Title
WHO GOES THERE? A DIALOGUE OF QUESTIONS AND ANSWERS ABOUT BENIGN HACKING

Permalink
https://escholarship.org/uc/item/57w3h3vj

Author
Stevens, D.F.

Publication Date
1987-04-01
WHO GOES THERE? A DIALOGUE OF QUESTIONS AND ANSWERS ABOUT BENIGN HACKING

D.F. Stevens

April 1987
DISCLAIMER

This document was prepared as an account of work sponsored by the United States Government. While this document is believed to contain correct information, neither the United States Government nor any agency thereof, nor the Regents of the University of California, nor any of their employees, makes any warranty, express or implied, or assumes any legal responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by its trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or the Regents of the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof or the Regents of the University of California.
Who Goes There? A Dialogue of Questions and Answers About Benign Hacking*

David F. Stevens
Lawrence Berkeley Laboratory
University of California
Berkeley, California 94720

Abstract: On August 23, 1986, it was noticed that the accounting files for one of LBL's computing systems failed to balance. On August 24, we received word that an unauthorized person was attempting entry into a US Navy computer from LBL. Preliminary investigation indicated that LBL was the victim of a benign hacker, where "benign" is used in the medical sense. It was thought that the perpetrator was a graduate student from a neighboring university, and that it would provide a useful object lesson to other such folk if he were caught and admonished. LBL therefore embarked upon a journey of detection and containment instead of prevention. That journey continues today, having led first across the country, then across the Atlantic. In the course of the journey we have gathered a number of observations that should be of interest to anyone running a computer with any connection to the outside world.

Why the Computer Measurement Group?
The first and most obvious question is "Why should this material be of interest to CMG?" There are two reasons. The first is that one element of successful performance management is ensuring that enough capacity is available to satisfy the legitimate demands of all authorized users. Every cycle stolen or file hidden by an unauthorized user reduces the resources available for legitimate use. The elimination of unauthorized use thus extends the useful life of your present configuration.

The second reason for CMG to take an interest is that some of the tools developed for measurement and management purposes can also be used to detect unauthorized access. You are in the business of knowing where demand and usage originate; it is but a small extra step to distinguish between authorized and unauthorized usages.

What do you mean by "benign hacking"?
"Hacking" has gone through two metamorphoses of meaning. Its original meaning in the

* This work was supported by the U.S. Depart of Energy under contract No. DE-AC03-76SF00098.
computing community was similar to its meaning in the golfing community. A hacker was one who butchered code. Then, some years ago, it was transformed from a term of opprobrium into one that indicated long hours willingly spent probing the dim recesses of system internals, searching for ways to accomplish Good Things. Finally, in the last decade or so, it has come to signify computing wizardry employed for personal purposes, frequently explicitly directed against governmental and large corporate installations.

In this dialogue I consider any activity resulting from (attempted or successful) unauthorized access to be hacking. (It is worth noting in passing that access by an authorized user at greater than authorized levels of privilege or for unauthorized purposes is unauthorized, and therefore a form of hacking.) Further, I define hacking that is limited to entry and consumption of resources, as distinct from intending to destroy or alter data, to be "benign". As noted in the abstract, benign is used in its medical sense: Not actively inimical, perhaps, but certainly intrusive and possibly painful. The presence of a benign hacker, like that of a benign tumor, is not to be considered a sign of good health.

Why limit the discussion to benign hackers?
Primarily because that’s the kind I’m best qualified to discuss, but there are other good reasons:

- Benign hacking is more prevalent than the malignant sort (we think).
- It is more difficult to get people concerned about "harmless" hacking, even though in some respects the damage done to the institution can be as great for benign hacking as for hacking for gain. (Your image can suffer more from imaginative media accounts of recreational hacking than from serious accounts of hacker theft.)
- It is more difficult to detect benign hacking than vandalism.
- If you can detect and prevent benign hacking you have a good start at detecting and preventing vandalism and hacking for gain.

What do benign hackers do?
The total range of hacking activities runs from access only, just to prove it could be done (simply collecting scalps, as it were), through theft of resources (for the hacker’s pleasure or do the hacker's personal work on someone else's computer), to grand larceny (altering bank balances or generating false invoices). We are concerned here only with benign hacking, which is essentially recreational in nature. In this context, most of the activity you are likely to encounter is generally related to snooping.
Benign hackers look around; they browse through all directories they can gain access to, looking for interesting files.

