



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 permitted without express written permission.

**Open VMS 7-3.1
An Administrators View**

**GSNA Practical Assignment (v.2.1)
Option 1**

Submitted by Randy Buchanan, January 14/2003

© SANS Institute 2004, Author retains full rights.

Table of Contents

TABLE OF CONTENTS	2
ASSIGNMENT 1.....	4
Abstract.....	4
Research in Audit, Measurement Practice and Control	4
Identify the system to be audited	4
Administrators.....	4
Scope	4
Evaluate the risk to the system.....	5
Current State of Practice	7
Auditing Tools used:	7
ASSIGNMENT 2.....	8
Create an Audit Checklist.....	8
Item 2: Change Control – software installation and patch management.....	9
Item 3: user access - second level support logging	10
Item 4: modification of system user authorization file (sysuaf.dat).....	10
Item 5: idle sessions	11
Item 6: users with dialup access.....	12
Item 7: login failure-intruder database	12
Item 8: accounts whose passwords do not expire	13
Item 9: accounts with special privileges.....	13
Item 10: users with remote access.....	14
Item 11: password length.....	15
Item 12: default proxy login accounts	15
Item 13: modification of system parameters using system generation (SYSGEN) utility.....	16
Item 14: authorization of password resets	16
Item 15: Field Service account.....	17
Item 16: User that have their password lifetime=none.....	17
Item 17: Accounts that have been created and never utilized.....	18
Item 18: Duplicate UIC (User Identification Code).....	18
Item 19: Welcome banner	19
Item 20: Inactive accounts that have never been deleted from SYSAUF.DAT file	20
ASSIGNMENT 3.....	21
Audit Evidence.....	21
Test 1: Using “Shadow Security Scanner” perform vulnerability assessment of OS (Item 1).....	21
Test 2: idle sessions (Item 5)	22
Test 3:modification of system user authorization file (sysuaf.dat) (Item 4).....	23
Test 4: user access - second level support logging (Item 3)	24
Test 5 : login failure-intruder database (Item 7)	25
Test 6: VPN users connecting to host (Item 6)	26
Test 7:modification of system parameters using system generation (SYSGEN) utility (Item 13)	26
Test 8: default proxy login accounts (Item 12)	27
Test 9: password length (Item 11).....	28

Test 10: Field Service account (Item 15).....	29
Measure Residual Risk - Low	29
Is this system auditable?	30
ASSIGNMENT 4.....	31
Risk Assessment	31
Summary	31
VMS Operating System Vulnerability Enumeration.....	31
User Access and how they are monitored.....	32
APPENDIX A: REFERENCES	35
APPENDIX B:.....	36

© SANS Institute 2004, Author retains full rights.

Assignment 1

Abstract

The purpose of this paper is to fulfill the requirements of the GSNA (GIAC Auditing Networks, Perimeters and Systems) certification. For the practical, I chose to audit the Open VMS 7-3.1 operating system within a company named "ABC" from the security administrator's perspective. The focus will be to evaluate the risks associated from user access, create a checklist based on those risks, conduct the audit from the checklist and then provide a summary of the results.

Research in Audit, Measurement Practice and Control

Identify the system to be audited

ABC is an IT outsourcing company whose primary role is to provide services for a large number of smaller financial institutions. The operating system to be audited will be Open VMS version 7.3-1 running in a clustered environment comprised of multiple node Compaq Alpha server DS20E's. These clustered DS20E's are not visible from the Internet and only a select few users can access these servers remotely. They are primarily used for financial applications however do have a secondary use, which is internal e-mail. Email on the VMS systems between ABC and its clientele, has become virtually non-existent due to the overwhelming growth of Internet e-mail.

Administrators

The duties of overseeing the VMS operating systems and their functions are segregated between the system administrators and the security administrators. The system administrators take care of all the system's activities. These activities include: all system upgrades and patches, creating, modifying and support of the client's databases as well as the modification of system file and parameters. The security administrators are responsible for overseeing all aspects of the user accounts, the permissions linked to those accounts, monitoring the user activity within the VMS cluster and auditing the systems.

Scope

The scope of the audit will focus on user access, how it is controlled and how it is monitored within the VMS clustered environment. Within this scope we will perform a vulnerability assessment on one specific node (NODE1) within the VMS cluster. The audit will be comprised of using specific auditing tools, which will show how our checklist provides auditing information on the Open VMS systems on a daily, weekly or monthly basis. The auditing tools used are PointAudit and System Detective AO

from PointSecure Inc¹, auditing utilities included with the VMS operating system and Shadow Security Scanner by Safety Lab².

Evaluate the risk to the system

As indicated, ABC is an IT outsourcing company whose primary role is to provide financial services for a large number of smaller financial institutions. Servers running these financial applications are deemed critical and any downtime, compromise or data loss would be detrimental to the institutions using these services. Each institution has their own database on the VMS cluster and is responsible for creating their own users and giving those users permissions within their database. ABC security administrators create the accounts on the VMS system at the request of the institution's administrator. There are a number of users at ABC that do have access to these production databases for support purposes.

Risk	Probability	Consequences
System becomes unavailable due to hardware or software failure, power failure or disaster.	Low - because these VMS systems are in a clustered environment if one system fails for any reason another node steps in for the failed system. There is also a hot site should a disaster strike the building. Redundancy, Disaster Recovery	Users would be unable to access the host for a very short period of time. This in fact would cause a short DOS for some institutions depending which node in the cluster they were logged into.
Unauthorized external access via internet (VPN, dialup)	Low – Although the VMS cluster is not visible from the internet, that is to say that one cannot see these production servers if they were performing a ping sweep, 99% of the user base gains access through the internal network. However with the changing times, there are employees that require a method of gaining access into the ABC network to support the development and production servers and those applications that run on these servers. The unauthorized user would need the VPN credentials as well as VMS credentials to be able to	Loss of data, confidentiality and integrity.

¹ Point Secure Inc, Open VMS Security Solutions, <http://www.pointsecure.com/>

² Safety-Lab, <http://www.safety-lab.com/en/>

	access these servers.	
Unauthorized internal access via username and password	Low- Passwords are restricted from 6 to 32 characters. Unauthorized user would have to guess username, password or both. There is also a lockout mechanism to prevent brute force password cracking.	User may gain access to system but only have access to whichever identifier or identifiers this account provides. Loss of data and confidentiality would arise should an unauthorized internal user gain access.
User Privileges – Normal Users	Low – restriction flags set in the sysuaf.dat file control user accounts. All users with the exception of the system and security administrators are created with captive accounts, this denies access to the DCL prompt when used in conjunction with the Disctly restrict flag. Users are also created with only NETMBX and TMPMBX privileges that are considered normal privileges in this environment.	User would have access to unrestricted files with world access should they receive a DCL command prompt. Loss of data, confidentiality and integrity.
User Privileges – Security and System Administrators	High – as with all system administrators, they have the access to do most functions to an operating system.	Loss of confidentiality, integrity and availability.
Unauthorized change control could produce system harm or outage	Medium – all changes, no matter how minute, are required to go through the proper change control procedure, which administrators must follow and have signed, by management, before any change can be completed. However this could not stop the administrator from doing an unauthorized change.	Loss of confidentiality, integrity and availability depending on what change had occurred.
Unnecessary services running	Low – Vulnerability assessment is performed monthly and compared against system benchmark. It is possible that a service could be turned on but highly unlikely.	Unnecessary service could lead to unauthorized system access.

Current State of Practice

My primary goal, while researching audit checklists and guidelines for VMS systems, was to find checks that were not necessarily used in previous GIAC practicals. Using this goal as a “filter”, I found that topics regarding, “how to secure your VMS system,” were more popular than topics such as, “VMS auditing checklists.” Both searches were performed on search engines, Google and Altavista. I did however find one checklist on a website hosted by the Computer Security Research Center³ that had a number of good checklists and implementation guidelines for several different operating systems. The checklist created by the Defense Information Systems Agency for VMS was very detailed with some items that were, in my opinion, out of scope for this audit as it had upwards of 50 checks. I also read several papers from the GIAC.org website, in particular a VMS audit practical completed by Jeff Parker. I decided to audit what is currently monitored in the ABC environment on a continual basis, and to create a checklist based on my own personal experience, knowledge and accessible internal resources.

Resources used:

Global Information Assurance Certification site: <http://www.giac.org/GSNA.php> and http://www.giac.org/GSNA_0100.php

Parker, Jeff “An Authentication Audit on Open VMS: An Auditor’s Perspective” Document available at http://www.giac.org/GSNA_0100.php

Defense Information Systems Agency, “VMS - OpenVMS Security Checklist”, 31 October 2003, url <http://csrc.nist.gov/pcig/cig.html> , “Vax VMS Checklist”

Google : <http://www.google.ca/>

Altavista: <http://www.altavista.com/>

PointSecure Inc, “PointAudit 3.2 User Guide” and “System Detective AO User Guide”

OpenVMS Guide to System Security:
<http://h71000.www7.hp.com/doc/731FINAL/6346/6346PRO.HTM>

ABC resources - System Administrator
- Network Administrator

Auditing Tools used:

System Detective AO⁴: provided by PointSecure Inc.

System Detective AO is an automated rules-based tool that is designed to help administrators secure their OpenVMS systems. This security and compliance

³ Computer Security Research Center, URL <http://csrc.nist.gov/>

⁴ PointSecure Inc , System Detective AO, <http://www.pointsecure.com/sysdetao.htm>

application can enforce user accountability by recording terminal activity as well as enhancing the OpenVMS access control capabilities by taking away privileges or restricting access to images. In addition, administrators have the ability to manage unattended inactive terminal sessions by locking the keyboard and/or terminating processes. This product is extremely flexible to use and through its rules-based system will allow your systems to be monitored with the least amount of system resources and overhead being added to the system.

PointAudit⁵: provided by PointSecure Inc.

PointAudit allows the administrator to quickly assess OpenVMS Security and generate custom reports and make changes to the system. User profiles, user privileges, flags, system settings and file settings can all be managed through this solution. In addition, PointAudit identifies vulnerabilities and suggests actions to correct exposures.

OpenVMS Guide to System Security: Administrator will be using audit commands provided with the VMS system. The online documentation can be found at:
<http://h71000.www7.hp.com/doc/731FINAL/6346/6346PRO.HTM>

Shadow Security Scanner: This network audit scanner will be used to perform our vulnerability assessment of the VMS node. The url is located at:
<http://www.safety-lab.com/en/products/1.htm>

Assignment 2

Create an Audit Checklist

The following is a checklist that is followed on either a daily, weekly or monthly basis. All audit checks performed are done so at the authorization from senior management and through ABC internal practices. Since this audit is an ongoing entity, there is no further authorization required from management.

