OpenVMS Technical Journal V5

Taking OpenVMS Security One Step Further

© Copyright 2005 Hewlett-Packard Development Company, L.P.

Taking OpenVMS Security One Step Further

Ted Saul, Off-site Software Support Consultant

Michael Grinnell, Off-site Software Support Engineer

Overview

According to Secure Enterprise Magazine, more than two million dollars is lost annually in the United States because of worms, viruses, scripts, and other Internet security problems that disrupt business operations. Larger operations, especially Global 5000 businesses, experience even greater losses. Even though OpenVMS is "virtually unhackable," according to the 2001 DEFcon9 event, lax security methods and irresponsible users can allow OpenVMS system security to break down. It would interesting to determine the amount of money lost in trying to track down these types of security problems that take place on OpenVMS systems.

The four most common security access problems that can be found in OpenVMS environments are as follows:

- User irresponsibility, in which users purposely or accidentally cause noticeable damage.
- User probing, in which users are authorized to access computer resources but use their privileges to exploit insufficiently protected parts of the system.
- User penetration, in which users breach security controls to gain access to a system.
- Social engineering, in which intruders gain access by deceiving legitimate users of the system. Intruders might impersonate users by obtaining access to their unsecured system or terminal or to their passwords, or they might persuade users to perform actions that compromise the security of the system.

OpenVMS provides many internal tools that protect the operating system from harm. However, there are times when it is necessary to take OpenVMS security one step further. These steps can include:

- Monitoring which users are touching particular files or resources.
- Logging what a user is doing with a privilege they have been granted.
- Ensuring that inactive sessions are managed.
- Implementing a stricter set of rules in place for the system.
- Taking and reporting out a snapshot of the current security settings.

When it becomes necessary to take these and other severe security precautions, a product from one of HP's partners can help. PointSecure, Inc., provides OpenVMS IT managers with three products that can help with the management of these and many more tasks.

PointAudit

What is PointAudit?

The PointAudit product is a vulnerability assessment tool designed to check certain profile, privilege, file, and system parameter settings, and to alert you to exposures that might exist on your OpenVMS system. Currently, there is no way on an OpenVMS system to get an "at-a-glance" check of security settings other than by looking up each setting individually. PointAudit provides this ability and provides a series of customizable reports that allow you to see how secure your system is.

© Copyright 2005 Hewlett-Packard Development Company, L.P.

How does PointAudit work?

PointAudit resides on a Windows® based server and pulls its data from the OpenVMS system. PointAudit stores this information in a database on the Windows server for reporting and for comparing against subsequent data captures. Before the first data capture can take place, a few required steps must first be performed. First, your company's security policy information is translated into settings that PointAudit can use for comparison of your OpenVMS systems. For example, required password lengths for system and nonsystem accounts are set, as are their respective expiration ages. Second, default values for SYSGEN parameters, UAF flags, privileges, and granted quotas are also recorded. Once these values are in place, the desired data and output formats can be generated. Finally, all the settings are saved to the PointAudit database on the Window server and for use in future analysis.

PointAudit performs a variety of tests, which are divided into four categories:

- User profile tests
- Privilege tests
- File checkup tests
- Parameter tests

The **User profile test** and the **Privilege test** analyze the SYSUAF.DAT file. These tests check for the following:

- Users within the DEVOUR privilege group
- Users within the SYSTEM privilege group
- Users within the OBJECT privilege group
- Users within the ALL privilege group
- Users whose password length is too short
- Users with passwords that never expire
- Users who haven't changed their password within a specified time
- Users with failed login attempts
- Users whose UIC is not found in the rights database

This data can then be compared against the company security policy that was replicated during setup of PointAudit. For example, if a 15-character password is required by the company, violations of this rule will show up on the report. (A later section of this article discusses the System Detective application, which can identify users who are using their privileges to set up accounts that bypass security policy.)

The **File checkup test** analyzes stored files and reports potential security flaws. This information includes:

- Files containing an invalid general identifier
- Files containing an invalid UIC identifier
- Files containing a wildcard identifier
- Files containing an invalid owner
- Files with world read and world delete access

OpenVMS does allow each of these settings; however, they might be considered a security breach in some environments. For example, files that do not have a valid owner might indicate that a user was deleted from the system without proper cleanup of their files. If a new user is then added to the system and the old UIC reused, the new user will immediately have access to the previous owner's

© Copyright 2005 Hewlett-Packard Development Company, L.P.

files. Depending on what is recorded in these files, this situation could represent a serious security breach.

