COMP 2555 Principles of Computer Forensics

Lecture 8

Ramki Thurimella, PhD

Overview

- Quiz 2
- Project 2 will be posted by tomorrow
- Experiment with commands from pp. 122—142, Module 3 of CERT Book

Download/Experiment

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

Download/Experiment

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

Logged on Users

- Pay attention to
  - recently added user accounts
  - 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 (Windows)

- w
- finger
- whoami
- su
- w –a
- last
- lastlog