THE BASICS OF HACKING: INTRO

Uploaded by Elric of Imrryr

THE FIRST OF A SET OF ARTICLES:
AN INTRODUCTION TO THE WORLD OF THE HACKER. BASICS TO KNOW BEFORE DOING ANYTHING, ESSENTIAL TO YOUR CONTINUING CAREER AS ONE OF THE ELITE IN THE COUNTRY...

THIS ARTICLE, "THE INTRODUCTION TO THE WORLD OF HACKING" IS MEANT TO HELP YOU BY TELLING YOU HOW NOT TO GET CAUGHT, WHAT NOT TO DO ON A COMPUTER SYSTEM, WHAT TYPE OF EQUIPMENT SHOULD I KNOW ABOUT NOW, AND JUST A LITTLE ON THE HISTORY, PAST PRESENT FUTURE, OF THE HACKER.

WELCOME TO THE WORLD OF HACKING!
WE, THE PEOPLE WHO LIVE OUTSIDE OF THE NORMAL RULES, AND HAVE BEEN SCORNED AND EVEN ARRESTED BY THOSE FROM THE 'CIVILIZED WORLD', ARE BECOMMING SCARCER EVERY DAY. THIS IS DUE TO THE GREATER FEAR OF WHAT A GOOD HACKER (SKILL WISE, NO MORAL JUDGEMENTS HERE) CAN DO NOWADAYS, THUS CAUSING ANTI-HACKER SENTIMENT IN THE MASSES.
ALSO, FEW HACKERS SEEM TO ACTUALLY KNOW ABOUT THE COMPUTER SYSTEMS THEY HACK, OR WHAT EQUIPMENT THEY WILL RUN INTO ON THE FRONT END, OR WHAT THEY COULD DO WRONG ON A SYSTEM TO ALERT THE 'HIGHER' AUTHORITIES WHO MONITOR THE SYSTEM.
THIS ARTICLE IS INTENDED TO TELL YOU ABOUT SOME THINGS NOT TO DO, EVEN BEFORE YOU GET ON THE SYSTEM. WE WILL TELL YOU ABOUT THE NEW WAVE OF FRONT END SECURITY DEVICES THAT ARE

BEGINNING TO BE USED ON COMPUTERS.
WE WILL ATTEMPT TO INSTILL IN YOU A
SECOND IDENTITY, TO BE BROUGHT UP AT
TIME OF GREAT NEED, TO PULL YOU OUT
OF TROUBLE.
AND, BY THE WAY, WE TAKE NO, REPEAT,
NO, RESPONCIBILITY FOR WHAT WE SAY IN
THIS AND THE FORTHCOMING ARTICLES.
ENOUGH OF THE BULLSHIT, ON TO THE FUN:

AFTER LOGGING ON YOUR FAVORITE BBS,
YOU SEE ON THE HIGH ACCESS BOARD A
PHONE NUMBER! IT SAYS IT'S A GREAT
SYSTEM TO "FUCK AROUND WITH!"
THIS MAY BE TRUE, BUT HOW MANY OTHER
PEOPLE ARE GOING TO CALL THE SAME
NUMBER? SO: TRY TO AVOID CALLING A
NUMBER GIVEN TO THE PUBLIC. THIS IS
BECAUSE THERE ARE AT LEAST EVERY OTHER
USER CALLING, AND HOW MANY OTHER BOARDS
WILL THAT NUMBER SPREAD TO?
IF YOU CALL A NUMBER FAR, FAR AWAY, AND
YOU PLAN ON GOING THRU AN EXTENDER OR
A RE-SELLER, DON'T KEEP CALLING THE
SAME ACCESS NUMBER (I.E. AS YOU WOULD
IF YOU HAD A HACKER RUNNING), THIS
LOOKS VERY SUSPICIOUS AND CAN MAKE
LIFE MISERABLE WHEN THE PHONE BILL
COMES IN THE MAIL. MOST CITIES HAVE
A VARIETY OF ACCESS NUMBERS AND
SERVICES, SO USE AS MANY AS YOU CAN.
NEVER TRUST A CHANGE IN THE SYSTEM...
THE 414'S, THE ASSHOLES, WERE CAUGHT
FOR THIS REASON: WHEN ONE OF THEM
CONNECTED TO THE SYSTEM, THERE WAS
NOTHING GOOD THERE. THE NEXT TIME,
THERE WAS A TREK GAME STUCK RIGHT IN
THEIR WAY! THEY PROCEDED TO PLAY SAID
GAME FOR TWO, SAY TWO AND A HALF HOURS,
WHILE TELENET WAS TRACING THEM! NICE
JOB, DON'T YOU THINK? IF ANYTHING
LOOKS SUSPICIOUS, DROP THE LINE
IMMEDIATELY!! AS IN, YESTERDAY!!
THE POINT WE'RE TRYING TO GET ACCROSS
IS: IF YOU USE A LITTLE COMMON SENCE,
YOU WON'T GET BUSTED. LET THE LITTLE
KIDS WHO AREN'T SMART ENOUGH TO
RECOGNIZE A TRAP GET BUSTED, IT WILL