The checklist items provide the following fields:

Reference: Provides reference to what user guide was used to perform this audit check. A reference guide is available in Appendix A.

Control Objective: Purpose of the audit check, what is the audit check supposed to achieve?

Risk: What risk is the check supposed to address?

Compliance: How the audit check conforms to the objective.

Testing: Step by step instructions to test compliance. For clarification, if a “ – “ is used at the end of a command line, it means that the command is carried over to the next line. For example:

```
sysdet report/database=openv$root:[system_detective.node1]-  
detective_database.dat/object=authorize/since=20-nov-2003
```

⁵ PointSecure Inc , PointAudit 3.2, <http://www.pointsecure.com/pointaudit.htm>

Objective/Subjective: Is this test objective or subjective? One if these words will be stated within the check.

Audited: This check is performed daily, weekly, monthly or other.

All tests are performed on only one node within the VMS cluster, that node being NODE1.abc

PointSecure's PointAudit software is used on numerous occasions during the testing portion of the checklist. These screen shots are identical up to a certain point in the testing process. I have included an example of these screen shots in Appendix B to use as a reference when following the testing.

Item1: Using “Shadow Security Scanner”, perform vulnerability enumeration of OS

Reference: Internal practice

Control objectives: Provide vulnerability enumeration of the VMS operating system and compare with benchmark assessment.

Risk: This is to provide management with assurance that no vulnerabilities or unnecessary services are running on this critical server. Any unnecessary services or vulnerabilities on this system could have a great impact should they be exploited.

Compliance: Current assessment will provide a report that will be compared with previous benchmark assessment to see if any changes have occurred.

Testing: Run Shadow Security Scanner to scan for all 65535 ports. Since we know the operating system we will deactivate all unnecessary plug-ins that includes the denial of service selections for this critical server. Only one node of the VMS cluster will be assessed for this practical, although all clustered systems are tested on a monthly basis.

Objective: Output provided by security scanner assessment.

Audited: Monthly

Item 2: Change Control – software installation and patch management

Reference: Internal practice

Control objectives: Provide a process by which system or security administrators perform upgrades or software installs under a controlled mechanism.

Risk: System or security administrators install unauthorized or untested software or change system parameters into production systems that could degrade the performance of the system.

Compliance: A change control process must be in place. A change control form must be completed and signed off by the following ABC departments: Operations, Quality Assurance and the Security Officer. The administrator performing the install must also sign off the form after completion.

Testing: No change can occur on the production system without proper change control management. All testing is completed on a development system that is running the same operating system and software as production. System administrators must follow change control procedure and have the necessary change control form completed before the implementation of any software can take place.

Subjective: Appropriate managers, before installation of any software or patches, must sign all change control forms.

Audited: Depending on the change control schedule

Item 3: user access - second level support logging

Reference: Internal practice, hp OpenVMS Guide to System Security

Control objectives: Check for session logging for financial database support. In ABC there was a need to monitor any modifications that occur within the institutions or clients databases when second level support was needed. An identifier is added to their accounts that force them to log into the system using a “forced_logging” account. Once second level support logs into the system with this account, it would trigger session logging. They would be prompted to login using their own account and would now be able to complete the support call.

Risk: Required to address second level support changes made to the database when called upon by the financial institution. The risk would have second level support adding, deleting or modifying records in the database with no logging or audit trail procedure in place.

Compliance: Check programming user account for “forced_logging” identifier. Check log files to make sure all sessions are logged.

Testing: We will give user SEC_TEST the “forced_logging” identifier
From a DCL prompt:
NODE1::>mcr authorize (This will allow us to modify the sysuaf.dat file)
From the UAF prompt:
UAF::>grant “forced_logging” identifier to user SEC_TEST
User SEC_TEST will try logging onto the system normally.
User SEC_TEST will then be forced to log into the system with the “forced_logging” user account and then will proceed to login with their own account.

Objective: Check user accounts for “forced_logging” identifier. Failure to log into forced_logging account first denies access to system.

Audited: Daily

Item 4: modification of system user authorization file (sysuaf.dat)

Reference: hp OpenVMS Guide to System Security, System Detective AO User Guide

Control objectives: Check for modifications of the sysauf.dat file.

Risk: This is probably the most critical file on the VMS system. There are only a select few users who have access to create, delete, or modify records within the sysuaf.dat file. Any user gaining access to this file could grant all privileges and gain control over the system. Because this file is so critical, all users that access this file are logged.

Compliance: Users accessing this file will receive a warning that this file is restricted. System detective will log all user sessions accessing this file.

Testing: From a DCL prompt

NODE1::> mcr authorize

UAF> show SEC_TEST

System detective also produced a report that shows who has accessed this file and when.

From a DCL prompt:

sysdet report/database=openv\$root:[system_detective.node1]-
detective_database.dat/-object=authorize/since=20-nov-2003

Objective: User will receive a warning that they are accessing a restricted file and system detective report will show who accessed the file and when. The system detective playback function will show us the logged session and what was modified.

Audited: Daily

Item 5: idle sessions

Reference: System Detective AO User Guide

Control objectives: Disable user sessions after one hour of idle time.

Risk: Some users have been known leave their workstations for extended periods of time and fail to logout of their VMS session, this includes leaving for the day. Another authorized user or unauthorized user could gain access to the database with the original user's privileges.

Compliance: Users will be warned after 45 and 55 minutes of idle time and will then have session terminated after the one hour of inactivity.

Testing: Run command from DCL prompt:

sysdet report/database=openv\$root:[system_detective.NODE1]-
detective_database.dat/result=terminate/since=date of query

This report will show all users sessions that have been terminated after one hour of idle time.

Objective: Report shows warnings and then actual termination of session.

Audited: Daily

Item 6: users with dialup access

Reference: Point Audit 3.2 User's Guide

Control objectives: Check user accounts for dial-up access and mitigating the risks surrounding dialup access through procedures.

Risk: A select few ABC users can log into the network via dial-up for support. Unauthorized users could wardial should modems be left on and attempt login.

Compliance: Point Audit shows all users accounts that have dial-up access. Documentation surrounding dialup access must also be available for viewing upon request. This process includes a procedure for turning the modems on and off only when support on the system is needed.

Testing: See Appendix B for screen shots

- Start Point Audit application
- You must connect to the host you are wishing to audit (in this case "node1.abc").
- Once you have connected, select and modify "Setup".
- Select the tab "Perform Test" and then select "All". This will run all tests (user profile, file check and system parameters)
- After the test has been completed, select the customized reports tab, and then select setup.
- There are 5 customized report setting tabs: Privilege, Flags, Error, Password/Access and Errors, clear all fields in all tabs.
- Select the "Error" tab and then select error 17 (Accounts with dial-up access)
- Select "OK" and then select Create, the software will return all user accounts with dial-up access.

Objective: Report shows accounts with dial-up access. Procedures for dialup access must be available for viewing upon request.

Audited: Daily

Item 7: login failure-intruder database

Reference: hp OpenVMS Guide to System Security, System Detective AO User Guide

Control objectives: A lockout mechanism is needed for unsuccessful login attempts.

Risk: Unauthorized user could try logging in numerous times via password guessing or password cracking.

Compliance: User will have 3 attempts to login correctly, after the 4th attempt the user will be locked and entered into the intrusion database.

Testing:

User attempts to login 4 times with an incorrect password

From the DCL prompt:
NODE1::>show intruder (this will give us a list of users accounts locked out from at least 4 unsuccessful attempts)
System detective testing:
The system detective configuration file is set to allow 3 incorrect login attempts but the fourth login failure will trigger an entry in the database. Run command from DCL prompt for report results.
sysdet report/database=openv\$root:[system_detective.NODE1]-
detective_database.dat/trigger=login_failure/since= date of query

Objective: Report from system detective shows login failures and results from VMS command “show intruder” will show users within the intruder database.

Audited: Daily

Item 8: accounts whose passwords do not expire

Reference: Point Audit 3.2 Users Guide, Internal practice

Control objectives: Check to see that all user account passwords do indeed expire.

Risk: Passwords that do not expire are deemed a security risk. An Intruder would not have to worry about changes to the password.

Compliance: Point Audit report will show users whose passwords do not expire.

Testing: See Appendix B for screen shots

- Start Point Audit software
- You must connect to the host you are wishing to audit (in this case “node1.abc”).
- Once you have connected, select and modify “Setup”.
- Select the tab “Perform Test” and then select “All”. This will run all tests (user profile, file check and system parameters).
- After the test has been completed, select the customized reports tab, and then select setup.
- There are 5 tabs: Privilege, Flags, Error, Password/Access and Errors, clear all fields in all tabs.
- Select the “Error” tab and select only error 16 (Accounts whose password do not expire)
- Select “OK”, then “Create” and software will return all accounts that do not expire.

Objective: Point Audit report will show accounts that do not expire.

Audited: Monthly

Item 9: accounts with special privileges

Reference: Point Audit 3.2 Users Guide

Control objectives: Check user accounts that have more than normal privileges. When new users are created they are given privileges deemed normal. These normal privileges are "NETMBX" and "TMPMBX".

Risk: Users with special privilege risks range from potentially consuming non-critical resources to completely destroying your system.

Compliance: To be compliant Point Audit software must show whether user account has or does not have special privileges.

Testing: See Appendix B for screen shots

- Start Point Audit software
- You must connect to the host you are wishing to audit (in this case "node1.abc").
- Once you have connected, select and modify "Setup".
- Select the tab "Perform Test" and then "All". This will run all tests (user profile, file check and system parameters)
- After the test has been completed, select the customized reports tab, and then select setup.
- there are 5 tabs Privilege, Flags, Error, Password/Access and Errors, clear all fields in all tab
- Select the Privilege tab
- Select all but NETMBX and TMPMBX fields
- Select "OK", then "Create" and the software will return all user accounts that have special privileges

Objective: Point Audit report will show users accounts with privileges other than NETMBX and TMPMBX.

Audited: Monthly

Item 10: users with remote access

Reference: System Detective AO User Guide

Control objectives: This check is to monitor those users who access production hosts remotely via VPN access.

Risk: More and more employees at ABC are now able to work from either home or some other remote site, the company wishes to log all those who access production remotely.

Compliance: To be compliant system detective must log all remote access via VPN. System detective will show the IP address, node, user and time of access.

Testing: run command from DCL prompt

sysdet report/database=openv\$root:[system_detective.NODE1]-
detective_database.dat/trigger=port/since= date of query

Objective: Report will show which users have logged into production via VPN.

Audited: Daily

Item 11: password length

Reference: hp OpenVMS Guide to System Security

Control objectives: Check to see that passwords are a minimum of 6 characters and a maximum of 32 characters.

Risk: Passwords on a VMS can be set from 0-32 characters long. Passwords under 6 characters can be easily guessed. Passwords with 6 characters are more secure and harder to crack.

