Forense

Capítulo destinado a técnicas y herramientas de análisis forense en sistemas operativos y otros

- Sistema operativo Linux
- Sistema operativo Windows

Sistema operativo Linux

Captura de memoria RAM

Requisitos:

- Aceso al sitema
- Privilegios de administrador
- Dispositivo USB con almacenamiento mayor a la RAM

Herramientas:

- LiME (Linux Memory Extractor)
- Volatility

Análisis forense al tráfico de red (Local)

Requisitos:

- Acceso al sistema
- Privilegios de administrador

Herramientas:

- Wireshark
- NetworkMiner
- PcapXray

Analisis forense al trafico de red (Remoto)

Requisitos:

- Logs de switches, routers, and firewalls

Herramientas

- Análisis manual

Copia forense del disco de almacenamiento de datos (Sin apagar el sistema)

Requisitos:

- Acceso al sistema
- Privilegios de root
- Dispositivo usb con almacenamiento mayor al disco a analizar

Posibles herramientas:

- Solo se identificaron herramientas para el sistema operativo Windows

Copia forense del disco de almacenamiento de datos (Servidor Apagado)

Requisitos

- Acceso fisico al disco de almacenamiento
- Dispositivo usb con almacenamiento mayor al disco a analizar

Posibles herramientas

- dc3dd
- dd
- FTK Imager

Otras técnicas

Ver los puertos abiertos y proceso asociados

```
lsof -i -P
```

Ver los archivos abiertos por un proceso

```
lsof -p <pid>
```

Ver los últimos logeos

```
last
```

Quién está logeado actualmente

```
who
w
```

Ver el historial de comandos

```
more ~/.bash_history
```

Investigar proceso sospechoso

```
cd /proc/<pid>
strings ./exe
```

Fuentes:

- Learn Computer Forensics: A beginner’s guide to searching, analyzing, and securing digital evidence
- Digital Forensics and Incident Response - Second Edition

Sistema operativo Windows

Análisis de conexiones

```
netstat -naob
netstat -f
```

Ver recursos compartidos

```
net view
```

Ver que equipos se estan comunicando con el sistema actual

```
net session


net use
```

Análisis de procesos

Ver servicios

```
tasklist /svc
```

Ver las DLLs asociadas a un proceso

```
tasklist /m /fi "pid eq <pid>"
```