Global Information Assurance Certification Paper

Security Audit on OpenVMS:
An Internal Auditor's Perspective

GSNA Practical Assignment (v.3.2)
Option 1

Submitted by Kevin Rich – November 2004

Abstract

The purpose of this paper is to fulfil the requirements of a practical assignment of the GIAC Systems and Network Auditor (GSNA) certification. This practical follows the assignment criteria set out in Version 3.2 of the GSNA Practical Assignment (July 1, 2004).

Although there are a number of opportunities to audit hardware and operating systems that have been recently implemented within this organization, I have chosen a system that is associated with a legacy operating system and application. It will be a DEC (now HP) DS-10 AlphaStation running OpenVMS v7.2-1 that serves as a web interface within the organization to several Operational Support Systems for monitoring and alarming the telco and IP networks.

I have also provided a background in the applicable industry standards for IT management, controls, and audit, and how this organization has applied them. This may provide some guidance if the reader is endeavouring to introduce a consistent audit approach to their own environment.

Table of Contents

* Note: the numbers in brackets in Part #2 indicate the number of tests associated with each control item in the checklist.

** Note: these items in Part #3 indicate the ten (10) technical tests that are being conducted.

Part #1 – Research in Audit, Measurement Practice, and Control

1.1 Audit Scope

1.1.1 Background on system security audits within the organization

Security audits, including Systems Security audits, are part of the fundamental internal audit plan in the organization. All submitted audits follow a prescribed template for submission to the Audit Committee, which is a committee of the Board of Directors.

The organization has selected ITIL as the IT Service Management standard. ITIL (Information Technology Infrastructure Library) was developed in the United Kingdom by the Office of Government Commerce (OGC) and eventually adopted internationally to promote sound IT management practices. It is a Best Practice Framework when used as a systematic approach to planning, development, delivery and support of IT services[1]. The Security of Information Services is not specifically covered under an ITIL Process, but is a function of Availability Management. This process optimizes the capability of the IT infrastructure to deliver a cost effective and sustainable level of availability that enables the business to meet its objectives. Security in ITIL is defined as the implementation of justifiable controls to ensure continued IT service within secure parameters of Confidentiality, Integrity, and Availability (CIA).

COBIT (Control Objectives for Information and related Technology) was developed as an industry standard for good Information Technology (IT) management and control practices. COBIT provides a reference framework for IT management and audit, and control and security practitioners[2]. This organization has adopted COBIT as the assessment and audit tool due to its strengths in IT controls and IT metrics. Auditors are increasingly being called on by management to proactively consult and advise on IT security and control-related matters. To support these management needs, the COBIT Management Guidelines provide specific Critical Success Factors, Key Goal Indicators, Key Performance Indicators and an associated Maturity Model for IT governance. COBIT consists of 34 IT Processes divided into Four Domains: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring. Detailed Control Objectives for Security are addressed under Delivery and Support, Process #5 (DS5).

Both ITIL and COBIT align with ISO17799, International Standards Organization Code of Practice for Information Security Management. Developed by the British Standards Institute (BSI) as BS7799, it is logically laid out in ten sections (see Appendix A) and can be used to develop an implementation schedule, with key controls as check points to ensure compliance. ISO17799 / BS7799 contains up-to-date recommendations on all aspects of Enterprise Security Policy including: formulating policy documentation;

---

[1] Information Technology Service Management Forum. *About ITIL*. ITSMF, 2004, http://www.itsmf.ca/about/itil.html, ITIL & ITSM World. *The ITIL and ITSM Directory*. 2004, http://www.itil-itsm-world.com/index.htm, Office of Government Commerce (UK). *The Official ITIL Webpages*. 2004, http://www.ogc.gov.uk/index.asp?id=2261

[2] Information Systems Audit and Control Association. *COBIT Overview*. ISACA, 2004, http://www.isaca.org/cobit.htm

allocating security responsibilities; performing risk assessment; defining and enforcing security perimeters and access controls; anti-virus strategy; and Internet and e-mail encryption[3].

ITIL is strong in IT processes, but limited in security and system development. COBIT is strong in IT controls and IT metrics, but does not provide process flows, and is not that strong in security. ISO 17799 is strong in security controls, but does not provide process flows. Therefore, the organization has decided to use a combination of all three to achieve the IT Infrastructure Auditing requirements, with a strategy based on ISO17799 to assess Systems Security.

The organization has written the Systems Security Policies to align to ISO17799 and a corresponding audit strategy has been developed to assess compliance to each section. This strategy was presented to and accepted by the Audit Committee.

1.1.2 Systems security issues within the organization

The organization provides voice and data telecommunications, cellular, ISP services, including digital television, and hosting services to business and residential customers. The infrastructure consists of digital telecommunications switches, cellular and fiber optic nodes, ATM switches, DSL nodes, hundreds of servers, routers and firewalls, and thousands of workstations to support both the internal business functions and customer services. Every brand and flavour of hardware and operating system may exist in this environment. Although network and IT architecture plans are working to minimize this, legacy systems will continue to be maintained on existing systems as long as it is operationally and financially prudent.

This creates a variety of potential security issues. Customer privacy and business confidentiality must be maintained, along with service availability and business continuity. And this must be done across all platforms in a ubiquitous manner, as much as possible.

To date, the focus on systems security has been on the newest systems and services that are being deployed. Vendors are providing better support for security on their newest platforms. However, some of the organization's operational support systems are running on, and being accessed by, legacy platforms. An example of this is the DEC VAX/Alpha platform used for network alarm monitoring and reporting. Although this system has been in use for over ten years, it is providing a critical function, and there has not been a justification or cost benefit to replace it with a newer application or platform. Upgrades and augmentation to the existing platform have kept the system performing satisfactorily.

[3] Securityauditor.net. *ISO 17799 Security Standard*. 2001 http://www.securityauditor.net/iso17799/, ISO 17799 Directory. *The ISO 17799 Service & Software Directory*. 2003, http://www.iso17799software.com/

1.1.3 System identification

Name: INSS1
Configuration: DS-10 AlphaStation e/w
- OpenVMS V7.2-1
- 2 - 36Gb HDD
- 512 Mb RAM
- 617 MHz processor (1 CPU)

IP: 1xx.xxx.208.25
DECnet: 10.xxx
Web Server: HP Secure Web Server based on Apache

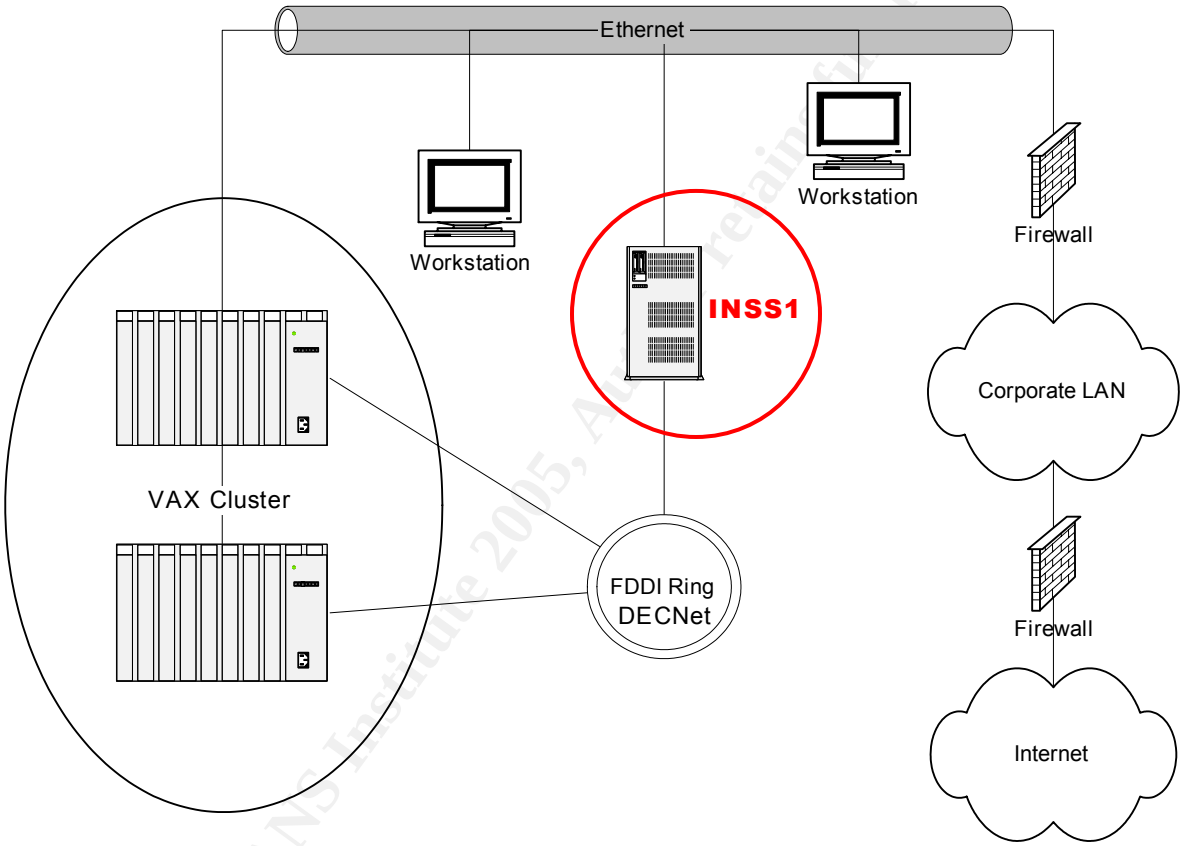

Figure 1 – System Architecture

1.1.4 Role of the system

This system is used as an internal web interface to Operational Support and Alarm Systems for the telco network. The system, itself, does not perform the actual business function, which we will define as "network alarming and monitoring". This system is not visible to the internet, and is not available on the corporate intranet to general users, but is available to specific users who require reports and information related to the status and alarms of the Operational Support Systems. Approximate number of persons accessing the system is 75.

1.1.5 Administration of the system

The system is administered within the Information Technology Management (ITM) department by several individuals who share the responsibility for Tier Three support for Operational Support Systems related to network monitoring and maintenance. Tier Three support is defined as system administration and primary interface for vendor maintenance. Tier Three support is responsible for system configuration, including hardware and software upgrades, and system security. In this case, they are also responsible for user account management. Tier Three support is not responsible for routine maintenance such as back-ups and patches.

1.1.6 Scope of this audit

This audit will assess the security configuration of the system, INSS1, with respect to the hardware, operating system and application. User access will be examined as it relates to issues identified in the significant risks at the system level. Network accessibility will be assessed only as it relates to this machine, not as it relates to external network elements (e.g. firewall protection). The complexities of evaluating the security from both the IP and DECnet network interfaces could provide enough work for a separate audit. A variety of tools and test methods will be used as well as direct interviews with the system administrator.

1.2 Significant Risks to the System

1.2.1 Business impact due to role of the system

This system performs a non-critical role in the organization. Complete loss or denial of service of this system would cause inconvenience and additional work for the users, but no loss of functionality of the business function itself (network alarming and monitoring). Compromising this system would allow unauthorized users access to information and, possibly, some control of the servers and devices that provide the business function.

1.2.2 Evaluation of the most significant risks to the system

The Risk to the system is a function of the Threat and Vulnerability, as well as the resulting Consequence if the Threat is realized. The threats are common to all systems, while the vulnerabilities are more specific to this system, depending on its location, both physically and logically, and how it is maintained and administered. The vulnerabilities in Table 1 were the result of the auditor's observations, and initial interviews and discussion with the System Administrator.

	Threat	Vulnerability	Risk	Consequence
1	Physical access to system /sabotage	System is in secured area in building with security desk at entrance	Low	Loss of access to information and control of other, more critical systems.
2	External access to system from unauthorized user with malicious intent	System is isolated behind multiple corporate firewalls on a private network	Medium/ High	Confidential business information may become public. Other, more critical systems may be open to attack
3	Loss of system access due to denial of service attack, virus, malicious code	System is isolated behind multiple corporate firewalls on a private network. A back-up system is configured on a test box.	Medium	Loss of access to information and control of other, more critical systems.
4	Internal access to system from unauthorized user	Access to system is restricted to valid user accounts with passwords. Users are further restricted to functions depending on user ID. Password lockout after 3 attempts.	Medium	Confidential business information may become public. Other, more critical systems may be jeopardized depending on intent of the user.
5	Improper use of system / damage to system through error from authorized user	Users are restricted to functions depending on user ID and level of expertise.	Medium	Loss of access to information and control of other, more critical systems.
6	Internal access to system from authorized user	Changes require the change request process to be completed. Malcontents with higher privileges could make system-impacting changes	Medium	Loss of access to information and control of other, more critical systems. Possible loss of more critical systems.
7	Critical security patches not installed	Critical patches are identified and installed as required.	Low	System may be more vulnerable to external access.

	Threat	Vulnerability	Risk	Consequence
8	Unnecessary ports /services running	Ports and services have been changed from default	Medium	System may be more vulnerable to external access.

Table 1 – Risk analysis

The system is not publicly accessible or internet-facing, so the risk is inherently reduced by the security of the corporate network. However, a breach of the corporate network would abruptly increase the risk of this system being compromised. External threats would immediately become internal threats, so it is imperative that systems be secure at the host level as well as the network level.

1.3 Current State of Practice

OpenVMS is considered to be one of the most secure operating systems. According to the late John Wisniewski, a former HP BCS Solutions Architect, "OpenVMS has had 52 CERT Advisories in 15 years – 10 times less than any other Operating System has had in the last 5 years."[4] There are currently no known viruses which infect OpenVMS systems[5]. This could be due to the prevalence of other operating systems in IT environments (Windows, UNIX), so less attention is paid to OpenVMS, or because it is acknowledged that OpenVMS is very difficult to compromise[6]. However, OpenVMS is used widely in installations that require high levels of security (finance, healthcare, government, telecommunications)[7], thus, in areas which may present attractive targets for hackers. Therefore, diligence is warranted.

Digital Equipment Corporation (DEC) initially designed OpenVMS with security in mind. Compaq, and then HP continued to support platform security as those companies merged. HP plans to support OpenVMS to at least 2011, and security continues to remain part of their product roadmap[8].

1.3.1 Resources for secure configurations and checklists

The best source for documentation for configuring OpenVMS is clearly the vendor. HP has many guides and manuals for configuring OpenVMS systems at: http://h71000.www7.hp.com/doc/os72_index.html

[4] Wisniewski, J., *Encompass Webcast OVMS Security*. MindIQ, 2004, p3, http://www.mindiq.com/resources/webcasts/JohnwEncompasswebcast031804.ppt
[5] Sophos Plc. *"Can my OpenVMS system become infected with a virus?"*. Sophos knowledgebase article, 2003, http://www.sophos.com/support/knowledgebase/article/156.html
[6] Jankowiak, P., Smiley, S., Wisniewski, J., "Virtually Unhackable" DEFCON9: Securing OpenVMS with System Detective, PointSecure Inc. White Paper, 2002. http://www.openvmsclub.ch/downloads/Defconwhite.pdf
[7] Hewlett-Packard. *Industry Solutions*, Hewlett-Packard Development Company, L.P., 2004, http://h71000.www7.hp.com/solutions/
[8] Hewlett-Packard, *OpenVMS Product Directions*. Hewlett-Packard Development Company, L.P., 2004, http://h71000.www7.hp.com/openvms/OpenVMSproductdirections.htm

The specific OpenVMS Guide to System Security for Version 7.2-1 can be found at: http://h71000.www7.hp.com/doc/72final/6346/6346pro.html
This is the vendor manual for securing the particular system being audited. It discusses the OpenVMS Security Model, and is targeted to system administrators and users who are responsible for protecting the operating system.