Compliance: System will not be compliant if user can log in using less than 6 characters. VMS security guidelines state that a minimum 6 characters and maximum of 32 characters are sufficient.

Testing: from a DCL prompt

- mcr authorize
- set password/user=welcome SEC_TEST
- user will then attempt to login in using less than 6 characters
- user will then attempt to login in using more than 32 characters

Objective: Pass or fail test. Either user will be able to login or not.

Audited: Monthly

Item 12: default proxy login accounts

Reference: hp OpenVMS Guide to System Security

Control objectives: Check for proxy login accounts, no users but system and security administrators should have default proxy logins.

Risk: Although proxy login have some security benefits, users with proxy accounts are able to copy files back and forth from development to production and visa versa.

Compliance: To be system compliant, only system and security administrators will have proxy accounts. In the ABC environment this is needed for some of their day-to-day operations.

Testing: from a DCL prompt

- mcr authorize
- UAF> sho/proxy node::* where node = remote host

Objective: Report shows who has default proxy login.

Audited: Weekly

Item 13: modification of system parameters using system generation (SYSGEN) utility

Reference: System Detective AO User Guide

Control objectives: Check for any system parameter modifications using the SYSGEN utility.

Risk: The system generation utility is a system management tool used to tailor a system for specific hardware and software configuration. Anyone with the privilege to run the SYSGEN utility can alter the operating system however they wish.

Compliance: Once user enters command they will be notified that they are accessing a restricted file.

Testing: From a DCL prompt run

- mcr sysgen
- SYSGEN> SHO/JOB - any command from the sysgen prompt will trigger an event

Objective: Report will show what user has accessed the sysgen utility and show a warning that the user is accessing a restricted image or file.

Audited: Weekly

Item 14: authorization of password resets

Reference: hp OpenVMS Guide to System Security

Control objectives: Procedures for proper authorization of password resets.

Risk: The system administrators at the institution level are the only users that are authorized to request password resets to the security administrators. Unauthorized users may use social engineering to call or request a password reset. Once that password is reset the user will have access to the system and institutions database.

Compliance: Password procedures must be in place that allows only institution system administrators to request resets. There must be a tracking mechanism in place to log all requests and who reset the passwords.

Testing:

- institution's system administrator will send a secure email to security administrator (an email must always be sent to the security administrator for auditing purposes)
- security administrator must check to see if user is in intrusion database and if so remove them
- show intrusion
- delete/intrusion "source" note: source = username if user is locked out
- security administrator will modify the password
 - mcr authorize
 - modify/password=welcome username

- security administrator would then complete the step and send an email to the banking system admin

Subjective: Based on ABC company procedures.

Audited: Procedure done on a daily basis

Item 15: Field Service account

Reference: Internal practice, hp OpenVMS Guide to System Security

Control objectives: Check that field service account is disabled.

Risk: This account is a high privileged account with system access. Anyone gaining access to this account could potentially do great damage.

Compliance: Account will be flagged as disused.

Testing: from a DCL prompt:

- mcr authorize
- show decfield

Objective: Report will show that decfield account has been disused.

Audited: Weekly

Item 16: User that have their password lifetime=none

Reference: Point Audit 3.2 Users Guide,

Control objectives: Objective is to make sure user accounts do not have their pwdlifetime set to none.

Risk: Accounts with no lifetime restriction may retain its password indefinitely. The account may be vulnerable to unauthorized user should the password be discovered.

Compliance: System will be compliant if no accounts are discovered with pwdlifetime=none.

Testing: See Appendix B for screen shots

- Start Point Audit software
- You must connect to the host you are wishing to audit
- Once you have connected, select and modify "Setup".
- Select the tab "Perform Test" and then "All". This will run all tests (user profile, file check and system parameters)
- After the test has been completed, select on the customized reports tab, and then select setup.

- There are 5 tabs Privilege, Flags, Error, Password/Access and Errors, clear all fields in all tabs
- Select the Password/Access tab and select the "Password Lifetime" checkbox.
- Select "OK" and then "Create", the software will return all user accounts with the passwords lifetime set to none.

Objective: Point Audit report will show all accounts with password lifetime set to none.

Audited: Monthly

Item 17: Accounts that have been created and never utilized

Reference: Point Audit 3.2 Users Guide, Computer Security Research Center - VMS VAX Checklist

Control objectives: Objective is to make find accounts that have been created and never been used.

Risk: Unused accounts can present opportunities to penetrate the system. These accounts have never been utilized on the system. This implies that these accounts are inactive and, therefore, may be unnecessary. They also present a potential security risk in that unauthorized users may attempt to gain access to the system using these accounts.

Compliance: System will be compliant if no accounts exist that have been created and not used.

Testing: See Appendix B for screen shots

- Start Point Audit software
- You must connect to the host you are wishing to audit
- Once you have connected, select and modify "Setup".
- Select on tab "Perform Test" and then "All". This will run all tests (user profile, file check and system parameters)
- After the test has been completed, select the customized reports tab, and then select setup.
- There are 5 tabs Privilege, Flags, Error, Password/Access and Errors, clear all fields in all tabs.
- Select the Error tab, and then check "error 11 Accounts that have never been used".
- Select "OK", then "Create" and the software will create report.

Objective: Point Audit report will show all accounts that have never been used.

Audited: Monthly

Item 18: Duplicate UIC (User Identification Code)

Reference: Point Audit 3.2 Users Guide, Computer Security Research Center - VMS VAX Checklist

Control objectives: Objective is to find accounts that have been created that have the same UIC.

Risk: Accounts that share a common UIC allow the user of one account to modify or delete the files of another account. These accounts share a single UIC and therefore share access to most security protected objects in the system. This is usually unintentional and usually the result of an error in creating the user accounts.

Compliance: Check will be compliant if no users have duplicate UIC's.

Testing: See Appendix B for screen shots

- Start Point Audit software
- You must connect to the host you are wishing to audit (in this case "node1.abc").
- Once you have connected, select and modify "Setup".
- Select on tab "Perform Test" and then "All". This will run all tests (user profile, file check and system parameters)
- After the test has been completed, select the customized reports tab, and then select setup.
- There are 5 tabs Privilege, Flags, Error, Password/Access and Errors, clear all fields in all tabs.
- Select the File/Identifier tab, and then check "Duplicate UIC".
- Select "OK" and then "Create", the software will create report of accounts with duplicate UIC's

Objective: Point Audit report will show all accounts that have duplicate UIC's.

Audited: Monthly

Item 19: Welcome banner

Reference: Internal practice, hp OpenVMS Guide to System Security, System Detective AO User Guide

Control Objectives: There are two control objectives here, one to check the welcome banner for messages containing system information and the other to use as a warning that unauthorized users are prohibited.

Risk: The only risk here would be if the banner disclosed pertinent information regarding OS version or other system information that an attacker could use in compromising the system.

Compliance: After opening VMS session and before login, the system will show whether banner reveals system information and an "unauthorized access prohibited" banner. Since all users are being monitored another banner is reveal after login. This banner is from the system detective software and makes users aware that their actions are being recorded.

Testing: Opening a VMS session

Objective: System at login will show whether check is compliant.

Audited: Monthly

Item 20: Inactive accounts that have never been deleted from SYSAUF.DAT file

Reference: Point Audit 3.2 Users Guide

Control objectives: Control objective is to seek out inactive or disused accounts in the sysuaf.dat file and delete the accounts that will be no longer in use.

Risk: Once an employee of either a financial institution is no longer an employee, their account is set to "not authorized" in the financial institutions database. However the deactivated user in the database must also be deactivated on the VMS system. The risk lies when the institutions system administrator deactivates the employee from the database but fails to contact the security administrator at ABC to deactivate the user on the VMS system. Failure to do this leaves an account active and a possibility of compromise.

Compliance: Compliance is not easily garnered here. We must first find all disused accounts by running the Point Audit Software. Once we have a list of disused accounts, we then contact the institutions in question to see if in fact these accounts should be removed. Once that information has been returned, we can then proceed to delete unused accounts.

Testing: See Appendix B for screen shots

- Start Point Audit software
- You must connect to the host you are wishing to audit
- Once you have connected, select and modify "Setup".
- Select on tab "Perform Test" and then "All". This will run all tests (user profile, file check and system parameters).
- After the test has been completed, select on the customized reports tab, and then select setup.
- There are 5 tabs Privilege, Flags, Error, Password/Access and Errors, clear all fields in all tabs.
- Select the Error tab, and then select "07 – DISUSERed Accounts".
- Select "OK", then "Create" and the software will create a disused account report

Objective: Point Audit report will show all accounts that have been disused.

Audited: Monthly

Assignment 3

All testing output will be shown in bold.

Audit Evidence

Test 1: Using “Shadow Security Scanner” perform vulnerability assessment of OS (Item 1)

FTP Servers: Anonymous FTP

Port	21
Description	Anonymous FTP is enabled.
Risk level	Medium
How to fix	Disable anonymous FTP.
CVE	CAN-1999-0497

Mail Servers: VRFY Command Enabled

Port	25
Description	An SMTP service supports VRFY.
Risk level	Low
How to fix	Disable the VRFY command.
CVE	CAN-1999-0531

Mail Servers: SMTP without AuthLogin

Port	25
Description	An SMTP service supports VRFY.
Risk level	Low
How to fix	Install authlogin.



21: FTP - File Transfer Protocol [Control]

TCP Banner	220-Connecting to a real system... OpenVMS 220 NODE1.abc HGFTP server V3.1 ready.
TCP Protocols	FTP
Current dir	/mgftp\$root/anonymous
STAT	211-NODE1.abc HGFTP server V3.1 for OpenVMS Alpha 211- 7-DEC-2003 07:44:00 -0600 211-Logged in as: ANONYMOUS since 7-DEC-2003 07:44:00 211-Restrictions: NOWRITE,NOCONTROL,NODELETE 211-The current data transfer parameters are: 211- MODE Stream 211- STRU File 211- TYPE AN (Ascii Noprint) 211- Data connection closed 211 Connection closes if idle for 5 min.
SYST	215 V M S V7.3-1 COMPAQ AlphaServer DS20E 500 MHz H G F T P (UNIX emulation) System type.

