Global Information Assurance Certification Paper

Hackers: Sleeping With The Enemy

Michael Whalen

October 15, 2001

"Hackers": We have all heard of them-- now more so than ever before. To most of the American public, the term conjures up visions of malevolent, unsavory characters clad in black that work to undermine the very principles of democracy, utilizing their underground knowledge of computing and sophisticated equipment to break into computer systems and wreak havoc. Hollywood has played its part in furthering this misconception by using second-rate actors, who have no comprehension of technology, to portray these individuals as the players of some fantastical arcade game of good vs. evil. Bottom line: hackers are criminals to the general public.

As Information Security professionals, we defend against hackers on a daily basis—they are our archenemies—or are they? To the contrary, I will demonstrate the importance of hackers & hacking to the Information Security Community and how they have been an invaluable asset to the InfoSec community and the American public as a whole in furthering the awareness and importance of information security.

Are you a Hacker?

I'll begin by defining the term "Hacker". Definitions of the term "Hacker" vary by source, as does the implied intent of the hacker.

Webster's Dictionary defines "hacker" as follows:

Hacker: (noun)

1. A person who is inexperienced or unskilled at a particular activity
2. An expert at programming and solving problems with a computer
3. A person who illegally gains access to and sometimes tampers with information in a computer system.

The Free Online Dictionary of Computing defines "Hacker" differently:

Hacker n. [originally, someone who makes furniture with an axe]
1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. 2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming. 3. A person capable of appreciating hack value. 4. A person who is good at programming quickly. 5. An expert at a particular program, or one who frequently does work using it or on it; as in `a Unix hacker'. (Definitions 1 through 5 are correlated, and people who fit them congregate.) 6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example. 7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations. 8. [deprecated] A malicious meddler who tries to discover sensitive information by poking around. Hence `password hacker', `network hacker'. The correct term for this sense is cracker.

Obviously, depending which side of the fence you are on, the legal implications of the hacker and their activities differ; otherwise, the descriptions are fairly similar and straightforward. For the sake of argument, we'll compromise: Both definitions (one, a literal and the other contextual) agree that a Hacker is an "expert with computers", both in "programming" and in "solving problems". Moreover, a hacker enjoys "circumventing and/or overcoming limitations". So then, it would be safe to say that in the context of information security, for the purposes of

this argument, a hacker is an individual who is skilled in computing that enjoys defeating or circumventing security systems—their intent notwithstanding.
As an information security professional, are you not trained to audit your passwords using "Hacker Tools"? Have you ever conducted a port scan? Are you in possession of software or code that could be used to disrupt or otherwise damage communications? Have you attempted to exploit vulnerabilities on a system, be it for the purpose of learning how to defend against it, or to see how it is done? If so, are you not a hacker? By definition, indeed you are. "Reformed" or "white-hat" hackers are often hired by companies to secure their networks for them. What better person to secure it than the one who broke it?
Securing your network is a hands-on effort. It is impossible to effectively secure a network by merely following instructions from a checklist. Every network implementation is unique and demands a unique security policy and practice. We must study our adversaries, much as we do in warfare, so that we might find a method to defeat them. Failure to do so could lead to disaster. How could we expect to defend ourselves against a threat without knowledge of how it works? In using and understanding the tools and tactics of the opposition, one is better prepared for an attack--especially attacks from novice "script kiddies" who use tools readily available on the Internet. Knowledge is power.

So how are hackers beneficial to the InfoSec community?

Hackers expose vulnerabilities and have raised the expectation of software quality.

Software today ships with a preposterous amount of vulnerabilities, (and no warning of this) right out of the box. To an uneducated user, this could spell disaster within minutes of connecting to the Internet or a network. Some vendors, in the name of functionality and operability, sacrifice security for ease of use, compounding this dilemma.
Software companies, especially those who monopolize the industry, are most concerned with making their product function adequately to sell—on time, and worry about other issues after distribution, if and when users bring them to their attention. Through service packs and subscription services, which they often sell at an additional price, or require advanced knowledge to locate, they take the steps to begin to properly secure the information handled by their product. The additional time required to do this during production often outweighs the profit from the sale. Furthermore, it would be nearly impossible to construct a facility in which to test the product in every implementation. Moreover, when 80% of the country uses your software and doesn't know how to operate a computer without it, there won't be much resistance. So where do these companies or the InfoSec community obtain knowledge of the vulnerabilities in these products? Hackers disclose them, (publicly or privately) or by users who have been compromised by hackers.

