Global Information Assurance Certification Paper

A simple and effective path to improving NT Security

Introduction

Many system/network administrators and users are often unaware that their systems have probably been compromised several times even before a real incident happens. According to a 2000 computer crime and security survey by Computer Security Institute, 27% of the respondents were unaware that unauthorized access or misuse has taken place.[1] Thus the methods and technology for prevention and detection are either absent or not effective.

Most organizations response to attacks have been to acquire security products such as firewalls and IDS. If planned and implemented properly, these are effective! Unfortunately, it is not without its drawbacks. As an example, IDS sensors must be placed in correct strategic locations. A proper period of 'adapting' to local environment is required to prevent false alarms, and alarms must be logged, analyzed and monitored carefully. And of course, the use of commercial IDS maybe beyond the budget and human resources of smaller organizations.

This paper will present ways where relatively cheap, accessible and easy to use security measures that can be performed on either workstations and servers. While they by no means replace the need for IDS or other security mechanisms, it does push security to the potential targets: individual workstations, servers and their users. To stretch it further, if the user workstations use the measures outlined in this paper (or even a selection of methods), every single user in the organization becomes a walking and talking IDS. Not only does this help to secure individual machines across an organization, security awareness is also raised and everyone feels involved as a security lookout; defending the fort!

The main criteria, becomes one of trying to find measures that are simple enough even for end-users or a busy system administrator. This can defer greatly from one organization to another. Nonetheless, this paper will present the technical measures that can be done. The only thing to note is that security is seldom effective without the cooperation of everyone in the organization. Everyone is a potential IDS. And that is worth more than the most expensive IDS.

Background

Audit guidelines do exist to help tighten security and reduce security risks on a desktop system or servers. At this present day, there are countless tightening measures that ought to be done by the system administrator. However, in reality such practices are often not carried out due to human nature to assume the best rather than the worst. Many relax after installing perimeter defenses such as firewalls and router filtering, assume that they are safe all attacks. More than often, malicious attackers keeping up-to-date with the latest discovered vulnerabilities found in system OS or software, exploit loopholes to gain access to internal network.

A few simple steps performed when setting up a fresh system would greatly reduce the chance of a machine being compromised if securing of the desktop is done correctly.

This document outlines some simple and effective steps to increase security on desktops/servers for NT platform using the basic tools already inherent in NT and freeware from the Internet

which are easy to implement and almost maintenance free. With proper action taken, these tools will help to shed light on what happened when an incident happens.

Some proposed steps to take :
There are some overlaps in function and may be selectively implemented according to needs. But security in depth is a good thing.

1. Enable Audit logs. (to check for unauthorized actions on computers)
2. Configure Security port filters (defend against unauthorized connections)
3. Tighten File sharing and remote access (prevent unauthorized access)
4. Customize account policy and enforce strong password policy (prevent unauthorized access)
5. Profiling a system (detect unauthorized filesystem changes)
6. Install virus scanner, host-based firewall and intrusion detection systems. (security defense packaged for the desktops)

1. Enable Audit logs

A very useful function provided by NT, is the audit logging within the User Manager administrative tools. With default setting of Windows NT™ installed, the audit options under the User Manager policies are disabled. It is often difficult to gather information from any compromised system after the incident if the audit logs were not switched on initially by the system administrator. Several events available for logging are shown below.

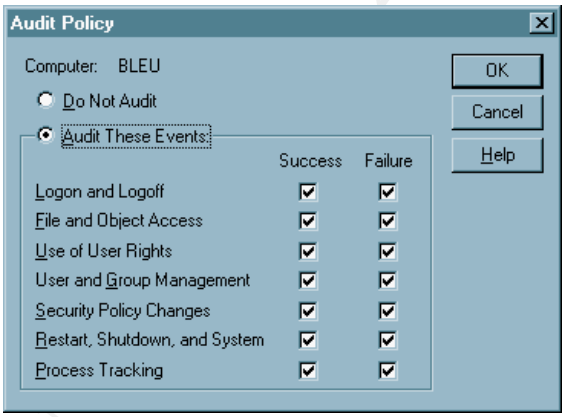


Figure 1 : Audit policy configuration window in User Manager

Naturally, the best would be to enable all the mentioned options but tradeoffs comes in huge logs taking up disk space. Especially for options like "File & Object access" and "Process Tracking". It is impractical on a daily operation and a fine balance should be drawn. An alternative would be to redirect the log files to remote monitoring station. Logs could be rotated or cleared on a regular basis and backed up to other media.

Unfortunately, in this "real" world, such functions are often not done and forgotten due to lack of skilled staff and appropriate equipment. With such limitations, a bare minimum would be to

switch on the audit logs for success and failures of all the options except for "File and Object Access" and "Process tracking".

Logging the success and failure of "Logon and Logoff" would provide clues to who has logged on and access to the computer. This is useful in conjunction with the logging of "Restart, Shutdown, and System". Several failure logon attempts, followed by a success and then restart of system with changes in security policy and user rights probably does give an good idea when the system has been compromised. A system administrator would be be able to detect such suspicious activity when checking the log files if there are any unauthorized changes in security policies and user rights.

2. Configure security port filters

A simple way to filter traffic to the NT server is available. Under advanced options in TCP/IP properties, an option to enable security on IP enables the user to enter the ports to filter for TCP, UDP and IP protocols.

