Hacking

HACK AND PHREAK
=-=-=-=-=-=-=-=
FILE #3

BY: THE HYAENA

PLEASE BE CAREFUL WHO YOU GIVE THIS FILE TOO...

I'M NOW GOING TO DISCUSS HACKING VAX AND UNIX.

TO BEGIN WITH UNIX IS A TRADEMARK OF BELL LABS, AND THAT COULD MEAN TROUBLE FOR THOSE OF YOU WHO DON'T KNOW WHAT YOU ARE DOING. IF YOU ARE ON ANOTHER UNIX-TYPE SYSTEM, SOME OF THE COMMANDS MAY VARY, BUT SINCE IT IS LICENSED TO BELL, THERE CAN'T BE TOO MANY CHANGES. HACKING ONTO A UNIX SYSTEM IS VERY DIFFICULT, AND IT IS GOOD TO HAVE AN INSIDE SOURCE, IF POSSIBLE. IT'S VERY DIFFICULT TO HACK A VAX SINCE, AFTER YOU GET A CARRIER FROM A VAX, YOU SEE "login:" THEY GIVE YOU NO CHANCE TO SEE WHAT THE LOGIN FORMAT IS. ALTHOUGH, MOST COMMONLY THESE ARE SINGLE WORDS, UNDER 8 CHARACTERS, AND USUALLY THE USER'S NAME. THERE IS HOWEVER A WAY AROUND THIS. MOST VAX HAVE AN ACCOUNT CALLED "suggest" FOR PEOPLE TO USE TO MAKE A SUGGESTION TO THE SYSTEM ROOT TERMINAL. THIS IS USUALLY WATCHED BY THE SYSTEM OPERATOR, BUT LATE AT NIGHT, HE IS PROBABLY NOT AROUND. SO NOW WE CAN WRITE A PROGRAM TO SEND TO THE VAX, THIS TYPE OF MESSAGE; A SCREEN FREEZE (CTRL-S), SCREEN CLEAR (SYSTEM DEPENDANT), ABOUT 255 GARBAGE CHARACTERS, AND THEN A COMMAND TO CREATE A LOGIN ACCOUNT, AFTER WHICH YOU CLEAR THE SCREEN AGAIN, THEN UNFREEZE THE TERMINAL. WHAT THIS DOES IS THAT WHEN THE TERMINAL IS FROZEN, IT KEEPS A BUFFER OF WHAT IS SENT. THE BUFFER IS ABOUT 127 CHARACTERS LONG, SO YOU OVERFLOW IT WITH TRASH, AND THEN YOU SEND A COMMAND LINE TO CREATE AN ACCOUNT (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 AN ACCOUNT CALLED "root", WHICH IS THE MOST POWERFUL ACCOUNT TO BE ON, SINCE IT HAS ALL THE SYSTEM FILES ON IT. IF YOU HACK YOUR WAY ONTO THIS ONE, THEN EVERYTHING IS EASY FROM HERE ON. THE ABORT KEY ON THE UNIX SYSTEM IS CRTL-D. WATCH HOW MANY TIMES YOU HIT THIS, SINCE IT IS ALSO AWAY TO LOG OFF THE SYSTEM. SOME USEFUL THINGS TO KNOW ABOUT THE UNIX ARCHITECHTURE; THE ROOT DIRECTORY, CALLED "root", IS WHERE THE SYSTEM RESIDES. AFTER THIS COME A FEW 'SUB' ROOT DIRECTORIES, USUALLY TO GROUP THINGS, SUCH AS STATS, PRIVATE STUFF, THE USER LOG, ETC. HERE. NEXT COMES THE SUPERUSER (THE SYSTEM OPERATOR), AND THEN FINALLY THE NORMAL USERS. IN THE UNIX SHELL EVERYTHING IS TREATED THE SAME. WHAT I MEAN BY THIS IS THAT YOU CAN ACCESS A PROGRAM THE SAME WAY AS YOU ACCESS A USER DIRECTORY, AND SO ON. THE WAY THAT THE UNIX SYSTEM WAS WRITTEN, IS THAT EVERYTHING, EVEN THE USERS, ARE JUST PROGRAMS BELONGING TO THE ROOT DIRECTORY. THOSE OF US THAT CAN HACK ONTO THE ROOT SMILE, SINCE YOU CAN SCREW EVERYTHING UP. THE MAIN LEVEL (OR EXEC LEVEL) PROMPT ON THE UNIX SYSTEM IS THE $, AND IF YOU AREON THE ROOT, YOU HAVE A # (SUPER-USER) PROMPT. NOW AS FOR A FEW BASICS OF THE SYSTEM; TO SEE WHERE YOU