Hackers Have Increased Awareness of the Need for an Online Security Standard

The presence of Hackers & Hacking on the Internet and the inherent risk they pose forces companies to implement and maintain a standard of security that would otherwise be disregarded. For example, the successful compromises of major e-commerce companies' customer and credit card databases has dictated an need for a security standard that will protect the identity and assets of consumers—something that should have been done in the first place.

Hence, the birth of SSL, Digital Certificates, PKI, etc. Though a national standard has not yet been adopted, many organizations have instituted their own policies in attempts to instill faith in consumers. This breeds competition as failure to offer this quality of service would put you at a disadvantage to a company that does.

Hackers Stimulate Economic Growth

The presence and activities of Hackers has prompted the growth of new industry, namely Information Security, especially over the past few decades. In the early days of the Internet, little attention was paid to security as the main concern was the availability of data. In the mid 90's, when the number of Internet Users soared from less than 10,000 in 1994 to over 120,000,000 today, the percentage of online commerce transactions also skyrocketed. Likewise, the percentage of computer crime and malicious Internet traffic followed.
In the consumer market, this led to the development of anti-virus software, personal firewalls, desktop encryption and other consumer software such as PGP and McAfee.
In the corporate market, this led to a need for Information Security Specialists, enterprise security solutions, Security Training, offsite storage, etc.
Currently, biometric authentication is on the horizon in response to the successful circumvention of the aforementioned security products, and with the occurrence of the September 11th attacks, there couldn't be any more of a need for security.

Hackers Influence Politics and Worldly Affairs

We hear about a new virus or attack on an almost daily basis in today' world. Oftentimes, these attacks are dismissed as "a few teenagers with nothing better to do" out of ignorance or fear. However, there are often strong political motivations behind these attacks and many times, they are highly organized and sophisticated. These hacker activists or "hacktivists" use the Internet as their means of attack, quite successfully and often anonymously. Hacktivism is defined as "hacking, phreaking or creating technology to achieve a political or social goal." That's all well and good, but how effective is it? Very.

"On the eve of Sweden's general election, Internet saboteurs targeted the Web site of that country's right-wing Moderates political party, defacing pages and establishing links to the homepages of the left-wing party and a pornography site." (Wired 9/22/98)

Hacktivist groups have been successful in making their point in many instances, most recently with the Taliban. Dissatisfied with the US Government's response to the recent terrorist attacks, a group of vigilante hackers known as "The Dispatchers" recently brought down the Taliban's website, the official website of the Presidential palace of Afghanistan and other sites related to the Afghanistan regime.
YIHAT (Young Intelligent Hackers Against Terrorism), a European hacktivist group led by Kim Schmitz (The wealthy German tycoon who recently offered a $10mil bounty for Bin Laden) claims they are fighting terrorism by searching for hidden Taliban bank accounts, the locations of which, they have purportedly divulged to the FBI, though they refuse to comment.
Hacktivism is an effective device that, when used correctly, could seriously affect the well being of an offending organization.

Hackers and computer criminals to date have largely managed to escape the grasp of the law, save for the few classics. However, since the attacks of September 11th, legislation has been passed making certain computer crimes acts of "cyber terrorism". Though the definition of what exactly constitutes cyber terrorism is broad, it is basically outlined as any hacking attempt that totals at least $5000 in damage within one year, any damage to medical equipment or "physical injury to any person", punishable by 5 to 20 years imprisonment. In their own manner, the true hackers, who adopt and follow the hacker ethic have managed initiate and have approved, legislation that will weed out the majority of malicious Internet traffic, generated by novices and "script kiddies" legally. Of course, the elite, who operate in clandestine sects, utilizing proprietary tools and methods will always exist and rarely be apprehended, working in the shadows to carry out their covert agendas…and in the daytime, get back to work as "Security Professionals".

Hackers and their ongoing efforts mandate vigilance (and keep us employed.)

In becoming an Information Security Professional, it is imperative to be knowledgeable of known vulnerabilities and exploits, policy implementation, offensive and defensive tools, encryption, etc. However, one of the often-overlooked aspects of security is the historical significance of our opposition. Security became necessary because of a compromise, and the inherent threat of another, thereafter. Likewise, our methods and tactics of security have been developed from past mistakes. Information Security is an iterative process; therefore, it is important to understand the threats we are dealing with so that we might have a better understanding of how to protect against them, without repeating the same mistakes that others have made.

