Ethical hackers: putting on the white hat

Tracey Caldwell

Tracey Caldwell, journalist

Ethical hackers are fast becoming an essential part of an enterprise's network security armoury. So-called 'white hats' – to distinguish them from their malicious black hat counterparts – are increasingly fulfilling a role beyond penetration testing. As the threats change, the skill sets of ethical hackers are changing too, encompassing social engineering, social networking and consumer mobile technologies.

"Web applications have become increasingly complex and highly vulnerable," says Peter Wood, member of the ISACA Security Advisory Group and CEO of First Base Technologies. "Social networking sites, consumer technologies – smartphones, tablets etc – and cloud services are all game changers this year. More enterprises are now requesting social engineering tests, which shows an increased awareness of threats beyond website attacks."

Starting out

The barriers to entry to becoming an ethical hacker are pretty low, according to Chris Larsen, senior malware researcher at Blue Coat Systems. "Buying or building a cheap computer and putting Linux, Apache, MySQL and PHP on it will get you started," he says. "Just set up a simple website on your box, hook it to the Internet, and start watching your server logs. You'll see the hackers coming to you in no time."

Chris Larsen, Blue Coat Systems.

He adds: "Ethical hackers have a valuable role to play in probing hardware, software or websites to look for weaknesses. By using the same techniques as hackers to try and breach security, white hats are performing a sort of crash test on websites that is similar to crash testing cars. Testers mimic real crashes to see if the car can handle the impact. Ethical hackers can assess not just the network defences but also corporate security policies and user behaviour for potential security risks."

Training

Enterprises must address network security concerns and – almost as important – must be able to show a world full of regulators and auditors that they are doing so. James Foster, principal consultant at Acumin Consulting, points out that recent regulations such as the Sarbanes-Oxley Act and the UK's Code of Connection have provisions that require networks (wired and wireless), firewalls, databases, servers, applications and mobile devices to be checked thoroughly for vulnerabilities. For this reason, certification for ethical hackers is becoming increasingly important.

"Most professional penetration testers will go on to accumulate at least two of the available certifications," says Foster. "Those with all three at the highest levels can demand very high salaries, although commercial experience is equally important to certifications."

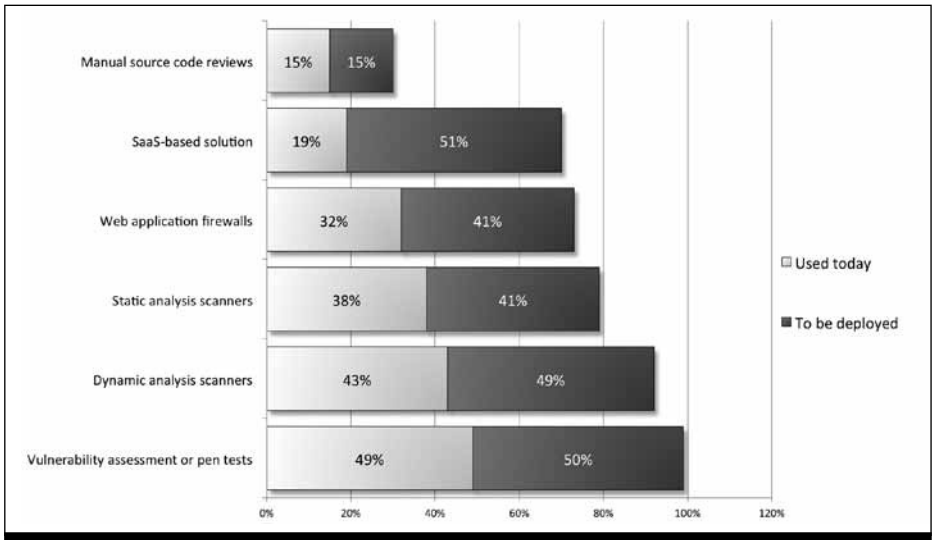
The EC-Council's Certified Ethical Hacker (CEH) is a widely recognised entry-level certification. Other qualifications include: CHECK Team Member (CTM), an experience-based certification limited to British nationals; and CHECK Team Leader (CTL), which incorporates a theory exam. TIGER Scheme Qualified Security Testers (QST) can also achieve CHECK Team Member equivalence. Council for Registered Ethical Security Testers (CREST) accreditations call for experience and exams. Qualifying as a Certified Information Systems Security Professional (CISSP) requires at least five full years of experience in information security. CISSP is accredited by the American National Standards Institute (ANSI) to ISO17024:2003.

