Unauthorised Access UK 0636-708063 10pm-7am 12oo/24oo

HACKING VAX'S VMS

INTRODUCTION

The VAX is made by DEC (Digital Equipment Corp) and can run a variety of operating systems. In this file i will talk about the VMS (Virtual Memory Operating System), VMS also runs on the PDP-11, both mainframes are 32 bit machines with 32 bit virtual address space.

ENTRANCE:

When you first connect to a VAX you type either a return, a ctrl-c or a ctrl-y. It will then respond with something similar to this:

```
USERNAME:
PASSWORD:
```

The most frequent way of gaining access to a computer is by using a 'default' password, this by the way is not very successful.......
When DEC sells a VAX/VMS, the system comes equipped with 4 accounts which are:

DEFAULT : This serves as a template in creating user records in the UAF (User Authorization File). A new user record is assigned the values of the default record except where the system manager changes those values. The default record can be modified but can not be deleted from the UAF.....

SYSTEM : Provides a means for the system manager to log in with full privileges. The SYSTEM record can be modified but cannot be deleted from the UAF.......

FIELD : Permits DIGITAL field service personnel to check out a new system. The FIELD record can be deleted once the system is installed.

SYSTEST: Provides an appropriate environment for running the User Environment Test Package (UETP). The SYSTEST record can be deleted once the system is installed.

Usually the SYSTEM MANAGER adds,deletes, and modifies these records which are in the UAF when the system arrives, thus eliminating the default passwords, but this is not always the case.....
some default passwords which have been used to get in a system are....

USERNAME	PASSWORD
SYSTEM	MANAGER or OPERATOR
FIELD	SERVICE or TEST
DEFAULT	USER or DEFAULT
SYSTEST	UETP or SYSTEST

Other typical VMS accounts are :
VAX
VMS
DCL
DEMO
GUEST
GENERAL
TEST
HELP
GAMES
DECNET

Or a combination of the various usernames and passwords. If none of these get you in , then you should try another system unless you have away of getting an account either by trashing or other means.....

YOUR IN!!!!!!

You will know that you are in by receiving the prompt of a dollar sign ($). You will be popped into the default directory which is dependent on what account you logged in as. If you get in as system manager (highly unlikely) you have full access....
If you get the FIELD or SYSTEST account , you may or may not have full access, but you may have the privileges to give your self full access.

To give privs to yourself:

```
$ SET PROCESS/PRIVS=ALL
```

The VMS system has full help files available by typing HELP. You can use the wildcard character of an '*' to list out info on every command:

```
$ help *
```

When you first logon, it may be to your advantage to get a list of all users currently logged onto the system if there are any at all. You can do this by:

```
$ SHOW USERS

VAX/VMS Interactive Users-Total=4
```

```
01-may-1989  11:37:21.73
0PAO:    DEMO      004C004C
TTD2:    FIELD     004E02FF
TTD1:   SYSMAN     0043552E
TXB3   TRTRTRRTR   01190057
```

It is highly recommended that if you are logged on in the day and there are people logged in, especially the system manager or the account you are logged on as appears twice.. log out straight away, and call back later. You do not want to call to late though as the system keeps a record of when each user logs in and out.

To communicate with other users or other hackers that are on the system, use the PHONE utility..

```
$ PHONE Username
```

If the system has DEC-NET you can see what available nodes there are by :

```
$ SHOW NETWORK
```

If you have mail the system will tell you as soon as you logon, simply type:

```
$ MAIL
```

This will invoke the Personal Mail Utility, you can then either read your mail or select help....

DIRECTORIES:
To see what you have in your directory type:

```
$ DIR
```

To get a list of directories on the system type:

```
$ DIR *.*
```

When a VAX/VMS is first installed, it comes with 9 directories which are not listed when you execute the DIR *.* command:

<SYSLIB>
This directory contains various macro and object libraries.

<SYSMSG>
This directory contains files used in managing the operating system.

<SYSMGR>
This directory contains text files and help libraries for the HELP library.

<SYSERR>
This is the directory for the error log file (ERRLOG.SYS).

<SYSTEST>
This directory contains files used in testing the functions of the operating system.

<SYSMAINT>
This directory contains system diagnostic programs.

<SYSUPD>
This directory contains filesused in applying system updates.

<SYSUPD.EXAMPLES>
This directory contains sample driver programs, user-written system services, and other source programs.

