Rom Com Windows $MFT and Zimmerman tools

Guia Forense Completo: Análise de `.vhdx` com EZ Tools no Kali Linux

Objetivo: Realizar uma análise forense de um ficheiro de disco virtual (`.vhdx`) do Windows, extraindo e analisando o Master File Table (`$MFT`) usando as ferramentas de Eric Zimmerman (EZ Tools) de forma nativa no Kali Linux. Este guia serve como um manual de metodologia e um registo completo do processo de investigação e depuração.

Fase 1: Preparação (A Estação de Trabalho Forense)

Nesta fase, preparamos o nosso ambiente de forma segura, garantindo que a prova original permanece intacta e que temos as pastas necessárias para uma investigação organizada.

A Regra de Ouro (Fazer uma Cópia): Nunca trabalhe diretamente na prova original. Isto garante a integridade da prova.

```
cp evidence.vhdx evidence_copy.vhdx
```

1.

Organizar o Espaço de Trabalho: Crie pastas para as suas ferramentas e para os ficheiros de saída da análise. Uma boa organização é a chave para uma investigação eficiente.

```
mkdir /home/nukitaro/EZTools
mkdir /home/nukitaro/Analysis_Output
```

2.

Novo Termo: .vhdx (Virtual Hard Disk v2)

- **O que é?**: Um contentor digital que funciona como um disco rígido completo. É uma "cápsula do tempo" digital da máquina que está a investigar.
- **Porque nos importamos?**: É a nossa cena do crime. Tudo o que precisamos está lá dentro, mas precisamos das ferramentas certas para a "abrir". [Imagem de um ícone de disco rígido virtual]

Fase 2: Aceder à Prova (Montar a Imagem)

O nosso objetivo é "abrir" o `.vhdx` para que possamos ver os ficheiros lá dentro. O processo de tornar um sistema de ficheiros acessível chama-se **montagem**.

Instalar as Ferramentas de Montagem: `libguestfs-tools` é o conjunto de chaves-mestras para abrir imagens de disco virtual em Linux.

```
sudo apt-get update
sudo apt-get install -y libguestfs-tools
```

1.

Criar um Ponto de Montagem: Uma pasta vazia que servirá de "portal" para o conteúdo do `.vhdx`.

```
sudo mkdir /mnt/vhdx_evidence
```

2.

Mapear o Disco: Antes de montar, vamos ver o mapa de partições dentro do `.vhdx`.

```
sudo virt-filesystems -a evidence_copy.vhdx
```

3. Isto irá listar as partições, como `/dev/sda1` e `/dev/sda2`. **Para este guia, vamos assumir que a partição principal do Windows é `/dev/sda2`.**

Montar a Partição Principal:

```
sudo guestmount -a evidence_copy.vhdx -m /dev/sda2 --ro /mnt/vhdx_evidence
```

4.

Novo Comando: guestmount

- **O que faz?**: Monta sistemas de ficheiros de imagens de disco virtuais.
- **`a`**: Adiciona a imagem de disco a ser processada.
- **`m /dev/sda2`**: Monta **manualmente** a partição específica que identificámos.

- `-ro`: A opção mais importante! Monta em modo **R**ead-**O**nly (apenas leitura), protegendo a nossa prova de qualquer alteração acidental.

O conteúdo do disco do Windows está agora acessível de forma segura em `/mnt/vhdx_evidence`.

Fase 3: Preparar as Ferramentas de Análise (PowerShell e EZ Tools)

Agora vamos usar o PowerShell para automatizar o download de todas as ferramentas de que precisamos.

Execute o PowerShell: O PowerShell já não é exclusivo do Windows; é uma ferramenta de automação multi-plataforma poderosa, incluída no Kali para interagir com ambientes modernos.

pwsh

1.

Descarregue, Descompacte e Execute o Script:

```
# --- DENTRO DO POWERSHELL (PS >) ---
wget <https://download.ericzimmermanstools.com/Get-ZimmermanTools.zip> -O /tmp/Get-ZimmermanTools.zip
unzip /tmp/Get-ZimmermanTools.zip -d /home/nukitaro/EZTools/
rm /tmp/Get-ZimmermanTools.zip
/home/nukitaro/EZTools/Get-ZimmermanTools.ps1 -Dest /home/nukitaro/EZTools/ -NetVersion 9
```

2.

