CERTIFIED ETHICAL HACKING OVERVIEW

Kathryn.Stephens@nsci-va.org
January 19, 2009

National Security Cyberspace Institute, Inc. (NSCI)

Through the combination of research and education, NSCI supports public and private clients aiming to increase cyberspace awareness, interest, knowledge, and/or capabilities. NSCI is committed to helping increase security in cyberspace whenever and wherever possible. NSCI publishes a bi-weekly newsletter (*CyberPro*), has published numerous whitepapers on various cyberspace topics, maintains an online cyber reference library, and has established an email distribution list for sharing cyber-related resumes to interested parties. NSCI is a small, veteran-owned business headquartered in Virginia.

Ethical hacking, also known as penetration tests, intrusion testing or red teaming, is increasingly being used by government and industry organizations to identify security risks. Ethical hackers, sometimes called white hats, are hackers that use penetration testing or security system attacks at the request of an organization in order to identify flaws or vulnerabilities before actual malicious hackers are able to exploit them. Ethical hackers duplicate the same attack methods as criminal hackers, but they report their findings back to the client. Ed Skoudis, Vice President of Security Strategy for Predictive Systems' Global Integrity consulting practice, says that ethical hacking has continued to grow despite drawbacks in the IT industry. Ethical hacking was first used primarily in the government and technology sectors, although many large companies are now requesting penetration tests. Other companies, such as IBM, keep employee teams of ethical hackers.[1]

Searchsecurity.com offers the following definition of an ethical hacker: "An ethical hacker is a computer and network expert who attacks a security system on behalf of its owners, seeking vulnerabilities that a malicious hacker could exploit. Ethical hackers use the same methods as their less-principled counterparts but report problems instead of taking advantage of them."[2] Ethical hackers usually have a professional background as programmers or network administrators, and usually have a variety of skills including: the ability to write programs in many programming languages; knowledge of assembly language; and some programming ability. Ethical hackers also benefit from knowledge of a variety of systems, especially Microsoft Windows and Linux. Ethical hackers must have in-depth networking knowledge and at least a basic understanding of TCP/IP protocols. Ethical hackers can obtain the Certified Ethical Hacker (CEH) certification and EC-Council Certified Security Analyst (ECSA) certifications from EC-Council. The Licensed Penetration Tester (LPT) certification requires candidates to agree to a code of ethics and provide evidence of professional security experience.

Security experts provide findings on security vulnerabilities, and also recommendations for clients to remediate security issues and improve overall security. Some services provided by hackers include: application testing, which identifies design and logic flaws; war dialing, which identifies unauthorized modems on a network; network testing, which looks for security flaws on external and internal networks, systems and devices; wireless security assessments that evaluate the security of a company's wireless infrastructure; and system hardening, which assesses configuration issues and vulnerabilities to measure overall network security.[3]

Paul Klahn, director of assessment services with FishNet, says that organizations need to remember that penetration testing does not guarantee network security, and that ethical hacking services return only statistics. Klahn says that the findings from ethical hacking services must be put into a business context to benefit the company. The identified security flaws must be prioritized according to the extent of threat and how critical a patch is. Experts also stress that ethical hacking is only another security tool, and should be used along with other tools to improve corporate security. There are four basic hacks that are used by ethical hackers:

---

[1] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci921117,00.html#
[2] http://www.globalknowledge.com/training/generic.asp?pageid=1595&country=United+States
[3] http://bt.counterpane.com/ethical-hacking.html

Kathryn.Stephens@nsci-va.org
January 19, 2009

- IP Hack: the company provides hackers with an IP address to try to attack with little other background information.
- Application Hack: A more in-depth hack that tries to penetrate deep into databases or shut down production servers.
- Physical Infrastructure Hack: Hackers try to physically gain access to facilities and systems looking for confidential information. Ethical hackers use technical methods as well as social engineering techniques for these hacks.
- Wireless Hack: Hackers target wireless access points and report findings of weak entry points back to clients.[4]

Certified Ethical Hackers are professionals that have completed the EC-Council CEH Program. The Certified Ethical Hacker certification requires participants to attend an Ethical Hacking and Countermeasures Course and pass the Ethical Hacking and Countermeasures Exam offered by EC-Council.[5] McAfee's Foundstone Professional Services unit, InfoSec Institute and New Horizons also offer the Certified Ethical hacker courses based on standards and guidelines from the EC-Council. The Certified Ethical Hackers courses are vendor-neutral, intense, five-day training classes which cover topics including intrusion detection, social engineering, DDoS attacks, and virus creation. Classes allow students to practice scanning and attacking their own systems in preparation for EC-Council Certified Ethical hacker exam 312-50.[6] EC-Council also offers the Certified Network Defense Architect (CNDA) certification, which contains the coursework as the CEH program, but is specifically for U.S. Government agencies and is only available to those agency members. Participants are awarded the CNDA certification upon passing the EC-Council CNDA exam 312-99.[7]

