GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

January 28, 2001 - Angelique Naylor, CISSP, MCSE

Diary of a self proclaimed security guru and self made hacker – an **unauthorized** Carolyn Meinel story:

Carolyn Meinel seems to be a very interesting woman. I say "seems" since I have never actually met her, talked to her, or even received an email from her. Yet, at 52, she is somewhat of a cult classic hero with some security industry gray hairs and many middle school age hacker neophytes. She is the author of at least two books *The Happy Hacker* and *Überhacker* and publishes a subscription called "*GUIDE TO (mostly) HARMLESS HACKING."*

She operates a site called "The Happy Hacker" – www.happyhacker.org[1] -, which offers hours of entertaining reading and some pretty useful security information to boot. At one time I thought the site offered a "safe" hacking practice zone, but I have been unable to locate that zone in the past few months. In an interview, she created the following description about her site: "We provide hands-on instruction in old-fashioned, mostly harmless computer hacking. This includes computer break-in games. We oppose computer crime and make fun of the computer crime subculture. Consequently, computer criminals hate us…"[5]

While many security professionals laud her work, over the years she managed to piss off some very angry young script kiddie punks (you know the kids who say Fu%# every other Fu%#ing word). Additionally, she has incurred the wrath of attrition.org, a well-known hacker hangout. http://www.attrition.org/shame/info.html[2] - in this article they publish details about Carolyn's alleged involvement in the September 13, 1998 website hack against the New York Times. Apparently, she was implicated by the FBI as a suspect, was questioned, refused a lie detector test, and was let go. None of my research has led me to believe that she was in any way involved with the HFG (Hacking for Girliez) gang that took credit for the NY Times hack.

When I need a good laugh, I curl up with a few good episodes of "*it sucks to be me*" – the section of her website in which Carolyn pokes fun at the morons who write to her for criminal hacking advice. She publishes the complete details of the emails along with her responses. It really is quite amusing…what people ask her to help with – anything from hacking a spouses email password, to breaking into financial networks, etc.

Many security professionals visit her website on a regular basis to obtain breaking news on hacker exploits, interesting security articles, and links to other security related sites. However, many hackers, crackers, and script kiddies also visit the site. Some of them come to see if Carolyn has published any information about them, others (especially script kiddies) to see if any new techniques and articles have been posted.

Several hacker / cracker organizations have joined forces in protesting her site (and even Carolyn personally): "http://happyhacker.org/news.html has links to news stories and commentary about the hacker war that has tried and failed to run us off the Internet."[5]

During my research, I pulled up a ton of angry emails, letters, and rants from the hacker community against Ms. Meinel. Here is one of the milder examples I found:

© SANS Institute 2000 - 2005 Author retains full rights.

[scr] Trinka Porrata should hook up with Carolyn P. Meinel [3]

Scott Beam scott@nokturnal.com
Tue, 9 May 2000 15:15:21 -0700

"Neither one of 'em know jack sh*% about the crusades they're fighting. But each are regarded as some kind of "experts." Whoever's responsible for deciding who the experts are needs a remedial lesson in common sense."

In her "Guide to Mostly Harmless Hacking", she comments a little on some of the "flames" she has received from the hacker community. Below is a "newbie note" in which she introduces the concept of flaming to interested readers who are new to the world of hacking:

"It is a bunch of obnoxious rantings and ravings made in email or a Usenet post by some idiot who thinks he or she is proving his or her mental superiority through use of foul and/or impolite language such as "you suffer from recto cranial inversion," f*** y***, d****, b****, and of course @#$%^&*!" [4]

Her MOTTO: Better living through (mostly) harmless hacking.
EDUCATION: MS, Industrial Engineering, U of Arizona
Thoughts on HACKERS & CRACKERS:
"The basic difference is, hackers build things, crackers break them."[5]

Carolyn's first book, The Happy Hacker, was published in 1998. The book has undergone several revisions (the third edition is now out, up to 428 pages from the 263 pages of the first edition).
I have searched numerous websites looking for this book and have been told everything from "it's out of print" to "3 weeks shipping time" for even a used version. I'm not sure who is buying up the most copies, security professionals looking to protect their computers and networks, or newbie hackers and wannbes looking for a quick score on how to break into systems.

