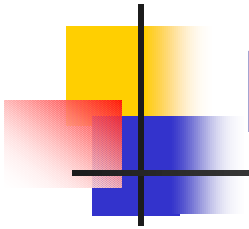
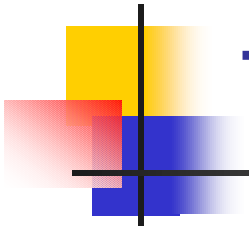
Life on a University Network

An Architecture for Automatically Detecting, Isolating, and Cleaning Infected Hosts



Background

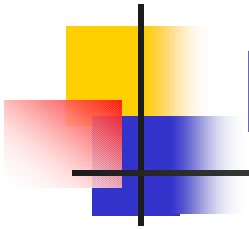
- Eric Gauthier – elg@bu.edu
- Boston University
  - Private University in downtown Boston, MA
  - 17,682 undergraduate
  - 11,367 graduate
- I'm a Network Engineer, not:
  - A security professional
  - A windows programmer
  - A lawyer



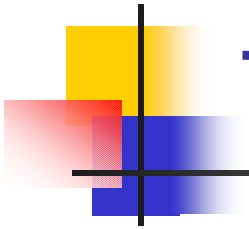
The BU Network

- 3-Tier hierarchical network with Multi-Gig backbone and w/10Mbps port per student
- We handle layers 1 – 4 and ISP services (DNS, DHCP...)
- ~ 20,000 Systems
- ~ 2,000 Switches/routers
- ~ 200 Buildings and ~ 20 Staff members
- Variety of network devices, vendors, features
- Host OS diversity, though ~ 2 – 4 years old
- Not everything supports trunking

Facing the Abyss... and not Flinching

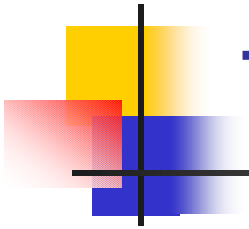


- 12,000 students all showing up on Friday, all with at least one computer, and Classes Start Tuesday.
- Hosts: 90% Microsoft, 75% post Win98/NT.
- ~ 1 in 3 systems are vulnerable if not infected (I.e. 50% of post Win98/NT).
- The Solution is a “Self-Help” type system
- Its all “Free” – except the labor
- Infrastructure and Host OS Independent
- Its not a Silver Bullet



The Team

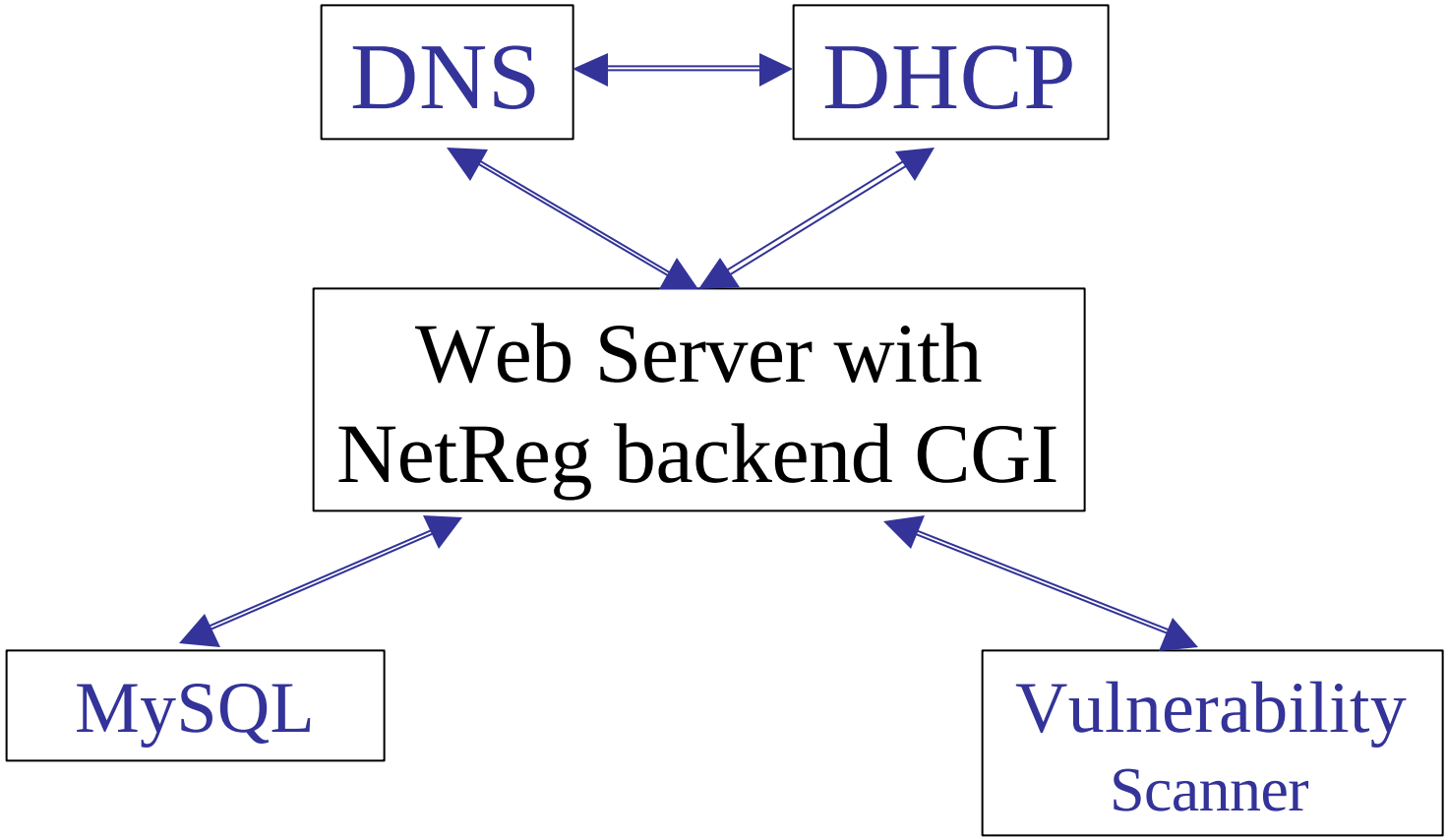
- NetReg as known/unknown tracker
- Nessus to scan
- Cleaning tool
- Later IDS/Vulnerability Scans
- Quarantining



