COMP 2555 Principles of Computer Forensics

Lecture 9

Ramki Thurimella, PhD

Overview

- Project 2 has been posted
- Review commands from pp. 122—142, Module 3 of CERT Book
- Material to be covered:
  - Chapter 5 from Vacca
- Simple PERL script for a PC
- Quiz 3 on Wednesday (covers Module 3, up to pp. 142 & Chapter 5)

Download/Experiment

- Unix/Linux commands
  - lsof
    - Unlinked files
    - Unix shutdown process: graceful vs sudden
  - find and locate
  - chkconfig
  - inittab
  - grep
  - crontab
  - top

Download/Experiment

- Windows Commands
  - dir
  - ntlast (turn on auditing)
  - MACMatch
  - Autorunsc
  - PsFile
  - handle
  - pclip

Logged on Users

- Pay attention to
  - recently added user accounts (research this question on UNIX/Windows)
  - escalated privileges
  - remote access accounts
  - the total number that have access or currently logged on
  - activity times

Logged on Users (Windows)

- Netusers
- PsLoggedOn
- net
- NTLast
- DumpUsers

Logged on Users (UNIX)

- w
- finger
- whoami
- su
- last
- lastlog

Chapter 5 Data Recovery

- Data erasure is lot harder than data recovery
- Data loss reasons
  - Hardware failure
  - Accidental deletion/reformatting
  - Viruses
  - Overwriting
  - Fire/disaster
- Hard to recover with common tools

Examples from real world

- A Dog's Dinner
  - Chewing up floppies/flash drives?
- Credit card monster
  - Electronic assembly failure
- Flying low
  - Physical damage (headstack swap)
- Accounts critical
  - Recording errors
- Sinking Ship
  - Seismic survey ship (media flaw)
  - Contained geological surveys
- All flooded out
  - Automotive engineers
  - 40 tape optical cartridges

Requirements for a backup

- nonintrusive
  - Obstacles (56% of all data not backed up)
    - Backup window (when to perform)
    - Network bandwidth
    - System throughput (I/O Bottlenecks)
    - Lack of resources (shortage of expertise)
- Avoid single point failures (centralized solutions with one back up server)
- Support for 24x7 data
- Support for user errors
- Quick restoration
- Host-processor independence

Some solutions

- Move tapes closer to data
- Incremental backup
- Mirroring
  - Does not protect against user error and replication of bad data
  - Synchronizing, breaking and resyncing is *not* trivial
- Backup and mirroring are complementary

Hiding & Recovering Data on Linux

- Linux undelete
  - Ext2/ext3 (to determine use df)
  - Debugfs
  - Grep/Strings command
    - Run grep on /dev/hda2
- Bmap
- Data wiping using dd
  - http://en.wikipedia.org/wiki//dev/zero

Backing up a PC

- Simple PERL script
- Another solution using 7-zip

Project 2

- Discussion
- Next class: Midterm Review
- CANVAS