

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Auditing ZoneAlarm

Martin Naedele

Part 1: An audit guideline for ZoneAlarm 3
1 Motivation 3
2 System under consideration 3
3 Existing audit information 3
Zonelabs 3
Specific Internet information sources 4
Internet search engines 4
4 State of the art for ZoneAlarm configuration 4
5 Audit guidelines 5
5.1 Configuration baseline creation phase 5
5.1.1 Operating system settings 6
5.1.1.1 Access rights 6
5.1.1.2 Logging 7
5.1.1.2.1 Log file settings 7
5.1.1.2.2 Enable file access logging 7
5.1.1.2.3 Audit settings 7
5.1.2 ZoneAlarm settings 8
5.1.2.1 General issues 8
5.1.2.2 Zone configuration 9
5.1.2.2.1 Configuration of the zone security level 9
5.1.2.2.2 Definition of the local zone hosts 10
5.1.2.3 Filtering rules 11
5.1.2.4 Other settings 12
5.1.2.5 Digital signature 13
5.1.2.6 Operational procedures 14
5.2 Firewall use phase 14
5.3 Audit phase 14
5.3.1 Subjective audit 14
5.3.2 Objective audit 15
6 Conclusion 16
References 17
General 17
Personal Firewalls 17
ZoneAlarm 17
Tools 18

© SANS Institute 2000 - 2005 Author retains full rights.

Part 2: Auditing a ZoneAlarm installation 19
1 Introduction 19
2 System configuration 19
2.1 Usage Scenario 19
2.2 Test scenario 19
3 Conducting the audit 19
3.1 Subjective audit 19
3.1.1 Settings 19
3.1.1.1 Access rights 19
3.1.1.2 Log file settings 20
3.1.1.3 Enable file access logging 20
3.1.1.4 Audit settings 20
3.1.1.5 ZoneAlarm version 21
3.1.1.6 Zone security levels 22
3.1.1.7 Local zone definition 22
3.1.1.8 Filtering rules 23
3.1.1.9 Other ZoneAlarm settings 23
3.1.2 Operational procedures 23
3.1.3 Logs 24
3.1.3.1 Review ZoneAlarm log 24
3.1.3.2 Review Windows2000 security log 24
3.2 Objective audit 25
3.2.1 Integrity check 25
3.2.2 Scanning 25
3.2.2.1 Internet zone 25
3.2.2.2 Local zone 27
3.2.3 Leak test 28
4 Evaluating the audit 30
5 Future work 31
References 32

© SANS Institute 2000 - 2005 Author retains full rights.

Part 1: An audit guideline for ZoneAlarm

1 Motivation

Nowadays, computers are often connected to the Internet or other unknown networks without protection of a firewall. Such situations include

- connection to an ISP via modem
- connection to the Internet in the terminal room of a conference
- connection of a consultant laptop to the internal network of the client company

Personal firewalls have gained popularity as a means to offer at least some kind of protection in these kinds of situations. Among the available personal firewall applications [Boran], Zonelabs' ZoneAlarm is one of the most popular [Ashworth, Baker, Zych, Zimmer, Hillman, Siow, Boran2], with around 8 million users [Wolfpak].

Like their big cousins, dedicated network firewalls, these personal firewalls also need to be properly configured and regularly audited. Arguably, frequent audits of these are even more necessary, because they are under the direct responsibility of the, possibly non-specialist, end-user, and the operating principle of ZoneAlarm is to prompt the user to define new filtering rules whenever a situation not previously encountered occurs.

Surprisingly, given this situation and the popularity of ZoneAlarm, no audit guidelines for it exist at this point in time (see section 3 below). This report describes an audit guideline for ZoneAlarm, which can be used for auditing to create a secure system baseline and for auditing to verify the conformance of a configured system to this baseline, according to the definition of auditing given in [Kolde].

2 System under consideration

The following work is based on the use of the non-for-profit version of Zonelabs' ZoneAlarm v2.6.88 on an IBM Laptop Thinkpad 570, PII, 330MHz, running Windows2000, build 2195, SP1.
Network connected user applications are IE5.5, Netscape Communicator, Lotus Notes, as well as Ping and Tracert, all as clients only.
The system is alternatively connected to the company home branch office LAN, to the company intranet from a different branch office, and to a private ISP.

3 Existing audit information

The first step when putting together a set of audit guidelines for ZoneAlarm was to inquire which publicly available material already exists. For this purpose, the following sources were investigated:

Zonelabs

- Help files [ZAhelp] and web site [ZAsupport] for Zonealarm.
- Direct inquiry to Zonelabs' technical support via email [ZAtech] which only resulted in a non-specific restatement of the instructions in the manual: start with defaults and loosen rules gradually as necessary.

Internet search engines

- Google [Google], general-purpose search engine
- Northern Light [NL], general purpose search-engine with special for-pay content

© SANS Institute 2000 - 2005 Author retains full rights.

- DejaNews [Dejanews], search engine for newsgroup archives, now also operated by Google searching for "zonealarm and audit"

Articles found via search engines

- Collection of complaints/tips around ZA [Horowitz]
- Some ZoneAlarm configuration tips, but not beyond what the manual offers and no tradeoffs are discussed [Lake]
- Personal firewall tests [Boran, Boran1]
- Good ZoneAlarm secure configuration tips with rationale [Raikow]

Specific Internet information sources

- SANS Global Incident Analysis Center (e.g. [Green1, Green2, Scarborough]) and SANS information security reading room [SANSreading], both via direct inspection and target search using Google.

  While there are quite a lot of reports in the reading room that motivate the use of ZoneAlarm, none of them goes beyond ZoneAlarm's help files in suggestion an encompassing secure configuration or an audit plan.
- Purdue University's CERIAS archive [CERIAS]: nothing relevant found
- CMU SEI's CERT [CERT]: nothing relevant found
- Virginia Tech's security pages: Short step-by-step ZoneAlarm configuration guide [DeBonis]

As stated above, this research into previous work returned as result only the original ZoneAlarm installation instructions [ZAhelp], a couple of articles with installation/ configuration instructions and remarks [Anonymous, DeBonis, Horowitz, Lake, Raikow], of which the last one the is most comprehensive and gives reasons for some recommendations, and a couple of warnings for vulnerabilities in previous versions of ZoneAlarm reported at various places (e.g. [Wolfpak]).

Therefore, there is still a need for an audit plan, which is more comprehensive than the installation instructions and is not only restricted to the configurations within the ZoneAlarm application, but also takes into account the system environment within which it is installed – an aspect neither of the previously discussed sources takes into consideration.

4 State of the art for ZoneAlarm configuration

State of the art is to follow the ZoneAlarm instructions, according to which the personal firewall is installed in "deny all" state. Then individual applications should be reallowed to connect either as client or server for the Internet or a to-be-configured set of trusted hosts whenever this functionality is needed or the first time. The user notices the need for allowing a connection either from a ZoneAlarm generated popup describing the connection attempt of from the fact that some application breaks.

