HackerTarget.com
everyone is a target

Security from the Cloud

Remote Vulnerability Scanning

Writer: Peter

Technical Review: David

Contact: info@hackertarget.com

Published: April 2008

Summary: This white paper describes advantages of using a remote Vulnerability Scanning Service that is contained within the “Cloud”. A service that is available from anywhere by any systems fully contained as a remote entity and managed by a third party. Using Open Source Vulnerability Analysis tools the Security from the Cloud is peer reviewed, open and world class. While acknowledging that Vulnerability Analysis is only a part of the solution to securing your server, it is clear that a well defined ongoing vulnerability assessment policy is a step in the right direction.

Table of Contents

1. Introduction

Vulnerability assessment is an important part of any Security Policy. Increasingly attacks on internet hosts are profit based and therefore more devious and widespread.

> Protecting internet servers against all but the most determined of attackers is not difficult.

Poor server configuration or out of date tools result in the majority of internet server attacks. The reason for this is that they are the easiest to find and exploit. Keeping a server up to date and with no configuration errors is not difficult however these tasks often get pushed aside due to time constraints.

A vulnerability assessment is a good way to pick up errors in the security configuration of your server as well as software holes that need to fixed by updated software versions and other security vulnerabilities.

By utilizing a remote vulnerability assessment from the Cloud you will achieve a significant cost benefit for your organization. With no specialist knowledge required for the configuration and management of the assessment tools you are able to get back to the running of your organization.

2. An increasing threat landscape

Automated methods of attack and easy access to exploits are the main reasons for the increasing ease that servers are being popped. In fact if you want to prove how easy it is go to http://www.milw0rm.com and select one of the recent web application exploits. Then go to Google and type in the "Google Dork" - such as "powered by *scriptname*". See how many vulnerable applications on servers all around the web you can find in 5 minutes. Please stop there unless you are testing your own system.

Please note that we have nothing personal against the service provided by Milw0rm they are just an example. HackerTarget.com are advocates of full disclosure and openness when it comes to security.

3. Common vectors for exploitation

3.1 Poorly Configured Servers

Bad file permissions, a mis-configured web or mail server or a temporary fix that was done when the clock was ticking - poorly configured servers are everywhere and often due to time constraints it doesn't take much for even an expert Systems Administrator to slip up now and then.

3.2 Software that is not updated

Server operating systems and applications all need to be updated when security updates are released. This is not optional! Use of Windows Update, Yum and Apt tools for easy updating of servers has been great for reducing the number of vulnerable hosts, however there are still many hosts that get overlooked. It is only a matter of time until vulnerable service is discovered and the system is compromised.

3.3 Web Scripts

PHP and ASP applications and scripts are a great way to get dynamic websites working quickly, however that is not the end. Like operating systems and software these must be updated when security updates are made available. An example of this is the popular wordpress blogging software, we pick on wordpress not because it is particularly insecure but because it is such a widespread and popular script – that has had some dangerous security holes in the past.

Updates for these scripts are constant and they can be easily overlooked - until the day your blog is compromised and starts serving up malicious iframes to your unsuspecting audience.

3.4 Poor password security

The use of strong passwords on all internet facing hosts is essential. It is a simple matter to view the logs for any internet facing host and see how often the system is being hit by brute force attacks. Common services that are attacked by brute force include ssh, rdp, ftp, web forms and vnc.

3.5 Password Reuse

Using a different password for every login is obviously not practical but using the same password everywhere is incredibly bad practice. Often we have investigated compromised systems that were the result of a server owner using the same password on a poorly configured web forum to the password they use on the web mail and the same password for root on the web host!!

4. Criminal Uses of your Server

4.1 Spam

A straight up spamming operation. Using your server to send out hundreds of thousands of spamming emails is a profitable use of your compromised host. This will go on until you stop it or you get blacklisted and the spammer finds another use for your server.

4.2 Distribution of Malware

Using your web server to serve up content - just what it was made for right? What if the content is malicious, loading and exploiting your customers or users, spreading nasty key logging malware that is compromising their desktops and eventually emptying their bank accounts.

