Network Management
Why do we care?

Dale Smith

dsmith@nsrc.org

UNIVERSITY OF OREGON

Why Network Management?

- Is your network up and running or is something wrong?
  - Your goal should know about problems before people start to complain
- Who is using the network?
- What are they using it for?
- What is “normal” for your network

What to Monitor

- Packet switching portions of the network
  - Switches and routers
- Servers that are important
  - DHCP and DNS
  - Web servers and web caches
  - Email and other servers

Network Management and Security

- You will have security issues
  - You will have compromises and hackers
  - You will have viruses
- You get a call from your ISP saying that they have a report that one of your hosts is participating in a SPAMing
  - What do you do?
  - How do you find the host (very hard if NAT)?

Understanding your Network

- Network management is the key to understanding your network
  - Is it up or down?
  - Are there other problems?
  - What devices are on your network and where are they?
  - Are there devices with viruses?

Network Traffic Analysis

- It is important to know what traverses your network
  - You learn about a new virus and find out that all infected machines connect to 128.223.60.21
  - What machines have connected?
- What tools are available?
  - netflow: you will learn about this
  - Snort: open source intrusion detection system that is very useful to find viruses

Log Analysis

- Can be just as important as traffic analysis
- Central syslog server and gather logs from:
  - DHCP server, DNS servers, Mail servers, switches, routers, etc.
  - Now, you have data to look at
  - Given an IP, you can probably find user
- Lots of tools to correlate logs and alarm on critical events

Centralized Authentication

- AAA: Authorization, Authentication, and Accounting
- Central database of users
  - Can be a single system that everyone has a login (or password file entry)
  - LDAP or Microsoft Active Directory
- Systems and Devices use database
  - Protocols: Radius, LDAP, Kerberos, LDAP, and Active Directory

Virus Protection

- Most viruses are spread through the action of users
  - Clicking “OK” or “Install” when they shouldn’t
  - Firewalls generally won’t help
  - Windows needs virus protection software (is MS Security Essentials enough?)
- Server-based viruses or intrusions are typically caused from external attacks
  - Firewalls might help

What do you need?

- You must have manageable devices
  - Without them, you are blind
- You must configure switches, routers, and servers to support SNMP
- You must install public domain software on a central server to watch over your network and gather data about its operation
  - This is what we are going to cover this week

What Do you Want to Learn?

- We are not sure what would be most useful to you
  - We are prepared to teach a variety of things
- I would like each person to introduce themselves
  - Indicate who operates their network (is it contracted to the telephone company)
  - Indicate what tools you currently use to monitor your network

Questions/Discussion?