TAKE THE HEAT OFF OF THE REAL HACKERS.
NOW, LET'S SAY YOU GET ON A COMPUTER SYSTEM... IT LOOKS GREAT, CHECKS OUT, EVERYTHING SEEMS FINE. OK, NOW IS WHEN IT GETS MORE DANGEROUS. YOU HAVE TO KNOW THE COMPUTER SYSTEM (SEE FUTURE ISSUES OF THIS ARTICLE FOR INFO ON SPECIFIC SYSTEMS) TO KNOW WHAT NOT TO DO. BASICALLY, KEEP AWAY FROM ANY COMMAND WHICH LOOKS LIKE IT MIGHT DELETE SOMETHING, COPY A NEW FILE INTO THE ACCOUNT, OR WHATEVER! ALWAYS LEAVE THE ACCOUNT IN THE SAME STATUS YOU LOGGED IN WITH. CHANGE _NOTHING_...
IF IT ISN'T AN ACCOUNT WITH PRIV'S, THEN DON'T TRY ANY COMMANDS THAT REQUIRE THEM! ALL, YES ALL, SYSTEMS ARE GOING TO BE KEEPING LOG FILES OF WHAT USERS ARE DOING, AND THAT WILL SHOW UP. IT IS JUST LIKE DROPPING A TROUBLE-CARD IN AN ESS SYSTEM, AFTER SENDING THAT NICE OPERATOR A PRETTY TONE. SPEND NO EXCESSIVE AMOUNTS OF TIME ON THE ACCOUNT IN ONE STRETCH. KEEP YOUR CALLING TO THE VERY LATE NIGHT IF POSSIBLE, OR DURING BUSINESS HOURS (BELIEVE IT OR NOT!). IT SO HAPPENS THAT THERE ARE MORE USERS ON DURING BUSINESS HOURS, AND IT IS VERY DIFFICULT TO READ A LOG FILE WITH 60 USERS DOING MANY COMMNDS EVERY MINUTE. TRY TO AVOID SYSTEMS WHERE EVERYONE KNOWS EACH OTHER, DON'T TRY TO BLUFF. AND ABOVE ALL: NEVER ACT LIKE YOU OWN THE SYSTEM, OR ARE THE BEST THERE IS. THEY ALWAYS GRAB THE PEOPLE WHO'S HEADS SWELL...
THERE IS SOME VERY INTERESTING FRONT END EQUIPMENT AROUND NOWADAYS, BUT FIRST LET'S DEFINE TERMS...
BY FRONT END, WE MEAN ANY DEVICE THAT YOU MUST PASS THRU TO GET AT THE REAL COMPUTER. THERE ARE DEVICES THAT ARE MADE TO DEFEAT HACKER PROGRAMS, AND JUST PLAIN OLD MULTIPLEXERS.
TO DEFEAT HACKER PROGRAMS, THERE ARE NOW DEVICES THAT PICK UP THE PHONE AND JUST SIT THERE... THIS MEANS