The CEH certification course work includes legal/ethic issues overviews and training on common hacking tools including:

Footprinting Techniques	Scanning	Enumeration
System Hacking	Trojans and Backdoors	Sniffers
Denial of Service	Session Hijacking	CEH Hacking Web Servers
Web Application Vulnerabilities	Web Based Password Cracking	SQL Injection
Hacking Wireless Networks	Virus and Worms	Physical Security
Hacking Linux	IDS, Firewalls and Honeypots	Buffer Overflows
Cryptography	Penetration Testing Methodologies[8]	

A full, current course outline is available from the EC-Council site.[9] Although the CEH certification is the most widely accepted certification program, there are several other common certifications of professional ethical hackers. A few of these can be found at the end of this paper.

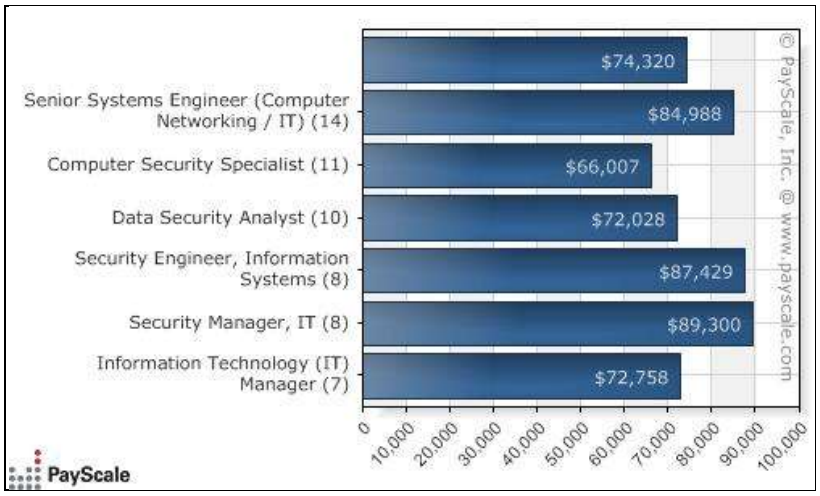
Common qualifications of professional ethical hackers include:

[4] http://www.cioupdate.com/trends/article.php/3303001/The-Pros-and-Cons-of-Ethical-Hacking.htm
[5] http://www.eccouncil.org/ceh.htm
[6] http://www.eccouncil.org/Course-Outline/Ethical%20Hacking%20and%20Countermeasures%20Course.htm
[7] http://en.wikipedia.org/wiki/Certified_Ethical_Hacker
[8] http://www.netwind.com/html/ceh-training-certification.html
[9] http://www.eccouncil.org/Course-Outline/Ethical%20Hacking%20and%20Countermeasures%20Course.htm

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Information Systems Security Architecture Professional (ISSAP)
- Information Systems Security Management Professional (ISSMP)
- Information Systems Security Engineering Professional (ISSEP)
- Certification and Accreditation Professional (CAP)
- Systems Security Certified Practitioner (SSCP)

In addition to these certifications and qualifications, candidates for ethical hacking positions will most likely be screened through background checks or personnel security investigations (PSI) for security clearances. In fact, security clearances are almost always required for positions at government agencies or private firms with government contracts. Candidates should also have more general computer certifications including A+ Certification, and certifications from Cisco, IBM, Microsoft, Novell or Oracle.[10]

IT professionals who have completed the Certified Ethical Hacker (CEH) certification program are able to go into a variety of job positions from various types of employers including government agencies, non-profit organizations, private firms and academic institutions. Average salary ranges can vary greatly due to many factors including years of experience, education, employers and industries. PayScale.com[11] charts the average salary of CEH certified professionals according to job type:

