Windows security at UiO
The situation before 2002

• daily script for *NIX; fundamental security checks

• sporadic scans

• Decentralized responsibility – local IT departments were partly responsible for maintaining and installing programs
Learning the hard way

• From V02: increasing activity against Windows 2000 (e.g. p 445)
• November 2002: The hidden SQL-server
  – 50,000 passwords
  – The control of applications not good enough
• 2003:
  – Slammer, Blaster, Welchia, SoBig
    • Summer vacation, 25-40% before lunch
• Labrea tarpit & endless access lists, and our young tools: scanorama and daily
• Useful: Get them early, before possible infection. We cannot impose operating system, but we can impose a certain level of security.
Tools at UiO

Elisabeth Høidal Strøm
elisabhs@usit.uio.no
Usit/SAS/OS
Windows system administrator
and security technician
Daily and Scanorama

- Daily – Reporting script running on every Windows client at UiO
- Scanorama – Portscanning and bannergrabbing system
Daily - purpose

• Control
  – Control of the machines in our AD domain
  – Ease maintenance for us and local IT (registered DNS name, machines not member of domain, )

• Security
  – Catch hacking/worm/incidents, register attacks and find other machines with corresponding behavior
  – Patch status
Daily

- machines report from the inside

• Perl script runs every night between 00:00 and 06:00.
• Distributed, machines report their status from ”the inside”.
• Runs on every machine in the AD Domain
• Gets installed when a machine reboots (GPO)
• Log and report useful information from the machines
Daily
- how it works

- Main script runs several other small scripts that collects information from the machine
- Result is stored locally
- Result is copied to central server
- Files get over written every time daily runs
- Report script parses the log files and generates various reports for pcadm (centralized IT) and local IT.
Daily
- what’s being logged

• OS information (version, type, language, sp, patches)
• Patch status (mbsa)
• Anti-virus status
• IP configuration
• HW information (Disk, mem, cpu usage)
• Shares
• Open ports (netstat, fport)
• Services (started/installled)
• Processes
Daily
- what’s being logged

- Members of administrators group
- Information and members of guest group and guest account
- Profiles – who has been logged in
- How it was installed
- Local authentications
- Failure attempts for administrator log ins
- Search for suspicious files (we maintain a list)
- Misc registry keys (winlogon, run, runonce, startup)
Daily
- the report

• Config file
  – OU’s and corresponding email addresses for responsible local IT
  – List of which information to send

• Enquires AD for list of all computes
• Reads the daily logs files from our log server
• Generates report
• Sends the report with email to responsible person(s)
• Stores all reports centrally
- report example

- Machines with suspicious files

NASTY (129.240.255.666) has these suspicious files:

- sfind.exe: Found in (c:/tools/)
- sfind.exe: Found in (c:/recycler/S-1-5-21-4146745624-1268266741-2650905777-1030/COM1/a/)  
- svchost.exe: Found in specified dir (c:/winnt/system32/wins)
Daily - report example

#################################################################
Machines missing important patches
#################################################################
UBHSPCXXX:
  WINDOWS SERVER 2003 STANDARD EDITION GOLD: Q902400
VLAB-XXX:
  WINDOWS 2000 SERVER SP4: Q902400
USITPCXXX:
  INTERNET EXPLORER 6 SP1: Q896688

#################################################################
Machines missing CRITICAL patches
#################################################################
BIRKELANDPCXX () is missing Q925902 Q930178
FRISCHXX (129.240.xxx.xxx) is missing Q925902 Q930178
HF-XXX-XXX (129.240.xxx.xxx) is missing Q925902
Daily challenges

- Dependent on AD to run daily
- Extremely UiO-specific 😞
- Laptops, home computers/VPN, wireless access, and computers outside the AD domain
- Developing daily2 at the moment
  - Run as a service/agent
  - Can be offered to other sites
  - Run a beta version at USIT and some test environments
Daily

- mail report example

C:\dailymail\webmail.php.htm
Scanorama

- Developed at USIT
- Can be found at http://sourceforge.net/projects/scanorama/
- A portscanning and bannergrabbing system
- Reports how the machines look from “the outside”
Scanorama

- background

- Wish to look for vulnerable services or indications of compromised machines
- Normal port scanning for known back doors might give false positives for non-relevant machines
- Often interesting to find combinations of parameters (certain open ports, open ports/OS)
- Correlation of data makes it possible to find interesting results without “drowning” in non-relevant information
Scanorama
-the system

- Dell server PE2650
- Runs Linux RHEL
- Data is stored in a postgresQL database.
- Scripts are mainly written in perl (some bash-scripts)
Scanorama
- the system

• The scanner –nmap performs the portscanning stores the results in XML
  – Ping scan: To register machines in DB
  – Light scan: For known TCP/UDP ports/services/backdoors/etc
  – Full Scan: port 1-65535 TCP/UDP (very slow)
  – OS scan: Guessing the OS of the machine

• Banner grabbing
  – Opens a socket and connects to the service ports to figure out what’s behind

• All results are stored in the database
Scanorama

-usage

- Find computers answering to suspicious ports
- Find computers not in AD
- Find computers that run unauthorized server services (IIS, MSSQL, non-standard samba, etc)
- Find computers that run old version of programs (Apache, ssh, etc)
- Find computers with a specific OS
- Much more
Scanorama
- possible extensions

• Better web interface for reports
• Possibility to generate and store reports in the web interface
• Automatic mail reports for IT personnel
• Snapshot when a computer is first seen, and alerts when this changes
• History and baseline checking
# Misc all OS views in Scanorama