SANS has a number of papers related to OpenVMS security. Ones that are particularly of interest are:

Fundamentals for Securing OpenVMS Systems, GSEC Practical by Mario Babineau, April 1, 2003, http://www.giac.org/practical/GSEC/Mario_Babineau_GSEC.pdf

- This document summarizes the OpenVMS Model as described in the vendor's Guide to System Security and provides examples.

Open VMS 7-3.1, An Administrators View, GSNA Practical by Randy Buchanan, January 14, 2003, http://www.giac.org/practical/GSNA/Randy_Buchanan_GSNA.pdf

- This is a good example of a practical that specifically follows Option 1 of the GSNA assignment criteria for an OpenVMS system.

OpenVMS 7.2 Security Essentials, GSEC Practical by Jeff Leving, November 4, 2002, http://www.giac.org/practical/GSEC/Jeff_Leving_GSEC.pdf

- This paper provides an overview of the basic steps required to securely install the OpenVMS operating system. It references the OpenVMS Guide to System Security.

A Primer on OpenVMS (VMS) Security, GSEC Practical by Steve Bourdon, May 13, 2002, http://www.sans.org/rr/papers/index.php?id=604

- This document summarizes the OpenVMS Model as per the OpenVMS Guide to System Security, and provides a primer to security concepts and features specific to OpenVMS.

An Authentication Audit on OpenVMS: An Auditor's Perspective, GSNA Practical by Jeff Parker, April 15, 2002, http://www.giac.org/practical/Jeff_Parker_GSNA.doc

- In my opinion, this document reflects the type of audit report that could be received from an external auditor hired to review the security of a specific system. It contains an Executive Summary and Audit Findings in an abridged format, as well as the details and the requirements for the GSNA assignment criteria.

An excellent resource for checklists is the Computer Security Resource Center (CSRC) of the National Institute of Standards and Technology (NIST). The list of Checklists / Implementation Guides is http://csrc.nist.gov/pcig/cig.html

A VMS/OpenVMS checklist is available at:
http://csrc.nist.gov/pcig/CHECKLISTS/vms-openvs-srrchklst-v2r11.zip

- This is an exhaustive security guide and checklist for OpenVMS provided by the Defense Information Systems Agency (DISA).

AuditNet.org has various audit papers and checklists that can be referenced. The following are relevant to VMS security auditing:

OpenVMS Access Controls, Michelle Nguyen, May 26, 2004, http://www.auditnet.org/docs/OpenVMS%20Access%20Controls.doc
- A specific checklist of OpenVMS access controls as used by the Industrial Bank of Japan. This is a good reference for a security audit.

DEC VAX/VMS Operating System Security Review, Rey LeClerc, February 12, 2002, http://www.auditnet.org/docs/decvaxvm.txt
- Provides general security information and a detailed audit program for VAX/VMS.

Digital VAX/VMS Audit Program, Carolann Lazarus, August 29, 2000, http://www.auditnet.org/docs/vax_vms2.txt
- A high level VAX/VMS step-by-step audit guide that includes VMS Security which can be used as a starting point for a security audit checklist.

DEC VAX/VMS Operating System/Logical Security Review, Andy Ellsweig, http://www.auditnet.org/docs/vaxsecur.txt
- Provides general security information and a detailed audit program for VAX/VMS.

OpenVMS Operating System Security Audit Plan, Justyna Pawlikowska, June 13, 2002, http://www.isaca.org.pl/warsztat/OpenVMS_audyt.doc
- Provides a detailed audit plan for OpenVMS.

PointSecure offers products and solutions for securing and auditing OpenVMS. They have several tools which provide automation of security auditing. A free tool "Security SnapShot" is available that tests certain parameters of user accounts, passwords and ACLs. This can provide a starting point for further investigation. The SnapShot tool is available for download here: http://www.pointsecure.com/products/snap_shot.asp

In addition to leveraging the knowledge of the system administrator responsible for the system being audited, internal documentation and policies were referenced. These included corporate policies and audit control documents for system security.

There are many other references available that are applicable to auditing system security, although they may not be specific to the DEC/VMS operating system. I have included some that I find useful in the References.

Part #2 – Create an Audit Checklist

2.1 Audit Scope

2.1.1 Role

The system is used as an internal web interface to Operational Support and Alarm Systems for the telco and IP networks. Loss of availability of this system would impair operations, administration and support of the network elements. Access to this system could allow a user to gain information on the network, including capacity, performance, connectivity, and administration, and could also allow a user to further access certain network elements or gain management capabilities of those elements.

It is therefore crucial that the system cannot be accessed externally via IP or DECnet. It is also important that unauthorized users cannot access the system logically or physically.

2.1.2 Controls

The Checklist in Section 2.2 was developed from references (as listed in each item) and the company's internal policy and controls. These control objectives were developed based on ISO 17799 and are referenced as they apply to this situation. Controls have been listed based on the risk and threat analysis in Part 1, Table 1. p5.

2.1.2.1 Discovery:

Information gathering (or system discovery, target reconnaissance, or fingerprinting) is the first step that malicious persons would take to compromise a system. It consists simply of obtaining all system and user information to understand the environment.

Threat # (from Table 1): All

- Information gathering
  (ISO 17799 – 9.4.2)
  Ensure that access to network services or network equipment is restricted to authorized personnel.
  (ISO 17799 – 9.5.2)
  Ensure that only a generic banner or warning is provided upon access.

2.1.2.2 Policies:

The company's security policies will determine the commitment of management and staff to information security across the organization. Documented policies and the communication of management support will determine the employees' approach to every aspect of securing the system.

Threat #: All

- Corporate security policies
  (ISO 17799 – 3.1.1)

Ensure that the company has developed and implemented policies to address information security, aligning with ISO17799.

2.1.2.3 Physical Security:

The location of the system should protect it from physical security threats.

Threat #: 1

- Equipment security

  (ISO 17799 – 7.2.1)

  Ensure that computer, network and data resources are located in facilities consistent with the need to house those facilities.

2.1.2.4 Operations:

Operational procedures should be in place to mitigate security issues.

Threat #: All

- Change management

  (ISO 17799 – 8.1.2)

  Ensure that change control procedures are utilized for changes to production equipment or software other than changes outlined in Operations Procedures.

- Incident management

  (ISO 17799 – 8.1.3)

  Ensure that effective processes and procedures are developed and implemented for identification, reporting and subsequent handling of security related incidents.

- Segregation of duties

  (ISO 17799 – 8.1.4)

  Ensure that there is sufficient segregation of duties, wherever feasible, in all business procedures to reduce the risk of fraud such that it requires the collusion of two or more employees to commit a fraud.

- Security Patching

  (ISO 17799 – 10.5.1)

  Ensure that all operating systems for computer, network and data services are maintained at the most current security configuration that meets business needs and mitigates risk to an acceptable level.

2.1.2.5 User Profiles and Accounts:

A default installation of OpenVMS installs a number of default accounts. These default accounts, along with their default passwords, are well-known in the internet community.

Threats #: 3, 4

- Default accounts

  (ISO 17799 – 9.2.1)

  Ensure that appropriate identification is required for access to computer, network and data services via a User ID and authentication with a password.

- Passwords

  (ISO 17799 – 9.5.4)

Ensure that employees actively manage their passwords used to authenticate to computer, network and data services for privileged access per this policy

2.1.2.6 Access to Files:

Proper security management of file access and ACLs is important to determine the privileges that users and groups of users are allowed on the system.

Threats #: 2, 3, 4, 6

- Access control lists (ACL)
  (ISO 17799 – 9.4.7)
  Ensure that logical segregation of computer, network and data services is provided such that employees have access to information and services required by them, but not access to other resources.
- Access to production files
  (ISO 17799 – 9.2.4)
  Ensure that employees are granted access to only those computer, network and data services that are required to complete their expected job functions.
- Access to system files
  (ISO 17799 – 9.5.5)
  Ensure that access to system utilities on computer, network or data services is restricted to authorized personnel and authorized utilities only.

2.1.2.7 User Privileges:

Proper security management of the privileges or the permitted actions that are allowed to those users or groups on a specific system

Threats #: 5, 6

- User privileges
  (ISO 17799 – 9.2.2)
  Ensure that only currently authorized personnel have access to the computer, network or data services for which they have a business need.
- User authentication files (UAF) / User identification codes (UIC)
  (ISO 17799 – 9.2.3)
  Ensure that employees manage their passwords that authenticate themselves, to minimize the risk of User IDs being used by unauthorized personnel.
  (ISO 17799 – 9.5.3)
  Ensure that all Company employees are assigned a unique User ID for their personal use to access corporate computer, network or data services.

2.1.2.8 System Access:

Restricting external access and monitoring such access limits the risk to a system or of a network breach from an external source. Monitoring also provides evidence in the case of a security incident.

Threats #: 2, 3, 4, 5, 6

- Monitoring/logging
  (ISO 17799 – 9.7.1)

Ensure that all activities and transactions that occur as part of normal business operating procedures are logged.

- External access – via IP/web, via DECnet
  (ISO 17799 – 9.4.3)
  Ensure that strong authentication processes are employed for remote access to network elements.

2.1.3 Scope

Compliance to the controls listed in 2.1.2 will be tested to determine the extent to which security has been applied to the report server for the company's operational support systems. The scope of this audit is to determine the level of risk of an internal or external security compromise, evaluate controls, and test specific items that would provide an evaluation of the security level of this system.

The scope will not include the related operational support systems, web application security or network architecture security (e.g.: firewall and router interfaces).

2.2 Audit Checklist

2.2.1 Discovery (3)

- Information Gathering from Banners
- Port Scan
- Discovery of User Accounts

Item 1.	**Information Gathering from Banners**
Reference: Galbraith, B., Woodruff, M. *Foundstone Ultimate Hacking Hands On, Course Material M9810C-003, January 2003*. Foundstone Inc., 2003, http://www.foundstone.com, p.62	
Risk: LOW Banners that are displayed at login and by services such as telnet and ftp can reveal information about the system, such as the o/s, and version, type of host, system name, etc. which can be used to compose an attack on the system. There is no significant threat until it is used to form an attack.	
Testing Procedure: • Attempt to set host to INSS1 and view warning banner • Attempt connectivity via telnet, ftp, smtp and review the information provided in the greeting banners, if any. Telnet: telnet 1xx.xxx.208.25 FTP: ftp 1xx.xxx.208.25 SMTP: telnet 1xx.xxx.208.25 25	
Compliance Criteria: The system will comply if there is only a generic warning banner displayed, which does not reveal any system information.	
Test Nature: Objective – results will be observable and repeatable	

Item 2.	**Port Scan**
Reference: Galbraith, B., Woodruff, M. *Foundstone Ultimate Hacking Hands On, Course Material M9810C-003, January 2003*. Foundstone Inc., 2003, http://www.foundstone.com, p.52	

Risk: HIGH If vulnerable or inherently insecure services are running, an exploit on that port could compromise the system.
Testing Procedure: • Run ucx on system to identify open ports and services. • Run SuperScan from remote computer to identify visible open ports that may be accessed externally. • Interview system administrator as to the requirement for the active services identified and controls that are in place.
Compliance Criteria: The system will comply if only those ports and services that are required are active.
Test Nature: Objective – results will be observable and repeatable

Item 3.	**Discovery of User Accounts**
Reference: Internet Security Systems, *X-Force Database*, Internet Security Systems, Inc., 2004, http://xforce.iss.net/xforce/xfdb/130	
Risk: LOW Information about users on the system, such as if they exist and their full names can be useful in further attacks. There is no significant threat until it is used to form an attack.	
Testing Procedure: • Attempt to discover user accounts using the SMTP verify "VRFY" command. The VRFY command allows an attacker to determine if an account exists on a system, providing significant assistance to a brute force attack on user accounts. Telnet to device on SMTP port 25 Command line: telnet 1xx.xxx.208.25 25 Use "vrfy" command to verify if user account exists.	
Compliance Criteria: The system will comply if the VRFY command cannot be used to gather user account information.	
Test Nature: Objective – results will be observable and repeatable	

2.2.2 Policies (1)

- Existence of Security Policy

Item 4.	**Existence of Security Policy**
Reference: Thiagarajan, V., *BS7799 Audit Checklist for SANS Institute*, SANS S.C.O.R.E, 2003, http://www.sans.org/score/checklists/ISO_17799_checklist.pdf p.9	
Risk: LOW Lack of a policy will make it difficult for employees to follow a consistent, appropriate procedure for securing the system. This could allow security vulnerabilities to exist.	
Testing Procedure: • Obtain a copy of any policies and standards related to systems security.	
Compliance Criteria: The system will comply if a documented, published and communicated policy exists.	
Test Nature: Objective – results will be observable and repeatable	

2.2.3 Physical Security (1)

- Physical Location of System

Item 5.	**Physical Location of System**
Reference: Internal practice/policy	
Risk: LOW The appropriate location of the equipment will minimize physical access to the system.	
Testing Procedure: • The physical location and related security controls of the system will be observed.	

Compliance Criteria: The system will comply if it is located in a secured area, not accessible to the general public. Physical controls, such as access control key cards and wearing of identification tags will be in effect.
Test Nature: Subjective – the results will be a judgement call on the part of the auditor based on observation and opinion of compliance

2.2.4 Operations (4)

- Change Management
- Incident Management
- Security Patching
- Segregation of Duties

Item 6.	**Change Management**
Reference: Internal practice/policy	
Risk: MEDIUM The appropriate authorization for any changes made to the system will allow control and monitoring of any such changes.	
Testing Procedure: • Review processes, documentation and controls for the change control process.	
Compliance Criteria: The system will comply if there is a documented change control process with audit logs.	
Test Nature: Subjective – the results will be a judgement call on the part of the auditor based on observation and opinion of compliance	

Item 7.	**Incident Management**
Reference: Internal practice/policy	

Risk: MEDIUM Procedures should be in place to respond to and mitigate security incidents.
Testing Procedure: • Review processes, documentation and controls for the incident management process.
Compliance Criteria: The system will comply if there is a documented incident management process with audit logs.
Test Nature: Subjective – the results will be a judgement call on the part of the auditor based on observation and opinion of compliance

Item 8.	**Security Patching**
Reference: Internal practice/policy	
Risk: HIGH Vulnerabilities to operating systems and applications are identified regularly. Vendors attempt to remedy these vulnerabilities with patches. If patches are not installed as soon as possible after they are released, the system is at risk.	
Testing Procedure: • Review latest security patch release for OpenVMS and compare to the most recent installed on the system. DCL Command: PRODUCT SHOW HISTORY Compare this to the latest patch history on HP's ITRC website: http://www1.itrc.hp.com/service/patch/search.do?pageContextName=openvms::	
Compliance Criteria: The system will comply if the latest patches have been installed, or if the System Administrator has evaluated the patches and has justification for not installing them.	
Test Nature: Objective/Subjective – results will be observable and repeatable, or alternatively may require a value judgement	

Item 9.	Segregation of Duties
Reference: Internal practice/policy	
Risk: LOW Duties and areas of responsibility should be separated to reduce opportunities for unauthorized and unmonitored modification and use of the system.	
Testing Procedure: • Review organization structure within the area to assure that segregation of duties is occurring.	
Compliance Criteria: The system will comply if assurance is obtained that segregation of duties and responsibilities is occurring.	
Test Nature: Subjective – the results will be a judgement call on the part of the auditor based on observation and opinion of compliance	

2.2.5 User Profiles and Accounts (5)

- Default DEC/VMS Accounts
- Password Strength
- Duplicate Accounts
- Orphan Files and Directories
- Seldom Used and Non-active Accounts

Item 10.	Default DEC/VMS Accounts
Reference: Nguyen, M., *OpenVMS Access Controls*. AuditNet, 2004 http://www.auditnet.org/docs/OpenVMS%20Access%20Controls.doc	
Risk: HIGH Default accounts that are well known can be used to compromise a system if the associated password has not been changed. Some of these accounts are necessary, however, the default password must be changed.	

