508.5 - Advanced Adversary and Anti-Forensics Detection

Anti-Forensics Overview.......................... 5-6

- Common anti-forensics..5-6

Recovery of Deleted files via VSS........... 9-17

- Overview/history 9
- Technical information 10
  - Scope Snapshots...10
- Volume shadow examination overview..........11-16
  - Overview... 11-12
  - 'vshadowinfo' - List available snapshots 13
  - 'vshadowmount' - Mount VSS drive.................. 14-15
  - Auto mount snapshots remotely............................16
- VSS Examination with log2timeline.py.................17
  - psort deduplication 17

Advanced NTFS Tactics..............................21

- History...21-22
- NTFS features 23
- Master File Table (MFT) 25-34
  - Overview..25
  - MFT entries..26
  - System files... 26-29
    - $Bitmap..26
    - $MFT, $MFTMIRR, $LOGFILE, $VOLUME, $ATTRDEF, $BOOT, $BADCLAUS, $SECURE, $UPCASE, $EXTEND..27-29
  - Allocated vs. unallocated 30
  - Sequential MFT entries 31
  - Typical MFT entry attributes 32
  - MFT entry overview 33-34
- MFT Analysis..35-55
  - 'istat' - Sleuth Kit 35-37
    - Analyzing filesystem metadata 35-36
    - Analyzing header & $STANDARD_INFORMATION..37-40
      - Bit breakdown 38-39
        - *MFT file signature, Fixup array, $LogFile, Sequence number, Hard link count, FILE RECORD Size, Extended Records.................38*
        - *Next available ID, Fixup information...........39*
        - *$STANDARD_INFORMATION Attribute..39-40*
        - *MACB 40*
        - *Attribute flags..40*
        - *Tracking numbers ($Secure, $Quota, $UsnJml) 40*
    - Analyzing $FILE_NAME & Attributes 41-43
      - Summary 41
      - $FILE_NAME Attribute...................................41-43
  - Time rules (Cheatsheets).................................. 44-45
    - $STANDARD_INFORMATION.................................44
    - $FILENAME 45
  - Detecting timestamp manipulation 46-48
    - Overview 46
    - Techniques...47
    - Example..48
  - Analyzing $DATA 49-52
    - Overview 49
    - $DATA Attribute...50
    - ADS – Alternate Data Streams............................51-52
  - 'icat' – Extracting data from MFT............................53
  - Zone.Identifier ADS (evidence of download)..... 54-55
- Filename analysis layer 56-57
  - Filenames & directory metadata....................... 56-57
    - $I30 – NTFS Directory Attributes 57
    - Directory slack...56
  - B-tree Index Searching 58-60
    - Overview 58
    - Index data carving...59
    - $I30 Index Breakdown......................................59-60
  - B-tree Index Rebalancing 61-62
  - Parsing $I30 directory indexes 63-64
    - Indx2csv, Indxparse.py, Velociraptor...................63-64
- Filesystem journaling..65-81
  - Overview...65

- $LogFile – Filesystem resilience 66-67
- $UsnJrnl – Change Tracking............................... 68-69
- Common activity patterns................................. 70-74
  - Overview 70
  - Patterns...71-72
  - $UsnJrnl "Reason" codes 73
  - $LogFile Operation Codes 74
- Useful filters and Searches 75-76
- LogFileParser.exe - $LogFile analysis................. 77-78
- 'MFTECmd.exe' - $UsnJrnl analysis.................... 79-80
- What happens when a file is deleted?.....................81

Advanced Evidence Recovery 83-

- Overview..84
- File wiping.. 85-91
  - SDelete example..85
  - Other wipers 87-91
    - BCWipe...88-89
    - Eraser...90
    - Cipher.exe...90-91
- Registry.. 92-93
  - Record recovery 92
  - Finding 'fileless' malware in registry 93
- File Recovery 94-98
  - Metadata method vs. Carving method................94-95
    - 'icat' - Metadata method...................................96
    - 'PhotoRec' – Carving method.........................97-98
- Recovering Volume Shadows 99-102
  - Overview 99
  - Carving for VSS in SIFT...................................100-101
  - 'vss_carver' – Example 102
- Event log & Filesystem stream carving 103-105
  - 'Bulk extractor' – Windows log carving............103-104
  - 'blkls' – Exctract/present unallocated clusters ..104-105
  - 'EVTXtract' – Extract raw XML events.....................105
- Carving for strings.. 106-107

Defensive Countermeasures....................... 108-111

- Leverage filesystem history........................... 109-110
  - VSS..109
  - $LogFile...109
  - USN...110
  - Monitoring admin tools..110
- Level up logging..111