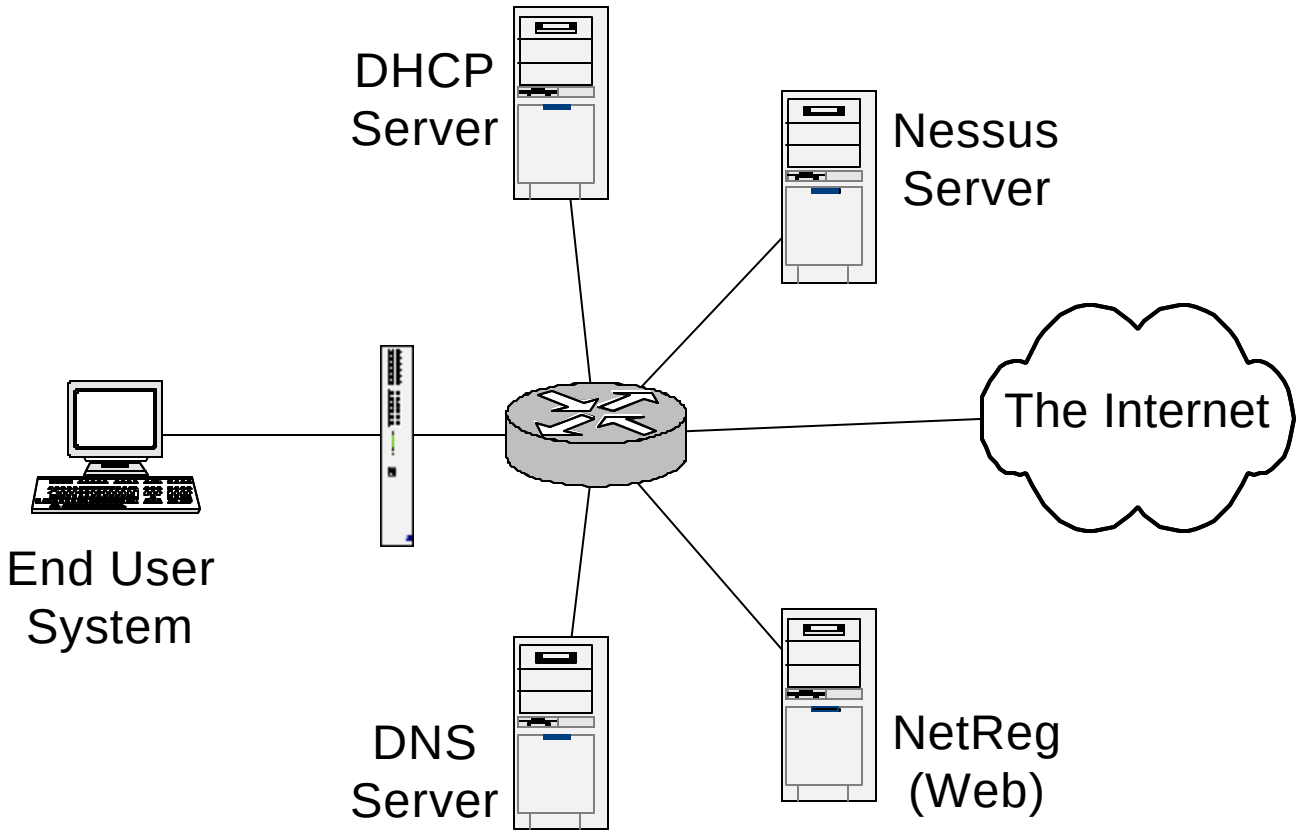
Thank You for Registering

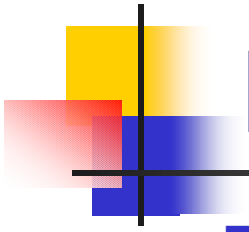
- Mac Address Registration System/Database
- DHCP (un)known = host (un)registered
- DNS multiviews and and web virtual hosting tricks are used to present registration information
- Single subnet/multi-subnet vlans
- Quarantines = Host in the database but not known to the DHCP server
- AUP: "*you accept responsibility for the actions of this system*".

What Does NetReg Use?



Network Registration