Novos Tipos de Ficheiro:

- `.zip` **(ZIP Archive)**: Um "caixote" que contém múltiplos ficheiros.
- `.ps1` **(PowerShell Script)**: Uma receita de comandos do PowerShell para automatizar tarefas. [Imagem do logótipo do PowerShell]

Fase 4: A Análise (Execução e Depuração)

Esta é a fase mais crítica, onde executamos a análise e resolvemos os problemas que surgem.

4.1 - Depuração: O Mistério do `dotnet`

A primeira tentativa de executar a análise como `root` falhou, pois o `root` não sabia onde encontrar o programa `dotnet` que foi instalado para o utilizador `nukitaro`.

A Caça: Usámos o comando `find` para localizar a instalação.

```
find /home/nukitaro -name "dotnet"
```

1. **Saída Esperada**: `/home/nukitaro/.dotnet/dotnet`

2. **A Solução**: Em vez de usar um `alias` ou um link simbólico, a forma mais garantida de executar a ferramenta é usar o **caminho absoluto para o `dotnet`** do utilizador `nukitaro`, mesmo quando se é `root`.

4.2 - A Execução Final (O Momento Eureka!)

Com o caminho exato para a versão correta do .NET, pudemos finalmente executar o comando com sucesso.

Torne-se Root: Para ler os ficheiros montados, precisamos de privilégios de administrador.

```
# Se ainda estiver no PowerShell, escreva 'exit'
sudo -s
```

1.

Execute o MFTECmd com o caminho correto e explícito:

```
# Dentro da sua shell de root (#)
/home/nukitaro/.dotnet/dotnet /home/nukitaro/EZTools/net9/MFTECmd.dll -f
/mnt/vhdx_evidence/'$MFT' --csv /home/nukitaro/Analysis_Output/mft_analysis
```

2.

Saída de Sucesso:

```
MFTECmd version 1.3.0.0
Author: Eric Zimmerman (...)
CSV output will be saved to
/home/nukitaro/Analysis_Output/mft_analysis/DATE_TIME_MFTECmd_$MFT_Output.csv
```

[Imagem de uma lupa sobre código de computador] Esta saída confirma que a análise foi bem-sucedida e o ficheiro CSV foi criado.

Novos Conceitos e Tipos de Ficheiro:

- `.dll` **(Dynamic Link Library)**: Uma biblioteca de código que contém as funções de um programa .NET.
- `dotnet`: O interpretador que executa aplicações .NET. Usar o caminho absoluto garante que estamos a usar a versão correta (9.0).
- `.csv` **(Comma-Separated Values)**: Um ficheiro de texto que representa uma tabela, perfeito para filtrar com `grep`.

Fase 5: Próximos Passos - Como Encontrar a Resposta

Agora que tem o seu ficheiro `mft_analysis.csv`, o segredo é **filtrar**. Use a sua shell de `root` ou de utilizador normal (depois de mover o ficheiro) para começar a caça.

Pergunta do Desafio: "Qual é o nome do ficheiro de arquivo na pasta de documentos da Susan que explora a vulnerabilidade ao ser aberto?"

A Solução na Linha de Comandos: Esta é a forma mais rápida de encontrar a resposta.

Mude o Dono do Ficheiro: Primeiro, dê a si mesmo a permissão para ler o ficheiro de saída.

```
 # Saia da shell de root
exit
# Mude o dono da pasta de resultados e do seu conteúdo
sudo chown -R nukitaro:nukitaro /home/nukitaro/Analysis_Output
```

1.

Use `grep` para Filtrar:

```
 # Navegue para a pasta de resultados
cd /home/nukitaro/Analysis_Output/mft_analysis

# Procure por ficheiros de arquivo na pasta de documentos da Susan
grep -i "Users\\\\Susan\\\\Documents" *.csv | grep -i -E "\\.zip|\\.rar|\\.7z"
```

2.

O nome do ficheiro na saída deste comando será a sua resposta.

A Solução Visual (LibreOffice Calc):

1. Abra o ficheiro `.csv` no LibreOffice Calc (lembre-se de definir o separador como vírgula).
2. Use a função `Data -> AutoFilter`.
3. Filtre a coluna **`ParentPath`** para conter `Users\\Susan\\Documents`.
4. Filtre a coluna **`Extension`** para mostrar apenas `zip`, `rar`, e `7z`.
5. A linha (ou linhas) que sobrarem conterão a sua resposta na coluna `FileName`.