"It is crucial for corporates to understand, even at just the conceptual level, what ethical hacking and penetration testing is about, so they can oversee the most effective risk assessment and management strategies"

"The ethical hacker most closely covers the aspects of a penetration tester, who simulates the attacks used by malicious hackers in order to best understand how to defend against them," says Jay Bavisi, EC-Council president. "This could include footprinting and reconnaissance, scanning networks, enumeration, system hacking, trojans and backdoors, viruses and worms, sniffers, social engineering, denial of service, session hijacking, hacking web servers, hacking web applications, SQL injection, hacking wireless networks, evading IDS, IPS, firewalls, and honeypots, buffer overflow,

and cryptography. It is crucial for corporates to understand, even at just the conceptual level, what ethical hacking and penetration testing is about, so they can oversee the most effective risk assessment and management strategies. Ethical hacking training serves to continuously reinforce the necessary skills of ethical hackers, by providing up-to-date courses, especially in a field that can change daily. In order to keep up with malicious hackers, ethical hackers must stay current."

The US Department of Defense (DoD) has recognised the CEH certification. The DoD issued Directive 8570 in 2004 to mandate baseline certifications for all Information Assurance positions. In February 2010, this directive was enhanced to include the Certified Ethical Hacker across its Computer Network Defense (CND) categories.



Solutions used to secure web applications. Source: Imperva, WhiteHat Security/Ponemon Institute.

Bedroom to boardroom

White hats have come out of the back bedroom and are heading for the boardroom. Ian Glover, president of CREST, a not-for-profit organisation that offers certification training, says: "The term ethical hacker still has negative connotations associated with someone working alone in a bedroom on a computer and skirting on the fringes of legality and ethics. The reality is very different. The penetration testing or ethical security testing industry is well organised, with highly professional organisations working for high-profile public- and private-sector organisations. The penetration testing market has moved from being a relative backwater and misunderstood element of the information assurance sector to being the most structured, with recognised professional qualifications overseen by the most respected individuals in the industry."

"Despite the numerous certification and training routes to the job, the belief that great ethical hackers are born and not made is prevalent in the industry"

He recommends would-be ethical hackers with good technical skills that can demonstrate a passion for the subject to approach CREST member companies. "Many of these companies have structured professional development programmes and educate their staff both in the technologies and the legal and ethical framework under which they must operate. These companies aim after two years to support individuals in their entry into the profession, with the CREST Registered Tester qualification."

People who have not made their minds up about a career can participate in activities within the CREST Cyber Security Challenge to assess their knowledge and aptitude for this type of work.

Despite the numerous certification and training routes to the job, the belief that great ethical hackers are born and not made is prevalent in the industry. "Training courses can deliver skills in using specific tools, but few if any provide the appropriate mindset," says Wood. "We [at FirstBase] believe the only way to become a professional ethical hacker is through an apprenticeship model and it takes more time than most people expect, at least five years." While FirstBase adopts this approach for its new staff, Wood acknowledges that this doesn't appear to be very common in the industry: "I still believe it's the right approach, however."

As an alternative, he recommends the University of Abertay, which offers ethical hacking degree and MSc courses. He also points to several other universities that are now offering ethical hacking courses in the UK, including Northumbria, Coventry and Glasgow Caledonian University.