This approach introduces a number of dangers:

- The user might, after evaluating the risks, allow a connection necessary temporarily to run a certain application, but will afterwards forget to re-activate the blocking rule.
- Even though there exists a support web site from Zonelabs [AlertAnalyzer] where one can from the alarm popup request further information about a number of

© SANS Institute 2000 - 2005 Author retains full rights.

registered applications, the user will often not be able to make an informed decision on whether the application wanting to access the network or being accessed is legitimate and whether the access is necessary for the program functionality or just a "phoning home" feature that the user is not interested in executing (For a discussion of such "Spyware" see [Replogle]) . Thus the user will often voluntarily let unnecessary or malicious traffic pass ZoneAlarm.

- From a psychological point of view the Zonelabs recommend approach of step-wise loosening filtering rules as the need arises, fosters a culture of evolution towards lower levels of security over time.

In addition, the interactive mode of configuring security "as you go" does not make use of the local zone settings that are valuable to create tight security, while permitting useful work. Using the local zone settings requires some considerations and configurations before starting to use ZoneAlarm.

The above mentioned issues suggest the following alternative approach to configuring and using ZoneAlarm:

1. Preconfigure ZoneAlarm with a configuration appropriate for the user (create and configure policy)
2. Lock settings down via permissions and audit functionality (enforce policy). Unfortunately, ZoneAlarm does not have built-in lock-down features and the work-around via permissions and audit is clumsy and not fully effective.
3. Justify, document, and monitor any changes that might be necessary in the configuration (change management for the policy)
4. Audit regularly whether the policy is still valid or can be tightened and whether the actual rule set is still in accordance with the policy

This approach will be detailed in the following.

5 Audit guidelines

According to [Kolde], auditing means to compare a system's current state to a predefined baseline. Therefore, the audit procedure must consist of two steps: creation/ reevaluation of the baseline, and evaluation whether the system under consideration is in accordance with this baseline.

In the following we will assume a non-malicious local user and the audit objective is to prevent degeneration of ZoneAlarm security to an insecure level.

5.1 Configuration baseline creation phase

This configuration phase realizes the "audit to create a secure system".

The configuration implements, and if no higher level security policy exists, also defines the policy. The policy has the following three levels of objectives:

- Computer is secure (ZoneAlarm filtering works as intended with appropriate settings and rules)
- ZoneAlarm is secure (no easy manipulations of settings and rules by non-authorized persons)
- Some malicious actions can be detected and analyzed (log files and system auditing functionality)

Some of the following configuration items address individual files of the ZoneAlarm

© SANS Institute 2000 - 2005 Author retains full rights.

application. The following table list these files, where they are stored, and what their purpose is.

FilePathPurposeIAMDB.RDB%system%\winnt\Internet LogsSettings and filtering rule base<host>.LDB%system%\winnt\Internet Logs?
ZALog.txt%system%\winnt\Internet LogsLog for rejected and user permitted connectionsZonealarm.exe%zonealarmpath%ZA
GUIZoneband.dll%zonealarmpath%Mini toolbar
GUIHtml.tdr%system%\winnt\system32\zonelabs\?
Minilog.exe%system%\winnt\system32\zonelabs\Alert loggerVsdb.dll%system%\winnt\system32\zonelabs\Firewall runtimeVsmon.exe%system%\winnt\system32\zonelabs\Firewall runtimeVsruledb.dll%system%\winnt\system32\zonelabs\Firewall runtimeVsutil.dll%system%\winnt\system32?
Vsmoniapi.dll%system%\winnt\system32?Vsdata.dll%system%\winnt\system32?
Vsdatant.sys%system%\winnt\system32?**Table 1ZoneAlarm files**

5.1.1 Operating system settings

5.1.1.1 Access rights

Action: The permissions for the ZoneAlarm files should be set as specified in the following table:

ZoneAlarm file AdministratorsAuthenticated usersSystemIAMDB.RDBFull controlRead/writeRead/write<host>.LDBFull controlRead/writeRead/write ZALog.txtFull controlRead/writeRead/writeZonealarm.exeFull controlRead/execute-Zoneband.dllFull controlRead/executeRead/executeHtml.tdrFull controlRead/ executeRead/executeMinilog.exeFull controlRead/executeRead/executeVsdb.dllFull controlRead/executeRead/executeVsmon.exeFull controlRead/executeRead/ executeVsruledb.dllFull controlRead/executeRead/executeVsutil.dllFull controlRead/ execute-Vsmoniapi.dllFull controlRead/execute-Vsdata.dllFull controlRead/execute-Vsdatant.sysFull controlRead/execute-**Table 2 Required file permissions**

Rationale: As a general principle, permissions should be as restrictive as possible. In experiments it has been determined that the above settings for authenticated user and system are the most restrictive that allow ZoneAlarm operation. It is assumed that the administrator account is only used for installations etc. by privileged personnel.
Procedure: Select the file of group of files with identical access rights settings in the windows explorer, invoke context menu, select properties, select security tab. Use the security tab GUI to verify or modify settings as desired.
Audit: OK, if settings are as specified above

5.1.1.2 Logging

5.1.1.2.1 Log file settings

Action: A suitable log file size and retention policy must be defined. As is pointed out in [Kolde] there is no ideal retention policy, a trade-off between security and availability is necessary.
Procedure: MMC -> Event Viewer snap-in -> Security log -> properties:

- log size 2048 KB (increase size later if it turns out to be insufficient).

© SANS Institute 2000 - 2005 Author retains full rights.

- overwrite events older than 100 days (assuming audit period shorter than 3 months (see [Kolde] for a discussion of the various log retention options).

Audit: Judgement must be exercised whether the combination of log size and overwrite policy represents a reasonable trade-off.

5.1.1.2.2 Enable file access logging

Action: The audit system must be turned on to enable auditing of accesses to certain files.

Procedure: MMC -> Group Policy snap-in -> Computer configuration -> Windows settings -> Security settings -> Local Policies -> Audit Policy:

- Audit object access: success and failure: (enables object access auditing in general, specific source objects still need to be configured (see below))

Additional settings may be required by other security policies for the system under consideration.

Audit: OK, if settings contain the one specified above

5.1.1.2.3 Audit settings

Action: The specific log event sources need to be configured.

Procedure: For each of the files in Table 1: select the file in the windows explorer -> properties -> security -> advanced -> auditing -> add (for verification: view/edit) -> Everyone -> successful&failed for

- traverse folder/execute file,
- list folder/read data,
- create files/write data,
- create folders/append data,
- delete subfolders and files,
- delete
- change permissions

Audit: OK, if settings are as specified above

How will different scenarios be reflected in the security log?

