
Hacking ARPANET -- Part VI

by

The Source

This last part of the Hacking ARPANET series provides some more information on the types of things that you can learn from the EXEC, and concludes by explaining how to log onto the system and how passwords are structured.

Once you are onto the EXEC, as explained in Part I, you should get into the QUERY function which is also explained earlier. QUERY will tell you just about all you need to know about anyone, including their business phone numbers and the locations of certain military employees.

@N

TOP

NIC/Query is a database system containing information about the Defense Data Network (DDN)...

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): 4

HOSTS

We have selected menu item 4, "HOSTS".

HOSTS -- Describes DDN hosts

1. BY NAME -- Description of hosts by DDN hostname
2. BY CPU -- List of hosts by CPU type
3. BY OS -- List of hosts by Operating System

_ for back, ^ for up, + for top, or menu # (1-3): 1

If we were especially interested in working on one or another computer, a CRAE, for example, we would select menu item 2. Or, if we wanted to learn a new

ARPA6.TXT

operating system, we could select menu item 3. But let's see what's available under menu item 1:

HOSTS BY NAME -- Description of hosts by DDN hostname

To show the entry for a host, type its official name or nickname.

To get a menu of hostnames, select the appropriate choice below.

1. ARPANET HOSTS-A-G
2. ARPANET HOSTS-H-R
3. ARPANET HOSTS-S-Z
4. MILNET HOSTS-A-F
5. MILNET HOSTS-G-M
6. MILNET HOSTS N
7. MILNET HOSTS-O-Z
8. ARPANET TACS
9. MILNET TACS
10. GATEWAYS

_ for back, ^ for up, + for top, or menu # (1-10): 10 <let's take a look>

GATEWAYS

1. AERONET-GW 2. AMES-NAS-GW 3. ARPA-MILNET-GW
4. BBN-CRONUS-GW 5. BBN-FIBERA-GW 6. BBN-MILNET-GW
7. BBN-MINET-A-GW 8. BBN-NET-GATEWAY 9. BBN-PR-GW
10. BBN-VAN-GW 11. BBN-X25-GW 12. BRAGG-PR-GW1
13. BRAGG-PR-GW2 14. BRL-GATEWAY 15. BRL-GATEWAY2
16. CIT-CS-GW 17. CMU-GATEWAY 18. COLUMBIA-GW
19. CORNELL-GW 20. CSNET-PDN-GW 21. CSS-GATEWAY
22. CSS-RING-GW 23. DARPA-GW 24. DCEC-GATEWAY
25. DCEC-MILNET-GW 26. DCEC-PSAT-IG 27. DCN-GATEWAY
28. DTNSRDC-GW 29. HARVARD-GW 30. HUEY-GW
31. IPTO-GW 32. ISI-GATEWAY 33. ISI-MCON-GW
34. ISI-MILNET-GW 35. ISI-PSAT-IG 36. LBL-MILNET-GW
37. LL-GW 38. LL-PSAT-IG 39. LOUIE-GW
40. MARYLAND-GW 41. MIT-GW 42. NLM-GW
43. NOSC-GW 44. NRL-CSS-GW 45. NSRDCOA-GW
46. NYU-GW 47. PURDUE-CS-GW 48. RAD-PSAT-IG
49. RIACS-GW 50. S1-B-GW 51. SAC-GATEWAY
52. SAC-GW-2 53. SAC-MILNET-GW 54. SRI-C3ETHER-GW
55. SRI-MILNET-GW 56. SRI-PR-GW1 57. SRI-PR-GW2
58. SRI-PR-GW3 59. STANFORD-GATEWAY 60. TACTNET-GW
61. UDEL-GW -- University of Delaware
62. UR-CS-GW -- University of Rochester
63. UTAH-GATEWAY -- University of Utah
64. UW-VLSI-GW -- University of Washington
65. WISC-GATEWAY -- University of Wisconsin
66. WSMR-NET-GW -- White Sands Missile Range
67. YALE-GW -- Yale University

