IPCOP, Firewalls, and remote access

How to get around the Quirks in a Microsoft Corporate Environment

Mike Warot - APCU - October 2004

Introduction

- My Job
- My Skill Set
- Live Marketing
- Our business requirements / tradeoffs
  - System Security
    - Weak passwords ok
    - Assumption of inevitable vulnerabilty
    - Outages acceptable if workarounds available
    - Separate systems where possible
      - *Phone*
      - *Fax*
      - *Network*
      - *Copier*
  - Backups vs "nonstop"
    - We can afford to lose a day or two if things go south, but no more
    - "Big Check Theory"
  - Client driven requirments
    - Support Media for Presentations
      - *Scripts (Word)*
      - *PowerPoint*
      - *Flash (authored externally)*
      - *Video (via Web/Email)*

How we got here

- Windows domain, Exchange 4, Ten-4 systems
  - Windows NT Server, with Domain, and NO default gateway to Internet
  - Windows 95 workstations (real IP addresses)
  - Microsoft Office 4
  - Smiley, the Access 2.0 database
  - Quirks
    - Random Blue Screen of Death on workstations
    - Page - Ok... everyone get out of Smiley! (Daily!)

- Email silent failures (~1/week)

Upgrade to Exchange Server 5.5

- First direct connection to the internet
  - Email became "reliable"

Office 97 invasion

- Smiley gets upgraded to Access 97
  - Smiley now fails less than 4 times/year
- Office 97 invades the office
- Quirks
  - Random Blue Screen of Death
  - Virii become issue ~4/year

Internet providers disappear

- Dual homed networking implemented
- Today
  - T1
  - DSL

Microsoft declairs death of NT4

- Upgrade to 2000 server

Server exploits proliferate

- Need for Firewall becomes overwhelming

Red Hat 9.0 based firewall

- Created a transparent bridged firewall
  - leading edge OS
  - separate authentication
  - could be bypassed if it failed
  - no change to existing IP addresses
- Quirks
  - External Outlook users died

VPN Server implemented

- Worked well, problem solved
- Quirks
  - Internet Stopped working when connected to VPN
  - Don't know enough Linux, behavior of Firewall on reboot uncertain
  - RedHat gets stupid, drops users including me!

Disabled Default Gateway

- Disabled the default gateway on the Windows VPN clients, solved the problem
- Not quite
- Quirks = VPN client bug, ignores Subnet mask!

New Private Network

- Set up 192.168.2.x private network
  - Subnet mask still issue
- Moved to 10.0.0.x
  - Still issue, but safer (Panera Bread free Internet?)
- Quirks
  - Server communication issues creep up
  - Need for NAT firewall becomes apparent
  - IPcop mentioned on Slashdot

IPcop

- tested it first: works well!
- Easy to administer

Today

- Quirks
  - Backup is manual
  - 10.0.0.x VPN client issue
  - Virii proliferation is scarey
  - Need to migrate to an GPL software environment
  - VPN MTU issue (outlook freaks with attachments, really disappearing packets)
    - *DrTCP from DSL Reports, set RAS MTU to 1328*

Why Firewall?

Windows vulnerabilities

- Ping of death
- Buffer overflows
- Defense in depth
  - Different OS, different vulnerabilties
  - Different passwords
  - Don't make it easy
  - Cut down annoyances
  - Make it safe to set up a computer

The average time to system compromise for an naked Windows XP computer is now 14 minutes, less than the time to download the patches to make it safe.

- Why not Firewall?
  - The need for a VPN
  - Can't dual-home hosts
  - Single point of failure

Why IPcop?

- Single source
- Open Source Software
- Web based administration

Free and Cheap

Features I found useful

Things left out

- Dual Homed networks

How it works

- Packet rewriting
- Transparent Proxy
- Port Forwarding

Firewalling Windows

- The Example network
- Services and implications
  - Outbound Connectivity
  - Web Server
  - Mail Server
  - File Server
  - VPNs
  - DNS and Active Directory
  - Active directory and IP addresses

Demonstration

- IPcop installation
- Update installation
- Port Forwarding configuration
- Testing the installation

Discussion

- Question and answer session