THAT YOUR DEVICE GETS NO CARRIER, THUS
YOU THINK THERE ISN'T A COMPUTER ON
THE OTHER END. THE ONLY WAY AROUND IT
IS TO DETECT WHEN IT WAS PICKED UP. IF
IT PICKES UP AFTER THE SAME NUMBER
RING, THEN YOU KNOW IT IS A HACKER-
DEFEATER. THESE DEVICES TAKE A MULTI-
DIGIT CODE TO LET YOU INTO THE SYSTEM.
SOME ARE, IN FACT, QUITE SOPHISTICATED
TO THE POINT WHERE IT WILL ALSO LIMIT
THE USER NAME'S DOWN, SO ONLY ONE NAME
OR SET OF NAMES CAN BE VALID LOGINS
AFTER THEY INPUT THE CODE...
OTHER DEVICES INPUT A NUMBER CODE, AND
THEN THEY DIAL BACK A PRE-PROGRAMMED
NUMBER FOR THAT CODE. THESE SYSTEMS
ARE BEST TO LEAVE ALONE, BECAUSE THEY
KNOW SOMEONE IS PLAYING WITH THEIR
PHONE. YOU MAY THINK "BUT I'LL JUST
REPROGRAM THE DIAL-BACK." THINK
AGAIN, HOW STUPID THAT IS... THEN
THEY HAVE YOUR NUMBER, OR A TEST LOOP
IF YOU WERE JUST A LITTLE SMARTER.
IF IT'S YOUR NUMBER, THEY HAVE YOUR
BALLS (IF MALE...), IF ITS A LOOP,
THEN YOU ARE SCREWED AGAIN, SINCE THOSE
LOOPS ARE _MONITORED_.
AS FOR MULTIPLEXERS... WHAT A PLEXER
IS SUPPOSED TO DO IS THIS: THE SYSTEM
CAN ACCEPT MULTIPLE USERS. WE HAVE
TO TIME SHARE, SO WE'LL LET THE FRONT-
END PROCESSOR DO IT... WELL, THIS IS
WHAT A MULTIPLEXER DOES. USUALLY THEY
WILL ASK FOR SOMETHING LIKE "ENTER
CLASS" OR "LINE:". USUALLY IT IS
PROGRAMMED FOR A DOUBLE DIGIT NUMBER,
OR A FOUR TO FIVE LETTER WORD. THERE
ARE USUALLY A FEW SETS OF NUMBERS IT
ACCEPTS, BUT THOSE NUMBERS ALSO SET
YOUR 300/1200 BAUD DATA TYPE. THESE
MULTIPLEXERS ARE INCONVENIENT AT BEST,
SO NOT TO WORRY.
A LITTLE ABOUT THE HISTORY OF HACKING:
HACKING, BY OUR DEFINITION, MEANS A
GREAT KNOWLEDGE OF SOME SPECIAL AREA.
DOCTORS AND LAWYERS ARE HACKERS OF A
SORT, BY THIS DEFINITION. BUT MOST
OFTEN, IT IS BEING USED IN THE COMPUTER

CONTEXT, AND THUS WE HAVE A DEFINITION
OF "ANYONE WHO HAS A GREAT AMOUNT OF
COMPUTER OR TELECOMMUNICATIONS
KNOWLEDGE." YOU ARE NOT A HACKER
BECAUSE YOU HAVE A LIST OF CODES...
HACKING, BY OUR DEFINITION, HAS THEN
BEEN AROUND ONLY ABOUT 15 YEARS. IT
STARTED, WHERE ELSE BUT, MIT AND
COLLEGES WHERE THEY HAD COMPUTER
SCIENCE OR ELECTRICAL ENGINEERING
DEPARTMENTS. HACKERS HAVE CREATED
SOME OF THE BEST COMPUTER LANGUAGES,
THE MOST AWESOME OPERATING SYSTEMS, AND
EVEN GONE ON TO MAKE MILLIONS. HACKING
USED TO HAVE A GOOD NAME, WHEN WE COULD
HONESTLY SAY "WE KNOW WHAT WE ARE
DOING". NOW IT MEANS (IN THE PUBLIC
EYE): THE 414'S, RON AUSTIN, THE NASA
HACKERS, THE ARPANET HACKERS... ALL
THE PEOPLE WHO HAVE BEEN CAUGHT, HAVE
DONE DAMAGE, AND ARE NOW GOING TO HAVE
TO FACE FINES AND SENTANCES.
THUS WE COME PAST THE MORALISTIC CRAP,
AND TO OUR PURPOSE: EDUCATE THE HACKER
COMMUNITY, RETURN TO THE DAYS WHEN
PEOPLE ACTUALLY KNEW SOMETHING...

