

ServerMask for IIS and ServerMask IP1000 Appliances

U.S. GSA Facility Deploys the Complete Anti-Reconnaissance Solution for Network Security... Results in a Successful Audit

We now have great anti-recon security and are protected against future attacks due to built-in features that extend beyond our current security requirements.

Protecting critical and sensitive data from the many threats that lurk in today's Web-based world is vital. This need becomes even more significant when the data resides within a large government agency's network, and the high profile data losses in 2006 from organizations like the United States Energy Department's National Nuclear Security Administration and the Department of Agriculture only underscore the reality that even government networks remain vulnerable to hackers. Today, successful Web attacks begin by probing and detecting network, computer operating system and Web server signatures to find the best attack vectors, and IT teams are beginning to focus on anti-reconnaissance as a viable, "best practice" hacker countermeasure.

Meeting Government Standards

A facility within the General Services Administration (GSA, <http://www.gsa.gov>), the premier U.S. federal agency responsible for government acquisitions and purchases, recently sought a complete security solution to camouflage its operating system, HTTP, and TCP/IP network signatures to prevent hackers from conducting any probes that would disclose critical technology platform details for a mission-critical application. This was essential, since new government requirements for the GSA dictated that the type of operating system and technologies being used internally should provide only a limited footprint to prevent outside reconnaissance.

The U.S. GSA facility had a number of Web servers running Microsoft's Windows 2000 and Windows Server 2003 (Microsoft Internet Information Services [IIS] 5 and 6 Web servers) to support a Web-based application for project tracking, document management, and document conversion used daily by over 300 employees on an internally hosted network. While the agency required transparent HTTP and TCP/IP anonymization and anti-reconnaissance that did not disrupt the functionality of its Web application, the cost of the solution was also a major factor due to limited budget.

Best Practices in Anti-Reconnaissance Exceed Standards

The GSA facility succeeded in finding an anti-reconnaissance solution that could meet its security and budgetary requirements with Port80 Software's ServerMask for IIS software and the ServerMask IP1000 security appliance, a hardware device based on patented technologies from Arxceo® Corporation, a leader in anti-reconnaissance and anomaly-based intrusion prevention appliances. ServerMask for IIS allowed the U.S. government agency to hide the identity of a Microsoft IIS Web server from potential hackers, masking key Windows operating system signatures as well. The agency was able to download a free trial of ServerMask for IIS from Port80 Software and then test HTTP anti-reconnaissance locally and cost-effectively. With successful IIS server anonymization, the agency then evaluated the ServerMask IP1000 security appliance to protect their network



against hacker scans and probes at the TCP/IP network level. Arxceo's patented technologies, *PnPro*[™] and *Tag-UR-IT*[™], significantly enhanced network protection through the ServerMask IP1000 security appliance by preventing the spread of worms across the different segments of a network and fortifying network protocols with real-time blacklists. The appliance transparently authenticated end-user TCP connections for the government agency without client software to authenticate the session, eliminating address spoofing, a common method used in both network reconnaissance and network attacks – including Denial of Service abuses.

According to the GSA's IT Manager and LAN Administrator responsible for the project, "The ServerMask Security Solutions allowed us to surpass our government requirements for host and network anti-reconnaissance. We looked at many security solutions from leading vendors, but they often provided many features beyond anti-reconnaissance that boosted the price. Port80 Software was able to deliver a focused solution that met our needs directly and kept the cost low – rather than an A-Z, off-the-shelf solution that duplicated firewall and IPS solutions we already had in place."

ServerMask Passes with Flying Colors

An outside penetration testing company was contracted in May 2006 for an annual audit of the GSA facility's security measures in a structured "hack" of their systems, and the agency passed with flying colors. "The ServerMask Security Solutions were the key to passing the audit," according to the GSA's IT Manager and LAN administrator. "They also allowed us to exceed the government's audit standards for limiting network technology footprints."

The system was subjected to penetration testing by using two Web server scenarios: one with the ServerMask for IIS and ServerMask IP1000 defense plus a standard firewall, and the other with only a standard firewall. Their goal was to identify the OS and technology, then attempt a variety of exploits. The testers used custom software packages for scanning and deploying known exploit hacker attacks. As a result, the penetration testers were not able to identify the ServerMask protected box's OS and Web server, but they were able to determine the technology footprint of the unprotected machine. In addition, the ServerMask IP1000 blocked all real-time exploits, protecting the original Web server and other file and print servers on the network with its 1 GB transfer capacity for security scanning. However, the testers attacking the server without the security appliance were able to launch over 1,300 successful exploits – demonstrating the powerful effectiveness of the ServerMask IP1000.

"With the ServerMask system in place, we've also been able to save a lot of money which we would have otherwise spent on custom software development, hardware and the man hours necessary to lockdown our Microsoft IIS Web servers and network with manual anti-recon configuration," said the GSA's IT Manager and LAN Administrator. "We now have great anti-recon security and are also protected against future attacks due to built-in features that extend beyond our current security requirements."

More information on ServerMask Security Solutions and trial downloads are available at <http://www.servermask.com>.



About Arxceo

Arxceo Corporation's Ally product family dramatically reduces successful network attacks. These award-winning appliances block network reconnaissance so intruders can't uncover internal information necessary for an attack. Arxceo's products are truly plug-and-protect, and work without signatures or tuning. There is no faster, more cost-effective means to streamline security and stop zero-day attacks. Arxceo's anti-reconnaissance intrusion prevention is based on a simple idea. Stop the reconnaissance. Stop the attack. It protects internal network segments, remote offices and wireless networks, as well the network perimeter. Arxceo Corporation is part of the JCI Group, an international wireless data solution provider servicing businesses requiring secure data communications.

© Copyright 2006 – 2007, Arxceo Corporation. All rights reserved worldwide.

Arxceo, Ally, and TAG-UR-IT are registered trademarks of Arxceo Corporation. Wi-Fi® is a registered certification mark of the Wi-Fi Alliance. All trademarks are used in an editorial context, with no intention of infringement.