<SYSEXE>
This directory contains the executable images of most of the functions of the operating system.
Inside these directoriesare files with the following file types:

File-Type:	Description:	command:
.hlp	system help file	TYPE filename
.dat	data file	TYPE filename
.msg	message file	TYPE filename
.doc	Documentation	TYPE filename
.log	LOG file	TYPE filename
.err	ERROR msg file	TYPE filename
.seq	sequential file	TYPE filename
.sys	system file	FILE-NAME
.exe	executable file	FILE-NAME
.com	command file	COMMAND NAME
.bas	basic file	RUN file-name
.txt	ascii text file	TYPE filename

There are others but you won't see them as much as the above. You can change the directories either by using the CHANGE command or by using the SET DEFAULT command:

```
$ CHANGE <DIR.NAM>
      or
$ SET DEFAULT <DIR.NAM>
```

You can now list and execute the files in this directory without first the directory name followed by the filename as long as you have sufficient access. If you don't have sufficient access you can still view files within directories that you cannot default to by:

```
$ TYPE <LOD.DIR> LOD.MAI;1
```

This will list the contents of the file LOD.MAI;1 in the directory of <LOD.DIR>

The use of wildcards is very helpful when you desire to view all the mail or something on the system. To list out all the users mail if you have access type:

```
$TYPE <*.*>*.MAI;*
```

As you may have noticed mail files have the extension of MAI at the end. The ;1 or ;2 etc are used to number files with the same name.

PRIVILEGES

Privileges fall into 7 categories according to the damage that the user possessing them could cause to the system:

NONE   - No privileges

NORMAL - minimum privileges to use the system.

GROUP - Potential to interfere with members of the same group.

DEVOUR - Potential to devour noncritical system-wide resources.

SYSTEM - Potential to interfere with normal system operation.

FILE   - Potential to comprimise file security.

ALL   - Potential to control the system (wouldn't that be good ahah).

THE UAF

The User Authorization File contains the names of the users who may log into the system and also contains a record of the users privileges. Each record in the UAF includes the following:

1. Name and Password.
2. User Identification Code(UIC)-- Identifies a user by a group number and a member number.
3. Default file specification --- Has the default device and directory

names for file access.

4. Login command file --- Names a command procedure to be executed automatically at login time.
5. Login flags --- Allows the system manager to inhibit the user of the ctrl-y functions and lock user passwords.
6. Priority ---- Specifies the base priority of the process created by the user at login time.
7. Resources --- Limits the system resources the user may perform.
8. Privileges --- Limits the activities the user may perform.

If you have SYSTEM MANAGER privileges, you will be able to add,delete, and modify records in the UAF.

The AUTHORIZE Utility allows you to modify the information in the UAF. It is usually found in the SYSEXE directory.
The commands for AUTHORIZE are:

```
ADD Username  <qualifier..> Adds a record to the UAF.
EXIT (or CTRL-Z) Returns you to command level.
HELP Lists the AUTHORIZE commands.
LIST <Userspec></FULL> Creates a listing file of UAF records.
MODIFY Username  Modifies a record.
REMOVE Username  deletes a record.
SHOW     Displays UAF records.
```

The most useful besides ADD is the SHOW command. SHOW displays reports for selected UAF records. YOU can get a /BRIEF listing of a /FULL listing. BUT before you do that, you may want to make sure no one is logged on besides you,to make sure know one can log on type the following:

```
$ SET LOGINS /INTERACTIVE=0
```

This establishes the max number of users able to log in to the system, this command does not affect users currently logged on.

To list out the userfile do the following:

```
$ SET  DEFAULT <SYSEXE>
$ RUN AUTHORIZE
UAF> SHOW * /BRIEF
```

UAF
Unfortunately you cannot get a listing of passwords,though you can get a listing of all the users as shown above... The passwords are encrypted just like the unix systems.
If you have sufficient privs you can create your own account.........

```
UAF> ADD <Username> /PASSWORD=HACKER /UIC=<014,006> /CPUTIME=0
```

```
/DEVICE=SYS$ROOT_/ACCOUNT=VMS /DIRECTORY=<SYSERR> /PRIVS=ALL
/OWNER=DIGITAL /NOACCOUNTING
```

1. ADD USERNAME
2. SPECIFY THE PASSWORD YOU WANT TO USE....
3. ASSIGN A UIC CONSISTS OF 2 NUMBERS FROM 0 TO 377 SEPERATED BY A COMMAND ENCLOSED IN BRACKETS....
4. CPUTIME IS IN DELTA FORMAT, 0 MEANS INFINITE......
5. SPECIFY THE DEVICE THAT IS ALLOCATED TO THE USER WHEN THEY LOGIN. OTHER DEVICES ARE SYS$DEVICE,SYS$SYSDISK ETC..
6. SPECIFYING AN ACCOUNT IS NOT REALLY NECCESSARY
7. PRIVS YOU ARE GOING TO WANT ALL THE PRIVS AREN'T YOU???
8. VERY IMPORTANT.... NOACCOUNTING WILL DISABLE THE SYSTEM ACCOUNTING RECORDS,THUS NOT ADDING INFORMATION TO THE ACCOUNTING.DAT FILE.

LOGGING OFF

Simply type:

```
$ LOGOUT
```

This file was written by Terry Gilligan if you want any more info on the vax contact me, i will help you as much as i can.. have lots more info on vax security if anyone is interested..