Global Information Assurance Certification Paper

Who forgot to lock the back door?

Peter Landers, GSEC Version 1.2c

Whilst there is a high level of security provided to the Organisation through the Internet gateway and internally there is a gaping hole – the back door – users who connect to the Organisation by use of Dial-up connections and at the same time connecting to other networks and/or the Internet!

- A staff member recently bragged that it was faster to get downloads from their home machine's cable connection and then transfer the results "inside" ***– this was being done completely without firewall or virus protection OR the Organisation's knowledge*** !!!

Quote: "Any time a remote user accesses your network, it poses a security risk, yet many companies do no more than install password protection and cross their fingers" [1]

- The Organisation is severely cash-strapped!!

- The Organisation supports the Government Health Departments and holds data that is highly sensitive from a client perspective as well as commercially sensitive research material and as with any organisation, company or individual – very private information.

The purpose of the exercise was to provide documentary evidence of the danger of home workers connecting to the Internet and the Organisation's network at the same time.

- The Organisation is planning to roll-out Windows2000 to a large number of client workstations, some of which are laptops and workstations which are used either on the road or at home accessing the Organisation's network by dial-up. In addition some of the workstations will be in "hostile" surroundings - they will be placed in other Organisations' environments but forbidden connection to networks other than the host Organisation's

- The Security Policy of the Organisation explicitly forbids concurrent connections WAN/LAN of the Organisation and to the Internet and/or other networks.

- All remote connections (either VPN or dial-up) are brought through the Organisation's firewall. Dial-up is to be phased out, but the current forecasts of expenditure do not take account of the additional bandwidth required on the Internet gateway to permit this in the [relative] short term.

  The host Organisation exclusively employs non-routable addresses, i.e, 10.n.n.n. Any traffic not bound for a "10" address is directed to the Organisation's default gateway.

Whilst the use of non-routable address is of some comfort it does not protect against a client being taken over by Trojan which could then simply "plunder" the network and forward information to the Internet without detection.

Whilst security has been given a "nod" in the past it has become abundantly clear that the current arrangements of the Organisation do not properly address the issues that face it.

- It is not only the Organisation and the information held by it that must be protected but also the legal liabilities of the staff's of the organisation.

The following has been undertaken to alert and document the Organisation to the risks it faces from this one gaping hole in the current infrastructure.

Prove that the vulnerability exists:

- The W2K client is set up with an "out of the box" configuration and SP1 applied.
- The baseline integrity of the client's file system was established by running LANguard (LG) and the results are transferred to removable media.
- The client is attached to the Internet and all traffic is permitted to "do its thing" on the client for a period of two days.
- NukeNabber (NN).
  NN is run to passively monitor the client for connections to "well known" Trojan ports.
- The client is disconnected from the Internet and LG is again run to observe any changes to the file system.
- The client has ZoneAlarm Pro (ZA) installed.
- The client is attached to the Internet:
  WinDump is run continuously to capture traffic to and from the client machine.
- ZA is run with minimal settings to gather information.
- LG is run to check the integrity of the files after the test period (two days).

Detect the forbidden connection:

Discover if the host network is at potential risk through the use of non-sanctioned connections to the internet by the use of ASDL, DSL, ISDN, POTS, etc ("always-on") or (additional) dial-up connections.

Quote: " . . . most companies are well protected by their Internet firewalls; inevitably, however they all have trivially navigated dial-up holes that lead right to the heart of their IT infrastructure" [2] "One of the most damaging threats can be a network security breach caused by dial-up modems, email, floppy disks, sophisticated viruses, vandals (malicious mobile code), denial-of-service attacks, or the insecure transmission of data over Internet connections. These breaches can result in loss of data, legal liability or systems failure" [3]

- When the client logs onto the Organisation's network the user's login script is run – it checks for the presence of a pre-compiled application which has been written in house. The application goes directly to the IP stack via the helper dll using "netstat type commands" ("RasAPI32.dll" Alias "RasEnumConnectionsA", extracts the OS, version and other information, the application sends information "back to base" every thirty seconds using "kernel32.dll" (ByVal dwMilliseconds As Long" and hangs up using " Alias "RasHangUpA" (ByVal hRasConnection As Long"

  (Source code available if required)

- If an "illegal" network is detected the connection is dropped immediately with an explanatory message to the client machine. See **Don't simply deny connections, offer a resolution** (below).

  ✓ Although it is possible to use Microsoft's SMS or other proprietary packages to look for interfaces and activity on them, many cash-strapped Organisations and small businesses cannot always afford it. This is certainly true in the current financial/political environment the Organisation is being run.

The Nuts and Bolts

ZoneAlarm Pro

(http://www.zonelabs.com)

Zone Alarm was used on the test client to observe unsolicited inbound traffic.

LANguard.

(http://www.languard.com)

LANguard was used to provide a baseline of the test client. Following unprotected

exposure to the Internet it was run again to observe any changed to the file system of the client.

WinDump:

(http://www.netgroup-serv.polito.it/windump)
When the host was connected to the Internet in an unprotected (no firewall) mode, WinDump was used to capture the traffic generated from the Internet.

NukeNabber

Obtained from http://www.zdnet.com/downloads/
Nukenabber was passively run in the "attack me" stage of the trial.

What was seen at each stage of the trials:

Zone Alarm:

It was "disappointing" to not see any untoward activity, in either paranoid, medium or low security levels. The only activity seen was thought to be legitimate. Although unsolicited messages were responded to the Mail client did not detect any "forbidden" attachment types in the messages received.

LANguard:

LANguard was run before the test applications were installed and performed well reporting the addition of applications and documents.