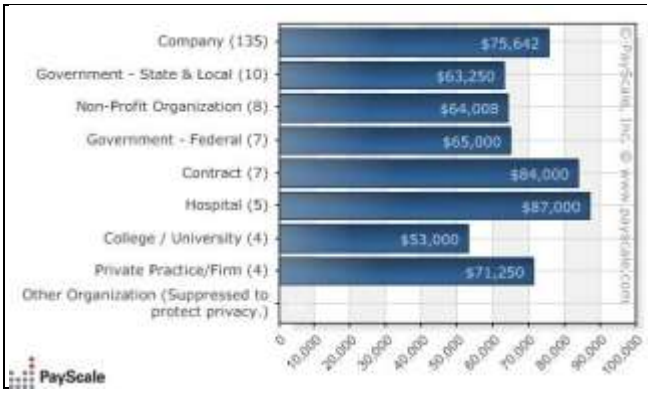


Currency: USD | Updated: 11 Jan 2009 | Individuals reporting: 184

The next chart from PayScale.com shows the average salary of CEH certified professionals based on the type of employer:

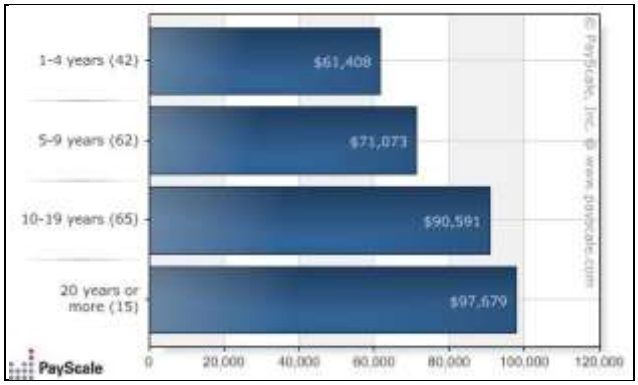
[10] http://jobsearchtech.about.com/od/careereducation/a/ceh_cert.htm
[11] http://www.payscale.com/research/US/Certification=Certified_Ethical_Hacker_(CEH)/Salary/show_all

Kathryn.Stephens@nsci-va.org
January 19, 2009



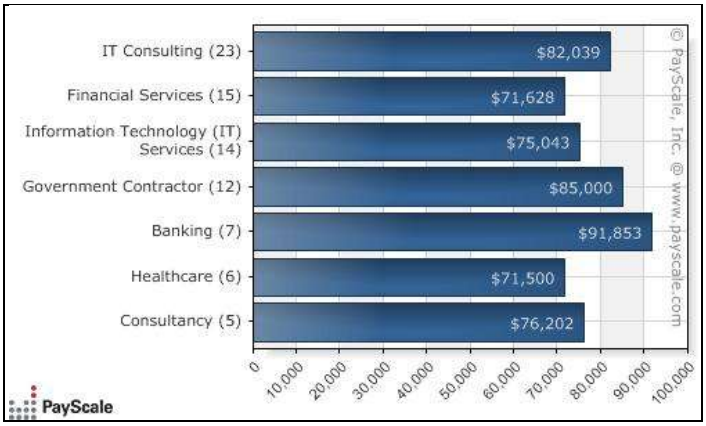
Currency: USD | Updated: 11 Jan 2009 | Individuals reporting: 184

The following table shows the effect of experience on salary ranges for CEH certified professionals:



Currency: USD | Updated: 11 Jan 2009 | Individuals reporting: 184

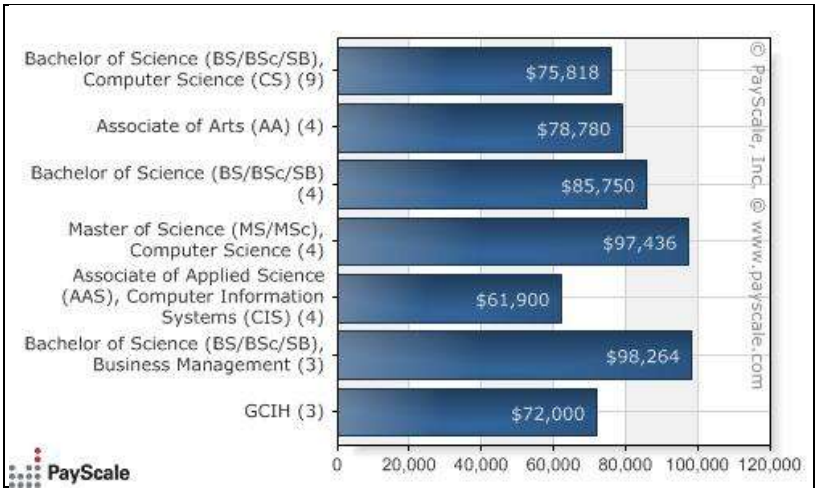
The next table shows the difference in salary ranges for CEH certified professionals based on which industry they work in:



Currency: USD | Updated: 11 Jan 2009 | Individuals reporting: 184

Kathryn.Stephens@nsci-va.org
January 19, 2009

This last table shows the salary ranges for CEH certified professionals based on their degree or major subject:



Currency: USD | Updated: 11 Jan 2009 | Individuals reporting: 129

The cost for ethical hacking services can also vary greatly based on the complexity of the network, system or application. The scope of the engagement and travel expenses may also increase service costs. Security expert Bruce Schneier explains that "penetration testing is a broad term" and can be one of many services including documenting network vulnerabilities, performing remote attacks, penetrating a data center or attempting social engineering attacks. Schneier also says that penetration testing services offer many different scanning tools and white-hat hackers with different skill levels. All of these factors could affect the total cost of penetration testing services.[12]

Security company, Plynt, which provides penetration testing services, application security testing and security code reviews, say that their penetration tests have ranged in price from $5,000 to $50,000 depending on the size of the application and skill of the testers.[13] According to a presentation by the Kansas Department of Revenue, most penetration testing projects will cost between $20,000 to $100,000 depending on the number on URLs and depth of the vulnerability assessments.[14] Web sites of companies that provide testing services all say that pricing information will be unique to each job based on size and complexity and recommend contacting the company with specific job details for pricing information. Companies also agree that most organizations outsource their penetration testing projects because of the high cost of training or acquiring skilled penetration testers. The development of automated penetration testing software has provided companies with a low cost alternative to outsourcing security testing.

Government Agencies are increasingly using third-party companies to perform vulnerability assessments/penetration testing, and some such as the Department of Defense have personnel that complete the Certified Ethical Hacker certification courses. As part of a set of security guidelines for protecting federal information systems, the National Institute of Standards and Technology (NIST) recommends that federal agencies conduct regular penetration tests. The NIST's *Guide for Assessing Security Controls in Federal Information Systems*, which was published in March 2008, says that government agencies should train selected personnel in penetration

[12] http://www.schneier.com/blog/archives/2007/05/is_penetration.html
[13] http://www.plynt.com/resources/learn/penetration-testing/how_much_does_a_pen_test_cost/
[14] http://www.taxadmin.org/fta/meet/08am/presentations/Blevins2.pdf

testing tools and techniques that should be frequently updated to include emerging vulnerabilities. The NIST also recommends using the more cost-effective automated penetration tools. Executive managing director of computer forensics consultants Stroz Friedberg, Scott Larson was the former head of the FBI's National Infrastructure and Computer Investigations division, and reports that many agencies already conduct penetration tests. Larson says that government agencies should go through outside auditors for testing.[15]

FISMA, the Federal Information Security Management Act, requires that federal agencies implement an agency-wide information security program that includes periodic risk assessments. Rapid7 Security Consultants offer NeXpose, an automated penetration testing program that locates threats, assesses the risk of each threat, and provides a remediation plan that specifically targets government agencies. Rapid7 offers penetration testing, best practices consulting, social engineering, and compliance testing to government agencies that aim to assist in FISMA requirement compliance.[16]

IntelArtisans is another company that provides assessment services specifically for Federal Government agencies. IntelArtisans provides federal agencies with system security planning, security testing and control assessments, certification and accreditation, risk management, continuous monitoring, and ISSO support with the goal of helping federal agencies comply with IT requirements and identity potential security threats before they are exploited.[17]

Core Security Technologies, who developed the CORE IMPACT penetration product, reported in 2007 that state government is a rapidly growing market for penetration testing services. Core Security Technologies also said that, at the time, 30 percent of states were using CORE IMPACT including Arizona, Colorado, Georgia, Louisiana, Maryland, Michigan, Minnesota, Pennsylvania, Rhode Island, and South Carolina. Steve Bass, chief information security officer for the Maryland Department of Public Safety said that penetration testing is becoming increasingly necessary as state agencies are extending their network boundaries for collaboration and information sharing. Automated penetration testing services are becoming increasingly popular among government agencies and state government agencies because of the pressures of satisfying rigid compliance requirements.[18]

Additional Ethical Hacking Information:

The following are some of the common types of testing involved in penetration testing services:

- **Application security testing**: Testing identifies vulnerabilities that result from organizations offering access to business functionality through web-based application. Tests may evaluate the application's use of encryption, how users are authenticated, and the use of cookies by the web server application.
- **Denial of Service (DoS) testing**: DoS testing evaluates the systems vulnerability to attacks that will completely deny service by blocking even legitimate access attempts.
- **War Dialing**: Tests aim to identify modems, remote access devices and maintenance connections of computers on an organization's network. Penetration testing is used to see if connections can be exploited to penetrate the organization's information systems network.
- **Wireless network penetration testing**: Tests look for security gaps or flaws in design, implementation or operation of the wireless network. These tests are becoming increasingly important as wireless devices are increasingly being used for business activities.