Testing Procedure:

Verify that the passwords for the DEC/VMS supplied user accounts have been changed or that the accounts have been removed:

SYSTEM	– MANAGER – OPERATOR – SYSTEM	DECNET	– DECNET	CLIG	– CLIG
		DEFAULT	– DEFAULT	USERP	– USERP
SYSTEST	– UETP – SYSTEST	USER	– USER	ALLIN1	– ALLIN1
FIELD	– SERVICE – FIELD	NETPRIV	– NETPRIV	GUEST	– no password is required
		NONETPRIV	– NONETPRIV		

- Telnet to device and attempt login with default username and password.
- Identify the default user accounts and review the date of the last password change.

DCL Command: MC AUTHORIZE SHOW [*,*]/BR

Compliance Criteria:

The system will comply if it is not possible to access the system using the default accounts and associated passwords.

Test Nature: Objective – results will be observable and repeatable

Item 11.	**Password Strength**

Reference:

Lazarus, C., *Digital VAX/VMS Audit Program*, AuditNet, 2000, http://www.auditnet.org/docs/vax_vms2.txt

Risk: HIGH

Easily guessed passwords, passwords that are identical to the user ID or that don't expire, weaken the access authentication process. Tools are available to crack passwords, so complex passwords that are changed regularly are required to ensure adequate security.

Testing Procedure:

- Review the PWDMINIMUM values of user accounts.
- Review accounts that have the DIPSWDDIC flag set, which prevents the system from screening repetitive password use.
- Review the PWDLIFETIME field.
- Review accounts that have the DIPSWDHIS flag set, which prevents the system from verifying previous use of a password.
- Obtain the password/shadow files for the user accounts and run a password cracking tool.

DCL Command: MC AUTHORIZE show *

Compliance Criteria:

Minimum password length is 8 characters. Maximum password lifetime is 45 days. The password cracker will not find a password from a typical word list, or brute force a password in less than 2 hours. No UAFs will have the DIPSWDDIC or DIPSWDHIS flags set.

Test Nature: Objective – results will be observable and repeatable

Item 12.	**Duplicate Accounts**

Reference:

National Institute of Standards and Technology, *VMS/OpenVMS checklist*. Defense Information Systems Agency, 2003, http://csrc.nist.gov/pcig/CHECKLISTS/vms-openvs-srrchklst-v2r11.zip

Risk: LOW

Accounts that share a common UIC would allow one user to modify the account of another user.

Testing Procedure:

- Review the system accounts description produced by the Authorize Utility.

DCL Command: MC AUTHORIZE show *

Compliance Criteria:

System will comply if no accounts with multiple users are discovered.

Test Nature: Objective – results will be observable and repeatable

Item 13.	Orphan Files and Directories
Reference: Nguyen, M., *OpenVMS Access Controls*. AuditNet, 2004 http://www.auditnet.org/docs/OpenVMS%20Access%20Controls.doc	
Risk: LOW Files that exist without owners may be inadvertently granted ownership through previously issued UICs. Such files may also indicate a prior breach and compromised system.	
Testing Procedure: • Review the system SYSUAF for all users for files and directories owned by UICs that are no longer on the system. DCL Command: MC AUTHORIZE show *	
Compliance Criteria: The system will comply if there are no orphan files/directories found.	
Test Nature: Objective – results will be observable and repeatable	

Item 14.	Seldom Used and Non-active Accounts
Reference: Pawlikowska, J., *OpenVMS Operating System Security Audit Plan*, AuditNet, 2002, http://www.isaca.org.pl/warsztat/OpenVMS_audyt.doc	
Risk: LOW Stale and unused accounts may be utilized as a means to gain unauthorized access to the system.	
Testing Procedure: • Review accounts that have not registered a login in the last month. DCL Command: MC AUTHORIZE show *	
Compliance Criteria: The system will comply if no accounts are discovered that have not registered a login in the last month.	
Test Nature: Objective – results will be observable and repeatable	

2.2.6 *Access to Files (2)*

- Access to System Files
- Access Control Lists (ACLs)

Item 15.	**Access to System Files**
Reference: Ellsweig, A., *DEC VAX/VMS Operating System/Logical Security Review*, AuditNet, 2000, http://www.auditnet.org/docs/vaxsecur.txt	
Risk: HIGH Access to system files must be restricted to the authorized administrator(s) and system level accounts. Access by unauthorized users may compromise the system, either accidentally or with malicious intent.	
Testing Procedure: • Review the following files to confirm that they have no group or world privileges associated with them. Only system and owner should have all privileges, READ, WRITE, EXECUTE and DELETE (RWED, RWED, ,). Certain executables require users to be able to READ and EXECUTE (e.g. Login) (RWED, RWED, RE, RE). DCL Command: DIRECTORY /SECURITY (SYS$SYSROOT: [*…]) SYS$SYSTEM:AUTHORIZE.EXE SYS$SYSTEM:PROXY.DAT SYS$SYSTEM:DCL.EXE SYS$SYSTEM:SETRIGHTS.EXE SYS$SYSTEM:VMS$OBJECTS.DAT SYS$SYSTEM:MODPARAMS.DAT SYS$SYSTEM:SYSUAF.LIS SYS$SYSROOT:SYSEXE.DIR SYS$ SYSROOT:SYSMGR.DIR SYS$MANAGER:SYLOGIN.COM SYS$MANAGER:LOGIN.COM SYS$MANAGER:LOADNET.COM SYS$MANAGER:VMSIMAGES.DAT SYS$MANAGER:VMS$AUDIT_SERVER.DAT SYS$SYSTEM:SYSUAF.DAT SYS$SYSTEM:LOGINOUT.EXE SYS$SYSTEM:JOB_CONTROL.EXE SYS$SYSTEM:STARTUP.COM SYS$SYSTEM:PARAMS.DAT SYS$SYSTEM:SETPARAMS.DAT SYS$SYSTEM:NETPROXY.DAT SYS$ SYSROOT:SYSLIB.DIR SYS$MANAGER:SYSTARTUP.COM SYS$MANAGER:SYSHUTDWN.COM SYS$MANAGER:STARTNET.COM SYS$MANAGER:RTTLOAD.COM SYS$MANAGER:SYSECURITY.COM	
Compliance Criteria: System will comply if only the system and owner of the system files have any privileges.	
Test Nature: Objective – results will be observable and repeatable	

Item 16.	Access Control Lists (ACLs)
Reference: LeClerc, R., *DEC VAX/VMS Operating System Security Review*. AuditNet, 2002, http://www.auditnet.org/docs/decvaxvm.txt	
Risk: MEDIUM ACLs are associated with and used to control access to objects. Improper management and assignment of ACL identifiers may allow unauthorized access to the system. Users that hold identifiers with privileges beyond their scope for a file with an ACL may have unauthorized access to the file or system. ACL overrides UIC protection.	
Testing Procedure: Verify proper management of ACLs. When a UIC is removed, all associated ACLs must be either reassigned or deleted to prevent unauthorized access to objects. Check for ACLs with: • Invalid General Identifier • Invalid UIC identifier • Wildcard identifier DCL Command: SHOW/SECURITY Run Point Secure Security SnapShot on INSS1	
Compliance Criteria: System will comply if the system administrator is following a procedure to properly use ACLs to protect files and directories. No unassociated ACLs will exist.	
Test Nature: Objective – results will be observable and repeatable	

2.2.7 User Privileges (3)

- User Identification Codes (UICs)
- Rights Identifiers
- Privileges

Item 17.	User Identification Codes (UICs)
Reference: Hewlett-Packard. *OpenVMS Guide to System Security for Version 7.2-1*. Hewlett-Packard Development Company, L.P., 1999, Section 4.1.5 http://h71000.www7.hp.com/doc/72final/6346/6346pro.html	
Risk: MEDIUM The UIC tells what system group a user belongs to and what their unique identification is within that group. Each user should have a unique UIC. Privileges are divided into categories according to the damage that the user possessing them could cause the system: • Within Devour group - Potential to consume non-critical system-wide resources • Within System group - Potential to interfere with normal system operation • Within Object group - Potential to compromise object security • Within All privilege group - Potential to control the system	
Testing Procedure: • Examine UICs within the following Privilege groups: Devour, System, Objects, All • Ensure there are no duplicate UICs DCL (AUTHORIZE) Command: SHOW/IDENTIFIER/FULL * Run Point Secure Security SnapShot on INSS1	
Compliance Criteria: System will comply if no UICs are found in the ALL Privilege Group (with the exception of the system accounts) and if any UICs found in Devour, System, and Object groups are legitimately assigned those privileges.	
Test Nature: Objective – results will be observable and repeatable	

Item 18.	Rights Identifiers
Reference: Hewlett-Packard. *OpenVMS Guide to System Security for Version 7.2-1*. Hewlett-Packard Development Company, L.P., 1999, Section 4.1.6 http://h71000.www7.hp.com/doc/72final/6346/6346pro.html	

Risk: MEDIUM

Rights identifiers define the rights of individual users or groups of users to use a process or access an object. The system administrator assigns identifiers depending on the type of access that should be granted to a user or group of users. A user should not hold an identifier that would provide access for which they are not authorized.

Testing Procedure:

- Review the Rights Identifiers of the system users.

DCL (AUTHORIZE) Command: SHOW/RIGHTS/USER=*

Compliance Criteria:

System will comply if no users hold identifiers for which they are not authorized.

Test Nature: Objective – results will be observable and repeatable

Item 19.	**Privileges**

Reference:

Hewlett-Packard. *OpenVMS Guide to System Security for Version 7.2-1*. Hewlett-Packard Development Company, L.P., 1999, Section 4.6
http://h71000.www7.hp.com/doc/72final/6346/6346pro.html

Risk: HIGH

Special privileges can be assigned to users that can raise a given user's ability to access a particular object. Privileges let a user perform or use system functions that they ordinarily would be denied.

BYPASS	A user with BYPASS privilege receives all types of access to the object, regardless of its protection.
SETPRV	A user with GRPPRV privilege receives the ability to create processes whose privileges are greater than its own.
READALL	A user with READALL privilege receives read access to the object, even if that access is denied by the ACL and the protection code. In addition, the user can receive any other access granted through the protection code.
SYSPRV	A user with SYSPRV privilege receives the access accorded to users in the system category.

Testing Procedure:

- Review users that have special Privileges (READALL, BYPASS, SETPRIV, SYSPRIV) with the system administrator.

DCL (AUTHORIZE) Command: SHOW/RIGHTS/USER=*

Compliance Criteria: System will comply if any users found with special privileges are legitimately assigned those privileges.
Test Nature: Objective – results will be observable and repeatable

---

2.2.8 System Access (4)

- Proxy Logins
- Web Access
- DECnet
- Monitoring and Logging

Item 20.	**Proxy Logins**
Reference: Hewlett-Packard. *OpenVMS Guide to System Security for Version 7.2-1*. Hewlett-Packard Development Company, L.P., 1999, Section 12.2 http://h71000.www7.hp.com/doc/72final/6346/6346pro.html	
Risk: MEDIUM A proxy login enables a user logged in at a remote node to be logged in automatically to a specific account at the local node, without having to supply any access control information. Although proxy access eliminates passwords going over the network, it is possible for a personal computer to bypass the proxy login mechanism by impersonating one of the authorized nodes.	
Testing Procedure: • Check incoming proxy access to sensitive data or applications. • Check for privileged proxy accounts. • Examine any login command procedures for a proxy account. Login command procedures should reside in a well-protected directory owned by a user other than the owner of the proxy account. They should prohibit write access for those who use the account. DCL Command: LIST/PROXY	

Compliance Criteria: System will comply if there is no proxy access to sensitive data or applications, and if no privileged proxy accounts are set up.
Test Nature: Objective – results will be observable and repeatable

Item 21.	**Web Access**
Reference: Center for Internet Security, *Apache Benchmark for UNIX*, CIS, June 4, 2004, http://www.cisecurity.org/bench_apache.html	
Risk: LOW Web services introduce further vulnerabilities on a system. An insecure web server could allow a hacker to utilize a number of attacks against common vulnerabilities such as buffer overflow, denial of service, vulnerable scripts, URL manipulation, etc. Apache is the most popular web server for the internet. This system is not available to the public internet, so the risk is low.	
Testing Procedure: • Run CISScan scoring tool for Apache. Review results against the CIS benchmark.	
Compliance Criteria: System will comply if results do not indicate any major security issues.	
Test Nature: Objective – results will be observable and repeatable	

Item 22.	**DECnet Access**
Reference: Hewlett-Packard. *OpenVMS Guide to System Security for Version 7.2-1*. Hewlett-Packard Development Company, L.P., 1999, Chapter 12 http://h71000.www7.hp.com/doc/72final/6346/6346pro.html	
Risk: LOW To perform any kind of network activity, all network users must have TMPMBX and NETMBX privileges. To connect to a DECnet node, a user needs explicit access information, a proxy account, an application account, or a default DECnet account. NCP (Network Control Program) are commands used to modify the network configuration database.	

Testing Procedure:

- Check for removal of the default DECnet user account
- Check for user privileges beyond TMPMBX (temporary mailbox) and NETMBX (general DECnet functions). Discuss unexpected findings and justify.

Have system administrator examine the UAF user records

- Check for proxy accounts (see Item 20)

DCL Command: LIST/PROXY

- Check for logging of NCP events

NCP Command: SHOW ACTIVE LOGGING

Compliance Criteria:

The system will comply if the system administrator provides assurance that the DECnet default account has been removed, that general users are limited to the TMPMBX and NETMBX privileges, that NCP event logging is occurring, and that proxy accounts are managed (per item 20).

Test Nature: Objective – results will be observable and repeatable

Item 23.	**Monitoring and Logging**

Reference:

Hewlett-Packard. *OpenVMS Guide to System Security for Version 7.2-1*. Hewlett-Packard Development Company, L.P., 1999, Chapter 9
http://h71000.www7.hp.com/doc/72final/6346/6346pro.html

Risk: MEDIUM

Monitoring and logging system events do not necessarily protect the system, but make it possible to analyze and monitor activities. The record of events may provide a means to reconstruct the events leading up to a system breach or security incident. The log itself should be protected against unauthorized access and tampering, so that malicious activities cannot be concealed.

Testing Procedure:

- Review the audit configuration with the system administrator to ensure appropriate events are being captured

DCL Command: SHOW AUDIT

- Review those events that are alarmed and those that are only being audited
- Review destination of event messages and storage of log files
- Review procedures used for log analysis and actions resulting from alarms

Compliance Criteria: System will comply if alarming is occurring on significant security events, logging of events for further analysis is taking place, and procedures are in place for response to alarms and analysis of the logs.
Test Nature: Objective/Subjective – some of the results will be observable and repeatable, others will be based upon a value judgement by the auditor

Part #3 – Conduct the Audit Testing, Evidence and Findings

Part #3 of the assignment calls for the selection of ten (10) items to demonstrate the performance of a technical audit. Not all of the 23 items in the checklist are technical in nature. Policy and physical security are not necessarily technical and are not specific to the system being audited. Therefore I have selected ten items that demonstrate a technical test, as well as included several that are not technical in nature. The technical items selected are indicated with (**).

3.1 Discovery

- Information Gathering from Banners
- Port Scan
- Discovery of User Accounts

*3.1.1 - Item 1 - Information Gathering from Banners **

Testing Procedure:

- Attempt to set host to INSS1 and view warning banner
- Attempt connectivity via telnet, ftp, smtp and review the information provided in the greeting banners, if any.

