

## Enterprise Security - The Battle for the Final Frontier

Discuss in Forums {mos\_smf\_discuss:/root}By Sangeetha Thomas, Chief Courseware Developer EC-Council  
Internet security vendor Symantec found an average of 10,352 bots online per day while tracking &lsquo;bot&rsquo; activity in the first half of this year. This figure was just 5000 per day six months ago. What is interesting here is that it is no longer software vulnerability that threatens to sound the death knell of enterprises relying on robust networks for their survival in business. In an era where being connected and staying connected differentiates the winner from the laggards, bot networks have caused high impact denial of service (DoS) attacks. DoS attacks jumped 680 percent in the last six months, to an average of 927 per day.

View an ordinary day in the life of a corporate systems administrator...

9:00 a.m. Mike arrives at work to see messages from the marketing communications department on more spam and slow e-mail transfer. He notes the announcement of a critical vulnerability patch from Microsoft cautioning all customers to update their systems immediately.

10:00 a.m. Senior Manager Linda calls to report problems with updates on the website. Partners are not able to access their secure pages and make necessary changes. Email server still being worked on&hellip;

11:00 a.m. Rebecca calls in from the front office to ask for help with her flickering monitor. Spam filtering software seems to have a bug; email server needs configuration changes and the B2B website changes have not been made yet! Time fleets.

Across the globe, Derek is unleashing his &lsquo;bot&rsquo; &ndash; an automated program that can scan networks for specific vulnerable conditions. He trades in data. Recently he had been able to trade information about high value credit card holders to an underground card trader. Derek is not a hard code programmer, though he does dabble in writing a script or two. He obtained the bot from an IRC channel he frequented.

3:00 a.m. Mike is besieged with messages from various departments regarding inability to access the Internet. He notices that the router keeps resetting itself and the network is experiencing a denial of service attack.

Enterprises live the myth that large scale security spending on perimeter defenses can protect its computing resources to a great extent. Placing an able administrator to man these gadgets should ensure security. This cannot be further from the truth. An average systems administrator is too busy attending to regular operational issues that he does not have the time or resources to proactively check the security posture of the enterprise.

The emerging role in enterprise security personnel is that of a systems administrator who can think beyond complacent defensive measures to protect the organizations resources. Enterprises need personnel who can think on their feet and react to symptoms before they become full blown incidents.

MyDoom virus processed between 50,000 and 60,000 new copies per hour. Imagine the havoc it could create if it managed to infiltrate through one security hole in the enterprise&rsquo;s armor.

Enterprises need to think beyond conventional defensive strategies to protect their computing resources. Smart enterprises are turning towards certified ethical hackers as they realize the importance of proactive testing of their networks before intruders and hackers take advantage of them.

The established approach of contracting an external agency or consultant to carry out penetration testing is no longer recommended as before. The risk of confidential information falling in the hands of an outsider outweighs that approach. Despite ensuring confidentiality through non-disclosure agreements, there have been instances where critical information have been acquired by unscrupulous individuals and great financial losses incurred.

Enterprises are increasingly equipping their system and network administrators with the knowledge to protect their networks proactively. Often, these people resort to offensive strategies to check the security posture of the network. They attempt to break into their networks as any intruder would do. Apart from outsider simulated attacks, these security professionals also attempt to compromise the integrity of the network from within.

The enterprise stands to gain in terms of confidentiality of sensitive information, decreased cost in maintaining a robust security posture and faster recovery from any lapses that might occur in the security posture. Third-party audits can raise costs for the enterprise apart from the fact that security lapses may lie undetected until a third-party agency is contracted to test it.

There are several certifications available for the network administrator to equip himself with the know-how to carry out penetration testing. Popular among these are CISSP and Certified Ethical Hacker (C|EH). CISSP addresses the

management perspective of security while C|EH tackles the hands-on security tactics. If enterprises can incorporate penetration testing on a regular basis in their security initiatives and equip in-house administrators with the necessary training, it will go a long way in producing cost-effective and reliable security management.