- Read access to log file
  Event 560, 562 by user to ZALog.txt
- Rejected attack
  4x560, 562 by user and SYSTEM account to ZALog.txt
- Shutdown of ZoneAlarm
  2x562 by SYSTEM, 2x 560 by SYSTEM (not consistent), 560 by user to minilog.exe, 2x 560, 562 by user to ZALog.txt
- Start up of ZoneAlarm:
  19x560, 562 by user to various ZA files
- Change of security settings
  no reaction in log,
- Allowing outgoing event:
  560, 562 by user on Zalog.txt
- Windows audit events will not catch the fact that a user kills the firewall task (vsmon.exe).

5.1.2 ZoneAlarm settings

The ZoneAlarm settings for the system under consideration need to be found, mostly by

© SANS Institute 2000 - 2005 Author retains full rights.

trial and error, by a person knowledgeable in ZoneAlarm operation principles, Windows2000 configuration, and general security issues.
The settings, zone definitions and filter rules can easily be transferred from one host to another by copying the IAMDB.RDB file.
The following settings refer to the policy for the system defined in section 2.

5.1.2.1 General issues

Action: Ensure the most recent version of ZoneAlarm is used. At the time of writing (6/01) this is version 2.6.88.
Procedure: Restore the ZA control center, go to the configure tab (the version is printed there), press button "check for update"

Audit: OK, if result of "check for update" is that no update for the current version exists.

5.1.2.2 Zone configuration

ZA allows two different sets of rules (one more, one less strict) depending on the host involved. The set of hosts for which the less strict rules are applied is called the "local zone", all other hosts are automatically in the "Internet zone". The hosts in the "local zone" do not necessarily be local in the sense of being on the same LAN segment.
Configuration of Zones involves two steps: Configuration of the zone security level and definition of the local zone hosts.

5.1.2.2.1 Configuration of the zone security level

Action: Configure zone security levels "high" for both zones [Raikow, Anonymous], decrease local zone to "medium" (allows NetBIOS traffic) if problems occur.
Rationale: The higher the security level, the better. Setting both sliders to high does not mean that both zones are regarded as one, as the application specific settings (see below) also make use of the two different zones.
Procedure: Restore the ZA control center, go to the security tab, select security levels using sliders.
Audit: OK, if "high" is set for both, or "medium" for local zone and an acceptable explanation is documented why this is necessary.

Action: Uncheck both "block … servers" boxes [DeBonis].
Rationale: This is unlikely to yield a configuration that allows useful work wih the computer; better use the fine grained control on application level (see "filtering rules" below).
Audit: OK, if settings are as specified above.

5.1.2.2.2 Definition of the local zone hosts

Action: Configure local zone hosts
Rationale: Name here IP addresses for which you want less restrictive than the general

© SANS Institute 2000 - 2005 Author retains full rights.

Internet zone application filtering rules (to be defined below) to apply. Examples include:

- Office LAN to access network printers and file servers,
- Lotus Notes/Mail server,
- Web proxy server
- Localhost,
- Other servers according to individual need

Procedure: Restore the ZA control center, go to the security tab, press the "advanced" button, define your "trusted" hosts using IP addresses, IP address ranges, or subnets. Use IP addresses instead of host names to prevent attacks using DNS spoofing.
Audit: Judgement must be exercised whether the hosts specified for the local zone, especially those outside the organisation's firewalls, are necessary and trustworthy. This judgement is also influenced by the differences in filtering rules between the two zones specified below.

Action: Uncheck the "adapter subnets"
Rationale: ZoneAlarm automatically checks the adapter subnet, meaning that all host connected to the LAN are trusted, in the assumption that this is the office net, and that it deservers treatment as local zone. However, in many relevant settings, e.g. connection to LAN at client office, ISP dial up, etc. this assumption is not justified [DeBonis].
Audit: OK, if box is unchecked.

5.1.2.3 Filtering rules

The association of a host with one of the two zones and the zone-specific security level define a default security setting for this host. Additional application specific filtering/ pass rules are necessary to configure a working but reasonably secure system.
Action: Do not follow the "decide on pop-up" strategy proposed by ZoneAlarm, instead configure the rule set up front.
Rationale: At the moment when the pop-up asking for permissions occurs the current user will in most cases neither have the patience nor the detailed knowledge to judge whether the requested access is necessary and desirable and whether the requesting application is legitimate. Therefore, the definition of the filtering rules should not be a side activity, but a focussed upfront activity.
Procedure:

1. Invoke all (network accessing) applications on the host, both from client and server side; go through all usage scenarios (as far as this is possible).
   This process will cause all the access request pop-ups to appear that are relevant for the applications to be run on this host.
2. Restore the ZoneAlarm control center, go to the programs tab, and set for each application the client/server permission level for the local and the Internet zone.
   The next figure shows these settings for the example configuration.

The two browsers, Netscape Navigator and MS Internet Explorer have client access

© SANS Institute 2000 - 2005 Author retains full rights.

to the Internet, but should not act as servers. Ndyncfg.exe, nlnotes.exe, and nwrdaemn.exe are parts of Lotus Notes. They only need to access the local zone, as the Lotus Notes serves has been defined to be part of the local zone. Ping and Traceroute are allowed to access the Internet and the local zone as clients. ZoneAlarm needs to access the Internet as client only in order to retrieve the extended help information associated with the access request pop-up, but this feature is only necessary in the configuration mode, therefore it can be disabled during operation. Services and Controller is part of the Windows 2000 operating system and needs client access to the local zone and the Internet for proper operation of the operating system. This permission seems to be uncritical with respect to security [Horowitz]. Note that in correspondence with the recommendations of [Raikow] none of the applications has server permissions.

3. Again, invoke all relevant applications and go through all relevant usage scenarios to verify that the selected permissions allow normal operations. Modify settings and retest if necessary.

Audit: In general, judgement must be exercised for each of the listed applications whether it should be run at all (e.g. instant messaging applications, peer-to-peer file sharing), and whether giving it network access on the specified level in any of the four categories, is necessary, desirable, and creates an acceptable risk. For the concrete system defined in section 2, the audit is OK, if the settings are as shown. It is more difficult to verify, that the user does not change the rule set (temporarily) during operations without proper documentation. The tools for this purpose are the Windows event log (changes to IAMDB.RDB) and ZoneAlarm log "PE" entries. However, this investigation is inefficient and not necessarily conclusive, as will be discussed in Part 2.

5.1.2.4 Other settings

ZoneAlarm allows a couple of additional configuration options the settings for which are recommended in the following:

- ZoneAlarm logging

  Action: enable logging [Raikow]

  Rationale: The log is the most important means of auditing and attack detection over a time span.

  Procedure: open ZoneAlarm control center, go to Alerts tab, check "log alerts to a text file"

  Audit: OK, if checked.

  Action: enable alarm notification [Raikow]

  Rationale: detection of attacks, get a feel for the frequency of suspicious network activity

  Procedure: open ZoneAlarm control center, go to Alerts tab, check "show the alert pop-up window"

  Audit: OK, if checked.