Telnet: telnet 1xx.xxx.208.25
FTP: ftp 1xx.xxx.208.25
SMTP: telnet 1xx.xxx.208.25 25

The warning banner that is displayed when attempting to "set host" from another VMS system is generic:

```
                    WARNING

"ACCESS TO, OR UNAUTHORIZED USE OF PROGRAMS AND
DATA ON THIS COMPUTER BY ANY PERSON, OTHER THAN
AUTHORIZED EMPLOYEE(S) OR OWNER(S) OF AN ACCOUNT IS
STRICTLY PROHIBITED AND MAY RESULT IN LEGAL ACTION
AGAINST SUCH PERSON.  THIS SYSTEM MAY BE MONITORED
AT ANY TIME FOR OPERATIONAL OR SECURITY REASONS."
```

Figure 2 – Set host banner

The telnet banner provides the same generic security warning:

```
                    WARNING

"ACCESS TO, OR UNAUTHORIZED USE OF PROGRAMS AND
DATA ON THIS COMPUTER BY ANY PERSON, OTHER THAN
AUTHORIZED EMPLOYEE(S) OR OWNERS(S) OF AN ACCOUNT IS
STRICTLY PROHIBITED AND MAY RESULT IN LEGAL ACTION
AGAINST SUCH PERSON. THIS SYSTEM MAY BE MONITORED
AT ANY TIME FOR OPERATIONAL OR SECURITY REASONS."
```

Figure 3 – Telnet banner screen shot

The SMTP banner, however, shows the system name, URL, o/s and version, and company name. This should be changed:

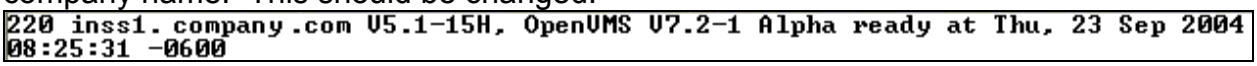

Figure 4 – SMTP banner screen shot

The FTP banner also provides more information than is necessary:

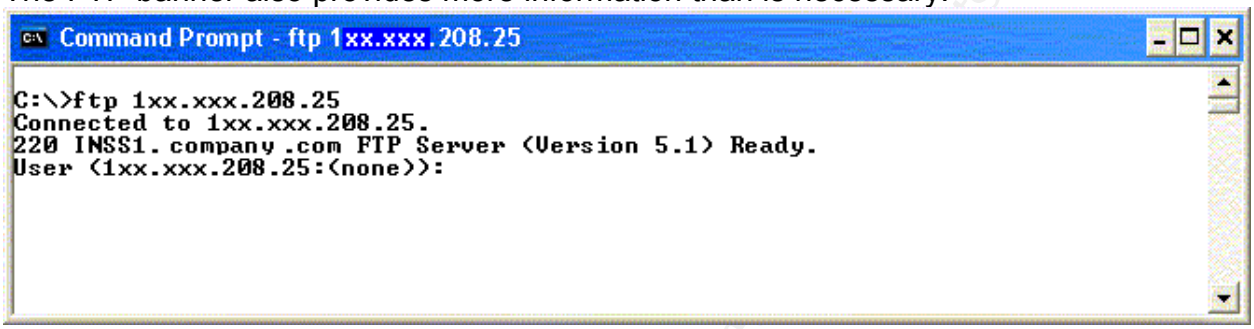

Figure 5 – FTP banner screen shot

Results: Does not fully comply: Not all logon banners are generic. Some banners provide information that could be used in an attack.

3.1.2 - Item 2 - Port Scan **

Testing Procedure:

- Run UCX on system to identify open ports and services.

DEC Command: ucx
TCPIP> sho dev

- Run SuperScan from remote computer to identify visible open ports that may be accessed externally.
- Interview system administrator as to the requirement for the active services identified and controls that are in place.

Using UCX (TCPIP sho dev) command, the system revealed that the following ports are in use:

21 – ftp (TCP)
23 – telnet (TCP)
25 – smtp (TCP)

80 – http (TCP)
512 – rexec (TCP) – remote execute
514 – rsh (TCP) – remote shell
123 – ntp (UDP)

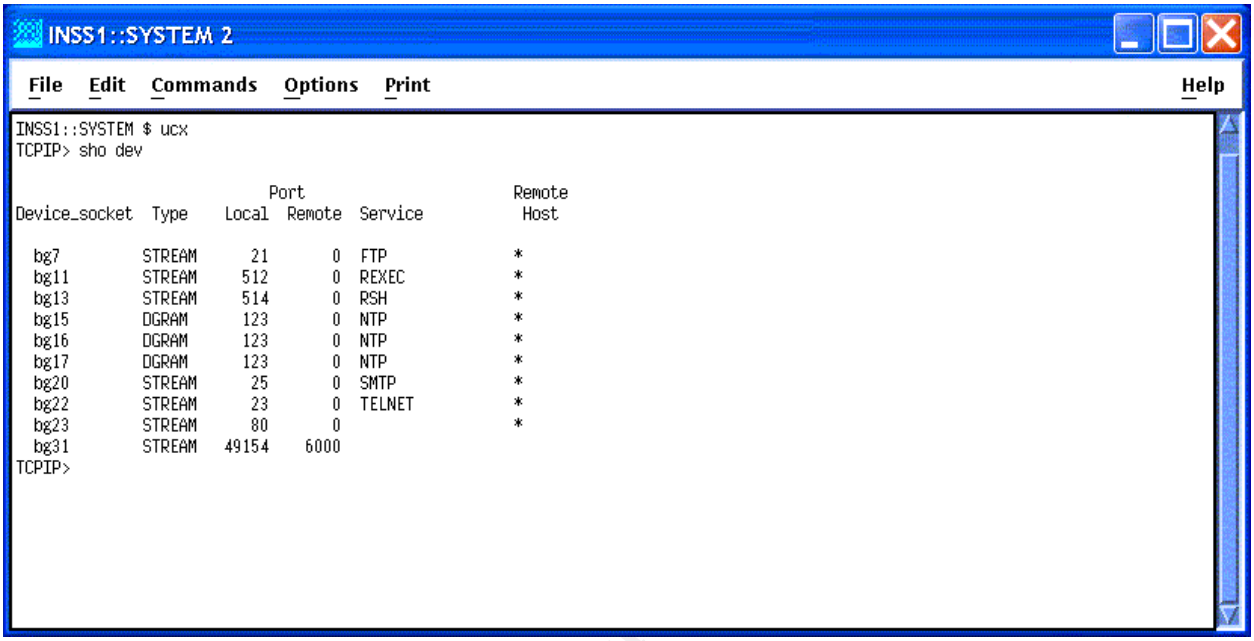

Figure 6 – UCX screen shot

The last port in the list (49154) relates to the connection from the remote computer.

SuperScan is a connect-based TCP port scanner, pinger and hostname resolver available from Foundstone[9].

SuperScan also reveals that the following ports are open:
23 – telnet
25 – smtp
80 – http (web)
512 – remote process execution; authentication performed using passwords and UNIX login names
514 – cmd; like exec, but automatic authentication is performed as for login server

[9] http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/freetools.htm

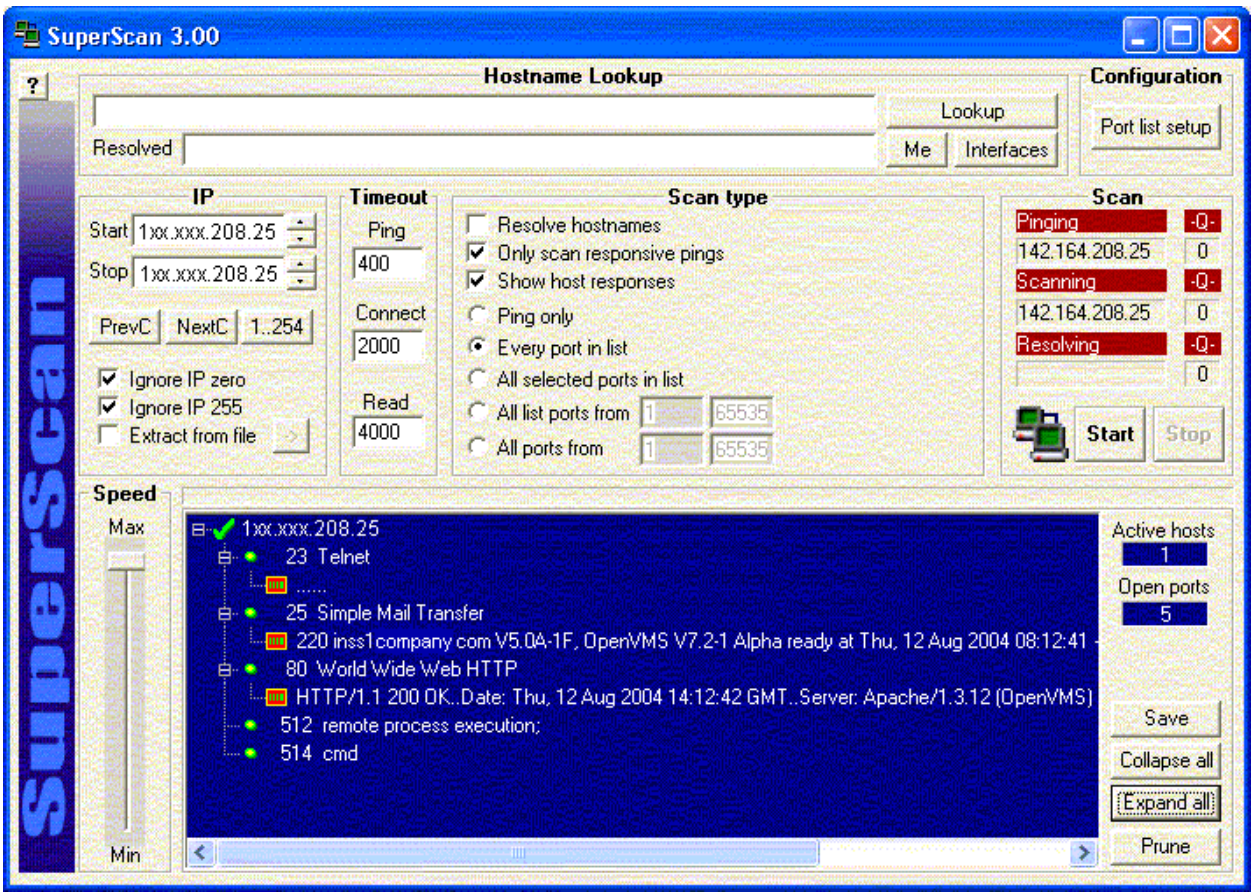

Figure 7 – SuperScan screen shot

Telnet and rsh are vulnerable services. Any connections that are made through these services are in clear text. This should be replaced with an SSH capable service.

Results: Does not fully comply: Open services with clear text capability exist.

3.1.3 - Item 3 - Discovery of User Accounts **

Testing Procedure:

Telnet to device on SMTP port 25
Command line: telnet 1xx.xxx.208.25 25
Use “vrfy” command to verify if user account exists.

The SMTP VRFY command is used to verify a user ID on a host and as such can be used to test for valid user IDs. Disabling the command helps prevent "spoofing" by not allowing someone outside the network to check if a user ID is valid.

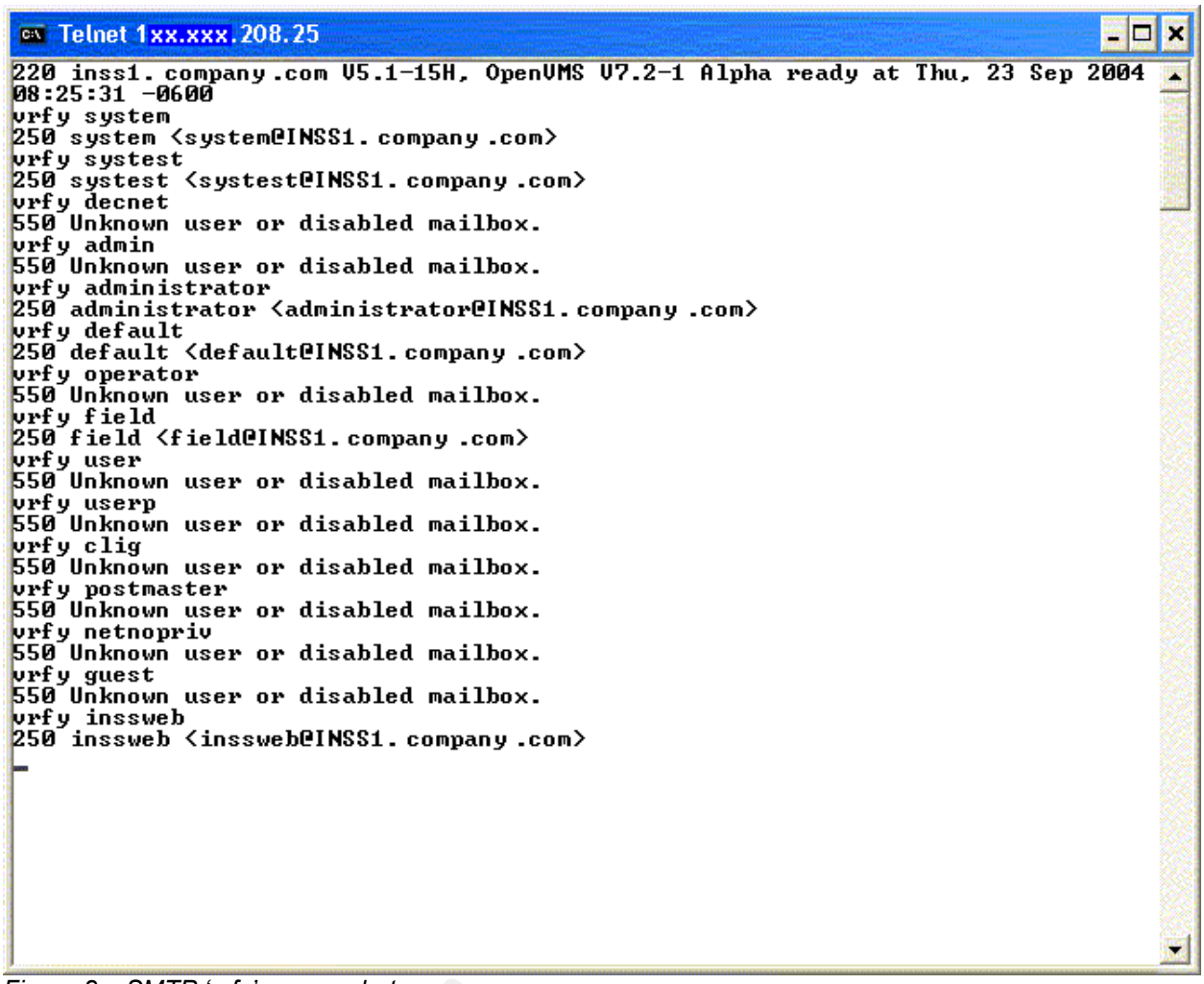

Figure 8 – SMTP 'vrfy' screen shot

Found six user accounts (other user accounts may exist). The last one was a guess based on my knowledge of the system.

Results: Does not comply: The SMTP "VRFY" command is not disabled. User IDs can be tested and their existence on the system verified.

3.2 - Policies

- Existence of Security Policy

3.2.1 - Item 4 - *Existence of Security Policy*

Testing Procedure:
• Obtain a copy of any policies and standards related to systems security.

The company's Corporate Security department has issued a comprehensive security policy based on ISO 17799. This policy has been rolled out corporately, and a corporate security awareness program is in place. There is a process to provide updates to the policy and related standards.

Results: Complies: Policies are in place.

3.3 - Physical Security

- Physical Location of System

3.3.1 - *Item 5 - Physical Location of System*

Testing Procedure:
• The physical location and related security controls of the system will be observed.

The system is located in a support area that is manned 8x5 (8 hours per day, 5 days per week) on the 2nd floor of an office tower. The only occupant of the office building is the same company. During the day, access is restricted to those that have valid identification tags. Visitors must sign in at the security kiosk on the main floor. Unknown visitors to the building or floor are challenged.