"It is often said that security is a mentality, and something certain people are born with; that is, they look at things around them and ask, 'How can I get around that?' It's not out of criminal intent, it's just how their mind works"

EC-Council's Bavisi accepts that the best ethical hackers may be born as well as made: "It's often said that security is a mentality, and something certain people are born with – that is, they look at things around them and ask, 'How can I get around that?' It's not out of criminal

James Foster, Acumin Consulting.

intent, it's just how their mind works. They are naturally inclined to want to figure out how to take things apart, figure out how they break, and what happens if they change things in a certain way. This personality is best because it's exactly how malicious hackers operate, so it perfectly captures the notion that 'it takes a thief to catch a thief'. In the case of the ethical hacker, he or she is merely pretending to be the thief, legally under contract with the company that has hired them."

White hat skillsets

Jeff Schmidt, executive global head of business continuity, security and governance at BT Global Services, believes effective ethical hackers need a range and depth of skills. "Becoming a white hat is more than just taking a few classes and getting a CEH accreditation. To be an effective white hat, you must learn the fundamental systems and tools that they work and interface with on a daily basis. It is more than using just tools. Tools are good for a baseline analysis, but to be effective one must understand the processes and use of an application or network to be able to find the flaws within the core. The most effective white hats are those that think outside the box and approach the network or application first and then apply their toolbox to find the vulnerabilities."

"You have to be very, very patient as often it's like panning for gold – loads and loads of work before you find the nugget that you're after"

This not a job for a techie. According to Wood: "You need much more than just technical skills unless you're going to be a back-room person. You must be able to look at things like an engineer and a child, asking 'what happens if I do this?' At the same time you must be highly ethical and professional, never exceeding the boundaries agreed with the client, which takes discipline. You also have to be very, very patient as often it's like panning for gold – loads and loads of work before you find the nugget that you're after."

The best ethical hacker's toolkit may contain some unexpected items. "For social engineering, my favourite is my BT engineer's kit, which has proved successful on several occasions," says Wood. "It includes a reflective jacket, a tool bag, a fake ID and some BT business cards."

White hats need business skills too, he says. "You need a good command of English and report-writing skills too, which need to be combined with an understanding of the points of view of the people who are going to read your report. If you can't make your findings (and recommendations) accessible, there's no point in doing the job."

Employment

The increasing number and complexity of threats facing enterprise networks is creating a rising demand for ethical hackers either on staff or under contract. BT's Schmidt says: "Today's networks are a myriad of systems, applications, hardware and end points. On top of a heterogeneous environment, add in the rate of change in technology, frequent updates and patches that happen inside the production environment, compression of the IT workforce, multi-person developed applications and a continued force to expand network presence. These add up to a risk profile that requires additional points of validation. Having good white hats on staff or a third-party specialist can be an effective countermeasure to look for the open holes within a company's production environment and is critical to reducing risk across systems, applications and end-points."

Simon Leech, manager, Solution Architects EMEA, HP TippingPoint Group, agrees. "Enterprises can definitely use ethical hackers to their advantage as part of an information security programme, especially in the face of some of the recent breaches against Sony and RSA," he says. "Retaining the services of an ethical hacker, or a group of ethical hackers, can be a useful step in determining the 'water-tightness' of an organisation's security infrastructure."

Simon Leech, HP TippingPoint.

The Zero Day Initiative (ZDI), founded by TippingPoint, is a programme for rewarding security researchers for disclosing vulnerabilities responsibly. When an ethical hacker researches and identifies vulnerabilities in a product, and brings the research to TippingPoint, HP will pay for the information.

Web application vulnerabilities

Researchers at WhiteHat Security found that the average website has serious vulnerabilities more than nine months of the year. The latest threats are to web applications. HP carries out regular research tracking the activities of black hats and its '2010 Top Cyber Security Risks Report' identified a significant increase in the volume of organised cybercrime targeting datacentres and networks.[1]

The report indicates that while the majority of attacks are against known and patched security vulnerabilities, many high-profile attacks use new vulnerabilities before vendors issue fixes. A key finding is the dramatic increase of web exploit toolkits. These 'packaged' attack frameworks are traded online, enabling attackers to access enterprise IT systems and steal sensitive data. According to the report, web exploit toolkits are rapidly growing as the weapon of choice by attackers due to ease of use and a high success rate.

