Global Information Assurance Certification Paper

Host-Based Vulnerability Assessments using *e*Trust
Written By: William Bloom
February 2002, version 1.3

I. Introduction

The number of computer vulnerabilities reported to Carnegie Mellon's Emergency Response Team (CERT) more than doubled from 1,090 vulnerabilities in the year 2000 to 2,437 vulnerabilities in the year 2001 (1). Furthermore, in recent months, there has been a heightened awareness and increased attention to the threat of attack against networked infrastructures by hackers, criminals, and others. The demand for tools and services that assist administrators and managers in identifying and analyzing network vulnerabilities has increased. Accompanying this heightened demand is the growing problem of how to evaluate the various vulnerability assessment tools and services offered against an organization's goals and expectations. There are two types of vulnerability assessments; network-based and host-based. Network-based assessments focus on scanning network devices and host-based assessments focus on individual systems and applications. Network vulnerability assessments are run from a remote host on the network, whereas, host based vulnerability assessment are run on the machine being assessed. This paper will provide a limited overview of a small number of host-based vulnerability assessment tools on the technology market today and select one tool to further describe its features and benefits.

In order to provide an adequate defense-in-depth security strategy, Information Security departments should consider using both types of vulnerability assessments. A company's security policy should address the overall security of a number of issues including operating system components, network security, user account and password management, and file system protection. When evaluating either host-based or network-based vulnerability assessment tools, some criteria that should be considered are the ability to identify potential security risks, an indication of how your system configurations measure up to your own standards as well as industry best practices, and it should make the necessary recommendations to address any discrepancies.

II. Host-Based Vulnerability Product Descriptions

There are numerous host-based vulnerability assessment tools available today that cover a wide-range of systems and platforms. These tools range from freeware to commercial products; however, this section will focus on commercial host-based vulnerability assessment products, which include Computer Associates' *e*Trust Policy Compliance, Symantec's Enterprise Security Manager, and PentaSafe Security Technologies' VigilEnt Security Agents. There are several other host-based vulnerability assessment vendors, however, for purposes of this discussion, I limited my overview to only three.

eTrust Policy Compliance (PCM) - reduces the cost and complexity of managing system security and delivers accelerated return on investment by providing a comprehensive security risk control solution that identifies potential policy vulnerabilities, recommends corrective actions, facilitates their resolution, and closely monitors system activity to prevent their recurrence. This enables security administrators to address inadequate security policies within their system environment. This product is compatible with the following system platforms: Windows NT, various flavors of UNIX, Oracle, Apache, Open VMS, and Windows 2000 (5). PCM currently searches for more than 2000 vulnerabilities. PCM provides a tiered pricing model, so the total price depends on

how managers and agents your organization would need and how many different platforms PCM would scan.

Enterprise Security Manager (ESM) – gives security administrators the ability to manage and control a company's security policy from one workstation. ESM includes a Graphical User Interface (GUI) that makes it easy to configure, manage, and report on security policy compliance (7). ESM comes equipped with industry best practice security settings to get you up and running quickly. However, it also lets you customize policies to meet the specific security needs of your organization. This product is compatible with the following system platforms: Windows NT, OS-390, AS-400, Windows 2000, NetWare, Linux, Solaris, and other flavors of UNIX (8). It currently searches for more than 2,200 vulnerabilities and prices start at $1995 per ESM manager.

VigilEnt Security Agents (VSA) – saves time while improving overall security by enabling you to audit, detect, and secure multiple servers from a central point of control. The built-in security base line is particularly useful in helping administrators balance risk and performance in order to properly implement security controls on mission-critical systems (6). This product is compatible with the following system platforms: Windows NT, Windows 2000, Netware, Linux, UNIX, Solaris, BEA, Oracle, Sybase, IIS, apache, Netscape (8). Prices start at $795 per platform and the number of vulnerabilities this product searches for varies by platform.