After hours, the area is secured by locking doors with combination locks. The area itself is in a building with restricted access and an entrance that has security guards.

Results: Complies: Physical location is secure.

3.4 - Operations

- Change Management
- Incident Management
- Security Patching
- Segregation of Duties

3.4.1 - Item 6 - Change Management

Testing Procedure:

- Review processes, documentation and controls for the change control process.

A documented change control process is in place for all changes, which is part of an overall configuration management process. A configuration management database (CMDB) contains the information for objects (servers, network elements, applications) in the inventory. This database is available on the company intranet. A change request is initiated from the inventory record, which notifies anyone who may be impacted by the change. A Change Manager reviews the request and any concerns via feedback from persons impacted by it, and then approves (or denies) the request. Maintenance windows for systems are adhered to as detailed in the CMDB. Impact severity and back-out plans are also required to be entered into the request.

Results: Complies: A detailed configuration and change management process is in place.

3.4.2 - Item 7 - Incident Management

Testing Procedure:

- Review processes, documentation and controls for the incident management process.

A documented Security Computer Incident Response process (CIR) is in place. The prime accountability falls to the company's Corporate Security Directors who "own" any incident that occurs. A policy exists detailing the responsibilities of everyone who may be involved in mitigation. The company has also organized Computer Incident Response Teams (CIRTs) as needed to handle computer incidents. If the incident becomes a major risk to the business, the CIRT will escalate the control of the incident to the Corporate Emergency Operations Committee (EOC).

Results: Complies: A detailed computer incident management process is in place.

3.4.3 - *Item 8 - Security Patching*

Not assessed at this time.

3.4.4 - *Item 9 - Segregation of Duties*

Not assessed at this time.

3.5 - User Profiles and Accounts

- Default DEC/VMS Accounts
- Password Strength
- Duplicate Accounts
- Orphan Files and Directories
- Seldom Used and Non-active Accounts

Using the DCL Command: MC AUTHORIZE SHOW [*,*]/BR, user accounts on the system are as follows:

Owner	Username	UIC	Account	Privs	Pri	Directory
SYSTEM MANAGER	SYSTEM	[1,4]	SYSTEM	All	4	SYS$SYSROOT:[SYSMGR]
SYSTEST-UETP	SYSTEST	[1,7]	SYSTEST	All	4	Disuser
FIELD_SERVICE	FIELD	[1,10]	FIELD	All	4	Disuser
	INSSWEB	[100,1]		All	4	DISK$USER:[INSSWEB]
INSSREPORT	INSSREPORT	[100,2]		All	4	APACHE$SPECIFIC:[INSSHELP.INSS_REPORT.INSSREPORT]
	DEFAULT	[200,200]		Normal	4	Disuser
	MEGAPOVRAY07	[200,201]		Normal	4	DISK$USER:[MEGAPOVRAY07]
	PSC	[210,1]		Devour	4	DISK$USER:[PSC]
Al Robinson	AROBI	[210,2]		Devour	4	DISK$USER:[AROBI]
	DHCP_USER	[211,1]		Normal	4	Disuser
	FTPGUEST1	[212,1]		Normal	4	DISK$USER:[FTPGUEST1]
Compaq Secure Web Server	APACHE$WWW	[300,1]		Devour	4	DISK$USER:[000000.APACHE$WWW]
DECEVENT	DIA$MANAGER	[375,300]		All	4	DIA$:[MANAGER]
MIRRO$SERVER DEFAULT	MIRRO$SERVER	[376,367]	DECNET	Normal	4	SYS$SPECIFIC:[MIRRO$SERVER]
VPM$SERVER DEFAULT	VPM$SERVER	[376,370]	DECNET	Normal	4	SYS$SPECIFIC:[VPM$SERVER]
NML$SERVER DEFAULT	NML$SERVER	[376,371]	DECNET	Normal	4	SYS$SPECIFIC:[NML$SERVER]
MAIL$SERVER DEFAULT	MAIL$SERVER	[376,374]	DECNET	Normal	4	SYS$SPECIFIC:[MAIL$SERVER]
ANONYMOUS	ANONYMOUS	[3375,1]	ANONY	Normal	8	APACHE$SPECIFIC:[DHCP]
TCPIP$RSH	TCPIP$RSH	[3655,1]	TCPIP	Normal	8	SYS$SYSDEVICE:[TCPIP$RSH]
TCPIP$REXEC	TCPIP$REXEC	[3655,2]	TCPIP	Normal	8	SYS$SYSDEVICE:[TCPIP$REXEC]
TCPIP$LPD	TCPIP$LPD	[3655,3]	TCPIP	Normal	8	SYS$SPECIFIC:[TCPIP$LPD]
TCPIP$FTP	TCPIP$FTP	[3655,4]	TCPIP	Normal	8	SYS$SYSDEVICE:[TCPIP$FTP]
TCPIP$SMTP	TCPIP$SMTP	[3655,5]	TCPIP	Normal	8	SYS$SPECIFIC:[TCPIP$SMTP]
TCPIP$NTP	TCPIP$NTP	[3655,6]	TCPIP	Normal	8	SYS$SPECIFIC:[TCPIP$NTP]

Table 2 – User accounts

This table will be used as a reference for the test of user profiles and accounts.

3.5.1 - Item 10 - Default DEC/VMS Accounts **

Testing Procedure:

Verify that the passwords for the DEC/VMS supplied user accounts have been changed or that the accounts have been removed:

SYSTEM	– MANAGER – OPERATOR – SYSTEM	DECNET	– DECNET	CLIG	– CLIG
		DEFAULT	– DEFAULT	USERP	– USERP
SYSTEST	– UETP – SYSTEST	USER	– USER	ALLIN1	– ALLIN1
FIELD	– SERVICE – FIELD	NETPRIV	– NETPRIV	GUEST	– no password is required
		NONETPRIV	– NONETPRIV		

- Telnet to device and attempt login with default username and password.
- Identify the default user accounts and review the date of the last password change.

DCL Command: MC AUTHORIZE SHOW [*,*]/BR (see Table 2)

Results of the telnet attempts are shown in Figures 8 and 9.

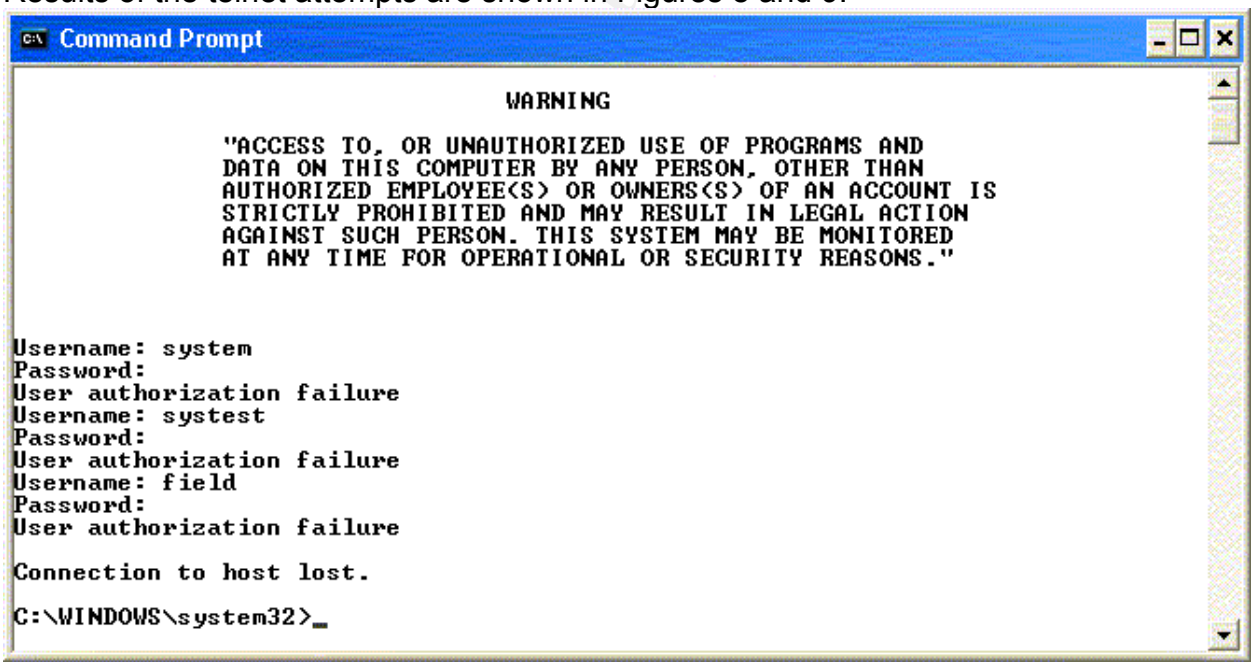

Figure 9 – Telnet screen shot 1

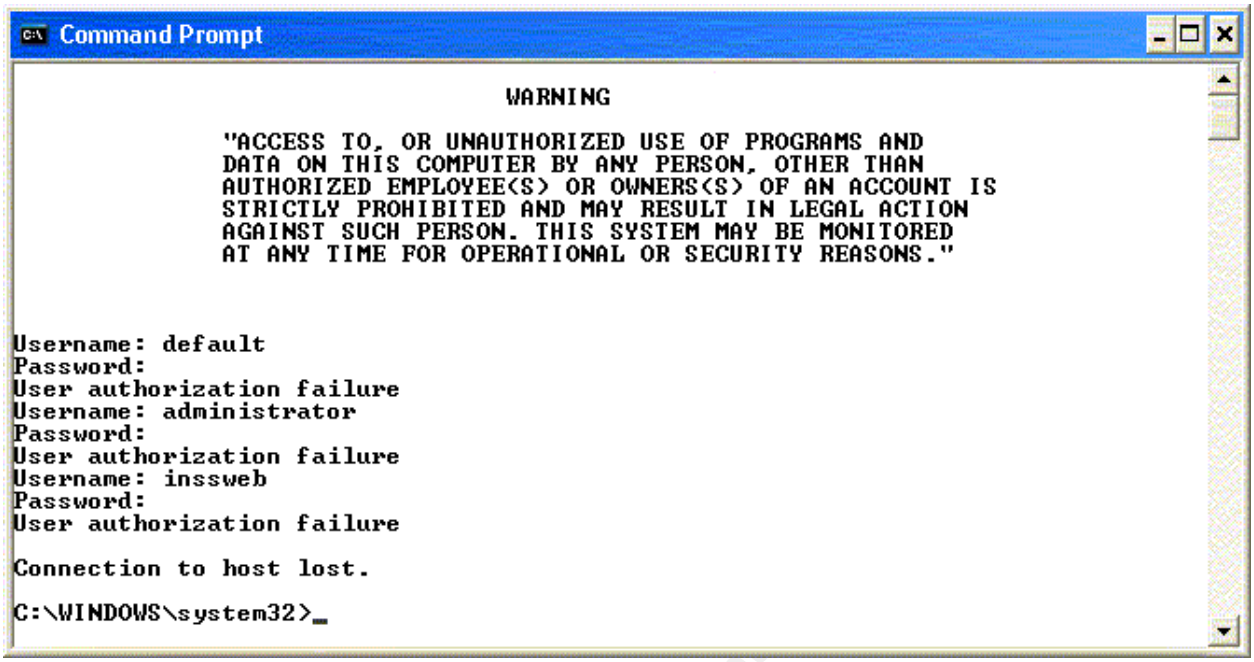

Figure 10 – Telnet screen shot 2

The system administrator was also requested to attempt logins to those accounts with the default passwords supplied. Default passwords have been changed. The system disconnects after three failed attempts.

The only default account that is in use is SYSTEM. The default password has been changed. However, the last password change for this account was July 5, 2004, which does not meet the password policy requirements.

Results: Complies: Unnecessary accounts have been removed or disabled (Disuser). Default passwords have been changed.

3.5.2 - *Item 11 - Password Strength* **

Testing Procedure:

- Review the PWDMINIMUM values of user accounts.
- Review accounts that have the DIPSWDDIC flag set, which prevents the system from screening repetitive password use.
- Review the PWDLIFETIME field.
- Review accounts that have the DIPSWDHIS flag set, which prevents the system from verifying previous use of a password.

- Obtain the password/shadow files for the user accounts and run a password cracking tool.

DCL Command: MC AUTHORIZE show * (see Table 2)

The account profiles (with the exception of "SYSTEM") are typical of the following example:

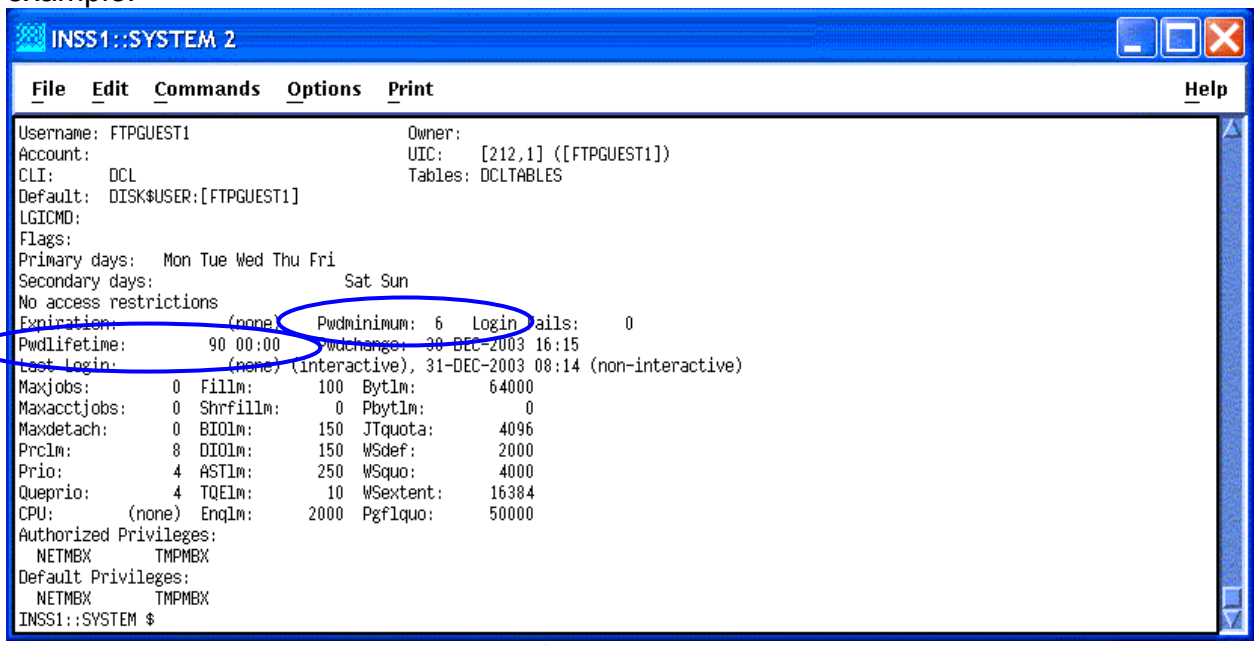

Figure 11 – User account profile screen shot

This indicates that the minimum password length is 6 characters (PWDMINIMUM) and that the time between password changes is set to 90 days (PWDLIFETIME). None of the accounts had the password history or dictionary disabled.

The SYSUAF.DAT file is a binary file that contains the passwords. There is no shadow file that is accessible that can be obtained and cracked to test password vulnerability. However, a VMS patch[10] for John the Ripper is available that will run on Alpha and VAX. This tool is designed for system administrators to detect users who too often select passwords that are simple and easily guessed.

After the John executables are extracted on the VMS system, the SYSUAF.DAT file must be converted to a format useable by John using UNUAF (a utility included in John).

```
unuaf -a sysuaf.dat > sysuaf.john
```

Then John is run against this file.

```
john -i:vms sysuaf.john
```

[10] Gailly, J., *Cracking OpenVMS passwords with John the Ripper*. Gailly.net, 2002. http://gailly.net/security/john-VMS-readme.html

This generates an output file called JOHN.POT which will contain the usernames and associated passwords that John was able to crack. Running John on INSS1 with default settings and a password list resulted in finding only a single password that was fairly simple and should be strengthened. However, this account had system privileges.

