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

*Net*Defender … *Intrusion Detection System*

Business Problem:

Every business that leverages the Internet needs advanced security protections, otherwise business operations can be disabled! Organizations may not have the time, interest or technical expertise required to administer and maintain these essential security services. In addition, the cost of popular commercial security products can be prohibitive. The N*et*Defender appliance, with managed service solves these problems by delivering advanced intrusion detection, malware detection, ARP monitoring at all levels in your LAN and DMZ.

Description:

The *Net*Defender appliance provides robust, enterprise-class security services including a state-full inspection firewall, port-scan detection, standards-based **IPsec**, 3DES Virtual Private Networking (VPN), Intrusion Detection System that utilizes **Snort** for real-time alert detection, **ACID** for Reporting of the Snort Database and our own **"Bacon"** software for Correlation and Escalation of "New" or "Escalating" Critical Alerts. The Snort database is updated, automatically every day. xDefenders provides essential IDS tuning and training to eliminate false-positives.

The *Net*Defender IDS is a compact, plug-n-play rack-mount appliance that is managed and monitored by xDefenders. Built upon a hardened, Linux operating system. *Net*Defender provides the highest levels of Internal security and have incorporated industry standards.

Administrators can monitor the appliance with a Web-based management interface to centralize and control policy. xDefenders maintains a Secure Shell (SSH) to the appliance for periodic updates and monitoring purposes.

xDefenders has a 24x7x365 **Security Operations Center** that can manage and monitor firewalls and intrusion detection systems for clients. Escalation Planning and Incident Response is provided with the client.

Features:

- HoneyPot will automatically detect and alert based on the presence of MalWare
- ARP monitoring reports on changes, updates to prevent Man-in-the-Middle attacks, IP address and MAC address reconciliation
- Web GUI and extensive IDS and ARP Reporting
- Daily updates of Snort and Bleeding Edge signatures
- ACID or BASE Reporting of the MY/SQL Snort Database
- BACON checks every 5 minutes for NEW & Escalating Alerts
- Automatic IDS Escalation via email or text messaging
- Fine-Tuning by xDefenders to your environment

HoneyPot

There is a built-in HoneyPot function into the NetDefender IDS and it is designed to alert, immediately, based on the pressence of MalWare in the network. This means that root-kits, spyware, bots and other dangerous code will be identified and detected. The alert goes to the xDefenders SOC and the SOC staff will contact the customer.

ARP Monitoring

Man-in-the-Middle attacks are the latest attack that can affect the LAN. By watching for changes to the LAN and comparing IP address with MAC address, this kind of attack can be identified. ARP Reporting is extensive and valuable to a Security Administrator. These reports will allow them to identify strange behavior and unplanned or unwanted changes.

Network Intrusion Detection (IDS)

This risk management service incorporates real-time monitoring of malicious and suspicious electronic activity within your business. Every 5 minutes, the IDS checks for NEW or ESCALATING Events and alerts the client or the xDefenders Security Operations Center (SOC) in Rochester, NY, where a Trouble Ticket is created and available via the Client Portal. This service includes attack signature database updates, real-time correlation, real-time web reporting (see below), administration support and monitoring with custom escalation/notification procedures. A (6) Month Forensic Database is kept. Escalation Plans w/ Incident Response are provided, 24x7.

Snapshot Views of the IDS Database using ACID:

- Most recent Alerts: any protocol, TCP, UDP, ICMP
- Today's: alerts unique, listing; IP src / dst
- Last 24 Hours: alerts unique, listing; IP src / dst
- Last 72 Hours: alerts unique, listing; IP src / dst
- Most recent 30 Unique Alerts UDP

Most frequent 15 Alerts
Most Frequent Source Ports:
any , TCP , UDP
Most Frequent Destination Ports:
any , TCP , UDP
Most frequent 30 addresses:
source, destination
Last Source Ports: any , TCP , UDP
Last Destination Ports: any , TCP ,

*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.

*Web*Defender …*enforcing your Internet Acceptable-Use-Policy*

Introduction:

The *Web*Defender appliance with managed service restricts access to undesirable and unwanted web material by providing high performance URL filtering, using policies and a current database of restricted sites. It is completely configured and installed in your DMZ or LAN to control web access and log user activity.

Benefits:

- Protects your organization and employees from embarrassment and liability of offensive material
- Increases employee productivity and system availability
- "Buys back" network bandwidth, computing resources and staff time for productive use.
- Leverages Open-Source tools and services for Lowest Cost of Ownership available.

Features:

- Popular *SmoothWall* application software or Cymphonix Firewall Appliance
- Policy-based filtering to enforce your Policy
- Restrict Access to Web Sites based on Domain Name, URL and Expressions
- Filtering based on specific words and phrases written and by the overall rating of the content
- Web page cache to boost performance
- Timely updates of websites with questionable content, from critical knowledge databases
- LDAP interface (Active Directory integration)

Description:

Typically, *Web*Defender will be installed in your DMZ or LAN and accepts all outbound HTTP traffic. Web pages are cached, then inspected.

The *Web*Defender database is automatically updated each day with new, websites, so that inspection is timely and current. You have the ability to over-ride (White-List) and add-to (Black-List) these automatic updates.

Web caching enhances the web browsing experience by caching commonly accessed web content and serving subsequent requests for the same content locally rather than requesting it from the actual web site.

Technical Features:

1. Host-based Denial of Service Prevention
2. Web-Based Administration Interface
3. Restrict Access to sites with Viruses (HTTP traffic)
4. User Tracking via Login & Password
5. User Authentication via LDAP or user database
6. Time of Day, User Controls if #4 and #5 is utilized
7. User Groups are supported
8. Forward Proxy with Cache

Filtering Process:

1. Checks the website to see if it is a banned site or not. Automatic daily updates are made to the database. Blacklisting and White-listing of websites is possible.
2. Checks to see if specific URL's are banned. Daily updates are made to the database. Blacklisting and White-listing of URL's is possible.
3. Keywords and Expressions are checked to see if they should be banned. There are 25 categories and 21 user-definable categories for management controls. Black-listing and White-listing is possible.
4. Web pages of certain type can be blocked. User-defined Blacklist is maintained.

Reports:

Top User – A report for each user broken down by sites visited, connections, and other info each day.

Top Sites – Top 100 sites visited by the users sorted by number of connections. This is a daily report.

Top 20 URLs Blocked - Because of virus, mime type, or category per day.

Top 20 Users Blocked - Because of virus, mime type, or category per day. The ranking is by number of blocked attempts.

Sites & Users Report – All sites accessed during the day and who accessed them.

Site Guard – All site access attempts that were blocked on a daily basis. This report includes the offending site, the user who made the attempt, the time of day, and the rule, which was violated (ie: porn, news sites etc.).

Daily User – this shows how much time a user is spending on the web hour by hour each day.

Blocked by Category – This simple report shows the number of blocked attempts for each category per day. Categories include gambling, porn, ads, news, etc.

Blocked by Virus or Mime Type - This simple report shows the number of blocked attempts that were blocked because they contained viruses, blocked by category, or mime type violations per day.