Lecture notes for “Stalking the Wily Hacker”

Targeted attacks
- Attacker wants specialized information
- Often not automated, driven by human attacker
  - [How do you know it's a human? Typos!]
- May use previously unknown attack methods

Context
- Lawrence Berkeley Labs (LBL) is US national lab attached to UC-Berkeley
- Attacked in August 1986
- Initially discovered as 75 cent accounting error
- Rather than immediately shutting down attacked systems, repurposed them to honeypots that collected attack information for 10 months
- Watched where attacks originated
- Watched what attacker did next

Honeypot
- Heavily monitored system designed to attract attackers
- Provides opportunity to observe the use of previously unseen attacks
- Here, line systems repurposed (dual-purposed) as honeypots

Traceback
- Follow network connections backward from victim system back to attack source
- Generally requires assistance from admins at each hop backward
- Step through routing hops
- Step through stepping stones

Stepping Stone
- A system that is both a victim and an attack source used by an attacker as an intermediary
- Step through several victim systems before reaching true target
- Obfuscates attack source, complicates traceback
- LBL was often a stepping stone

Lessons
- Most vulnerabilities due to errors by vendors, users, & admins
  - Emacs bug worsened by setuid-root
  - Tested common account names (incl “field”) and passwords
    - (world password file no longer true... now has shadow file)

        - (shadow password file first created in 1988... 2 years after this)
    - Vendors shipped software with default accounts and backdoors left over from testing
        - [google android]
- Attacker used known attacks
- Sensitivity of stolen data increased when data was aggregated
- Logging was invaluable (here, logging was done via physical printer)
- Stealth logging important (attacker looked for evidence that s/he was detected
    - [IDS without IP]
- Police care only about monetary loss

Espionage

- Targets
    - Jet Propulsion Labs
    - Anniston Army Depot
    - Air Force Systems Command Space Division
    - Optimus Database Pentagon
    - MIT
    - US Air Force Ramstein, West Germany
    - US Navy Costal Systems
    - US Army Ft Stewart, GA
    - SRI International
    - Mitre
    - BBN
- Investigators
    - CIA
    - FBI
    - NSA
    - Air Force Office of Special Investigations
    - Bundespost
    - Bundeskriminalamt (german fbi)
- Outcome
    - Five hackers in West Germany selling information to Soviet KGB via East Berlin
    - All five charged in Germany with espionage
    - One committed suicide by self-immolation