

ARPA2.TXT

Hacking ARPAnet -- Part II

by

The SOURCE

of

-=>*The Listening Post*<=-

408-923-7575

LEARNING WHO's WHO

As mentioned earlier, ARPANET can be made to disclose a great deal of information before you have logged on or even hacked a password. Among the most useful commands are those that tell you who else is on the system and what the status of the system is. These files give you information that will help your future hacking activities. In this section we discuss commands that disclose data about users that are available from the EXEC level.

@HELP WHOIS <user entry>

NICNAME (alias WHOIS) is a utility for cross-net access of the NIC user registration database. NICNAME has been chosen as the global name for the program, although many sites will choose to use the more familiar WHOIS name for the program.

For the convenience of sites without user programs to interact with the NICNAME server, WHOIS may be run on the SRI-NIC machine via Telnet service without logging in. The documentation below is slightly inaccurate in this case, since there is no need to reach further through the net to access the database, as the user program and the database are both on SRI-NIC.

The initial procedure is a one-reach, one-response query, which allows users at any Internet site to obtain information about an organization or individual by providing either a name or an IDENT. The protocol used is a TCP protocol. A server program running at SRI-NIC takes the user's request, accesses the NIC database and sends back the reply.

The reply can be in one of three forms:

- 1) Record for individual or organization found, information (including

ARPA2.TXT

name, ident, organization, mailing address and network address) is returned to user.

- 2) Given name matches more than one record. A short entry is returned for each matching record and the user is told to re-query the system using the ident to match any one individual or organization shown.
- 3) No record matched. If an ident was given, this response means that the ident is free for use by an individual or organization, and can be obtained for such by contacting NIC.

Examples of use follow. For clarity, the user's typing appears in uppercase:

I. Request for help information.

@WHOIS

Ident: ?

; Accessing NICNAME server at SRI-NIC...

Please enter a name or a handle ("ident"), such as "Smith" or "SRI-NIC". Starting with a period forces a name-only search; starting with exclamation point forces handle-only. Examples:

Smith [looks for name or handle SMITH]

!SRI-NIC [looks for handle SRI-NIC only]

.Smith, John [looks for name JOHN SMITH only]

Adding "... " to the argument will match anything from that point, e.g.

"ZU..." will match ZUL, ZUM, etc.

To search for all the authorized users of a host, use:

%HOST

To search for mailboxes, use one of these forms:

Smith@ [looks for mailboxes with username SMITH]

@Host [looks for mailboxes on HOST]

Smith@Host [Looks for mailboxes with username SMITH on HOST]

To have the ENTIRE membership list of a group or organization, if you are asking about a group or org, shown with the record, use an asterisk character "*" directly preceding the given argument. [CAUTION: If there are a lot of members this will take a long time!]

You may of course use exclamation point and asterisk, or a period and asterisk together.

II. Search by name only.

@WHOIS .GRAY

; Accessing NICNAME server at SRI-NIC...

There are 9 matching entries.

Gray, Beth (BG10)	BGRAY@UDEL-RELAY	(202) 274-9446 (AV) 284-9446
Gray, Bobby R. (BRG)	BRGray@RADC-MULTICS	(315) 330-4846 (AV) 587-4846
Gray, Bruce (BG17)	DRSEL-TCS-MCF@OFFICE-7	(201) 544-3671 (AV) 995-3671

ARPA2.TXT

Gray, Charles W. (CWG1) CWGray@RADC-MULTICS (315) 330-2116 (AV) 587-2116
Gray, Gilbert R. (GRG2) gray@NEMS (202) 227-1270 (AV) 287-1270
Gray, Neil (NG1) GRAY@SUMEX-AIM (415) 497-1712
Gray, Purnell (PG5) DRSTS-DS@OFFICE-1 (314) 263-3397 (AV) 693-3397
Gray, Randy K. (RKG) DRSEL-CP-RA@OFFICE-7 (201) 544-4733
Gray, Richard M. (RMG) WESTDIV@USC-ISI (707) 646-3514

To single out any one of these, repeat the command, using "IDENT" or "!IDENT" instead of "NAME" (e.g., "vw" or "!vw" instead of "white").