III. Host-Based Assessments using *e*Trust Policy Compliance

Based on my research results of these commercial vulnerability assessment tools, I selected *e*Trust Policy Compliance (PCM) to further describe how it performs a host-based vulnerability assessment. This assessment will focus on the Windows NT operating system. Although Policy Compliance checks for common vulnerabilities on each operating system, it also checks for vulnerabilities specific to that operating system, as well. This assessment tool begins by evaluating the mechanisms established to secure the operating system and related components. Next it looks at the network programs that can provide unexpected access to your system. It then performs an analysis of accounts, highlighting potential weaknesses. Passwords, as the true keys to the system, are investigated in detail next. To conclude, the review evaluates the degree to which data is protected. This section will also define the specific security risks and assessment criteria used by Policy Compliance to check for vulnerabilities that you may find in the Windows NT operating system.

A. Windows NT Operating System

Policy Compliance (PCM) focuses on these key areas within Windows NT when conducting a vulnerability assessment: **1**-System Analysis, **2**-Network Analysis, **3**-User Account Analysis, **4**-Password Analysis, **5**-User Access Rights, **6**-Windows System Policy, and **7**-Windows System-wide User Policy.

1. System Analysis

The security of the operating system itself is important to limiting the security of the system as a whole. If the operating system can be modified, either accidentally or otherwise, the security of the entire system is at risk. The issues that are addressed here concern the protection of system

files and directories, as well as the ownership and permission settings for system objects such as devices and queues.

1.1. Registry Protection - The Registry Editor allows users to review and, depending on access rights, modify Registry entries, such as REGEDIT.EXE or REGEDT32.EXE. Regardless of the care used in setting appropriate access rights for the Registry Editor, if copies of these executable files are left on the system, it provides an avenue of access for a destructive intruder. PCM checks to see that no copies of these executables are found on the system.

1.2 Registry Access Control - Depending on the access rights given them, users could change access rights, create sub keys, delete, set new values for, or create links to critical keys in the Registry, potentially subverting system security. To protect the integrity of the system, it's critical that administrators carefully monitor and control which users have which types of access to the keys in the Registry. PCM checks critical Registry keys in the registry hive and all of their sub keys to ensure that none have inappropriate or excess permissions:

1.3 System Files - Improper ownership and inadequate protection of system files increases the likelihood of unauthorized modifications to the operating system. The subdirectories in critical system directories are checked by PCM for incorrect or excessive permissions, especially the "Everyone" group having more than read access or files in FAT file systems.

1.4 Services - Services present a security risk because most are installed by default. Running nonessential services can present another place for an unauthorized user to attack. The system is checked to see if the following services are running: Alerter, Directory Replicator, Messenger, NetLogon, NTLM Security Support Provider, and Schedule. When Directory Replicator is running, a check is made to ensure that it is running under the Replicator account. When Schedule is running, a check is made to ensure that it is running under the Scheduler account.

2. Network Analysis

Today's systems are usually made up of networked computers. Most systems are connected to other computers through a LAN, WAN, or a global enterprise network that includes remote access through dial-in and the Internet. While these connections make data sharing easy, they also make the data vulnerable to accidental or intentional disclosure, corruption, or misuse.

2.1 All Shared Directories – The shared directory permissions determine if and how a user group can access a shared directory. The default permission for a share is to grant full control to the "Everyone" group. Full control lets users create, modify, and delete files and subdirectories as well as create and modify NT File System (NTFS) file permissions and take ownership of NTFS files and directories. PCM identifies all drives and directories that are marked as shared on the target host, regardless of whether they are hidden or not.

2.2 Hidden Shares – Because hidden shares are shares made available to other administrators, including those on remote systems, they should be closely monitored. PCM identifies all resources that are marked as shared on the target host and that are hidden.

2.3 Shared Printers – Shared printers present a risk in that a user with access to a shared printer can print any file or document on it. PCM identifies all print queues that are marked as shared on the target host.

2.4 User-Visible Shared Directories – The default permission for a share is to grant full control to the "Everyone" group. Full control lets users create, modify, and delete files and subdirectories as well as create and modify NTFS file permissions and take ownership of NTFS files and directories. PCM identifies all drives and directories that are marked as shared and not marked as hidden. These directories are visible to other networked systems and users.

2.5 World-Accessible Shared Objects – Because shares are defined points of entry to the system, they provide not only entry for appropriate users, but also an attractive target for intruders. PCM identifies all directories, printers, communication devices, and IPC's marked as shared on the target host and accessible to everyone.