23: TELNET - Telnet

TCP Banner ŷû_ŷû_

Node NODE1

Unauthorized Access Prohibited

Username:

25: SMTP - Simple Mail Transfer Protocol

TCP Banner 220 NODE1.abc V5.3-18E, OpenVMS V7.3-1 Alpha ready at Sun, 7
Dec 2003 07:42:36 -0600 (CST)

TCP Protocols SMTP

515: PRINTER - Printer Spooler

Reply Banner in _
Request

123: NTP - Network Time Protocol

Description No More Details Available

110: POP3 - Post Office Protocol - Version 3

TCP Banner	+OK TCPIP POP server V5.3-18C, OpenVMS V7.3-1 Alpha at node1.abc,up since 2003-10-27 18:30:34 <23600428._7_DEC_2003_07_42_39_47@node1.abc>
------------	---

Test 2: idle sessions (Item 5)

Sessions will be terminated after one hour of inactivity

NODE1::>

Message at 20-NOV-2003 14:31:09.90 to terminal TNA1193=>

You have been inactive for 45 minutes

NODE1::>

Message at 20-NOV-2003 14:41:09.90 to terminal TNA1193=>

You have been inactive for 55 minutes

NODE1::>

Message at 20-NOV-2003 14:46:09.90 to terminal TNA1193=>

You have been inactive for 60 minutes

NODE1::>

Message at 20-NOV-2003 14:46:09.90 to terminal TNA1193=>

Your session has been terminated due to inactivity

User has been logged but has left their session idle for over one hour. The user gets two warnings, one at 45 minutes and then 55 minutes. The last warning is 60 minutes and then termination of session.

System detective will also produce a report showing users that were terminated after one hour of inactivity. From DCL prompt run
sysdet report/database=openv\$root:[system_detective.node1]-
detective_database.dat/result=terminate/since=10-nov-2003

You can see by the output and the system detective report that user SEC_TEST was terminated at 14:46

```
=====
20-NOV-2003 14:46:09 => Event Severity: INFORM
Username: SEC_TEST, Process: SEC_TEST, Node: NODE1
Terminal: TNA1193, Port: Host:_192.168.2.105_Port:_4287, Security Event ID:
214747475210654461
> Event Description: User has been TERMINATED due to inactivity
>   Event Trigger: USERNAME = *
>   Event Reason: User SEC_TEST is using OpenVMS username *
```

Test 3:modification of system user authorization file (sysuaf.dat) (Item 4)

User SEC_TEST logs in and enters DCL command "mcr authorize" for the User Authorization File prompt

```
NODE1::> mcr authorize
UAF>
```

Message at 20-NOV-2003 16:49:17.79 to terminal TNA1219=>
You are accessing a restricted file or image

```
UAF>
```

You can see that user SEC_TEST has been notified that they are accessing a restricted file or image, that image being the sysuaf.dat file.

System detective also produced a report that shows who has accessed this file and when.

From a DCL prompt
sysdet report/database=openv\$root:[system_detective.node1]-
detective_database.dat/object=authorize/since=20-nov-2003

```
=====
20-NOV-2003 16:49:17 => Event Severity: CRITICAL
Username: SEC_TEST, Process: SEC_TEST, Node: NODE1
Terminal: TNA1219, Port: Host:_192.168.2.105_Port:_2678, Security Event ID:
128291878410654478
Event Description: User has TRIGGERED an alarm due to trigger event
Event Trigger: IMAGE = AUTHORIZE
Event Reason: User SEC_TEST has executed image AUTHORIZE
```

```
=====
20-NOV-2003 16:49:17 => Event Severity: CRITICAL
Username: SEC_TEST, Process: SEC_TEST, Node: NODE1
```


Terminal: TNA1219, Port: Host: _192.168.2.105_Port: _2678, Security Event ID: 128291878410654478

Event Description: User is PREVIOUSLY MONITORED (NO LOG) due to trigger event

Event Trigger: IMAGE = AUTHORIZE

Event Reason: User SEC_TEST has executed image AUTHORIZE

=====

Test 4: user access - second level support logging (Item 3)

Second level support has an identifier that forces them to log into a forced logging account. Failure to do so denies access to system. User SEC_TEST has been granted the forced_logging identifier which forces them to log into this account.

NODE1::> grant forced_logging SEC_TEST

%UAF-I-GRANTMSG, identifier FORCED_LOGGING granted to SEC_TEST

User SEC_TEST logs in using their password. System tells them they are not authorized to access without account logging.

Unauthorized Access Prohibited

Username: SEC_TEST

Password:

Welcome to NODE1

Last interactive login on Thursday, 20-NOV-2003 17:03:59.97

Last non-interactive login on Saturday, 18-OCT-2003 17:56:05.81

SYSTEM-F-NOAUTH, You are not authorized to access this system without account logging

SEC_TEST logged out at 20-NOV-2003 17:05:20.22

As you can see from the output, user SEC_TEST having the identifier forced_logging forces them to login into that account (forced_logging) before logging into their own. This creates a log file which shows what was done in that session.

Production Node NODE1

Unauthorized Access Prohibited

Username: forced_logging

Password:

Welcome to NODE1

Last interactive login on Thursday, 20-NOV-2003 10:52:06.19

All activity for the duration of this session will be logged.

Production Node NODE1

Unauthorized Access Prohibited

Username: SEC_TEST

Password:

Welcome to NODE1

Last interactive login on Thursday, 20-NOV-2003 17:05:20.11

Last non-interactive login on Saturday, 18-OCT-2003 17:56:05.81

Test 5 : login failure-intruder database (Item 7)

Shows user SEC_TEST attempted logins. The threshold for user attempts is 3 with the 4th resulting in account lockout.

Production Node NODE1

Unauthorized Access Prohibited

Username: SEC_TEST

Password:

User authorization failure

Username: SEC_TEST

Password:

User authorization failure

Username: SEC_TEST

Password:

User authorization failure

Production Node NODE1

Unauthorized Access Prohibited

Username: SEC_TEST

Password:

User authorization failure

The second output shows that user SEC_TEST is in the intrusion database. This user will need to be removed from the intrusion file and have their password reset by the security administrator.

NODE1::> sho intru

Intrusion	Type	Count	Expiration	Source
-----	----	----	-----	-----
USERNAME	INTRUDER	4	21-NOV-2003 18:18:17.62	SEC_TEST on

NODE1

Using our system detective auditing tool we can see that SEC_TEST did indeed log in more than three times. To get this report from a DCL prompt:
sysdet report/database=openv\$root:[system_detective.NODE1]-
detective_database.dat/trigger=login_failures/since=20-nov-2003

```
=====
20-NOV-2003 18:18:17 => Event Severity: CRITICAL
Username: SEC_TEST, Process: SEC_TEST, Node: NODE1
Terminal: TNA307:, Port: Host:_192.168.2.105_Port:_4520, Security Event ID:
90547369610652849
Event Description: User is PREVIOUSLY MONITORED (NO LOG) due to trigger
event
Event Trigger: LOGIN_FAILURES = 3
Event Reason: User SEC_TEST has login failures in excess of 3
=====
```

Test 6: VPN users connecting to host (Item 6)

All remote users using VPN will be accessing the host via the xxx.xxx.0.0/16 subnet. In the configuration file of system detective we will be monitoring all users logging in starting with the xxx.xxx.0.0/16 subnet. Here we can see that SEC_TEST logged into host NODE1 on Nov 9/2003 at 08:22:31. The event was triggered by port=xxx.xxx. The user is now being monitored and if need be, the session may be played back using the sysdet playback function.

```
=====
9-NOV-2003 08:22:31 => Event Severity: INFORM
Username: SEC_TEST, Process: SEC_TEST, Node: NODE1
Terminal: TNA253:, Port: Host:_xxx.xxx.251.253_Port:_1042, Security Event ID:
36328528010652195
Event Description: User has TRIGGERED an alarm due to trigger event
Event Trigger: PORT = xxx.xxx.
Event Reason: User SEC_TEST has logged in from source port xxx.xxx.
=====
```

Test 7:modification of system parameters using system generation (SYSGEN) utility (Item 13)

Any user with privilege to use the system generation utility will be monitored once that user invokes the utility. User will receive warning that they are accessing a restricted image or file. From the command prompt :

```
NODE1::> mcr sysgen
SYSGEN> show/job
```

Message at 13-NOV-2003 19:11:38.03 to terminal TNA318:=>
You are accessing a restricted file or image

System detective then shows this report. From the DCL command prompt:
sysdet report/database=openv\$root:[system_detective.NODE1]-
detective_database.dat/object=sysgen/since=13-nov-2003

```
=====
13-NOV-2003 19:11:38 => Event Severity: CRITICAL
Username: SEC_TEST, Process: _TNA318:, Node: NODE1
Terminal: TNA318:, Port: Host:_192.168.2.105_Port:_2442, Security Event ID:
182895536010653090
Event Description: User has TRIGGERED an alarm due to trigger event
Event Trigger: IMAGE = SYSGEN
Event Reason: User SEC_TEST has executed image SYSGEN
=====
```

```
=====
13-NOV-2003 19:11:38 => Event Severity: CRITICAL
Username: SEC_TEST, Process: _TNA318:, Node: NODE1
Terminal: TNA318:, Port: Host:_192.168.2.105_Port:_2442, Security Event ID:
182895536010653090
Event Description: User is PREVIOUSLY MONITORED (NO LOG) due to trigger
event
Event Trigger: IMAGE = SYSGEN
Event Reason: User SEC_TEST has executed image SYSGEN
=====
```

Test 8: default proxy login accounts (Item 12)

In this environment only privileged accounts should have proxy logins, those being system and security administrators. Proxy logins are used to copy files from development to production when software install arise. From our output you can see that only two accounts, SEC_TEST and ADM_TEST are allowed to copy from node NODE1 to NODE2.

```
NODE1::> mcr authorize
UAF>
```

```
Message at 20-NOV-2003 17:27:17.10 to terminal TNA1228=>
You are accessing a restricted file or image
```

```
UAF> show/proxy NODE1:.*
```

```
Default proxies are flagged with (D)
LOCAL:.NETWORK.PRODUCTION.NODE2::SEC_TEST
SEC_TEST (D)
LOCAL:.NETWORK.PRODUCTION.NODE2::ADM_TEST
ADM_TEST (D)
LOCAL:.NETWORK.PRODUCTION.NODE2::ADM_TEST
ADM_TEST (D)
LOCAL:.NETWORK.PRODUCTION.NODE2::ADM_TEST
ADM_TEST (D)
UAF>
```

Test 9: password length (Item 11)

When setting up a new user or resetting a current users password, any length of password will suffice for the initial password. That is when the user logs in with that initial password they must create a new password for themselves. Here is where the password must be 6-32 characters in length. The output will show the resetting of the password with length fewer than 6 characters (password=abc). The system will set the password with 3 characters.

```
NODE1::> mcr authorize
UAF>
```

Message at 20-NOV-2003 17:34:38.80 to terminal TNA1228=>
You are accessing a restricted file or image

```
UAF> modify/password=abc user_8224
%UAF-I-PWDLESSMIN, new password is shorter than minimum password
length
%UAF-I-MDFYMSG, user record(s) updated
UAF>
```

I will attempt to login as that user with a password fewer than 6 characters and again with more than 32 characters. You will see the user must select a password between 6 and 32 characters.