Results: Does not comply: The policy states that passwords must be at least 8 characters and expire in 45 days. Also, password strength should be improved on at least one user account.

3.*5.3 - Item 12 - Duplicate Accounts*

Testing Procedure:

- Review the system accounts description produced by the Authorize Utility.

DCL Command: MC AUTHORIZE show * (see Table 2)

As per Table 2, all user accounts and UICs are unique. No duplicate accounts exist.

Results: Complies: No accounts with multiple users were discovered.

3.*5.4 - Item 13 - Orphan Files and Directories*

Testing Procedure:

- Review the system SYSUAF for all users for files and directories owned by UICs that are no longer on the system.

DCL Command: MC AUTHORIZE show * (see Table 2)

As per Table 2 and interviews with the System Administrator, UICs have not been reassigned. Unused accounts are DISUSERed. No orphan files/directories were discovered.

Results: Complies: No orphan files/directories were discovered.

3.5.5 - *Item 14 - Seldom Used and Non-active Accounts*

Testing Procedure:

- Review accounts that have not registered a login in the last month.

DCL Command: MC AUTHORIZE show * (see Table 2)

As per Table 2 and interviews with the System Administrator, accounts that are no longer used or accessed are DISUSERed or removed. Several accounts had not been accessed in the previous month, but upon review, the users are still active. Vacation and training are cited as the reasons for the inactivity on those accounts.

Results: Complies: No accounts were discovered that have not registered a login in the last month without a reasonable explanation.

3.6 - Access to Files

- Access to System Files
- Access Control Lists (ACLs)

3.6.1 - *Item 15 - Access to System Files* **

Testing Procedure:

- Review the following files to confirm that they have no group or world privileges associated with them. Only system and owner should have all privileges, READ, WRITE, EXECUTE and DELETE (RWED, RWED, ,). Certain executables require users to be able to READ and EXECUTE (e.g. Login) (RWED, RWED, RE, RE).

DCL Command: DIRECTORY /SECURITY (SYS$SYSROOT: [*…])

The following Table 3 illustrates the findings for the SYSEXE directories:

```
Directory SYS$SYSROOT:[000000.SYSEXE]

MODPARAMS.DAT;4                [SYSTEM]              (RWED,RWED,RE,)
PARAMS.DAT;7                   [1,1]                 (RWED,RWED,RE,)
SETPARAMS.DAT;7                [1,1]                 (RWED,RWED,RE,)
SYSUAF.LIS;1                   [1,1]                 (RWD,RWD,R,)
SYSEXE.DIR                     [1,1]                 (RWE,RWE,RE,RE)
SYSMGR.DIR                     [SYSTEM]              (RWE,RWE,RE,RE)
SYSLIB.DIR                     [SYSTEM]              (RWE,RWE,RE,RE)


Directory SYS$COMMON:[000000.SYSEXE]

AUTHORIZE.EXE;1                [SYSTEM]              (RWED,RWED,RE,RE)
DCL.EXE;1                      [SYSTEM]              (RWED,RWED,RE,RE)
JBC$JOB_CONTROL.EXE;1          [SYSTEM]              (RWED,RWED,RE,RE)
LOGINOUT.EXE;1                 [SYSTEM]              (RWED,RWED,RE,RE)
NETPROXY.DAT                   Does not exist on
                               system
RIGHTSLIST.DAT                 [SYSTEM]              (RWED,RWED,,)
SETRIGHTS.EXE;1                [SYSTEM]              (RWED,RWED,RE,RE)
STARTUP.COM;1                  [SYSTEM]              (RWED,RWED,RE,RE)
SYSUAF.DAT;1                   [1,1]                 (RWE,RWE,RWE,)
TCPIP$PROXY.DAT;1              [1,1]                 (RWED,RWED,RE,)
VMS$OBJECTS.DAT;1              [SYSTEM]              (RWE,RWE,RE,)
VMS$PASSWORD_HISTORY.DATA;1    [1,1]                 (RWE,RWE,,)
VMSMAIL_PROFILE.DATA;1         [SYSTEM]              (RWE,RWE,,)
```

Table 3 – SYSEXE directory

Although most of these files do not have any "world" privileges, there are several other files that should be reviewed. Specifically JOB_CONTROL.EXE, SETRIGHTS.EXE and STARTUP.COM should be considered for removal of the EXECUTE privilege for "world" users.

The following Table 4 illustrates the findings for the SYSMGR directory:

```
Directory SYS$COMMON:[000000.SYSMGR]

LOADNET.COM;1                    [SYSTEM]          (RWED,RWED,RE,RE)
LOGIN.COM;3                      [SYSTEM]          (RWED,RWED,RE,RE)
RTTLOAD.COM;1                    [SYSTEM]          (RWED,RWED,RE,RE)
STARTNET.COM;1                   [SYSTEM]          (RWED,RWED,RE,RE)
SYLOGIN.COM;1                    [SYSTEM]          (RWED,RWED,RE,RE)
SYSECURITY.COM;1                 [SYSTEM]          (RWED,RWED,RE,RE)
SYSHUTDWN.COM;1                  [SYSTEM]          (RWED,RWED,RE,RE)
SYSTARTUP_VMS.COM;31             [SYSTEM]          (RWED,RWED,RE,RE)
VMS$AUDIT_SERVER.DAT;1           [SYSTEM]          (RWE,RWE,RE,)
VMSIMAGES.DAT;1                  [SYSTEM]          (RWED,RWED,RE,RE)
```

Table 4 – SYSMGR directory

None of these files have "group" or "world" WRITE or DELETE privileges. However, the EXECUTE privilege for "world" should be reviewed for all of these files.

Results: Does not fully comply: Several files should be reviewed to determine if "group" and "world" privileges should be removed.

3.6.2 - *Item 16 - Access Control Lists (ACLs)* **

Testing Procedure:

Verify proper management of ACLs. When a UIC is removed, all associated ACLs must be either reassigned or deleted to prevent unauthorized access to objects. Check for ACLs with:

- Invalid General Identifier
- Invalid UIC identifier
- Wildcard identifier

Run Point Secure Security SnapShot on INSS1

Interviews with the System Administrator reveal that this system uses ACLs sparingly. Although ACLs provide another level of security, they are difficult to manage and administer. The System Administrator does not allow others to create ACLs.

No ACLs were identified that had invalid or wildcard identifiers (see Figure 12).

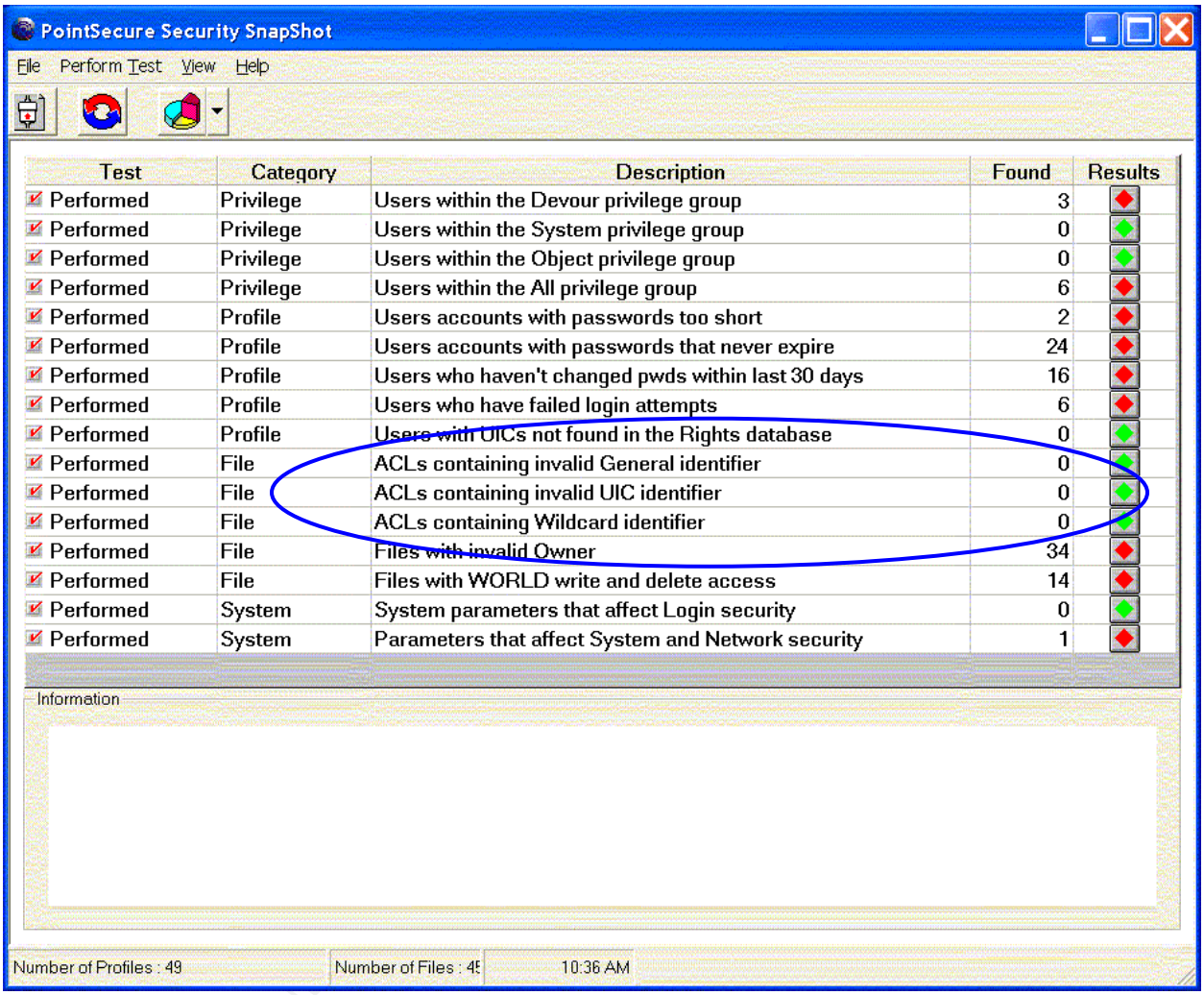

Figure 12 – PointSecure Security SnapShot screen report - ACLs

Results: Complies: ACLs are managed appropriately.

3.7 - User Privileges

- User Identification Codes (UICs)
- Rights Identifiers
- Privileges

3.7.1 - Item 17 - User Identification Codes (UICs) **

Testing Procedure:

- Examine UICs within the following Privilege groups: Devour, System, Objects, All
- Ensure there are no duplicate UICs

DCL (AUTHORIZE) Command: SHOW/IDENTIFIER/FULL *

Run Point Secure Security SnapShot on INSS1

Table 5 shows the users that are in the All privilege group.

Owner	Username	UIC	Account	Privs	Directory
SYSTEM MANAGER	SYSTEM	[1,4]	SYSTEM	All	SYS$SYSROOT:[SYSMGR]
SYSTEST-UETP	SYSTEST	[1,7]	SYSTEST	All	Disuser
FIELD_SERVICE	FIELD	[1,10]	FIELD	All	Disuser
	INSSWEB	[100,1]		All	DISK$USER:[INSSWEB]
INSSREPORT	INSSREPORT	[100,2]		All	APACHE$SPECIFIC:[INSSHELP.INSS_REPORT.INSSREPORT]
DECEVENT	DIA$MANAGER	[375,300]		All	DIA$:[MANAGER]

Table 5 – ALL Privilege Group

Table 6 shows the users that are in the Devour privilege group.

Owner	Username	UIC	Account	Privs	Directory
	PSC	[210,1]		Devour	DISK$USER:[PSC]
Al Robinson	AROBI	[210,2]		Devour	DISK$USER:[AROBI]
Compaq Secure Web Server	APACHE$WWW	[300,1]		Devour	DISK$USER:[000000.APACHE$WWW]

Table 6 – DEVOUR Privilege Group

No users were discovered in the System and Objects privilege groups.

Upon examining those UICs in the ALL Privilege Group, it was determined that two UICs have elevated privileges. The users INSSWEB and INSSREPORT should not be within the ALL Privilege Group.

A review of the UICs in the Devour Privilege Group verified those users.

The results from the Security SnapShot confirm that users are found only in the Devour and All privilege groups:

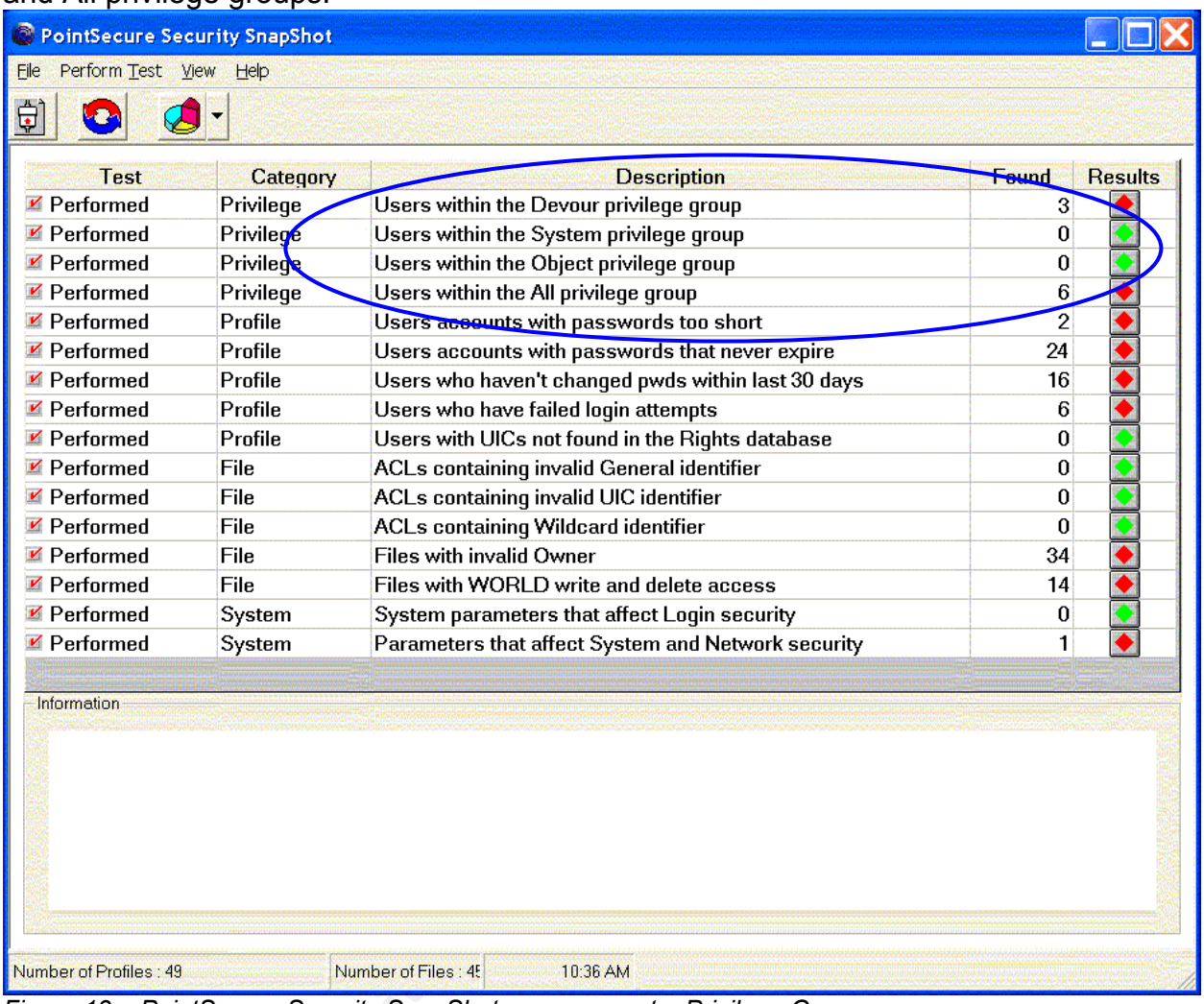

Figure 13 – PointSecure Security SnapShot screen report – Privilege Groups

As per Table 2 and Item 12, no duplicate UICs exist.