3. User Account Analysis

User names represent the accounts by which users gain access to the system. They contain the information that identifies a user in the Windows environment. User account security includes uniquely identifying accounts, setting appropriate password policies, and ensuring that users have only the permissions they need for using the system and accessing resources. Accounts that have excess privileges, that are not needed, or that have been given unnecessary access present a potential risk to the security of the system.

3.1 Account Policy - Nonstandard account policies can seriously impact the security of your system. The account policy settings should be appropriate to your security policy, which should address the following:

- **Minimum password length** - The minimum length required for passwords. A security policy that requires passwords to be at least 8 alphanumeric characters is recommended. The value should never be 0, which allows blank passwords.

- **Minimum password age** - The minimum number of days that a user's password must exist before the user can change it. A security policy that requires passwords to exist for at least 1 day is recommended. The value should never be 0, which allows passwords to be changed immediately, defeating any password uniqueness policy.

- **Maximum password age** - The maximum number of days a password can be used before it must be changed. A security policy that requires password changes at least every 60 days is recommended. The value should never be 0, which means that the password never expires.

- **Password uniqueness** - The number of unique passwords an account must use before a particular password can be repeated. A security policy that requires between 6 and 12 unique password changes before a password can be reused is recommended. The value should never be 0, which allows a user to "change" the password to the same value.

- **Account lockout** - Whether user accounts are locked out after a certain number of failed login attempts. A security policy that enables account lockouts is recommended.

- **Failed login attempts** - When account lockouts are enabled, the number of failed login attempts that are allowed before the account is locked out. A security policy that allows no more than 3 failures is recommended.

- **Lockout reset period** - The number of minutes that must elapse between login attempts before the failed-logins counter is reset. A security policy that resets the failed-logins counter after no less than 24 hours is recommended.

- **Lockout duration** - The length of time that a locked-out account remains locked out. A security policy that sets lockout duration to "forever", which requires that a system administrator reset the locked-out account before it can be used is recommended.

PCM will scan, evaluate, and identify any user accounts that are not in compliance with the aforementioned user account policies.

3.2 Guest Account - By default, Windows creates a special guest account called "Guest", which can be used by multiple users. Since more than one person can use the "Guest" account, it poses a security risk by making it difficult to isolate who took a specific action or caused a specific event. PCM checks to see whether or not the "Guest" account exists on the system

3.3 Accounts with Guest Privileges - Accounts are typically assigned to the "Guests" group to limit the rights and privileges of those accounts. These may be temporary accounts set up to allow a group of users limited access for a short period of time. It is important that accounts assigned to the "Guests" group are not also assigned to other groups through which they inherit less restrictive privileges, especially the privilege to change user passwords. The global password-change privilege should be reserved only to accounts for which it is appropriate. PCM counts the number of accounts on the system that are members of the "Guest" group.

3.4 Accounts with Missing Descriptions, No Full Name, or No Home Directory – Accounts created without descriptions, no full user name, or no home directory may indicate that these accounts were created without proper authorization, or, they were created for illegitimate purposes. PCM identifies missing information that may help you audit the validity of accounts in order to assess whether these exceptions were properly authorized or if accounts were created for illegitimate purposes.

3.5 Automatic Logon - Permitting anyone to access a system and the network to which it connects without providing authentication is a serious security breach. Even if the computer is in a secured area, a disgruntled employee could turn it on and perform any tasks the authorized account is allowed to perform. There is no accountability and no means to trace the actions back to a specific user. PCM checks to see if automatic logins have been enabled.

3.6 Disabled Accounts - Disabled accounts cannot be used to access the system and thus do not pose an immediate security concern. However, care should be taken that any files owned by these accounts remain unavailable to users other than the Administrator in case the account is enabled for any reason. PCM counts the number of accounts on the system that are disabled.

3.7 Expired Accounts - Expired accounts cannot be used to access the system and thus do not pose an immediate security concern. However, if the Administrator account were breached, these accounts could be enabled and the files owned by these accounts could be exposed to unauthorized use. PCM counts the number of accounts on the system that are expired.

3.8 Locked Accounts - Locking out user accounts after a specified number of failed login attempts are consistent with best security practices and should be part of your security policy. Although a failed login can be simply the result of a user forgetting the account password, it can also indicate a cracker attempting to guess account passwords. If the account is not locked out, the cracker can continue to try cracking the password forever. Since lockout records are removed once the administrator resets the user's password, a large number of locked out accounts could indicate a concerted password-cracking attempt. PCM counts the number of locked out accounts on the system.

