
GUIDE TO (mostly) HARMLESS HACKING

Vol. 1 Number 2

In this issue we learn how to forge email -- and how to spot forgeries. I promise, this hack is spectacularly easy!

Heroic Hacking in Half an Hour

How would you like to totally blow away your friends? OK, what is the hairiest thing you hear that super hackers do?

It's gaining unauthorized access to a computer, right?

So how would you like to be able to gain access and run a program on the almost any of the millions of computers hooked up to the Internet? How would you like to access these Internet computers in the same way as the most notorious hacker in history: Robert Morris!

It was his "Morris Worm" which took down the Internet in 1990. Of course, the flaw he exploited to fill up 10% of the computers on the Internet with his self-mailing virus has been fixed now -- on most Internet hosts.

But that same feature of the Internet still has lots of fun and games and bugs left in it. In fact, what we are about to learn is the first step of several of the most common ways that hackers break into private areas of unsuspecting computers.

But I'm not going to teach you to break into private parts of computers. It sounds too sleazy. Besides, I am allergic to jail.

So what you are about to learn is legal, harmless, yet still lots of fun. No pulling the blinds and swearing blood oaths among your buddies who will witness you doing this hack.

But -- to do this hack, you need an on-line service which allows you to telnet to a specific port on an Internet host. Netcom, for example, will let you get away with this.

But Compuserve, America Online and many other Internet Service Providers (ISPs) are such good nannies that they will shelter you from this temptation.

But your best way to do this stuph is with a SHELL ACCOUNT! If you don't have one yet, get it now!

****
Newbie note #1; A shell account is an Internet account that lets you give Unix commands. Unix is a lot like DOS. You get a prompt on your screen and type out commands. Unix is the language of the Internet. If you want to be a serious hacker, you have to learn Unix.
****

Even if you have never telnetted before, this hack is super simple. In fact, even though what you are about to learn will look like hacking of the most heroic sort, you can master it in half an hour -- or less. And you only need

to memorize *two* commands.

To find out whether your Internet service provider will let you do this stuph, try this command:

telnet callisto.unm.edu 25

This is a computer at the University of New Mexico. My Compuserve account gets the vapors when I try this. It simply crashes out of telnet without so much as a "tsk, tsk."

But at least today Netcom will let me do this command. And just about any cheap "shell account" offered by a fly-by-night Internet service provider will let you do this. Many college accounts will let you get away with this, too.

****
Newbie note #2: How to Get Shell Accounts

Try your yellow pages phone book. Look under Internet. Call and ask for a "shell account."

They'll usually say, "Sure, can do." But lots of times they are lying. They think you are too dumb to know what a real shell account is. Or the underpaid person you talk with doesn't have a clue.

The way around this is to ask for a free temporary guest account. Any worthwhile ISP will give you a test drive. Then try out today's hack.
****

OK, let's assume that you have an account that lets you telnet someplace serious. So let's get back to this command:

telnet callisto.unm.edu 25

If you have ever done telnet before, you probably just put in the name of the computer you planned to visit, but didn't add in any numbers afterward. But those numbers afterward are what makes the first distinction between the good, boring Internet citizen and someone slaloming down the slippery slope of hackerdom.

What that 25 means is that you are commanding telnet to take you to a specific port on your intended victim, er, computer.

****
Newbie note #3: Ports
A computer port is a place where information goes in or out of it. On your home computer, examples of ports are your monitor, which sends information out, your keyboard and mouse, which send information in, and your modem, which sends information both out and in.

But an Internet host computer such as callisto.unm.edu has many more ports than a typical home computer. These ports are identified by numbers. Now these are not all physical ports, like a keyboard or RS232 serial port (for your modem). They are virtual (software) ports.
****

But there is phun in that port 25. Incredible phun. You see, whenever you

telnet to a computer's port 25, you will get one of two results: once in awhile, a message saying "access denied" as you hit a firewall. But, more often than not, you get something like this:

```
Trying 129.24.96.10...
Connected to callisto.unm.edu.
Escape character is '^]'.
220 callisto.unm.edu Smail3.1.28.1 #41 ready at Fri, 12 Jul     96 12:17 MDT
```

Hey, get a look at this! It didn't ask us to log in. It just says...ready!

Notice it is running Smail3.1.28.1, a program used to compose and send email.