Results: Does not fully comply: Two users were identified that should not be within the ALL Privilege Group.

3.7.2 - *Item 18 - Rights Identifiers*

Testing Procedure:

- Review the Rights Identifiers of the system users.

DCL (AUTHORIZE) Command: SHOW/RIGHTS/USER=*

Only SYSTEM was discovered to have an Identifier assigned:

Owner	Username	UIC	Account	Ident
SYSTEM MANAGER	SYSTEM	[1,4]	SYSTEM	NET$MANAGE

Table 7 – Identifiers

Results: Complies: Rights Identifiers are being managed and assigned appropriately.

3.7.3 - *Item 19 - Privileges*

Testing Procedure:

- Review users that have special Privileges (READALL, BYPASS, SETPRIV, SYSPRIV) with the system administrator.

DCL (AUTHORIZE) Command: SHOW/RIGHTS/USER=* (use a search string e.g.: search sys$input username, [priv])

Table 8 summarizes the findings for users with special privileges:

Owner	Username	UIC	Account	Priv
SYSTEM MANAGER	SYSTEM	[1,4]	SYSTEM	BYPASS SYSPRV SETPRV READALL
SYSTEST-UETP	SYSTEST	[1,7]	SYSTEST	SYSPRV SETPRV
FIELD_SERVICE	FIELD	[1,10]	FIELD	SETPRV
	INSSWEB	[100,1]		BYPASS SYSPRV SETPRV READALL
INSSREPORT	INSSREPORT	[100,2]		BYPASS SYSPRV SETPRV READALL

Table 8 – Special Privileges

Upon examining those users that have Special Privileges assigned, it was determined that two UICs have elevated privileges. The users INSSWEB and INSSREPORT should not have system level privileges that would be attained from BYPASS, SETPRIV, or SYSPRIV. The READALL privilege should be reviewed and another method of access to the necessary files assigned.

Results: Does not comply: Two users were discovered that have escalated privileges due to the assignment of Special Privileges.

3.8 - System Access

- Proxy Logins
- Web Access
- DECnet
- Monitoring and Logging

3.*8.1 - Item 20 - Proxy Logins*

Testing Procedure:

- Check incoming proxy access to sensitive data or applications.
- Check for privileged proxy accounts.
- Examine any login command procedures for a proxy account. Login command procedures should reside in a well-protected directory owned by a user other than the owner of the proxy account. They should prohibit write access for those who use the account.

DCL Command: LIST/PROXY

The NETPROXY.DAT file does not exist on the system (see Table 3, page 45).

No DECnet proxy accounts were discovered. The TCP proxy file has no entries, which would allow access from anywhere. However, as long as the TCP ports for rsh (port 514) and rexec (port 512) are open, connectivity could be established once a user ID and password are known. See Item 2, page 30.

Results: Complies: There is no proxy access to sensitive data or applications. No privileged proxy accounts are set up.

3.*8.2 - Item 21 - Web Access*

Not assessed at this time.

3.8.3 - *Item 22 - DECnet* **

Testing Procedure:

- Check for removal of the default DECnet user account
- Check for user privileges beyond TMPMBX (temporary mailbox) and NETMBX (general DECnet functions). Discuss unexpected findings and justify.

Have system administrator examine the UAF user records

- Check for proxy accounts (see Item 20)

DCL Command: LIST/PROXY

- Check for logging of NCP events

NCP Command: SHOW ACTIVE LOGGING

The UAF does not contain an entry for username DECNET, revealing that the default has been removed. Attempts to login as user DECNET were unsuccessful.

General user privileges are reflected in this example:

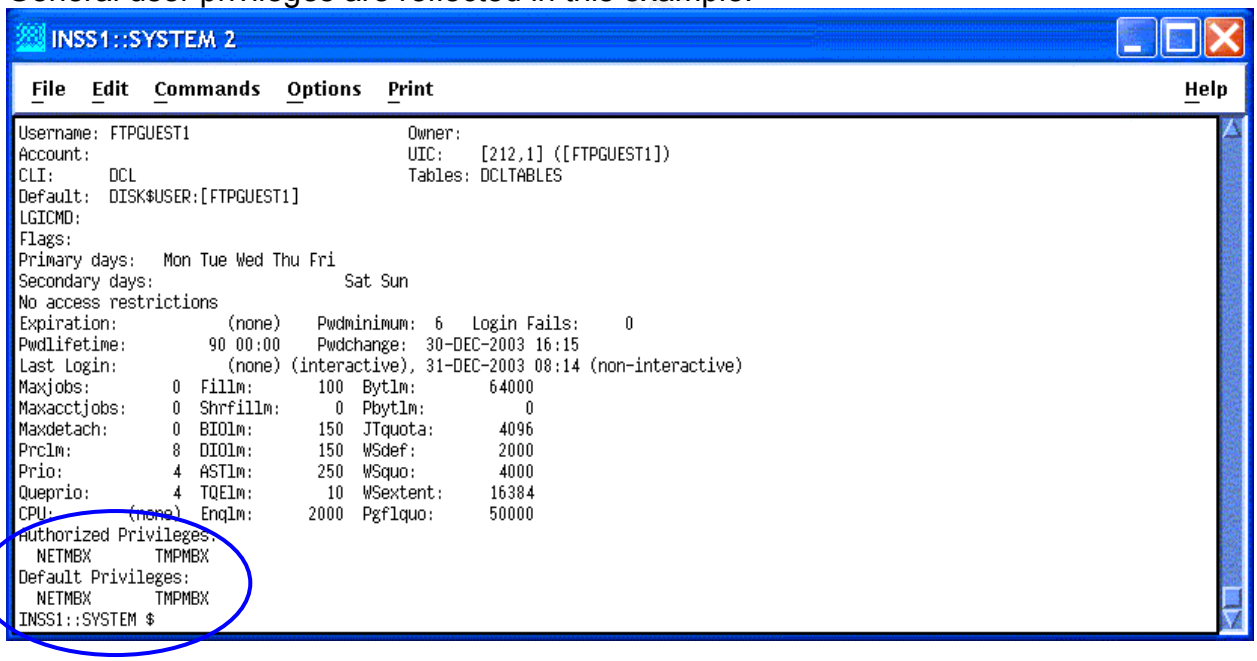

Figure 14 – Network Privileges

Proxy accounts were tested in Item 20. No proxy accounts were found.

NCP events are being logged as follows:

```
NCP>show active logging
Active Logging Volatile Summary as of 5-OCT-2004 09:19:54
 Logging sink type = monitor

    Sink Node       Source              Events                    State Name
   10.xxx (INSS1)   (All sources)       0.0-9                      on
                    (All sources)       2.0-1
                    (All sources)       4.2-13 15-16
                                        18-19
                    (All sources)       5.0-18
                    (All sources)       128.0-4
```

Figure 15 – NCP auditing

Refer to Appendix B for DECnet events that can be logged and the associated event numbering.

Results: Complies: The DECNET user account has been removed. Logging of NCP events is occurring. General network privileges are limited to NETMBX and TMPMBX. There is no proxy access to sensitive data or applications. No privileged proxy accounts are set up.

3.8.4 - *Item 23 - Monitoring and Logging* **

Testing Procedure:

- Review the audit configuration with the system administrator to ensure appropriate events are being captured

DCL Command: SHOW AUDIT

- Review those events that are alarmed and those that are only being audited
- Test logging capability

Attempt break-in and review log for event records

DCL Command: ANALYZE/AUDIT

- Review destination of event messages and storage of log files
- Review procedures used for log analysis and actions resulting from alarms

The audit configuration reveals that alarms and logs are being generated for the same events.

```
INSS1::SYSTEM $ show audit
System security alarms currently enabled for:
  ACL
  Authorization
  Audit:          illformed
  Breakin:        dialup,local,remote,network,detached
  Logfailure:     batch,dialup,local,remote,network,subprocess,detached

System security audits currently enabled for:
  ACL
  Authorization
  Audit:          illformed
  Breakin:        dialup,local,remote,network,detached
  Logfailure:     batch,dialup,local,remote,network,subprocess,detached
```

Figure 16 – System auditing

These are the default for a system that requires low security settings. However, too many alarms will obscure actual break-in attempts, and make real-time monitoring difficult. As well, too few log events are being collected. This creates difficulties in analysis to determine if and how an actual compromise has occurred.

Evaluation of the requirements for alarms is necessary. Alarming every login and logout, for example, could generate so many alarms that administrators may choose to ignore them and miss a legitimate alarm. The addition of alarming the use of the SECURITY privilege should be considered as shown in Figure 17:

```
System security alarms currently enabled for:
  ACL
  Authorization
  Audit:          illformed
  Breakin:        dialup,local,remote,network,detached
  Logfailure:     batch,dialup,local,remote,network,subprocess,detached
  Privilege use: SECURITY
```

Figure 17 – System alarms (recommended)

As well, a determination of event logging requirements needs to be done. The current configuration is quite limited in providing information that would be useful in forensic activities after a system is compromised. For example, successful logins and logouts, privilege use and failure, and file access via special privileges could be logged (not alarmed) and would provide much more information to enable analysis.

The following example would be more representative of the resulting configuration:

```
System security audits currently enabled for:
  ACL
  Authorization
  INSTALL
  Time
  SYSGEN
  Audit:          illformed
  Breakin:        dialup,local,remote,network,detached
  Login:          batch,dialup,local,remote,network,subprocess,detached
  Logfailure:     batch,dialup,local,remote,network,subprocess,detached
  Logout:         batch,dialup,local,remote,network,subprocess,detached
  Privilege use:
    ACNT       ALLSPOOL   ALTPRI     AUDIT      BUG        BYPASS     CMEXEC     CMKRNL
    DIAGNOSE   DOWNGRADE  EXQUOTA    GROUP      GRPNAM     GRPPRV     IMPORT     IMPERSONATE
    LOG_IO     MOUNT      NETMBX     OPER       PFNMAP     PHY_IO     PRMCEB     PRMGBL
    PRMMBX     PSWAPM     READALL    SECURITY   SETPRV     SHARE      SHMEM      SYSGBL
    SYSLCK     SYSNAM     SYSPRV     TMPMBX     UPGRADE    VOLPRO     WORLD
  Privilege failure:
    ACNT       ALLSPOOL   ALTPRI     AUDIT      BUGCHK     BYPASS     CMEXEC     CMKRNL
    DIAGNOSE   DOWNGRADE  EXQUOTA    GROUP      GRPNAM     GRPPRV     IMPORT     IMPERSONATE
    LOG_IO     MOUNT      NETMBX     OPER       PFNMAP     PHY_IO     PRMCEB     PRMGBL
    PRMMBX     PSWAPM     READALL    SECURITY   SETPRV     SHARE      SHMEM      SYSGBL
    SYSLCK     SYSNAM     SYSPRV     TMPMBX     UPGRADE    VOLPRO     WORLD
  FILE access:
    SYSPRV:         read,write,execute,delete,control
    BYPASS:         read,write,execute,delete,control
```

Figure 18 – System audits (recommended)

A test of the logging with an attempted break-in revealed that the logs are enabled to capture the events:

```
INSS1::SYSTEM $ anal/audit
    Date / Time       Type       Subtype   Node    Username      ID       Term
------------------------------------------------------------------------------
5-OCT-2004 08:50:10.11 LOGFAIL  REMOTE   INSS1  <login>      0000622D REMSYS::SYSADMIN
5-OCT-2004 08:51:45.08 LOGFAIL  REMOTE   INSS1  FIELD        00006230 REMSYS::SYSADMIN
5-OCT-2004 08:51:56.96 LOGFAIL  REMOTE   INSS1  <login>      00006230 REMSYS::SYSADMIN
5-OCT-2004 08:56:48.61 LOGFAIL  REMOTE   INSS1  MAIL$SERVER  00006237 REMSYS::SYSADMIN
5-OCT-2004 08:56:54.21 LOGFAIL  REMOTE   INSS1  MAIL$SERVER  00006237 REMSYS::SYSADMIN
5-OCT-2004 08:57:55.95 LOGFAIL  REMOTE   INSS1  MAIL$SERVER  00006238 REMSYS::SYSADMIN
5-OCT-2004 08:58:10.92 BREAKIN  REMOTE   INSS1  NML$SERVER   00006238 REMSYS::SYSADMIN
```

Figure 19 – Event capture

Log files are currently stored locally on the system. Storage of the log files should be remote from the server. Local files can be altered if the system is breached and thus conceal the record of events that led to the breach.

There is currently no formal procedure for alarm response or log analysis. Alarms are only investigated if the system is exhibiting uncharacteristic performance. Logs are analyzed on an exception basis, when something unexplainable has occurred.

Results: Does not comply: System alarms and logging requirements need to be examined. There are too few log events being collected. Log files are not stored remotely. Procedures are lacking for alarm response and log analysis.

Part #4 – Audit Report

Executive Summary

The purpose of this audit was to determine the extent to which security has been applied to a report server for the company's operational support systems. Security was examined at a logical, physical and operational perspective. The scope was to determine the level of risk of an internal or external security compromise, evaluate controls, and test specific items that would provide an evaluation of the security level.

The system itself is an HP/DEC DS-10 Alpha workstation that is running the OpenVMS 7.2-1 operating system. It is accessible only internally to specific users via the intranet (TCP/IP) and DECnet. The system is running the HP version of Secure Apache Web Server.

The audit has achieved its objectives in identifying strengths and weaknesses in the security of this system.

Interviews with the System Administrator reveal an awareness of security and policies, but not an overall concern with the security of this server, due to the internal nature of the system's function and the physical location of the system.

Policy and process reviews related to the security of this system found that comprehensive systems security policies are in place, corporately. Processes for change and configuration management are instituted.

Technical assessments discovered several areas of the system security that comply with the company's security requirements. These include:

- Securing user accounts on the system
- Managing access control lists
- Managing external access to the system
- Network security

The following areas of this system's security require improvement:

- Password strength
- Discovery of system information through scanning and access attempts
- Access to system files
- Managing user privileges
- Monitoring and logging of system events

Recommendations for corrective action have been provided. The implementation of these recommendations is required to strengthen the security of this system against unauthorized access, intrusions and malicious acts. Specific findings and analysis follow.

Audit Findings and Recommendations

The following table summarizes the findings of this audit:

Item	Description	Compliance	Ref. Page
Discovery			**30**
1	Information Gathering from Banners	**No**	30
2	Port Scan	**No**	31
3	Discovery of User Accounts	**No**	33
Policies			**35**
4	Existence of Security Policy	Yes	35
Physical Security			**36**
5	Physical Location of System	Yes	36
Operations			**37**
6	Change Management	Yes	37
7	Incident Management	Yes	37
8	Security Patching	Not Assessed	
9	Segregation of Duties	Not Assessed	
User Profiles and Accounts			**39**
10	Default DEC/VMS Accounts	Yes	40
11	Password Strength	**No**	41
12	Duplicate Accounts	Yes	43
13	Orphan Files and Directories	Yes	43
14	Seldom Used and Non-active Accounts	Yes	44
Access to Files			**45**
15	Access to System Files	**No**	45
16	Access Control Lists (ACLs)	Yes	46
User Privileges			**48**
17	User Identification Codes (UICs)	**No**	48
18	Rights Identifiers	Yes	50
19	Privileges	**No**	50

Item	Description	Compliance	Ref. Page
System Access			**52**
20	Proxy Logins	Yes	52
21	Web Access	Not Assessed	
22	DECnet	Yes	53
23	Monitoring and Logging	**No**	54

Table 9 - Summary of audit findings

Action Items

Audit Finding #1 – Minimal protection against system enumeration and discovery

Reference Items: 1, 2 & 3

The system is vulnerable to discovery of information from superficial scanning and login attempts. This information contains system name and type, company name, type of operating system and version, which could be used in an attempt to compromise the system. It is also possible to test the system for valid user IDs through the SMTP "vrfy" command.

