Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

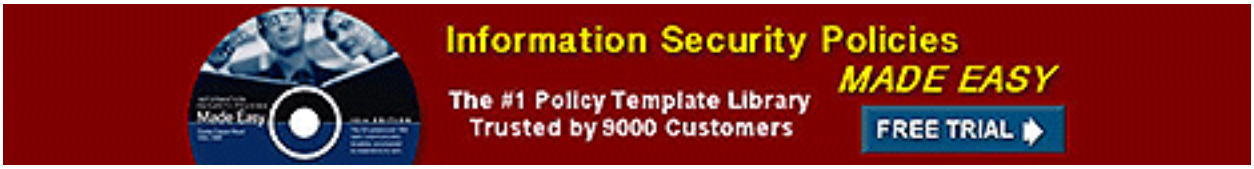
This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

OpenVMS 7.2 Security Essentials

This paper attempts to build on the foundational article submitted by Steven Bourdon in March 2002 (Bourdon), by providing a security-focused overview of the basic tasks performed when installing a standalone OpenVMS server. The steps outlined below were carried out on a MicroVAX 3100 Model 40 using a standard OpenVMS installation kit for V7.2 of the operating system (OS), but they also can apply to most VAX or Alpha Server systems. These security essentials are a distillation of the concepts and counsel provided by th...

Copyright SANS Institute
Author Retains Full Rights

AD



OpenVMS 7.2 Security Essentials

Jeffrey A. Leving

November 4, 2002

To fulfill the requirements for Practical Assignment 14.b, Option 1

Abstract

With the apparent willingness of HP to embrace the effort to port OpenVMS to Itanium (see https://www.showexhibit.com/hp_openvmstour/), the news of OpenVMS' death - as Twain would have put it - is greatly exaggerated. This paper is an expansion on the foundational paper submitted by Steven Bourdon back in March of 2002 ("A Primer on OpenVMS Security").

The purpose of this effort is to construct a Security Essentials paper on OpenVMS 7.2 to satisfy Option 1 of the GSEC V1.4b Practical Assignment by doing the following:

1) Distill the concepts and counsel provided by the OpenVMS manual "Guide to System Security" down to a basic set of implementable practices to be followed when installing and configuring the first OpenVMS system on a network;

2) Assess strengths and weaknesses of the following aspects of an OpenVMS system:

- physical environment and security,
- a basic OS installation,
- objects commonly used from the Authorization Database files and facilities,
- default state and basic configuration of key system files and directories,
- Digital's (...Compaq's...HP's...whatever!) implementation of TCP/IP for OpenVMS, and
- additional TCP/IP-based access services, like SSH;

3) Evaluate OpenVMS as a practical and "secure-able" server OS; and

4) Provide references to additional resources to take OpenVMS beyond the essentials.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

OpenVMS 7.2 Security Essentials
Jeffrey A. Leving
November 4, 2002
To fulfill the requirements for Practical Assignment 14.b, Option 1

Introduction

This paper attempts to build on the foundational article submitted by Steven Bourdon in March 2002 (Bourdon), by providing a security-focused overview of the basic tasks performed when installing a standalone OpenVMS server. The steps outlined below were carried out on a MicroVAX 3100 Model 40 using a standard OpenVMS installation kit for V7.2 of the operating system (OS), but they also can apply to most VAX or Alpha Server systems.

These security essentials are a distillation of the concepts and counsel provided by the OpenVMS manual Guide to System Security, and the features of various components of an OpenVMS server. Each feature is assessed on its strengths and weaknesses as delivered. Improvements over delivered defaults are offered. Additional resources to take OpenVMS beyond the delivered essentials also are provided.

Physical Considerations

One of the most important considerations for securing a system is physical location. Like most operating systems, OpenVMS can be easily compromised if someone gains physical access to the host server. Console control merely requires access to either a graphical console or a simple serial terminal connection to the correct serial port. All VAX and Alpha systems have a halt or "soft reset" option (though some can be physically secured with a key), so a system restart easily can be forced. With a little knowledge about the hardware and firmware architecture of the target machine, access to the console subsystem is but seconds away.