ARE AND WHAT PATHS ARE ACTIVE IN REGUARDS TO YOUR USER ACCOUNT, TYPE "PWD". THIS SHOWS YOUR ACCOUNT, SPERATED BY A SLASH WITH ANOTHER PATHNAME (ACCOUNT), POSSIBLE MANY TIMES. TO CONNECT THROUGH TO ANOTHER PATH, OR MANY PATHS, YOU WOULD TYPE "path1/path2/path3" AND THEN YOU ARE CONNECTED ALL THE WAY FROM PATH 1 TO PATH 3. YOU CAN RUN THE PROGRAMS ON ALL THE PATHES THAT YOU ARE CONNECTED TO. IF IT DOES NOT ALLOW YOU TO CONNECT TO A PATH, THEN YOU HAVE INSUFFICIENT PRIVILEGES, OR THE PATH IS CLOSED AND STORED ON TAPE. YOU CAN ALSO RUN PROGRAMS BY TYPING "path1/path2/path3/program-name". SINCE UNIX DOES TREAT EVERYTHING AS A PROGRAM, THERE ARE A FEW COMMAND THAT YOU MAY HAVE TO LEARN. TO SEE WHAT YOU HAVE ACCESS TO, YOU TYPE "ls" FOR LIST, THIS SHOWS THE PROGRAMS THAT YOU CAN RUN. YOU CAN CONNECT TO THE ROOT DIRECTORY AND RUN ITS PROGRAMS BY TYPING "/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 YOU GET THEIR PASSWORD AS IT PASSES THROUGH THE FILE. TO CONNECT TO A DIRECTORY USE THE COMMAND "cd pathname". THIS ALLOWS YOU TO DO WHAT YOU WANT WITH THE DIRECTORY. YOU MAY BE ASKED FOR A PASSWORD, BUT THIS IS A GOOD WAY OF FINDING OTHER USERS NAMES TO HACK ONTO. THE WILDCARD CHARACTER IN UNIX, IF YOU WANT TO SEARCH DOWN A PATH FOR A CERTAIN GAME OR PROGRAM, IS THE * SYMBOL. "ls /*" SHOULD SHOW YOU WHAT YOU CAN ACCESS. THE FILE TYPES ARE THE SAME AS ON A DEC. TO SEE WHAT IS IN A FILE TYPE "pr filename", STANDING FOR PRINT FILE. IT'S A GOOD IDEA TO PLAY AROUND WITH THE PATHNAMES SO THAT YOU GET THE HANG OF IT. THERE IS ALSO ON-LINE HELP AVAILABLE BY TYPE "help" OR HITTING ?. IT'S A GOOD IDEA TO LOOK THROUGH ALL THE HELP FILES, SINCE IT MAY GIVE YOU SOME INFO ON PATHNAMES AND THE COMMANDS USED ON THE SYSTEM. AS A USER, YOU CAN CREATE OR DESTROY DIRECTORIES ON THE TREE BENEATH YOU. THIS MEANS THAT ROOT CAN KILL EVERYTHING BUT ROOT, AND YOU CAN KILL EVERYTHING THAT IS BELOW YOU. "mkdir pathname" IF FOR MAKING A DIRECTORY AND "rmdir pathname" IS FOR KILLING A PATHNAME. REMEMBER THAT YOU ARE NOT ALONE ON THE SYSTEM. TYPE "who" TO SEE WHO THE OTHER USERS ARE THAT ARE PRESENTLY LOGGED ONTO THE SYSTEM. IF YOU WANT TO TALK TO THEM TYPE "write username" AND THIS WILL ALLOW YOU TO CHAT. IF YOU WANT TO SEND MAIL TO ANOTHER USER TYPE "mail" AND THIS WILL PUT YOU INTO THE MAIL SUB-SYSTEM. TO SEND MAIL TO ALL OF THE USERS ON THE SYSTEM TYPE "wall" WHICH STANDS FOR WRITE ALL. ON SOME SYSTEMS ALL YOU HAVE TO DO IS HIT THE RETURN KEY TO END THE MESSAGE, WHERE AS ON OTHERS YOU WILL HAVE TO HIT CTRL-D. TO SEND A MESSAGE TO A SINGLE USER TYPE "write username". IF YOU SEND THE SEQUENCE OF CHARACTERS THAT I DISCUSSED AT THE BEGINNING, YOU CAN HAVE THE SUPER-USER TERMINAL DO TRICKS FOR YOU. IF YOU WANT SUPER-USER PRIVELEGES, YOU CAN EITHER LOG IN AS ROOT, OR EDIT YOUR ACCOUNT. IF YOU TYPE "su" THIS WILL GIVE YOU THE # PROMPT, AND THIS WILL ALLOW YOU TO COMPLETELY BY-PASS THE PROTECTION. THE WONDERFUL SECURITY CONSCIOUS DEVELOPERS AT BELL MADE IT VERY DIFFICULT TO DO ANYTHING WITHOUT PRIVELEGES, BUT ONCE YOU HAVE THE PRIVELEGES, THERE IS ABSOLUTELY NOTHING THAT CAN STOP YOU FROM DOING ANYTHING THAT YOU WANT. TO DOWN A UNIX SYSTEM TYPE "chdir /bin" THEN "rm *" AND THIS WILL WIPE OUT THE PATHNAME BIN, WHERE ALL THE SYSTEM MAINTENANCE FILES ARE. OR TRY TYPING "r -r" WHICH WILL RECURSIVELY REMOVER EVERYTHING FROM THE SYSTEM EXCEPT THE REMOVE COMMAND. OR YOU CAN ALSO TRY "kill -1,1" THEN "sync" AND THIS WILL WIPE OUT THE SYSTEM DEVICES FROM OPERATION. NOW WHEN YOU GET BORED OF HACKING AT THE VAX SYSTEM, JUST KEEP