[15] http://www.scmagazineus.com/NIST-Fed-agencies-should-mount-penetration-attacks/article/100210/
[16] http://www.rapid7.com/securitycenter/government.jsp
[17] http://www.intelartisans.com/industries/government.html
[18] http://www.advfn.com/news_State-Government-Agencies-across-the-Country-Assure-Network-Security-with-CORE-I_20895628.html

Kathryn.Stephens@nsci-va.org
January 19, 2009

- **Social Engineering**: Social engineering tests involve some form of social interaction, usually with employees or suppliers. Tests aim to gather information which could help hackers penetrate the organization's systems. Hackers may pretend to be an employee to obtain account and password information, intercepts mail that contains sensitive information, or gain physical access to restricted areas that hold confidential information.[19]

A recent article from ComputerWorld provides some recommendations for successful and more cost effective penetration testing. The article recommends that companies set specific goals with high priority systems to reduce costs from an unnecessarily large test. Senior training engineer Joe Basirico of Security Innovations, Inc. says that companies must assign staff and resources to the project, even if they are bringing in a third party to perform the testing. This can make the process faster and reduce costs. Providing testing companies should also be provided with documentation including details about encryption and system configurations in order to reduce the amount of time they will spend on legwork. Following penetration testing, companies should also prioritize the results and begin with findings that would have an immediate effect on IT security.

Common Certifications of Professional Ethical Hackers		
CEPT	Certified Expert Penetration Tester	The Certified Expert Penetration Tester certification, awarded following successful completion of a certification exam, is for security professionals who require expert level knowledge of evaluating computer system, network and software security through simulated attacks. The class includes an active system analysis that identifies vulnerabilities from system configuration flaws. Certified professionals should also be able to identify and exploit unknown vulnerabilities in targeted software and systems. Training covers nine domains which are: penetration testing methodologies; network attacks; network recon; windows shellcode; Linux & Unix shellcode; reverse engineering; memory corruption vulnerabilities; exploit creation – Windows; exploit creation – Linux/Unix; and web application vulnerabilities.[20]
ECSA	EC-Council's Certified Security Analyst	The EC-Council Certified Security Analyst certification program complements the CEH certification by focusing on how to analyze the results of penetration tests and vulnerability assessments. The interactive class for security professionals trains participants on how to perform security assessments as well as how to mitigate identified security risks. Certification is awarded following successful completion of the EC-council exam 412-79.[21]
GPEN	GIAC Certified Penetration Tester	The GPEN certification is awarded following a proctored exam. The certification program targets security professionals who are involved in network and system assessments for identifying security vulnerabilities. Training includes key areas including penetration testing methodologies, the legal issues of penetration testing, and how to properly conduct penetration testing.[22]
CPTE	Certified Penetration Testing Expert	The CPTE certification requires participants to perform all stages of an actual penetration test, and offers more in-depth attacks, techniques, technologies and countermeasures than foundation courses such as CPTS, CEH and OSPT.

[19] http://www.deloitte.com/dtt/cda/doc/content/ITAC_-_ethical_hacking_-_e(4).pdf
[20] http://www.iacertification.org/cept_certified_expert_penetration_tester.html
[21] http://www.eccouncil.org/ecsa.htm
[22] http://www.giac.org/certifications/security/GPEN.php

Kathryn.Stephens@nsci-va.org
January 19, 2009

Common Certifications of Professional Ethical Hackers		
		The courses also focus on the "business side" of penetration testing including authorization issues, security policy review and compliance.[23]
CPTS	Certified Penetration Testing Specialist	The Certified Penetration Testing Specialist certification, awarded upon successful completion of the Thompson Prometric CPTS examination, trains students through hands-on Penetration Testing methodologies. Courses are continually updated to include the latest vulnerabilities and defenses. The class also focuses on justifying business testing activities and optimizing security controls to meet business needs.[24]
CHFI	Certified Hacking Forensic Investigator	The Certified Hacking Forensic Investigator certification from the EC-Council prepares investigators for discovering data in computer systems and recovering deleted, encrypted, and damaged file information for use in criminal cases. The certification, which is awarded after successful completion of the exam ECO 312-49, is aimed at police and law enforcement personnel, defense and military personnel, security professionals, systems administrators, legal professionals, government agencies, and IT managers.[25]
CREST	Council of Registered Ethical Security Testers Certified Consultant	The CREST Certified Consultant certification, provided by the Council of Registered Ethical Security Testers, is a three year certification that prepares professionals for using tools and techniques for identifying and exploiting system vulnerabilities. The thorough required certification exam ensures that the CREST certification is one of the highest available in security testing.[26]
OSCP	Offensive Security Certified Professional	IT professionals can take online courses that introduce students to hacking tools and techniques via a live computer lab that is legally safe and confined to a local network. Following the course, students can participate in the Certification Challenge, which tests students through a Hack Challenge in an unfamiliar environment. Upon successful completion, the student is awarded the Offensive Security Certified Professional certification.[27]

