Linux Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

@ppolstra
http://philpolstra.com

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

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

©SecurityTube.net

Inodes and Extended Attributes

©SecurityTube.net

Extended Attributes

- Can be stored in
  - Extra space between inodes (256 – inode size, usually=100)
  - A data block pointed to by file_acl in inode
- First use was Access Control Lists (ACL)
- Can be used to store most anything as a user attribute if name starts with “user.”
- If ACLs are used the filesystem must be mounted with correct options for older kernels

©SecurityTube.net

Extended Attribute Structures

- Header (Magic number only in inodes)

Offset	Size	Name	Description
0x0	4	Magic no	0xEA020000

Offset	Size	Name	Description
0x0	4	Magic no	0xEA020000
0x4	4	Ref count	Reference count
0x8	4	Blocks	Blocks used to store extended attributes
0xC	4	Hash	Hash
0x10	4	Checksum	Checksum
0x14	12	Reserved	Should be zeroed

©SecurityTube.net

Extended Attribute Entries

Offset	Size	Name	Description
0x0	1	Name len	Length of attribute name
0x1	1	Name index	0x0 = no prefix 0x1 = user. Prefix 0x2 = system.posix_acl_access 0x3 = system.posix_acl_default 0x4 = trusted. 0x6 = security. 0x7 = system. 0x8 = system.richacl
0x2	2	Value offs	Offset from first inode entry or start of block
0x4	4	Value block	Disk block where value stored or zero for this block
0x8	4	Value size	Length of value
0xC	4	Hash	Hash for attribs in block or zero if in inode
0x10		Name	Attribute name w/o trailing NULL

©SecurityTube.net

Examining Extended Attributes

©SecurityTube.net