**xDefenders, inc.**
1100 Pittsford-Palmyra Rd
Pittsford, NY 14534
585-385-2770
jthon@xdefenders.com
www.xdefenders.com

# *Sys*Defender … *Vulnerability Testing Service, Appliance*

## Business Problem:

If your organization depends on the Internet to conduct business, you have to stay one step ahead of emerging hackers, viruses and threats. If you do not, your business will be disrupted and that could be very costly. It makes good business sense to frequently test then patch your Internet, I/T Technologies and Communications services for vulnerabilities and risks.

## Types of Assessments:

1. *External Vulnerability Assessment* simulates a "hacker" trying to penetrate your firewall. www.modsecurity.org
2. *Internal Vulnerability Assessment* simulates a "disgruntled employee" and attempts to exploit vulnerabilities inside your firewall and on your LAN.
3. *CIS (Center for Internet Security) Benchmarks* provide a score from 0-100, grading your servers and databases for security competence against "best industry practices". www.cisecurity.org
4. *Social Engineering* attempts to gain access and vital knowledge by communicating with employees and business partners.
5. *Wireless Vulnerability Assessment* uses "drive-by and walk-by" attempts to gain access to private wireless networks and assets, using modern technology.
6. *Database and Web Application Assessment* to determine security protections at these levels of the business.

## Description:

For External and Internal Vulnerability Assessments, xDefenders offers *SysDefender,* a hardened Linux based server with powerful open-source scanning (up to 65,000+ open ports) software. The appliance is updated periodically to stay current with known vulnerabilities and vendor patches. Thousands of built-in tests automatically interrogate IP based network devices and servers. A database of "findings" is created with severity/ risk levels assigned to help network and system administrators quickly identify and remedy vulnerable ports, operating systems and applications. An Executive Summary and Technical Report are created and findings are reviewed with the client.

**Features:**

- **Plug-in architecture**. Each security test is written as an external plug-in. This way, you can easily add your own tests without having to read the code of the testing engine.
- **ASL**. The Security Scanner includes an Attack Scripting Language, designed to write security tests easily and quickly. Security checks can also be written in C.
- **Up-to-date security vulnerability database**. We mainly focus on the development of security checks for **recent security holes**. Our security checks database is updated on a *daily* basis, and all the newest security checks are available, including FTP servers and mirrors.
- **Client-server architecture**. The Security Scanner is made up of two parts: a server, which performs the attacks, and a client which is the front end. You can run the server and the client on different systems. That is, you can audit your whole network from your personal computer, whereas the server performs its attacks from the *Sys*Defender, which is in the data-center. There are several clients: one for X11, one for Win32 and one written in Java
- **Smart service recognition**. *Sys*Defender does not believe that the target hosts will respect the IANA assigned port numbers. This means that it will recognize a FTP server running on a non-standard port (31337 say), or a web server running on port 8080
- **Multiples services**. Imagine that you run **two** web servers (or more) on your host, one on port 80 and another on port 8080. When it comes to testing their security, *Sys*Defender **will test both of them**
- **Tests cooperation**. The security tests performed by *Sys*Defender coordinate with your configuration so that useless tests are not performed. If your FTP server does not offer anonymous logins, then anonymous-related security checks will not be performed.
- **Complete reports**: *Sys*Defender will not only tell you what's wrong on your network, but will, most of the time, tell you how to prevent crackers from exploiting the security holes found and will give you the risk level of each problem found (from *Low* to *Very High*)
- **Exportable reports**: The Unix client can export *Sys*Defender reports as ASCII text, LaTeX, HTML, "spiffy" HTML (with pies and graphs) and an easy-to-parse file format.
- **Full SSL support**: *Sys*Defender has the ability to test SSLized services such as https, smtps, imaps, and more. You can even supply *Sys*Defender with a certificate so that it can integrates into a PKI-field environment

- **Smart plug-ins** (optional): *Sys*Defender will determine which plugins should or should not be launched against the remote host (for instance, this prevents the testing of SendMail vulnerabilities against Postfix or "optimizations")
- **Non-destructive** (optional): If you don't want to take the risk to bring down services on your network, you can enable the "safe checks" option of *Sys*Defender, which will make *Sys*Defender rely on banners rather than exploiting real flaws to determine if a vulnerability is present
- **Independent developers**. The *Sys*Defender developers are independent. We will not suppress vulnerabilities because we have a relationship with the authors.