %159 %160 %161 %162 %163 %164 %165 %166 %167 %168 %169 %170 %171 %172 %173 %174 %175 %176 %177 %178 %179 %180 %181 %182 %183 %184 %185 %186 %187 %188 %189 %190 %191 %192 %193 %194 %195 %196 %197 %198 %199 %200 %201 %202 %203 %204 %205 %206 %207 %208 %209 %210 %211 %212 %213 %214 %215 %216 %217 %218 %219 %220 %221 %222 %223 %224 %225 %226 %227 %228 %229 %230 %231 %232 %233 %234 %235 %236 %237 %238 %239 %240 %241 %242 %243 %244 %245 %246 %247 %248 %249 %250 %251 %252 %253 %254 %255 %256 %257 %258 %259 %260 %261 %262 %263 %264 %265 %266 %267 %268 %269 %270 %271 %272 %273 %274 %275 %276 %277 %278 %279 %280 %281 %282 %283 %284 %285 %286 %287 %288 %289 %290 %291 %292 %293 %294 %295 %296 %297 %298 %299 %300 %301 %302 %303 %304 %305 %306 %307 %308 %309 %310 %311 %312 %313 %314 %315 %316 %317 %318 %319 %320 %321 %322 %323 %324 %325 %326 %327 %328 %329 %330 %331 %332 %333 %334 %335 %336 %337 %338 %339 %340 %341 %342 %343 %344 %345 %346 %347 %348 %349 %350 %351 %352 %353 %354 %355 %356 %357 %358 %359 %360 %361 %362 %363 %364 %365 %366 %367 %368 %369 %370 %371 %372 %373 %374 %375 %376 %377 %378 %379 %380 %381 %382 %383 %384 %385 %386 %387 %388 %389 %390 %391 %392 %393 %394 %395 %396 %397 %398 %399 %400 %401 %402 %403 %404 %405 %406 %407 %408 %409 %410 %411 %412 %413 %414 %415 %416 %417 %418 %419 %420 %421 %422 %423 %424 %425 %426 %427 %428 %429 %430 %431 %432 %433 %434 %435 %436 %437 %438 %439 %440 %441 %442 %443 %444 %445 %446 %447 %448 %449 %450 %451 %452 %453 %454 %455 %456 %457 %458 %459 %460 %461 %462 %463 %464 %465 %466 %467 %468 %469 %470 %471 %472 %473 %474 %475 %476 %477 %478 %479 %480 %481 %482 %483 %484 %485 %486 %487 %488 %489 %490 %491 %492 %493 %494 %495 %496 %497 %498 %499 %500 %501 %502 %503 %504 %505 %506 %507 %508 %509 %510 %511 %512 %513 %514 %515 %516 %517 %518 %519 %520 %521 %522 %523 %524 %525 %526 %527 %528 %529 %530 %531 %532 %533 %534 %535 %536 %537 %538 %539 %540 %541 %542 %543 %544 %545 %546 %547 %548 %549 %550 %551 %552 %553 %554 %555 %556 %557 %558 %559 %560 %561 %562 %563 %564 %565 %566 %567 %568 %569 %570 %571 %572 %573 %574 %575 %576 %577 %578 %579 %580 %581 %582 %583 %584 %585 %586 %587 %588 %589 %590 %591 %592 %593 %594 %595 %596 %597 %598 %599 %600 %601 %602 %603 %604 %605 %606 %607 %608 %609 %610 %611 %612 %613 %614 %615 %616 %617 %618 %619 %620 %621 %622 %623 %624 %625 %626 %627 %628 %629 %630 %631 %632 %633 %634 %635 %636 %637 %638 %639 %640 %641 %642 %643 %644 %645 %646 %647 %648 %649 %650 %651 %652 %653 %654 %655 %656 %657 %658 %659 %660 %661 %662 %663 %664 %665 %666 %667 %668 %669 %670 %671 %672 %673 %674 %675 %676 %677 %678 %679 %680 %681 %682 %683 %684 %685 %686 %687 %688 %689 %690 %691 %692 %693 %694 %695 %696 %697 %698 %699 %700 %701 %702 %703 %704 %705 %706 %707 %708 %709 %710 %711 %712 %713 %714 %715 %716 %717 %718 %719 %720 %721 %722 %723 %724 %725 %726 %727 %728 %729 %730 %731 %732 %733 %734 %735 %736 %737 %738 %739 %740 %741 %742 %743 %744 %745 %746 %747 %748 %749 %750 %751 %752 %753 %754 %755 %756 %757 %758 %759 %760 %761 %762 %763 %764 %765 %766 %767 %768 %769 %770 %771 %772 %773 %774 %775 %776 %777 %778 %779 %780 %781 %782 %783 %784 %785 %786 %787 %788 %789 %790 %791 %792 %793 %794 %795 %796 %797 %798 %799 %800 %801 %802 %803 %804 %805 %806 %807 %808 %809 %810 %811 %812 %813 %814 %815 %816 %817 %818 %819 %820 %821 %822 %823 %824 %825 %826 %827 %828 %829 %830 %831 %832 %833 %834 %835 %836 %837 %838 %839 %840 %841 %842 %843 %844 %845 %846 %847 %848 %849 %850 %851 %852 %853 %854 %855 %856 %857 %858 %859 %860 %861 %862 %863 %864 %865 %866 %867 %868 %869 %870 %871 %872 %873 %874 %875 %876 %877 %878 %879 %880 %881 %882 %883 %884 %885 %886 %887 %888 %889 %890 %891 %892 %893 %894 %895 %896 %897 %898 %899 %900 %901 %902 %903 %904 %905 %906 %907 %908 %909 %910 %911 %912 %913 %914 %915 %916 %917 %918 %919 %920 %921 %922 %923 %924 %925 %926 %927 %928 %929 %930 %931 %932 %933 %934 %935 %936 %937 %938 %939 %940 %941 %942 %943 %944 %945 %946 %947 %948 %949 %950 %951 %952 %953 %954 %955 %956 %957 %958 %959 %960 %961 %962 %963 %964 %965 %966 %967 %968 %969 %970 %971 %972 %973 %974 %975 %976 %977 %978 %979 %980 %981 %982 %983 %984 %985 %986 %987 %988 %989 %990 %991 %992 %993 %994 %995 %996 %997 %998 %999 %1000 %1001 %1002 %1003 %1004 %1005 %1006 %1007 %1008 %1009 %1010 %1011 %1012 %1013 %1014 %1015 %1016 %1017 %1018 %1019 %1020 %1021 %1022 %1023 %1024 %1025 %1026 %1027 %1028 %1029 %1030 %1031 %1032 %1033 %1034 %1035
