

# **Security at NCAR**

**David Mitchell**

**February 20th, 2007**

# Overview

- What are we trying to accomplish? What are *they* trying to accomplish?
- What are the different pieces?
- How do they fit together in order to protect us?

# Why?

- Attackers generally have a single technical goal.
  - Get their code to run on our machines
- Many motivations
  - launch more attacks
  - steal passwords
  - send spam
  - bragging rights

# How?

- Direct attack on servers
  - open a connection directly to a listening server and take advantage of a misconfiguration or software bug
- Stolen credentials
  - many users re-use their passwords and usernames at different sites
- Get *you* to run their code
  - Email the program to victims, or trick them into downloading it from a web site

# Router Filters

- Block inbound traffic to most hosts at NCAR
- Slows or prevents direct network attacks
  - Morris worm hit infected as much as 10% of the Internet on November 2nd, 1988
  - SQL Slammer infected about 75,000 hosts in 10 minutes on January 24th, 2003.
- Simple stateless filters are used.
- They really only block the packets which open new TCP connections.

# Router Filters

- Some hosts are outside the filters. These are known as 'external.'
- Other hosts are inside the filters, but some selected services are allowed in. These are 'exposed' or 'semi-exposed.'
- Once an attacker is inside, filters don't slow them down.

# VPN

- Provides a way for hosts physically outside of our security filters to be temporarily inside them.
- All traffic between the client and VPN server is encrypted.
- Growing importance as more staff work from home and carry laptops.
- Allows the filters to be more stringent than might otherwise be acceptable.

# Tipping Point

- Intrusion Prevention System or IPS.
- Watches all traffic in and out of the VPN for known types of attacks.
- Will drop connections which appear to be part of an attack.
- Home machines are often poorly maintained, so extra scrutiny of their traffic is prudent.

# Patching

- Keeping software up to date with fixes to known security problems.
- Vital for servers accessible from the outside.
  - Automated attacks happening all the time.
- Increasingly important for all hosts as attacks move to 'data driven' ones directed at the client machines.
- Fortunately, OS vendors are getting better at making this easy to do.

# Tokens

- New password for every login.
- Mitigate risk from stolen passwords.
- Expect to see increased usage of tokens over time. Particularly for the VPN.

# Client Based Tools

- Various software tools used on the client computers to check for suspect software and behaviour
  - Virus scanning
  - Personal firewalls

# Email Scanning

- All inbound email scanned for attachments.
- Some, such as .exe files, blocked outright.
- Others are run through virus scanners.

# Traffic Monitoring

- Security group monitors all network traffic to and from the Internet.
- Can sometimes spot an attack in progress.
- Assist in clean-up after an attack by identifying affected hosts.

# Web Scanning

- Currently no attempt is made to scan web browsing of staff.
- For now, prompt patching seems to be sufficient.

# Conclusion

- Security is a moving target.
- Web didn't exist, email used to be 'safe.'
- We try to slow or prevent known avenues of attack while still allowing users to get their work done.
- Somewhat like the Dutch boy sticking his finger in the dyke.