3.9 Login Failures - A high number of failed login attempts could indicate a concerted password-cracking attempt. PCM compares the number of login failures to the total number of accounts on the system.

3.10 Never-Expire Accounts - Never-expire accounts are accounts with no expiration date. Accounts that never expire pose a potential security risk to your Windows system. PCM counts the number of accounts on the system that never expire.

3.11 Never-Used Accounts - Accounts that have not been logged into since they were created can provide easy access for intruders. PCM counts the number of accounts on the system that have never been used.

3.12 Accounts with No Time Restrictions - Restricting access to user accounts to normal business hours limits your exposure to off-hours intruders or crackers, as well as to authorized users who may be abusing their privileges. PCM counts the number of accounts on the system that have no time restrictions.

3.13 Old Accounts - Dormant accounts can provide easy access for intruders since no one is paying attention to them. The presence of old or unused accounts increases the potential for security breaches that could compromise the system. PCM counts the number of accounts on the system that have not been used for more than a specified number of days.

3.14 Privileged Accounts - Privileged accounts are accounts that have Administrator privileges. This includes the Administrator account and any accounts that belong to the Administrators group. Because of the power given to members of the Administrators group, you should carefully limit its membership. The privileges granted to these accounts make them prime

targets for intruders. PCM counts the number of accounts on the system that are members of the Administrators group.

3.15 Unprotected User Files - Protection applied to individual files and directories is the last line of defense against casual attacks. Any files or directories that allow write access by the global "Everyone" group puts the contents of that file or directory at risk. PCM counts the number of files in users' home directories that allow write access by the global "Everyone" group.

4. Password Analysis

In most organizations, the user ID conforms to an enterprise standard (i.e. last name, first name, employee number), which means that only the password really protects the account.

4.1 Expired Passwords - The longer a password remains on an account, the more time a cracker has to attempt to guess it and gain unauthorized access to your system. PCM finds active user accounts whose passwords are older than the password maximum specified by your password aging policy as specified in the User Manager.

4.2 Locked Passwords - Windows administrators can specify that a user does not have to change their password. By doing this, there is limited accountability for accounts whose password remains the same for long periods of time and they may become susceptible to cracking. PCM finds accounts with locked passwords.

4.3 Password Aging - Users should not be required to change passwords so often that they have trouble remembering the new password, but they should not be allowed to change passwords repeatedly in a short length of time. This defeats your password uniqueness and password aging policy by allowing the user to run through a series of password changes quickly, effectively retaining the original password. PCM reports the number of passwords that do not comply with the password aging criteria specified for the report.

4.4 Passwords Not Required - An account without a password is an open door to anyone who wants to gain access to a system. These accounts are even more dangerous if they are members of the "Administrators" group. PCM counts the number of accounts that allow blank passwords.

5. User Access Rights

User access rights let administrators specify the permissions a user account has with fine granularity. There are two groups of user rights: standard and advanced.

5.1 Standard User Access Rights - The following table lists the standard user access rights for Administrators, Domain Users, Server Operators, Account Operators, Print Operators, and Backup Operators. Some of the user access rights are potential security risks and should only be granted to trusted individuals. PCM reports the number of inappropriate accounts that have each access right. An account is considered inappropriate if it does not belong to one of the groups listed in the table for that access right.

Administrators - Add workstation to domain, change system time, access computer from the network, back up files and directories, force shutdown from remote system, logon locally, manage audit and security logs, shut down the system, take ownership of files and other objects, remove computer from docking stations, and mark accounts trusted for delegation.
Domain Users - Access computer from the network.
Server Operators - Access computer from the network, logon locally, shut down the system.
Account Operators - Access computer from the network, shut down the system.
Print Operators - Access computer from the network.
Backup Operators – Access computer from the network, back up files and directories, logon locally, and restore files and directories.

6. Windows System Policy

Windows System Policy settings apply to the Windows system as a whole rather than to a user of the system. These settings control the proper behavior of your Windows server.

6.1 Allow Network Connection Components - This setting determines how the system responds when a user tries to install device driver files that are not digitally signed. Installing unsigned drivers, or not knowing that the system can install unsigned drivers, might result in the installation of malicious drivers and worms. PCM checks the state of the device drivers. The minimum setting should be "Warn."

