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: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Hackers and Crackers: Who can we trust?

By Chad Sehn

The advent of the personal computer has brought about a new war; it is one that is fought without boundaries and knows no fear. It is fought by people who sit behind computer screens, faceless to their enemies. Some are ever persistent in the latest conquest. Some are vigilant against the latest attack.

You hear it in the news almost every day. Websites, corporations and even governments, "hacked" into, websites defaced, or Denial of Service (DoS) attacks, perpetrated by some "hacker". They have colourful names like "Mafiaboy", "Disorder", "Cap'n Crunch" and "Condor". All of them have contributed to the security of the Internet and networks, some honestly, some not so honestly.

The media labels them as "Hackers", bent on causing disruption and/or destruction. Hackers label them "Crackers". Which one is which, and who can be trusted?

To truly understand the difference we first have to define the terms. For the purpose of this paper we will use the definition provided by Net Sams[1]:

- A *hacker* is a person intensely interested in the arcane and recondite workings of any computer operating system. Most often, hackers are programmers. As such, hackers obtain advanced knowledge of operating systems and programming languages. They may know of holes within systems and the reasons for such holes. Hackers constantly seek further knowledge, freely share what they have discovered, and never, ever intentionally damage data.

- A *cracker* is a person who breaks into or otherwise violates the system integrity of remote machines, with malicious intent. Crackers, having gained unauthorized access, destroy vital data; deny legitimate users service, or basically cause problems for their targets. Crackers can easily be identified because their actions are malicious.

To break these down to the simplest form we could say that a hacker is basically a programmer who has "a desire to better what now exists."[1] A true Cracker creates nothing and destroys much[1].

Cracking involves persistence and the dogged repetition of a handful of fairly well known tricks that exploit common weaknesses in the security of target systems. Accordingly, most crackers are only mediocre hackers.[2]

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

To the security professional it would seem fairly black and white. However, with the misuse of the terms by the Media, these terms seem to have interchangeable meanings. This does not help the general public to discern the differences.

So, to the question at hand, who can be trusted? Before we answer that, it may be helpful to look at some examples.

- Dennis Ritchie and Ken Thompson. Together they created UNIX in 1969. Ritchie also authored the C programming language.[3]
- John Draper, also known as Cap'n Crunch. He figured out how to make free phone calls using a plastic prize whistle he found in a cereal box. He introduced generations of hackers to the concept of phone "phreaking." [3]
- Kevin Mitnick, also known as Condor. He has the distinction of being the first hacker to be on the FBI's ten most wanted list for his computer crimes. His activities ranged from coping proprietary software to stealing ISP services.[4]
- MafiaBoy. He is known for his alleged denial of service (DoS) attacks on some well known websites such as CNN, Yahoo and others.[5]

These are just a few examples of hackers and crackers. They show some good and some bad. For the sake of argument, the hacker "could" be thought of as a "good guy". This is the person that will find a security hole and let the software makers know about it so it can be patched. Hackers have created some of the best tools available to security professionals. L0pht Heavy Industries is a prime example of hackers coming together to create programs for the benefit of security on the Internet and internal networks. They work towards "understanding the problems at hand and becoming able to address them 'before the fact'"[6] and making the knowledge available to those who want it to better secure their own computer systems.

The cracker will let other crackers know so that they can exploit it for their own means. They have websites available with tools and scripts to exploit known weaknesses, not to help secure or correct a problem but to create them. They work towards destruction, to bring down a large website or to deface it. The motivation is not important, just the end result.

Now enter into the equation a new breed, the "reformed" hacker. This new type furthers to cloud the issue. An example of this new breed is Kevin Mitnick (also known as Condor). Recently he was invited to be the keynote speaker at a conference hosted by Giga Information Group. In a press release from Giga, they feel "…his perspective is important as organizations must be able to understand the hacker mind-set in order to effectively combat unauthorized access and hacker attacks."[7] Can the "reformed" hackers be trusted? That is a question that has yet to be answered.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Who can you trust? Both hackers and crackers have a vast amount of information at their fingertips. They all can find the resources to defend or attack, the question is now down to a matter of ethics. An ethical person would not launch an attack against a website or try to capture passwords for their own gain.

The answer to the question is not a simple one. Still, if you look at the definitions of each, and relate that to the actions and accomplishments – good or bad -, it is possible to associate them to a group. This could work in most cases, some hackers jump back and forth. There is no sure way to tell if you can trust either.

The best advice is to be skeptical of everyone. Double check information. We also have a vast amount of information at our fingertips. It is, in the end, your security or the security of your network that is at stake.

Bibliography

1: Sams, Net. “Maximum Security: A Hackers Guide to Protecting your Internet site and Network”. 6 June 1997. URL: http://www.itknowloedge.com/referance/archive/1575212684/ch03.htm (14 Aug. 2000)

2: Raymond, Eric S. “Jargon File Resources” 4.1.2 version, Spring 1999. URL: http://murrow.journalism.wisc.edu/jargon/jargon_17.html#SEC24 (14 Aug. 2000)

3: Slatalla, Michelle. “Hackers Hall of Fame” URL: http://www.discovery.com/area/technology/hackers/hackers.html (15 Aug. 2000)

4: Shimomura, Tsutomu. “Takedown: The Pursuit and Capture of America's Most Wanted Computer Outlaw -- By The Man Who Did It” with John Markoff. (January 1996). URL: http://www.takedown.com/ (16 Aug 2000)

5: Reuters. “'Mafiaboy' hacker faces 64 new charges, pleads not guilty” August 4, 2000 Web posted at: 9:50 a.m. EDT (1350 GMT) URL: http://www.cnn.com/2000/TECH/computing/08/03/crime.mafiaboy.reut/index.html (16 Aug. 2000)

6: L0pht heavy industries. “L0pht web site to Merge with @stake web site.” 7 Jul. 2000. http://www.l0pht.com/ (16 Aug. 2000)

7: Kitchen, David. “Kevin Mitnick to Speak on Corporate Security and the Internet at Giga Information Group Conference” 31 July 2000. URL: http://www.gigaweb.com/Content/Adhoc/RAH-072000-00036.html (16 Aug. 2000)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.