

ASPEN1.TXT

[R.A.W Productions]
[01.13.92]

[A Complete Guide To Hacking and Use of ASpEN Voice Mail Systems]
[Written by: Caveman]

[Introduction]

ASpEN, or "Automated Speech Exchange Network," is a voice mail system used by small businesses for individual employees' when away from their desks. It is, in my opinion, by far the easiest system to use. There are other vms's to hack on, but many can be difficult, including systems that require a "box/password" number to be entered (which any stupid shit knows is as difficult as a GOOD meal with spam in it; close to impossible of course.)

I will be discussing the basics and commands of the ASpEN systems, If you need information on voice mail systems in general, or info on another specific type of voice mail system, I highly suggest the LoL article on hacking voice mail boxes, as well as the article on hacking voice mail boxes by Night Ranger in Phrack #34, both are good sources of information.

[Finding An ASpEN System]

In order to find an ASpEN system, you will need to get some form of wardialer. I've heard a lot of shit about what's the best, I don't give a fuck, they all do the same damn thing. The easiest way to find a voice mail system is set up a wardialer, connect a spare phone to the second phone slot on your modem, and set up the wardialer to an exchange that is known to carry voice mail systems (i.e. 1-800-666-XXXX) After a shitload of ringings, stanky operators, and fax machine ringings, you will come across something that sounds like an answering machine. If you are extremely lucky, you will come across the generic message that comes with the ASpEN system. You will hear:

"Hello, this is ASpEN, the Automated Speech Exchange Network. Please enter the number of the person you are calling. If you have a mailbox on this system, please press pound."

Otherwise you will get a recording from the company itself, in which case you need to press the star key to enter the voice messaging system. If you get a message saying, "Mailbox number please" you have found a voice mail system. It is not necessarily an ASpEN system, it could be one of a number of systems. In order to know absolutely that the system you have found is ASpEN, you will need to recognize the ASpEN computer voice. If you need a sample of the voice, call 1-800-852-MAIL and press pound (#). You will get a sample of the ASpEN voice from this system. After determining that you have indeed found an ASpEN system, you are ready to go to work. You have already done the hardest part,

finding an ASpEN system.

[The 800 Exchange Problem]

1-800 voice mail systems are by far the most useful, for obvious reason of low cost calling from around the country, so that phreaks and hackers from coast-to-coast are able to contact you. However, there has been a problem with attempting to hack an 800 exchange. It is the simple fact the each time you call the 800 system, the system itself gets billed for the call. Even if you are lucky enough to find a local 800 voice mail system, the system will still be billed for the call. If you are calling a long distance 800 exchange, the system will be billed for the LONG DISTANCE bill. Thus, if you call the system many times in search of a box, then the System Administrator will be notified of irregular patterns in the bill at the end of the month, including multiple long distance calls from the same source in a short period of time. The System Administrator, if competent, will check the system for hackers, and will eventually find your box. The risk of the System Administrator sighting the irregular phone bill, or practicing "Preventive Maintenance Exercises," all depends on the size of the system, the size of the company paying for its use, as well as if the system regularly receives many long distance calls.

[3-Digit Error]

The reason that ASpEN is the easiest is some "errors" in the programming of the automated system. Among the most useful is the 3-digit error. If you enter three numbers SLOWLY, such as 1-5-2, taking your time with each number you enter, then at the end of the THIRD number, the ASpEN computer-generated voice will tell you:

"Box 1-5-2 is not a recognized mailbox, please try again. Please re-enter your mailbox number."

By not allowing the user to enter the fourth number, the ASpEN system has, in effect, told you that there are NO mailboxes in the 152 exchange, in other words, no 1520, 1521, 1522, 1523, etc... up to 1529. Instead of having to check all ten of these boxes, you only need enter the first three numbers slowly and wait for the system to tell you that they are invalid. If the 1-5-2 exchange is invalid, then try the next exchange, 1-5-3. However, if you enter 1-5-2 and the system pauses and waits for another number, then BINGO, orgasm, you have found a valid exchange, meaning that there is a valid mailbox between 1520 and 1529. In the pause between the 1-5-2 you entered and the computer voice not coming on, you then enter another number between 1-9. If you get the invalid box voice again, try another number between 1-9, if the system paused with this exchange, there is definately a box there. It may take you a while to find an exchange that the system will pause on, but I suggest looking in the range of 2400-6000, this is where I personally had the most success. Once you have found a mailbox, don't spooge in your pants yet,

ASPEN1.TXT

you must begin the next step, finding a box not in use.

