Campus Network Security
High Level Overview

Dale Smith
Network Startup Resource Center
dsmith@nsrc.org

This document is a result of work by the Network Startup Resource Center (NSRC at http://www.nsrc.org). This document may be freely copied, modified, and otherwise re-used on the condition that any re-use acknowledge the NSRC as the original source.
Campus Networks and Security

• Goal: Prepare for problems you will have
  – 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 Denial of Service (DoS) attack
  – What do you do?
  – How do you find the host (very hard if NAT)?
Security is a Process

- You can never achieve security – it is a process that you have to continually work on
  - Assessment – what is at risk
  - Protection – efforts to mitigate risk
  - Detection – detect intrusions or problem
  - Response – respond to intrusion or problem
  - Do it all over again
Security Policy Framework

• Why is policy important?
  – How do your users know what is permissible?
  – How do you know what you can do?
    • Can you disconnect users from the network?
    • Can you eavesdrop on network traffic?

• What do you include?
  – Typical policy framework for a University is an “Acceptable Use Policy” or AUP
    • Google “University Acceptable Use Policy”
Typical Acceptable Use Policy

• Use of University computing and network for University-related use only (prohibits commercial use)
• Shall not interfere with use of computing or network of others (prohibits hogging of resources)
• Copyright must be respected
• Violators can be denied access
• Use of computing and network is not private and can be monitored by IT Staff
• And more. Use Google and find examples
• Make this an official University Policy so that violations of AUP will be treated as violations of University policy
Design with Security in Mind

• Segmentation and IP addressing schemes
  – Follow campus network best practices
  – Route in the core
  – One IP Subnet per building
  – Put campus-level servers on IP subnet that is separate from users

• Where to put firewalls and IDSs
  – Firewalls protect critical assets
  – IDS needs to see as much traffic as possible
Typical Design

- REN or ISP
- Border Router
- Firewall
- Core Router
- Central Servers for campus
- Port configured on router as a mirrored or SPAN port
- Intrusion Detection System
- At least one IP Subnet for every building
Another Typical Design

- REN or ISP
- Border Router
- Intrusion Detection System
- Port configured on switch as a mirrored or SPAN port
- Firewall
- Core Router
- At least one IP Subnet for every building
- DMZ
- Public Servers
- Central Servers for campus
- Core Router
Another Typical Design

- REN or ISP
- Border Router
- Intrusion Detection System
- Port configured on switch as a mirrored or SPAN port
- Core Router
- Firewall
- At least one IP Subnet for every building
- DMZ
- Public Servers
- Central Servers for campus

---

NSRC
Network Security Resource Center
Security Foundation

- You must have managed equipment in your network
- You must have some basic network management running
- Network Management is the foundation that much of the security framework operates on
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
Encryption

• Encryption is important
  – Protect sensitive data
  – Protect passwords

• Disable clear-text password protocols
  – Disable telnet, ftp
  – Only allow TLS based POP and IMAP
  – Move all web traffic to HTTPS that involves passwords or sensitive data
SSL Certificates

• Don’t use self-signed for public services
  – They teach users bad habits
• Get certificates from well known certificate authorities (CA)
• Larger campus may want to provide certificate service
Wireless

• Best practice is to authenticate users
  – This allows you to know who your users are
  – Requires central AAA database
  – Log the access to your central syslog server

• How to do this
  – Captive Portal
  – 802.1x WPA2 Enterprise

• Who can install access points (AUP)?
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
Responding to Incidents

• This is not an “if”, but “when”. You will have incidents.

• Need to establish policy & procedures

• This is different from an AUP – it is an internal operating policy
  – Who do you notify?
  – Can you disconnect a system from the network?
High Level Wrapup

• Security is hard – you are never done
  – You are always in the Assessment, Prevention, Detection, Response cycle

• Many security tools and practices builds upon your network management framework
  – Build your network management framework first and get started on all of this

• Acceptable Use Policy a high priority
Resources

• Lots of resources on the Internet
  – www.sans.org – subscribe to the SANS newsletter
  – www.cert.org – a good resource for lists of vulnerabilities
  – www.wikipedia.org – good source of information for lots of topics