Unauthorized Access Prohibited

Username: user_8224
Password:

Welcome to NODE1

Last interactive login on Monday, 3-NOV-2003 14:01:32.33

New password:
Verification:
Password length must be between 6 and 32 characters; password not changed
Please try again or press <CTRL/Y> to abort login

New password:
Verification:
Password length must be between 6 and 32 characters; password not changed
Please try again or press <CTRL/Y> to abort login

New password:

Test 10: Field Service account (Item 15)

We check the field service account to verify that the flag field shows disusered.
Account cannot login unless flag is removed.

```
NODE1::> mcr authorize
UAF>
```

Message at 20-NOV-2003 20:33:19.40 to terminal TNA1236=>
You are accessing a restricted file or image

```
UAF> show decfield
```

```
Username: DECFIELD          Owner: Field Service
Account: SYSTEM             UIC:  [1,10] ([DECFIELD])
CLI:   DCL                  Tables: DCLTABLES
Default: SYS$SYSROOT:[SYSMGR]
LGICMD: LOGIN
Flags: DisUser
Primary days: Mon Tue Wed Thu Fri
Secondary days:              Sat Sun
No access restrictions
```

Measure Residual Risk - Low

There always seems to be risks with any device connected to a network, whether it be development or production. In our case we are auditing a mission critical production server that needs to be online at all times. The checks found in section 2 are on going audits on a daily, weekly and monthly basis. When running the vulnerability enumeration it was determined that all clients connect to the host via the telnet service. This would be an extreme vulnerability had the clients been connecting via the internet but these clients are connecting via an internal network not seen on the internet. There still is a possibility that an insider could use a product to sniff the wire to enumerate usernames and passwords. This risk is still considered low as all institutions are on segregated networks so clear text information, such as telnet authentication could not be seen by a malicious user on another segment. We then have to think about a malicious user sniffing the wire on their network segment. After speaking with an ABC network resource it was found that approx 75% of the institutions run a switched network, this does reduce the risk. As more and more institutions upgrade their networks, ABC recommends that switched networks be used to replace hubs but ultimately it is up to the client as they are in complete control over their own network segment. Throughout the checklist in section 2, focus was given to the monitoring and checking of user parameters of those logging into and using the system. With the changing times more and more users within ABC are now working from home or are road warriors working from other remote sites. The users do log in remotely via VPN and this is something that not only ABC has to deal with but thousands of other companies. The risk of an unauthorized user logging into the

production server would be very minimal as most users in ABC do not have access to production servers. The unauthorized user would need credentials to a VPN account as well as credentials to the VMS servers in order to gain access. Laptop users connecting to their home computer networks, possibly catching a worm or virus and then plugging into the ABC network is another risk that ABC has to deal with. Although this might affect other operating systems, VMS seems to be immune to the various outbreak in vulnerabilities. With this audit I feel all control objectives were achieved.

Is this system auditable?

Since the system is mission critical in the ABC environment, protection and detection are a necessity. Running the vulnerability assessment tool on the VMS cluster on a monthly basis provides the security administrators a baseline that can be compared with the previous month's audits and should be a definite part of the checklist. Using the audit tool by Point Secure, System Detective AO helps the security administrators monitor login failures, intrusions, the accessing of critical files, and provides a session timeout mechanism should users leave their workstations unattended for an extended period of time. The Point Audit software by Point Secure is used to check user account parameters, privileges, and system and file security settings. All of these tools mentioned produce reports that demonstrate that controls in place are working correctly.

© SANS Institute 2004, Author retains full rights.

Assignment 4

Risk Assessment

Summary

The focus of the audit was to look at the security controls regarding the VMS production cluster in the ABC environment. In particular we looked at three types of audit checks: services running on the VMS system and vulnerabilities if any, change control and the monitoring of user access. The security administrator started off with running a vulnerability assessment on node "NODE1" to find what services were running on this system and if any vulnerabilities were associated with those services. We used the Shadow Security Scanner by Safety-Lab to perform this assessment. An important component of an audit process should include the process surrounding change control, we need to identify a good process in place that identifies who signs off on the process and who does the install or change to the operating system. The main focus of the audit was to look at user access, their accounts and how we were to monitor the over 1000 clients on the clustered systems. We completed this audit by using VMS audit software from PointSecure and the hp Open VMS Guide to System Security utilities. Below are the audit findings.

VMS Operating System Vulnerability Enumeration

Open Ports - Compliant

The security administrator ran the Shadow Security Scanner to assess what services were running. I found that ports 21, 23, 25, 123, 110 and 515 were open. When comparing with the previous months scan, it was found that the results were the same. I will however, attempt to explain why these services are needed.

Port 21 – Users on the VMS operating system do have access to FTP but it was found that Anonymous FTP was enabled. This account has now been disabled. You can see that when trying to login with the "anonymous" account the output shows this account disabled.

NODE2::> ftp NODE1

220-CONNECTING TO A REAL SYSTEM... OPENVMS

220 node1 HGFTP server V3.1 ready.

Connected to Node1.abc

Name (node1.abc:sec_test): anonymous

331 Guest login Okay, send ident or e-mail address as password.

Password:

530-Not logged in.

530 Account is disabled

User account "anonymous" flag is set to disuser

Username: ANONYMOUS

Account: MGFTP

Owner: FTP Anonymous

UIC: [2000,2000] ([MGFTP,ANONYMOUS])

- 31 -

CLI: DCL **Tables: DCLTABLES**
Default: MGFTP\$ROOT:[ANONYMOUS]
LGICMD: LOGIN
Flags: DisUser

Port 23 – users login via telnet. There is a possibility that an insider could use some type of network sniffing product to enumerate usernames and passwords as telnet is transported in clear text. The institutions are on segregated networks so institutions would not be able to see each other's username and password information passing through the wire. There is still the possibility that a malicious user could sniff the wire within the institutions own network. 75% of the clients do have switched networks so this reduces the risk within their network. ABC recommends that those institutions upgrading their hardware implement a switched network.

Port 25 - Needed for the VMS mail functionality between users and ABC. TCP banner shows system information, which could be used by an attacker. Risk - Low

Port 123 - Network Time Protocol, all systems within the cluster must be synchronized.

Port 110 – Needed to receive VMS email. TCP banner shows system information, which could be used by an attacker. Risk - Low

Port 515 – Port is currently open to support printing functionality

User Access and how they are monitored

Test 5: Login failure – Intruder database - Compliant

One of the more important audits from a security or system administrator's standpoint is to guarantee that there is a lockout mechanism in place when it comes to logging into the system. Here we tested to make sure that only 3 attempts were allowed and that on the fourth attempt, the user or unauthorized user's account would be placed into an intruder file. The account is held in the intruder file for 24 hours or until the account is removed from the intruder database. Once in the intruder file, a legitimate user would have to request a password reset from the security administrator. We feel this is a sufficient amount of attempts to log into the system. This might not deter an unauthorized user from using brute force software to break into the system but the risk of logging into an account would be minimal. The security administrator analyzes the reports produced by System Detective on a daily basis.

Test 9: Password length - Compliant

During our testing we wanted to make sure we had a sufficient password length when it came to authenticating to our VMS system. Passwords under 6 characters were deemed insufficient in ABC so we checked password length from 6 to 32 characters. We used the parameters stated in the hp Open VMS "Guide to System Security". From the test you can see that we first modified the password for user_8224 to "abc". As security or system administrators we are able to set the initial password to whatever length we wish. The password length comes into effect not when the user logs in with the initial password of "abc" but when they create their password. Here the password length must be from 6 to 32 characters. The test includes 2 attempts to set

the password, one under 6 characters and the other over 32 characters. The only recommendation to management would be to change the password length to between 8 and 32 characters.

Test 2: Idle Sessions - Compliant

There have been problems in the past where users would leave their workstations for extended periods of time or leave for the day without logging out of the VMS system. With this audit check we wanted to monitor those that were most notorious for doing this. This is a security risk, in that, if they happen to leave their workstation for a period of time, their VMS session is still active and anyone passing by could gain access to the system with that users privileges. Using system detective, we have set up the configuration file to warn users after 45 and 55 minutes with their session being terminated after 60 minutes. At this time, security administrators and users feel this is an appropriate time for warnings and session termination.

Test 4: User access - Second level support logging - Compliant

Second level support is a necessity at ABC when institutions have problems regarding database functionality. The question surfaces around how to monitor and log this activity when second level support needs to be involved. The security administrators have created a forced_logging identifier for all support users which forces them to log into another account that starts the logging process. They will then login using their own VMS account. The session is logged until they are completed with the support call and logged out of the system. The audit findings show that support user SEC_TEST attempted to log into the system with their own VMS account without success. They must log into the forced_logging account prior to logging into their own account. Log files are created in a directory that cannot be tampered with. Currently system detective is not monitoring users with the forced_logging identifier however all users logging into the system are monitored. It is the security and system administrators' recommendation that this be done as an added detection and for easier queries and reporting.

Test 3 and 7: Check for modification of system user authorization file (SYSUAF.DAT) and system generation utility (SYSGEN) - Compliant

As with most systems, it is important to log who has control over the creation, modification and deletion of accounts and what privileges those accounts have on the system. It is also equally important to know who has authorization to change system parameters. These two utilities are currently monitored by system detective and analyzed on a daily basis. Currently the system detective configuration file alerts when any user attempts to access these files. From our audit checks 3 and 7 you can see that the user receives a message that they are accessing a restricted file or image. The only users that should have access to these utilities are the security and system administrators. Users with privileges deemed normal (TMPMBX and NETMBX) will receive an insufficient or file protection violation. From our audit checks, you will see that from the system detective report SEC_TEST was monitored while using these two functions. We can use the system detection playback function to analyze just what was modified during this session. The security administrator recommendation is to change the system detective configuration file to delete the session for any user (with the exception of the security and system administrators) that try and access these utilities instead of just receiving the warning.

Test 6: VPN users connecting to host - Compliant

We wanted to audit this item since more and more users have the ability to log into the host remotely. Using system detective we modified the system detective configuration file to monitor the alert trigger port or IP address (xxx.xxx) of those logging in remotely. The system detective report shows that user SEC_TEST logged in through the VPN on port xxx.xxx.251.253. We can use the system detective playback function to analyze this session should there be a need.

Test 10: Field Service Account - Compliant

The field service account is used for support when maintaining or upgrading hardware and software on the Compaq Alpha Servers. This does not include OS upgrades and patch management. This field service account is very powerful and should be disabled when not in use. This check provides assurance that the account is indeed disabled and is checked on a regular basis. From the audit check it is determined that the account “decfield” was disabled. There are procedures in place with regards to when the account is enabled and disabled.

