MOPR:
Cleaning Up The Resnet With Next Generation Patch And Anti-Virus Enforcement

Nathan Hall (hallnk@oneonta.edu)
and
Justin St. Onge (stongejc@oneonta.edu)
SUNY Oneonta
SUNY Oneonta

- Member of the State University of New York system
- 5,800 Students
- 3,000 student computers on campus
- 4 /22 networks allocated to students
Existing Network Configuration

- Homegrown registration system similar to Netreg
- MAC addresses associated with a user
- Vlans are set dynamically based on registration status of MAC
- Unknown MACs are placed on an isolated vlan
The Problem

• Students do not patch
• Students fail to run current anti-virus
• Infections spread rapidly
• Infections are difficult to track down and time consuming to fix
• Just a few infected machines can cause network problems
Early Solution

• Similar to solution presented by Brown at Educause Security Conference 2004
  – Nessus security scanner
  – Net::Nessus::ScanLite Perl module
  – Scan before registration
  – Background scans
Early Solution (Cont.)

• Squid/SquidGuard allow access to Windows Update
• Snort to find infected machines
• Had some shortcomings
  – Few Windows vulnerabilities checked
  – Firewalled clients not checked
Ideal Solution

• Check for ALL patches
• Anti-virus checks (installed, running, updated)
• Work with any client
• Easy and quick for the user
• Minimize administrative work
• Ability to update easily when needed
Our Creation

- MOPR – Malware Outbreak Prevention for Resnet
- Web based
- Check for anti-virus and all Windows patches
MOPR Pieces

On the Client:
- Microsoft Baseline Security Analyzer (MBSA)
- .Net Framework/J#
- .Net security configuration
- Anti-Virus updater

On the Server:
- two XML configuration files
- MOPR .dll
Demo – Running the scanner

Try it online at http://autoregadmin.oneonta.edu/test.htm
Goals Met

- Easily updateable
  - .NET Framework on local machine checks for newer version of dll on server
- Very little maintenance
- Can be inserted into existing reg system
- Simple two step process
  - Step 1: Install prerequisites and configure security
  - Step 2: Run scanner
- Campus anti-virus package rolled into installer
Results: Windows Patches

- 50% of computers were missing patches
- 76% of computers automatically install updates
Results: Anti-Virus

- 23% of students had old AV
- 9% had NO AV

Of those needing AV updates:
- 35% chose to update their existing AV
- 65% chose to install Sophos

![Anti-Virus Use On Campus Pie Chart]

- Norton: 20%
- McAfee: 4%
- Sophos: 76%
Other Benefits

- “cleaner” network
- Reduced load on helpdesk and student support
- User education/participation
Problems Encountered

- Viruses
- Spyware
- Personal Firewalls
- AV Software Variety
Acknowledgments:

• Everyone at SUNY Oneonta
• Open Source Software Developers – especially for Perl, Nessus, Squid, SquidGuard, Snort, Linux and the NullSoft installer
• SUNY Oswego (Greg Fuller and Matt Tehonica) for AV Installer (http://www.oswego.edu/~gfuller)