A PROGRAM GUIDE:
THREE MORE ARTICLES WILL BE WRITTEN IN
THIS SERIES, AT THE PRESENT TIME.
BASICS OF HACKING I: DEC'S
BASICS OF HACKING II: VAX'S (UNIX)
BASICS OF HACKING III: DATA GENERAL
IT IS IMPOSSIBLE TO WRITE AN ARTICLE
ON IBM, SINCE THERE ARE SO MANY SYSTEMS
AND WE ONLY HAVE INFO ON A FEW...

THIS ARTICLE HAS BEEN WRITTEN BY:
THE KNIGHTS OF SHADOW

THE BASICS OF HACKING II: VAX'S
UNIX

UNIX IS A TRADEMARK OF AT&T

(AND YOU KNOW WHAT _THAT_ MEANS)

Uploaded by Elric of Imrryr

WELCOME TO THE BASICS OF HACKING II: VAX'S AND UNIX. IN THIS ARTICLE, WE DISCUSS THE UNIX SYSTEM THAT RUNS ON THE VARIOUS VAX SYSTEMS. IF YOU ARE ON ANOTHER UNIX-TYPE SYSTEM, SOME COMMANDS MAY DIFFER, BUT SINCE IT IS LICENCED TO BELL, THEY CAN'T MAKE MANY CHANGES.

HACKING ONTO A UNIX SYSTEM IS VERY DIFFICULT, AND IN THIS CASE, WE ADVISE HAVING AN INSIDE SOURCE, IF POSSIBLE. THE REASON IT IS DIFFICULT TO HACK A VAX IS THIS: MANY VAX, AFTER YOU GET A CARRIER FROM THEM, RESPOND=>
LOGIN:
THEY GIVE YOU NO CHANCE TO SEE WHAT THE LOGIN NAME FORMAT IS. MOST COMMONLY USED ARE SINGLE WORDS, UNDER 8 DIGITS, USUALLY THE PERSON'S NAME. THERE IS A WAY AROUND THIS: MOST VAX HAVE AN ACCT. CALLED 'SUGGEST' FOR PEOPLE TO USE TO MAKE A SUGGESTION TO THE SYSTEM ROOT TERMINAL. THIS IS USUALLY WATCHED BY THE SYSTEM OPERATOR, BUT AT LATE HE IS PROBABLY AT HOME SLEEPING OR SCREWING SOMEONE'S BRAINS OUT. SO WE CAN WRITE A PROGRAM TO SEND AT THE VAX THIS TYPE OF A MESSAGE:
A SCREEN FREEZE (CNTRL-S), SCREEN CLEAR (SYSTEM DEPENDANT), ABOUT 255 GARBAGE CHARACTERS, AND THEN A COMMAND TO CREATE A LOGIN ACCT., AFTER WHICH YOU CLEAR THE SCREEN AGAIN, THEN UN-FREEZE THE TERMINAL. WHAT THIS DOES: WHEN THE TERMINAL IS FROZEN, IT KEEPS A BUFFER OF WHAT IS SENT. WELL, THE BUFFER IS ABOUT 127 CHARACTERS LONG. SO YOU OVERFLOW IT WITH TRASH, AND THEN YOU SEND A COMMAND LINE TO CREATE AN ACCT. (SYSTEM DEPENDANT). AFTER THIS YOU CLEAR THE BUFFER AND SCREEN AGAIN, THEN UNFREEZE THE TERMINAL. THIS IS