Test 8: Default proxy login accounts - Compliant

Proxy logins let you access files across a network without specifying a username or password. These logins are used in the ABC Company only by security and system administrators. This check provides assurance that only these accounts have proxy logins.

Appendix A: References

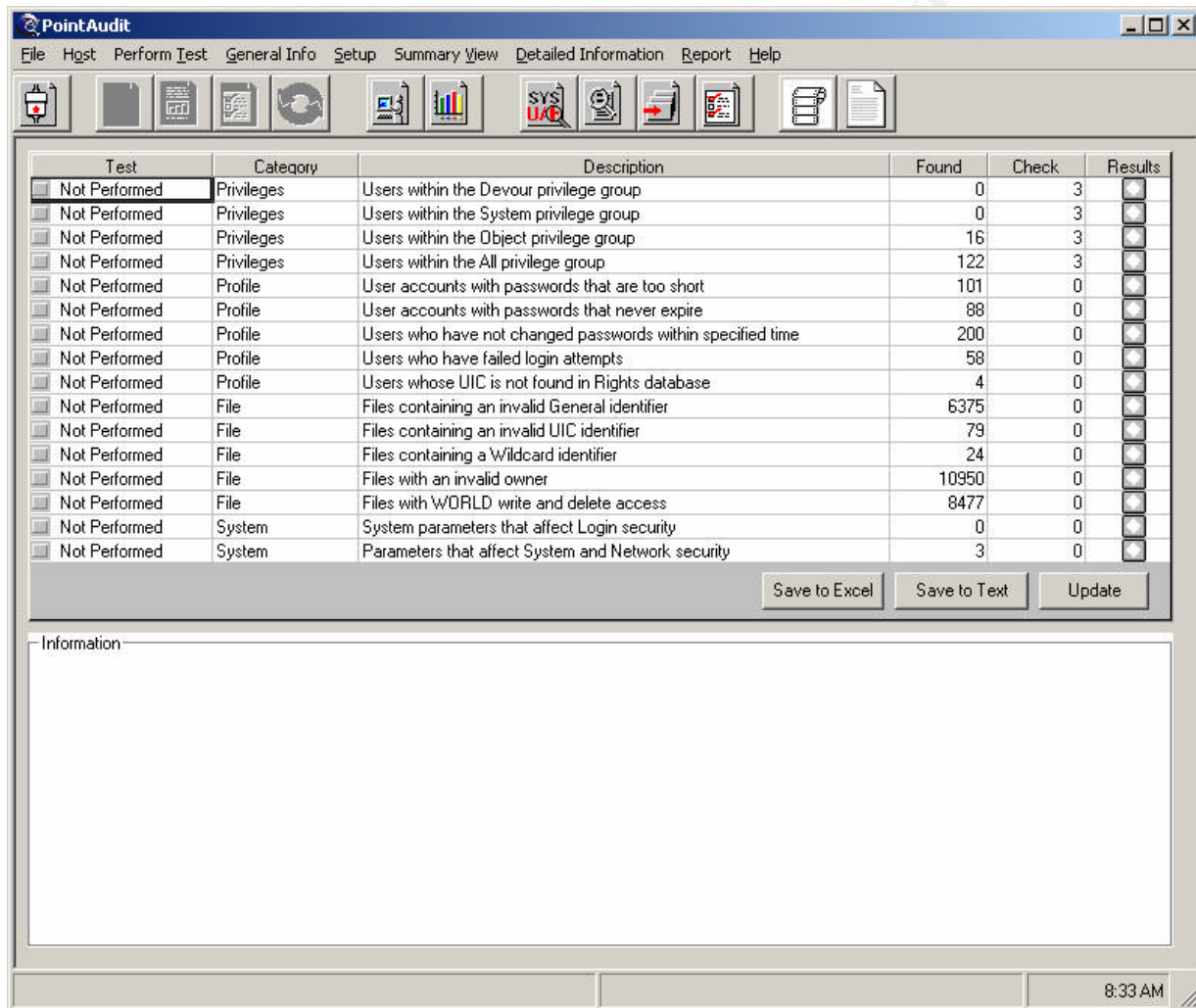
1. Point Audit 3.2 Users Guide, PointSecure Inc.
2. System Detective AO User Guide, PointSecure Inc.
3. Defense Information Systems Agency, "VMS - OpenVMS Security Checklist", 31 October 2003, url <http://csrc.nist.gov/pcig/cig.html> , "Vax VMS Checklist"
4. Safety-lab, Shadow Security Scanner, URL <http://www.safety-lab.com/en/products/1.htm>
5. hp OpenVMS Guide to System Security Available at: <http://h71000.www7.hp.com/doc/731FINAL/6346/6346PRO.HTM>, (2002, June)

© SANS Institute 2004, Author retains full rights.

Appendix B:

PointAudit 3.2

We must first start the application by selecting Start→Programs→PointSecure→PointAudit 3.2. Below is a screenshot of the application.



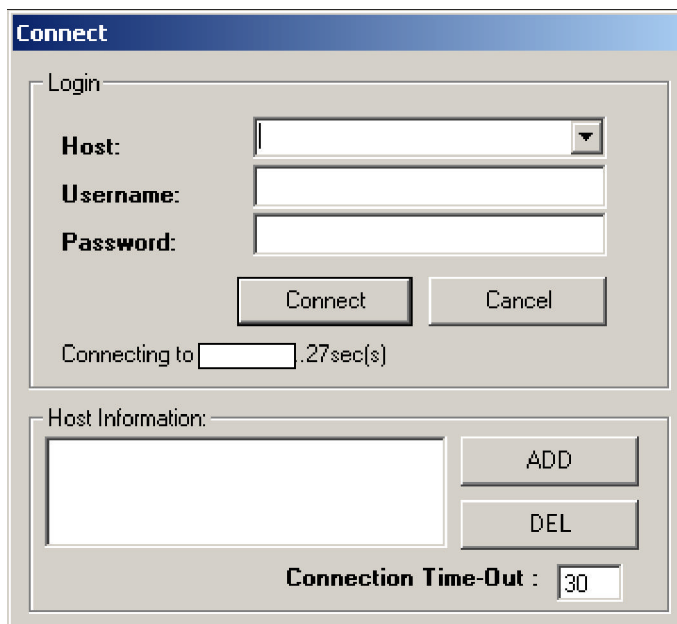
Once the application has started, the administrator must first connect to the VMS host they wish to analyze. Enter the host, username and password parameters as noted below. Select "Connect" and the connection will be established to the VMS host node1.abc.

Host: node1.abc

Username: sec_test

Password: xxxxxxxx

We would then select on connect



Connect

Login

Host:

Username:

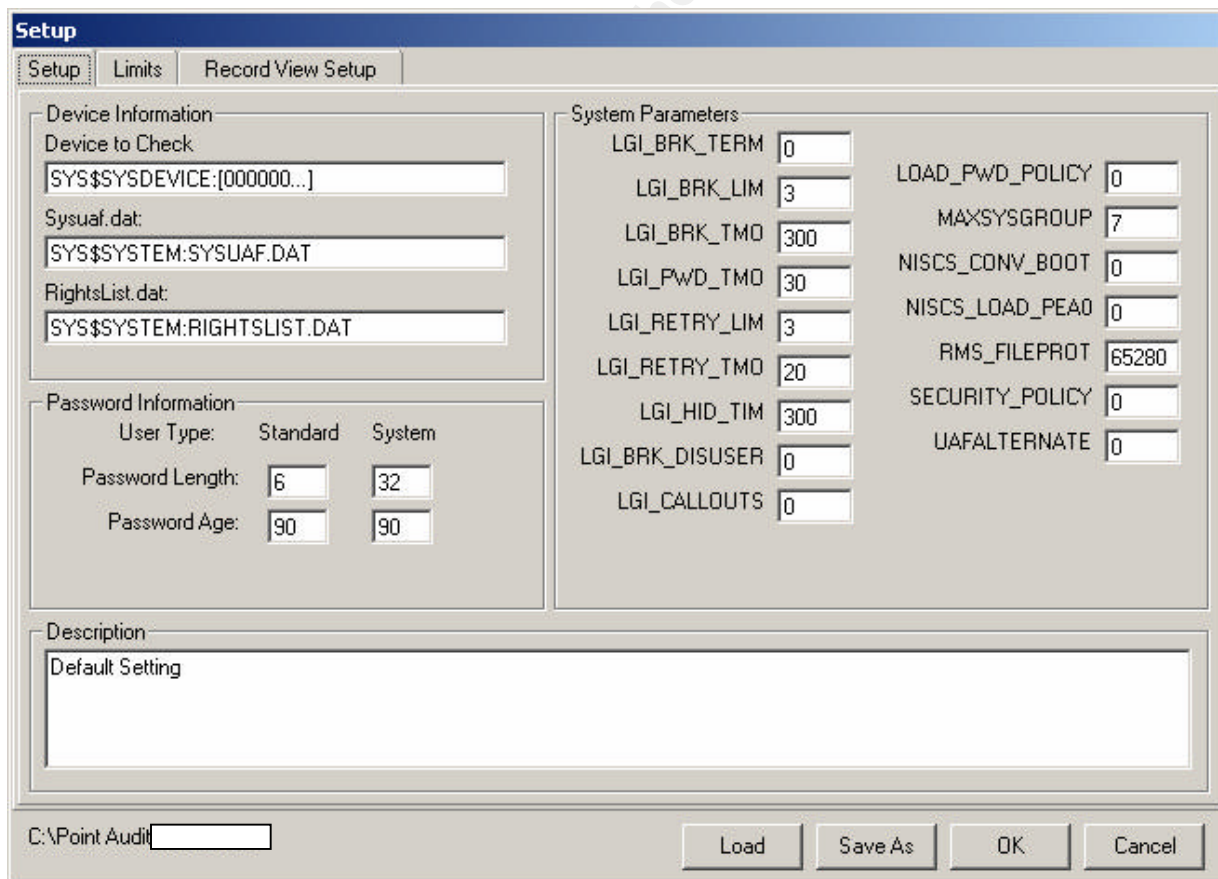
Password:

Connecting to .27sec(s)

Host Information:

Connection Time-Out :

Select "Setup" to look at our system parameters and modify if need be. Shown are default settings. The setup tab is divided into four sections: password Information, device information, system parameters and description.



Setup

Setup Limits Record View Setup

Device Information

Device to Check:

Sysuaf.dat:

RightsList.dat:

Password Information

User Type: Standard System

Password Length:

Password Age:

System Parameters

LGI_BRK_TERM

LGI_BRK_LIM

LGI_BRK_TMO

LGI_PWD_TMO

LGI_RETRY_LIM

LGI_RETRY_TMO

LGI_HID_TIM

LGI_BRK_DISUSER

LGI_CALLOUTS

LOAD_PWD_POLICY

MAXSYSGROUP

NISCS_CONV_BOOT

NISCS_LOAD_PEA0

RMS_FILEPROT

SECURITY_POLICY

UAFALTERNATE

Description

Default Setting

C:\Point Audit

The “Limits Tab” section is divided into six sections: flags, privileges, errors, password lifetime, password change and access.

