How to Become an Ethical Hacker

Not all hackers do evil work. Here's what you need to know to use your hacking skills to do good.

By Eric Geier, PCWorld  Feb 15, 2012 9:00 pm

Do viruses, DDoS attacks, or buffer overflows tickle your fancy? If so, you might consider becoming a legal hacker, aka an ethical hacker, "white hat" hacker, or penetration tester.

Businesses and government-related organizations that are serious about their network security hire ethical hackers and penetration testers to help probe and improve their networks, applications, and other computer systems with the ultimate goal of preventing data theft and fraud. You may not get the same adrenaline rush that you might with underground hacking, but you can earn a good and honest living—and not end up facing prison time, as some illegal "black hat" hackers do.

How does the job market look like for ethical hackers? Extremely good! The IT market overall continues to grow despite the current economic turmoil. Research firm Gartner estimates that worldwide enterprise IT spending grew by 5.9 percent between 2009 and 2010, to a total of $2.7 trillion. At the same time, security is becoming a more pressing concern. Gartner expects to see an increase of nearly 40 percent in spending on worldwide security services during the five-year period from 2011 to 2015, eventually surpassing $49.1 billion.

In your first years as an ethical hacker, you'll be in a position to earn anywhere from $50,000 to $100,000 per year, depending on the company that hires you, and on your IT experience and education. With several years of professional experience, you could command $120,000 or more per year, especially if you do your own independent consulting.

You can't just dive into an ethical hacker position, however. Without IT security experience, you won't get very far, even with degrees and certifications. As is true for other IT jobs, employers typically want candidates who have college degrees, but related experience is king. And experience with certifications can typically take the place of some degree requirements.

Getting Started

What you need to do to get started on the road to becoming an ethical hacker depends on where you are in the IT field. If you haven't started your IT career yet, you might even consider military service. The military offers many IT opportunities, and you get paid to go to school, even if you enlist in a part-

www.pcworld.com/article/250045/how_to_become_an_ethical_hacker.html#tk_nlp_spx_h_cbintr
time branch such as the National Guard or Reserves. Military service also looks good to employers that require security clearances.

Start with the basics: Earn your A+ Certification and get a tech support position. After some experience and additional certification (Network+ or CCNA), move up to a network support or admin role, and then to network engineer after a few years. Next, put some time into earning security certifications (Security+, CISSP, or TICSA) and find an information security position. While you're there, try to concentrate on penetration testing--and get some experience with the tools of the trade. Then work toward the Certified Ethical Hacker (CEH) certification offered by the International Council of Electronic Commerce Consultants (EC-Council for short). At that point, you can start marketing yourself as an ethical hacker.

For a hacker, networking know-how is vital; but make sure that you gain experience in related areas as well. Discover and play with Unix/Linux commands and distributions. Make sure you also learn some programming—maybe C, LISP, Perl, or Java. And spend some time with databases such as SQL.

Soft Skills
Hacking isn't all technical. It also requires so-called soft skills, just as any other IT job does. You'll need a strong work ethic, very good problem-solving and communications skills, and the ability to say motivated and dedicated.

Ethical hackers also need street smarts, people skills, and even some talent for manipulation, since at times they need to be able to persuade others to disclose credentials, restart or shut down systems, execute files, or otherwise knowingly or unknowingly help them achieve their ultimate goal. You'll need to master this aspect of the job, which people in the business sometimes call "social engineering," to become a well-rounded ethical hacker.

Stay Legal!
It's important never to engage in "black hat" hacking--that is, intruding or attacking anyone's network without their full permission. Engaging in illegal activities, even if it doesn't lead to a conviction, will likely kill your ethical hacking career. Many of the available jobs are with government-related organizations and require security clearances and polygraph testing. Even regular companies will perform at least a basic background check.

Becoming a Certified Ethical Hacker (CEH)
As noted earlier, becoming a Certified Ethical Hacker (CEH) involves earning the appropriate credential from the EC-Council after a few years of security-related IT experience. The certification will help you understand security from the mindset of a hacker. You'll learn the common types of exploits, vulnerabilities, and countermeasures.

Qualification for a CEH (a vendor-neutral certification) involves mastering penetration testing, footprinting and reconnaissance, and social engineering. The course of study covers creating Trojan horses, backdoors, viruses, and worms. It also covers denial of service (DoS) attacks, SQL injection, buffer overflow, session hijacking, and system hacking. You'll discover how to hijack Web servers and Web applications. You'll also find out how to scan and sniff networks, crack wireless encryption, and evade IDSs, firewalls, and honeypots.