Web application vulnerabilities are contributing heavily to the workload of ethical hackers, representing half of all security vulnerabilities, according to the data generated by HP WebInspect, an HP Fortify product. The report identifies third-party plug-ins to content management systems as a leading cause of web application vulnerabilities.

"Web application vulnerabilities are contributing heavily to the workload of ethical hackers, representing half of all security vulnerabilities"

The traditional boundaries of network security are breaking down. It is now necessary to look beyond the boundary of the traditional enterprise network and ethical hackers have the skills and mindset to do this. Bjoern Rupp, CEO of GSMK CryptoPhone, highlights some of the other emerging risks that are being handled by ethical hackers: "With the advent of ubiquitous mobile computing devices and the infamous 'Internet of things', security threats that used to be the domain of datacentre managers and corporate IT professionals have inevitably spread out to tiny everyday devices that we carry with us all the time. This is especially true in mobile communications."

Starting points

Today's ethical hacker needs to work within the business case of the enterprise, assessing the value of the assets being protected and the costs of protecting them. John Stock, senior security consultant at Outpost24, says three key questions must be asked to ensure that an effective test is carried out. What is the company trying to protect? What is the company trying to protect against? And how much time, effort and money is the company willing to expend to obtain adequate protection? Once all this is decided the method of testing must be determined. There are three basic approaches:

- **Black box testing**: No exposure of the company or its environment is given. The information ethical hackers are given is the company name and then they will have to find out all other relevant information elsewhere. This is the best method to determine exactly how secure your system is.
- **White box testing**: The ethical hackers are given full exposure to the company, including what network topology and technology the company is using. They may even be given access to the company system. This method is designed to ascertain if insiders at the company are able to access information for which they are not authorised.
- **Grey box testing**: This is somewhere in the middle of the above two methods, giving partial exposure of some areas.

Career development

Ethical hackers need to invest considerable time in keeping up with the world of network security, including architectures, devices and communication protocols, multi-vendor operating systems, applications and security software. There is also a need to keep up to date with how the technology is applied within different industry sectors and evolving standards and approaches to security.

Mick Scott, security director at Deloitte, specialises in cyber-threats and penetration testing. "It requires a great deal of passion, patience, personal investment of time and an understanding of people and operational challenges," he says. "This is because victories are often small and require an initial area of focus in order to grow. Staying ahead of the curve is always important. Thinking outside of the box, continuous study, subscription to informative sources and attendance at conferences like Black Hat, OWASP and SANS are always beneficial."

Those considering a career as an ethical hacker should consider related disciplines that may suit them better. "Anti-malware writers and anti-virus companies analyse viruses and design programmes to prevent malware activating, whereas ethical hackers try and hack into networks," says Eddy Willems, G Data security evangelist. "Ethical hacking is a niche role, and those wanting to enter into the industry should be aware of other roles too. It is important to note the difference between the process of writing malware (hacking), and writing anti-malware. The tools are very different and writing anti-malware is more complex than writing malware."

A common misconception is that the ranks of the white hats are populated by reformed black hats. "It is important to stress the term 'ethical' when discussing hacking as a career, as reputation is paramount in the security industry," says Willems. "If a hacker has engaged in unethical hacking, it is often difficult to then embark upon or return to a career as an ethical hacker, as distrust and suspicion are difficult to shake in this industry."

But for practitioners who have kept to the straight and narrow, with a wealth of network security experience and a lateral turn of thought, ethical hacking is fast becoming a mainstream career choice.

About the author

Tracey Caldwell is a freelance business technology writer who writes regularly on network and security issues. She is editor of Biometric Technology Today*, also published by Elsevier.*

References

1. '2010 Top Cyber Security Risks Report'. HP TippingPoint DVLabs, June 2011. <http://dvlabs.tippingpoint.com/img/FullYear2010%20Risk%20Report.pdf>.

Resources

- 'State of Web Application Security'. Imperva & WhiteHat Security. Conducted by Ponemon Institute, 26 April 2010.
- 'WhiteHat Website Security Statistics Report'. June 2011. <https://www.whitehatsec.com/resource/stats.html>.