Setup Limits Record View Setup

Flags

- LOCKPwD
- DISUSER
- DISREPORT
- DISRECONNECT
- DISIMAGE
- GENPwD
- DISMAIL
- DISNEWMAIL
- DISWELCOME
- CAPTIVE
- NONE

0

Privileges

- ACNT
- ALLSPOOL
- ALTPRI
- BUGCHK
- BYPASS
- CMEXEC
- CMKRNL
- DETACH
- DIAGNOSE
- EXQUOTA
- GROUP

0

Error

- No Error
- Error1
- Error2
- Error3
- Error4
- Error5
- Error6
- Error7
- Error8
- Error9
- Error10

0

Password Lifetime (Days)

- None
- >301
- 151-300
- 90-151
- 60-90
- 30-60
- <30

0

Password Change (Days)

- None
- >301
- 151-300
- 90-151
- 60-90
- 30-60
- <30

0

Access

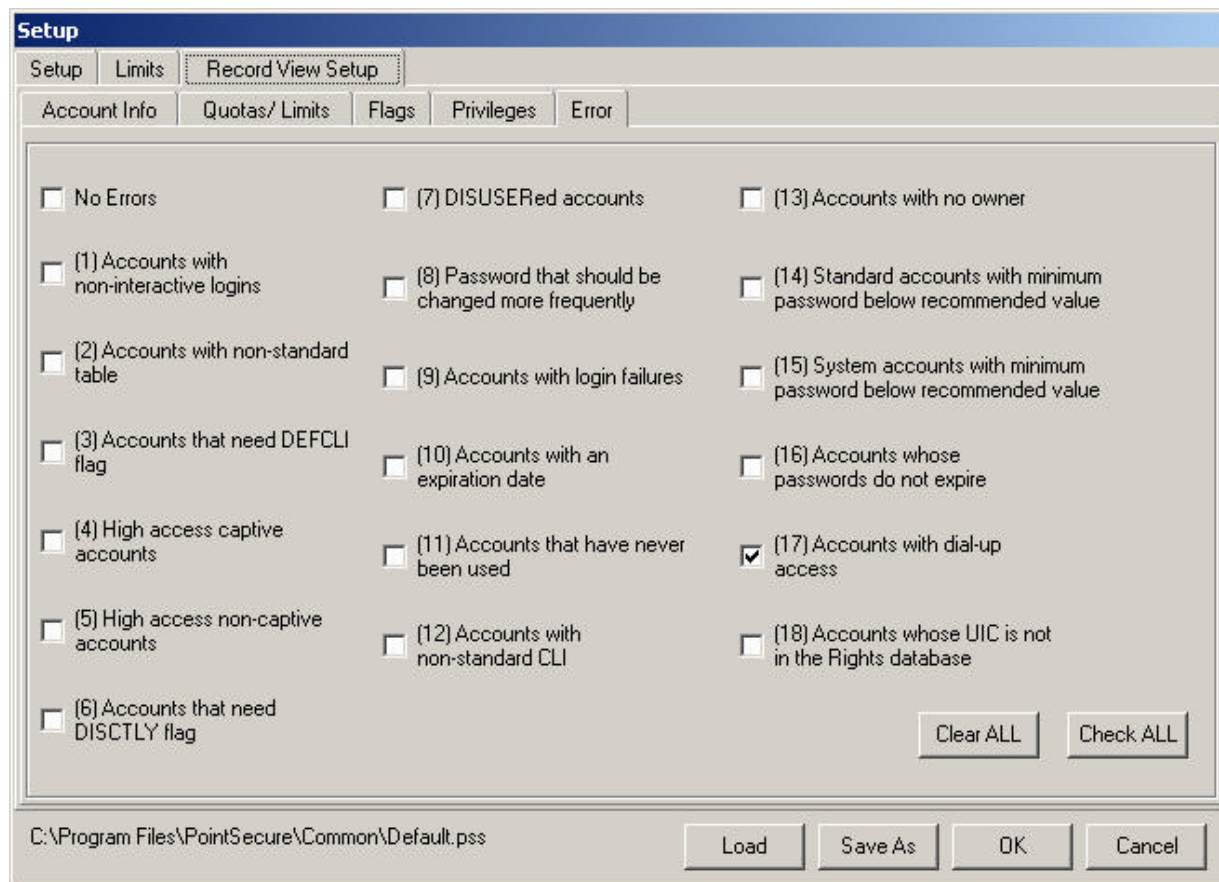
- Network
- Batch
- Local
- Dialup
- Remote

0

C:\Program Files\PointSecure\Common\Default.pss

Load Save As OK Cancel

The record view tab contains five additional tabs: account info, quotas/limits, flags, privileges and errors. These tabs allow you to select what information you would like displayed. Shown in the screen shot is an example of selecting just error 17 (accounts with dial-up access). For our auditing purposes we are going to modify the setup tab and enable all checks in the record view setup tab.



We are now ready to perform our checks. Select “PerformTest” and then select “All”. This will run profile, privilege, file and system checks. Here is a screen shot after all tests have been performed. You will notice under the “Test” tab that all checks were performed.

Test	Category	Description	Found	Check	Results
✓ Performed	Privileges	Users within the Devour privilege group	0	3	●
✓ Performed	Privileges	Users within the System privilege group	0	3	●
✓ Performed	Privileges	Users within the Object privilege group	16	3	◆
✓ Performed	Privileges	Users within the All privilege group	122	3	◆
✓ Performed	Profile	User accounts with passwords that are too short	101	0	◆
✓ Performed	Profile	User accounts with passwords that never expire	88	0	◆
✓ Performed	Profile	Users who have not changed passwords within specified time	200	0	◆
✓ Performed	Profile	Users who have failed login attempts	58	0	◆
✓ Performed	Profile	Users whose UIC is not found in Rights database	4	0	◆
✓ Performed	File	Files containing an invalid General identifier	6375	0	◆
✓ Performed	File	Files containing an invalid UIC identifier	79	0	◆
✓ Performed	File	Files containing a Wildcard identifier	24	0	◆
✓ Performed	File	Files with an invalid owner	10950	0	◆
✓ Performed	File	Files with WORLD write and delete access	8477	0	◆
✓ Performed	System	System parameters that affect Login security	0	0	●
✓ Performed	System	Parameters that affect System and Network security	3	0	◆

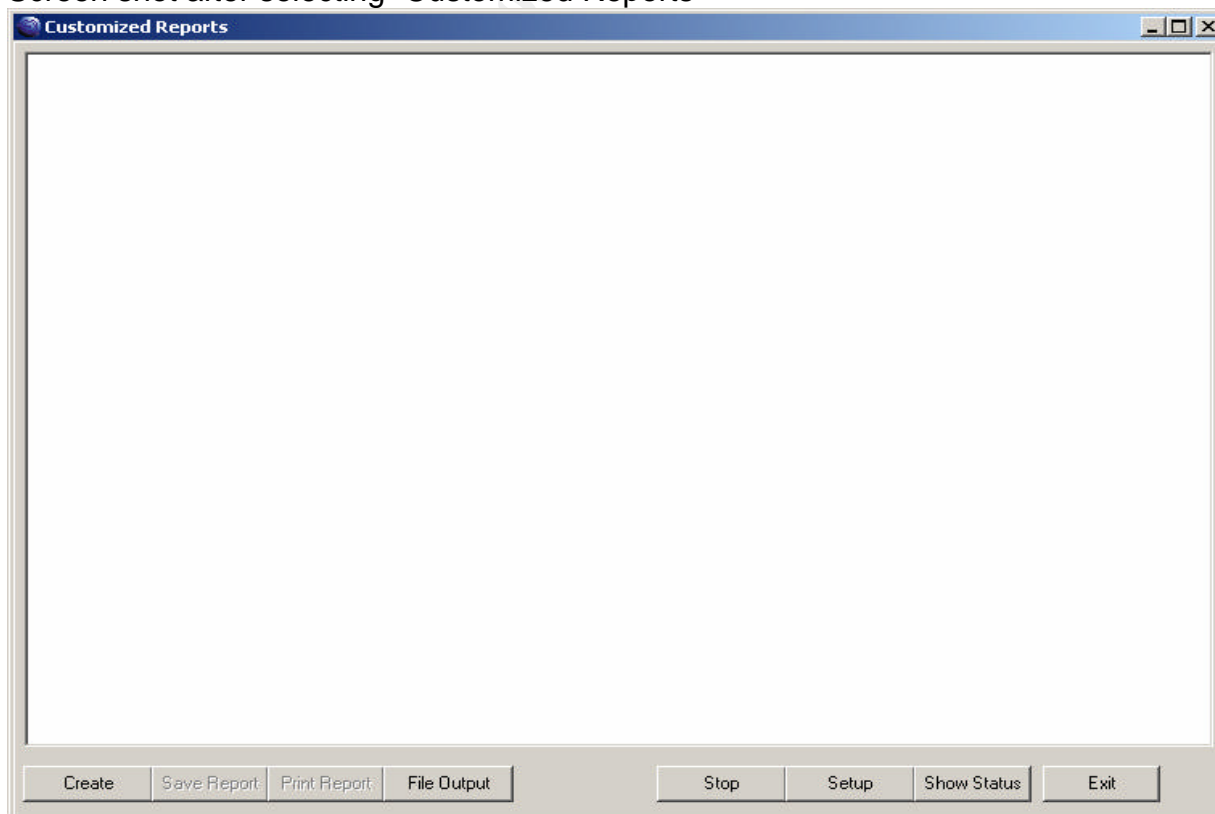
Information

9:55 AM

We can now create our audit reports from the tests that were just conducted. We select “Report” and then “Customized Report”.

Test	Category	Description	Found	Check	Results
✓ Performed	Privileges	Users within the Devour privilege group	0	3	✓
✓ Performed	Privileges	Users within the System privilege group	0	3	✓
✓ Performed	Privileges	Users within the Object privilege group	16	3	✗
✓ Performed	Privileges	Users within the All privilege group	122	3	✗
✓ Performed	Profile	User accounts with passwords that are too short	101	0	✗
✓ Performed	Profile	User accounts with passwords that never expire	88	0	✗
✓ Performed	Profile	Users who have not changed passwords within specified time	199	0	✗
✓ Performed	Profile	Users who have failed login attempts	59	0	✗
✓ Performed	Profile	Users whose UIC is not found in Rights database	4	0	✗
✓ Performed	File	Files containing an invalid General identifier	6375	0	✗
✓ Performed	File	Files containing an invalid UIC identifier	79	0	✗
✓ Performed	File	Files containing a Wildcard identifier	24	0	✗
✓ Performed	File	Files with an invalid owner	11073	0	✗
✓ Performed	File	Files with WORLD write and delete access	8470	0	✗
✓ Performed	System	System parameters that affect Login security	0	0	✓
✓ Performed	System	Parameters that affect System and Network security	3	0	✗

Screen shot after selecting “Customized Reports”



To set up our customized reporting we must select “Setup”, which will provide us with this screen shot. Here we can check off which audit reports we wish to see, in this case we would be looking for an error report on one or perhaps all 18 items..