Through approved EC-Council training partners, you can take a live, five-day onsite or online training course to prepare for the CEH cert. You can generally take live online classes over five consecutive days; onsite courses typically offer the content spread over a couple weeks for locals. In addition,
you can take self-paced courses and work with self-study materials (including the CEH Certified Ethical Hacker Study Guide book) with or without the training courses. The EC-Council also offers iLabs, a subscription based-service that allows you to log on to virtualized remote machines to perform exercises.

The EC-Council usually requires that you have at least two years of information-security-related work experience (endorsed by your employer) in addition to passing the exam before it will award you the official CEH certification.

Resources

If you're interested in ethical hacking, you can consult many useful resources for more information. To start, check the resources section of the EC-Council site. A quick Amazon search will reveal many books on ethical hacking and the CEH certification, as well.

With some googling, you can find simple hacking how-tos, which may motivate you even more. Consider downloading the Firefox add-on Firesheep or the Android app Droidsheep, and hijack your online accounts via Wi-Fi (but don't use these tools to hijack others' accounts—you could find yourself in legal trouble if you do).

Another option is to experiment with the BackTrack live CD. Try enabling WEP security on your wireless router at home, and then take a stab at cracking it. Check out Hack This Site to test and expand your skills. You could even set up a Linux box with Apache or buy a used Cisco router and see what you can do with it. If you want to play with malware, consider downloading—cautiously, and at your own risk—a malware DIY kit or a keylogger, and use it to experiment on a separate old PC or virtual machine.

Like other IT areas, hacking has conventions and conferences dedicated to it, such as DefCon, one of the oldest and largest of these. Such gatherings can be a great place to meet and network with peers and employers, and to discover more about hacking. DefCon also has affiliated local groups in select areas.

And remember, never attack or intrude on anyone else's network or computers without full written permission.

Eric Geier is the founder of NoWiresSecurity, which helps businesses easily protect their Wi-Fi networks with the Enterprise mode of WPA/WPA2 security by offering a hosted RADIUS/802.1X service. He is also a freelance tech writer—become a Twitter follower or use the RSS Feed to keep up with his writings.

Would you recommend this story?  YES 27  NO 3

Recommend: Like 21 52 3 73 Email 0 Comments Print

Sponsored Links

BlackBerry® Smartphones
Make the most of every moment with the latest BlackBerry smartphones.
BlackBerry.com

Overstock iPads: $23.47
Get 32GB iPads for $23.47. Limit 1 Per Customer. Get yours today!
ipadsforcheapnow.com

No Contract Smartphones
The Best Deals On The Best Phones - No Contracts. Learn More Now
Incredicell.com

Robots Like Us
You will too. 50-90% off local fun, new adventures & more. Try us!
www.Groupon.comSign-Up
Today's Special Offers

Panasonic Toughbook? mobile computers.
Panasonic Toughbook? computers deliver rugged and reliable performance and can withstand the rigors of your workday.

Technology for Tomorrow's Cloud
Help Secure Your Cloud with Intel® Technology

Brother printers rated #1 in reliability
See why PC Mag readers gave Brother the #1 overall rating for printers. Again.

Introducing the EPSON WorkForce Pro.
The World's Fastest 2-sided inkjet small business printer.

Experience the MAINGEAR Difference
Discover the MAINGEAR SHIFT with Super Stock options, overclocked, liquid cooled and specially painted just for you.

Release the Doer in You
$50,000 Prize plus Lenovo laptops and Amazon Gift cards.

Synology Reliable NAS for Every Budget
For home or business, Synology DiskStations provide reliable backup, file sharing, streaming & more.

Brother printers rated #1 in reliability
See why PC Mag readers gave Brother the #1 overall rating for printers. Again.

Experience the MAINGEAR Difference
Discover the MAINGEAR SHIFT with Super Stock options, overclocked, liquid cooled and specially painted just for you.

Dice - The Career Hub of Tech
Dice - The Career Hub of Tech

Capture Competitive Advantage with Windows Embedded
See how one Texas hospital is saving $50,000 and seeing 1,500 more patients each year.

Realize radical efficiencies with HP. Get the tech dossier and unleash the true power of virtualization.
Realize radical efficiencies with HP. Get the tech dossier and unleash the true power of virtualization.

Synology Reliable NAS for Every Budget
For home or business, Synology DiskStations provide reliable backup, file sharing, streaming & more.

Technology for Tomorrow's Cloud
Help Secure Your Cloud with Intel® Technology

Experience the MAINGEAR Difference
Discover the MAINGEAR SHIFT with Super Stock options, overclocked, liquid cooled and specially painted just for you.

Brother printers rated #1 in reliability
See why PC Mag readers gave Brother the #1 overall rating for printers. Again.

Capture Competitive Advantage with Windows Embedded
See how one Texas hospital is saving $50,000 and seeing 1,500 more patients each year.

Bitdefender Sphere
Complete Antivirus Protection for ALL you MAC+PC+Android devices (Save $89).