According to her website, she has written five other technical books and is a co-founder of the L-5 Society an organization now known as the National Space Society. Her site also claims that "*The Happy Hacker* is…written in non-technical language…gives the reader a Black Belt in digital self defense."[1]

Ms. Meinel runs a high tech consulting business out of her home and updates the late breaking hacker news almost daily (the website says that it is updated every 15 minutes, but I have not verified the validity of that statement). She claims to be the only "over 50 year old woman hacker" in the world and I'll bet she is probably right. My mother is 49 and won't come near a computer.

In an article / interview by Verbosity, she shares a little insight into how she entered the world of hacking and teaching others to hack:

CM: All sorts of guys were begging me, "Teach me how to hack." I'm an industrial engineer (MS, U of Arizona, 1983). I believe in efficiency. Instead of teaching all these guys one-on-one, I figured I'd set up a production line. Also, a bunch of elite hackers joined the list so they can show off how brainy they are. So they end up doing most of the work. I'm learning more than I

© SANS Institute 2000 - 2005 Author retains full rights.

teach.[6]
Ms. Meinel has written several articles for e-zines such as antionline.com – two of which are titled "*The Granny Hacker From Heck,"* and *"Granny Hacker visits DefCon."* She claims to have gotten her start in hacking during the 1995 DefCon III conference when she found a live phone line and telneted into a shell account. Additionally, in an article for antionline.com, she mentions famed hacker Brian Martin (Jericho) as one of the "victims" in her pursuit to bring computer criminals to justice.[7]

Mr. Martin has subsequently replied with several attacks against her, and has written many public retorts to her in his own defense against some of her accusations. Carolyn claims not to hate this young man, in fact she jokingly calls him her "PR agent" – each time he mentions her name, someone buys a copy of one of her books. It sounds like a classic "love/hate" relationship to me – each of them continues to feed off the other. Each time one of them writes an article, it fuels the fame and notoriety of the other.

So how did this mother of four, horse rancher, granny, and industrial engineer become an information security superhero / guru / and fighter of cybercrime? Her resume is checkered with a number of activities – not very many of her job titles were directly related to information security (attrition.org claims that she has made at least 17 career changes). Regardless of not having years of direct security experience, she has written quite few articles and has been sited / quoted as an information security expert by several in the technical media circles. While doing a simple search on "Carolyn Meinel" through search engine www.google.com, I found over 2,000 references to her name. Many of the links lead to angry hacker posts and ridiculous flames from adolescent teenage boys who claim to be elite hackers.

Many hackers have bashed her expertise and say that she is neither an expert in the subject of hacking nor security. They go on to say that her books and recommended hacking techniques are flawed. (see reference to attrition.org articles). As far as I know, she does not have any formal security certifications (none that are indicated on the site or mentioned in her credentials section). She is often sought after by technology magazines to do security related interviews, or to comment on successful hacks / hack attempts. Her resume lists her as a columnist for MessageQ magazine – writing on security and business, a Beta tester for the BRICKServer secure operating system, and owner of the Happy Hacker website.

Here is the rest of the resume she posts on her website[1]:

> In 1999, worked on the DARPA Intrusion Detection Evaluation program, MIT Lincoln Lab, researching Windows NT exploits.
> Owner of the Happy Hacker web site, which is viewed by an average of some 10,000 distinct hosts per day. (Site traffic audited by Burst Media.)
> Wrote How to Meet Your Future Most Valued Employee for the Oct. 1999 issue of **Info Security** magazine, the world's highest circulation computer security magazine.
> Wrote "How Hackers Break in and How they Are Caught," **Scientific American**, Oct. 1998, pp. 98 -- 105; and **The Happy Hacker: A Guide to Mostly Harmless Computer Hacking,** currently in third edition, 400 pages, American Eagle Publications, 1998. Her latest book, ***Überhacker!***, was published Oct. 2000 by Loompanics.
> Performed denial of service vulnerability tests for Interpact, Inc.