This filters off unwanted connections. Settings (shown in Figure 2) could be customized to allow only a few well-known ports or any proprietary ports used by services on servers or clients to be opened for connection. E.g. http, telnet, ftp runs on famous ports such as 80, 23, 21. This method, though simple, is very effective in limiting unsolicited connections.

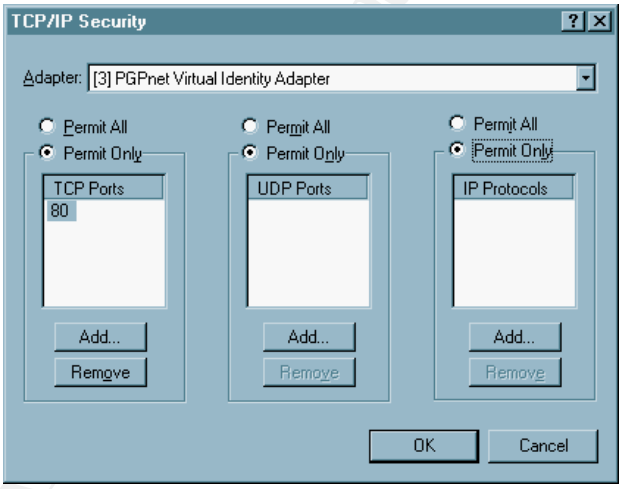


Figure 2: Port filters under TCP/IP Properties

3. Tighten file sharing and remote access

"NetBIOS (Network Basic Input/Output System) is a program that allows applications on different computers to communicate within a local area network ." [12] While NetBIOS has fast become the de facto standard on LANs for file and printer sharing, it poses as a security risk when configured incorrectly and no access control tightening has been applied.

A user connected to the Internet, might inadvertently expose share files on their own system to an outside world if the windows file sharing is enabled and binds to the IP protocol. [14]. Shares created with weak passwords or even with no passwords are a cause for concern as weak passwords can easily be cracked by common cracking tools. Malicious users may not only gain access to the machine, but also gain information on the system.

If file and printer sharing are necessary :

- Set control access to file shares needed by others. Create "shares" only for files or directory that are needed for sharing. Otherwise, disable File and Printer sharing. Unbind TCP/IP from file and printer sharing if using NetBEUI.

- Using strong passwords would prove a good deterrent. While the password for NetBIOS is not case sensitive, using characters mixed with numbers and non-existent word would prove to be rather difficult to break. Although one may reason that no password is safe enough with brute force guessing.

  However as noted in [13], "Even assuming 100 trials per second, and that an attacker would know what kind of attack to use, cracking a simple **two-word** password (*e.g.*, "rocktowel") with a minimal (64K) dictionary-based approach would take on the order of a **year or more of *continuous non-stop* attack** (probably much more)."

- Set ScopeID to limit this file sharing amongst the group of computers authorised for file sharing. It can be found under network TCP/IP properties Wins Address ScopeID.

  What ScopeID does is to "isolate a group of computers that only communicate with each other." [14] within the NetBIOS protocol (even when running over TCP). Using a character string value appended to the computer name, this provides extended naming service which serves to isolate NetBIOS traffic to those computers with identical Scope ID. Computers with different Scope ID will disregard packets from this computer.

4. Customize account policy and enforce strong password policy

A good password is a precondition to any computer security. As a saying goes - "A chain is only as strong as its weakest link". Weak passwords have always been the largest bane to computer security. Users often compromise their systems or accounts by using easy-to-guess words. Nowadays, hacker could easily brute-force crack a password by running a password file through dictionary templates and pattern matching. Increasing computing power also aids the speed in cracking a password.

Although users have often been advised to use strong passwords and keep them private and confidential. However, security breaches from stolen passwords or guessing are still very common. Hence, it is just as important for a system administrator to set a strong password policy as well as educating users on protecting their passwords. The right balance for the policy has to be where users would find it sufficiently easy enough to remember their password. And

not to write it down on slips of paper, attaching them to their desktops or leaving slips of paper with passwords in unlocked drawers.

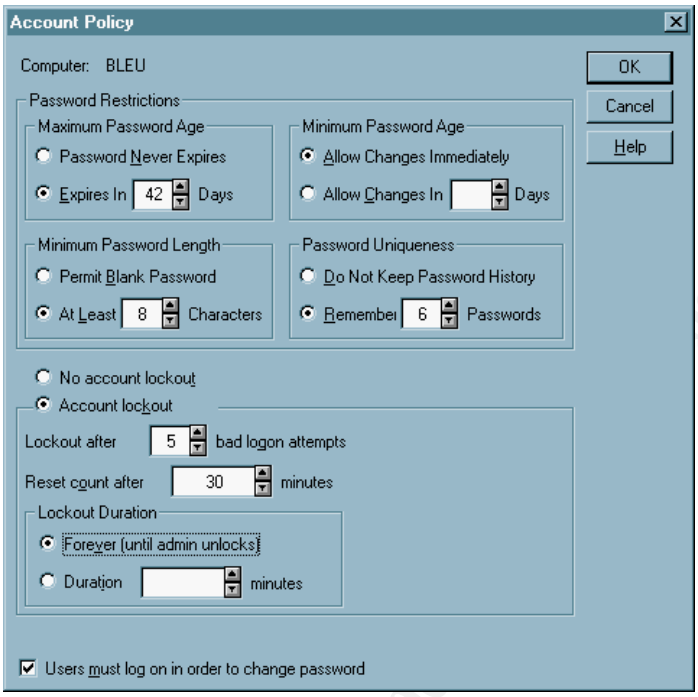


Figure 3 : Account Policy configuration window under User Manager

Figure 3 shows the account policy in NT User Manager window that allows the administrator to set the rules for the users. Depending on company security policy, the administrator may choose strategy appropriate to the company.