- Internet lock

  Action: do not use

  Rationale: The lock creates an additional usability hurdle while not providing

© SANS Institute 2000 - 2005 Author retains full rights.

considerable more security for the host under consideration. The system is not continuously connected to an always-on home network, which might justify the use of this feature, but is mostly only online when somebody is working on it, which means, that in these times the lock would not be active anyway.
Procedure: open ZoneAlarm control center, go to Lock, check "Automatic lock: disable".
Audit: OK, if not checked.

- MailSafe
  Action: activate mailsafe [Raikow]
  Rationale: While this feature is not effective for the two email scenarios in the system under consideration, web mail and Lotus Notes mails, it doesn't cost anything to activate this additional protection.
  Procedure: open ZoneAlarm control center, go to Security, check "Enable MailSafe protection…".
  Audit: OK, if checked.

- On top during Internet activity
  Action: uncheck
  Rationale: Most Internet activity is intended part of the normal work. In this case it is needlessly intrusive to have the ZoneAlarm GUI cover a considerable part of the screen [Raikow].
  Procedure: open ZoneAlarm control center, go to Configure, check "On top during Internet activity".
  Audit: OK, if not checked.

- Load at start-up
  Action: check [Raikow]
  Rationale: ZoneAlarm can only monitor applications that are started after the ZoneAlarm firewall runtime, so this should be started as early as possible.
  Procedure: open ZoneAlarm control center, go to Configure, check "Load ZoneAlarm at start-up".
  Audit: OK, if checked.

- Check for updates automatically
  Action: deactivate
  Rationale: Checking for and installing updates is part of the auditing process and not in the responsibility of the end-user during his/her day-to-day activities.
  Procedure: open ZoneAlarm control center, go to Configure, uncheck "Yes, I want to check for updates automatically".
  Audit: OK, if not checked.

- Notify about communication with ZoneAlarm
  Action: activate
  Rationale: We don't want any application to "phone home" without the user knowing and approving it, not even the ZoneAlarm firewall itself.

© SANS Institute 2000 - 2005 Author retains full rights.

Procedure: open ZoneAlarm control center, go to Configure, check "Notify me before I exchange information with Zone Labs".
Audit: OK, if checked.

5.1.2.5 Digital signature

Action: Generate digital signatures of vsmon.exe, vsruledb.dll, vsdb.dll, minilog.exe, html.tdr, zonealarm.exe, vsutil.dll, vsmonapi.dll, vsdata.dll, vsdatant.sys, and store them to a safe place off the host (e.g. to a disk).
Rationale: A Trojan trying to undermine the ZoneAlarm functionality would change these binaries, so verifying the signatures is a guarantee that the binaries have not been tampered with. The other files will change during normal operation and therefore can not be secured this way.
Procedure: Use a tool for digital signatures like PGP and follow the instructions for generating signatures that come with the tool.
Audit: OK, if signature verification with the above named files from off-line stored signatures is successful.

5.1.2.6 Operational procedures

- Backup

  Action: A separate copy of the current approved versions of the IAMD.RDB and <hostname>.LDB files is kept on secure storage outside the host under consideration, e.g. on a disk.
  Rationale: This allows quick restoration of the approved configuration after attacks or misconfigurations.
  Audit: OK, if current copies exist at off-line storage.

5.2 Firewall use phase

For the usage phase it is assumed that the user does not work with Administrator privileges, even though in many cases the day-to-day user will be the same person as the one configuring and auditing the firewall.
During the normal usage phase, all additional permission requests are denied. If a necessary internal application breaks, a change of the ZoneAlarm configuration must be formally requested, investigated, approved, and documented.
In case of a ZoneAlarm alert, the user contacts his IT security responsible person to take the necessary steps. Incident handling is outside the scope of this document.

5.3 Audit phase

The audit phase realizes the "audit to maintain a secure configuration" [Kolde].
The means and procedures described in the following also help to answer questions like: What went wrong? Why did something get through the firewall that shouldn't have? Is the ZoneAlarm installation still intact?

5.3.1 Subjective audit

The subjective audit produces results from which an indirect conclusion about the security state of the system is made:

Settings

Action: Verify all the settings described in sections 5.1.1 and 5.1.2.
Audit: OK, if the audit success criteria specified for each setting are met.
Subjective, because the specified ZoneAlarm and system configurations and settings are

© SANS Institute 2000 - 2005 Author retains full rights.

assumed to increase the security of the ZoneAlarm protected system or the ZoneAlarm installation itself, but are not guaranteed to do so.

Operational procedures
Action: Verify that operational procedures exist and are/were followed for
- Modifying filering rules,
- Making backups of the ZoneAlarm configuration
- Reacting on alerts and handling incidents
- Updating the ZoneAlarm installation

Audit: Judgement must be exercised to evaluate whether the defined procedures are sufficient for the operational environment and whether available evidence (backup files, log entries, etc.) proves that they are followed.
Subjective, because the following of the procedures can not be absolutely proven and because their existence only provides support for a more secure system.

Logs
Action: Review ZoneAlarm logs
Rationale: Information about attempted intrusions and access requests can be found in the log
Procedure: Analyse the ZALog.txt file, possibly using a tool like ZoneLog Analyser [ZoneLog] or ClearZone [ClearZone]. An explanation of the types of entries is in the ZoneAlarm log can be found in [Anderson].
An example of the aggregated results of four months of ZoneAlarm logging with some advice on analysis can be found in [Stinson].
After reviewing the log, store it to a save, offline location by simply copying the Zalog.txt file, and clear the log: Open the ZoneAlarm Control Center -> tab Alerts -> button Delete Log.
Audit: The log file audit has no clear pass/no pass result. The review of the event patterns in the log files may deliver evidence about successful and unsuccessful attacks from the network, about Trojans trying to communicate with the outside from the inside, and about unauthorized modifications of the filtering rules.

Action: Review the Windows2000 security event log
Rationale: Information about user and application events concerning the ZoneAlarm installation an operation can be found in the Windows2000 security log (see section 5.1.1.2).
Procedure: Analyse the Windows2000 security event log either using the built-in event viewer (start->programs->administrative tools->event viewer) or any 3rd party tools (refer to [Kolde] for an overview of some Windows log analysis tools and procedures).
After reviewing the log, store it to a secure, offline location: MMC -> Event viewer -> security -> context menu -> Save log file as, and clear the log: MMC -> Event viewer -> security -> context menu -> clear all events.
Audit: The Windows security event log file audit has no clear pass/no pass result. The review of the event patterns in the log files may deliver evidence about unauthorized modifications of the ZoneAlarm configuration and tampering with the operation.

© SANS Institute 2000 - 2005 Author retains full rights.

Subjective, because suspicious log entries are not necessarily associated with intrusions and tampering but provide just some hints that a security critical ebent may have happened. On the other hand, an example for a false alarm is described in [Armstrong]. Also, absence of suspicious traces in the log does not provide certainty that no security critical event has happened.