```

Se descargó el Chrome, además del archivo "2.2.0 20200918 Zerologon encrypted.zip" para posteriormente ejecutar Mimikatz (herramienta de post-explotación poderosa con la cual se puede obtener contraseñas en texto claro, obtener hashes NTLM, así como extraer credenciales de sesiones actuales o pasadas entre otras funciones.)

Además, como se puede observar en el NTUSERDAT se ha realizado los siguiente:


```

1017 {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
1018 Fri May 7 12:59:31 2021 Z
1019 | Microsoft.Windows.Explorer (12)
1020 | C:\Users\Administrador\Desktop\mimikatz_trunk\x64\mimikatz.exe (1)
1021 | {6D809377-6AF0-4448-8957-A3773F02200E}\7-Zip\7zFM.exe (1)
1022 | {6D809377-6AF0-4448-8957-A3773F02200E}\7-Zip\7zFM.exe (1)
1023 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (9)
1024 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (9)
1025 | Fri May 7 11:50:29 2021 Z
1026 | wj32.Process Hacker2 (1)
1027 | wj32.Process Hacker2 (1)
1028 | Fri May 7 11:44:00 2021 Z
1029 | {6D809377-6AF0-4448-8957-A3773F02200E}\SoftPerfect Network Scanner\netscan.exe (1)
1030 | {6D809377-6AF0-4448-8957-A3773F02200E}\SoftPerfect Network Scanner\netscan.exe (1)
1031 | windows.immersivecontrolpanel_cw5n1h2txyewy\microsoft.windows.immersivecontrolpanel (2)
1032 | windows.immersivecontrolpanel_cw5n1h2txyewy\microsoft.windows.immersivecontrolpanel (2)
1033 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\UserAccountControlSettings.exe (1)
1034 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\UserAccountControlSettings.exe (1)
1035 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\ServerManager.exe (1)
1036 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\ServerManager.exe (1)
1037 | Microsoft.Windows.ControlPanel (4)
1038 | Microsoft.Windows.ControlPanel (4)
1039 | Chrome (1)
1040 | Chrome (1)
1041 | Fri May 7 10:13:52 2021 Z
1042 | C:\Users\Administrador\Desktop\ChromeSetup.exe (1)
1043 | C:\Users\Administrador\Desktop\ChromeSetup.exe (1)
1044 | Fri May 7 09:53:32 2021 Z
1045 | {6D809377-6AF0-4448-8957-A3773F02200E}\Wireshark\Wireshark.exe (5)
1046 | {6D809377-6AF0-4448-8957-A3773F02200E}\Wireshark\Wireshark.exe (5)
1047 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe (20)
1048 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe (20)
1049 | Fri May 7 08:02:57 2021 Z
1050 | Microsoft.InternetExplorer.Default (1)
1051 | Microsoft.InternetExplorer.Default (1)
1052 | Thu May 6 15:32:28 2021 Z
1053 | C:\Users\Administrador\Desktop\Wireshark-win64-3.4.5.exe (2)
1054 | C:\Users\Administrador\Desktop\Wireshark-win64-3.4.5.exe (2)
1055 | Thu May 6 14:24:40 2021 Z
1056 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe (3)
1057 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe (3)
1058 | Thu May 6 14:36:42 2021 Z
1059 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\WF.msc (2)
1060 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\WF.msc (2)
1061 | Thu May 6 14:24:49 2021 Z
1062 | {6D809377-6AF0-4448-8957-A3773F02200E}\Windows Defender\MSASCui.exe (1)
1063 | {6D809377-6AF0-4448-8957-A3773F02200E}\Windows Defender\MSASCui.exe (1)
1064 | Thu May 6 14:10:53 2021 Z
1065 | D:\VBoxWindowsAdditions.exe (1)
1066 | D:\VBoxWindowsAdditions.exe (1)
1067 | Thu May 6 14:19:47 2021 Z
1068 | D:\VBoxWindowsAdditions-amd64.exe (1)
1069 | D:\VBoxWindowsAdditions-amd64.exe (1)
1070 | Thu May 6 14:17:09 2021 Z
1071 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (14)
1072 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (14)

```

Dicha imagen identifica los distintos softwares instalados en el sistema, así como las veces que se ha ejecutado cada uno de ellos, registrando la hora en la que se ha realizado la última ejecución.