The console subsystem on the VAX platforms is known as the "the triple prompt" or "chevron" because it presents three greater-than characters (">>>"). This prompt appears after a system's POST is completed. At this point, there are no further security layers; any valid console command is authorized.

Newer Alpha servers do provide a way to secure what is known as the SRM console, putting it into secure mode (Compaq 1, p. 2-26). Yet, publicly available owner's guides for all Alpha servers also give a step-by-step procedure on how to clear the secure-mode console password (Compaq 1, p. 2-31)!

Only "security by obscurity" remains. This can be foiled once an understanding is gained of how boot control is passed from the console subsystem to OpenVMS … or by following the procedure outlined at the KJSL web site (KJSL.com). In most cases,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

even the procedure documented in one of the system management manuals delivered with OpenVMS is enough to gain privileged access to any system (Compaq 4, pp. 4-11 – 4-13). It is basically a means of bypassing the system authorization database and entering the operating environment without any password whatsoever, yet having full system privileges.

Another way of compromising an OpenVMS system once physical access is obtained is to utilize another administrative boot mode known as standalone backup. Typically, a standalone boot kit is loaded to one or more of the hard drives on a server. In addition, a standalone boot is provided on the OpenVMS installation media. When a server is in console mode, commands can be given to boot to standalone backup mode from any of these media. Once in standalone mode, the BACKUP command can be executed. Files from a backup "saveset" on any readily available media, such as a burned CD, a magnetic tape medium, or even a SCSI hard drive added to an existing bus, can subsequently be loaded to any other available media – including the hard drive on which the OS has been loaded – and the process executes in a security bypass mode.

OpenVMS Security Essential #1: Carefully consider the location of your server and ensure that console mode access is restricted to appropriate personnel.

Planning the OS Installation

From the inception of VMS, Digital Equipment Corp went to great lengths to provide system administrators with exhaustive documentation resources so that they might succeed in deploying and maintaining VMS systems. The legacy of this effort can be seen today as HP continues to provide high quality documentation for OpenVMS. The base documentation set alone for OpenVMS 7.2 includes more than 50 manuals. The Upgrade and Installation Manual provides more than 150 pages of planning helps and step-by-step instructions, an invaluable resource for deploying OpenVMS for the first time (Compaq 6). For the security-conscious, the Guide to System Security provides an explanation of security concepts as well as detailed instructions on how to implement and maintain the security features provided by OpenVMS (Compaq 3).

Planning and preparation for an OpenVMS install is distilled into a "Preinstallation Checklist" in the upgrade manual (Compaq 6, pp. 2-7 – 2-8). The assumption, however, is that the proprietary networking protocol DECnet is still the protocol of choice. Today, OpenVMS finally does live up to its name and provides almost all services over TCP/IP. Therefore, the following additional checklist items should be considered prior to an OS installation:

- Obtain an IP address, the IP subnet mask, the default gateway IP address from your network administrator. These will allow you to add your server to your network segment.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Obtain DNS domain name in which you will need to place your server, the IP address for one or more DNS name servers for that domain, and (optionally) register a DNS name for your server with your zone administrator.
- Obtain the MAC address for your network interface using the appropriate console command or tool provided from your NIC vendor. Your network administrator may need this. You should know this.
- Determine which TCP-based applications or services you intend to provide on your server. Note the TCP ports they will use, especially if you desire to utilize what would be considered a non-standard port for an application (e.g. using port 7080 for an internal HTTP server)
- Determine the TCP/IP software provider you will use. Several packages exist at varying prices, including a free package from Carnegie-Mellon University. (Note: to use the functionality of all OpenVMS tools and utilities, your TCP provider must supply what is known as "UCX compatibility" or "UCX emulation"). Obtain the installation kit media for the chosen product.

OpenVMS Security Essential #2: Use the planning tools provided by HP/Compaq but realize that they need to be augmented by your own needs analysis and resulting deployment plan.