[23] http://www.ethicalhacker.net/content/view/38/3/
[24] http://www.careeracademy.com/index.asp?PageAction=VIEWPROD&ProdID=219
[25] http://www.eccouncil.org/chfi.htm
[26] http://en.wikipedia.org/wiki/Council_of_Registered_Ethical_Security_Testers_Certified_Consultant
[27] http://www.offensive-security.com/

Kathryn.Stephens@nsci-va.org
January 19, 2009

Bibliography

Advanced Ethical Hacking and Penetration Testing Courses. (n.d.). Retrieved from InfoSec Institute: http://www.infosecinstitute.com/courses/advanced_ethical_hacking_training.html

Bernard, A. (2004, January 23). *The Pros & Cons of Ethical Hacking*. Retrieved from CIO Update: http://www.cioupdate.com/trends/article.php/3303001/The-Pros-and-Cons-of-Ethical-Hacking.htm

Bernard, A. (2004, 01 23). *The Pros & Cons of Ethical Hacking*. Retrieved from CIO Update: http://www.cioupdate.com/trends/article.php/3303001/The-Pros-and-Cons-of-Ethical-Hacking.htm

Brodkin, J. (2008, April 23). *Ethical Hacking Certification Offered by McAfee*. Retrieved from NetworkWorld: http://www.networkworld.com/newsletters/edu/2008/042108ed1.html

CEH Program. (n.d.). Retrieved from EC-Council: http://www.eccouncil.org/ceh.htm

Certified Ethical Hacker. (n.d.). Retrieved from Wikipedia: http://en.wikipedia.org/wiki/Certified_Ethical_Hacker

Certified Ethical Hacker CEH Certification Training Course. (n.d.). Retrieved from Netwind Learning Center: http://www.netwind.com/html/ceh-training-certification.html

Certified Expert Penetration Tester (CEPT) Course Information. (n.d.). Retrieved from Information Assurance Certification Review Board: http://www.iacertification.org/cept_certified_expert_penetration_tester.html

Certified Penetration Testing Specialist / Certified Ethical Hacker. (n.d.). Retrieved from CareerAcademy.com: http://www.careeracademy.com/index.asp?PageAction=VIEWPROD&ProdID=219

Computer Hacking Forensic Investigator Course Information. (n.d.). Retrieved from EC-Council: http://www.eccouncil.org/chfi.htm

CPTE - Certified Penetration Testing Expert. (n.d.). Retrieved from The Ethical Hacker Network: http://www.ethicalhacker.net/content/view/38/3/

Ethical Hackers. (2007, June 05). Retrieved from Search Security: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci921117,00.html#

Ethical Hackers. (2007, 06 05). Retrieved from Search Security: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci921117,00.html#

Ethical Hacking Certifications. (n.d.). Retrieved from The Ethical Hacker Network: http://www.ethicalhacker.net/content/category/1/31/3/

Ethical Hacking Services. (n.d.). Retrieved from Managed Security Solutions Group: http://bt.counterpane.com/ethical-hacking.html

Kathryn.Stephens@nsci-va.org
January 19, 2009

Fletcher, S. (n.d.). *Ethical Hackers: Hacking for Fun and Profit*. Retrieved from Global Knowledge: http://www.globalknowledge.com/training/generic.asp?pageid=1595&country=United+States

Gatford, C. (2008, January 24). *Penetration Testing/Ethical Hacking Certifications*. Retrieved from PenetrationTesting.Com: http://penetrationtester.com/2008/01/penetration-testing-ethical-hacking.html

Gittlen, S. (2008, May 27). *Five steps to successful and cost-effective penetration testing*. Retrieved from ComputerWorld Security: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9087440

Information Security Qualifications. (n.d.). Retrieved from IT Governance: http://www.itgovernance.co.uk/infosec_quals.aspx