Some recommended steps are :

- First of all, install drivers like passfilt.dll which have been included in Microsoft NT Service pack 2, to strengthen password policy. The policy enforces minimum rules like password must not include the username or part of the username. It must be at least 6 characters long and must include 3 out of the 4 elements such as Upper case, lower case, numeric and special characters.
- Setting a password to expire in a period so as to encourage users to change their password from time to time. One that never expires isn't that attractive. It is impractical to assume that the password will always be secure.
- Keeping history of passwords require the user to use different password and NOT reuse old passwords repetitively. Good passwords used again and again are just as ineffective and insecure! A balance between security and user acceptance since keeping a long history of passwords would provoke strong reaction from users and results in some unable to come up with good passwords and forgetting them very often. A good history to keep before expiring would be 3 passwords. Then again it depends on the system administrator to enforce a policy that caters to the company's needs.

- Enforcing a minimal number of characters for the passwords. The longer the number of characters, the harder it is to crack. Combined it with special characters and non-dictionary words increase the time and difficulty to brute crack a password.
- Disabling generic accounts like guests to prevent unwanted logins.
- Remove all rights to the "administrator" account to set it up as a honeypot to alert the system administrator should there be unauthorized attempts to access that account. Create the real administrator account under another name.

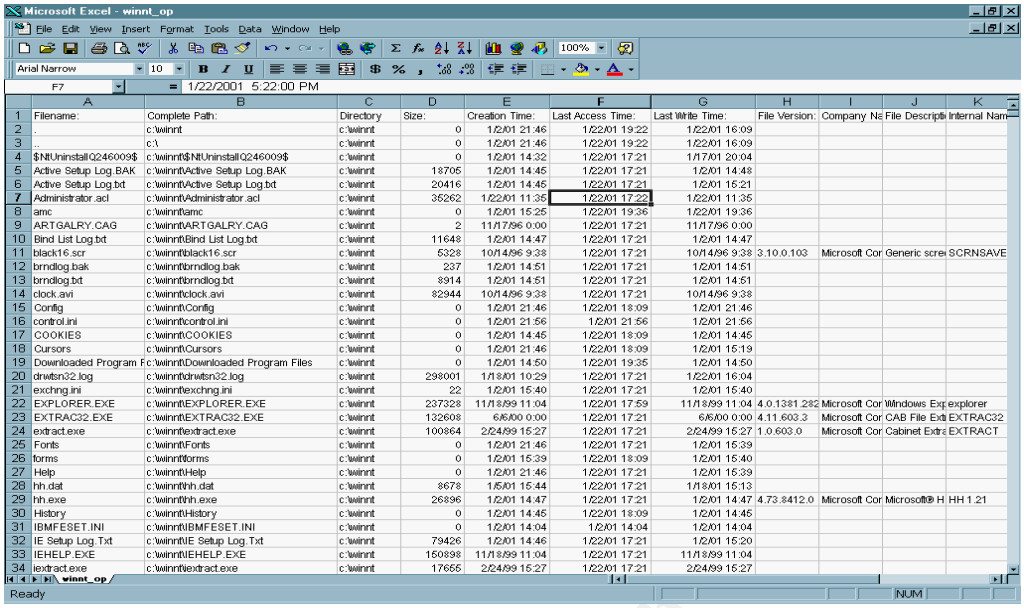
5. Profiling a system

Checking the integrity of file system is a way to determine whether certain files have been altered. Expert hackers would be adept in erasing their tracks, altering the audit logs and reinstalling their own versions of service files. File integrity check tools such as Tripwire™ and Intact™ comes in handy. By comparing MD5 checksums or SHA hashes of the files after the incident with a record of all the checksums of the files, one would be able to determine if the file has been tampered with. It is also a good way of detecting trojans that may have replaced the executable copy of a file with a modified one. Here is a brief overview of the tools that could be used to profile a system.

Versioner™
Versioner™ is provided as a freeware by Kirby Kuehl, it provides features such as last access time of the file, MD5 Hash, filename and pathname, Size and other file attributes. The results can be saved to an Excel spreadsheet and fed to database. It can then used for comparison with other similar results as a means to track changes to the file of a directory.

Figure 4 : Configure window for Versioner

Figure 5 shows a screenshot of the control panel of Versioner™. The program allows the user to just focus on a particular directory and scan for all the files. The output file can be specified as either a *.csv or *.txt. The screenshot below show the output after it has been imported into Microsoft Excel. A profile can be taken when the computer has been freshly setup and the results used as a baseline for comparison with any records in the future.