6.2 Disable Automatic Update of ADM Files - This setting prevents the system from updating the Administrative Templates source files automatically when you open "Group Policy". When applying policies, one might not be aware of changes that could result in the application of a different policy than expected. PCM checks whether automatic update of ADM files is disabled.

6.3 IP Security Policy Processing - This setting determines when IP security polices are updated. This policy affects all policies that use the IP security component of Group Policy, such as policies in Computer Configuration\Windows Settings\Security Settings\IP Security Policies on Local Machine. Disabling IP security policy processing could result in improper IP security configuration. PCM checks to see if IP security policy processing is enabled.

6.4 Registry Policy Processing - This setting determines when Registry policies are updated. This policy affects all policies in the Administrative Templates folder and any other policies that store values in the Registry. If Registry policy processing is disabled, a policy mismatch could happen. PCM checks to see if Registry policy processing is enabled.

6.5 Run Logon Scripts Hidden - Logon scripts are batch files of instructions that run when the user logs on. Enabling this setting hides the instructions in logon scripts for Windows NT. One might not want to expose the different scripts run during the logon process. PCM checks to see if this feature is enabled.

7. Windows System-wide User Policy

Windows System-wide User Policy settings apply to system users rather than to the system. These settings also control the proper behavior of your Windows server.

7.1 Disable Boot, Logon, Logoff, Shutdown Status Messages - Enabling this setting suppresses system status messages. If you enable this policy, the system does not display a message reminding users to wait while their system starts or shuts down, or while users log on or off. Disabling status messages can result in loss of data if system is turned off quickly. PCM checks to see if this policy is enabled.

7.2 Disable Change Password - Enabling this setting prevents users from changing their Windows password on demand. PCM checks the status of the Disable Change Password setting.

7.3 Disable Command Prompt - Enabling this setting prevents users from running the interactive command prompt, Cmd.exe. PCM checks to see if the command prompt is enabled.

7.4 Disable Patching - Enabling this setting prevents users from using Windows Installer to install patches. Patches are updates or upgrades that replace only those program files that have changed. PCM checks to see if patching is disabled.

7.5 Disable Registry Editing Tools - Enabling this setting disables the Windows Registry editors Regedt32.exe and Regedit.exe. If this policy is enabled and the user tries to start a Registry editor, a message appears explaining that a policy prevents the action. Registry editing might lead to system compromises or malfunctioning of system and applications. PCM checks to see if this option is enabled.

7.6 Disable Rollback - Enabling this setting prohibits Windows Installer from generating and saving the files it needs to reverse an interrupted or unsuccessful installation. As a result, Windows Installer cannot restore the computer to its original state if the installation does not complete. This option also prevents malicious users from interrupting an installation to gather data about the computer or to search system files. Disabling this setting might result in intrusion. PCM checks to see if this policy is enabled.

IV. Conclusion

Although there are several quality host-based vulnerability assessment tools on the market today, I would recommend using Computer Associates' *e*Trust Policy Compliance software because of its comprehensive vulnerability analysis, ability to obtain up-to-date vulnerability information from various sources via the Internet, and its user-friendly GUI. In addition, a typical computer user does not have to be highly technical in order to successfully use Policy Compliance.

V. References

1. Al Berg. ***'Feeling Vulnerable'***. *Information Security Magazine*. February 2002:42-47
2. Krutz, Ronald L., & Vines, Russell Dean. (2001). '***The CISSP Prep Guide 'Mastering the Ten Domains of Computer Security'*** Wiley Computer Publishing
3. Harold F. Tipton, Micki Krause. (2000). ***'Information Security Management Handbook'*** 4th Edition. Auerbach Publications
4. Symantec. ***"Enterprise Security Strategy"***. September 2000. http://enterprisesecurity.symantec.com/article.cfm?articleid=354
5. Computer Associates, Home Page, http://www.ca.com
6. PentaSafe, Home Page, http://www.pentasafe.com/
7. Symantec, Home Page, http://enterprisesecurity.symantec.com/
8. Network World Fusion, ***"Buyer's Guide: Vulnerability Assessment Tools"***, 4 Feb. 2002. http://www.nwfusion.com/reviews/2002/vulnerability0204.jsp