5.3.2 Objective audit

The objective audit directly verifies the desired functionality of the firewall by simulating malicious activities and observing the firewall behavior.

Integrity check

Action: Check the digital signatures of vsmon.exe, vsruledb.dll, vsdb.dll, minilog.exe, html.tdr, zonealarm.exe, vsutil.dll, vsmonapi.dll, vsdata.dll, vsdatant.sys
Rationale: see section 5.1.2.5
Procedure: Use a tool for digital signatures like PGP and follow the instructions for verifying the previously generated signatures.
Audit: see section 5.1.2.5
Objective, because any integrity violation is a direct indicator that tampering with the firewall has happened.

Scanning

Action: Scan the ZoneAlarm-protected host for open ports from a host in the Internet zone
Rationale: This is the test that the ZoneAlarm firewall catches and rejects all connection attempts except for those in the permitted rule set.
Procedure: Use a tool like NMAP (or NMAPNT) to run a UDP and TCP scan on all ports of the host specifying a source host in the Internet zone.
Audit: OK, if all open ports found are the ones that are expected and legal according to the rule set for the Internet zone.
Objective, because this test directly verifies actual firewall functionality for the Internet zone.

Action: Scan the ZoneAlarm-protected host for open ports from a host in the local zone
Rationale: This is the test that the ZoneAlarm firewall catches and rejects all connection attempts except for those in the permitted rule set.
Procedure: Use a tool like NMAP (or NMAPNT) to run a UDP and TCP scan on all ports of the host specifying a source host in the local zone.
Audit: OK, if all open ports found are the ones that are expected and legal according to the rule set for the local zone.
Objective, because this test directly verifies actual firewall functionality for the local zone.

Leak test

Action: Execute the leak test
Rationale: This is the test that the ZoneAlarm firewall catches and rejects all unauthorized outgoing communication attempts and thus prevents (malicious)

© SANS Institute 2000 - 2005 Author retains full rights.

applications from “calling home”.
Procedure: Follow the instructions in [Leaktest]
Audit: OK, if the leak test succeeds, that is, if the test program is prevented from communicating with the outside.
Objective, because this test directly verifies the actual firewall behavior.

6 Conclusion

This report presents audit guidelines for the ZoneAlarm personal firewall that go much further than previous works in this direction in that it not only explains on how to configure ZoneAlarm but also gives experimentation-based and explanation-backed recommendations for specific settings. Also, the operating system is included in the configuration and audit considerations and some tool-based objective auditing procedures are suggested. The most important point of the presented auditing guidelines is to not follow the ZoneAlarm suggested approach of evolutionary permission definition by the end-user but to clearly separate the configuration and the usage phase and to audit this separation.

References

General

[Kolde] J. Kolde, J. Green: Advanced Systems Audit and Forensics; Track 7 course notes, SANS 2001, Baltimore

[CERIAS] Purdue University Center for Education and Research in Information Assurance and Security, http://www.cerias.purdue.edu/hotlist/

[CERT] Carnegie Mellon University CERT Coordination center, http://search.cert.org/

Personal Firewalls

[Boran] Sean Boran: Personal Firewalls/Intrusion Detection Systems, June 14, 2001, http://www.securityportal.com/articles/pf_main20001023.html

[Boran2] Sean Boran: Personal Firewall Test: ZoneAlarm, November 29, 2000, http://securityportal.com/articles/pf_zonealarm20001023.html

[SANSreading] SANS Information Security Reading Room: http://www.sans.org/infosecFAQ/index.htm

[Replogle] Daniel M. Replogle, Spyware - Recent Evolving Issues, November 13, 2000, http://www.sans.org/infosecFAQ/casestudies/spyware.htm

[Ashworth] Robert Ashworth, Protecting your Home Computer from the Internet - Can You Keep the Heat Out?, 12/9/2000, http://www.sans.org/infosecFAQ/homeoffice/heat.htm

[Baker] Andrew S. Baker ,Connecting Your Home LAN to the Internet – Securely, 03/27/2001, http://www.sans.org/infosecFAQ/homeoffice/home_LAN.htm

[Zych] Tina Zych , Personal Firewalls: What are they, how do they work?, August 22, 2000, http://www.sans.org/infosecFAQ/homeoffice/personal_fw.htm

[Zimmer] Kevin Zimmer, Protecting Your Company from the Small Office or Networked Home Office, February 12, 2001, http://www.sans.org/

© SANS Institute 2000 - 2005 Author retains full rights.

infosecFAQ/homeoffice/protecting.htm

[Hillman] Dale Hillman, How Complicated Is Home Protection?, November 23, 2000, http://www.sans.org/infosecFAQ/homeoffice/protection.htm

[Armstrong] Del Armstrong, Practical Exam GIAC Intrusion Detection Curriculum, San Jose, 2000, http://www.sans.org/y2k/practical/Del_Armstrong.htm

[Stinson] Jack Stinson, Are You Being Scanned?, November 13, 2000, http://www.sans.org/infosecFAQ/homeoffice/scanned.htm

[Siow] Patricia Siow, A Simple and Effective Path to Improving NT Security, March 21, 2001, http://www.sans.org/infosecFAQ/win/path.htm

ZoneAlarm

[ZAdowload] Zone Labs ZoneAlarm download page http://www.zonelabs.com/products/za/moreinfo.html

[ZAhelp] Zone Labs ZoneAlarm user manual (collection of help file information): http://www.zonelabs.com/pdf/ZA_Manual.pdf

[ZAsupport] Zone Labs support web site for ZoneAlarm: http://www.zonelabs.com/services/support_za_zap.htm

[ZAtech] Personal email communication with Zone Labs technical support, 15.6.2001

[Horowitz] Michael Horowitz, Zone Alarm Gripes, July 7, 2001, http://www.computergripes.com/ZoneAlarm.html

[Green] John Green, Global Incident Analysis Center, Report of detects analysed 4/27/00; http://www.sans.org/y2k/042700.htm

[Green2] John Green, Global Incident Analysis Center, Report of detects analysed 4/30/00; http://www.sans.org/y2k/043000.htm

[Scarborough] Matt Scarborough, Global Incident Analysis Center, Reports of detects, 12/27/2000; http://www.sans.org/y2k/122700.htm

[Wolfpak] The WolfPak: Multiple Vulnerabilities in ZoneAlarm, 12/20/2000, http://wolfpak.dynip.com/advisories/za_release.txt

[Schumacher] Robert Schumacher: Re: I've got a Firewall--now what???, 06/20/2001, Newsgroups: alt.windows98

[Anonymous] Nospam@pacbell.net: Re: Securing an NT box, 03/20/2001, Newsgroups: comp.os.ms-windows.nt.admin.security

[Lake] Matt Lake: Instant Internet Security, July 13, 2000, http://www.pcworld.com/hereshow/article/0,aid,17587,00.asp

[Anderson] Rob Anderson: Rob's ZoneAlarm Log Page, 02/05/2001, http://home.swbell.net/anumber1/zalog1.html

[Raikow] David Raikow: Installing ZoneAlarm, August 2, 2000, http://www.zdnet.com/filters/printerfriendly/0,6061,2610364-77,00.html

[DeBonis] Marc DeBonis: Basics on how to use ZoneAlarm (ZA) from ZoneLabs, http://security.vt.edu/lockitdown/zonealarm.phtml

© SANS Institute 2000 - 2005 Author retains full rights.