	A	B	C	D	E	F	G	H	I	J	K
1	Filename:	Complete Path:	Directory	Size:	Creation Time:	Last Access Time:	Last Write Time:	File Version:	Company Na	File Descripti	Internal Nam
2	.	c:\winnt	c:\winnt	0	1/2/01 21:46	1/22/01 19:22	1/22/01 16:09				
3	..	c:\	c:\winnt	0	1/2/01 21:46	1/22/01 19:22	1/22/01 16:09				
4	$NtUninstallQ246009$	c:\winnt\$NtUninstallQ246009$	c:\winnt	0	1/2/01 14:32	1/22/01 17:21	1/17/01 20:04				
5	Active Setup Log.BAK	c:\winnt\Active Setup Log.BAK	c:\winnt	18705	1/2/01 14:46	1/22/01 17:21	1/2/01 14:48				
6	Active Setup Log.txt	c:\winnt\Active Setup Log.txt	c:\winnt	20416	1/2/01 14:46	1/22/01 17:21	1/2/01 15:21				
7	Administrator.acl	c:\winnt\Administrator.acl	c:\winnt	35262	1/22/01 11:35	1/22/01 17:22	1/22/01 11:35				
8	amc	c:\winnt\amc	c:\winnt	0	1/2/01 15:25	1/22/01 19:36	1/22/01 19:36				
9	ARTGALRY.CAG	c:\winnt\ARTGALRY.CAG	c:\winnt	2	11/17/96 0:00	1/22/01 17:21	11/17/96 0:00				
10	Bind List Log.txt	c:\winnt\Bind List Log.txt	c:\winnt	11648	1/2/01 14:47	1/22/01 17:21	1/2/01 14:47				
11	black16.scr	c:\winnt\black16.scr	c:\winnt	5328	10/14/96 9:38	1/22/01 17:21	10/14/96 9:38	3.10.0.103	Microsoft Cor	Generic scree	SCRNSAVE
12	brndlog.bak	c:\winnt\brndlog.bak	c:\winnt	237	1/2/01 14:51	1/22/01 17:21	1/2/01 14:51				
13	brndlog.txt	c:\winnt\brndlog.txt	c:\winnt	8914	1/2/01 14:51	1/22/01 17:21	1/2/01 14:51				
14	clock.avi	c:\winnt\clock.avi	c:\winnt	82944	10/14/96 9:38	1/22/01 17:21	10/14/96 9:38				
15	Config	c:\winnt\Config	c:\winnt	0	1/2/01 21:46	1/22/01 18:09	1/2/01 21:46				
16	control.ini	c:\winnt\control.ini	c:\winnt	0	1/2/01 21:56	1/2/01 21:56	1/2/01 21:56				
17	COOKIES	c:\winnt\COOKIES	c:\winnt	0	1/2/01 14:45	1/22/01 18:09	1/2/01 14:45				
18	Cursors	c:\winnt\Cursors	c:\winnt	0	1/2/01 21:46	1/22/01 18:09	1/2/01 15:19				
19	Downloaded Program F	c:\winnt\Downloaded Program Files	c:\winnt	0	1/2/01 14:50	1/22/01 19:35	1/2/01 14:50				
20	drwtsn32.log	c:\winnt\drwtsn32.log	c:\winnt	298001	1/18/01 10:29	1/22/01 17:21	1/22/01 16:04				
21	exchng.ini	c:\winnt\exchng.ini	c:\winnt	22	1/2/01 15:40	1/22/01 17:21	1/2/01 15:40				
22	EXPLORER.EXE	c:\winnt\EXPLORER.EXE	c:\winnt	237328	11/18/99 11:04	1/22/01 17:59	11/18/99 11:04	4.0.1381.282	Microsoft Cor	Windows Exp	explorer
23	EXTRAC32.EXE	c:\winnt\EXTRAC32.EXE	c:\winnt	132608	6/6/00 0:00	1/22/01 17:21	6/6/00 0:00	4.11.603.3	Microsoft Cor	CAB File Extr	EXTRAC32
24	extract.exe	c:\winnt\extract.exe	c:\winnt	100864	2/24/99 15:27	1/22/01 17:21	2/24/99 15:27	1.0.603.0	Microsoft Cor	Cabinet Extra	EXTRACT
25	Fonts	c:\winnt\Fonts	c:\winnt	0	1/2/01 21:46	1/22/01 17:21	1/2/01 15:39				
26	forms	c:\winnt\forms	c:\winnt	0	1/2/01 15:39	1/22/01 18:09	1/2/01 15:40				
27	Help	c:\winnt\Help	c:\winnt	0	1/2/01 21:46	1/22/01 17:21	1/2/01 15:39				
28	hh.dat	c:\winnt\hh.dat	c:\winnt	8678	1/5/01 15:44	1/22/01 17:21	1/18/01 15:13				
29	hh.exe	c:\winnt\hh.exe	c:\winnt	26896	1/2/01 14:47	1/22/01 17:21	1/2/01 14:47	4.73.8412.0	Microsoft Cor	Microsoft® H	HH 1.21
30	History	c:\winnt\History	c:\winnt	0	1/2/01 14:45	1/22/01 18:09	1/2/01 14:45				
31	IBMFESET.INI	c:\winnt\IBMFESET.INI	c:\winnt	0	1/2/01 14:04	1/22/01 14:04	1/2/01 14:04				
32	IE Setup Log.Txt	c:\winnt\IE Setup Log.Txt	c:\winnt	79426	1/2/01 14:46	1/22/01 17:21	1/2/01 15:20				
33	IEHELP.EXE	c:\winnt\IEHELP.EXE	c:\winnt	150898	11/18/99 11:04	1/22/01 17:21	11/18/99 11:04				
34	iextract.exe	c:\winnt\iextract.exe	c:\winnt	17665	2/24/99 15:27	1/22/01 17:21	2/24/99 15:27				

Figure 5 : Results imported into Excel spreadsheet format

Chk-Safe

While it may be useful to install a file integrity checker, a nifty command-line tool written by Don Peters, Robert Bullock, Bill Lambdin called "Chk-Safe" that computes the MD5 hash sums of a particular file or directory, proves to be extremely handy.