User Account Concepts and Practices

Because the security of any OS hinges upon the design and implementation of user account policies, it is critical that we focus on this aspect of OpenVMS next. The native authentication and authorization mechanism for this OS is an authorization database employed under a Reference Monitor security model known as SYSUAF (Bourdon). Though a move toward tying OpenVMS systems into industry-standard directory servers is underway (Compaq 7), many applications written for OpenVMS over the years have been designed to take advantage of the very clean API provided into the native authorization scheme. As such, care must be taken when choosing which authentication path to take.

In the native SYSUAF, user account properties and access control information are stored in the two system files mentioned above: SYSUAF.DAT and RIGHTSLIST.DAT. The AUTHORIZE system management utility provides a command line interface into these files. Chapters 3 and 4 in the Guide to System Security offer details on the features available as well as constraints in how they can be used (Compaq 3).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
Username: DEFAULT                                Owner:
Account:                                         UIC:    [200,200] ([DEFAULT])
CLI:      DCL                                    Tables: DCLTABLES
Default:  USERROOT1:[USER]
LGICMD:   LOGIN
Flags:  DisUser
Primary days:   Mon Tue Wed Thu Fri
Secondary days:                     Sat Sun
No access restrictions
Expiration:            (none)    Pwdminimum:  6   Login Fails:     0
Pwdlifetime:         90 00:00    Pwdchange:      (pre-expired)
Last Login:            (none) (interactive),            (none) (non-interactive)
Maxjobs:         0  Fillm:       300  Bytlm:        32768
Maxacctjobs:     0  Shrfillm:      0  Pbytlm:           0
Maxdetach:       0  BIOlm:        40  JTquota:       4096
Prclm:           2  DIOlm:        40  WSdef:          256
Prio:            4  ASTlm:        40  WSquo:          512
Queprio:         0  TQElm:        40  WSextent:      1024
CPU:        (none)  Enqlm:       200  Pgflquo:      32768
Authorized Privileges:
  NETMBX    TMPMBX
Default Privileges:
  NETMBX    TMPMBX
```

Figure 1
Output from SHOW DEFAULT in the AUTHORIZE utility

The following list condenses these features down to a set of essentials to which you must attend:

- Determine a group design and apply a UIC group and member assignment strategy to it (Compaq 3, pp. 4-4 – 4-5)
- Use the same group design to establish UIC rights identifiers, which are simply descriptive names given to the UIC numerical groups (Compaq 3, pp. 4-5 – 4-8)
- Determine a good location on your file system for the home directories for your user accounts. If you have more than one hard disk on your system, user directories should be placed on a disk other than the one housing the OS files.
- Give each UIC group its own top-level directory on the disk. Define a rooted logical in the global system logical name table for that directory, as in the following example:

  DEFINE/SYSTEM/EXEC/TRANS=CONCEAL USERROOT1 DKA300:[USERS1.]
- Set appropriate access restrictions. A good practice is to deny all "Local" access unless you will have users logging in via devices that will be connected directly to your system's serial ports.
- Determine which account privileges – including the ones that are enabled upon logging in – the various groups of users require. A policy of "allow explicitly, deny by default" is best.
- Define password characteristics. Options include minimum length, "life" (how long until you force users to change their password), requiring a user to change an expired password upon successful login, the use of checking password strength against a dictionary, ensuring passwords are not reused via the password history maintenance facility, even whether or not to use a password generation facility (Compaq 4, pp. 11-2 – 11-6).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- The default settings for many of the above attributes can be found in a special username within the SYSUAF database, appropriately named DEFAULT (Figure 1). They are reasonable, but should not be misconstrued as the best settings for your environment.

A few settings that directly relate to account settings are known as Login Parameters and can be found in the system parameters tables using the SYSGEN utility (Figure 2). These global settings include settings like number of allowed login failures before break-in action is taken, how long an account is locked out if a break-in attempt threshold is exceeded, and how long the user has to enter a password when the Password: prompt is displayed at login. Again, the default for these parameters are reasonable but can be tailored to fit your needs.