Tools

[Google] Google Internet search engine: http://www.google.com

[Dejanews] Google newsgroup search engine: http://groups.google.com

[NL] Northern Light Internet search engine, http://www.northernlight.com

[ClearZone] ClearZone ZoneAlarm Log Analyser, http://clearzone.hypermart.net/#ClearZone

[ZoneLog] ZoneLog Zone Alarm Log Analyzer, http://www.zonelog.co.uk

[Analyzer] ZoneLabs AlertAnalyzer and knowledgebase, http://fwalerts.zonelabs.com/fwalerts/fwalertresult, browsing interface at http://fwalerts.zonelabs.com/fwalerts/process?main

[Leaktest] Steve Gibson: LeakTest, July 07, 2001, http://grc.com/lt/howtouse.htm

© SANS Institute 2000 - 2005 Author retains full rights.

Part 2: Auditing a ZoneAlarm installation

1 Introduction

This part describes an actual audit of an installation of the ZoneAlarm personal firewall following the audit plan detailed in part 1 of this report.

2 System configuration

The relevant system configuration is a IBM Laptop Thinkpad 570, PII, 330MHz, running Windows2000, build 2195, SP1 and the not-for-profit version of Zonelabs' ZoneAlarm v2.6.88.

2.1 Usage Scenario

Network connected user applications are IE5.5, Netscape Communicator, Lotus Notes, as well as Ping and Tracert, all as clients only.
The system is alternatively connected to the company home branch office LAN, to the company intranet from a different branch office, and to a private ISP.
In the home branch office LAN shared drives of a server need to be mounted.

2.2 Test scenario

Most parts of the audit can be conducted using at the audited host in isolation. For the scan from the outside, a second computer running NMAPNT [Nmapnt, Green3] was connected to the audited host via cross-over cable so that no live network was subjected to the scan traffic.

3 Conducting the audit

3.1 Subjective audit

3.1.1 Settings

3.1.1.1 Access rights

Procedure: The desired settings and the set/verify procedure is described in Section 5.1.1.1 of part 1. The figures below show some of the results.

Evaluation: OK, the actual access rights settings are as required.

3.1.1.2 Log file settings

Procedure: The desired settings and the set/verify procedure is described in Section 5.1.1.2.1 of part 1. The figure below shows the result.

Evaluation: OK, with a size of 2MB and overwrite after 100 days the actual log settings are reasonable assuming an audit interval of 30 days. Also, the current size of the log file smaller than the maximum size setting.

3.1.1.3 Enable file access logging

Procedure: The desired settings and the set/verify procedure is described in Section 5.1.1.2.2 of part 1. The figure below shows the result.

Evaluation: OK, the actual audit settings are as required.

© SANS Institute 2000 - 2005 Author retains full rights.

3.1.1.4 Audit settings

Procedure: The desired settings and the set/verify procedure is described in Section 5.1.1.2.3 of part 1. The figure below shows the results for the files html.tdr, minilog.exe, vsdb.dll, vsmon.exe, and vsruledb.dll in c:\WINNT\system32\ZoneLabs.

Evaluation: OK, the actual audit settings are as required.

3.1.1.5 ZoneAlarm version

Procedure: The desired settings and the set/verify procedure is described in Section 5.1.2.1 of part 1. The figures below shows the results.

Evaluation: OK, the most recent ZoneAlarm version (2.6.88) at the time of the audit (7/01) is used.

3.1.1.6 Zone security levels

Procedure: The desired settings and the set/verify procedure is described in Section 5.1.2.2.1 of part 1. The figure below shows the result.

Evaluation: OK, in conformance with the requirements, the security level for both zones is set to “high”.

3.1.1.7 Local zone definition

Procedure: The desired settings and the set/verify procedure is described in Section 5.1.2.2.2 of part 1. The figure below shows the result.

Evaluation: OK, the local zone definition conforms to the requirements: The specified hosts are in accordance with the requirements of the usage scenario described above. All hosts in the local zone are defined using their IP addresses. The adapter entry is unchecked to prevent automatic integration of untrusted LANs, to which the host may be connected e.g. at a customer site, into the more trusted local zone.

3.1.1.8 Filtering rules

Procedure: The desired settings and the set/verify procedure is described in Section 5.1.2.3 of part 1. The figure below shows the result.

Evaluation: OK, the filtering rules are set as required in Section 5.1.2.3 of part 1. See Section 4 for remarks on evaluating rule evolution history using the logs.

© SANS Institute 2000 - 2005 Author retains full rights.

3.1.1.9 Other ZoneAlarm settings

The remaining ZoneAlarm settings have been verified to conform to the requirements of Section 5.1.2.4 in part 1 with binary evaluation criteria, but the results will not be shown here in detail.

3.1.2 Operational procedures

Procedure: Interview the user of the audited host.
Evaluation: Copies of the configuration files are kept on a separate disk as postulated in Section 5.1.2.6 of part 1. The additional operational procedures named in 5.3.1 in part 1 are not formalized and documented. This is not optimal, but acceptable for this particular audited host, considering the usage scenario and environment, where the one user of the audited host is anyway responsible for configuration, operations, and incident handling.

3.1.3 Logs

3.1.3.1 Review ZoneAlarm log

Procedure: The ZoneAlarm log has been reviewed using ZoneLog [ZoneLog]. The figure below shows part of the log reflecting an UDP scan (which was done as part of the audit).

Evaluation: The audit of logs is a fuzzy issue, because some important information can often only be derived by experienced correlation between multiple log entries. The log that was reviewed in this audit did not show indications of external attacks or scans (except for those generated as part of the experimentations for this report). Outgoing traffic attempts stopped by ZoneAlarm could be clearly associated with the correct, expected, and non-malicious working of an installed program. No Trojan activity was detected. In summary, the ZoneAlarm log audit is OK.

3.1.3.2 Review Windows2000 security log

Procedure: The Windows2000 security event log has been reviewed using the MMC event viewer following the procedure described in section 5.3.1 in part 1. The figure below shows part of the log.

Evaluation: No log entries of failed actions were found, and no entries indicated unauthorized changing of permissions on files of the ZoneAlarm installation. While the information found was OK, it did all in all not considerably contribute to the evaluation of the security of the system. See Section 4 for further comments.