Niznik, J. S. (n.d.). *Tech Careers: Certified Ethical Hacker*. Retrieved from About.com: http://jobsearchtech.about.com/od/careereducation/a/ceh_cert.htm

Rogers, J. (2007, December 27). *NIST: Fed agencies should mount penetration attacks*. Retrieved from SC Magazine: http://www.scmagazineus.com/NIST-Fed-agencies-should-mount-penetration-attacks/article/100210/

Salary Survey Report for Certification: Certified Ethical Hacker (CEH). (2009, January 11). Retrieved from PayScale.com: http://www.payscale.com/research/US/Certification=Certified_Ethical_Hacker_(CEH)/Salary/show_all

Schneier, B. (2007, May 15). *Is Penetration Testing Worth it?* Retrieved from Schneier on Security Blog: http://www.schneier.com/blog/archives/2007/05/is_penetration.html

State Government Agencies across the Country Assure Network Security with CORE IMPACT. (2007, June 04). Retrieved from ADVFN News: http://www.advfn.com/news_State-Government-Agencies-across-the-Country-Assure-Network-Security-with-CORE-I_20895628.html

Using an Ethical Hacking Technique. (2003, June). Retrieved from The Canadian Institute of Chartered Accountants, Information Technology Advisory Committee: http://www.deloitte.com/dtt/cda/doc/content/ITAC_-_ethical_hacking_-_e(4).pdf

Kathryn.Stephens@nsci-va.org
January 19, 2009

Ethical Hacking Companies / Services

- **Plynt**
  - Plynt offers penetration testing, application security testing/certification, and security code reviews. Plynt clients include businesses from 15 industries including financial, healthcare, software and eCommerce. Clients also represent 25 U.S. states and 15 nations worldwide.
  - Examples of Plynt clients: Bermuda Commercial Bank, Bermuda; Citizens First Bank, FL; eFunds Corporation, AZ; Mid-Atlantic Corporate FCU, MD; Center for Medicare & Medicaid Services (HHS); University of Michigan, MI; Medmarc Insurance, VA; AmericaToGo, CA; Pathways Community Network, GA; Franklin Covey, UT; Keane Inc, CA; ING Group; Reuters Group; Prudential Group; SBI Group; and many others!
- **SecureWorks**
  - SecureWorks performs penetration tests and attempted hacks in order to evaluate how difficult it is to obtain data from outside the network, which information is at risk, and what measures clients can take to better protect their assets.
  - SecureWorks currently works with over 2,000 networks including many in the financial, healthcare and utilities sectors. SecureWorks also boasts that their attack database holds over one billion attacks that they have prevented.
- **Security Innovation, Inc.**
  - Security Innovation offers vulnerability analysis and software security risk assessment services. The vulnerability analysis includes tests of multiple systems using attack techniques, identification of the most critical application risks, and a code review to uncover security flaws.
  - The software security risk program helps to identify software security flaws from poor policies or software development processes. Security Innovation provides remediation recommendations, and helps organizations address compliance issues.
  - Security Innovation, Inc. clients include government agencies and top corporations which they list on their Web site according to industries. Some customers listed are Federal Reserve Bank, Liberty Mutual, Nationwide, ING, VISA, SAIC, the State of Florida, Harris Corporation, Northrop Grumman, Lockheed Martin, Microsoft, Sony, Google, HP, IBM, AOL, Symantec, and many others.
- **FishNet Security**
  - FishNet Security's Information Assurance Division offers several assessment services that identify risks to the clients' systems through policy/process evaluation and vulnerability tests. Services offered by FishNet include: regulatory compliance services; web application & database security assessments; network vulnerability and penetration assessments; incident response and digital forensics; and wireless security assessments.
  - FishNet Security – Federal specializes in providing information security services to Federal government agencies through assessing security posture, developing security roadmaps and implementing a secure environment. FishNet offers the following services to federal agencies: information assurance services; federal policy and compliance; security architecture and engineering; and security program management.
- **ControlScan**
  - ControlScan offers clients web application scanning or application penetration testing services. Web application scanning uses SQL injection and cross-site scripting techniques testing to identify security

flaws. ControlScan prioritizes applications by the severity of the identified vulnerabilities and provide sample code fixes for the flaws.

- Application penetration testing evaluates the security of web applications through a simulated attack. Testing also includes a manual review of the clients' application for risks and a comprehensive report that lists the steps taken, identified vulnerabilities and remediation options.
- ControlScan protects thousands of small and mid-size businesses' ecommerce Websites. Customers include the United Community Bank of North Dakota, Cybrhost.com, Sportsflicks.com, Excess Revenue, Inc., FireFold.com, and Onlinetaxpros.com among others.