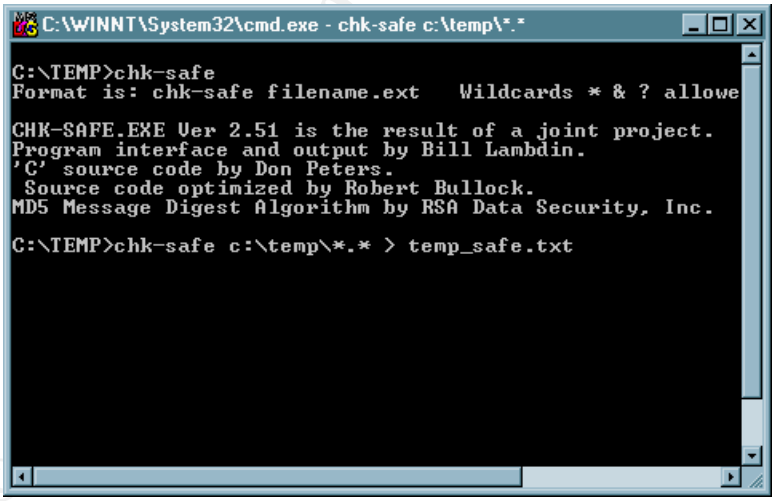


Figure 6 : Running the chk-safe from the command line window

Figure 6 shows the DOS command prompt print. The program allows user to scan another directory and redirecting it to a text file for viewing. Figure 7 shows the results. The program is DOS based and results can be saved to a text file. This program is highly portable, as it is very small and can fit nicely into a floppy diskette and just used without having to install it on a system.

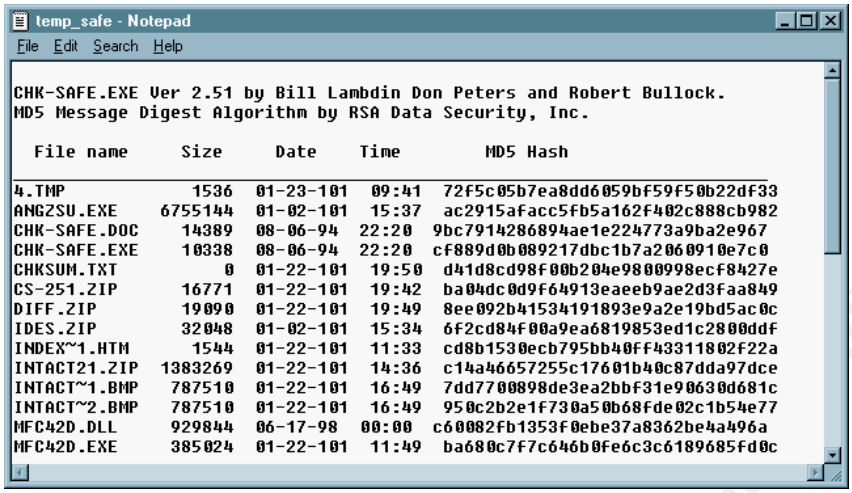


Figure 7 : Text file output of chk-safe with all the MD5 hash

Checking the file system integrity is only useful if the administrator profiled the system when the computer was freshly setup. If this has been done, even without IDS installed or logs enabled, comparing with a baseline profile could check integrity of a file system.

System Integrity checkers

A system integrity checker would be able to track changes in registries, files and security settings in SAM. Changes made to registry or any security settings are channeled to a file as shown below in an example of a system integrity checker, Intact™ . Intact comes as a freeware but provides extra features at an extra cost.

Intact

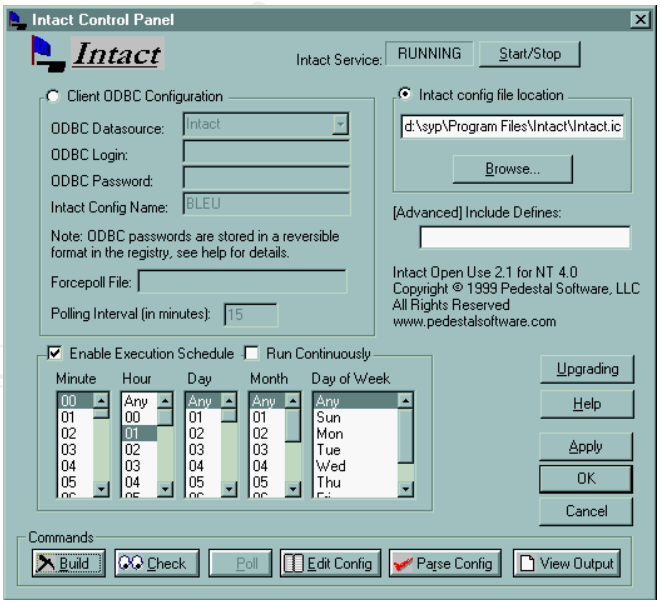


Figure 8 : Control Panel of Intact

Figure 8 shows the configuration panel of the program. The user first builds a database of the system profile. This provides a baseline of the system that will be checked against as and when the user schedules it.