4.3 Phishing sites

Those phony email's we have all seen with a fake paypal page or internet banking page. What if those fake pages are being served up from your web host.

4.4 Warez File Storage

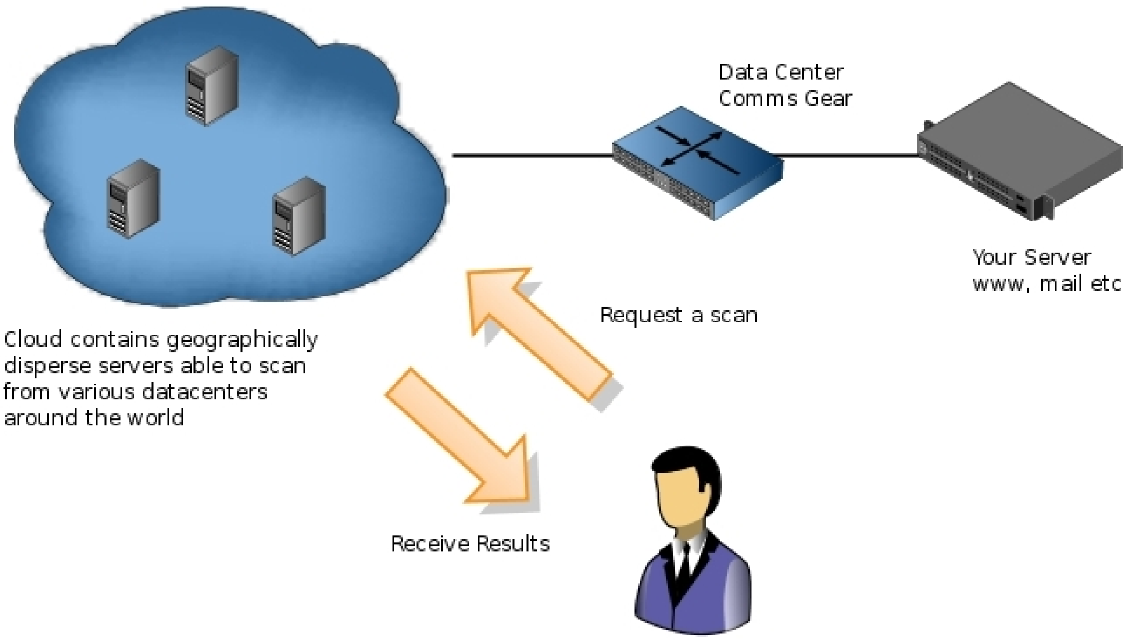
Pirated software, movies or other valuable illegal files may be stored and served up from your server.

5. The Security of Your System

- **An attack will cost you server downtime, this could be a significant cost if you run an online business.**
- **It will waste your time, getting things fixed. Organizing Incident Response and clearing up the mess.**
- **A compromised system should be rebuilt from a clean backup this is not a small task.**
- **Your reputation will suffer and you will lose customers.**

6. Security from the Cloud

Technical management of the security scanning tools is all contained with the cloud. Ongoing updates to the security tools and optimization of the scans is all undertaken by technical specialists rather your overworked information technology staff.


Data Center
Comms Gear
Your Server
www, mail etc
Request a scan
Cloud contains geographically disperse servers able to scan from various datacenters around the world
Receive Results

Security from the Cloud provides:

- a non-intrusive scan of your network / host perimeter
- a simulated attack against your environment similar to what an attacker would do
- a test of intrusion detection and incident response systems / policies
- an easy way to add a layer to your security. Security is an ongoing process that requires a variety of layers.
- a detailed technical report delivered to you by email for further investigation
- Technical Security Intelligence that will allow follow up remediation by your staff, consultants or if you prefer HackerTarget.com staff.
- you with time that will allow you to concentrate on doing what you do best - getting on with business
- an affordable way to ensure your servers are secure - security shouldn't cost the earth

7. Contact HackerTarget.com

Further information on the scanning options available can be found at our website.

Visit HackerTarget.com today for an immediate vulnerability scan or contact us for a free consulting services quote.

Email: info@hackertarget.com

web: http://www.hackertarget.com