- They document your commands (via trial and error; "HELP" facilities are a great help to them in this regard).
- They make lists of authorized users (the more valid ID's they know the more likely they are to get additional privilege).
- They read everybody's electronic mail (they are especially interested in messages about security breaches and countermeasures; they also look for passwords written in files).
- They look for programs that are looking for them.
- They look for (and try to crack) the password files.

More active pursuits, but in the same general vein (that is, oriented towards allowing themselves undetected free use of your resources), are

- Attempting to disable accounting for their jobs;
- Stealing stale or unused accounts (usually by changing the password);
- Hiding files;
- Setting up bulletin boards;
- Attempting to disable security alarms;
- Playing games;
- Connecting to other systems from yours (and if you have a dial-out modem, they will try to use that, while you pay the phone bill).

How do they get in in the first place?

There are many avenues, ranging from the direct (someone gives them a valid password/ID combination) to the brute force (random dialing followed by random probes), but most of them take advantage of your cooperation.

- Retention of default or generic logins with their original passwords;
- Use of common "temporary" ID's (such as test or demo or guest) with trivial passwords;
- Use of passwords identical to or derivable from ID's;
- Use of null passwords;
- Use of the same password/ID combination on multiple systems;
- Writing a password/ID combination for system A in a file on system B;
- Use of an unprotected remote login or file transfer from one system to another;
• The existence of commands (who, for instance) that can be executed without logging in.

They also run an extensive grapevine, and pass successful password/ID combinations around, both directly and through hacker-oriented nationwide bulletin boards.

**How long does it take to break into a system?**

That depends, of course, upon how much the hacker knows, how good your protection is, and how well your users follow good password practice. If you still use the default system operator or maintenance passwords that come with the system when it is delivered, it takes about 10 seconds (for those are the first things tried). If you are well protected, and good practices are observed by all your users, it will generally take too long for casual hacking. Remember, however, that if another installation has network access to your system, you are only as secure as that installation and its user community. (This is a larger community than you might at first think. Widespread network access is now available to students at most of the institutions of higher learning in North America and Western Europe, plus many of the high schools, as well.)

**Don’t they have to know what kind of system it is before they start?**

Most systems are very helpful to anyone who achieves a connection, and the login prompt often tells the caller the name of the company as well as the system and version number. Others are easily identified by the style of response to unsuccessful login attempts.

**How many commercial sites are connected to networks?**

Probably most of them of a size large enough to send someone to CMG. The telephone system, after all, is a worldwide network (and has been used to support transcontinental and transatlantic hacking). And any system with remote diagnostic capabilities has network access. Many service engineers have occasion to access many different systems, with differing password/ID combinations. It is fairly natural that they tend to record these nuggets of hackery on the fly leaves and back covers of their maintenance manuals, where they can be discovered through trashing. (In the '60's the term "trashing" referred to the intentional destruction of property. It now refers to a favorite phreak/hacker activity: the careful sifting of selected trash barrels looking for access-oriented jottings. It is successful often enough to encourage dedicated hackers and phreaks to fly across the country to raid a particularly fruitful site.) The point being, of course, that you are at risk not only from your own site, but from the engineer's trash bins in Boulder or White Plains or Dallas, as well.
But our dial-in numbers are unlisted....
Random dialers don't read directories, they just start dialing and hanging up if they don't get a modem tone. Many set their systems up to dial sequential numbers automatically for hours at a time while they are off doing more interesting things. And once they get a tone, as often as not, they announce the number (through a bulletin board or in the magazine 2600) even if they haven't yet figured out what kind of a computer is on the other end. Some systems provide assistance, too: they have very helpful dialout programs that tell the user the previous number dialed.

Why should we care? (We don't have any secrets on our system.)
(This question tends to arise more often in the academic and research areas than in the commercial sector, but it has been heard there, as well.) You have data that is difficult or expensive to replace. You have data that contributes to strategic planning, to legal reporting requirements, to inventory management. Many of you have data that your employees and customers consider to be confidential. Some of you also have controllers who already think you're spending too much on computing, and who would not be happy to learn that some of it was going to unauthorized use.

But is this a real threat? Can anybody really get in this way?
My institution has observed a single hacker, over a four-month period, make more than 400 one-minute attempts to break into other systems from our site. Using a very limited repertoire of techniques (it's difficult to be truly creative in such a short time) he:

- reached about half the sites (i.e. was invited to try to login);
- succeeded in logging into 25 systems;
- became system manager at 9 sites!