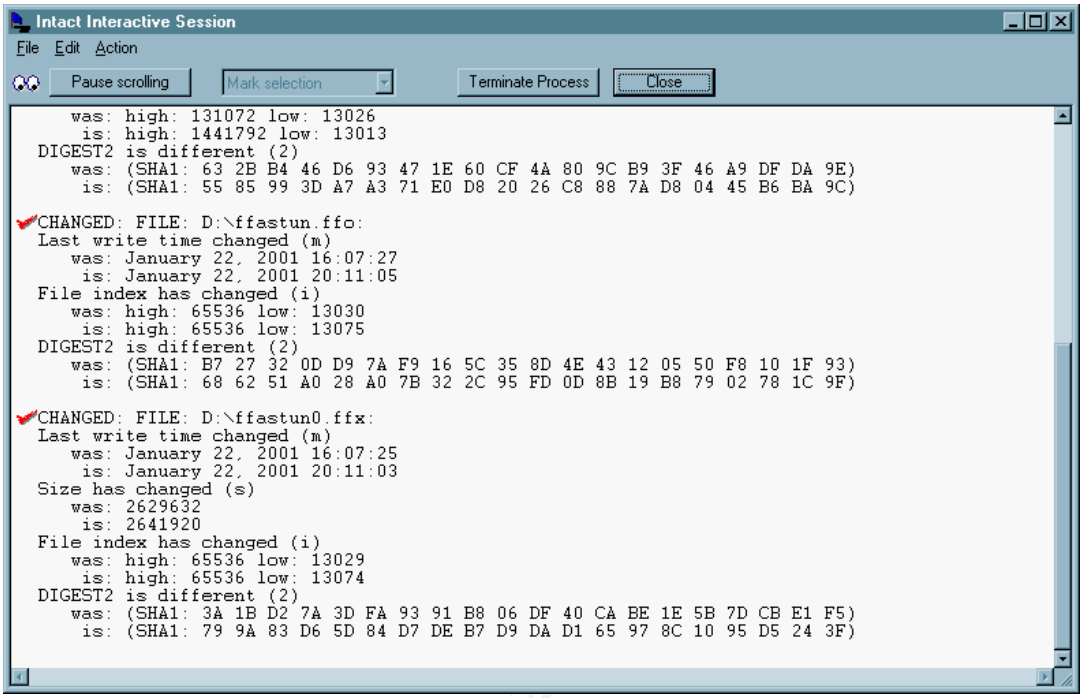


Figure 9 : Output screen from Intact after running a scan presents the files that has been changed since the last profile was taken.

Figure 9 shows the output when a scheduled check was run and the program upon comparing the MD5 hashes presents the results which shows all the files changed. The results also include registry changes. Hence a check can be made on SAM entry in the registries to see if it has been changed even if the administrator has not made any policy changes.

Some files which would be good to monitor would be :

- Windows SAM settings
- Startup files
- Changing Network Configuration Settings
- Windows NT / system32

6. Installing Virus Scanner and Host-based Intrusion Detection System and Firewall

Virus Scanners

With computer virus becoming so rampant, it is unimaginable that any system should go without an anti-virus installed. As reported in the 2001 Computer crime and security survey, an alarming "94% of the respondents detected computer viruses"[1]. Most of the systems are connected to a

network and the rate at which a virus spreads has been increasing due to greater interconnectivity between computers.

Currently, operating systems does not provide the feature of virus scanning and such products has to be downloaded from the Internet or purchased. However, this is one good way of keeping the system free from Trojans and malicious codes that could delete or destroy important information and anyone should consider investing in such a product. Apart from choosing good anti-virus software with good support – that has frequent updates on virus signature files, the onus is on the system administrator to keep the anti-virus software updated with the latest signatures.

Common ways of virus, worms or Trojans injection are through e-mail, opening infected attachments, floppy diskettes and Internet. Here are some steps you could take apart from installing anti-virus software and keeping up to date:

- For systems that doesn't require a floppy, it should be disabled to prevent unwitting users from running infected files on that system. Macro virus are often spread this way by infecting the template.
- On systems that doesn't require emails, remove email programs such as Outlook which has become a HUGE target for worms.
- The virus scanner should be configured to scan all the files that are being downloaded to the machine as well as scan for all the files that are being run. Set schedule for daily scans of systems.
- Sometimes, it is necessary to combine a personal firewall integrated with intrusion detection systems and an anti-virus software. As in the case of Trojans, the personal firewall would be able to stop any unsolicited connections or outflow of traffic and alerts the user.

Vendors such as Mcafee and Norton have released versions of their security package software that combines virus scanner with personal firewall and intrusion detection systems.

The following section takes a look at a free firewall software ZoneAlarm™ by Zone Labs that is available for download from their website at http://www.zonelabs.com to home users and academic users. A more feature-rich `version is available to business users.

ZoneAlarmÔ

This host based firewall is compatible with all Windows platform and offers simple user interface with auto-configuration of rules. For all attempts to access the Internet, a pop up box will prompt the user if this program is allowed access.

- **Alerts** : Shows attempts by programs to access the internet but was stopped by the firewall. Alerts are channeled to a text file that could be checked for unauthorized access.