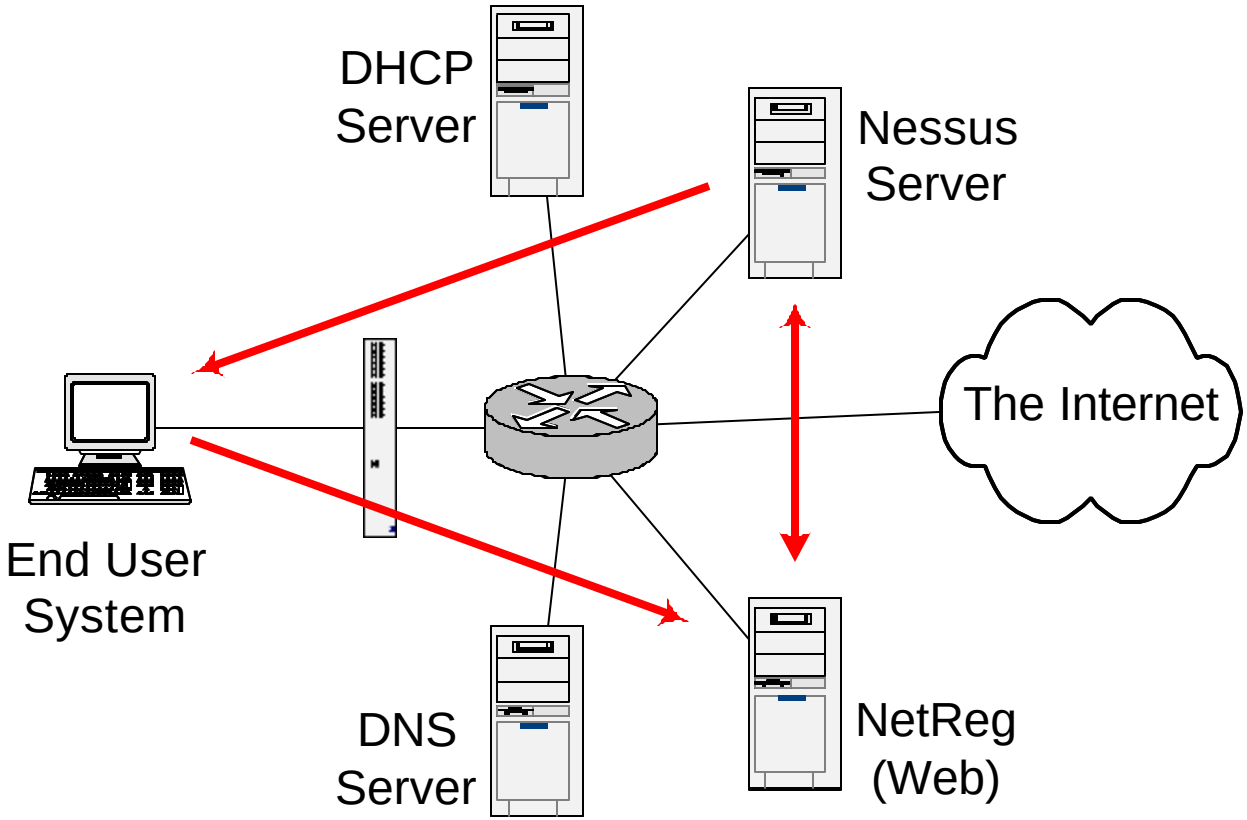


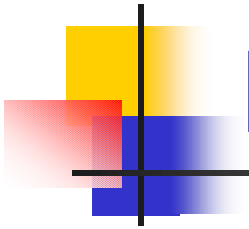


Big Brother is Watching

- Nessus: Scan host for a particular/set of vulnerabilities
- Client/Server version
  - Heavy “client” has list of scans to do
  - Server performs scans and returns result details
  - Client designed to run once for a range of hosts
  - Client has list of all scans to perform
- NASL
  - No Server needed
  - Single Scan / single return code / no details
- We scanned for MS03-026, then MS03-039

