Tool of the Week: Snort

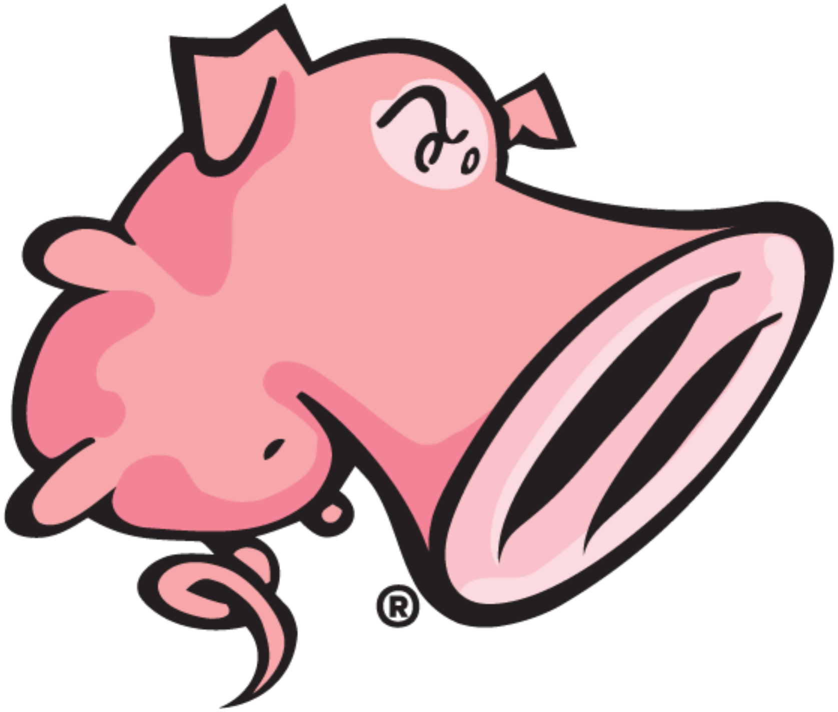
Eric Scott

Steven Pitman

What is Snort?

- Open-Source Network Intrusion Prevention System

- Provides real-time traffic analysis and packet logging



Sniffer Mode

- Sniffer Mode displays packet headers and/or contents to the screen

- **snort –vde**
  - -v = verbose (prints all packets)
  - -d = display application layer data
  - -e = display link layer packet headers

Packet Logger Mode

- Packet Logger Mode allows packet data to be written to a log file

- **snort -vde –l <*path_to_log_directory*>**
  - -l = location of log directory

- Log files generated depend on how data is captured

Playback Mode

- Playback mode allows the user to read packet data that has been written to log files, tcpdumps, etc

- **snort -dv –r <*path_to_file*>**
  - -r = read file at provided location

Network Intrusion Detection System Mode (NIDS)

- NIDS mode takes advantage of a rules system to generate alerts based on network traffic
- **snort.conf** used in this mode for determining rules files
- ***<rules_name>*.rules** used to group related rules
  - EX. **gamer.rules** for alerting on video game related traffic

Use Case: Excessive Slackers

- Managers suspect poor productivity is being caused by excessive use of non-work related sites during work

- System administrator can use Snort’s NIDS mode to track how often suspected non-work related sites are being used

Questions?