That's better than a 2% success ratio at becoming system manager; more than three times that for simple access. That means that several of you here today are at risk. The odds today are certainly that if the hacker community wants you badly enough, they can gain entry.

How did you find this guy? Why didn't you shut him out?
We found him through a combination of events, one of which was an imbalance in a double-entry bookkeeping system maintained for chargeback purposes. The discovery of the imbalance coincided with a report from another installation that an unauthorized remote entry had been attempted from LBL.
Our first thought was that the culprit was a student from a nearby college, so we set out to catch
him in the act and create an example, rather than shut him out. In so doing we discovered much
of the content of this paper. ("We", by the way, is primarily Dr. Clifford Stoll of our staff, assisted
by folks from a number of affected institutions and law-enforcement bodies; chief among these
outside folks was Steve White at Tymnet.) We did keep a rather close watch on our friend’s
activities -- for we had no assurance that they would continue to be relatively harmless -- and
warned other sites whenever he succeeded in gaining entry.

One of the things we learned from having watched him for a while is that had we tried to shut
him out when we first discovered him we would probably have failed, for he had already stolen
several accounts. Thus, once we learned that it was not just a local student hack, we thought it
worth pursuing to the end in the hopes of learning more.

**How can one be sure one is safe?**

If you are connected to a network or have a dialin port you can be reasonably sure you’re not safe.
Collusion with your own staff aside, however, you can be as safe as you want to be. Safety
consists in knowing all your users and in knowing the ownership of all files in the system.
"Knowing your users" includes not only knowing who they are (a process of authorization and
validation), but also of verifying that they are, indeed, who they say they are (authentication)
every time they attempt to access the system. This is the fundamental purpose of a password
scheme.

**How much should we spend on protection?**

This is a question of insurance, and as with all such questions you should weigh the cost against
the expected value of the loss, and not overspend. Some of the costs on each side of the balance
are relatively non-obvious. The cost of protection includes not only the cost of acquisition and
implementation of protective measures, but also the costs inherent in the education of the users
and in the irritation they experience at having to retrain their fingers to the new passwords. In
estimating the expected value of a loss you must also include the cost of cleaning up after a
breach. Even a “harmless” breach involves staff time and effort in detection, elimination of
unauthorized files and accounts, tracing and prosecution (if warranted), and elimination of the
system or procedural flaw that allowed the breach. These costs can be considerable. (In our case,
they amounted to at least three months’ full-time effort of a senior analyst, plus assorted bits and
pieces of management time.)
What did you learn from your experience?

- When it starts, you never know how big it's going to get, or how far it's going to reach. We thought it would reach about a mile, and it turned out to extend from Berkeley to Europe. The level of interconnection of the world today makes it easy for a hacker to reach you in several hops, and he may choose to do so either to conceal his real origin, or because each step is limited for some technical or financial reason.

- The further it reaches, the more important it is to have a well-defined procedure to follow, and the more difficult it is to achieve coordination. The telephone company, for instance, prefers to deal with law-enforcement people in matters of call-tracing, rather than with technical people. So does the FBI. It has been difficult to get real cooperation from some agencies when contact is at the technical level, but technical contact is essential so that the sites being attacked can pool their knowledge of the hacker.

- Have clear communication paths. Know whom the telephone company will listen to, whom to call in any network to which you are connected, whom to call at the FBI or your local law enforcement agencies, etc.

- TYMNET has the tools and the willingness to help. Once alerted, they can complete a trace in minutes.

- The telephone company won't willingly trace beyond state boundaries without a federal warrant.

- Inform any other victims as soon as you can. Not only is this good citizenship, it will encourage them to notify you when the shoe is on the other foot.

- People use poor password practice -- even those who ought to know better. Among the poor practices exploited by our hacker are: continued use of default passwords; password identical to ID; trivial password (i.e., easily guessable, such as name when ID is initials, location, system name, same password on several systems); existence of non-password-protected ID's (e.g., who on some unix systems); listing of ID and associated password in the clear in files with suggestive names.

- Passwords decay with time. Other people get to know them through several mechanisms (accident, gift, guesswork, ...).

- Whenever people are required to use system-generated passwords, they will write them down where a hacker may find them.
• Be careful when demonstrating systems to unknown people (at least one hacker claims to have gotten a password by looking over a salesman's shoulder during a demonstration).