Pregunta 3 (1 puntos):

¿Cuándo termina las acciones del intruso? Indique el detalle de las evidencias (archivo, evento, etc.) de las que se deduce esta información.

Respuesta:

Las acciones del intruso finalizan (al menos visiblemente) a las **15:01:08** del **07/05/2021**, con la ejecución de la tarea programada CreateObjectTask mediante shell32.dll. Esta acción puede indicar un intento de establecer persistencia en el sistema. Es el último evento asociado al usuario Administrador en el fichero "LastActivityView.html".

Pregunta 4 (2 puntos):

Realice una línea de tiempos de lo ocurrido el día 7/5/2021 con la hora y el evento ocurrido.

Respuesta:

Hora	Evento
11:44:00	Netscan.exe (UserAssist- NTUSER.DAT)
12:44:44	Instalación de chrome.exe
12:19:45	Se abre Zerologon encrypted.zip

12:36:25	Selección de curriculum1.pdf
13:42:23	Logon remoto RDP desde IP 129.205.96.3
13:52:42	Acceso carpeta Mimikatz
14:54:29	Acceso a Z:\ (posible red compartida)
14:54:36	Se abre mimikatz_trunk.zip
15:01:08	Se ejecuta tarea programada CreateObjectTask (persistencia)

Pregunta 5 (2 puntos):

Realice un resumen forense con los siguientes apartados:

1. Antecedentes del caso.

En este apartado se deberán explicar los motivos que han llevado a la empresa a pensar que el equipo ha sido atacado.

2. Informe ejecutivo.

- a. Introducción.
- b. Descripción.
- c. Recomendaciones.

3. Informe técnico.

- a. Objetivos y alcance.
- b. Metodología del análisis.
- c. Listado de evidencias.
- d. Proceso de análisis forense.
- e. Conclusiones.
- f. Recomendaciones.

El informe no debe tener una extensión superior a 1 o 2 hojas y debe realizarse dentro de la siguiente casilla de respuesta.

Respuesta:

1. Antecedentes del caso

Se piensa que la empresa puede haber sido atacada ya que, en el archivo de recursos compartidos, en vez de encontrar un archivo con el curriculum vitae de varios empleados, un trabajador, se encontró un archivo comprimido con contraseña, además de una instancia de NetScan ejecutándose en segundo plano. El sistema presentaba actividades no autorizadas, como el acceso con cuentas privilegiadas, ejecución de herramientas ofensivas y conexiones remotas desde una IP externa desconocida. Esto motivó el análisis forense.

2. Informe ejecutivo

a. Introducción.

Se realiza un análisis forense sobre el servidor WIN-SF01JTM2DHI ante la sospecha de un acceso y ejecución de software malicioso por parte de un usuario con conocimientos avanzados al sistema.

b. Descripción.

Durante la investigación se identificaron accesos locales con la cuenta del Administrador, así como accesos via RDP. Se realizó la apertura/ejecución de herramientas de explotación: Zerologon y mimikatz, así como la ejecución de herramientas de escaneo de red como NetScan así como wireshark. Además, se constató el acceso via RDP desde una ip pública.

c. Recomendaciones.

- Revisión de las cuentas privilegiadas.
- Auditoria del acceso remoto RDP.
- Remplazo de las contraseñas de cuentas con permisos de Administración.
- Revisar las políticas de red para evitar accesos no deseados.

3. Informe técnico

a. Objetivos y alcance.

El objetivo de dicho informe es confirmar si el sistema ha sido comprometido, identificar cómo y cuándo sucedió, así como identificar las acciones realizadas por el sospechoso para poder evaluar el alcance del ataque.

b. Metodología del análisis.

Para realizar el análisis del sistema, se realizará un análisis de las distintas evidencias del sistema. Para ello se analizarán distintos ficheros, entre otros, LastActivityView.txt y NTUSER.DAT, para poder determinar las acciones llevadas a cabo por el sospechoso. Se revisarán los logs del sistema, así como los distintos eventos del sistema para determinar las acciones llevadas a cabo en el servidor.

c. Listado de evidencias.