III. Search by name or ident specifying an ident.

@WHOIS VW

Accessing NICNAME server at SRI-NIC...

White, Victor A. (VW) VIC@SRI-KL
SRI International
Network Information Center
Telecommunications Sciences Center
333 Ravenswood Avenue
Menlo Park, California 94025
Phone: (415) 859-5303

Send additions or changes to NIC@SRI-NIC

IV. Search by name or handle specifying a name with an ellipsis.

@WHOIS STEPH...

Squires, Stephen L. (STEPH) SQUIRES@USC-ISI (202) 694-5917
Stephany, Michael (MS30) USARCCO@STL-HOST1 (620) 538-8285 (AV) 879-8285 (FTS)
769-8285
Stephen-Smith, Kay (SS2) STEPHENSMITH@SRI-KL (01) 681-1751
Stephens, Donald L. (DLS2) LAOFTHOOD@STL-HOST1 (AV) 737-6608 or 737-3103
Stephens, Eugene F. (EFS1) LAOFTPOLK@STL-HOST1 (AV) 863-4876 or 863-4888
Stephens, Nadine Y. (NYS) DSDC-SGY@GUNTER-ADAM (205) 279-4901

V. Search for mailboxes.

@WHOIS MIKE@

Muuss, Michael John (MJM2) MIKE@BRL (301) 278-6678 or 278-6239 (FTS) 939-66
78 or 939-6239
Wahrman, Mike (MW19) mike@CCA-UNIX (703) 522-1717
Liveright, Mike (ML1) MIKE@KESTREL (415) 494-2233
Wahrman, Michael L. (MLW) mike@RAND-UNIX (213) 393-0411
Stonebraker, Michael R. (MRS) mike@UCB-VAX (415) 642-5799 or 642-3068

ARPA2.TXT

@WHOIS GPARK@DDN1

Parker, Glynn (GP) gpark@DDN1
Defense Communications Agency
Code B627
Washington, D.C. 20305
Phone: (703) 285-5133
MILNET TAC user

@WHOIS @MIT-ML

Ressler, Andrew L. (ALR) ALR@MIT-ML (617) 253-3504
Kuipers, Benjamin (BK2) BEN@MIT-ML (617) 628-5000 ext 6650
Davies, Byron (BD5) BYRON@MIT-ML (617) 253-3507

.
.
(items omitted here for brevity)
<the job autologs itself out and the monitor is ready for the next command>

FINGER YOURSELF?

Let's try the command:

@FINGER

User	Personal name	Job	Subsys	Idle	TTY	Console	location
???		34	FINGER		.106	Internet:	SU-TAC#13
DOMAIN	Domain Server	28	DSV	*:**	102	Job 0,	OPERATOR, SYSJOB
FEINLER	Jake Feinler	31	:BASE		30	EJ200	Jake Feinler x6287
HENRY	Henry Chen	41	EXEC	.		Detached	
KLH	Ken Harrenstien	26	EMACS	1	17	TSC MICOM 30	[P235]
X-MAN	Jeff Thompson	27	EXEC	12.	3	EK205 Operator	Fishbowl x4664
		35	EMACS		14	TSC MICOM 30	[P232]

@HELP SYSTAT

The SYSTAT command lists information about jobs logged into the system in order of job number, along with the date and time, how long the system has been up, the number of jobs logged in, and load average information.

If the user is logged in from another host, the name of that host is given under the Foreign host heading.