Hackers and hacking created a need for information security—and hence, our employment. Moreover, the continued existence of malicious code/traffic mandates constant vigilance (and continued demand for Security Professionals.
Complacency, I feel, is the single most contributing factor to the failure of policy, no matter how well crafted.

Example:
The terrorist attacks of September 11th have brought to light many inadequacies in our National security that, for decades, have gone unrecognized and/or overlooked. Since the attack on Pearl Harbor over half a century ago (The only other time we have been attacked on our soil since becoming the United States), our nation has gradually lulled itself into a dangerous complacency in regards to security, on both a national and a personal level. This complacency resulted in a failure of our policy and hence, the successful execution of an attack on well-known vulnerabilities in our system that could, and should have been prevented.
The United States has been the leading Military power in the world for almost a century. We pride ourselves on our National Security and our Armed Forces. We possess some of the most sophisticated military equipment in the world. How and why were we then successfully attacked? Because since Pearl Harbor, there was no significant event that took place to warrant continued efforts of security and or disaster preparation. Over the past 50 years, there has been a steady decline in military funding and enrollment in the Armed Forces is at an all time low.

Now that something has happened which exploited our vulnerabilities, we are revising our policies and reallocating resources to the level they should have been at prior to September 11th. In a similar fashion, well-known vulnerabilities are exploited on a daily basis by elite hackers as well as novice "script-kiddies", using tools and instructions readily available on the Internet. Leading corporations, government agencies, military and even information security companies are compromised by vulnerabilities that have been disclosed to the public for over a year, resulting in loss of business, a tarnished reputation and in some cases, bankruptcy. Time is money in today's world. Even a few minutes of downtime could spell disaster for some of the major e-commerce companies.
With so much at stake, it is often mind-boggling that companies and even our own government cannot justify the money or the time to properly secure their infrastructure until an incident takes place. Prior to September 11th or the Nimda worm, one might have commented that there hadn't been a significant event whose effects were so disastrous that it would warrant a revision of policy. However, many companies learned the hard way from the World Trade Center disaster. The importance of security policy and disaster recovery plans became shockingly apparent. But how long will that last? Policy is useless without proper and continued implementation

Conclusion

As Information Security Professionals, our livelihood rests on the basic principle that there is an imminent threat from an often-invisible adversary: the hacker. Mitigating that threat allows one to remain online and hence, competitive. Our job, thus far, has been to define and protect against this threat with acquired knowledge, hardware, software, policy implementation, auditing and iterative revision. As long as there are hackers, there will be a threat to the integrity, confidentiality and availability of the information we protect. It is our job to learn from our adversaries and experiences and attempt to acquire the knowledge that they possess; understand and accept the integral role that they play in the Information Security Industry, all the while maintaining constant vigilance.

Sources:

Forno, Richard "You say "Hacker", the Feds say "Terrorist", Nov 20 2001
URL: http://www.securityfocus.com/cgi-bin/columnists-item.pl?id=38&msg=9052#MSG

The Free Online Dictionary of Computing
URL: http://www.foldoc.org

Graham, Jefferson "Hackers Strike Middle Eastern Sites" Oct 2 2001
URL: http://www.usatoday.com/life/cyber/tech/2001/09/19/hack-attack-launched.htm

Heller, Martha "Would you Hire a Hacker?" CIO Magazine, Sept 1, 2000.

MacDonald, Tim "Hackers Mobilize For War Against Islaamic Websites" Sept 17 2001
URL: http://abcnews.go.com/sections/scitech/DailyNews/strikes_hacker_yihat_011015.html

Olsen, Eric "Hacking for the Cause", Nov 15 2001

URL: http://abcnews.go.com/sections/scitech/DailyNews/strikes_hacker_yihat_011015.html

Schwartz, Matthew "For Hire, Hackers to help Pentagon Preven Attacks" Aug 1, 2000
URL: http://www.cnn.com/2000/TECH/computing/08/01/pentagon.at.defcon.idg/

USA Patriot Act Congress HR 3162 RDS (courtesy of Electronic Frontier Foundation)
URL:http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011025_hr3162_usa_patriot_bill.html

Webster's Online Dictionary
URL: http://www.m-w.com/dictionary.htm

Last Updated: September 20th, 2017

Upcoming Training

SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401*	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Minneapolis, MN	Oct 03, 2017 - Nov 14, 2017	Mentor
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401*	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401**	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event