<table>
<thead>
<tr>
<th>Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>FileMaker Web-server</td>
<td>Machines running FileMaker Webserver</td>
</tr>
<tr>
<td>Last boot</td>
<td>Shows &quot;last boot&quot; from machines showing this</td>
</tr>
<tr>
<td>MacOS (7,8,9)</td>
<td>Machines running old version MacOS (7,8 or 9)</td>
</tr>
<tr>
<td>MySQL</td>
<td>Machines running MySQL</td>
</tr>
<tr>
<td>NONstandard Samba</td>
<td>Machines running samba not provided by USIT</td>
</tr>
<tr>
<td>NetBIOS OS-stats U1O</td>
<td>Summary of NetBIOS-server types in U1O domain</td>
</tr>
<tr>
<td>NODES</td>
<td>Machines not registered in DNS</td>
</tr>
<tr>
<td>OS: AIX</td>
<td>Machines running AIX</td>
</tr>
<tr>
<td>OS: HP-UX</td>
<td>Machines running HP-UX</td>
</tr>
<tr>
<td>OS: IRIX</td>
<td>Machines running IRIX</td>
</tr>
<tr>
<td>OS: Linux</td>
<td>Machines running Linux</td>
</tr>
<tr>
<td>OS: Mac OS</td>
<td>Machines running Mac OS</td>
</tr>
<tr>
<td>OS: Solaris</td>
<td>Machines running Solaris</td>
</tr>
<tr>
<td>OS: True64</td>
<td>Machines running True64</td>
</tr>
<tr>
<td>OS: Win9X</td>
<td>Machines running Windows 95/98/ME</td>
</tr>
<tr>
<td>OS: WinNT</td>
<td>Machines running Windows NT4.0</td>
</tr>
<tr>
<td>OS: Windows</td>
<td>Machines running Windows</td>
</tr>
<tr>
<td>dns-servers</td>
<td>Machines running BIND nameserver</td>
</tr>
<tr>
<td>ftp-servers</td>
<td>Machines running ftp-server on port 21</td>
</tr>
<tr>
<td>imap-servers</td>
<td>Machines running imap-server on port 143</td>
</tr>
<tr>
<td>mysql-servers</td>
<td>Machines running Microsoft SQL Server</td>
</tr>
<tr>
<td>pop-servers</td>
<td>Machines running pop-server on port 110</td>
</tr>
<tr>
<td>printers</td>
<td>Lists all networkprinters</td>
</tr>
<tr>
<td>samba-servers</td>
<td>Machines running samba</td>
</tr>
<tr>
<td>sendmail</td>
<td>Machines running Sendmail SMTP-server</td>
</tr>
<tr>
<td>smtp-servers</td>
<td>Machines running smtp-server on port 25</td>
</tr>
<tr>
<td>ssh</td>
<td>Machines running SSH servers</td>
</tr>
<tr>
<td>web-servers</td>
<td>Machines running web-server on port 80</td>
</tr>
<tr>
<td>Host</td>
<td>IP Address</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------</td>
</tr>
<tr>
<td>silo.uio.no</td>
<td>129.240.5.35</td>
</tr>
<tr>
<td>rix010.uio.no</td>
<td>129.240.8.229</td>
</tr>
<tr>
<td>miho.uio.no</td>
<td>129.240.11.101</td>
</tr>
<tr>
<td>marv.uio.no</td>
<td>129.240.11.103</td>
</tr>
<tr>
<td>kronos.uio.no</td>
<td>129.240.11.196</td>
</tr>
<tr>
<td>dad.uio.no</td>
<td>129.240.11.204</td>
</tr>
<tr>
<td>finn.uio.no</td>
<td>129.240.11.214</td>
</tr>
<tr>
<td>mist.uio.no</td>
<td>129.240.11.221</td>
</tr>
<tr>
<td>fm7server.uio.no</td>
<td>129.240.11.222</td>
</tr>
<tr>
<td>winblade1.uio.no</td>
<td>129.240.11.224</td>
</tr>
<tr>
<td>megaloserver.uio.no</td>
<td>129.240.11.227</td>
</tr>
<tr>
<td>partnersentral.uio.no</td>
<td>129.240.11.230</td>
</tr>
<tr>
<td>valhall.uio.no</td>
<td>129.240.12.15</td>
</tr>
<tr>
<td>helheim.uio.no</td>
<td>129.240.12.23</td>
</tr>
<tr>
<td>hinsidge.uio.no</td>
<td>129.240.12.27</td>
</tr>
<tr>
<td>webdav-test2.uio.no</td>
<td>129.240.12.38</td>
</tr>
<tr>
<td>webdav-test.uio.no</td>
<td>129.240.12.62</td>
</tr>
<tr>
<td>trofast-css.trofast.uio.no</td>
<td>129.240.13.5</td>
</tr>
<tr>
<td></td>
<td>129.240.13.6</td>
</tr>
<tr>
<td>ephortetest.uninett.no</td>
<td>129.240.13.7</td>
</tr>
<tr>
<td>fotsopp.trofast.uio.no</td>
<td>129.240.13.64</td>
</tr>
<tr>
<td>isop.trofast.uio.no</td>
<td>129.240.13.98</td>
</tr>
<tr>
<td>lastinn.trofast.uio.no</td>
<td>129.240.13.115</td>
</tr>
</tbody>
</table>