```
SYSGEN>  SHOW/LGI
Parameters in use: Active
Parameter Name            Current    Default     Min.     Max.     Unit  Dynamic
--------------            -------    -------    -------  -------   ----  -------
LGI_BRK_TERM                    1          1          0        1 Boolean    D
LGI_BRK_DISUSER                 0          0          0        1 Boolean    D
LGI_PWD_TMO                    30         30          0      255 Seconds    D
LGI_RETRY_LIM                   3          3          0      255 Tries      D
LGI_RETRY_TMO                  20         20          0      255 Seconds    D
LGI_BRK_LIM                     5          5          1      255 Failures   D
LGI_BRK_TMO                   300        300          0  5184000 Seconds    D
LGI_HID_TIM                   300        300          01261440000 Seconds    D
```

Figure 2
Output from SHOW/LGI in the SYSGEN utility

Finally, some account policies relate to practices and procedures outside the control of any specific system utility. These include establishing answers to questions like

- what constitutes an unused account?
- how long will unused accounts remain on the system?
- how long and in what format will unused accounts and files from the login directory be archived?

OpenVMS Security Essential #3: Establishing user account policies and settings before installing an OpenVMS system is paramount if you want to start with a secure system. Trying to retrofit security to a system already in use can be a real bear!

(Note: It is also good system planning practice to

- ✓ *Design your file system layout*
- ✓ *Establish a backup scheme and rotation*
- ✓ *Determine what processes should be enabled on system startup*
- ✓ *Determine what processes require special handling during the system shutdown sequences and devise a graceful shutdown procedure for them*
- ✓ *Establish policies and procedures for system features that affect performance, such as page file locations and defragmentation schedules for hard drives*

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- ✓ *Set resource thresholds on things like CPU, disk, memory, and network interface utilization, and implement alert mechanisms to notify administrators when these limits are being exceeded*
- ✓ *Determine if disk quota management is necessary, and design and implement a management plan*

But these fall outside the scope of this paper.)

Installing the Operating System

Again, the documentation from Compaq shines. Chapter 3 of the Upgrade and Installation Manual is essentially a copy of the installation script annotated with coaching tips on how to answer script prompts during the install process (Compaq 6). For most basic, non-clustered OpenVMS installations, the prompt defaults provide very reasonable options.

During the "Selecting Optional OpenVMS Components" questioning (Figure 3), it is possible to implement all services using only the TCP/IP protocol family, so answering "No" to queries concerning the installation of DECnet products is preferred.

```
Select optional software you want to install. You can install one
 or more of the following OpenVMS or DECwindows components:

 o OpenVMS library                                -  52200 blocks
 o OpenVMS optional                               -  19000 blocks
 o OpenVMS Help Message                           -  10400 blocks
 o OpenVMS Management Station                     -  20000 blocks
 o DECwindows base support                        -   4400 blocks
 o DECwindows workstation support                 -  23800 blocks
       -  75 dots per inch video fonts            -   (included)
       - 100 dots per inch video fonts            -   6200 blocks
 o DECnet-Plus networking                         -  80000 blocks
 o DECnet Phase IV networking                     -    800 blocks
```

Figure 3
Sample dialog information during installation

Both usernames and passwords are case-insensitive in OpenVMS. The LOGINOUT.EXE program that controls interactive logins performs an "upcase" function on these character strings. However, all ASCII characters found on most keyboards (ASCII Hex 21 through 7E) – not just alphanumeric characters – can be used in these authentication strings. The installation procedure only counsels that the length of these passwords should be greater than eight characters. You should instead choose strong passwords by including non-alphanumeric characters in the password string (CERN). To be fair, this is one of the first topics covered in the Guide to System Security mentioned earlier (Compaq 3, p. 3-1).

OpenVMS Security Essential #4: Following the installation "Yellow Brick Road" is fine until you come to Password Junction. Take the path that leads to stronger passwords!

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Securing OpenVMS after the OS Installation

The installation guide does provide you with a chapter of things to do after completing the initial installation of the OS. These tasks even give the novice OpenVMS administrator some idea of the types of activities that are required to effectively manage and OpenVMS server from this point onward. Yet, the primary emphases are more in the areas of system reliability and performance, rather than security (Compaq 6, p. 4-1, note bulleted items).

Even before you install networking software on an OpenVMS system, you should carefully perform the following security-related tasks:

- Keep non-privileged users from perusing key system directories by executing the following commands **in order**:
  - set security/class=file/prot=(w:e) sys$sysroot:[000000]*.dir
  - set security/class=file/prot=(w:e) sys$common:[000000]*.dir
  - set security/class=file/prot=(w:re) sys$sysroot:[000000]*lib*.dir
  - set security/class=file/prot=(w:re) sys$sysroot:[000000]*hlp*.dir
  - set security/class=file/prot=(w:re) sys$common:[000000]*lib*.dir
  - set security/class=file/prot=(w:re) sys$common:[000000]*hlp*.dir
- Keep non-privileged users from accessing **anything** (except the global login command file) in SYS$MANAGER by issuing the following commands **in order**:
  - set security/class=file/prot=(w) *.*;*
  - set security/class=file/prot=(w:e) sylogin.com
- Keep non-privileged users from accessing system data and command files in SYS$SYSTEM by executing the following commands **in order:**
  - set security/class=file/prot=(w) *.dat
  - set security/class=file/prot=(w:e) *.com
  - set security/class=file/prot=(w) startup.com
  - set security/class=file/prot=(w) shutdown.com
- Make backup copies - or at least get printouts – of the seven key system startup and shutdown command files in the SYS$MANAGER system directory: SYCONFIG.COM, SYLOGICALS.COM, SYLOGIN.COM, SYPAGSWPFILES.COM, SYSECURITY.COM, SYSHUTDWN.COM, and SYSTARTUP_VMS.COM. Do this every time you modify one of these, too.
- Make backup copies of the two key authorization files in the SYS$SYSTEM system directory: SYSUAF.DAT and RIGHTSLIST.DAT
- Edit the text file associated with the SYS$ANNOUNCE system logical. Be sure to add a disclaimer in the text that indicates that only authorized users should be even attempting to gain access to your system. For example:

  This is a private computing facility. Unless you have been specifically authorized to access this system, your continued attempts to do so will expose you to criminal and/or civil proceedings.
- Edit the text file associated with the SYS$WELCOME system logical, too. Some login facilities, such as the one presented by David L. Jones' port of

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

SSHD (Jones), do not display the SYS$ANNOUNCE message text. To ensure that every interactive user is given notice about your policy concerning unauthorized system access, you should include a post-access statement in this text file.

- Use the INSTALL utility to make a baseline listing of all "known images." Because known images can be granted elevated processing privileges, back doors or trap doors into system-level processes are possible under OpenVMS. Read section 16.9 in the advanced System Manager's manual and keep an updated listing of known images (Compaq 5).

OpenVMS Security Essential #5: The default state of the file system immediately after installation is fairly secure, but can be improved. Disable snooping privileges for non-privileged users.

OpenVMS Security Essential #6: You can never have too many backups of critical system files! Backup early, backup often.

Installing "TCP/IP Services for OpenVMS"

If you want the most secure OpenVMS system possible, stop here.

If your OpenVMS system cannot be an island unto itself, you will need to install a network transport protocol.

If your OpenVMS system cannot be isolated to "DECnet LANd," you will need to install a TCP/IP package like Compaq's "TCP/IP Services for OpenVMS."

The HP TCP/IP package for OpenVMS still has Digital in its official name (Compaq 2). The installation and configuration guide for this package provides a comprehensive look at the product. Like the OS guide, an installation planning section is included. The TCP/IP items mentioned in the **Planning the OS Installation** section above can be used to answer most of the questions in Table 1-2 in this planning section, but there are a few other items that need attention.

Of particular note is the question about enabling SNMP. If you or your network administrator are not running a management tool that uses SNMP (e.g. HP OpenView), then it is best not to enable this service. A recent search on SNMP vulnerabilities on the CERT Coordination Center's web site returned 318 entries under "Vulnerability Notes" alone! (CERT).

During the actual product installation, the option defaults provide adequate answers to all the questions. Chapter three of the installation guide steps you through the configuration of TCP/IP services once the product is installed.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
DIGITAL TCP/IP Services for OpenVMS Configuration Menu

 Configuration options:

         1  -  Core environment
         2  -  Client components
         3  -  Server components
         4  -  Optional components
         5  -  Shut down DIGITAL TCP/IP Services for OpenVMS
         6  -  Start up DIGITAL TCP/IP Services for OpenVMS
         7  -  Run tests

         A  -  Configure options 1 - 3
        [E] -  Exit configuration procedure

 Enter configuration option:
```