HITTING CTRL-D AND EVENTUALLY YOU WILL BE LOGGED OUT. SINCE BELL HAS 7 LICENSED VERSIONS OF UNIX OUT, I HAVE DESCRIBED THE COMMANDS THAT ARE COMMON TO ALL OF THEM. LASTLY, I RECOMMEND THAT YOU HACK ONTO THE ROOT OR BIN DIRECTORY, SINCE THEY HAVE THE HIGHEST LEVELS OF PRIVELEGES, AND BESIDES THERE IS NOT MUCH THAT YOU CAN DO WITHOUT THEM.

NOW HERE'S A NICE LITTLE THING YOU CAN DO TO MAKE A 3-WAY PHONE, IE. TALK TO TWO OTHER PEOPLE AT THE SAME TIME, KIND-OF LIKE CONFERENCE CALLING I GUESS.

FIRSTLY, YOU WILL NEED 2 DIFFERENT TELEPHONE LINES IN YOUR HOUSE. NOW TAKE OFF BOTH OF THE BOXES THAT COVER THE WIRES.
NEXT, TAKE THE GREEN AND RED WIRES FROM EACH BOX AND ATTACH A WIRE TO EACH OF THESE. 1 WIRE TO GREEN AND 1 WIRE TO RED. DO THE SAME FOR THE OTHER BOX.
FINALLY, AFTER YOU HAVE 4 WIRES, 2 FROM EACH BOX, YOU HAVE TO GET A 2 WAY SWITCH WITH 2 TERMINALS, AND THEN HOOK UP THE 2 GREEN WIRES TO ONE SIDE AND THE 2 RED WIRES TO THE OTHER SIDE. NOW WHEN YOU SWITCH THE SWITCH, YOU SHOULD HERE A DIAL TONE AND THEN YOU CAN DIAL OUT AND YOU WILL BE ABLE TO TALK TO 2 PEOPLE AT THE SAME TIME.