Setup

Setup Limits **Record View Setup**

Account Info Quotas/ Limits Flags Privileges Error

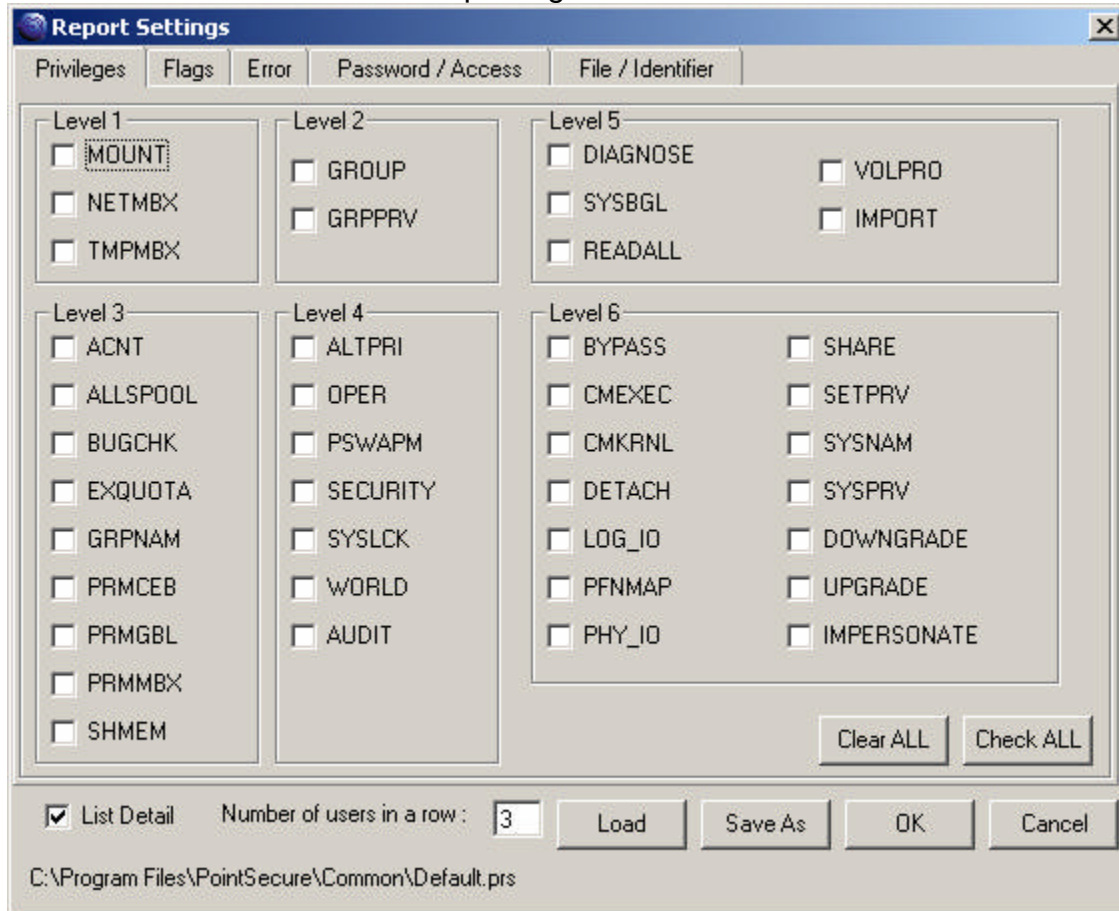
<input type="checkbox"/> No Errors	<input type="checkbox"/> (7) DISUSERed accounts	<input type="checkbox"/> (13) Accounts with no owner
<input type="checkbox"/> (1) Accounts with non-interactive logins	<input type="checkbox"/> (8) Password that should be changed more frequently	<input type="checkbox"/> (14) Standard accounts with minimum password below recommended value
<input type="checkbox"/> (2) Accounts with non-standard table	<input type="checkbox"/> (9) Accounts with login failures	<input type="checkbox"/> (15) System accounts with minimum password below recommended value
<input type="checkbox"/> (3) Accounts that need DEFCL flag	<input type="checkbox"/> (10) Accounts with an expiration date	<input type="checkbox"/> (16) Accounts whose passwords do not expire
<input type="checkbox"/> (4) High access captive accounts	<input type="checkbox"/> (11) Accounts that have never been used	<input type="checkbox"/> (17) Accounts with dial-up access
<input type="checkbox"/> (5) High access non-captive accounts	<input type="checkbox"/> (12) Accounts with non-standard CLI	<input type="checkbox"/> (18) Accounts whose UIC is not in the Rights database
<input type="checkbox"/> (6) Accounts that need DISCTLY flag		

Clear ALL Check ALL

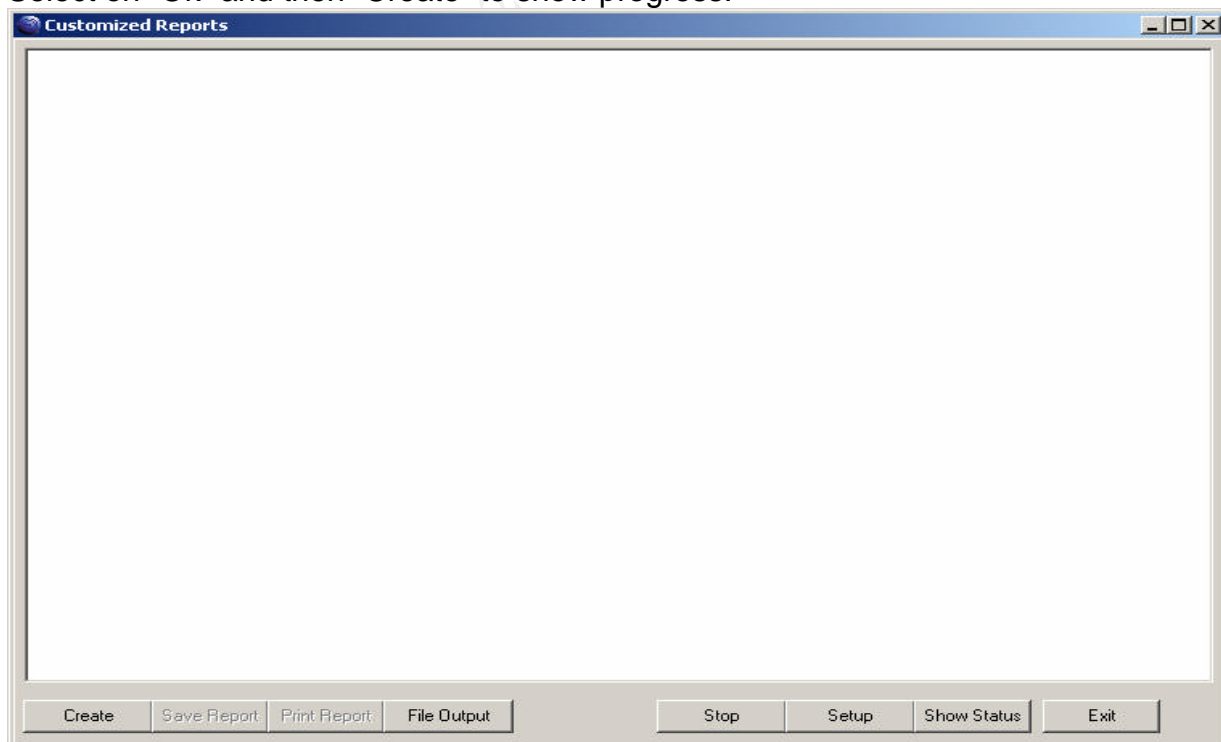
C:\Point Audit

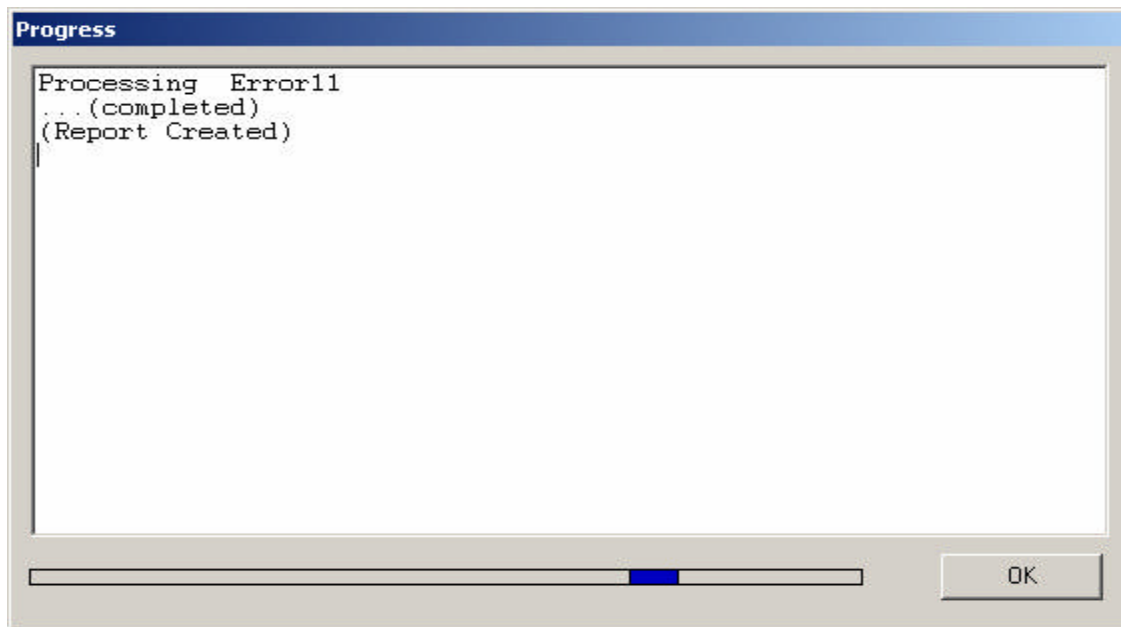
Load Save As OK Cancel

Here is another screen shot of the “Customized Report Settings”. In this case we wish to see which users have certain privileges.



Select on “Ok” and then “Create” to show progress.





Report created