A BAD WAY TO DO IT, AND IT IS MUCH
NICER IF YOU JUST SEND A COMMAND TO
THE TERMINAL TO SHUT THE SYSTEM DOWN,
OR WHATEVER YOU ARE AFTER...
THERE IS ALWAYS, *ALWAYS* AN ACCT.
CALLED ROOT, THE MOST POWERFUL ACCT.
TO BE ON, SINCE IT HAS ALL OF THE
SYSTEM FILES ON IT. IF YOU HACK YOUR
WAY ONTO THIS ONE, THEN EVERYTHING IS
EASY FROM HERE ON...
ON THE UNIX SYSTEM, THE ABORT KEY IS
THE CNTRL-D KEY. WATCH HOW MANY TIMES
YOU HIT THIS, SINCE IT IS ALSO A WAY TO
LOG OFF THE SYSTEM!
A LITTLE ABOUT UNIX ARCHITECHTURE:
THE ROOT DIRECTORY, CALLED ROOT, IS
WHERE THE SYSTEM RESIDES. AFTER THIS
COME A FEW 'SUB' ROOT DIRECTORIES,
USUALLY TO GROUP THINGS (STATS HERE,
PRIV STUFF HERE, THE USER LOG HERE...).
UNDER THIS COMES THE SUPERUSER (THE
OPERATOR OF THE SYSTEM), AND THEN
FINALLY THE NORMAL USERS. IN THE UNIX
'SHELL' EVERYTHING IS TREATED THE SAME.
BY THIS WE MEAN: YOU CAN ACCESS A
PROGRAM THE SAME WAY YOU ACCESS A USER
DIRECTORY, AND SO ON. THE WAY THE UNIX
SYSTEM WAS WRITTEN, EVERYTHING, USERS
INCLUDED, ARE JUST PROGRAMS BELONGING
TO THE ROOT DIRECTORY. THOSE OF YOU
WHO HACKED ONTO THE ROOT, SMILE, SINCE
YOU CAN SCREW EVERYTHING...
THE MAIN LEVEL (EXEC LEVEL) PROMPT ON
THE UNIX SYSTEM IS THE $, AND IF YOU
ARE ON THE ROOT, YOU HAVE A # (SUPER-
USER PROMPT).
OK, A FEW BASICS FOR THE SYSTEM...
TO SEE WHERE YOU ARE, AND WHAT PATHS
ARE ACTIVE IN REGUARDS TO YOUR USER
ACCOUNT, THEN TYPE => PWD
THIS SHOWS YOUR ACCT. SEPERATED BY
A SLASH WITH ANOTHER PATHNAME (ACCT.),
POSSIBLY MANY TIMES.
TO CONNECT THROUGH TO ANOTHER PATH,
OR MANY PATHS, YOU WOULD TYPE:
YOU=> PATH1/PATH2/PATH3
AND THEN YOU ARE CONNECTED ALL THE
WAY FROM PATH1 TO PATH3. YOU CAN

RUN THE PROGRAMS ON ALL THE PATHS
YOU ARE CONNECTED TO. IF IT DOES
NOT ALLOW YOU TO CONNECT TO A PATH,
THEN YOU HAVE INSUFFICIENT PRIVS, OR
THE PATH IS CLOSED AND ARCHIVED ONTO
TAPE. YOU CAN RUN PROGRAMS THIS WAY
ALSO:
YOU=> PATH1/PATH2/PATH3/PROGRAM-NAME
UNIX TREATS EVERYTHING AS A PROGRAM,
AND THUS THERE A FEW COMMANDS TO
LEARN...
TO SEE WHAT YOU HAVE ACCESS TO IN THE
END PATH, TYPE=> LS
FOR LIST. THIS SHOW THE PROGRAMS
YOU CAN RUN. YOU CAN CONNECT TO
THE ROOT DIRECTORY AND RUN IT'S
PROGRAMS WITH=>
/ROOT
BY THE WAY, MOST UNIX SYSTEMS HAVE
THEIR LOG FILE ON THE ROOT, SO YOU
CAN SET UP A WATCH ON THE FILE, WAITING
FOR PEOPLE TO LOG IN AND SNATCH THEIR
PASSWORD AS IT PASSES THRU THE FILE.
TO CONNECT TO A DIRECTORY, USE THE
COMMAND: => CD PATHNAME
THIS ALLOWS YOU TO DO WHAT YOU WANT
WITH THAT DIRECTORY. YOU MAY BE ASKED
FOR A PASSWORD, BUT THIS IS A GOOD
WAY OF FINDING OTHER USER NAMES TO
HACK ONTO.
THE WILDCARD CHARACTER IN UNIX, IF
YOU WANT TO SEARCH DOWN A PATH FOR
A GAME OR SUCH, IS THE *.
=> LS /*
SHOULD SHOW YOU WHAT YOU CAN ACCESS.
THE FILE TYPES ARE THE SAME AS THEY
ARE ON A DEC, SO REFER TO THAT SECTION
WHEN EXAMINING FILE. TO SEE WHAT IS
IN A FILE, USE THE => PR FILENAME
COMMAND, FOR PRINT FILE.
WE ADVISE PLAYING WITH PATHNAMES TO
GET THE HANG OF THE CONCEPT. THERE
IS ON-LINE HELP AVAILABLE ON MOST
SYSTEMS WITH A 'HELP' OR A '?'.
WE ADVISE YOU LOOK THRU THE HELP
FILES AND PAY ATTENTION TO ANYTHING
THEY GIVE YOU ON PATHNAMES, OR THE
COMMANDS FOR THE SYSTEM.