```

└─ LiveResponseData
  └─ BasicInfo
    │ └─ DiskDriveList_wmic.txt
    │ └─ DiskDriveList_wmic.txt:Zone.Identifier
    │ └─ Full_file_listing.txt
    │ └─ Full_file_listing.txt:Zone.Identifier
    │ └─ Hashes_md5_Startup_and_Dates.txt
    │ └─ Hashes_md5_Startup_and_Dates.txt:Zone.Identifier
    │ └─ Hashes_md5_System32_AllFiles_and_Dates.txt
    │ └─ Hashes_md5_System32_AllFiles_and_Dates.txt:Zone.Identifier
    │ └─ Hashes_md5_System_TEMP_AllFiles_and_Dates.txt
    │ └─ Hashes_md5_System_TEMP_AllFiles_and_Dates.txt:Zone.Identifier
    │ └─ Hashes_md5_User_TEMP_AllFiles_and_Dates.txt
    │ └─ Hashes_md5_User_TEMP_AllFiles_and_Dates.txt:Zone.Identifier
    │ └─ Hashes_sha256_Startup_and_Dates.txt
    │ └─ Hashes_sha256_Startup_and_Dates.txt:Zone.Identifier
    │ └─ Hashes_sha256_System32_AllFiles_and_Dates.txt
    │ └─ Hashes_sha256_System32_AllFiles_and_Dates.txt:Zone.Identifier
    │ └─ Hashes_sha256_System_TEMP_AllFiles_and_Dates.txt
    │ └─ Hashes_sha256_System_TEMP_AllFiles_and_Dates.txt:Zone.Identifier
    │ └─ Hashes_sha256_User_TEMP_AllFiles_and_Dates.txt
    │ └─ Hashes_sha256_User_TEMP_AllFiles_and_Dates.txt:Zone.Identifier
    │ └─ Installed_software_wmic.txt
    │ └─ Installed_software_wmic.txt:Zone.Identifier
    │ └─ LastActivityView.html
    │ └─ LastActivityView.html:Zone.Identifier
    │ └─ List_hidden_directories.txt
    │ └─ List_hidden_directories.txt:Zone.Identifier
    │ └─ Loaded_system_drivers_wmic.txt
    │ └─ Loaded_system_drivers_wmic.txt:Zone.Identifier
    │ └─ LogicalDisk_name_wmic.txt
    │ └─ LogicalDisk_name_wmic.txt:Zone.Identifier
    │ └─ LogicalDisk_size_caption_wmic.txt
    │ └─ LogicalDisk_size_caption_wmic.txt:Zone.Identifier
    │ └─ Possible_unicode_files_and_directories.txt
  
```

- └─ Possible_unicode_files_and_directories.txt:Zone.Identifier
- └─ PrcView_extended_long.txt
- └─ PrcView_extended_long.txt:Zone.Identifier
- └─ PrcView_extended.txt
- └─ PrcView_extended.txt:Zone.Identifier
- └─ psfile.txt
- └─ psfile.txt:Zone.Identifier
- └─ psinfo.txt
- └─ psinfo.txt:Zone.Identifier
- └─ PsList.txt
- └─ PsList.txt:Zone.Identifier
- └─ PsLoggedon.txt
- └─ PsLoggedon.txt:Zone.Identifier
- └─ PsLoglist.txt
- └─ PsLoglist.txt:Zone.Identifier
- └─ Running_processes.txt
- └─ Running_processes.txt:Zone.Identifier
- └─ system_date_time_tz.txt
- └─ system_date_time_tz.txt:Zone.Identifier
- └─ system_info.txt
- └─ system_info.txt:Zone.Identifier
- └─ system_info_wmic.txt
- └─ system_info_wmic.txt:Zone.Identifier
- └─ Windows_codepage.txt
- └─ Windows_codepage.txt:Zone.Identifier
- └─ Windows_Version.txt
- └─ Windows_Version.txt:Zone.Identifier
- └─ CopiedFiles
 - └─ amcache
 - └─ Amcache.hve
 - └─ Amcache.hve:Zone.Identifier
 - └─ info_amcache.log
 - └─ info_amcache.txt
 - └─ chrome
 - └─ Administrador
 - └─ cache
 - └─ data_0
 - └─ data_0:Zone.Identifier
 - └─ data_1
 - └─ data_1:Zone.Identifier
 - └─ data_2
 - └─ data_2:Zone.Identifier
 - └─ data_3
 - └─ data_3:Zone.Identifier
 - └─ cookies
 - └─ Cookies
 - └─ Cookies:Zone.Identifier
 - └─ history
 - └─ History
 - └─ History:Zone.Identifier
 - └─ eventlogs
 - └─ Logs
 - └─ Application.evtx
 - └─ Application.evtx:Zone.Identifier
 - └─ HardwareEvents.evtx
 - └─ HardwareEvents.evtx:Zone.Identifier
 - └─ Internet Explorer.evtx
 - └─ Internet Explorer.evtx:Zone.Identifier
 - └─ Key Management Service.evtx
 - └─ Key Management Service.evtx:Zone.Identifier
 - └─ Microsoft-Client-Licensing-Platform%4Admin.evtx
 - └─ Microsoft-Client-Licensing-Platform%4Admin.evtx:Zone.Identifier
 - └─ Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx
 - └─ Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx:Zone.Identifier
 - └─ Microsoft-Windows-Application-Experience%4Program-Compatibility-Troubleshooter.evtx

		Microsoft-Windows-Application-Experience%4Program-Compatibility-Troubleshooter.evtx:Zone.Identifier
		Microsoft-Windows-Application-Experience%4Program-Inventory.evtx
		Microsoft-Windows-Application-Experience%4Program-Inventory.evtx:Zone.Identifier
		Microsoft-Windows-Application-Experience%4Program-Telemetry.evtx
		Microsoft-Windows-Application-Experience%4Program-Telemetry.evtx:Zone.Identifier
		Microsoft-Windows-Application-Experience%4Steps-Recorder.evtx
		Microsoft-Windows-Application-Experience%4Steps-Recorder.evtx:Zone.Identifier
		Microsoft-Windows-ApplicationResourceManagementSystem%4Operational.evtx
		Microsoft-Windows-ApplicationResourceManagementSystem%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-AppModel-Runtime%4Admin.evtx
		Microsoft-Windows-AppModel-Runtime%4Admin.evtx:Zone.Identifier
		Microsoft-Windows-AppReadiness%4Admin.evtx
		Microsoft-Windows-AppReadiness%4Admin.evtx:Zone.Identifier
		Microsoft-Windows-AppReadiness%4Operational.evtx
		Microsoft-Windows-AppReadiness%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-AppXDeployment%4Operational.evtx