Parameter tests look at login, system, and network SYSGEN parameters to determine whether the environment is as secure as possible. This test looks at specific parameters related to login security, including LGI parameters, and compares them against the recommended values list. Those that do not match are flagged and reported as potential security breaches. Parameters that affect system and network security are also checked and compared. (The comparison values are set during the initial configuration.) The test also reports information about installed licenses and products as well as installed and removed patches. This information is useful in determining a patch level for a particular server and whether any attempt has been made to change the performance level of the machine.

Most of the PointAudit tests can be run either as a group or individually. A GUI interface on the Windows server indicates when each test has run and whether or not it was successful. The number of users and files that have met the test criteria is also reported, as is an immediate indication of security risks.

How does PointAudit enhance OpenVMS security?

The PointAudit product enhances OpenVMS security by allowing for the quick viewing of critical security settings. This "at-a-glance" view eliminates the need for issuing commands like DIR/SEC throughout the system and entering multiple SYSUAF and SYSGEN commands, thereby quickly uncovering violations of the security policy. By running tests and saving information over a period of time, changes that might compromise the system are discovered much more quickly, thereby allowing for a faster reaction time. A baseline for almost every aspect of the system's security can also be set for use in this quick comparison. PointAudit can perform this comprehensive security check in a short amount of time and can give an immediate indication of whether unauthorized personnel have been granted potentially damaging privileges.

PointSecure System Detective (Automatic Operations)

What is System Detective?

The PointSecure System Detective application runs on an OpenVMS server in the background and performs three primary functions:

- Monitors user activity.
- Manages inactive sessions.
- Provides access management and protect against intrusion.

With the use of screen messages, log files that contain details of user's session keystrokes, and database searches, the OpenVMS system administrator can see what is currently taking place on the system. They can also look back to view what has taken place previously. System Detective automatically takes action when certain events take place on the system.

© Copyright 2005 Hewlett-Packard Development Company, L.P.

How does System Detective work?

To monitor user sessions, rules are set up to report activity. These rules can be created to watch for certain behaviors, including the following:

- When a user logs on and takes certain actions
- What a user is doing and has done on the system
- Who a user is and to what security group they may belong
- Why a user may be carrying out a particular function such as enabling a privilege

System Detective can be set to turn on monitoring when a particular action takes place in order to watch a user or even to disable that user. Conversely, monitoring can be turned off when another event takes place. For example, a system administrator might want to turn on monitoring when a user invokes the Authorize utility (AUTHORIZE). All keystrokes can be recorded to a file, thereby enabling an audit trail if suspicious behavior occurs. When the user exits AUTHORIZE, monitoring can be turned off and all recording stopped.

When monitoring turns on, two actions take place:

- Every keystroke is recorded to a log file. This log file can be reviewed during the session or at a later time.
- The System Detective database records that a monitor event has taken place so that the system administrator can be notified.

Setup of System Detective begins with the editing of a configuration text file. Three types of commands are available to define the rules by which the system policy is defined:

- **Action commands** tell System Detective what to do when a particular event occurs on the system. Some of these commands are:
    - Monitor_User – Tells the automatic operations when, what, who, and why a user should be monitored. When this action takes place, keystroke collection and event monitoring to the database can begin.
    - Disable_User – Manages inactive sessions that have been detected on the system. Actions that can be defined include issuing warnings, and locking, suspending, or even terminating sessions.
    - Lockout_User – Sets the rules for locking an active user out of the system. The system administrator has the choice of simply suspending the user, of warning an offending user, or of terminating them altogether. Details of the action taken are then recorded in the Automated Operations database.

- **Global commands** direct System Detective and allow the system administrator to define commands to be used either throughout the entire configuration file or only in certain sections of the file. Global commands can also define values to be used by other commands. Commands available include:
    - Exclude_User – Exempts a particular user from actions take by other commands. For instance, you might want to exempt the SYSTEM account from being locked out for any reason.
    - No_Suspend – Prevents System Detective from being locked out for any reason.
    - Set_User_Class – Defines a group or class of users. For instance, you might want to group certain users together for monitoring purposes and to eliminate the need for listing separate commands in the configuration file.
- **Supplementary commands** include the following:
    - Report_User_Event – Records all user logins and batch job creations.