Ohmigosh, what do we do now? Well, if you really want to look sophisticated, the next thing you do is ask callisto.unm.edu to tell you what commands you can use. In general, when you get on a strange computer, at least one of three commands will get you information: "help," "?", or "man." In this case I type in:

```
help
```

... and this is what I get

```
250 The following SMTP commands are recognized:
250
250   HELO hostname              startup and give your hostname
250   MAIL FROM:<sender address>  start transaction from sender
250   RCPT TO:<recipient address>    name recipient for message
250   VRFY <address>           verify deliverability of address
250   EXPN <address>              expand mailing list address
250   DATA                     start text of mail message
250   RSET                   reset state, drop transaction
250   NOOP                       do nothing
250   DEBUG [level]            set debugging level,default 1
250   HELP                     produce this help message
250   QUIT                       close SMTP connection
250
250 The normal sequence of events in sending a message is to state the
250 sender address with a MAIL FROM command, give the recipients with
250 as many RCPT TO commands as are required (one address per command)
250 and then to specify the mail message text after the DATA command.
250 Multiple messages may be specified.  End the last one with a QUIT.
```

Getting this list of commands is pretty nifty. It makes you look really kewl because you know how to get the computer to tell you how to hack it. And it means that all you have to memorize is the "telnet <hostname> 25 " and "help" commands. For the rest, you can simply check up on the commands while on-line. So even if your memory is as bad as mine, you really can learn and memorize this hack in only half an hour. Heck, maybe half a minute.

OK, so what do we do with these commands? Yup, you figured it out, this is a very, very primitive email program. And guess why you can get on it without logging in? Guess why it was the point of vulnerability that allowed Robert Morris to crash the Internet?

Port 25 moves email from one node to the next across the Internet. It automatically takes incoming email and if the email doesn't belong to someone with an email address on that computer, it sends it on to the next

computer on the net, eventually to wend its way to the person to who this email belongs.

Oftentimes email will go directly from sender to recipient, but if you email to someone far away, or if the Internet is clogged with traffic, email may go through several computers.

There are millions of computers on the Internet that forward email. And you can get access to almost any one of these computers without a password! Furthermore, as you will soon learn, it is easy to get the Internet addresses of these millions of computers.

Some of these computers have very good security, making it hard to have serious fun with them. But others have very little security. One of the joys of hacking is exploring these computers to find ones that suit ones fancy.

OK, so now that we are in Morris Worm country, what can we do with it? Well, here's what I did. (My commands have no number in front of them, whereas the computer's responses are prefixed by numbers.)

helo santa@north.pole.org
250 callisto.unm.edu Hello santa@north.pole.org
mail from:santa@north.pole.org
250 <santa@north.pole.org> ... Sender Okay
rcpt to:cmeinel@nmia.com
250 <cmeinel@nmia.com> ... Recipient Okay
data
354 Enter mail, end with "." on a line by itself
It works!!!
.
250 Mail accepted

What happened here is that I sent some fake email to myself. Now let's take a look at what I got in my mailbox, showing the complete header:

Here's what I saw using the free version of Eudora:

X POP3 Rcpt: cmeinel@socrates

This line tells us that X-POP3 is the program of my ISP that received my email, and that my incoming email is handled by the computer Socrates.

****
Evil Genius Tip: incoming email is handled by port 110. Try telnetting there someday. But usually POP, the program running on 110, won't give you help with its commands and boots you off the minute you make a misstep.
****

Return Path: <santa@north.pole.org>

This line above is my fake email address.

Apparently From: santa@north.pole.org
Date: Fri, 12 Jul 96 12:18 MDT

But note that the header lines above say "Apparently-From" This is important because it alerts me to the fact that this is fake mail.

Apparently To: cmeinel@nmia.com
X Status:

It works!!!

Now here is an interesting fact. Different email reading programs show different headers. So how good your fake email is depends on part on what email program is used to read it. Here's what Pine, an email program that runs on Unix systems, shows with this same email:

Return Path: <santa@north.pole.org>
Received:
from callisto.unm.edu by nmia.com
with smtp
(Linux Smail3.1.28.1 #4)
id m0uemp4 000LFGC; Fri, 12 Jul 96 12:20 MDT

This identifies the computer on which I ran the smail program. It also tells what version of the smail program was running.

Apparently From: santa@north.pole.org

And here is the "apparently-from" message again. So both Pine and Eudora show this is fake mail.

Received: from santa@north.pole.org by callisto.unm.edu with smtp
(Smail3.1.28.1 #41) id m0uemnL 0000HFC; Fri, 12 Jul 96 12:18 MDT
Message Id: <m0uemnL 0000HFC@callisto.unm.edu>

Oh, oh! Not only does it show that it may be fake mail -- it has a message ID! This means that somewhere on Callisto there will be a log of message IDs telling who has used port 25 and the smail program. You see, every time someone logs on to port 25 on that computer, their email address is left behind on the log along with that message ID.

Date: Fri, 12 Jul 96 12:18 MDT
Apparently From: santa@north.pole.com
Apparently To: cmeinel@nmia.com

It works!!!

