



International Consortium Releases List of the Top Twenty Internet Security Vulnerabilities

October 8, 2003, Washington, DC.

The US Department of Homeland Security, the UK National Infrastructure Security Co-ordination Centre (NISCC), and the Government of Canada's Office of Critical Infrastructure Protection and Emergency Preparedness (OC�PEP), along with the SANS Institute, today released a list of the Internet security vulnerabilities that are most commonly exploited by hackers. The list defines an absolute minimum level of security protection for computers that may be connected to networks. Hundreds of automated attack programs take advantage of these vulnerabilities, so their elimination is essential as a first line of defense to protect the privacy of information stored on systems and to avoid having systems taken over and used in attacks on other victims.

“Internet vulnerabilities, or weaknesses, are a global problem. They affect all of us – from corporate giants to home users. It is therefore vital that we continue to tackle this problem,” said Steve Cummings, Director of NISCC. He went on to say, “Our colleagues at the SANS institute have been undertaking essential work and we have been pleased to add our own expertise. We have helped to produce descriptions and remedial advice.” Sallie McDonald, Director of Outreach Programs at DHS, called the Top 20 project, “a useful example of how the National Strategy for Securing Cyberspace is being implemented. The public/private partnership that created the Top 20 is a central theme of the strategy.”

The Canadian government announced the Top 20 in Ottawa at the same time the US and UK representatives were unveiling the list in Washington, D.C. "The security of our shared critical infrastructure is a global challenge that requires a global solution. We can only create that solution through cooperation and coordinated efforts. This year's SANS Top 20 Internet Security Vulnerabilities list is one example of how we can work together to create a valuable tool that will help us to address our common vulnerabilities," said Jim Harlick, Assistant Deputy Minister for OC�PEP.

The Top 20 list reflects the experience of the sponsoring organizations and more than thirty other security-savvy corporations and universities around the world. According to Alan Paller, Director of Research at the SANS Institute, “The list is a consensus of the knowledge of people around the world who are on the front lines in the battle to fight back against cyber crime.”

The Top 20 team not only listed the vulnerabilities, but under director Erik Kamerling, the team also developed a consensus guide explaining the vulnerabilities and showing how to correct each of them. That guide is available at <http://www.sans.org/top20> There is no cost, and no registration is required.

According to Randy Marchany of Virginia Tech in Blacksburg, VA, the university considers the elimination of the Top 20 vulnerabilities important enough that it is requiring all vendors of IT equipment and software to certify that the systems they deliver to the University are free of all of the Top 20 vulnerabilities. So far contracts for more than 600 products have included that certification.

The security industry is also acting to support the Top 20. Both of the two leading vulnerability testing companies, Qualys and Foundstone, are announcing that their customers will be able to test for the Top20. Qualys is also offering a free network auditing service (available at <https://sans20.qualys.com>) to allow corporations or government agencies to test their Internet-connected systems for evidence of the Top 20 vulnerabilities.

Traditionally, auditors and security managers have used vulnerability scanners to search for thousands of vulnerabilities, blunting the focus administrators need to ensure that all systems are protected against the most common attacks. When a system administrator receives a report showing thousands of vulnerabilities across hundreds of machines, he is often paralyzed. The Top 20 is a critical tool in providing focus to the cyber security fight.

More information about each of the participants can be found at their web sites

DHS: <http://www.dhs.gov/dhspublic/display?theme=31>

NISCC: <http://www.niscc.gov.uk/>

OCIPEP: www.ocipep.gc.ca

SANS: www.sans.org

Qualys: www.qualys.com

Foundstone: www.foundstone.com