YOU CAN, AS A USER, CREATE OR DESTROY
DIRECTORIES ON THE TREE BENEATH YOU.
THIS MEANS THAT ROOT CAN KILL EVERY-
THING BUT ROOT, AND YOU CAN KILL ANY
THAT ARE BELOW YOU. THESE ARE THE
=> MKDIR PATHNAME
=> RMDIR PATHNAME
COMMANDS.
ONCE AGAIN, YOU ARE NOT ALONE ON THE
SYSTEM... TYPE=> WHO
TO SEE WHAT OTHER USERS ARE LOGGED IN
TO THE SYSTEM AT THE TIME. IF YOU
WANT TO TALK TO THEM=> WRITE USERNAME
WILL ALLOW YOU TO CHAT AT THE SAME
TIME, WITHOUT HAVING TO WORRY ABOUT THE
PARSER. TO SEND MAIL TO A USER, SAY
=> MAIL
AND ENTER THE MAIL SUB-SYSTEM.
TO SEND A MESSAGE TO ALL THE USERS
ON THE SYSTEM, SAY => WALL
WHICH STANDS FOR 'WRITE ALL'
BY THE WAY, ON A FEW SYSTEMS, ALL YOU
HAVE TO DO IS HIT THE <RETURN> KEY
TO END THE MESSAGE, BUT ON OTHERS YOU
MUST HIT THE CNTRL-D KEY.
TO SEND A SINGLE MESSAGE TO A USER,
SAY => WRITE USERNAME
THIS IS VERY HANDY AGAIN! IF YOU SEND
THE SEQUENCE OF CHARACTERS DISCUSSED
AT THE VERY BEGINNING OF THIS ARTICLE,
YOU CAN HAVE THE SUPER-USER TERMINAL DO
TRICKS FOR YOU AGAIN.
PRIVS:
IF YOU WANT SUPER-USER PRIVS, YOU CAN
EITHER LOG IN AS ROOT, OR EDIT YOUR
ACCT. SO IT CAN SAY => SU
THIS NOW GIVES YOU THE # PROMPT, AND
ALLOWS YOU TO COMPLETELY BY-PASS THE
PROTECTION. THE WONDERFUL SECURITY
CONSCIOUS DEVELOPERS AT BELL MADE IT
VERY DIFFICULT TO DO MUCH WITHOUT
PRIVS, BUT ONCE YOU HAVE THEM, THERE
IS ABSOLUTELY NOTHING STOPPING YOU
FROM DOING ANYTHING YOU WANT TO.
TO BRING DOWN A UNIX SYSTEM:
=> CHDIR /BIN
=> RM *
THIS WIPES OUT THE PATHNAME BIN, WHERE

ALL THE SYSTEM MAINTENANCE FILES ARE.
OR TRY:
=> R -R
THIS RECURSIVELY REMOVES EVERYTHING
FROM THE SYSTEM EXCEPT THE REMOVE
COMMAND ITSELF.
OR TRY:
=> KILL -1,1
=> SYNC
THIS WIPES OUT THE SYSTEM DEVICES FROM
OPERATION.
WHEN YOU ARE FINALLY SICK AND TIRED
FROM HACKING ON THE VAX SYSTEMS, JUST
HIT YOUR CNTRL-D AND REPEAT KEY, AND
YOU WILL EVENTUALLY BE LOGGED OUT.

