Protecting University Networks Using Automated Scanning

Josh Richard
University of Minnesota Duluth

Nancy Magers
Brown University

Educause Security Professionals Workshop
Fairmont Hotel in Washington, D.C.
May 17, 2004

Copyright Josh Richard, Nancy Magers 2004. This work is the intellectual property of the authors. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.
Introduction

Format:

• 25 minutes UMD
• 25 minutes Brown
• 10 minutes Questions
University of Minnesota Duluth
ITSS

- Member of the University of Minnesota System

- ITSS is responsible for all phone, networking, and central systems for the campus community

- 10,000 Students

- 7,500 + Ethernet connections (2,750 Ethernet in residence halls)

- 29 /24 networks across 13 different broadcast domains allocated to residence halls
Crowd Control

- Maintaining a baseline patch level among a population of computers you do not control is difficult, if not impossible
- User notification of recent vulnerabilities costs time
- It would be nice to combine the notification and scanning into an automated process to reduce staff time
The Problem...

- A large percentage of users do not patch quickly
- IT Departments may not own user machines
- Internet == HOSTILE
- DHCP vs. Static addressing trade off
Solution Description

- Southwestern University's NetReg
- NetReg Extensions (scan code, auth, sql)
- Address shortcomings of current scanner
- Describe Brown University's implementation of NetReg
Southwestern University's NetReg

- Software which forces unknown DHCP clients to register their computer hardware before gaining full network access.
- Uses DHCP pools, Web registration server and bogus DNS
- Active development, helpful list

http://www.netreg.org
NetReg Scanner

- Perl CGI and C scanner which checks for DCOM vulnerabilities in Microsoft machines
- Redirects hosts based on scan results.
- Unix based scanner (dcom_scanz), modified by U of Minnesota Duluth, and UCONN to work with NetReg
Preemptive Scanning and NetReg
Current Setup

Good Network information

Known clients

Router forwards dhcp

Unknown clients

DHCP

Bogus Network information

Scan launched

DNS redirect

HTTP DNS dcom_scanz

Scan ok

Scan fail
Authentication and Accounting

- Terms and conditions on HTTPS page
- User agrees and authenticates to register computer
- SQL stores connection and user information
- Flag set to rewrite DHCP configuration
- Web based management interface on registration server
Scan Failures

- Machines which fail the scan test are directed to a patch page
- Router restrictions limit access
- LOCATION redirect from https server to patch server
- FACT: 42% of machines scanned September 2003 were not patched to MS03-026/039
Leverage SQL data to:

- Populate another databases with connection specific demographic info
- Trend registration count over time:
**dcoscanz**

**Pros**

- Very fast, low rate of false positives
- Open source

**Cons**

- Only checking for one problem
- You end up reinventing the wheel
- Unsupported code -> support non-existent

_A general scanning solution is needed_
Generalized Solution

- User agrees to terms and authenticates to register computer
- Nessusd scan is launched after authentication using Net::Nessus::ScanLite. SQL record is made if SCANOK
- SQL stores connection and user information
- Flag set to rewrite DHCP configuration is set
- Web based management interface on registration server
Reggie
A Host Vulnerability Detection and Access System

Nancy Magers
Manager Unix Systems
Nancy_Magers@brown.edu
Brown Resnet Environment

- 49 Class C subnets dedicated to the student’s residential facilities
- 6000 registered hosts
- Netreg and Nessus
- CPAN - Net::Nessus::ScanLite
Dependencies

• Web Environment

• Patch Library

• Scan Plugins Prioritization

• Process Management

• Documentation and Training

• TESTING _ TESTING _ TESTING
Implemented Vulnerability Scans

- 11808 – Microsoft RPC Interface Buffer Overrun
- 11835 – Microsoft RPC Interface Buffer Overrun
- 12029 – MyDoom Virus Backdoor
- 12055 – ASN.1 Parsing Vulnerabilities (HTTP)
- 12054 – ASN.1 Parsing Vulnerabilities (NTLM Check)
- 12209 – LSASS MS04-011 Microsoft Security Patch
Welcome to myConnection!

Please log in

Please enter your Brown NetID or AuthID and password, received when you activated your electronic services. If you have not activated your account, use the link at the left to do so, then return to the registration process.

Username: imagers
Password: ********

Processing... Please wait.

If you have not yet activated your Brown account, please do so before registering your computer on the network.

Please wait.
Alert: Your machine has been found to be vulnerable and you must update your machine before you can register on Brown’s network.

Your machine has 1 vulnerability. More information is listed below.

Your machine is vulnerable to an ASN.1 Parsing vulnerability (NTLM check). You can secure your machine by following the steps outlines on this web page: [http://software.brown.edu/safe/win/](http://software.brown.edu/safe/win/).

