Snort - Wiki

"Snort's open source network-based intrusion detection system (IDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching and matching. The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, semantic URL attacks, buffer overflows, server message block probes, and stealth port scans. Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk. In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified."

1) Installation and user manual
    a. Download - https://www.snort.org/downloads
    b. User Manual - http://manual-snort-org.s3-website-us-east-1.amazonaws.com/
    c. Please note, WinPcap is also required but default installation should work for our experiment on all versions of Windows.
    d. See: https://www.youtube.com/watch?v=_snieZtj8fQ
2) Basic Packet Capture with Snort
    a. Use both command line and the GUI interface, if available, on the OS release chosen.
        i. If working in windows, you may need to temporarily disable your firewall.
    b. From a terminal prompt type snort -v and analyze the results. If you need to generate traffic, open a browser or use another terminal to ping. Use Ctrl + c to stop the packet captures.
    c. What information is disclosed in these captures?
    d. Try snort -dv and a browser connection.
    e. What additional data is revealed?
    f. What other flags are available with snort?
    g. Experiment with -K ascii (and logs).
        i. Logs by default are stored in \snort\logs by ipaddress.
    h. What does -A do?
3) IDS Alerts
    a. Use the following command to initialize snort in Alert mode using the default rules
    b. snort -q -A console -i eth0 -c /etc/snort/snort.conf
    c. Test snort's responses by generating suspicious traffic such as nmap scan of all ports on this system.
    d. See: https://www.youtube.com/watch?v=RUmYojxy3Xw
    e. View some of the rules provided, such as cat /etc/snort/rules/icmp.rules

(Windows: c:\snort\rules -- If this folder is empty, download from www.snort.org/pub-bin/downloads.cgi -- VRT Certified Rules for Snort and extract them to this folder. These may be viewed in notepad.)