3.2 Objective audit

3.2.1 Integrity check

Procedure:

1. Insert write-protected disk with the signatures of vsmon.exe, vsruledb.dll, vsdb.dll, minilog.exe, html.tdr, zonealarm.exe, vsutil.dll, vsmonapi.dll, vsdata.dll, vsdatant.sys generated as part of the baselining into disk drive of the audited host.

© SANS Institute 2000 - 2005 Author retains full rights.

2. For each signature file (e.g. binary: vsmon.exe -> signature: vsmon.exe.sig) invoke context menu -> PGP -> verify signature
3. In the directory browser select the corresponding binary (see table 1 in part 1)
4. In the then appearing signature verification result window check that the signature is valid and that the signer and signing date are as expected.
5. Repeat procedure for all the files named above

Evaluation: OK, as the signatures could be verified for all binaries of the ZoneAlarm distribution.

3.2.2 Scanning

3.2.2.1 Internet zone

Procedure:

1. Connect audited host (with running ZoneAlarm firewall) via crossover cable to auditor's computer.
2. On audited host run IPCONFIG to obtain target IP address.
3. On auditor's host run IPCONFIG to obtain source IP address.
4. Ensure that the auditor's host (source address) **is not** in the local zone: Open ZoneAlarm Control -> security tab -> advanced -> verify that none of the checked addresses and address ranges covers the source address, uncheck specified address if necessary

TCP scan:

5. Connect auditor's host to another network, e.g. by dial-up modem. This is necessary for NMAPNT to find the available network adapters (Is this a bug?).
6. On auditor's host run

```
NMAPNT -sT -P0 -v –n –r -e0 –Taggressive –oN tcpscan.txt –O
<target IP address>
```

Explanation:

-sT: TCP connect scan. This option does not work together with the –S (specify source address) option, therefore the procedure of step 4 is necessary.

-P0: Don't ping – ZoneAlarm would not react on ping and thus cause the scanner to skip the host

-v: Verbose output

-n: Never do DNS resolution: Speed up the scan

-r: Don't randomise port numbers: The stealth function of randomised ports is not needed for the audit. Sequential ports are more pleasant to review in the ZoneAlarm log file. This option is available, but undocumented for the NT version.

-e0: Specifies the network adapter to be used on the auditor's host to find the target. This value must be changed as necessary.

-Taggressive: Second highest scan speed. Highest speed was not acceptable to the audited host and led to termination of the scan.

-oN tcpscan.txt: Send output to the specified file in human readable form.

-O: Try to identify target operating system.

© SANS Institute 2000 - 2005 Author retains full rights.

7. After ca. 5 seconds the second network connection may be disconnected.
8. Wait for NMAPNT to finish scan.
9. Review results in tcpscan.txt (see figure below)

UDP scan:
10. Connect auditor's host to another network, e.g. by dial-up modem. This is necessary for NMAPNT to find the available network adapters (Is this a bug?).
11. On auditor's host run

```
NMAPNT -sU -P0 -v –n –r -e0 –Taggressive –oN udpscan.txt
<target IP address>
```

12. After ca. 5 seconds the second network connection may be disconnected.
13. Wait for NMAPNT to finish.
14. Review results in udpscan.txt (see figure below)

15. Restore local zone settings, if necessary: If in step 4 an address (range) has been unchecked, go back to the ZoneAlarm Control center as described above and re-check this address (range).

Evaluation: The ZoneAlarm filtering rules specify that no application on the audited host acts as server, therefore no ports should be open for TCP or UDP. The port scan result verifies this, so this part of the audit is OK. As a counter test to verify proper operation of the scanner, the scan has also been run with ZoneAlarm shut down. As expected, a number of open ports were found:

3.2.2.2 Local zone

Procedure:
1. Connect audited host (with running ZoneAlarm firewall) via crossover cable to auditor's computer.
2. On audited host run IPCONFIG to obtain target IP address.
3. On auditor's host run IPCONFIG to obtain source IP address.
4. Ensure that the auditor's host (source address) **is** in the local zone: Open ZoneAlarm Control -> security tab -> advanced -> verify that one of the checked addresses and address ranges covers the source address; add a definition covering the source host if necessary.

TCP scan:
5. Connect auditor's host to another network, e.g. by dial-up modem. This is necessary for NMAPNT to find the available network adapters (Is this a bug?).
6. On auditor's host run

```
NMAPNT -sT -P0 -v –n –r -e0 –Taggressive –oN
tcpscan_local.txt –O <target IP address>
```

7. After ca. 5 seconds the second network connection may be disconnected.

© SANS Institute 2000 - 2005 Author retains full rights.

8. Wait for NMAPNT to finish scan.
9. Review results in tcpscan_local.txt (see figure below)

UDP scan:
10. Connect auditor's host to another network, e.g. by dial-up modem. This is necessary for NMAPNT to find the available network adapters (Is this a bug?).
11. On auditor's host run

```
NMAPNT -sU -P0 -v –n –r -e0 –Taggressive –oN
udpscan_local.txt   <target IP address>
```

12. After ca. 5 seconds the second network connection may be disconnected.
13. Wait for NMAPNT to finish.
14. Review results in udpscan_local.txt (see figure below)

15. Restore local zone settings, if necessary: If in step 4 an address has been added, go back to the ZoneAlarm Control Center as described above and remove this address.

Evaluation: The ZoneAlarm filtering rules specify that no application on the audited host acts as server, therefore no ports should be open for TCP or UDP. The port scan result verifies this, so this part of the audit is OK. .

3.2.3 Leak test

Procedure:
1. Download LEAKTEST.EXE form [LTdownload]
2. Rename the file to one of the applications that have client Internet access according to the ZoneAlarm filtering rules, e.g. PING.EXE
3. Run the renamed application

4. Answer the question for access permission with "No"

5. Remove the new entry for LEAKTEST from the ZoneAlarm rule base in the Control Center.

Evaluation: OK, the "malicious" application was recognized and access was denied.

4 Evaluating the audit

The audit guidelines presented in part 1 of this report are, with some restrictions that are noted below, effective to evaluate

- the current configuration of the ZoneAlarm installation, including settings, permissions, and filtering rules,
- the integrity of the current ZoneAlarm installation,
- the actual, objective effectiveness of the current ZoneAlarm installation against attacks from the outside.

© SANS Institute 2000 - 2005 Author retains full rights.

Assuming, as the underlying scenario does, a non-malicious user who would not delete or manipulate logs, and excluding that this can happen by accident, it is also in theory effective to evaluate, by means of the ZoneAlarm log, whether and which attacks from the outside the system was subjected to since the last audit and whether/which Trojans tried to connect from the inside to the outside.