For example:

@systat

Tue 14-Aug-84 15:29:38 Up 45:40:40
20+13 Jobs Load av 1.70 1.33 1.43
Job Line Program User Foreign host
13 102 DSV DOMAIN

ARPA2.TXT

```

14    40 EXEC    NAN
15    16 VOID    KLH
16    DET EXEC    HENRY
17   106 FTPSRT  ANONYMOUS      (SRI-KL)
18    54 TYPE    OLE
19     3 EXEC    SAPPHO
20*   51 SYSTAT  STACIA
22    11 EXEC    SAPPHO
25    60 MM      OLE

```

There are a number of arguments which can be given to the SYSTAT command. These can be listed by typing SYSTAT ?. These arguments include:

```

.    All    Charge    Class    Controlling
Directory    Header    In-Class    Limit    Line
Lpt    No    Program    State    System
Time    What    Where    Who
or user name
or directory name
or Decimal job umber
or ","
or confirm with carriage return

```

combinations of arguments may be given:

```
@sys stacia all header
```

```

Tue 14-Aug-84 15:35:12 Up 45:46:14
20+13 Jobs    Load av   3.37   2.67   2.02

```

```

Job  CJB Line Program State  Time      Limit      User, <Directory> Foreign host
20*      51 SYSTAT  RUN    0:09:35      STACIA, PS:<HELP>

```

```
@sys stacia all no directory
```

```

Tue 14-Aug-84 15:35:44 Up 45:46:46
20+13 Jobs    Load av   3.09   2.67   2.04

```

```

Job  CJB Line Program State  Time      Limit      User      Foreign host
20*      51 SYSTAT  RUN    0:09:37      STACIA

```

The first listed all SYSTAT information about user STACIA. The second listed all of the information given before, without listing the connected directory.

WHAT'S AVAILABLE ON THE DDN

```

@NIC <enter NIC after @ prompt>
TOP  <enter TOP to start at beginning of file>

```

NIC/Query is a database system containing information about the Defense Data

ARPA2.TXT

Network (DDN), including MILNET and ARPANET. Each list of topics is presented to the user as a numbered menu of selections.

- To see more detail on any of the topics below, type its corresponding number followed by a carriage return, <CR>.

- To leave NIC/Query, type 'quit<CR>'.

- For more help and additional commands, type 'help<CR>'.

1. INTERNET PROTOCOLS -- Describes Internet protocols
2. PROGRAMS -- Describes programs available on DDN hosts
3. PERSONNEL -- Directory of DDN users
4. HOSTS -- Describes DDN hosts
5. RFCS -- Requests For Comments technical notes
6. IENS -- Internet Experiment Notes
7. NIC DOCUMENTS -- Documents available from the NIC

_ for back, ^ for up, + for top, or menu # (1-7): QUIT <let's return to this menu later>

LOGGING OUT -----

You haven't really logged in yet, and a quick way of logging out is to enter a "C" at the prompt or to simply unplug your phone. However, ARPANET's own files can be revealing:

@HELP KK

The LOGOUT command logs you off of the system and expunges all deleted files in your directory. Synonyms for LOGOUT include K and KK.

You may also log out another job logged in on your account by specifying the job number after the LOGOUT command. In this case a message describing the job to be logged out is printed, and a confirming RETURN is required.

If your job hangs, you might wish to log in at another terminal and then LOGOUT the other job, as described in the last paragraph. First find the other job number, as follows:

```
@systat jsmith
27*  54  SYSTAT  JSMITH
32   112 BASIC   JSMITH
```

The * indicates the job number of the job issuing the SYSTAT command. You will want to use the other job number -- 32 in this case:

```
@logout 32
JSMITH, TTY112, BASIC
[Confirm]
```

ARPA2.TXT

and you confirm by pressing the RETURN key.

MORE HELP

@HELP ATTACH

ATTACH allows you to move a job to a different terminal or to return it to a terminal from detached status.

To ATTACH, say

@attach USERNAME

Password:

At the Password prompt, type in your password (which will not be echoed to the screen) and your job will be attached.

If you have more than one job logged on to the system, you will need to supply a job number after your username. Finger yourself to find out this information. If you are attaching a job which is already attached to another terminal, you will be asked to confirm with carriage return before the Password prompt.

(In Part III of Hacking ARPANET by The Source, some of the best information ARPANET will tell any "anonymous guest" once you leave the Exec.)

Cracking ARPANET by The Source, some of the best information