



UNIVERSITY
OF OSLO

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 collect information from the machine
- Result is stored locally
- Result is copied to central server
- Files get overwritten every time daily runs
- Report script parses the log files and generates various reports for pcam (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/installed)
- 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



Daily

- 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 postgresSQL 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 personell
- Snapshot when a computer is first seen, and alerts when this changes
- History and baseline checking

Scanorama screenshot



Misc all OS views in Scanorama

[/]

Name	Comment
FileMaker Web-server	Machines running FileMaker Webserver
Last boot	Shows "last boot" from machines showing this
MacOS (7,8,9)	Machines running old version MacOS (7,8 or 9)
MySQL	Machines running MySQL
NONstandard Samba	Machines running samba not provided by USIT
NetBIOS OS-stats UIO	Summary of NetBIOS-server types in UIO domain
NoDNS	Machines not registered in DNS
OS: AIX	Machines running AIX
OS: HP-UX	Machines running HP-UX
OS: IRIX	Machines running IRIX
OS: Linux	Machines running Linux
OS: Mac OS	Machines running Mac OS
OS: Solaris	Machines running Solaris
OS: Tru64	Machines running Tru64
OS: Win9X	Machines running Windows 95/98/ME
OS: WinNT	Machines running Windows NT4.0
OS: Windows	Machines running Windows
OS: Windows 2003	Machines running Windows 2003
dns-servers	Machines running BIND nameserver
ftp-servers	Machines running ftp-server on port 21
imap-servers	Machines running imap-server on port 143
mssql-servers	Machines running Microsoft SQL Server
pop-servers	Machines running pop-server on port 110
printers	Lists all networkprinters
samba-servers	Machines running samba
sendmail	Machines running Sendmail SMTP-server
smtp-servers	Machines running smtp-server on port 25
ssh	Machines running SSH servers
web-servers	Machines running web-server on port 80



Scanorama screenshot

L J

windows_http (65)		
silu.uio.no	129.240.5.35	Microsoft-IIS/6.0
rix010.uio.no	129.240.8.229	Apache/2.0.54 (Win32)
miho.uio.no	129.240.11.101	Microsoft-IIS/6.0
marv.uio.no	129.240.11.103	Microsoft-IIS/6.0
kronos.uio.no	129.240.11.198	Microsoft-IIS/6.0
dad.uio.no	129.240.11.204	Microsoft-IIS/6.0
finn.uio.no	129.240.11.214	Microsoft-IIS/6.0
mist.uio.no	129.240.11.221	Microsoft-IIS/6.0
fm7server.uio.no	129.240.11.222	Microsoft-IIS/6.0
winblade1.uio.no	129.240.11.224	Microsoft-IIS/6.0
megaloserver.uio.no	129.240.11.227	Microsoft-IIS/6.0
gartnersentral.uio.no	129.240.11.230	Microsoft-IIS/6.0
valhall.uio.no	129.240.12.16	Microsoft-IIS/6.0
helheim.uio.no	129.240.12.23	Microsoft-IIS/6.0
hinsidige.uio.no	129.240.12.27	Microsoft-IIS/6.0
webdav-test2.uio.no	129.240.12.58	Apache/2.2.4 (Win32) DAV/2
webdav-test.uio.no	129.240.12.62	Microsoft-IIS/6.0
trofast-css.trofast.uio.no	129.240.13.5	Microsoft-IIS/6.0
	129.240.13.6	Microsoft-IIS/6.0
ephortetest.uninett.no	129.240.13.7	Microsoft-IIS/6.0
fotsopp.trofast.uio.no	129.240.13.64	Microsoft-IIS/6.0
isop.trofast.uio.no	129.240.13.98	Microsoft-IIS/6.0
	129.240.13.115	Microsoft-IIS/6.0