OK HERE'S SOMETHING THAT MOST OF YOU NEVER HEARD OF. I'LL DISCUSS SOME THINGS THAT I KNOW ABOUT STEP LINES AND SOME INTERESTING THINGS THAT CAN BE DONE.

FIRST, FIND OUT IF YOU HAVE STEP LINES IN YOUR PREFIX. A GOOD WAY OF DOING THIS IS TO GO TO THE PAY PHONES AROUND YOUR HOME, AND IF THEY ARE ROTARY, THEN YOU ARE IN LUCK, SINCE YOU HAVE STEP LINES. I USED TO HAVE STEP LINES IN MY AREA, BUT UNFORTUNATELY NOT ANYMORE. WELL, ANYWAYS FOR THOSE OF YOU WITH STEP LINES, DIAL '0' FROM YOUR HOME, THIS WILL NOT WORK ON PAY PHONES. YOU WILL THEN HEAR A FEW SOUNDS LIKE COIN DROPPINGS. NOW IF YOU HIT THE HANG UP BUTTON WHEN THE SECOND LAST COIN DROP IS HEARD, THEN THE OPERATOR WILL GET ON AND BE VERY CONFUSED. I'LL TELL YOU WHY SHE IS CONFUSED LATER ON, BUT NOW SAY THAT YOU ARE TRYING TO COMPLETE A CALL WHEN SHE GOT ON. SHE WILL ASK YOU FOR THE NUMBER THAT YOU ARE TRYING TO CALL. TELL HER THE NUMBER, LONG DISTANCE OF COURSE, AND THEN SHE WILL ASK YOU FOR YOUR NUMBER. SO JUST PICK A NUMBER OUT OF YOUR HEAD, IT MUST BE IN YOUR PREFIX, AND TELL IT TO HER. NOW SHE WILL BELIEVE YOU AND CONNECT YOU TO YOUR DESIRED NUMBER, WITH THE CHARGES GOING TO THE FAKE NUMBER THAT YOU GAVE. NOW IF YOU DIDN'T HIT THE HANG UP BUTTON AT THE RIGHT TIME, JUST TELL THE OPERATOR THAT YOU ARE SORRY AND GIVE SOME BULLSHIT EXCUSE AND TRY AGAIN.
WHAT YOU DID, WAS SCREW UP THE AUTOMATIC NUMBER FIND THAT WAS BUILT INTO THE FIRST STEP LINES. THIS IS WHAT WOULD TELL THE OPERATOR YOUR NUMBER, SO THAT SHE COULD BILL YOU IF SHE HAD TO COMPLETE A CALL FOR YOU. THE OPERATOR WILL GET SOME GARBAGE ON HER SCREEN THAT IS SUPPOSED TO BE YOUR NUMBER, BUT SINCE YOU INTERUPTED THAT PROCESS, IT LOOKS REALLY STRANGE.
SOMETHING THAT IS REALLY FUN TO DO IS TO COMPLAIN TO THE OPERATOR THAT THIS IS THE FOURTH TIME TODAY THAT YOU HAVE NOT BEEN ABLE TO GET THROUGH AN SHE WILL GIVE YOU SOME STORY LIKE, "WE'RE SORRY BUT WE'VE HAD A COMPUTER MALFUNCTION AND IT'S BEING FIXED RIGHT NOW."
I DON'T KNOW IF THE PHONE COMPANY KNOWS ABOUT THIS, BUT DON'T WORRY, THE WORST

THAT COULD HAPPEN IS THAT YOU WOULD GET A CALL FROM THE OPERATOR, ASKING WHY YOU HAVE HUNG UP ON THE OPERATOR SO MANY TIMES. JUST GIVE HERE SOME EXCUSE LIKE YOU ARE TEACHING YOUR KID SISTER TO USE THE PHONE, OR SOMETHING LIKE THAT.

END OF FILE #3...

[Time Left 00:39] 1. the_NeoPsychedelic_UnderGround_ Computer Philes:
Command ? MEMBER THAT YOU ARE NOT ALONE ON THE SYSTEM. TYPE
"who" TO SEE WHO THE OTHER USERS AR