THE REASON THIS FILE SEEMS TO BE VERY
SKETCHY IS THE FACT THAT BELL HAS 7
LICENCED VERSIONS OF UNIX OUT IN THE
PUBLIC DOMAIN, AND THESE COMMANDS ARE
THOSE COMMON TO ALL OF THEM. WE
RECOMMEND YOU HACK ONTO THE ROOT OR
BIN DIRECTORY, SINCE THEY HAVE THE
HIGHEST LEVELS OF PRIVS, AND THERE
IS REALLY NOT MUCH YOU CAN DO (EXCEPT
DEVELOPE SOFTWARE) WITHOUT THEM.

THIS ARTICLE WRITTEN BY:
THE KNIGHTS OF SHADOW

Description: Hacking DEC's (Knights of Shadow II)
  File Date: 6-21-87
  File Time: 6:31 am

****
****
** **
** Hacking : DEC's **
** **
****
****

Welcome to Basics of Hacking I: DEC's In this article you will learn how to log in to DEC's, logging out, and all the fun stuff to do in-between.

All of this information is based on a standard DEC system. Since there are DEC systems 10 and 20, and we favor, the DEC 20, there will be more info on them in this article. It is also the more common of the two, and is used by much more interesting people (if you know what we mean...)
Ok, the first thing you want to do when you are receiving carrier from a DEC system is to find out the format of login names. You can do this by looking at who is on the system.

```
DEC=> @   (the 'exec' level prompt)
YOU=> SY
```

SY is short for SY(STAT) and shows you the system status. You should see |he format of login names... A SYSTAT usually comes up in this form:

```
Job  Line  Program  User
```

```
Job:     The JOB number (Not important unless you want to log them off later)
Line:    What line they are on (used to talk to them...)
         These are both two or three digit numbers.
Program: What program are they running under?  If it says 'EXEC' they aren't
         doing anything at all...
User:    ahhhAHHHH!  This is the user name they are logged in under...
```

Copy the format, and hack yourself out a working code...
Login format is as such:

```
DEC=> @
YOU=> login username password
```

Username is the username in the format you saw above in the SYSTAT. After you hit the space after your username, it will stop echoing characters back to your screen. This is the password you are typing in... Remember, people usually use their name, their dog's name, the name of a favorite character in a book, or something like this. A few clever people have it set to a key cluster (qwerty or asdfg). PW's can be from 1 to 8 characters long, anything after that is ignored.
   It would be nice to have a little help, wouldn't it? Just type a ? or the word HELP, and it will give you a whole list of topics...
Some handy characters for you to know would be the control keys, wouldn't it? Backspace on a DEC 20 is rub which is 255 on your ASCII chart. On the DEC 10 it is Ctrl-H. To abort a long listing or a program, Ctrl-C works fine. Use Ctrl-O to stop long output to the terminal. This is handy when playing a game, but you don't want to Ctrl-C out. Ctrl-T for the time. Ctrl-U will kill the whole line you are typing at the moment. You may accidently run a program where the only way out is a Ctrl-X, so keep that in reserve. Ctrl-S to stop listing, Ctrl-Q to continue on both systems. Is your terminal having trouble?? Like, it pauses for no reason, or it doesn't backspace right? This is because both systems support many terminals,

and you haven't told it what yours is yet... You are using a VT05 (Isn't
that funny? I thought i had an apple) so you need to tell it you are one.

```
DEC=> @
YOU=> information terminal
      or...
YOU=> info ter
```

This shows you what your terminal is set up as...

```
DEC=>  all sorts of shit, then the @
YOU=>  set ter vt05
```

This sets your terminal type to VT05. Now let's see what is in the account
(here after abbreviated acct.) that you have hacked onto...

```
SAY => DIR
```

short for directory, it shows you what the user of the code has save to the
disk. There should be a format like this: xxxxx.ooo   xxxxx is the file
name, from 1 to 20 characters long. ooo is the file type, one of:
exe, txt, dat, bas, cmd   and a few others that are system dependant.
Exe is a compiled program that can be run (just by typing its name at the @).
Txt is a text file, which you can see by typing=> type xxxxx.txt
Do not try to=> type xxxxx.exe This is very bad for your terminal and
will tell you absolutly nothing. Dat is data they have saved.
Bas is a basic program, you can have it typed out for you.
Cmd is a command type file, a little too complicated to go into here.

```
TRY => take xxxxx.cmd
```

By the way, there are other usersout there who may have files you can
use (Gee, why else am i here?).

```
TYPE => DIR <*.*>   (DEC 20)
     => DIR [*,*]   (DEC 10)
```
* is a wildcard, and will allow you

to access the files on other accounts if the user has it set for public
access. If it isn't set for public access, then you won't see it.
to run that program:

```
DEC=> @
YOU=> username program-name
```

Username is the directory you saw the file listed under, and file name was
what else but the file name?

