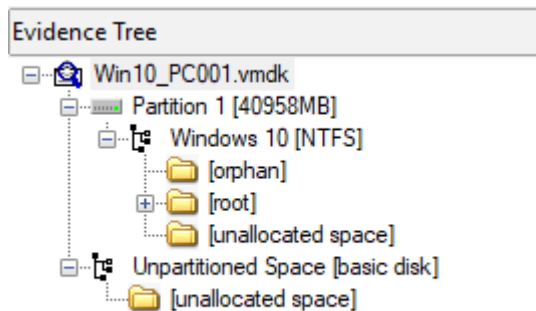


Práctica Windows

En primer lugar, descargamos la evidencia desde el enlace proporcionado.

Para la realización de la práctica, utilizaremos la herramienta FTK Imager.

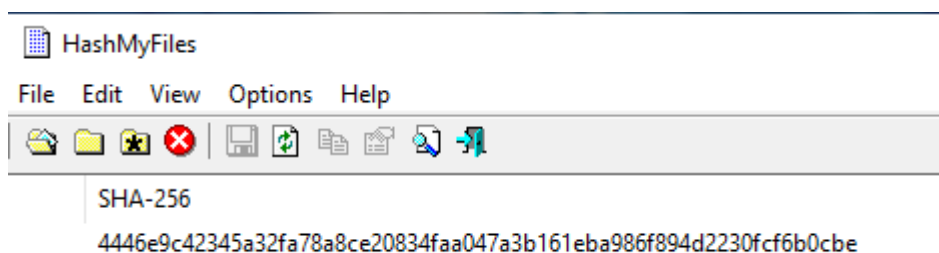
El primer paso será cargar la evidencia descargada;



Hash del fichero

Como analistas de la máquina, lo primero que debemos obtener es el hash sha-256 de la evidencia.

Para ello, utilizaremos la herramienta HashMyFiles a la cual le pasaremos el archivo para que nos de el hash sha-256



Nombre del fichero

Desde el ftk imager nos vamos a la ruta windows/system32/config y exportamos los ficheros SAM, security,system,software,default y sus logs

Abrimos la herramienta WRR y cargamos los ficheros previamente descargados.

Ahora, nos vamos al fichero system → windows installation y abajo del todo vemos el apartado Machine name: **PEGASUS01**

Free to use for private, educational and non-commercial purposes

DEFAULT SAM SECURITY SOFTWARE **SYSTEM**

NAVIGATOR

- File Information
- Security Records
- SAM
- Windows Installation**
- Hardware
- Startup Applications
- Services and Drivers
- Network Configuration
- Windows Firewall Settings
- Environment
- Shell Folders
- Outlook Express
- Raw Data

General Installed Software (0) Hot Fixes (0) Start Menu (0)

Product Name:

Owner:

Organization:

Product ID:

Product Key:

Product Version:

Install Date:

Service Pack:

System Root:

Release Id:

Build Lab: 17763.rs5_release.180914-1434

Build Lab Ex: 17763.1.amd64fre.rs5_release.180914-1434

Last Boot (UTC): 29/04/2022 11:45:38

Last Shutdown (UTC): 29/04/2022 10:30:16

User Name:

Machine name: **PEGASUS01**

Contraseñas débiles

Utilizaremos la herramienta mimikatz averiguar la contraseña del usuario.

Debemos ejecutar la herramienta y a continuación ejecutar el siguiente comando;

```
lsadump::sam /system:C:\Users\forensic\Desktop\Practica\SYSTEM  
/sam:C:\Users\forensic\Desktop\Practica\SAM
```


Esto nos mostrará los hashes de las contraseñas de los usuarios. En este caso, utilizaremos la del usuario IEuser

```
User : IEUser  
Hash NTLM: 2d20d252a479f485cdf5e171d93985bf
```

Cogemos su Hash NTLM y lo pasamos por la herramienta de crackstation para que nos de su contraseña en claro:

2d20d252a479f485cdf5e171d93985bf

No soy un robot


Privacidad - Términos

Crack Hashes

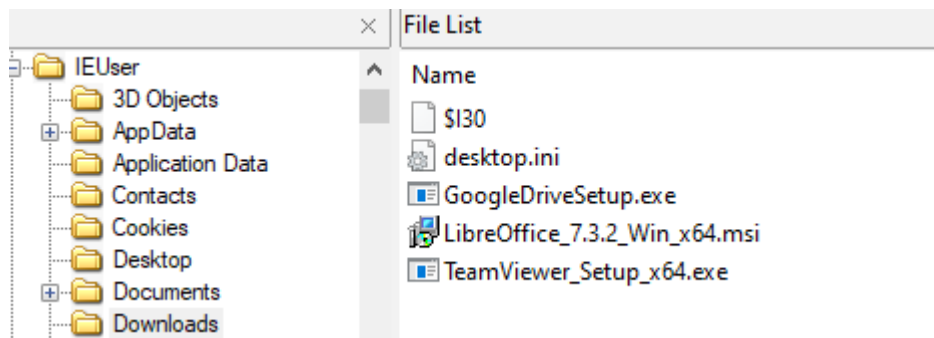
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
2d20d252a479f485cdf5e171d93985bf	NTLM	qwerty

Obtenemos la contraseña: **qwerty**

Descarga fichero de control remoto

Desde el ftk imager, navegamos a la carpeta de descargas del usuario y encontramos el archivo **TeamViewer_Setup_x64.exe**



Fecha descarga software control remoto

Para ello, nos descargamos el archivo y analizamos sus metadatos, viendo que ha sido creado el **29 de abril de 2022**



TeamViewer_Setup_x64.exe

Tipo de archivo: Aplicación (.exe)

Descripción: TeamViewer_Setup_x64.exe

Ubicación: C:\Users\forensic\Desktop\Practica

Tamaño: 35,6 MB (37.398.984 bytes)

Tamaño en disco: 35,6 MB (37.400.576 bytes)

Creado: viernes, 29 de abril de 2022, 19:11:25

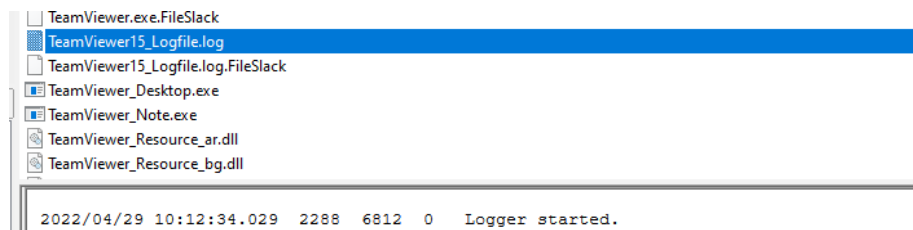
Modificado: viernes, 29 de abril de 2022, 19:11:34

Último acceso: hoy, 14 de diciembre de 2024, hace 1 minuto

Fecha de ejecución programa de control remoto

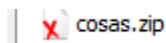
Desde el ftk, dentro de la carpeta de TeamViewer, encontramos el archivo **TeamViever15_LogFile.log** y al abrirlo vemos la fecha de ejecución del programa

29/04/2022



Ficheros eliminados

Con autopsy, buscamos los ficheros eliminados y filtramos por la extension zip, encontrando el archivo **cosas.zip**



Ficheros maliciosos

Navegando con el ftk imager a través de las carpetas + utilizadas por los atacantes para dejar sus ficheros de malware, nos encontramos dentro de las carpeta TMP varios ficheros sospechosos, entre los que se encuentra el powershell que buscábamos **WMIBackdoor.ps1**;

File List			
Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	08/05/2022 19:...
127.0.0.1.txt	1	Regular File	11/10/2014 3:0...
d.txt	10	Regular File	11/10/2014 3:4...
nbtscan.exe	36	Regular File	04/02/2018 19:...
p.exe	373	Regular File	27/04/2010 10:...
p.exe.FileSlack	4	File Slack	
scan1.tmp	0	Regular File	08/05/2022 19:...
scan2.tmp	0	Regular File	08/05/2022 19:...
scan3.tmp	0	Regular File	08/05/2022 19:...
sys.txt	8	Regular File	08/05/2022 19:...
WMIBackdoor.ps1	20	Regular File	10/08/2015 13:...
xCmd.exe	824	Regular File	29/07/2014 15:...