If someone were to use this email program to do a dastardly deed, that message ID is what will put the narcs on his or her tail. So if you want to fake email, it is harder to get away with it if you send it to someone using Pine than if they use the free version of Eudora. (You can tell what email program a person uses by looking at the header of their email.)

But -- the email programs on port 25 of many Internet hosts are not as well defended as callisto.unm.edu. Some are better defended, and some are not defended at all. In fact, it is possible that some may not even keep a log of users of port 25, making them perfect for criminal email forgery.

So just because you get email with perfect-looking headers doesn't mean it is genuine. You need some sort of encrypted verification scheme to be almost certain email is genuine.

****
You can go to jail note: If you are contemplating using fake email to commit

a crime, think again. If you are reading this you don't know enough to forge email well enough to elude arrest.
****

Here is an example of a different email program, sendmail. This will give you an idea of the small variations you'll run into with this hack.

Here's my command:

telnet ns.Interlink.Net 25

The computer answers:

Trying 198.168.73.8...
Connected to NS.INTERLINK.NET.
Escape character is '^]'.
220 InterLink.NET Sendmail AIX 3.2/UCB 5.64/4.03 ready at Fri, 12 Jul 1996 15:45

Then I tell it:

helo santa@north.pole.org

And it responds:

250 InterLink.NET Hello santa@north.pole.org (plato.nmia.com)

Oh, oh! This sendmail version isn't fooled at all! See how it puts "(plato.nmia.com)" -- the computer I was using for this hack -- in there just to let me know it knows from what computer I've telnetted? But what the heck, all Internet hosts know that kind of info. I'll just bull ahead and send fake mail anyhow. Again, my input has no numbers in front, while the responses of the computer are prefaced by the number 250:

mail from:santa@north.pole.com
250 santa@north.pole.com... Sender is valid.
rcpt to:cmeinel@nmia.com
250 cmeinel@nmia.com... Recipient is valid.
data
354 Enter mail. End with the . character on a line by itself.
It works!
.
250 Ok
quit
221 InterLink.NET: closing the connection.

OK, what kind of email did that computer generate? Here's what I saw using Pine:

Return Path: <santa@north.pole.org>
Received:
from InterLink.NET by nmia.com
with smtp
(Linux Smail3.1.28.1 #4)
id m0ueo7t 000LEKC; Fri, 12 Jul 96 13:43 MDT
Received: from plato.nmia.com by InterLink.NET (AIX 3.2/UCB 5.64/4.03)
id AA23900; Fri, 12 Jul 1996 15:43:20 0400

Oops. Here the InterLink.NET computer has revealed the computer I was on

when I telnetted to its port 25. However, many people use that Internet host computer.

> Date: Fri, 12 Jul 1996 15:43:20 0400
> From: santa@north.pole.org
> Message Id: <9607121943.AA23900@InterLink.NET>
> Apparently To: cmeinel@nmia.com
>
> It worked!

OK, here it doesn't say "Apparently-From," so now I know the computer ns.Interlink.Net is a pretty good one to send fake mail from. An experienced email aficionado would know from the Received: line that this is fake mail. But its phoniness doesn't just jump out at you.

I'm going to try another computer. Hmmm, the University of California at Berkeley is renowned for its computer sciences research. I wonder what their hosts are like? Having first looked up the numerical Internet address of one of their machines, I give the command:

> telnet 128.32.152.164 25

It responds with:

```
Trying 128.32.152.164...
Connected to 128.32.152.164.
Escape character is '^]'.
220 remarque.berkeley.edu ESMTP Sendmail 8.7.3/1.31 ready at Thu, 11 Jul
1996 12
help
214 This is Sendmail version 8.7.3
214 Commands:
214     HELO    EHLO    MAIL    RCPT    DATA
214     RSET    NOOP    QUIT    HELP    VRFY
214     EXPN    VERB
214 For more info use "HELP <topic>".
214 To report bugs in the implementation send email to
214     sendmail@CS.Berkeley.EDU.
214 For local information send email to Postmaster at your      site.
214 End of HELP info
```

Oh, boy, a slightly different sendmail program! I wonder what more it will tell me about these commands?

```
HELP mail
214 MAIL FROM: <sender>
214     Specifies the sender.
214 End of HELP info
```

Big f***ing deal! Oh, well, let's see what this computer (which we now know is named remarque) will do to fake mail.

```
MAIL FROM:santa@north.pole.org
250 santa@north.pole.org... Sender ok
```

Heyyy... this is interesting ... I didn't say "helo" and this sendmail program didn't slap me on the wrist! Wonder what that means...

```
RCPT TO:cmeinel@techbroker.com
250 Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
This is fake mail on a Berkeley computer for which I do not     have a password.
.
250 MAA23472 Message accepted for delivery
quit
221 remarque.berkeley.edu closing connection
```