68. YUMA-GW -- Army Yuma Proving Ground

<menu item 9>

MILNET TACS

- | | |
|--|-----------------------|
| 1. ACCAT-TAC | 2. AFGL-TAC |
| 3. AFSC-AD-TAC | 4. AFSC-HQ-TAC |
| 5. AFSC-SD-TAC | 6. AFWL-TAC |
| 7. AMES-TAC | 8. ANNIS-MIL-TAC |
| 9. ARDC-TAC | 10. ARPA1-MIL-TAC |
| 11. ARPA2-MIL-TAC | 12. BBN-MIL-TAC |
| 13. BRL-TAC | 14. BROOKS-AFB-TAC |
| 15. CINCPAC-TAC | 16. CORADCOM-TAC |
| 17. CORADCOM2-TAC | 18. DARCOM-TAC |
| 19. DAVID-TAC | 20. DCEC-MIL-TAC |
| 21. DCEC-TAC | 22. DDN-PMO-MIL-TAC |
| 23. DUGWAY-MIL-TAC | 24. FRANKFURT-MIL-TAC |
| 25. GUNTER-TAC | 26. KOREA-TAC |
| 27. MICOM-TAC | 28. MINET-BRM-TAC |
| 29. MINET-CPO-TAC | 30. MINET-HDL-TAC |
| 31. MINET-HLH-TAC | 32. MINET-LON-TAC |
| 33. MINET-OBL-TAC | 34. MINET-RAM-TAC |
| 35. MINET-RDM-TAC | 36. MINET-SIG-TAC |
| 37. MINET-VHN-TAC | 38. MITRE-TAC |
| 39. NCAD-MIL-TAC | 40. NORL-MIL-TAC |
| 41. NPS-TAC -- Naval Postgraduate School | |
| 42. NSWG-TAC -- Naval Surface Weapons Center | |
| 43. NWC-TAC -- Naval Weapons Center | |
| 44. PAX-RV-TAC -- Naval Electronics Systems Command | |
| 45. PENTAGON-TAC -- Air Force Data Services Center/SFA | |
| 46. RADC-TAC -- Rome Air Development Center | |
| 47. RAND2-MIL-TAC -- The Rand Corporation | |
| 48. ROBINS-TAC -- Warner-Robins ALC/MMECDM | |
| 49. SAC1-MIL-TAC -- Strategic Air Command/ADXCC Headquarters | |
| 50. SAC2-MIL-TAC -- Headquarters, Strategic Air Command | |
| 51. SCOTT-TAC -- Air Force Communications Command | |
| 52. SCOTT2-MIL-TAC -- Air Force Communications Command | |
| 53. SRI-MIL-TAC -- SRI International | |
| 54. STLA-TAC -- Army Information Systems Command - St. Louis | |
| 55. TINKER-MIL-TAC -- Tinker Air Force Base | |
| 56. USGS2-TAC -- U.S. Geological Survey | |
| 57. USGS3-TAC -- U.S. Geological Survey | |
| 58. WPAFB-TAC -- Aeronautical Systems Division/ADOS | |
| 59. WSMR-TAC -- White Sands Missile Range | |
| 60. YUMA-TAC -- Army Yuma Proving Ground | |

<If you're interested in more information about the system, simply enter its menu number as in the examples below:>

43. NWC-TAC -- Naval Weapons Center

SRI-MIL-TAC

SRI International (SRI-MIL-TAC)

Telecommunications Sciences Center

Network Information Center

333 Ravenswood Avenue

Menlo Park, California 94025

NetNumber: 26.3.0.73

Configuration: C/30

Protocols: TCP/TELNET,ICMP

Liaison:

Roode, R. David ROODE@SRI-NIC

(RAND2-MIL-TAC)

Room 145

1700 Main Street

Santa Monica, California 90406

NetNumber: 10.0.0.7

Configuration: C/30

Protocols: TCP/TELNET,ICMP

Liaison:

Collins, Colleen S. Colleen@RAND-UNIX

(213) 393-0411

<note that the data always includes the system's network number, NetNumber, this is a useful feature if you want to use your local node to dial up the remote system>