© Copyright 2005 Hewlett-Packard Development Company, L.P.

- Session_Lock – Manages the session lock utility, which provides users with a method of locking their terminal.
- Disable_DEC_Windows – Enables inactivity management for DECwindows workstations.

To enhance each of these commands, a series of objects, object types, options, and parameters are available. The use of these modifiers allows OpenVMS system administrators to integrate their system security policy into System Detective for automatic monitoring of systems. Such modifiers provide the in-depth granularity that allows monitoring of every aspect of the system.

Finally, the SYSDET command is also available to system administrators. Used from DCL level, SYSDET has the ability to start and stop System Detective as well as to manage licensing and reporting. Batch processing can also be used to take action when a certain event takes place on the system. This functionality is useful for sending email or for setting off a pager to notify the system administrator of security breaches as soon as they take place.

How does System Detective enhance OpenVMS security?

OpenVMS has the ability to put the first level of defense to protect its operating environment. By itself, OpenVMS has proven to be quite effective. System Detective, however, gives the system administrator the ability to guard against specific attacks and to take appropriate action against specific threats. Because most OpenVMS attacks typically come from within the system, automated operations can aggressively protect against and alert when intrusions or privilege abuses take place. OpenVMS does take action against security threats such as suspected break-ins and login failures. The addition of System Detective allows the careful monitoring of all users who are logged in to the system as well as the logging of precise actions that are taking place. In this way, the four vulnerable areas of an OpenVMS system can be closely monitored and managed in an unattended environment.

Using System Detective also provides the system administrator with a better understanding of how to use OpenVMS security internal features. Because of the depth of monitoring provided by the product, the system manager must be extremely familiar with the security settings of their system. Functional areas of the system that are not normally monitored might be exposed and would be served well by the use of System Detective. For example, the product can reduce the chance that privileges granted to a user is accidentally forgotten about or that an improper file protection is left in place on a critical image. System Detective helps to organize all security-related changes, thus allowing even the most inexperienced system administrator a good understanding of their system.

HP and PointSecure Services

Two key security concerns face OpenVMS system administrators, security administrators, and IT directors:

- Managing a system that requires elevated privileges for programmers, operators, third-party consultants, and vendors. The more privileges that are granted, the greater the potential security risks.
- An increased demand from internal and external audit requirements, such as HIPAA, Sarbanes-Oxley, and Graham-Leech-Bliley. Companies are being forced to build strong security polices in order to comply with new laws, internal pressures, and more stringent internal auditing demands. It is vital that customers can prove they are keeping their clients' data private.

© Copyright 2005 Hewlett-Packard Development Company, L.P.

HP has joined forces with PointSecure, Inc., to offer the OpenVMS System Security Audit Service. The goal of this service is to provide customers with:

- A comprehensive understanding of their OpenVMS security settings
- A solution for continued security management and system auditing

The OpenVMS System Security Audit Service is sold on a per-node basis and is based on tier (Workgroup, Departmental, or Enterprise). A single component or a combination of components can be chosen:

Option 1: Active Audit provides a snapshot security audit and installation of the PointAudit software.

Option 2: Proactive Audit provides a snapshot security audit and the installation and configuration of the System Detective monitoring environment.

Option 3: Ultimate Audit provides a snapshot security audit, installation of the PointAudit software, and installation and configuration of the System Detective monitoring environment.

Key Benefits of the Service

Customers can benefit from the OpenVMS System Security Audit Service in several ways:

- The security audit provides an HP-certified report of the OpenVMS system that compares current security level against best industry security practices.
- The installation and configuration of PointAudit includes a license and maintenance contract for one year of telephone support.
- System Detective provides the ability to proactively enforce security policies, along with the license and maintenance telephone support contract.

Summary

With the increased concern about security, it is imperative that system administrators take the most proactive steps possible to secure their systems. With the help of PointSecure and HP, even OpenVMS -- the most secure operating system in the world -- can have a more secure environment and can also be managed easily. If an audit from the PointAudit software doesn't report the same level of security you thought you had, then it might be time to consider deploying these products on a full-time basis.

For more information

For more information about PointSecure products, visit http://www.pointsecure.com. For more information about the HP OpenVMS System Security Audit Service, visit http://www.hp.com/hps,

© 2005 Hewlett-Packard Development Company, L..P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.