Now we go to Pine and see what the header looks like:

```
Return Path: <santa@north.pole.org>
Received:
from nmia.com by nmia.com
        with smtp
       (Linux Smail3.1.28.1 #4)
id m0ueRnW 000LGiC; Thu, 11 Jul 96 13:53 MDT
Received:
from remarque.berkeley.edu by nmia.com
        with smtp
       (Linux Smail3.1.28.1 #4)
id m0ueRnV 000LGhC; Thu, 11 Jul 96 13:53 MDT
Apparently To: <cmeinel@techbroker.com>
Received: from merde.dis.org by remarque.berkeley.edu   (8.7.3/1.31)
id MAA23472; Thu, 11 Jul 1996 12:49:56  0700 (PDT)
```

Look at the three "received" messages. My ISP's computer received this email not directly from Remarque.berkeley.edu. but from merde.dis.com, which in turn got the email from Remarque.

Hey, I know who owns merde.dis.org! So the Berkeley computer forwarded this fake mail through famed computer security expert Pete Shipley's Internet host computer! Hint: the name "merde" is a joke. So is "dis.org."

Now let's see what email from remarque looks like. Let's use Pine again:

```
Date: Thu, 11 Jul 1996 12:49:56  0700 (PDT)
From: santa@north.pole.org
Message Id: <199607111949.MAA23472@remarque.berkeley.edu>

This is fake mail on a Berkeley computer for which I do not     have a password.
```

Hey, this is pretty kewl. It doesn't warn that the Santa address is phony! Even better, it keeps secret the name of the originating computer: plato.nmia.com. Thus remarque.berkeley.edu was a really good computer from which to send fake mail. (Note: last time I checked, they had fixed remarque, so don't bother telnetting there.)

But not all sendmail programs are so friendly to fake mail. Check out the email I created from atropos.c2.org!

```
telnet atropos.c2.org 25
Trying 140.174.185.14...
Connected to atropos.c2.org.
Escape character is '^]'.
220 atropos.c2.org ESMTP Sendmail 8.7.4/CSUA ready at Fri, 12 Jul 1996 15:41:33
help
```

502 Sendmail 8.7.4 HELP not implemented

Gee, you're pretty snippy today, aren't you... What the heck, let's plow ahead anyhow...

helo santa@north.pole.org
501 Invalid domain name

Hey, what's it to you, buddy? Other sendmail programs don't give a darn what name I use with "helo." OK, OK, I'll give you a valid domain name. But not a valid user name!

helo satan@unm.edu
250 atropos.c2.org Hello cmeinel@plato.nmia.com [198.59.166.165], pleased to meet you

Verrrry funny, pal. I'll just bet you're pleased to meet me. Why the #%&@ did you demand a valid domain name when you knew who I was all along?

mail from:santa@north.pole.com
250 santa@north.pole.com... Sender ok
rcpt to: cmeinel@nmia.com
250 Recipient ok
data
354 Enter mail, end with "." on a line by itself
Oh, crap!
.
250 PAA13437 Message accepted for delivery
quit
221 atropos.c2.org closing connection

OK, what kind of email did that obnoxious little sendmail program generate? I rush over to Pine and take a look:

Return Path: <santa@north.pole.com>

Well, how very nice to allow me to use my fake address.

Received:
from atropos.c2.org by nmia.com
with smtp
(Linux Smail3.1.28.1 #4)
id m0ueqxh 000LD9C; Fri, 12 Jul 96 16:45 MDT
Apparently To: <cmeinel@nmia.com>
Received: from satan.unm.edu (cmeinel@plato.nmia.com [198.59.166.165])

Oh, how truly special! Not only did the computer atropos.c2.org blab out my true identity, it also revealed that satan.unm.edu thing. Grump... that will teach me.

by atropos.c2.org (8.7.4/CSUA) with SMTP id PAA13437 for cmeinel@nmia.com; Fri, 12
Jul 1996 15:44:37 0700 (PDT)
Date: Fri, 12 Jul 1996 15:44:37 0700 (PDT)
From: santa@north.pole.com
Message Id: <199607122244.PAA13437@atropos.c2.org>

Oh, crap!

So, the moral of that little hack is that there are lots of different email programs floating around on port 25 of Internet hosts. So if you want to have fun with them, it's a good idea to check them out first before you use them to show off with.

Want to share some kewl stuph? Tell me I'm terrific? Flame me? For the first two, I'm at cmeinel@techbroker.com. Please direct flames to dev/null@techbroker.com. Happy hacking!