© SANS Institute 2000 - 2005 Author retains full rights.

Assisted Computing Devices International (now part of General Dynamics Information Systems and Technology) in winning a contract for payload computers for the Teledesic communications satellite constellation. [1]

Regardless of anyone's personal opinions, the happyhacker.org site does provide many security professionals and network administrators with valuable security information that can be used to protect their own systems and networks from attack. Here are some of the sections of her website[1]:

Happy Hacker Digests - The Happy Hacker Digest is a moderated list for discussions of legal hacking.
Hacker Links - Small list of other hacking sites
Hacker Wargames – A listing of sites offering reward money for hackers to test their security mechanisms
Help for Beginners – A list of various topics such as hacking Macs, Unix, and Windows
Hacker Bookstore – Various resources on hacking, hacker culture, and computer crime / laws
It Sucks to Be Me! – Moronic requests from people soliciting Carolyn's help in illegal hacking
Self Defense – Links, books, and more information about how to protect computers from cyber criminals
How to Commit Computer Crime! – Misleading title to a section on computer crime law and a disclaimer about how her site "might" teach you things that would allow you to break the law – She does not advocate breaking the law and is very clear about that in many places throughout the site
Software for Hackers – Seems to be a push for Linux and barnesandnoble.com (affiliate store)
News from the Hacker WarFront – Many articles pointing to famous hackers and their many publicity stunts (guess what, more publicity for Mr. Brian Martin).

Apparently there have been several attempts by hackers to deface the happyhacker.org website. Carolyn has been attributed with the following quote: "Hackers wanting to protest my Web site are just plain out of luck. These digital vandals have hacked the White House, New York Times, NASA, and many other web pages with protests against me -- but they haven't been able to touch my Web site since implementing BRICKHouse." -- Carolyn Meinel, 5/18/99 [8]

It has long been said that in order to protect ourselves from computer criminals, we need to arm ourselves with as much information about their tactics and culture as possible. Carolyn's site does do a good job of providing such information.

Some may argue that providing so much detailed information about hacking is dangerous and further propagates the risk that malicious hackers will use the information available to wreak more havoc. Deciding whether providing information on hacking to the untrained public is exactly ethical is beyond the scope of this paper and a matter of personal opinion left up to the reader.

Sited sources:

1). www.happyhacker.org
Carolyn's cult classic website on "safe" hacking practices

2). http://www.attrition.org/shame/info.html

© SANS Institute 2000 - 2005 Author retains full rights.

Attrition.org article blasting Carolyn for a number of practices

3). http://www.socal-raves.org/archives/scr/Week-of-Mon-20000508/004567.html
Quote from "Scott" – an apparently irritated script kiddie punk

4). *GUIDE TO (mostly) HARMLESS HACKING - Beginners' Series Number 4*
Per Carolyn's request at the end of the guide, I am including this copyright notice:
Copyright 1997 Carolyn P. Meinel. You may forward or post this GUIDE TO (mostly) HARMLESS HACKING on your Web site as long as you leave this notice at the end.

5). Subject: Interview w/ Carolyn Meinel -
http://www.siliconsalley.com/archive/carolmeinel.html

6). Verbosity Interview - verbosity -- Carolyn Meinel: Hack 101
The interview was conducted via e-mail by Jess Morrissette

7). http://www.antionline.com/cgi-bin/News?type=antionline&date=02-22-1999&story=granm.news - The Granny Hacker from Heck article

8). http://www.genocide2600.com/~tattooma/quotes.txt - Lists several quotes attributed to Carolyn on the famous hacker site 2000.com

© SANS Institute 2000 - 2005, Author retains full rights.