Hidden Evidence

Challenge Description Category: Forensics / Windows Post-Exploitation

1. Discovery

The challenge presents a raw disk image named evidence.dd captured from a compromised Windows workstation. The objective is to locate data hidden by an attacker who obtained Administrator-level access.

Initial inspection of the disk geometry using mmls reveals the partition layout:

```
$ mmls evidence.dd
...
002:  000:000   0000000128   0000100351   NTFS / exFAT (0x07)
...
```

This indicates an NTFS partition starting at sector offset **128**.

2. Artifact Analysis

Standard file analysis tools might miss data if it is not stored in standard files. We utilize The Sleuth Kit's fls tool to recursively list the file system contents starting at the identified offset.

Command: fls -o 128 -f ntfs -r evidence.dd | grep ":"

The output reveals a suspicious entry attached to a standard text file: r/r 39-128-3: Documents/project_notes.txt:hiddendata

3. The Logic

This finding indicates the presence of an **NTFS Alternate Data Stream (ADS)**.

- **Standard File:** project_notes.txt contains the visible data (Meeting notes).
- **Hidden Stream:**: hiddendata is a secondary stream attached to the file entry.

4. Solving

To retrieve the flag, we must extract the contents of the specific stream inode (39-128-3) identified in the analysis phase. We use the icat tool to dump the raw data from that stream.

Payload: Execute the extraction command targeting the hidden stream's Inode.

Console Output:

```
$ icat -o 128 -f ntfs evidence.dd 39-128-3

LNMHACKS{NTFS_Streams_Are_Invisible}
```