NOTE: Once you access these pages, please complete the process. IF YOU ARE NOT READY TO REGISTER, PLEASE EXIT NOW.
Make Windows Network Safe

Your computer has been found to have security vulnerabilities requiring you to update software on your computer. This page provides access to the updates, patches, and security software to help make your computer more secure. Follow the steps below to make your computer more secure:

1. Update and Patch Windows

Patch DCOM/RPC vulnerability (RPC1/RPC2)
You must patch your computer to close a Remote Procedure Call (RPC) exploit (details). You may need to install Windows service packs prior to installing this patch (see below). Download DCOM/RPC patch

Patch ASN.1 Vulnerability
You must patch your computer to close an ASN.1 library vulnerability (details). You may need to install Windows service packs prior to installing this patch (see below). Download ASN.1 Patch.

Install latest Service Packs
The latest Windows service pack may be required prior to installing other security updates.
- Download Windows 2000 SP 4
- Download Windows XP SP 1a

2. Update Internet Explorer

Install Internet Explorer 6 with Service Pack 1
Internet Explorer 6 with Service Pack 1 is the most secure version of IE - if you have an older version please upgrade.
Download Internet Explorer 6 with Service Pack 1

Patch Internet Explorer with latest security updates (details)
Patch Internet Explorer 6 with any critical updates released since Service Pack 1. (Last update 2004.02.03)
Download Internet Explorer critical updates

3. Virus removal and scanning

Remove MyDoom/Novarg virus/worm
If you are infected with the MyDoom/Novarg virus/worm download and run the Symantec cleanup tool FxMyDoom (instructions).
Download FxMyDoom

Scan for viruses, trojans, and worms
Download and run Stinger from McAfee to detect and clean common viruses, worms, and trojans (details).
Download Stinger

Install Symantec AntiVirus
Download and install Symantec AntiVirus to scan and protect against viruses, worms, and trojans. After installation, run the Symantec AntiVirus LiveUpdate feature daily to maintain a set of the most recent virus definitions.
Important! You must uninstall all other anti-virus products, from Symantec or other sources, prior to installing this version of Symantec AntiVirus.
Download Symantec AntiVirus

Restore Windows HOSTS file
Download and run Restore Windows Hosts File Tool to restore the Windows HOSTS file back to its original state.
Download Restore Windows HOSTS file tool

4. Additional Security

...
Reggie's Mission

- Enforce compliance network acceptable use policy in regards to host security vulnerabilities
  - Fully automated system
  - Deliver consistent message
  - Only address vulnerable hosts
  - Teach the user first
  - Enforce second
Phase 1 – Scan

- Daemon process
- 3 hours to cycle
- Processes sequentially
- Subnet.dat
- Adds systems with vulnerabilities (holes)
- Clearing systems that have been fixed
Phase 2 – Identify

- Periodically run out of Cron – 15 Minutes
- Identifies host owner
  - dhcp.leases
  - dhcp.conf
  - LDAP Lookup
Phase 3 – Rescan

- Periodically run out of Cron – 15 Minutes
- Checks Identified Hosts For Vulnerability
Phase 4 – Notification

- Periodically run out of Cron – 15 Minutes
- Emails owner of vulnerable host
- Provides specific instructions how to fix the issue
- Updates database and marks hole as notified
ASN.1 Vulnerability Email:

Dear Test Student08:

A scan of the Brown University network on Tuesday, February 24, 2004 found that your machine (MAC address: 00:B0:D0:CF:B1:6B) is vulnerable to attack.

We have found the following vulnerabilities on your computer:

---

Your machine is vulnerable to an ASN.1 Parsing vulnerability (NTLM check). You can secure your machine by following the steps outlines on this web page: http://software.brown.edu/safe/win/.

---

Failure to patch your machine as directed by IT Security is in violation of Section 3.4 of the Network Connection Policy (http://www.brown.edu/cis/policy/network.html) which reads: "Computer owners must install the most recent security patches on the system as soon as practical or as directed by IT Security." This section also requires that you be running anti-virus software and keep it up-to-date. You agreed to abide by this policy when you registered your computer with myConnection.

Should your machine still be vulnerable in 24 hours, CIS will un-register your connection.
Phase 5 – Purge

- Periodically run out of Cron – 15 Minutes
- 24 Hours
- Rescans one more time...
- Removes host from DB and dhcpd.conf
- Requires reregistration
Database View
Reggie Statistics

From February 12 – April 30
• 5861 Vulnerabilities Found
• 5472 Vulnerabilities Fixed Without Interruption of Network Services
• 389 Hosts Lost Network Services and Required ReRegistration
• 12 Hosts may have required help from the help desk
Psychology of Patching

We are training our users to want do the right thing by informing them of their shortcoming and allowing them to fix them before we enforce our policies.

Source code available upon request – EMAIL Nancy_Magers@brown.edu
Thank You

• Attendees
• Educause, Internet2
• Southwestern University, NetReg list

• The Open Source Universe:
  - Apache Foundation
  - ISC (DHCPD, BIND)
  - Perl Community
  - Nessus
  - MySQL
  - Orca / RRD

Questions?