- **NCC Group**
  - The NCC Group's UK Penetration Testing division offers penetration testing services that identify clients' vulnerabilities without interrupting business operations. NCC Group uses the latest techniques and technologies from genuine hackers, and invites clients to observe the testing process at the NCC Group laboratory to increase their knowledge of security methods.
  - NCC Group testing services include: network security testing accounting for both internal and external attacks; remote access security testing that addresses laptop and teleworker security and access to remote servers; application security testing; social engineering testing that covers unauthorized access, obtaining sensitive information and impersonation and deception.
  - Clients of NCC Group include Amec, Carphone Warehouse, DTI, Flybe< Greenwich Council, Investec, National Australia Bank, Stroud and Swindon Building Society, Watson Wyatt, and others.
- **Pivot Point Security**
  - Pivot Point Security provides security auditing, penetration testing and vulnerability assessment services to organizations in the NY/NJ/PA metro area.
  - PivotPoint offers a comprehensive approach to security testing by focusing on three key areas: controls auditing; penetration testing and enterprise security management. Unlike other penetration testing service providers, PivotPoint presents their findings to clients through a comprehensive remediation plan that emphasizes IT efficiency, financial and business report accuracy, and compliance with applicable laws and regulations.
- **En Garde Systems**
  - En Garde Systems provide digital risk management, penetration testing and security training services that cover technical vulnerabilities, policy risks, risks of public information exposure, internal threats, core data protections and relationship risks.
  - Since 1994, En Garde Systems has provided risk evaluation services to more than 100 banking, healthcare, and enterprise customers. Clients include Fortune 500 companies, banks, the military, law enforcement agencies and the intelligence community.
- **BT Group**
  - BT INS offers ethical hacking services including application testing, network testing, wireless security, system hardening, and war dialing. BT INS performs testing at their Ethical Hacking Centre of Excellence (EHCOE).
  - BT INS offers clients a team of more than 30 ethical hacking experts at the BT INS EHCOE, testing methodologies that guarantee high-quality results, and a team of over 100 security experts that provide support to the Ethical Hacking team.
  - BT Group has locations in more than 50 countries, and provides services to more than 170 countries including the United States.

Kathryn.Stephens@nsci-va.org
January 19, 2009

- **GoSecure**
  - GoSecure's Ethical Hacking Services include testing for more than 1000 known vulnerabilities, logic flow problems, and other risks. GoSecure utilizes commercial and public domain tools as well as manual tests and custom-developed tools.
  - GoSecure clients include law enforcement agencies, financial institutions, transportation firms and multinationals organizations.
- **Microland**
  - Microland consultants provide clients with testing for existing or published vulnerabilities as well as unknown flaws within custom applications. Penetration testing services address IT infrastructure issues including: perimeter security; database security; web application/services security; wireless security; and source code security auditing.
  - Microland performs testing at a state of the art Penetration Testing Center of Excellence (CoE) that utilizes innovative, contemporary security testing tools and techniques. Microland's methodology is based on international standards like OSSTMM, OWASP, WASC, NIST and ISSAF.
  - Microland works with over 70 clients that include Fortune 100 organizations and global enterprises worldwide.
- **Churchill Security Limited**
  - Churchill Security penetration testing services provide an analysis of a company's security measures including: network security; port scanning; application testing & code review; router testing; firewall testing; intrusion detection system testing; password cracking; denial of service testing; and containment measures testing.
  - Churchill Security aims to provide clients with a comprehensive assessment of security that covers policies, procedures and implementation. Churchill also works to reduce an organization's security cost and increase returns on IT security investments by resolving security flaws.
- **Core Security Technologies**
  - Core Security Technologies offers the CORE IMPACT security testing software programs that customers can use to expose vulnerabilities, measure operational risk, and assure security effectiveness across information systems. The software presents users with actionable information that will aid in improving security to sensitive information assets and critical technology infrastructure.
  - Core Security Technologies has many high-profile customers from several different industries and includes a full customer list on their website. Examples of clients include the U.S. Air Force, U.S. Coast Guard, U.S. Navy, U.S. Army, Transportation Security Administration, United States Postal Service, Apple, Dell, IBM, Washington Trust Bank, MasterCard, NYSE Group, Countrywide Financial, JPMorgan Chase, MoneyGram International, VISA, Allstate, and countless others.