Linux Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

@ppolstra
http://philpolstra.com

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

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

Filesystem Analysis: Incompatible Features

Incompatible Features

- Filesystem should not be mounted, not even read-only, if these features are not supported
- The fsck utility should not be run against this filesystem

Why do we care about features?

- Affect the structure of block groups
- That in turn affects where data is located
- Affects how data is stored in inodes, etc.
- Some features might supply additional metadata for analysis

Incompatible Features

Bit	Name	Description
0x1	Compression	Filesystem is compressed
0x2	Filetype	Directory entries include the file type
0x4	Recover	Filesystem needs recovery
0x8	Journal Dev	Journal is stored on an external device
0x10	Meta BG	Meta block groups are in use
0x40	Extents	Filesystem uses extents
0x80	64Bit	Filesystem can be 2^64 blocks (as opposed to 2^32)
0x100	MMP	Multiple mount protection
0x200	Flex BG	Flexible block groups are in use

Incompatible Features (cont.)

Bit	Name	Description
0x400	EA Inode	Inodes can be used for large extended attributes
0x1000	DirData	Data in directory entry
0x2000	BG Meta Csum	
0x4000	LargeDir	Directories > 2GB or 3-level htree
0x8000	Inline Data	Data inline in the inode
0x10000	Encrypt	Encrypted inodes are used in this filesystem

Features that affect layout

- Flexible block groups
  - Multiple BG treated as one logical BG
  - Bitmaps and inode table for whole logical group in first BG
- Meta block groups
  - Filesystem partitioned into several meta block groups
  - Group descriptors (for meta group) in first, second, and last BG
- 64-bit mode
  - Indirectly affects layout by changing some structure sizes

Getting Compatible Feature Information