In practice however, no certain statements can be made about the period between audits. This is, because ZoneAlarm neither supports locking down of a configuration – that is against the operational philosophy of evolutionary rule definition – nor does it at least provide reliable logging of its operational and configuration history. That is, from neither the ZoneAlarm log nor the Windows 2000 security event log it is possible to clearly answer in hindsight for all points in time the following questions :

- Was the ZoneAlarm firewall process running (and started at system start-up before other applications could open ports)?
- Were there any temporary, transient changes in the active filtering rules?

The approach of the above audit guidelines to get some confidence about this by using the Windows 2000 file audit facilities was clearly not successful:

- The amount of collected data in the Windows security event log is too large.
- The event descriptions are so cryptic as to be (almost) useless.
- No suitable built-in analysis tools exist.
- The event types and granularity is not suitable to define triggers that would easily help to answer the above questions.
- The ZoneAlarm system has a couple of design "flaws" that prohibit to reason from external criteria (e.g. rule file has been written to, "PE" entry has been added to the ZoneAlarm log file, …) about actual changes of the valid rule set.

Minor problems

Some minor issues were discovered during the development and execution of the audit plan:

- NMAPNT (version 2.53sp1) seems to have a bug that prevents the use of the –p command line option which is necessary to specify arbitrary port ranges to be scanned. At the moment, NMAPNT will only execute the –F option which scans the ports provided in the NMAP-SERVICES file.
- It is not reasonably feasible to scan with all source and target port combinations, thus special behavior for certain ports as documented in [Green, Green2] will most likely not be discovered.
- Similarly, the audit would not systematically discover whether there are certain source address ranges, source applications for which ZoneAlarm exhibits special behavior (see also the discussion in [Leaktest]). Note: Due to the fact that ZoneAlarm recognizes applications by their cryptographic checksum, not by their name, which is good, it is unfortunately not easily possible to use the LEAKTEST application to investigate whether ZoneAlarm implements special behaviour for certain applications. This issue can only be addressed by inspection of the ZoneAlarm code, following the security argument of the Open Source community.
- Not all information sources I found are clear about the fact that the "PE" entry in

© SANS Institute 2000 - 2005 Author retains full rights.

the ZoneAlarm log does only indicate that the popup was shown to the user, but that it does not imply that the user a gave a positive or negative answer to it.

Summary
The presented audit approach is not sufficient to ensure security of a host used by another person.
It is, however, very well suitable to support a single, all in one administrator, user, auditor, of a host, in reassuring himself in regular intervals that his/her ZoneAlarm installation still stands as it should, by providing a systematic procedure for verifying all issues that matter. As lesson learned from the actual audit in part 2, the guideline items referring to defining Windows system auditing events and reviewing the Windows security event log should be dropped for this audit scenario.
Important: Without any means to lock down and enforce the configuration and regular operation of ZoneAlarm, self-discipline of the user is important!

5 Future work

Besides audit efficiency enhancements through the use of some more suitable tools such as

- Tripwire to monitor file integrity instead of manually generating and verifying individual digital signatures, and
- Unix Nmap to be able to scan all ports, which Nmapnt can not do due to the bug mentioned above,

the area of the ZoneAlarm audit guidelines described above that would need most additional work is the issue of detecting transient changes in configuration and operation of ZoneAlarm, especially in usage scenarios where the user and the auditor are not identical and the user's security awareness can not be completely trusted. The proposed approach of manually reviewing the Windows security event log is not practicable. This leaves two basic approaches: Creation of an automatic analysis tool or modification of certain ZoneAlarm features – the latter can unfortunately only be realized by Zone Labs themselves in forthcoming versions of the program.

A log analysis tool would be fed the Windows security event log, the Windows application log, the Windows system log, and the ZoneAlarm log. It would then extract and reduce the amount of ZoneAlarm related entries currently generated in Windows security event log according to timestamps, patterns as described in Section 5.1.1.2.3, correlation with the two other Windows logs, e.g. to obtain indications of system startup and shutdown, and the information contained in the events to produce a number of ZoneAlarm relevant consolidated events. These could then be correlated with each other and with entries in the ZoneAlarm log to obtain an even small number of events indicating instances of policy violation such as

- shutdown of ZoneAlarm while on the network,
- start of ZoneAlarm after system startup, resulting in its inability to control applications started before, or
- temporary unauthorized modification (loosening) of the filter rule set.

The auditor could then concentrate his/her time and energy on investigating these isolated incidents, e.g. by interviewing the user and examining the system for anomalies manifesting themselves after this point in time of the incident.

© SANS Institute 2000 - 2005 Author retains full rights.

However, writing this kind of ZoneAlarm log auditing tool, especially if it should be reusable in different system configurations, would require a non-trivial effort and amount of experimentation with different systems.

The task of auditing a ZoneAlarm installation would be much easier if future versions of ZoneAlarm would incorporate some audit-friendly features:

- ZoneAlarm log entries of type “PE “entry should provide info about the actual decision made by the user.
- Changes of the configuration, modifications of the filtering rules, as well as startup and shutdown of the firewall should generate corresponding events for the ZoneAlarm log.
- The ZoneAlarm logger should use a special account for writing to the log so that modifications of the log by the normal, non-admin user can be prevented via file permissions.
- ZoneAlarm should not require user account write access to the rule base (IAMDB.RDB) during normal operation, so that the rule base could be locked down using Windows file permissions.

Another very worthwhile project, considering the user base of approximately 8 million for the ZoneAlarm firewall alone, would be an Open Source implementation of a personal firewall for Windows. Not only would this allow to easily add audit extensions as they become necessary, it would also create a personal firewall that can be trusted not to be malicious software itself, a concern that is these days, based on evidence of variable quality, repeatedly raised against various personal firewalls, among them ZoneAlarm [Malware].

References

[Nmapnt] Nmap network scanner port for MS Windows, http://www.eeye.com/html/Research/Tools/nmapnt.html

[Green3] John Green: Auditing networks with Nmap and other tools; Track 7 course notes, SANS 2001, Baltimore

[Green] John Green, Global Incident Analysis Center, Report of detects analysed 4/27/00; http://www.sans.org/y2k/042700.htm

[Green2] John Green, Global Incident Analysis Center, Report of detects analysed 4/30/00; http://www.sans.org/y2k/043000.htm

[Scarborough] Matt Scarborough, Global Incident Analysis Center, Reports of detects, 12/27/2000; http://www.sans.org/y2k/122700.htm

[ZoneLog] ZoneLog Zone Alarm Log Analyzer, http://www.zonelog.co.uk

[Leaktest] Steve Gibson: LeakTest Howto, July 07, 2001, http://grc.com/lt/howtouse.htm

[LTdownload] Steve Gibson: Leaktest, http://grc.com/files/LeakTest.exe

[Malware] Discussion about suspected malicious functionality in ZoneAlarm; thread on newsgroup comp.security.firewalls started on 2000/05/09 by message

© SANS Institute 2000 - 2005 Author retains full rights.

“Subject: Zone Alarm - I may have been WRONG!”

© SANS Institute 2000 - 2005 Author retains full rights.