[Finding YOUR Box]

First, I will stress NEVER FUCKING TAKE A BOX THAT IS ALREADY IN USE BY SOMEONE. I can tell you, all that this accomplishes is that you get a VMB and you feel good for a couple of days, but as soon as the owner checks their box, but finds that some little shit took it over, they will report directly to the System Administrator, who will make a complete system check, and destroy any other box that WASN'T originally in use, that some hacker obtained through hard work. By finding a box that isn't already in use, you are insuring that other hackers on the system will not be caught, as well as guaranteeing the safety of your own box. So how DO you find a box not in use on an ASpEN system? Any box that is not in use is NOT going to have a recorded name (a feature discussed later in the text.) While trying to find a box in the 3-digit method described above, you will enter a box number and come up with the normal ASpEN voice stating the following:

"Hello. This system can enable you to receive messages while you are away from your desk... [After a lot more shit, the voice will say] Your System Administrator has assigned you a temporary password. Please enter that password now."

When you have come upon this generic message, you have found an activated mailbox that is not in use, but rather reserved for a future user of the system. NOW HOW CAN I PUT THIS KNOWLEDGE TO WORK FOR ME? At this time, you begin to try the defaults for the ASpEN systems as named in Night Ranger's article in Phrack #34. The defaults that I have had the most success with is 1111, the box number itself, and 1234. But before you give up, expend ALL of the defaults.

[Once In The Box]

Once you have entered the correct default password for the box that of course was NOT IN USE, the computer voice will say:

"Thank you. You should now change the default password. Make it a number that will be easy for you to remember but hard for others to guess..."

At this point, the ASpEN will also ask you to change your recorded name and recorded message (discussed later, and I'm sure, really difficult to figure out.) Now, you have complete control of the mailbox. Once you have a mailbox, post the number on your local board, so that others may share in your joy, and posting the default is helpful as well as the number range of the boxes.

[Commands]

ASPEN1.TXT

When in your box, there will be a number of commands available to you. Once you are in your mailbox, the mailbox will tell you "No messages. Send, press two, check receipts press three.) The option that it does not tell you on some systems (the most important option) is "Personal Options," which menu you can enter by pressing 4 on your numeric telephone pad. The following is an outline of the options available from each menu that can be entered on the ASpEN system (all quoted options are taken from the "rapid prompts;" which is what I suggest you set your prompt level to when taking over the box):

[MAIN MENU]

"Send, press 2" - to send a message from YOUR mailbox to a fellow hacker on the system. It will record your message, then ask which box to send the message to. You can enter multiple box numbers, which serves as a multi-mail service.

"Check receipts, press 3" - Once you have sent a message, and want to check whether the person has received the message, or if the message you have sent is still in their mailbox, you use this option. It will ask which box to check, once you have entered this, it will play their recorded name, and say either "One message from you in that mailbox" and play the message over to you, or say "All messages have been received."

"Personal options, press 4" - This is basically command central of your box, a number of options are contained (see PERSONAL OPTIONS SUBMENU)

"Restart, press 5" - This will bring you to the original logon message of your particular voice messaging system.

"Disconnect, press *" - If you cannot figure this out, you do not need a box.

[PERSONAL OPTIONS SUBMENU]

"Notification on or off, press 1" - This is an option that you NEVER WANT TO ACTIVATE. This is an option that will call your house whenever you receive an "urgent" message. Of course, if you activate this, and give your home phone number, then if the System Administrator is not a shit-for-brains (as many of them are) they will be able to contact you at your home and cause you more trouble than this option is worth.

"Administrative options, press 2" - This is another submenu (see ADMINISTRATIVE OPTIONS SUBMENU) that contains the maintenance options.