Figure 4
Main configuration menu in SYS$MANAGER:TCPIP$CONFIG.COM

While stepping through the four menu options that deal with enabling or disabling various services (Figure 4), it is obvious that HP continues to take the conservative approach started by Digital many years ago: start with everything implicitly disabled and require the system administrator to explicitly enable any desired services. A quick run through the service options reveals that the more recently developed secure services are not available under HP's TCP package. Other vendor offerings, like MultiNet from Process Software, come with services like Secure Shell or Secure Copy Protocol that provide "strong authentication and secure, encrypted communications over insecure channels" (Process).

Enabling the client versions of some of the older services poses minimal risks. The LPR/LPD client provides the ability to define TCP-based print queues on the OpenVMS server, so users could print to network-based printers like HP LaserJets with network cards. The FTP client would facilitate accessing sites on the Internet from which other software packages or tools for OpenVMS could be obtained.

Unfortunately, the TELNET server service must be enabled in order to enable the TELNET client. The 118 vulnerability notes on the CERT site relating to TELNET should cause the average system administrator to pause before allowing these services to run.

Fortunately, there a still a few souls willing to devote some time to OpenVMS out in the Open Source realms. By carefully utilizing their opuses, you can provide a fairly useful set of services by which OpenVMS can play on the Internet and still keep the bad guys out of your playground.

OpenVMS Security Essential #7: Know your TCP package. Better yet, know your TCP services and decide which ones you can afford to run on your server from a security viewpoint.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Installing OpenSSL and a basic SSH server

An example of a secure counterpart to the remote terminal emulator service known as TELNET is Secure Shell. Secure Shell has been around since 1995 (VanDyke). It has gone through a significant revision (SSH V1 to SSH V2), and its functionality even has expanded to include a secure file transport service known as SFTP (OpenSSH). A commercial version of SSH is available as well as a free version (via the OpenBSD Project).

David L. Jones in Ohio State University's College of Engineering adapted SSH V1 into a basic yet very functional SSH Server for OpenVMS. A Zip'd version of his installation kit is available at his website (Jones). The ZIP file expands out into one directory, and the file AAAREADME.TXT provides a terse overview and installation instructions.

Jones' SSH server depends on an Open Source version of SSL for VMS like the port of OpenSSL 0.9.2b and/or SSLeay 0.8.1a done by Richard Levitte. Levitte improved on an OpenSSL development effort started by Eric A. Young, Tim J. Hudson and Robert Byer, calling his release OpenSSL 0.9.4 for VMS (Levitte). After obtaining the compressed installation kit via FTP, expanding it into a working directory, installation instructions for a VMS install can be found in the INSTALL.VMS file.

A C compiler must be installed in order to "make" both OpenSSL and the SSH server that follows. OpenSSL must be made before the SSH Server.

A complete MAKE command file for OpenSSL - called MAKEVMS.COM - can be invoked right from a DCL command line to build OpenSSL:

```
@makevms all norsaref nodebug decc
```

Except for a few informational compiler messages, the build is clean. Levitte even provides a fairly comprehensive set of test procedures to verify the product's functionality once it is built. These tests can be found in the [.TEST] subdirectory. Once the application startup procedure is added to one of your system startup command files and invoked interactively (with SYSPRV permissions), OpenSSL installation is complete.