		Microsoft-Windows-AppXDeployment%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-AppXDeploymentServer%4Operational.evtx
		Microsoft-Windows-AppXDeploymentServer%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-AppXDeploymentServer%4Restricted.evtx
		Microsoft-Windows-AppXDeploymentServer%4Restricted.evtx:Zone.Identifier
		Microsoft-Windows-BackgroundTaskInfrastructure%4Operational.evtx
		Microsoft-Windows-BackgroundTaskInfrastructure%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-Biometrics%4Operational.evtx
		Microsoft-Windows-Biometrics%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-Bits-Client%4Operational.evtx
		Microsoft-Windows-Bits-Client%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-CodeIntegrity%4Operational.evtx
		Microsoft-Windows-CodeIntegrity%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-Containers-Wcifs%4Operational.evtx
		Microsoft-Windows-Containers-Wcifs%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-Containers-Wcnfs%4Operational.evtx
		Microsoft-Windows-Containers-Wcnfs%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-Crypto-DPAPI%4BackupKeySvc.evtx
		Microsoft-Windows-Crypto-DPAPI%4BackupKeySvc.evtx:Zone.Identifier
		Microsoft-Windows-Crypto-DPAPI%4Operational.evtx
		Microsoft-Windows-Crypto-DPAPI%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider%4Admin.evtx
		Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider%4Admin.evtx:Zone.Identifier
		Microsoft-Windows-DeviceSetupManager%4Admin.evtx
		Microsoft-Windows-DeviceSetupManager%4Admin.evtx:Zone.Identifier
		Microsoft-Windows-DeviceSetupManager%4Operational.evtx
		Microsoft-Windows-DeviceSetupManager%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-Dhcp-Client%4Admin.evtx
		Microsoft-Windows-Dhcp-Client%4Admin.evtx:Zone.Identifier
		Microsoft-Windows-Dhcpv6-Client%4Admin.evtx
		Microsoft-Windows-Dhcpv6-Client%4Admin.evtx:Zone.Identifier
		Microsoft-Windows-Diagnosis-PLA%4Operational.evtx
		Microsoft-Windows-Diagnosis-PLA%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-Diagnosis-Scheduled%4Operational.evtx
		Microsoft-Windows-Diagnosis-Scheduled%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-FileServices-ServerManager-EventProvider%4Admin.evtx
		Microsoft-Windows-FileServices-ServerManager-EventProvider%4Admin.evtx:Zone.Identifier
		Microsoft-Windows-FileServices-ServerManager-EventProvider%4Operational.evtx
		Microsoft-Windows-FileServices-ServerManager-EventProvider%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-GroupPolicy%4Operational.evtx
		Microsoft-Windows-GroupPolicy%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-HomeGroup Control Panel%4Operational.evtx
		Microsoft-Windows-HomeGroup Control Panel%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-IKE%4Operational.evtx
		Microsoft-Windows-IKE%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-International%4Operational.evtx
		Microsoft-Windows-International%4Operational.evtx:Zone.Identifier

	Microsoft-Windows-lphlpsvc%4Operational.evtx
	Microsoft-Windows-lphlpsvc%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-Kernel-Boot%4Operational.evtx
	Microsoft-Windows-Kernel-Boot%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-Kernel-IO%4Operational.evtx
	Microsoft-Windows-Kernel-IO%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-Kernel-PnP%4Configuration.evtx
	Microsoft-Windows-Kernel-PnP%4Configuration.evtx:Zone.Identifier
	Microsoft-Windows-Kernel-Power%4Thermal-Operational.evtx
	Microsoft-Windows-Kernel-Power%4Thermal-Operational.evtx:Zone.Identifier
	Microsoft-Windows-Kernel-ShimEngine%4Operational.evtx
	Microsoft-Windows-Kernel-ShimEngine%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-Kernel-StoreMgr%4Operational.evtx
	Microsoft-Windows-Kernel-StoreMgr%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-Kernel-WHEA%4Errors.evtx
	Microsoft-Windows-Kernel-WHEA%4Errors.evtx:Zone.Identifier
	Microsoft-Windows-Kernel-WHEA%4Operational.evtx
	Microsoft-Windows-Kernel-WHEA%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-Known Folders API Service.evtx
	Microsoft-Windows-Known Folders API Service.evtx:Zone.Identifier
	Microsoft-Windows-LiveId%4Operational.evtx
	Microsoft-Windows-LiveId%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-MUI%4Admin.evtx
	Microsoft-Windows-MUI%4Admin.evtx:Zone.Identifier
	Microsoft-Windows-MUI%4Operational.evtx
	Microsoft-Windows-MUI%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-NCSI%4Operational.evtx
	Microsoft-Windows-NCSI%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-NetworkProfile%4Operational.evtx
	Microsoft-Windows-NetworkProfile%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-NlaSvc%4Operational.evtx
	Microsoft-Windows-NlaSvc%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-Ntfs%4Operational.evtx