ASPEN1.TXT

"Greetings, press 3" - This contains another submenu full of options for your greetings. (see GREETINGS SUBMENU)

"Notification schedule" - This is the option to set the time that the system should call your house with "urgent" messages. As I said before, you've got to be fucked up to activate this, it's a deathwish.

[ADMINISTRATIVE OPTIONS SUBMENU]

"Passwords, press 1" - Simply the passwords of your system. (see PASSWORDS SUBMENU)

"Prompt level, press 3" - The level of explanation the ASpEN system gives you when reciting your options. Prompt level 1 is set for morons, level 2 is for a user just getting used to the commands of the ASpEN system, and level 3 is rapid prompts, the briefest ASpEN messages the system allows.

"Date and time options, press 4" - This allows you to enable or disable the date and time option, which stamps each incoming message with the date and time of receipt.

"To exit, press *" - Whenever you are in a submenu, and want to exit to the menu you were in prior to the submenu, press the star key. You will be transferred to the previous menu, or if you are in the main menu, you will disconnect.

[GREETINGS SUBMENU]

"Personal greeting, press 1" - Your personal greeting is what the caller will hear when calling your box.

"Extended absence greeting, press 2" - This is used by companies when their employees take vacations, and there is no need for them to receive messages. With this option on, you will not be able to receive messages until the extended absence greeting is deleted. This is useful when you are switching mailboxes, and want to convey to the caller your new system and box number, and make it impossible for the caller to leave a message.

"Recorded name, press 3" - This is the name that will be played when you call your box to check your messages. Upon calling your box, the ASpEN system will say: "Hello, [recorded name played,]"

ASPEN1.TXT
please enter your password."

[PASSWORD SUBMENU]

"Guest 1 password, press 1" - This is the password for a friend that you can leave messages to. This friend will have his own password, as well as message section, but will not have access to your messages, or personal options.

"Guest 2 password, press 2" - This is the same as guest 1, but for another friend (if you have that many friends.)

"Home password, press 3" - This password enables the user to access private messages, and send messages, and disconnect. No other options are available to the user with this password.

"Secretary password, press 4" - This is of course for your secretary. The user of this password will have access only to hear message summaries, in other words, they will hear who the message is from, what time and date it was sent, and how long it is, but not the message itself. This was obviously designed with the thought that the secretary can use this to notify her boss that messages are waiting in his mailbox.

"Your personal password, press 5" - This is the master password, the password that gives you access to ALL options of the box. You will be using this one, so change it from the default.

[Avoiding Deletion]

On all of the systems that I have been on, I have found that the System Administrators only check for hackers on the first of the month, every month. Some stupid System Administrators, such as the one in charge of the system I am on right now, will send a multi-mail to ALL users of the system, stating that they plan on shutting down the system for an hour on the first of the month for what they call "Preventive Maintenance Excercises." This means that the System Administrator on your ASpEN system will be checking all boxes for validity. Some systems will check at the first of the month WITHOUT sending such a helpful message. My suggestion is to change your recorded name as well as your message to say something like: "Hello, this is Joe Blow, I'm not in the office at the present time, if you leave me a message, I will get back to you as soon as possible. Thank you." Don't sound too fluent either, most users have no idea what the fuck they are doing. After the first of the month change your message back to normal, and you should be set until the next month.

ASPEN1.TXT

[Disclaimer]

I could say that I don't want anyone to do anything contained in this file, and that it is strictly for informational purposes, but I know that people are going to go out and do this shit. So, Mr. Law Enforcement Agent, cram it, you can't find me, for all you know, I could be your father (and knowing your mother, I probably am.) AMF.

[Bullshit]

If you have suggestions, comments, or have nothing better to do, you can reach me (Caveman) at [Legion 1]: 202.337.2844 [12/24/96/14.4]

[PEACE]

Peace to Mr. Black, my partner in crime.
Peace to Tomellicas, Legion creator.
Peace to G-Spot, for finding the systems to hack on.
Peace to Night Ranger, for his article.

[The Boards]

Legion 1 [202]
Powerdome, INC. [703]
Midian Private [703]
School For Scandal [301]

Copyright 1992 R.A.W Productions. All Rights Reserved.
{PEACE OUT}

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