Risk: **LOW**

Recommendation #1
Employ generic banners that present no system or company information and provide a legal warning for misuse. Disable the SMTP "vrfy" command.

Audit Finding #2 – Services are running that provide clear text communication

Reference Item: 2

The system is running telnet and rsh. These are vulnerable protocols. Any connections that are made through telnet and rsh are in clear text.

Risk: **HIGH**

Recommendation #2
Replace all clear text communication such as telnet and rsh with a secure connection method such as SSH.

Audit Finding #3 – Password management requires improvement

Reference Item: 11

Default password length is less than that recommended in policy (6 instead of 8 characters). The default time between password changes is longer than that recommended in policy (90 instead of 45 days).

Password complexity of user accounts is satisfactory. Only 1 user password was easily cracked using a publicly available tool. However, this account had system privileges.

Risk: **HIGH**

Recommendation #3
Increase the default password length to 8 characters. Decrease the default time between password changes to 45 days to comply with policy. Educate users to provide them with the knowledge to strengthen their passwords.

Audit Finding #4 – Access to system files needs to be more secure

Reference Item: 15

For most system files, only 'system' and 'owner' should have all privileges, READ, WRITE, EXECUTE and DELETE (RWED, RWED, ,). Certain executables require users to be able to READ and EXECUTE (e.g. Login) (RWED, RWED, RE, RE). Several system files unnecessarily allow 'world' to have the EXECUTE privileges.

Risk: **HIGH**

Recommendation #4
Review and remove any privileges on system files for 'group' and 'world' that are unnecessary.

Audit Finding #5 – User privileges need to be reviewed and revised

Reference Items: 17 & 19

Two users were discovered that had elevated privileges due to assignment of ALL and DEVOUR privilege groups. These two users also had special privileges assigned allowing system level access.

Risk: **MEDIUM**

Recommendation #5
Review privilege groups and special privileges for all users on a regular basis.

Audit Finding #6 –System event monitoring and analysis requires improvement

Reference Item: 23

This system has auditing (event logging) enabled. However, there are too few log events being collected. As well, log files are not stored remotely. Procedures are lacking for alarm response and log analysis.

Risk: **MEDIUM**

Recommendation #6
Review the requirements for system alarms and event logs. The number of logged events should be increased. Implement procedures to review event logs. Scrutinize suspicious activities. Analyze the audit logs to become familiar with activity that is normal. Develop procedures to respond to alarms and analyze log files.

Commendatory Items

Audit Finding #7 – Policies and procedures are established and well documented

Reference Items: 4, 6 & 7

The company's Corporate Security department has issued a comprehensive security policy based on ISO 17799. This policy has been rolled out corporately, and a corporate security awareness program is in place. There is a process to provide updates to the policy and related standards.

Audit Finding #8 – The system is in a secure location

Reference Item: 5

The physical location and security controls are appropriate.

Audit Finding #9 – Accounts, files and directories are managed well

Reference Items: 10, 12, 13, 14 & 16

Default accounts have been removed or passwords changed, user accounts, files and directories are managed securely. No duplicate or inactive accounts were found. No orphan files or directories were discovered. Access Control Lists (ACLs) are managed well.

Audit Finding #10 – External access is secure

Reference Items: 20 & 22

There is no proxy access to sensitive data or applications. No privileged proxy accounts are set up. DECnet access is well managed and controlled.

Cost of Remediation

The majority of the recommendations can be implemented with little cost other than administrative labour expense. Due diligence in the administration of the security features and settings of the system will address most of the findings and mitigate the associated risks. Minimal expenditures may be incurred due to the introduction of a secure connection protocol, and a remote logging configuration, but these issues are already planned for implementation in other areas of the organization.

Conclusion

Of those items assessed, 20% of the items are high risk that do not comply, 10% are medium risk that do not comply, and another 10% are low risk that do not comply. The remaining 60% of the items are compliant. Refer to the chart below.

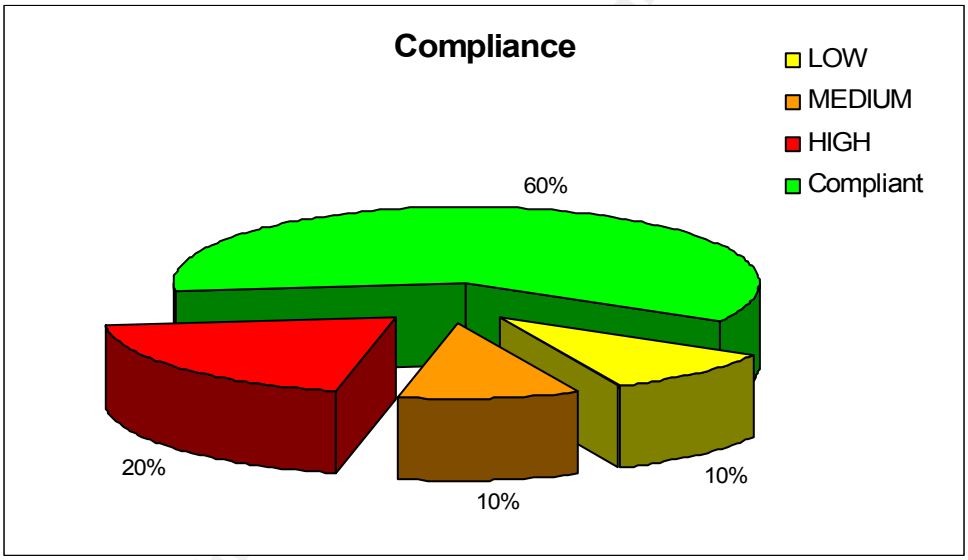

Figure 19 – System Compliance

The system can be made more secure with the implementation of the audit recommendations.

Appendix A – ISO17799 Synopsis

The 10 Controls of ISO17799[11]

ISO17799 comprises ten controls on which actions shall be taken to ensure meeting their objectives. The controls are:

Security Policy

Management defines in their security policy a strategic direction for information security and demonstrates support and commitment. The security policy, both documented and applied, is a core requirement for the success of the ISMS.

Security Organisation

The organisation of security means principles and procedures to manage information security. These also include security of third party access and outsourced information processing.

Asset Classification and Control

To protect information assets there first has to be made an inventory of all information assets given in an organisation. A classification of the information assets helps to characterise these and assign appropriate protective actions.

Personnel Security

It is the objective of personnel security to reduce the risks of human error, theft, fraud or misuse of facilities.

User training is a very important focus of personnel security to establish an understanding for information security and encourage an appropriate behaviour. This also includes training in responding to security incidents and malfunctions.

Physical and environmental security

Secure areas prevent unauthorised access, damage, and interference to business premises and protect against loss, damage, compromise of assets and interruption to business activities.

Communications and Operations Management

This control area serves (a) to ensure correct and secure facility management of information processing, (b) to mitigate the risk of systems failure, (c) to protect

[11] Fiedler, A.E., *The Standard ISO17799 as international basis*. Northwest Controlling Corporation Ltd., 2002. http://www.noweco.com/wp_iso17799e.htm

information and software integrity, (d) to ensure integrity and availability of information processing and communication services, (e) to protect information security in networks and supporting infrastructure, (f) to prevent damages to assets and ensure on-going business activities, and (g) to prevent loss, modification or misuse of information that is shared between organisations.

Access Control

Access control determines access to information systems. Unauthorised user access, computer access, access to information shall be prevented Network services shall be protected. Further some focus is put on mobile computing and teleworking.

Systems Development and Maintenance

Already during development of systems consideration must be given to sufficient security. In application systems loss, modification or misuse of user data shall be prevented. Cryptographic controls help to protect the confidentiality, authenticity, and integrity of information. Generally, IT projects and support activities shall be conducted in a secure manner.

Business Continuity Management

Corrective and preventive action shall be taken to prevent interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

Compliance with Legal Requirements

The last of the ten controls focuses on avoiding breaches of any criminal and civil law, and statutory, regulatory or contractual obligations as well as any security requirements. Further organisational security policies and standards shall be met. Audits of the ISMS shall be planned and agreed to mitigate the risk of disruptions to business processes.

Appendix B – DECnet Logs

The following provides a reference for the DECnet events that can be logged on an OpenVMS system (extract from VMS help file).

```
EVENTS

  The following is the list of events that can be reported with event
  logging.  Not all events are generated by DECnet for OpenVMS, but if a
  DECnet for OpenVMS system acts as a sink node for another system, it
  may report any of these events.

  0.0  Event records lost
  0.1  Automatic node counters
  0.2  Automatic line counters
  0.3  Automatic line service
  0.4  Line counters zeroed
  0.5  Node counters zeroed
  0.6  Passive loopback
  0.7  Aborted service request
  0.8  Automatic counters
  0.9  Counters zeroed

  2.0  Local node state change
  2.1  Access control failure

  3.0  Invalid message
  3.1  Invalid flow control
  3.2  Data base reused

  4.1  Node unreachable packet loss
  4.2  Node out-of-range packet loss
  4.3  Oversized packet loss
  4.4  Packet format error
  4.5  Partial routing update loss
  4.6  Verification reject
  4.7  Circuit down, circuit fault
  4.8  Circuit down
  4.9  Circuit down, operator initiated
  4.10 Circuit up
  4.11 Init failure, line fault
  4.12 Init failure
  4.13 Init failure, operator initiated
  4.14 Node reachability change
  4.15 Adjacency up
  4.16 Adjacency rejected
  4.17 Area reachability change
  4.18 Adjacency down
  4.19 Adjacency down, operator initiated

  5.0 Locally initiated state change
  5.1 Remotely initiated state change
  5.2 Protocol restart received in maintenance mode
```

```
5.3 Send error threshold
5.4 Receive error threshold
5.5 Select error threshold
5.6 Block header format error
5.7 Selection address error
5.8 Streaming tributary
5.9 Local buffer to small
5.13 Line initialization error
5.14 Send failure on line
5.15 Receive failed on line
5.16 Collision detect check failed on line
5.17 DTE up
5.18 DTE down
5.19 Retransmit maximum exceeded
5.20 FRMR received
5.21 Illegal frame received

7.0 DTE state change
7.1 Illegal packet received
7.2 Invalid LCN
7.3 Flow control invalid
7.4 Restart
7.5 Clear
7.6 Reset
7.7 Diagnostic
7.8 Reject
7.9 Retransmission maximum exceeded
7.10 Call failed
7.11 State change

128.1 DAP CRC error detected
128.2 Duplicate Phase 2 address error
128.3 Process created
128.4 Process terminated
```

References

Babineau, M., *Fundamentals for Securing OpenVMS Systems*. SANS GSEC Practical, April 1, 2003. http://www.giac.org/practical/GSEC/Mario_Babineau_GSEC.pdf

Bourdon, S., *A Primer on OpenVMS (VMS) Security*. SANS GSEC Practical, May 13, 2002. http://www.sans.org/rr/papers/index.php?id=604

Buchanan, R., *Open VMS 7-3.1, An Administrators View*. SANS GSNA Practical, January 14, 2003, http://www.giac.org/practical/GSNA/Randy_Buchanan_GSNA.pdf

Center for Internet Security, *Apache Benchmark for UNIX*, CIS, June 4, 2004. http://www.cisecurity.org/bench_apache.html

Ellsweig, A., *DEC VAX/VMS Operating System/Logical Security Review*, AuditNet, 2000. http://www.auditnet.org/docs/vaxsecur.txt

Fiedler, A.E., *The Standard ISO17799 as international basis*. Northwest Controlling Corporation Ltd., 2002. http://www.noweco.com/wp_iso17799e.htm

Gailly, J., *Cracking OpenVMS passwords with John the Ripper*. Gailly.net, 2002. http://gailly.net/security/john-VMS-readme.html

Galbraith, B., Woodruff, M. *Foundstone Ultimate Hacking Hands On, Course Material M9810C-003, January 2003*. Foundstone Inc., 2003. http://www.foundstone.com

Hewlett-Packard. *Industry Solutions*, Hewlett-Packard Development Company, L.P., 2004. http://h71000.www7.hp.com/solutions/

Hewlett-Packard. *OpenVMS Guide to System Security for Version 7.2-1*. Hewlett-Packard Development Company, L.P., 1999. http://h71000.www7.hp.com/doc/72final/6346/6346pro.html

Hewlett-Packard, *OpenVMS Product Directions*. Hewlett-Packard Development Company, L.P., 2004. http://h71000.www7.hp.com/openvms/OpenVMSproductdirections.htm

Information Systems Audit and Control Association. *COBIT Overview*. ISACA, 2004. http://www.isaca.org/cobit.htm

Information Technology Service Management Forum. *About ITIL.* ITSMF, 2004. http://www.itsmf.ca/about/itil.html

ISO 17799 Directory. *The ISO 17799 Service & Software Directory*. 2003. http://www.iso17799software.com/

ITIL & ITSM World. *The ITIL and ITSM Directory*. 2004. http://www.itil-itsm-world.com/index.htm

Jankowiak, P., Smiley, S., Wisniewski, J., *"Virtually Unhackable" DEFCON9: Securing OpenVMS with System Detective*, PointSecure Inc. White Paper, 2002. http://www.openvmsclub.ch/downloads/Defconwhite.pdf

Lazarus, C., *Digital VAX/VMS Audit Program*, AuditNet, 2000. http://www.auditnet.org/docs/vax_vms2.txt

LeClerc, R., *DEC VAX/VMS Operating System Security Review*. AuditNet, 2002. http://www.auditnet.org/docs/decvaxvm.txt

Leving, J., *OpenVMS 7.2 Security Essentials*. SANS GSEC Practical, November 4, 2002. http://www.giac.org/practical/GSEC/Jeff_Leving_GSEC.pdf

National Institute of Standards and Technology, *VMS/OpenVMS checklist*. Defense Information Systems Agency, 2003. http://csrc.nist.gov/pcig/CHECKLISTS/vms-openvs-srrchklst-v2r11.zip

Nguyen, M., *OpenVMS Access Controls*. AuditNet, 2004. http://www.auditnet.org/docs/OpenVMS%20Access%20Controls.doc

Office of Government Commerce (UK). *The Official ITIL Webpages*. OGC, 2004. http://www.ogc.gov.uk/index.asp?id=2261

Parker, J., *An Authentication Audit on OpenVMS: An Auditor's Perspective*, SANS GSNA Practical, April 15, 2002. http://www.giac.org/practical/Jeff_Parker_GSNA.doc

Pawlikowska, J., *OpenVMS Operating System Security Audit Plan*, AuditNet, 2002. http://www.isaca.org.pl/warsztat/OpenVMS_audyt.doc

Securityauditor.net. *ISO 17799 Security Standard*. 2001. http://www.securityauditor.net/iso17799/

Sophos Plc. "*Can my OpenVMS system become infected with a virus?"*. Sophos knowledgebase article, 2003. http://www.sophos.com/support/knowledgebase/article/156.html

Thiagarajan, V., *BS7799 Audit Checklist for SANS Institute*, SANS S.C.O.R.E, 2003. http://www.sans.org/score/checklists/ISO_17799_checklist.pdf

Wisniewski, J., *Encompass Webcast OVMS Security*. MindIQ, 2004, p3. http://www.mindiq.com/resources/webcasts/JohnwEncompasswebcast031804.ppt