Network Intrusion Detection

CSC 196n
Computer System Attacks and Countermeasures
Class Objectives

• Students will:
  – Define the types of intrusion detection systems
  – Understand HIDS vs NIDS
  – Understand Snort/ACID
Intrusion Detection

- Reactive
- Passive
- Can trigger investigation
- More useful as a tool after an investigation has started
- Can require big resources (false positives, frequent reconnaissance scans, *etc.*)
Network-based ID

• Sniff the network and look for patterns
• Signature-based NIDS look for “evil” traffic
• Or, build a profile of known good traffic and alert on anomalies
• Snort is one of the best lightweight NIDS that happens to be open source
• Commercial NIDS have many features but often won’t let you examine or manipulate individual rules
Host-based ID

• Best kind of ID because the target host is the only place you can *really* see what’s going on
• Keeps track of important files on the system and alerts you when they change
  Tripwire is most popular
Poor man’s IDS

• Network-based: NetFlow, tcpdump
• Host-based: scripting with find, mtree, ncheck, etc.
• Can be every bit as useful as a full-blown IDS product
Ways to use ID

• Hire a full-time team of people to handle alerts from the IDS
  – Filter out false positives
  – Try to prevent future false positives
  – Handle credible threats

• Just keep the IDS running and consult it whenever you’re looking for a specific detect
Snort

• Lightweight
  – Lean code
  – Doesn’t try to implement lofty features such as anti-virus integration
  – *Fast* -- can handle a saturated 100-Mb link

• Open source

• Well-supported
Snort Rules

• Can be obtained from the Snort web site, usually within hours of a detect’s discovery
• Easy to create on your own
• Rules can be used for basis of other research and documentation
Other Snort Features

• Supports modules for sophisticated handling of alerts
  – Can detect broad port scans instead of alerting on each probe
  – Can send alerts to you via e-mail or pager
• Can store alert data in an SQL database
• Can obfuscate IP addresses
ACID

- Analysis Console for Intrusion Databases
- Web interface to Snort
- Excellent tool for an incident response team
Snort/ACID Deployment (Standalone)

• Build boxes with both Snort and ACID
• Sprinkle them throughout your network
• Connect to a specific box to investigate that particular portion of your network
Snort/ACID Deployment (Sensor/Analysis)

- Build many sensor boxes with Snort
- Install one ACID analysis console
- Snort sensors report back to ACID console, a single point for you to do your analysis
Resources

• **SNORT** snort.org
• **ACID** http://acidlab.sourceforge.net/