MIG’s Approach to Security Management

Marc DeBonis
Senior Systems Architect
MIG - Virginia Tech
Nov 12th, 2003
Central IT is focused on administrative systems
- ED / AD
- SCT Banner
- Websites, university portal, etc.

Departments may or may not have local IT staff
- Engineering has many IT staff
- Fine Arts has none

Need to secure our own systems first!
Disables users’ ability to add workstations to domain
Remove event log access from authenticated users
Modify user account settings
- 10 bad attempts in 30 minutes locks for 30 minutes
- Unlock accounts automatically after 30 minutes
Allow NTLMv2 if negotiated
Require swift installation of SPs and required hotfixes by root and child domains
Disable unnecessary services running on DCs
AD security, part 2

- **EOL**: end of life document
  - **Step 1**: Increase Restrict Anonymous setting to level 2
    - Breaks existing NT 4 trust relationships
    - Stops hackers from enumerating and locking out user accounts
  - **Step 2**: End LM authentication, remove hashes
    - Breaks Windows 9x systems (unless DS client is installed)
    - Breaks Mac Outlook 2001
    - LM auth is weak, #3 in SANS Top 10 Windows list
Tripwire/ Tripinator

- Full and intensive tripwiring of all production systems
  - EXTREMELY time intensive to set up
  - Developed in-house tools to mitigate
    - Tripinator demo
    - [http://tripinator.w2k.vt.edu](http://tripinator.w2k.vt.edu)
  - Provides great insight into daily system operations and how registry/SAM/drivers interoperate

- Beware SPs, hotfixes, and IPsec policy pushes
Event Log/ Synopsis

- Monitor success/fail of nearly all event sources on all production systems
  - EXTREMELY time intensive to set up
  - Developed in-house tools to mitigate
    - Synopsis
  - Very valuable early warning system
  - “Ounce of prevention is worth a pound of cure”
  - ~ 200 actions per system
Account Monitoring

- Eventsucker application retrieves security events from all DCs every 15 minutes, collates them.
  - Does calculations based on number and type of event failures.
  - Emails administrators on machine name, account name, number and type of events, and if account is/was locked out.
  - Allows quick response to worms/ trojans/ hackers who are targeting our systems, probing for accounts.

- When/ if IP is discovered for intruders we:
  - Contact abuse@isp with nastygram.
  - Use IPsec to block entire address range until we hear from the ISP.
Eventsucker Example

- **WARNING**: Potential attack occurring on fud

  ---------------
  ATTACK INFO
  ---------------
  Attack noticed at: 2003:11:07:02:45:02
  Workstation doing the Attacking: PC-5
  Total Number of Occurrences of Events 529 & 681 caused by PC-5 : 72
  Since Time: 20031107011017
  ---User Accounts Guessed---
  guest -> Bad User Account
  admin  -> Bad User Account
  administrator -> Bad User Account

  Machine: fud
  529 Occurrences: 36
  681 Occurrences: 36
Passwords

Requirements
- Minimum 8 characters, 127 max
- Password complexity on
- Dictionary checks if changed through HSS

Strength checking
- Monthly dump of hashes via pwdump3
- Run against dictionary checks via L0phtCrack v4

Averages 5-6% weak passwords

Still have accounts grandfathered in from NT 4 migration

MS password complexity rules still allow weak passwords (considering writing own pwd filter)
Hotfix Patching

- **Daisy**: in-house tool
  - Wrapper around Shavlik’s free hfnetchk, MS’s qfecheck and MS’s qchain
  - Run interactively or via scheduled task
  - Can identify, download, install, and reboot systems
  - Must manually update FTP site where hotfixes reside
  - Some hotfixes don’t script well (Java, Office, etc.)
  - Doesn’t do service packs

- 1,300+ downloads of current version (2.1)
- [http://opensource.w2k.vt.edu](http://opensource.w2k.vt.edu)
Port Management

- Portinator: in-house tool, a tripwire for network ports
  - Wrapper around Foundstone’s fport
  - Builds a baseline around a system’s network footprint
  - If new exes open listening ports, an email is sent to the admin
  - Does md5 checksum of application, verifies file path, and what port(s) are opened

- Difficult to nail down the SYSTEM thread
- Currently in open beta
- http://opensource.w2k.vt.edu
University Services, SFM

- SFM runs in-house app **Sunflower** once/week
  - Wrapper around hfnetchk in network mode
  - Emails the owner of the machine, informs them of missing hotfixes
  - Requires administrative rights to workstation (often unwittingly removed)
  - Many users have misconfigured firewalls
    - Hampers Sunflower
    - Hfnetchk has many dependencies when run in network scanning mode
University Services, MFM