	Microsoft-Windows-Ntfs%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-Ntfs%4WHC.evtx
	Microsoft-Windows-Ntfs%4WHC.evtx:Zone.Identifier
	Microsoft-Windows-PrintService%4Admin.evtx
	Microsoft-Windows-PrintService%4Admin.evtx:Zone.Identifier
	Microsoft-Windows-Program-Compatibility-Assistant%4CompatAfterUpgrade.evtx
	Microsoft-Windows-Program-Compatibility-Assistant%4CompatAfterUpgrade.evtx:Zone.Identifier
	Microsoft-Windows-PushNotification-Platform%4Admin.evtx
	Microsoft-Windows-PushNotification-Platform%4Admin.evtx:Zone.Identifier
	Microsoft-Windows-PushNotification-Platform%4Operational.evtx
	Microsoft-Windows-PushNotification-Platform%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Admin.evtx
	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Admin.evtx:Zone.Identifier
	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx
	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-RemoteDesktopServices-SessionServices%4Operational.evtx
	Microsoft-Windows-RemoteDesktopServices-SessionServices%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-Resource-Exhaustion-Detector%4Operational.evtx
	Microsoft-Windows-Resource-Exhaustion-Detector%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-RestartManager%4Operational.evtx
	Microsoft-Windows-RestartManager%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-Security-SPP-UX-Notifications%4ActionCenter.evtx
	Microsoft-Windows-Security-SPP-UX-Notifications%4ActionCenter.evtx:Zone.Identifier
	Microsoft-Windows-ServerManager-DeploymentProvider%4Operational.evtx
	Microsoft-Windows-ServerManager-DeploymentProvider%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-ServerManager-MgmtProvider%4Operational.evtx
	Microsoft-Windows-ServerManager-MgmtProvider%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-ServerManager-MultiMachine%4Admin.evtx
	Microsoft-Windows-ServerManager-MultiMachine%4Admin.evtx:Zone.Identifier
	Microsoft-Windows-ServerManager-MultiMachine%4Operational.evtx
	Microsoft-Windows-ServerManager-MultiMachine%4Operational.evtx:Zone.Identifier
	Microsoft-Windows-SettingSync%4Debug.evtx

		Microsoft-Windows-SettingSync%4Debug.evtx:Zone.Identifier
		Microsoft-Windows-SettingSync%4Operational.evtx
		Microsoft-Windows-SettingSync%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-Shell-ConnectedAccountState%4ActionCenter.evtx
		Microsoft-Windows-Shell-ConnectedAccountState%4ActionCenter.evtx:Zone.Identifier
		Microsoft-Windows-Shell-Core%4ActionCenter.evtx
		Microsoft-Windows-Shell-Core%4ActionCenter.evtx:Zone.Identifier
		Microsoft-Windows-Shell-Core%4AppDefaults.evtx
		Microsoft-Windows-Shell-Core%4AppDefaults.evtx:Zone.Identifier
		Microsoft-Windows-Shell-Core%4LogonTasksChannel.evtx
		Microsoft-Windows-Shell-Core%4LogonTasksChannel.evtx:Zone.Identifier
		Microsoft-Windows-Shell-Core%4Operational.evtx
		Microsoft-Windows-Shell-Core%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-SmartCard-DeviceEnum%4Operational.evtx
		Microsoft-Windows-SmartCard-DeviceEnum%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-SmbClient%4Connectivity.evtx
		Microsoft-Windows-SmbClient%4Connectivity.evtx:Zone.Identifier
		Microsoft-Windows-SMBClient%4Operational.evtx
		Microsoft-Windows-SMBClient%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-SmbClient%4Security.evtx
		Microsoft-Windows-SmbClient%4Security.evtx:Zone.Identifier
		Microsoft-Windows-SMBServer%4Audit.evtx
		Microsoft-Windows-SMBServer%4Audit.evtx:Zone.Identifier
		Microsoft-Windows-SMBServer%4Connectivity.evtx
		Microsoft-Windows-SMBServer%4Connectivity.evtx:Zone.Identifier
		Microsoft-Windows-SMBServer%4Operational.evtx
		Microsoft-Windows-SMBServer%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-SMBServer%4Security.evtx
		Microsoft-Windows-SMBServer%4Security.evtx:Zone.Identifier
		Microsoft-Windows-SMBWitnessClient%4Admin.evtx
		Microsoft-Windows-SMBWitnessClient%4Admin.evtx:Zone.Identifier
		Microsoft-Windows-SMBWitnessClient%4Informational.evtx
		Microsoft-Windows-SMBWitnessClient%4Informational.evtx:Zone.Identifier
		Microsoft-Windows-StateRepository%4Operational.evtx
		Microsoft-Windows-StateRepository%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-StateRepository%4Restricted.evtx
		Microsoft-Windows-StateRepository%4Restricted.evtx:Zone.Identifier
		Microsoft-Windows-StorageSpaces-ManagementAgent%4WHC.evtx
		Microsoft-Windows-StorageSpaces-ManagementAgent%4WHC.evtx:Zone.Identifier
		Microsoft-Windows-Store%4Operational.evtx
		Microsoft-Windows-Store%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-TaskScheduler%4Maintenance.evtx
		Microsoft-Windows-TaskScheduler%4Maintenance.evtx:Zone.Identifier
		Microsoft-Windows-TerminalServices-LocalSessionManager%4Admin.evtx
		Microsoft-Windows-TerminalServices-LocalSessionManager%4Admin.evtx:Zone.Identifier
		Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx
		Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-TerminalServices-Printers%4Admin.evtx
		Microsoft-Windows-TerminalServices-Printers%4Admin.evtx:Zone.Identifier
		Microsoft-Windows-TerminalServices-Printers%4Operational.evtx
		Microsoft-Windows-TerminalServices-Printers%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Admin.evtx
		Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Admin.evtx:Zone.Identifier
		Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx
		Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-TWinUI%4Operational.evtx
		Microsoft-Windows-TWinUI%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-UniversalTelemetryClient%4Operational.evtx
		Microsoft-Windows-UniversalTelemetryClient%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-UserPnp%4ActionCenter.evtx
		Microsoft-Windows-UserPnp%4ActionCenter.evtx:Zone.Identifier
		Microsoft-Windows-UserPnp%4DeviceInstall.evtx
		Microsoft-Windows-UserPnp%4DeviceInstall.evtx:Zone.Identifier
		Microsoft-Windows-User Profile Service%4Operational.evtx

		Microsoft-Windows-User Profile Service%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-VolumeSnapshot-Driver%4Operational.evtx
		Microsoft-Windows-VolumeSnapshot-Driver%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-VPN%4Operational.evtx
		Microsoft-Windows-VPN%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-Wcmsvc%4Operational.evtx
		Microsoft-Windows-Wcmsvc%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-WFP%4Operational.evtx
		Microsoft-Windows-WFP%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-Windows Defender%4Operational.evtx
		Microsoft-Windows-Windows Defender%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-Windows Defender%4WHC.evtx
		Microsoft-Windows-Windows Defender%4WHC.evtx:Zone.Identifier
		Microsoft-Windows-Windows Firewall With Advanced Security%4ConnectionSecurity.evtx
		Microsoft-Windows-Windows Firewall With Advanced
Security%4ConnectionSecurity.evtx:Zone.Identifier		
		Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx
		Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx:Zone.Identifier
		Microsoft-Windows-WindowsUpdateClient%4Operational.evtx
		Microsoft-Windows-WindowsUpdateClient%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-WinINet-Config%4ProxyConfigChanged.evtx
		Microsoft-Windows-WinINet-Config%4ProxyConfigChanged.evtx:Zone.Identifier
		Microsoft-Windows-Winlogon%4Operational.evtx
		Microsoft-Windows-Winlogon%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-WinRM%4Operational.evtx
		Microsoft-Windows-WinRM%4Operational.evtx:Zone.Identifier
		Microsoft-Windows-WMI-Activity%4Operational.evtx
		Microsoft-Windows-WMI-Activity%4Operational.evtx:Zone.Identifier
		Security.evtx
		Security.evtx:Zone.Identifier
		Setup.evtx
		Setup.evtx:Zone.Identifier
		System.evtx
		System.evtx:Zone.Identifier
		Windows PowerShell.evtx
		Windows PowerShell.evtx:Zone.Identifier
		firefox
		forecopy_handy.log
		forecopy_handy.log:Zone.Identifier
		hosts
		hosts
		hosts:Zone.Identifier
		ie
		logfile
		\$LogFile
		\$LogFile:Zone.Identifier
		mft
		\$MFT
		\$MFT:Zone.Identifier
		prefetch
		registry
		Administrador_NTUSER.DAT
		Administrador_NTUSER.DAT:Zone.Identifier
		COMPONENTS
		COMPONENTS:Zone.Identifier
		DEFAULT
		Default_NTUSER.DAT
		Default_NTUSER.DAT:Zone.Identifier
		Default User_NTUSER.DAT
		Default User_NTUSER.DAT:Zone.Identifier
		DEFAULT:Zone.Identifier
		SAM
		SAM:Zone.Identifier
		SECURITY
		SECURITY:Zone.Identifier

```

| | └─ SOFTWARE
| | └─ SOFTWARE:Zone.Identifier
| | └─ SYSTEM
| | └─ SYSTEM:Zone.Identifier
| └─ SRUMDB
└─ usnjrnl
    └─ $UsnJrnl_$J.bin
        └─ $UsnJrnl_$J.bin:Zone.Identifier

└─ NetworkInfo
    └─ cports.html
    └─ cports.html:Zone.Identifier
    └─ nbtstat.txt
    └─ nbtstat.txt:Zone.Identifier
    └─ NetBIOS_sessions.txt
    └─ NetBIOS_sessions.txt:Zone.Identifier
    └─ netstat_anb_results.txt
    └─ netstat_anb_results.txt:Zone.Identifier
    └─ TCPView.txt
    └─ TCPView.txt:Zone.Identifier

└─ PersistenceMechanisms
    └─ autoruncs.csv
    └─ autoruncs.csv:Zone.Identifier
    └─ autoruncs.txt
    └─ autoruncs.txt:Zone.Identifier
    └─ Driver_group_load_order_wmic.txt
    └─ Driver_group_load_order_wmic.txt:Zone.Identifier
    └─ Loaded_dlls.txt
    └─ Loaded_dlls.txt:Zone.Identifier
    └─ scheduled_tasks.txt
    └─ scheduled_tasks.txt:Zone.Identifier
    └─ services_aw_processes.txt
    └─ services_aw_processes.txt:Zone.Identifier
    └─ Startup_wmic.txt
    └─ Startup_wmic.txt:Zone.Identifier

└─ UserInfo
    └─ All_logons_wmic.txt
    └─ All_logons_wmic.txt:Zone.Identifier
    └─ whoami.txt
    └─ whoami.txt:Zone.Identifier

```

23 directories, 373 files

Entre ellos se pueden descartar los siguientes:

- LastActivityView.html
- NTUSER.DAT
- Carpeta de eventos

d. Proceso de análisis forense.