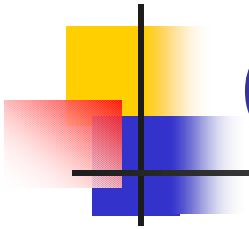
Nessus Scanning:





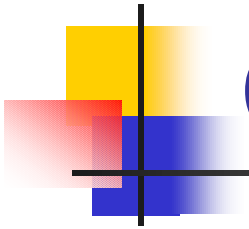
Fall Cleaning

- Single “help desk” tool (well 3 of them)
- Designed for NT/2000/XP/ME
- Wrapper written with SMS Installer
- Adds itself to the Run Once
- Verifies minimum Service Packs
  - NT: SP5 Win2k: SP2 WinXP: SP1
- Verifies certain Hotfixes
  - MS03-026 or MS03-039
- Load patches with wget



Check this, and this, and this...

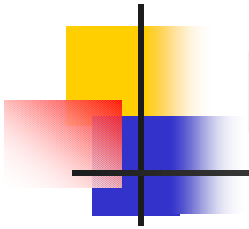
- Runs in the background with a notice window
- Stinger: NAI general cleaning tool (~20)
- FixWelch: Symantec Welchia Cleaner
- “result” email generated
- Windows Update/AV Setup Messages



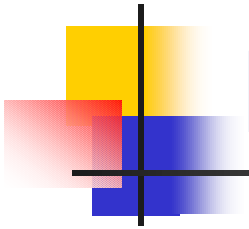
Oh, and Don’t Forget

- Its an iterative process
- We run Microsoft Vulnerability Scans
- Correlate Hosts with Nessus
- Quarantine Hosts when found
  - Working on automate un-quarantine

Oops - Issues and future plans Network Registration



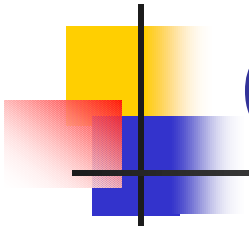
- Where's the web browser on my Xbox?
- Apache dDOS
  - Spyware & HTTP-like things
  - Can you handle the load
- Network Registration:
  - Bypass Monitoring
  - Automated Unquarantining



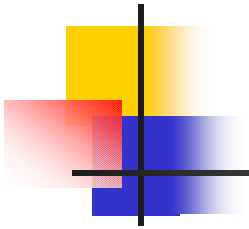
Oops - Issues and future plans Nessus

- Security model: failure goes to “open” state
- Nessus client vs. NASL: overhead vs. scan diversity
- IDS/Vulnerability scan integration feedback
- The one Linux oddball

Oops - Issues and future plans Cleaning

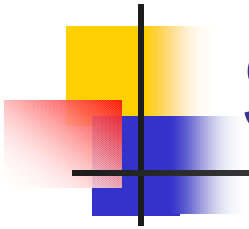


- SP1 Issues
  - Language detection
  - Illegal version keys
- Invasive ☺
- Doesn’t catch/clean everything



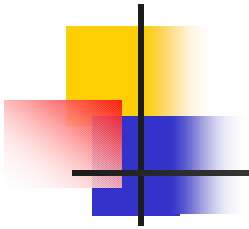
How Did We Do - Summary

- 90% Effective during Registration
- 90% Effective during Quarantine
- No one is ‘trapped’
- Reduced the cases to a “manageable” load
- Infection isn’t spreading! 10% getting through is a decreasing number over time, not an exponentially increasing one



Special Thanks

- Boston University's Security and Help Desk teams
- Southwestern University for NetReg
- Anyone who ever made a tool and released it for free to the world



Helpful URLs

- ISC DHCP/DNS servers: http://www.isc.org
- Apache: http://www.apache.org
- NetReg: http://www.netreg.org
- Nessus: http://www.nessus.org

- Eric's brief write-up and some configuration examples: http://www.roxanne.org/~eric/blaster.html

More Helpful URLs

- Stinger: http://vil.nai.com/vil/stinger
- Fixwelch: http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.removal.tool.html
- SMS Installer: http://www.microsoft.com/smserver/downloads/20/tools/installer.asp
- MS03-026/MS03-039 Scanner: http://support.microsoft.com/default.aspx?scid=kb;en-us;827363