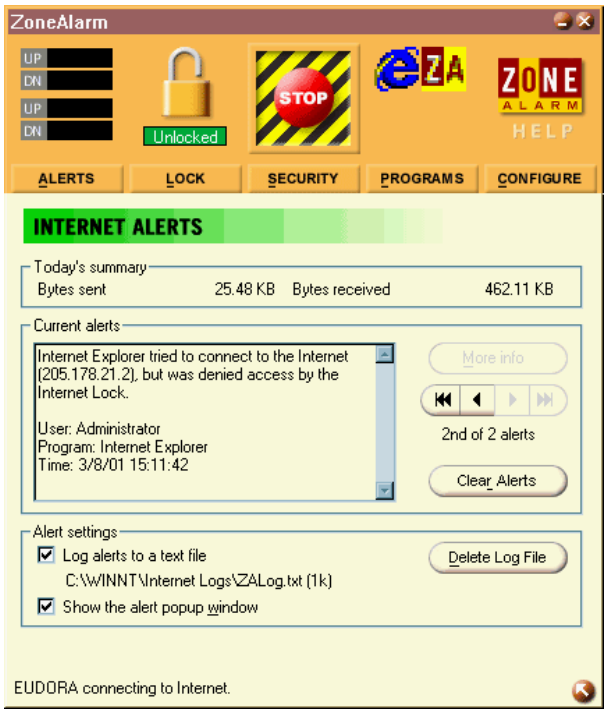


Figure 10 : Alerts and Lock Tabs

Lock : Sets a lock on internet connections and may allow the user to choose if they allow programs to continue to access internet or totally block all connections.

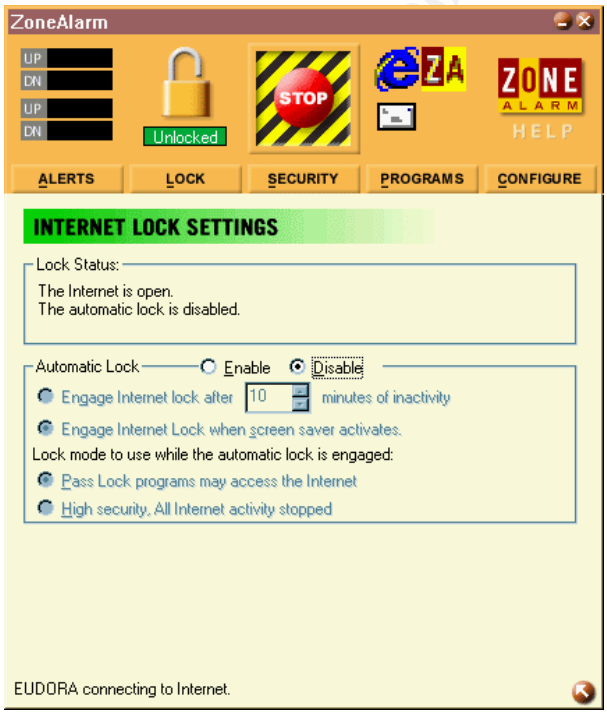


Figure 11 : Lock Settings

- **Security** : Different security settings could be configured for local or Internet access. Advanced options are only available to the paid version of this software which includes advance firewall control that allows more customized configuration.

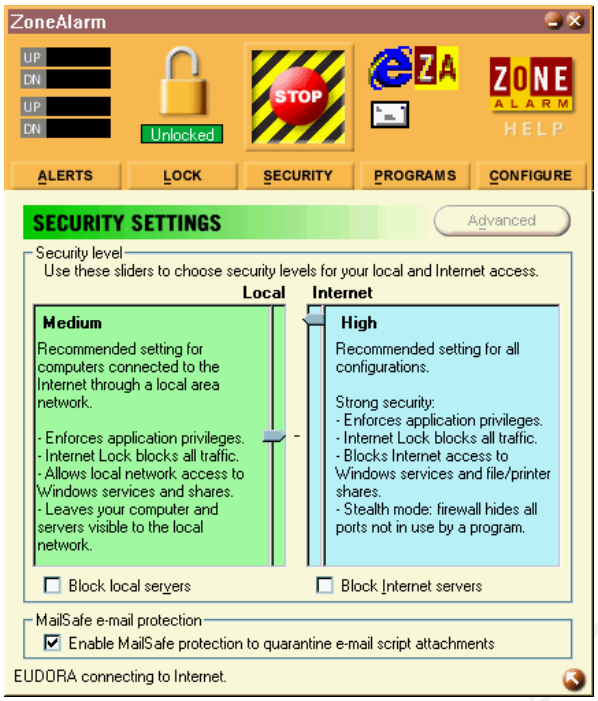


Figure 12 : Security Tab

- **Programs** : Shows all the programs which attempts to access the Internet. Allows user to deny or allow the connection.

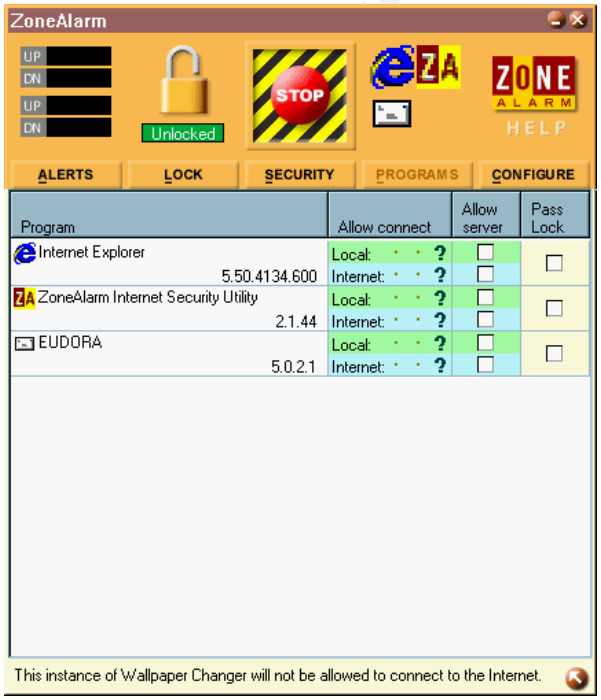


Figure 13 : Programs Tab

- **Configure** : General settings for the program.