The build for the SSH server lacks a few of the niceties provided by the OpenSSL installation kit, but, hey, it's free! The April 17, 2002, version of Jones' BUILD_SSH_SERVER.COM has one minor error during the linking phases, and it does not provide a set of commands to move the application files into a target directory. Nevertheless, the installation can be accomplished with just a little understanding about the VMS Linker, sharable, run-time executables, and some basic DCL skills. Everything except for the linker patch is documented in the AAAREADME.TXT file mentioned earlier. For the sake of maintaining this paper's brevity, these corrections are left as an exercise for the reader.

Once these packages are installed, TELNET is no longer a necessary service, so at least the server component of TELNET can be disabled via the management

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

interface for your TCP stack. A secured, remote OpenVMS login session is now possible using any SSHV1-compliant client utility, such as SSH's Secure Shell or PuTTY.

Figure 5
Warning dialog box from SSH's Secure Shell V2.4.0

OpenVMS Security Essential #8: TANSTAAFL (There Ain't No Such Thing As A Free Lunch). While there are a few free Open Source packages available for OpenVMS, they have their limitations (see Figure 5) and improvements will come only as more people pitch in with development or enhancement efforts. Better products are available, but they come with a price tag. Nevertheless, OpenVMS can indeed play safely in the Internet.

A Basic Security Evaluation Using Nmap

After all these baselining activities have been completed, it is a good idea to find a few of the tools the black hats use and try them out against your system. One such tool – Nmap from eEye Digital Security – is a commonly used reconnaissance tool. In addition to providing a TCP port scanning function, Nmap can also

- use TCP/IP fingerprinting to guess a remote OS
- use TCP "ping" to determine what hosts are around on an IP segment, and
- operate under a bunch of stealth options to hide what's being done!

Overall, Nmap does not find very much of interest on an OpenVMS server other than a trivial TCP sequencing scheme (Figure 6). Even before installing the SSH/SSL combination above, only the explicitly enabled services show to be open. In addition, Nmap's OS fingerprints database cannot determine the OS.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
C:\apps\Nmapnt>nmapnt -P0 -sS -O bastia


Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org  ( www.insecure.org/nmap/ )

Interesting ports on bastia.noname.com (192.168.135.86):
(The 1522 ports scanned but not shown below are in state: closed)
Port       State       Service
23/tcp     open        telnet

TCP Sequence Prediction: Class=64K rule
                         Difficulty=1 (Trivial joke)
No OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
TSeq(Class=64K)
T1(Resp=Y%DF=N%W=C6C%ACK=S++%Flags=AS%Ops=MNW)
T2(Resp=N)
T3(Resp=Y%DF=N%W=C6C%ACK=O%Flags=A%Ops=)
T4(Resp=Y%DF=N%W=BB8%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(Resp=N)


Nmap run completed -- 1 IP address (1 host up) scanned in 38 seconds
```

Figure 6
Output from NmapNT on a Windows 2000 workstation

After installing SSH and SSL, Nmap does take a stab at guessing the OS, but it wrongly identifies the server as a system running Digital Unix (Figure 7)!

```
C:\apps\Nmapnt>nmapnt -P0 -sS -O bastia


Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org  ( www.insecure.org/nmap/ )

Interesting ports on bastia.noname.com (192.168.135.86):
(The 1522 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh

TCP Sequence Prediction: Class=64K rule
                         Difficulty=1 (Trivial joke)
Remote operating system guess: Digital UNIX OSF1 V 3.0,3.2,3.2C

