Why Compromises Matter - Access Control

Monday, July 29, 2013
9:21 AM

User Access Control

What files can user read and/or write?
What programs can the user run?

root or Admistrator account
- can access everything
- "superuser"

Normal users
- Windows & Unix/Linux allow user groups to be set up to say what "extra" access users in that group have
- default is to just give access to user's own files/programs & to "system-wide" programs
- risk - privilege escalations

root kits
- any program that acts w/ superuser privileges
- often hide their presence by changing system programs

anomaly based intrusion detection
- detect "abnormal" behavior
- also called heuristic-based intrusion detection