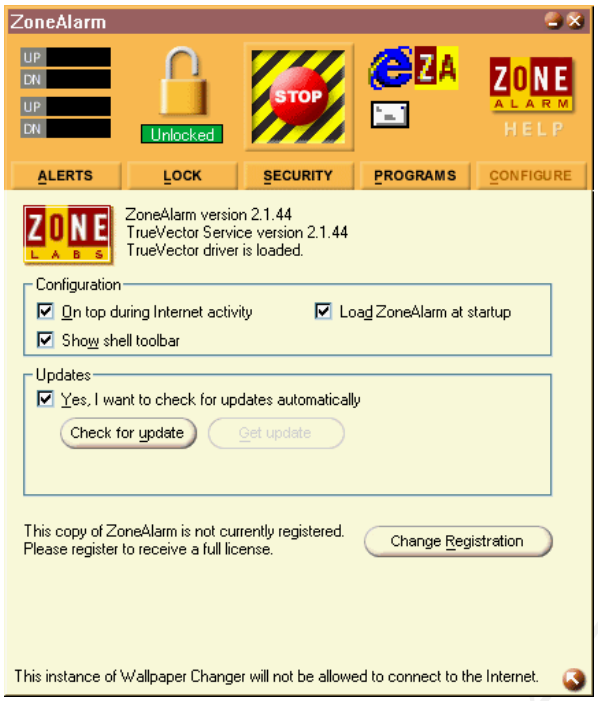


Figure 14 : Configure tab

Conclusion

In any computer network, it is a joint-effort of both the system administrators and users to ensure that their network security is not compromised by irresponsible behavior of computer resource misuse and negligence. Steps described above provide simple and effective security measures for NT systems.

Bibliography

1. Computer Security Institute and San Francisco Federal Bureau of Investigation "2001 Computer Crime and Security Survey" URL : http://www.gocsi.com/prelea_000321.htm (19th March 2001).
2. Versioner Tool, http://www.datanerds.net/~vacuum/versioner/ (23 Jan. 2001)
3. Hurwicz, Michael. "Cracker Tracking: Tighter Security with Intrusion Detection", May 1998. URL:http://www.byte.com/art/9805/sec20/art1.htm (23 Jan. 2001)
4. Cooper, Mark. "An Overview of Intrusion Detection Systems" URL:http://www.xinetica.com/tech_explained/general/ids/wp_ids.html (26 Jan. 2001).
5. Fred Cohen & Associates. "Intrusion Detection and Response" URL: http://www.all.net/journal/ntb/ids.html (29 Jan. 2001).
6. Panagiotis Astithas. "Intrusion Detection Systems"URL:http://www.daemonnews.org/199905/ids.html, May 1999 (29 Jan. 2001).
7. Meinel, Carolyn . "The ABCs of IDSs (Intrusion Detection Systems)" URL:http://www.messageq.com/security/meinel_2.html . (29 Jan 2001).

8. Carnegie Mellon Research Institute "State of the Practice of Intrusion Detection Technologies." CMU/SEI-99-TR-028, ESC-TR-99-028, January 2000.
URL:http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028chap03.html (29 Jan 2001).

9. Turcato, Lance M. "Audit work program - Windows NT", 1998.
URL:http://www.sfisaca.org/oldfiles_not_in_use/NTpgm.htm (19th Mar 2001).

10. 101 Security Solutions "Intrusion Detection and Vulnerability testing tools : What works ?" , 8 Nov 2000. URL: http://www.101com.com/securitysolutions/article.asp?ArticleID=1826 (19 Mar 2001).

11. Malmgren, Robert. "NT Security - Frequently Asked Questions version 0.41", 1996, 1997. URL : http://www.it.kth.se/~rom/ntsec.html (19 Mar 2001)

12. What is ? Com. "NetBIOS" URL:http://whatis.techtarget.com/WhatIs_Definition_Page/0,4152,212633,00.html (19 Mar 2001)

13. The Navas Group. "File and Printer Sharing (NetBIOS) Fact and Fiction", 1999 - 2001. URL : http://cable-dsl.home.att.net/netbios.htm (19 Mar 2001)

14. "ScopeID" http://support.microsoft.com/support/kb/articles/Q138/4/49.asp (19 Mar 2001)

15. Ivens, Kathy. "Managing Windows NT Logon" Chapter 2 - Password Problems, Jan 2001. URL : http://www.oreilly.com/catalog/ntlogon/chapter/ch02.html (19 Mar 2001)

16. Duke Communications International Inc. "Chapter 9 Attacking your own NT networks - Password Crackers and Grabbers" Internet Security on Windows NT, 2000. URL:
http://www.sure.org.ru/docs/hack/ntsecur/page.asp-id=-ch9toc.htm#9 (19 Mar 2001)

17. http://www.zonelabs.com(19 Mar 2001)

18. Microsoft support. "Passfilt.dll", Dec 2000. URL :
http://msdn.microsoft.com/library/psdk/logauth/pswd_about_9x7w.htm, (19 Mar 2001)

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event