PROGRAMS

The EXEC also stores a list of programs and you can find out where to look for them on various network nodes. The programs are organized by menu as in the examples below:

PROGRAMS

1. BY NAME

2. PROGRAM LIST

2

PROGRAM LIST

1. 11COPY	2. 2LABEL	3. @	4. PROGRAMS-A
5. PROGRAMS-B	6. PROGRAMS-C	7. PROGRAMS-D	8. PROGRAMS-E
9. PROGRAMS-F	10. PROGRAMS-G	11. PROGRAMS-H	12. PROGRAMS-I
13. PROGRAMS-J	14. PROGRAMS-K	15. PROGRAMS-L	16. PROGRAMS-M
17. PROGRAMS-N	18. PROGRAMS-O	19. PROGRAMS-P	20. PROGRAMS-Q
21. PROGRAMS-R	22. PROGRAMS-S	23. PROGRAMS-T	24. PROGRAMS-U
25. PROGRAMS-V	26. PROGRAMS-W	27. PROGRAMS-X	28. PROGRAMS-Y
29. PROGRAMS-Z			

menu # (1-29): <note there are 29 flavors, but we're choosing flavor 3>

@

Examines a file and creates a checksum of each page. Upon subsequent runs it will detect which pages have changed and print only the altered pages, so that they can be added to the existing listing in place of the old pages. Has special features for updating cross-reference listings from compilers.

CMU hosts (called AT)

MIT-AI

MIT-ML

MIT-MC

SRI-KL

<it wasn't very thrilling, but the hosts that offer the feature are listed in case we want to use it. Let's try another menu selection, #4>

4

PROGRAMS-A

- | | |
|-------------------------|--------------------|
| 1. A6502 | 2. ACCTS |
| 3. ACT | 4. ACTFRK |
| 5. ADA | 6. ADUMP |
| 7. AGE-1 | 8. AGII |
| 9. AI-HANDBOOK | 10. AID |
| 11. AIQUIZ | 12. ALG606 |
| 13. ALGOL | 14. ALGOL-W |
| 15. ALIAS | 16. ALLPRT |
| 17. ALTER | 18. ALTER.SNO |
| 19. ALTRAN | 20. ANALYSIS |
| 21. ANALYZ | 22. APEX-III |
| 23. APL | 24. APL.GST |
| 25. APL25.KST | 26. APLCOM |
| 27. APLED | 28. APT-III |
| 29. ARCBITS | 30. ARCHIVE-LOOKUP |
| 31. ASSEMBLER-F | 32. ASSEMBLER-G |
| 33. ASSEMBLER-HONEYWELL | 34. ASSEMBLER-IBM |
| 35. ASSIST | 36. AT |
| 37. AUG3 | 38. AUGMEN |
| 39. AUGMENT | |

<again, for more information, type your selection>

9

AI-HANDBOOK

The AI Handbook is aimed at making the results of AI research accessible to the large, multi-disciplinary community of scientists who want to build AI systems in their own problem areas. Students and researchers at Stanford and other AI laboratories have prepared over 300 short articles describing the fundamental ideas, useful techniques, and exemplary programs developed in the field over the last 20 years. These articles have been written for computer-

ARPA6.TXT

literate scientists and engineers in other fields who are unfamiliar with AI research and jargon. The Handbook will provide a scientist who, for instance, might want to know" front end, with information about all of the relevant AI techniques and existing systems, as well as abundant pointers into the field's literature.

SUMEX-AIM

menu # (1-39): 15

ALIAS

Allows a dummy name to be set up for a program.

CMU hosts

SUMEX-AIM

SRI-KL

menu # (1-39): 35

ASSIST

ASSIST is a compiler for a large subset of the IBM Assembler Language instruction set. ASSIST is oriented toward instructional use but is also useful for program checkout. ASSIST features simplified I/O statements and detailed assembly and execution error messages. ASSIST was developed at Pennsylvania State University and the University of Tennessee.