Para realizar el análisis forense, en primer lugar, se ha realizado un estudio de las distintas evidencias aportadas para el caso. Se han estudiado en primer lugar, los logs de acceso al servidor, proporcionados por los eventos de Windows del sistema, donde se puede determinar quién accedió al servidor y la manera en la que accedió.

Para determinar las acciones realizadas por el usuario sospechoso, se ha realizado un análisis del LastEventView.html donde aparecen reportadas las distintas actividades de los usuarios. Para poder analizar de manera mas minuciosa los eventos del sistema, mediante la herramienta RegRipper, se ha procedido a ver el contenido de diversos archivos, entre ellos en NTUSER.DAT donde aparece información relativa a la ejecución de software en dicho servidor. Además de usar RegRipper, se han utilizado otras

herramientas:

- Hayabusa
- Autopsy
- DB-browser
- FullEventLogView
- NTFS data tracker
- WinPrefetch
- RegistryExplorer

e. Conclusiones.

Se ha realizado un acceso sospechoso al servidor por RDP desde la ip 129.205.96.3, previamente a dicho acceso se han llevado a cabo una serie de acciones entre las que podemos destacar las indicadas en la siguiente imagen:

```
1017 {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
1018 Fri May 7 12:59:31 2021 Z
1019 | Microsoft.Windows.Explorer (12)
1020 | Fri May 7 12:54:54 2021 Z
1021 | C:\Users\Administrador\Desktop\mimikatz_trunk\x64\mimikatz.exe (1)
1022 | Fri May 7 12:12:47 2021 Z
1023 | {6D809377-6AF0-444B-8957-A3773F02200E}\7-Zip\7zFM.exe (1)
1024 | Fri May 7 11:52:41 2021 Z
1025 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (9)
1026 | Fri May 7 11:50:29 2021 Z
1027 | wj32.ProcessHacker2 (1)
1028 | Fri May 7 11:44:00 2021 Z
1029 | {6D809377-6AF0-444B-8957-A3773F02200E}\SoftPerfect Network Scanner\netscan.exe (1)
1030 | Fri May 7 10:50:30 2021 Z
1031 | windows.immersivecontrolpanel_cw5n1h2txyewy\microsoft.windows.immersivecontrolpanel (2)
1032 | Fri May 7 10:50:27 2021 Z
1033 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\UserAccountControlSettings.exe (1)
1034 | Fri May 7 10:41:59 2021 Z
1035 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\ServerManager.exe (1)
1036 | Fri May 7 10:40:28 2021 Z
1037 | Microsoft.Windows.ControlPanel (4)
1038 | Fri May 7 10:33:45 2021 Z
1039 | Chrome (1)
1040 | Fri May 7 10:13:52 2021 Z
1041 | C:\Users\Administrador\Desktop\ChromeSetup.exe (1)
1042 | Fri May 7 09:53:32 2021 Z
1043 | {6D809377-6AF0-444B-8957-A3773F02200E}\Wireshark\Wireshark.exe (5)
1044 | Fri May 7 09:47:44 2021 Z
1045 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe (20)
1046 | Fri May 7 08:02:57 2021 Z
1047 | Microsoft.InternetExplorer.Default (1)
1048 | Thu May 6 15:32:28 2021 Z
1049 | C:\Users\Administrador\Desktop\Wireshark-win64-3.4.5.exe (2)
1050 | Thu May 6 15:24:40 2021 Z
1051 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe (3)
1052 | Thu May 6 14:36:42 2021 Z
1053 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\WF.msc (2)
1054 | Thu May 6 14:24:49 2021 Z
1055 | {6D809377-6AF0-444B-8957-A3773F02200E}\Windows Defender\MSASCui.exe (1)
1056 | Thu May 6 14:19:53 2021 Z
1057 | D:\VBoxWindowsAdditions.exe (1)
1058 | Thu May 6 14:19:47 2021 Z
1059 | D:\VBoxWindowsAdditions-amd64.exe (1)
1060 | Thu May 6 14:17:09 2021 Z
1061 | {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (14)
```

El usuario sospechoso ha descargado varios programas externos para su posterior instalación. En las actividades de post-explotación ha utilizado el software Mimikatz para entre otras cosas obtener credenciales de los usuarios.

f. Recomendaciones.

- Limitar el acceso de red para no permitir accesos por la red pública, reforzando las medidas de segmentación de red
- Cambiar las credenciales de los usuarios locales.
- Centralizar los logs en un SIEM para detección temprana.

