CEH: The 8th Paper of MCSE

Discuss in Forums {mos_smf_discuss:Opinions}By Sanjay Bavisi, VP EC-Council and S. Thomas, Chief Courseware Developer EC-CouncilOn May 22nd 2005, Card Systems Solutions, a third-party processor of payment card transactions noticed that a hacker had gained unauthorized access to its database, installed a script to screen for particular transactions placing over 40 million credit cards at stake. Of the cards involved, 13.9 million were MasterCard-branded cards, which include Maestro and Cirrus, and 22 million were Visa cards. The FBI was notified and investigations started. This is not an ideal world for most of us.
Imagine a corporate network that operates seamlessly across geographical regions on multiple platforms while still improving productivity. Now imagine it without ever causing a single glitch, users of computing resources are shielded from malicious code and forgotten passwords are easily restored. Can you imagine your regular systems administrator assuring you of such a guarantee? Had there been regular system administrators like that, the pentagon would not have had thousands of hack attempts and quite a few dangerous penetrations!The amazing fact remains that some corporations still stifle themselves within the clutches of corporate arrogance. They tend to equate the strength of their corporate networks with the huge budget they have on equipment. What they fail to understand is that even if they invest in the best technology possible, security is only as good as the weakest link including the human link. The human link can be in the form of an ill-informed administrator, a disgruntled employee or a dumb security guard. Corporations also need to realize that no matter how good their production systems are in terms of functionality, they can be compromised easily if vulnerabilities remain unpatched.How can corporations empower their network administrators to man their information highways efficiently? Consider the average administrator today. He spends more time managing a slow internet connection, damaged mouse or even a fuzzy monitor. This should not be the case with a proactive administrator who should be continuously monitoring the network, analyzing log files and screening for intrusions both externally and internally. Few understand the complexities of the hacking world or that the most recent hacking tools available for download on the Internet can be used to compromise the network with a simple 'point and click.'

So who do we blame for this serious situation? One of the most damaging reasons that we are in this state is because system administrators have been trained in a vendor biased environment by the very companies that manufacture the equipment or the operating systems in use. If we take a look at the vulnerabilities today, the disclosure seldom comes from the vendor. Most often, users discover them and the vendor is subsequently notified. The world hears about it loudly when the vendor issues a hot-fix or a patch. For instance, consider the number of fixes issued by the world’s leading operating system manufacturer.

When malicious hackers discover these vulnerabilities, they are traded as 'zero-day' exploits and subsequently exploited by malicious code such as a virus. The vendor-biased program is important to a certain degree as it trains the candidate on the inner workings of the system. Nevertheless, this leads to a feeling of complacency that the vendor based program alone would make them proficient in securing the systems. They are oblivious to the fact that hackers are adept at compromising any vulnerable system. This myopia is costing corporations billions in losses through various security compromises. Whether it is a simple denial of service or a more complex 'man in the middle' attack, hackers cause damage that puts corporate reputations and, ultimately, survival at stake.

System administrators come in various flavors general system administrators, network administrators, application administrators, database administrators and security administrators are some of them. What makes a system administrator stand out in the crowd? What makes him differentiate himself from the 'rest of them?'

A systems administrator is not a professional capable of orchestrating the situation we have described above. The operating system itself may have glitches. Hackers and malicious code are forever looking for ways to penetrate those operating system glitches to compromise the network and its users. Unscrupulous employees are willing to resort to unethical means to compromise the integrity of the corporation. How does a system administrator with only specific product knowledge defend the corporate computing resources?

The Certified Ethical Hacker (C|EH) certification arms the system administrator with critical information to identify, counter and defend the corporate network against harmful agents. It takes him into the mind of an attacker and equips him to assess the security posture of his network from an attacker's perspective. This differentiated perspective allows agile system administrators to deploy proactive countermeasures and stay at the bleeding edge of information security developments.

An MCSE equipped with C|EH leads his organization's information security resources in a sharp, focused and adaptable manner. He deals with security initiatives productively rather than restricting the efficiency of the organization. Functionality is enhanced not lost in the process of securing the organization. The C|EH certification is one that perfectly complements MCSEs from a practical perspective. Microsoft's operating systems are indeed the most widely deployed and hence constantly subjected to intrusion attempts. There have been times when vulnerabilities discovered in other operating systems have been greater than the ones discovered in MS operating system. However, Microsoft's heightened visibility makes it especially vulnerable and a hacker target. An MCSE who is C|EH is certified is trained to be an expert in the workings of the operating system and also in counteracting security incidents that are bound to occur. It isn't surprising that most MCSEs take up C|EH to complement their credentials as an administrator knowledgeable in

ethical hacking.

Most critics are ready to shoot down the vendor of the operating system the minute it gets hacked. What they fail to understand is that it is not always a vulnerability of the operating system that led to a hack. Quite often, it is the user who has misconfigured the system and, therefore, bears the ultimate responsibility. If an MCSE is armed with the knowledge of a hacker, he can significantly reduce the number of security breaches.

The International Council of Ecommerce Consultants (EC-Council) offers a certification course in ethical hacking. Certified Ethical Hacker training gives IT systems professionals a mastery of hacking tools and security systems as well as knowledge of how to hack via Windows and Linux. Students learn strong security system techniques including how to deploy countermeasures that will prevent or contain hacker attacks. Information Security professionals that carry the C|EH certification are qualified to administer nondestructive penetration testing to e-Commerce, e-Business, IT security, and other types of computer networks or systems.

The Certified Ethical Hacking Program of EC-Council has had much success worldwide with EC-Council certifying some of the largest multinationals and Government Agencies globally. The five day hands-on training prepares the aspirant for the ultimate seal of approval, C|EH certification. An MCSE equipped with C|EH leads his organization's information security resources in a sharp, focused and adaptable manner. He deals with security initiatives productively without restricting the efficiency of the organization. Functionality is enhanced not lost in the process of securing the organization.

An MCSE with C|EH stands out from the crowd because he is armed with the critical knowledge that makes him an extraordinary systems administrator. He is sought after by organizations as he brings more value to the table. He improves the organization's return on security investment and saves on external security assessments. He is more than the 'guy who makes sure that cables connect or printers work.' He is the vigilant system administrator constantly reassessing and defending the organization's network allowing other employees to improve efficiency in a productive workspace.Are you a C|EH yet?Sanjay Bavisi, VP
EC-CouncilS. Thomas
EC-Council