- Next facilities management OU will push
  - Basic IPsec for firewall-ish features
  - Comprehensive security GPO (reviewed by auditors)
  - Hotfixes through Ivy, a server-side version of Daisy
  - Service packs through MSI

- Issues
  - GPOs are difficult to master, easy to break things
  - Difficult to tell users how settings apply
  - Difficult to back out if GPOs interfere locally
  - Did you know XP required DFS service? Neither did we...
Proactive Scanning

- During MSblaster outbreak used E eye tool to proactively scan all VT IP ranges
  - Posted results to a technical support listserv
  - Proved motivational, except for delayed political repercussions
- Began weekly scans
  - RPC/DCOM vulnerable systems
  - Systems that might be trojaned (ports 69, 707, 4444)
  - Systems with Messenger vulnerabilities
  - Results sent to network liaisons responsible for machines’ DNS zones (if nslookup resolved system)
- Issues
  - Some NLs are secretaries - probably threw reports away
  - Some NLs had no power over faculty with bad systems
  - Some admins became upset, threatened to go to legal
## Proactive Scanning Statistics

**Of 15,000 pingable systems**

<table>
<thead>
<tr>
<th>Date</th>
<th>Systems</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/ 30</td>
<td>2000+</td>
<td>RPC/DCOM</td>
</tr>
<tr>
<td>8/ 14</td>
<td>105</td>
<td>RPC/DCOM</td>
</tr>
<tr>
<td>8/ 18</td>
<td>77, 81</td>
<td>RPC/DCOM trojaned</td>
</tr>
<tr>
<td>8/ 25</td>
<td>126, 347</td>
<td>RPC/DCOM trojaned</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/\ Students returned /\</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9/ 2</td>
<td>110, 179</td>
<td>RPC/DCOM trojaned</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
<th>Systems</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/ 8</td>
<td>77, 164</td>
<td>RPC/DCOM trojaned</td>
</tr>
<tr>
<td>9/ 15</td>
<td>1747</td>
<td>RPC/DCOM #2</td>
</tr>
<tr>
<td>9/ 22</td>
<td>916</td>
<td>RPC/DCOM #2</td>
</tr>
<tr>
<td>9/ 29</td>
<td>(no scanning)</td>
<td></td>
</tr>
<tr>
<td>10/ 6</td>
<td>(no scanning)</td>
<td></td>
</tr>
<tr>
<td>10/ 13</td>
<td>670</td>
<td>RPC/DCOM #2</td>
</tr>
<tr>
<td>10/ 20</td>
<td>753</td>
<td>RPC/DCOM #2</td>
</tr>
</tbody>
</table>
PFWs

- Developed a policy push for end users
  - Activate XP firewall
  - Gave away ZoneLabs ZA or Black Ice Defender
  - Use derived IPsec policies as basic firewall
- People became complacent
  - If they brought the FW down, they got MSblaster-ed
  - Made it difficult to diagnosis if they DID have a problem
  - Doesn’t stop trojan/ macro attacks
  - A unpatched system was compromised in an average of 10 minutes on VT network
Antivirus

- Site license for Norton AntiVirus
  - Some IT departments use the centralized management system to manage the clients
  - Most do not and don’t have a handle on the problem
- Many clients have
  - Disabled antivirus (“it makes the system slow…”)
  - Out of date definitions
- Layered security with spam and antivirus filters on POP/SMTP and Exchange mail systems
VPN / IPsec

- CNS developed a VPN solution tied with modem pool
  - Haven’t decided on cost recovery mechanism
  - Won’t go production until cost recovery is in place
  - Would love to IPsec AD DC’s to only allow VT IP traffic - can’t if VPN solution costs users $$$
  - Must service laptop users from many locations
  - Difficult to implement behind a NAT

- MS IPsec MMC
  - Difficult to use
  - Batch scripts and IPsecpol easier to implement
  - Netsh?
Security in the Future

- **SafetyNet**
  - A web-based application that allows NL’s (authorized users) to scan their IP ranges and securely receive reports
  - Considering closed and open source

- **Neighborhood Watch**
  - Passive IDS detects compromised systems and alert appropriate parties
  - Possibly push IPsec to block suspect systems

- **Synopsis v2.0**
  - No client
  - Use WMI to develop real-time syslog type solution
  - Rewrite of web application for better response over slow links
MIG’s Approach to Security Management

Marc DeBonis
Senior Systems Architect
MIG - Virginia Tech
Nov 12th, 2003