** YOU ARE NOT ALONE **
Remember, you said (at the very start) SY short for SYSTAT, and how we said this showed the other users on the system? Well, you can talk to them, or at least send a message to anyone you see listed in a SYSTAT. You can do this by:

```
DEC=> the user list (from your systat)
YOU=> talk username     (DEC 20)
      send username     (DEC 10)
```

Talk allows you and them immediate conferencing.

Description: Hackign Data General (Knights of Shadow IV)
  File Date: 6-21-87
  File Time: 6:36 am

```
**************************************
**************************************
**                                  **
**       Hacking III: Data          **
**                    General       **
**                                  **
**************************************
**************************************
```

   Welcome to the basics of hacking III: Data General computers. Data General is favored by large corporations who need to have a lot of data on-line. The Data General AOS, which stands for Advance on of bastardized UNIX. All the commands which were in the UNIX article, will work on a Data General. Once again, we have the problem of not knowing the format for the login name on the Data General you want to hack. As seems to be standard, try names from one to 8 digits long. Data General designed the computer to be for businessmen, and is thus very simplistic, and basically fool proof (but not damn fool proof). It follows the same login format as the unix system:

```
DG=> login:
DG=> password:
YOU=> password
```

Passwords can be a maximum of 8 characters, and they are almost always set to a default of 'AOS' or 'DG'. (any you know about businessmen...)

A word about control characters:
Ctrl-O stops massive print-outs to the screen, but leaves you in whatever mode you were. (A technical word on what this actually does: It tells the CPU to ignore the terminal, and prints everything out to the CPU! This is about 19200 baud, and so it seems like it just cancels.) Ctrl-U kills the line you are typing at the time. Now for the weird one: Ctrl-C tells the CPU to stop, and wait for another ctrl character. To stop a program, you actually need to type Ctrl-C and then a Ctrl-B.

Once you get on, type 'HELP'. Many DG (Data General) computers are sold in a package deal, which also gets the company free customizing. So you never know what commands there might be. So we will follow what is known as the 'ECLIPSE STANDARD', or''ctory like. To find out the files on the directory you are using, type

```
=> DIR
```

To run a program, just like on a DEC, just type its name. Other than this, and running other people's programs, there really isn't a standard...

*** HARK, yon other system users ***

To see who is on, type => WHO remember?). This shows the other users, what they are doing, and what paths they are connected across. This is handy, so try a few of those paths yourself. To send a message, say

```
=> send username
```

This is a one time message, just like send on the DEC 10. From here on, try commands from the other previous files and from the 'HELP' listing.

superuser:
If you can get privs, just say:

```
=> superuser on
```

and you turn those privs on!
By the way, you remember that computers keep a log of what people do? type:

```
=> syslog /stop
```

and it no longer records anything you do on the system, or any of the other users. It screams to high heaven that it was you who turned it off, but it keeps no track of any accounts created or whatever else you may do. You can

say=> syslog /start

to turn it back on (now why would you want to do something like that?????)
To exit from the system, type=> BYE and the system will hang up on you.

   Most of the systems around, including DECs, VAX's, and DG's, have games. These are usually located in a path or directory of the name games or <games> or games: Try looking in them, and you might find adventure, zork, wumpus (with bent arrows in hand) or a multitude of others. There may also be games called 'CB' or 'FORUM'. These are a sort of computer conference call. Use them on weekends, and you can meet all sorts of interesting people.

   If you would like to see more articles on hacking (this time far more than just the basics), or maybe articles on networks and such, then leave us mail if we are on the system, or have the sysop search us down. We call a lot of places, and you may just find us.

****
****
This completes the series of articles on hacking...
The Basics of Hacking: Introduction
The Basics of Hacking I: DEC's
The Basics of Hacking II: VAX's (UNIX)
The Basics of Hacking III: DG's
****
****
This and the previous articles by:
The Knights of Shadow
****
****

Downloaded From P-80 International Information Systems 304-744-2253