Of particular interest was the changes to security logs and SAM :

C:\WINNT\system32\config\SAM has changed !
File name : C:\WINNT\system32\config\SAM
Size before change : 20480 bytes
Size after change : 20480 bytes
Size difference : 0 bytes
C:\WINNT\system32\config\SAM.LOG has changed !
File name : C:\WINNT\system32\config\SAM.LOG
Size before change : 1024 bytes
Size after change : 1024 bytes
Size difference : 0 bytes
C:\WINNT\system32\config\SECURITY has changed !
File name : C:\WINNT\system32\config\SECURITY
Size before change : 24576 bytes
Size after change : 24576 bytes
Size difference : 0 bytes
C:\WINNT\system32\config\SECURITY.LOG has changed !
File name : C:\WINNT\system32\config\SECURITY.LOG
Size before change : 1024 bytes
Size after change : 1024 bytes
Size difference : 0 bytes

The files changed at approximately 03:00 during the test period.

WinDump:

This application too performed well, but like ZA (above) did not appear to report any anomalous behaviour – all addresses sending were checked out and in the absence of any well-known Trojan ports and other ports reported as being "signatures" in the SANS course material were not found.

NukeNabber:

An excellent freeware package.
Nukenabber observed many attempts to connect to "well known" Trojan ports,

The report clearly shows that unprotected clients are a severe risk to the Organisation and will be used as leverage to obtain more funding for covering the "back-door"(remote clients and home users connecting on uncontrolled machines via dial-up and VPN) vulnerability that the Organisation has.

An extract of the log file follows:

19:00:09.891 GMT]	Port	31337 (Backorifice/BO-2K)
19:00:09.891 GMT]	Port	31337 (Backorifice/BO-2K)
19:00:09.871 GMT]	Port	34324 (BigGluck, TN)
19:00:09.841 GMT]	Port	65000 (Devil)
19:00:09.861 GMT]	Port	40421 (Master's Paradise Trojan)
19:00:09.931 GMT]	Port	20034 (NetBus 2 Pro)
19:00:09.851 GMT]	Port	53001 (Remote Windows Shutdown)
19:00:09.841 GMT]	Port	61466 (Telecommando)
19:00:09.861 GMT]	Port	40412 (The Spy)
19:00:09.911 GMT]	Port	24680 <Unknown Trojan>
19:00:09.881 GMT]	Port	32418 Acid Battery
19:00:09.901 GMT]	Port	30029 AOL Trojan
19:00:09.881 GMT]	Port	31666 BOWhack
19:00:09.841 GMT]	Port	63485 Bunker-Hill Trojan
19:00:09.851 GMT]	Port	61348 Bunker-HillTrojan
19:00:09.851 GMT]	Port	60000 Deep Throat
19:00:09.911 GMT]	Port	26274 Delta Source
19:00:09.861 GMT]	Port	47262 Delta Source

(The file from which the above has been extracted is attached to the assignment Mail message)

Don't simply deny connections, offer a resolution.

- One should not underestimate the inventiveness of users wishing to circumvent security policies, either for personal convenience or for more sinister motives.

  Quote: "Most of the attacks and vulnerabilities listed in this chapter were the result of bypassing prevention mechanisms. Given this reality, detection and response are essential" [4]

- The organisation employs a very high percentage of scientists and students who are these days very computer literate personnel and though not directly IT employed have learned over many years to circumvent the "traditional" stumbling blocks (dial-up numbers, passwords, etc.,) by social engineering [mostly by force/threat!!] and by configuring their own machines at home.

  - Although the security policy of the organisation explicitly forbids the concurrent connection to "other" networks it is of little use unless it can be policed and when breaches are observed action is taken, and a resolution is suggested

    Quote: The solution needs centralized management capabilities, including the ability to push security policies out to client firewalls from a centralized policy server. [5]

    It is perceived by the Organisation that rather than "fight 'em" a more constructive approach is to offer to assist with their home security for both their benefit and that of the organisation.

  A strategic decision by the Organisation is to only support (allow) machines only if they are running Windows, machines running other operating systems will not be permitted to connect to the network.

  - ✓ This vastly simplifies support by the Help Desk and provides a "helping hand" for the remote user.

  Although ZA proved to be a good tool and is highly regarded by the author, it is user-configurable and therefore at risk of being changed by users to permit traffic other than permitted by the Organisation's policies.

  The organisation has made an "in principle" decision to purchase a solution from ICEworks. (www.networkice.com)

  The ICEworks product range offers a centrally managed "personal firewall" solution that can be run in " silent mode" thus removing the ability of the user to reconfigure it. The client application is administered by ICEcap on a central server

with all alerts being forwarded to it to for recording and for alerting Administrators and Network Managers. ICEcap will push new policies at login time and/or other times as determined by the administrator.

- ✓ Clearly this application will be searched for on the client machine and if not found, the connection would be terminated.

References:

[1] http://www.techrepublic.com/article.jhtml?src=search&id=r00520010328law01.htm

[2] Network Magazine – 26/2/2001 - Curtis Dalton.

[3] http://www.ealaddin.com/home/solutions/Business/corporate.asp

[4] " Secrets & Lies. Digital Security in a Networked World" Ch1, p9:
Schneier, B. Wiley. ISBN 0-471-25311-1

[5] " Hacking Exposed. Network Security Secrets and Solutions" 2nd Ed. Ch8,p405:
Scambray,J McClure,S Kurtz, McGraw Hill. ISBN 0-07-212748-1

© SANS Institute 2000 - 2005 Author retains full rights.