Nmap run completed -- 1 IP address (1 host up) scanned in 29 seconds
```

Figure 7
More output from NmapNT

Here again OpenVMS benefits a bit from its lack of prevalence within the Internet community. If you can obtain useful, stable, OpenVMS versions of applications you need to run, this OS is less frequently targeted for intrusion attempts. This is not a

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

guarantee that intrusions will not occur, but the arcane nature of OpenVMS is a definite plus.

OpenVMS Security Essential #9: Every success you have in implementing a security mechanism on OpenVMS is sweet, but a security administrator's work is never done.

"Never, never, never underestimate your adversaries."

- George Bakos at SANSFIRE 2002, Boston, MA

Concluding Observations

Aside from the physical vulnerabilities inherent in almost every server architecture, an OpenVMS server provides a very securable platform to run networked applications. Many of its strengths and weaknesses come from the facts that

1) OpenVMS did not adopt TCP/IP as its preferred, native network transport protocol until later in life,
2) OpenVMS has been viewed as a proprietary OS, serving niche markets rather than the Open Source community at large, and
3) OpenVMS is dying or already dead (end-of-life'd by its owners).

Yet, with the apparent willingness of HP to embrace the effort to port OpenVMS to the new Intel Itanium architecture (Hewlett Packard), the news of the death of OpenVMS - as Mark Twain would have put it - is greatly exaggerated. If OpenVMS is truly "opened," many may find it an attractive, alternative, multi-tasking OS to both Unix and Windows Server.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

Bourdon, Steven. "A Primer on OpenVMS (VMS) Security." March 13, 2002. URL: http://rr.sans.org/start/openvms.php

CERN. "CERN Security Handbook." December 12, 1996. URL: http://consult.cern.ch/writeups/security/security_3.html

CERT(R) Coordination Center. "Search the Collections." Copyright © 1997, 2002 Carnegie Mellon University. URL: http://search.cert.org

Compaq Computer Corporation. "AlphaServer ES45 Owner's Guide." Houston: Compaq Computer Corporation, February 2002. URL: http://www.compaq.com/alphaserver/download/ek-es450-ug-b01.pdf

Compaq Computer Corporation. DIGITAL TCP/IP Services for OpenVMS: Installation and Configuration (HTML version). Houston: Compaq Computer Corporation, January 1999. Order Number: AA--LU49L--TE.

Compaq Computer Corporation. Guide to System Security. Houston: Compaq Computer Corporation, January 1999. Order Number: AA-Q2HLD-TE.

Compaq Computer Corporation. OpenVMS System Manager's Manual: Essentials. Houston: Compaq Computer Corporation, January 1999. Order Number: AA-PV5ME-TK.

Compaq Computer Corporation. OpenVMS System Manager's Manual: Tuning, Monitoring, and Complex Systems. Houston: Compaq Computer Corporation, January 1999. Order Number: AA-PV5NE-TK.

Compaq Computer Corporation. OpenVMS VAX Version 7.2 Upgrade and Installation Manual. Houston: Compaq Computer Corporation, January 1999. Order Number: AA-QSBQC-TE.

Compaq OpenVMS Support Forum. Message: "Can eDir replace SYSUAF et al?" Oct 4, 2002. URL: http://161.114.17.92/forum?14@168.zGulh2rEbEc.1@.ef0bcfa!SearchMark=1#1 (Note 1: you may need a free login account to access this forum's information; Note 2: HP scheduled to move the Compaq Support Forums to the HP Support Forums in mid-October of 2002)

Hewlett Packard (HP.com and Compaq.com combined web site). "Alpha to Itanium®-based systems: OpenVMS." Copyright © 1994-2002 Hewlett-Packard Company. URL: http://www.compaq.com/hps/ipf-enterprise/openvms.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Jones, David L. "SSH server (V1.5 protocol)." April 2002. URL: http://kcgl1.eng.ohio-state.edu/~JONESD/ssh/

KJSL.com. "VMS frequently asked questions: System Management: MGMT5. I've forgotten the SYSTEM password - what can I do?" Last updated January 14, 2000. URL: http://mate.kjsl.com/vmsfaq/mgmt.htm#MGMT5

Levitte, Richard. "SSLeay/OpenSSL." January 16, 2002. URL: http://www.free.lp.se/openssl/

OpenSSH. Copyright © 1999-2002 OpenBSD. "Project History and Credits ." URL: http://www.openssh.com/history.html

Process Software. "MultiNet® for OpenVMS V4.4: Data Sheet." October 2002. http://www.process.com/tcpip/multinetds.html

The Blue Letter Bible. "Job - Chapter 5." URL: http://www.blueletterbible.org/kjv/Job/Job005.html#4

VanDyke Software. "History of the Protocol." Copyright © 2002 VanDyke Software, Inc. All rights reserved. URL: http://www.vandyke.com/solutions/ssh_overview/ssh_overview_history.html

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 2nd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced