# Linux Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

@ppolstra
http://philpolstra.com

Certifications:
http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

# From Inodes to Filenames

# Directories

- Map names to inodes
- Each directory is treated as a file

| Offset | Size | Name | Description |
|---|---|---|---|
| 0x0 | 4 | Inode | Inode |
| 0x4 | 2 | Rec len | Record length |
| 0x6 | 2 | Name len | Name length |
| 0x8 | | Name | Name string (up to 255 characters) |

# Directories (Filetype feature)

| Offset | Size | Name | Description |
|---|---|---|---|
| 0x0 | 4 | Inode | Inode |
| 0x4 | 2 | Rec len | Record length |
| 0x6 | 1 | Name len | Name length |
| 0x7 | 1 | File type | 0x00 Unknown<br>0x01 Regular<br>0x02 Directory<br>0x03 Char device<br>0x04 Block device<br>0x05 FIFO<br>0x06 Socket<br>0x07 Sym link |
| 0x8 | | Name | Name string (up to 255 characters) |

# Directory Tail

- Phony entry at the end of each directory block
- Adds checksum to directories

| Offset | Size | Name | Description |
|---|---|---|---|
| 0x0 | 4 | Inode | Set to zero (inode zero is invalid so it is ignored) |
| 0x4 | 2 | Rec len | Record length (set to 12) |
| 0x6 | 1 | Name len | Name length (set to zero so it is ignored) |
| 0x7 | 1 | File type | Set to 0xDE |
| 0x8 | 4 | Checksum | Directory leaf block CRC32 checksum |

# Hash Directories

- Meant to improve performance
- Fools old systems by storing hash entries after “end” of directory block
- Directory nodes are stored in a hashed balanced tree (hashed btree = htree)
- The ext4_index flag is set for an inode if it contains a directory htree
- “.” and “..” entries stored in traditional way at start of the block

# Root Hash Directory Block

| Offset | Size | Name | Description |
|---|---|---|---|
| 0x0 | 12 | Dot rec | “.” directory entry (12 bytes) |
| 0xC | 12 | DotDot rec | “..” directory entry (12 bytes) |
| 0x18 | 4 | Inode no | Inode number set to 0 to make following be ignored |
| 0x1C | 1 | Hash version | 0x00 Legacy 0x03 Legacy unsigned<br>0x01 Half MD4 0x04 Unsigned half MD4<br>0x02 Tea 0x05 Unsigned Tea |
| 0x1D | 1 | Info length | Hash info length (0x8) |
| 0x1E | 1 | Indir levels | Depth of tree |
| 0x1F | 1 | Unused flag | Flags (unused) |
| 0x20 | 2 | Limit | Max number of entries that follow this header |
| 0x22 | 2 | Count | Actual number of entries after header |
| 0x24 | 4 | Block | Block w/i directory for hash=0 |
| 0x28 | | Entries | Remainder of block is 8-byte entries |

# Interior Node Hash Directory Block

| Offset | Size | Name | Description |
|---|---|---|---|
| 0x0 | 4 | Fake inode | Set to zero so this is ignored |
| 0x4 | 2 | Fake rec len | Set to block size (4k) |
| 0x6 | 4 | Name length | Set to zero |
| 0x7 | 1 | File type | Set to zero |
| *0x8* | *2* | *Limit* | *Max entries that follow* |
| *0xA* | *4* | *Count* | *Actual entries that follow* |
| *0xE* | *4* | *Block* | *Block w/i directory for lowest hash value of block* |
| 0x12 | | Entries | Directory entries |

# Hash Directory Entry

| Offset | Size | Name | Description |
|---|---|---|---|
| 0x0 | 4 | Hash | Hash value |
| 0x4 | 4 | Block | Block w/i directory of next node |

| Offset | Size | Name | Description |
|---|---|---|---|
| 0x0 | 4 | Reserved | Set to zero |
| 0x4 | 4 | Checksum | Block checksum |

# Examining Directories