

Educational Opportunities

Hacking Through a Firewall

Internet Security Presentation and Intrusion Prevention Workshop

“Hacking Through a Firewall” shows how vulnerable networks may be compromised and helpful suggestions network administrators and corporate officers should consider to make those environments more secure. The demonstration is presented using only a laptop computer, sound system, PowerPoint presentation, and a projector. The technical level is low-to-medium, so as to be of interest to a general audience of business professionals. The firewall-protected network belongs to a fictional company and is one of many in the process of being penetrated by a professional hacker. The audience sees how the hacker collects information on the target, penetrates the firewall, steals critical data, and leaves an easy way to return.

The Presenter



David A. Lissberger is founder of EcoNet.com, Inc. and serves as the president and CEO of the firm. EcoNet.com is one of Dallas's oldest Internet application development firms and the inventors of Network Cloaking™ technology. EcoNet.com manufactures the Sentinel IPS, a network Intrusion Prevention System (IPS), which protects private networks from hackers and malicious activity through their Internet gateway.

Four years ago, EcoNet started selling the first commercial versions of this technology under the name of Sentinel IPS. Since that time, Sentinels have been installed across the US, Canada and Europe. Clients include Fortune 100 firms, industry, government, and small business. Sentinel IPS devices currently defeat approximately 100 million intrusion attempts per month.

David holds an M.B.A. in International Marketing and Finance from Southern Methodist University Cox School of Business and a B.A. from Texas A&M University. He is an avid private pilot and a Texas real estate broker.

Target Audience

Professional organizations, CEOs, CIOs, CFOs, COOs, CSOs, IT Directors, Network Engineers, Security Compliance Officers for HIPAA, SarBox, GLB, & ISO 17799.

Continuing Education for lawyers, accountants, real estate and other professionals.

Law enforcement organizations, federal, state, and local governments, military, Homeland Security, and universities.

Time Requirements

30 to 60 minutes, Q&A optional.

Equipment Requirements*

Projector and laser pointer, sound system with 1/8" input, sound system with microphone for audiences of 25 or more, white board and dry erase markers for more technical audiences. Multiple monitors may be required for audiences over 100.

Reimbursement Requirements

Generally, only reimbursement for travel is requested, however travel outside the United States may require an honorary.

**Please make prior arrangements if equipment is not available*

Hacking Through a Firewall is a user-friendly demonstration of a hacker successfully penetrating a standard firewall protecting a typical small- to medium-sized business's network. The audience sees how the hacker collects information on the target, penetrates the firewall, steals critical data, and leaves himself an easy way to return later.

Previous Audiences

AFCOM
US Secret Service
North Texas Global Telecom Society
Texas Society of CPAs
Greater Dallas Board of Realtors
Texas Association of IT Managers
Vanguard Security Conference
Texas Bankers Association
Association of IT Professionals
Hi-Tech Electronic Crimes Task Force
Department of Homeland Security