• It's more difficult to discover unauthorized use after a valid account has been stolen than before.

• Don't use E-mail to discuss any aspect of a hack, unless you want the hacker to read it, too.

• An attached printer is an indispensable tool for serious tracing. Without one it is generally impossible to reconstruct the hacker's session. (If he has system privilege, he can destroy the log of his session before you can read it.) A printer linked in parallel with his output gives you a real-time track that he cannot erase.

• A network is weaker than its weakest link. (And all of the networks we belong to have some extremely weak links.)

**What can we do to detect benign hacking and to protect against it?**

The following lists are suggestive rather than exhaustive. No attempt is made to rank the items in order of effectiveness or cost; individual situations are too different to make such an attempt meaningful.

**To detect:**

• Look for hidden files. Many systems have legitimate ways to "hide" utility files so that they don't clutter up working directories. In *unix, for instance, any file name beginning with a dot (such as `.login`) is hidden. It is also possible to place files into directories that are not usually searched.

• Look for files with "unauthorized" contents. (Since different organizations have different rules about off-hour use of computers, the definition of "unauthorized" can vary widely.) If you employ this procedure, it is important to ensure that the looker is ethical, and does not divulge the contents of any of the files looked at.

• Require that every network access carry traceback information so that you (or the network operator) can determine the source of all traffic. Review the log from time to time and look for anomalies.

• Provide your users with enough accounting information so that they can discover if anyone else is using their accounts.

• Institute chargeback, so that they have a reason to read the accounting information and to inform you if it seems to be out of line.
• Employ double-entry bookkeeping. (One way is to keep a write-only record of all resource usage and then to compare that to all "charged" usage.)
• Tell users of unsuccessful entry attempts in their name.
• Tell users the date and time of their last successful login.
• Encourage the users to read those messages and notify you of any anomalies.

To protect:

• Authorize users individually and personally.
  Verify the user's identity (and employer) before granting access.

• Require the use of passwords for access, and adopt a sensible password policy. Some possibilities are:
  -- Password cannot equal login name.
  -- Changes of password cannot equal previous passwords.
  -- Password must be at least 6 characters long, and contain at least one non-alphabetic character.
  -- Password cannot be all the same character.
  -- Password cannot contain a recognizable part of the login name.
  -- Password must expire within 180 days of being issued.
  -- Passwords belonging to terminated employees should be terminated.

• Require password changes. One practitioner has said "Treat your password like your toothbrush: Change it once in a while, and don't pass it around."

• Control access to particularly sensitive data by location (terminal or port of origin) as well as by name (password/ID).

• Let login ID's expire (to avoid proliferation of stale accounts).
  -- Initial logins should be deactivated very quickly if they are not used.
  -- "Active" logins should expire after some reasonable period of non-use.
  -- A login should be terminated as soon as any employee who knows it leaves the company (for any reason).

• Fix any known loopholes that allow someone to increase his level of privilege.

• Protect network access.
  -- Avoid network access procedures that require or encourage the writing of passwords in files.
-- Limit the privileges of any process that originates remotely.
-- Monitor the use of remote logins.
-- Install password protection on network access ports, including those used for remote maintenance.
-- Adopt a dial-back verification procedure for remote telephone access.
-- Restrict physical access to workstations possessing automatic login procedures for access to your mainframes.

• Protect log and journal files that give the history of interactive sessions. These can be read, and they can be as useful to a hacker as ordinary text files.

• Set file access protection defaults to something more restrictive than world.

• Require your system to remain anonymous until after you get a valid login. (Many systems provide a great deal of help by welcoming login attempts, or even when responding to a modem call. Don't provide anything other than bare ID and password prompts until you know who's at the other end.)

What do we do when we find someone?
That's up to you, of course. That depends upon what's at risk, what has been damaged, and how much effort you are willing to devote to the chase and possible prosecution of the offender.

Do you have any last words?
Only the following warning, adapted from Tolkien: It does not do to leave a live dragon out of your calculations if he has network access to your computer.
This report was done with support from the Department of Energy. Any conclusions or opinions expressed in this report represent solely those of the author(s) and not necessarily those of The Regents of the University of California, the Lawrence Berkeley Laboratory or the Department of Energy.

Reference to a company or product name does not imply approval or recommendation of the product by the University of California or the U.S. Department of Energy to the exclusion of others that may be suitable.