UCLA-CCN

menu # (1-39): 3

ACT

Acquisition of Cognitive Procedures, combines a semantic network data-base with a production system to simulate human cognition. ACT possesses a number of learning mechanisms which have been used to model the learning of procedural skills such as language comprehension and geometry theorem proving. It can also model human limitations.

SUMEX-AIM

menu # (1-39): PERSONNEL

To view information about an individual when you know his or her LAST NAME

Type: LASTNAME <CR> (where 'LASTNAME' is the person's last name; e.g., Smith)

PARTIAL NAME

Type: LASTN... <CR> (where 'LASTN...' is a partial spelling of the person's last name followed by three periods, e.g., Sm...)

FULL NAME

Type: FULLNAME <CR> (where 'FULLNAME' is the person's last name followed by a comma and his or her first name; e.g., Smith, Mary)

IDENT

Type: XYZ <CR> (where 'XYZ' is the ident)

ARPA6.TXT

<so let's try one...>

MA...

There are 631 matching entries.

<oops, for the purpose of this printout we'll just show a few of them>

Accetta, Michael (MA) MIKE.ACSETTA@CMU-CS-A (412) 578-7681
Asato, Mino (MA1) NEEAPAC@HAWAII-EMH (808) 471-3444 (AV) 421-6834
Amaro, Manny (MA10) MAMARO@SIMTEL20 (505) 678-9500 (AV) 258-9500 (FTS) 898-9500
Aguilar, Mary (MA11) mary@RAND-UNIX (213) 393-0411
Aronstein, Michael (MA12) ARONSTEIN@BBNA (619) 224-3243
Adams, Marilyn (MA13) MADAMS@BBNA (617) 497-3678
Abe, Michael (MA14) PACDET@PAXRV-NES (808) 471-0821
Ackerman, Mark (MA15) ACKERMAN@JPL-VLSI (818) 354-4467
Altenau, Mike (MA17) CENCOMS-F4@USC-ISID --
Addison, Michael (MA19) MARCOMMS@PAXRV-NES (703) 521-8835
Allerding, Martin (MA20) 600140@LANL (703) 326-7028
...

LOGIN

ARPANET very graciously tells us just about all we know to be able to log into the system in the related HELP file below:

.HELP LOGIN

Only people with authorized accounts may log in on this system, though some programs can be run without logging in. Type "HELP GUEST" for a list of these "free" programs. Type "HELP ACCOUNT" for information on opening an account.

To log in, type the word LOGIN (this may be abbreviated L) followed by a space, your project name, a comma, and your programmer name:

L PRJ,PRG

This will log you in, and type out any system messages or personal mail for you which may exist. You can stop the message timeout by typing the CALL eg (CONTROL-C twice from other characters in place of the ",") namely:

/ - types only system messages that have been posted since you last logged in.

. - suppresses all messages.

% - lets you specify a new password.

In order to log in from the network or remotely, you must have a password.

For a more complete description of LOGIN options, see the printed Monitor Command Manual or its online version MONCOM.BH[S,DOC], whose updates are in MONCOM.UPD[S,DOC].

Remember, ARPANET has already shown us how to find out the PRG (programmer name) part of the login:

.FINGER INT where INT are the initials of a programmer. If the initials don't

ARPA6.TXT

exist you will get an error message. Keep trying until you find the correct initials.

Passwords are often the same as the programmer's initials. If not, then try the programmer's first name which you can learn from using the Personnel option on the menu in the Exec's QUERY.

Once you have a password, you may then log onto just about any ARPANET computer. Instead of typing "0 0,11", enter the machine's NetWork number!

All that's left to be hacked is the first section of the logon code -- the PRJ name, which may be as long as three letters and which may include nubmers.

HAPPY HACKING!

THIS SERIES OF ARTICLES WAS BROUGHT TO
YOU BY **THE SOURCE**. COPY IT; SPREAD
IT AROUND; USE IT FREELY BUT DON'T
FORGET TO PUT THE AUTHOR'S NAME IN IT