HackerTarget.com
everyone is a target

Don't Get Hacked

Automated Remote Vulnerability Scanning

Writer: Peter
Technical Review: David
Contact: info@hackertarget.com

Published: August 2007

Summary: This white paper describes advantages of using Open Source Vulnerability Analysis tools to protect your Internet facing servers. While acknowledging that Vulnerability Analysis is only a part of the solution to securing your server, it is clear that a reliable ongoing vulnerability analysis is a step in the right direction.

Table of Contents

1. Introduction..1

2. Reasons for an increasing threat landscape..2

3. Common areas that are attacked..3

3.1 Poorly Configured Servers...3

3.2 Software that is not updated...3

3.3 Web Scripts..3

3.4 Poor ssh password security...3

3.5 Password Reuse...3

4. Uses of a compromised host...4

4.1 Spamming host...4

4.2 Distribution of Malware..4

4.3 Phishing sites..4

4.4 Warez File Storage..4

5. Do you really need a reason to stay secure?..4

6. Why you should use HackerTarget.com...5

6.1 Other Options...5

7. Contact HackerTarget.com...5

1. Introduction

Online threats against internet servers are becoming more widespread, with attacks becoming more devastating everyday. Examples like the recent "Italian Job" Mpack attack and the Microsoft UK Defacement are only 2 of an increasing number of serious attacks. It is not only well known high value targets that are being attacked, in fact the number of small web hosts and web sites being attacked is increasing dramatically. Increasingly profit is the main motive in compromising hosts, and when examining the intended use of the compromised host we can find many examples where a number of small web hosting servers can be of more value than a major corporate web server.

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

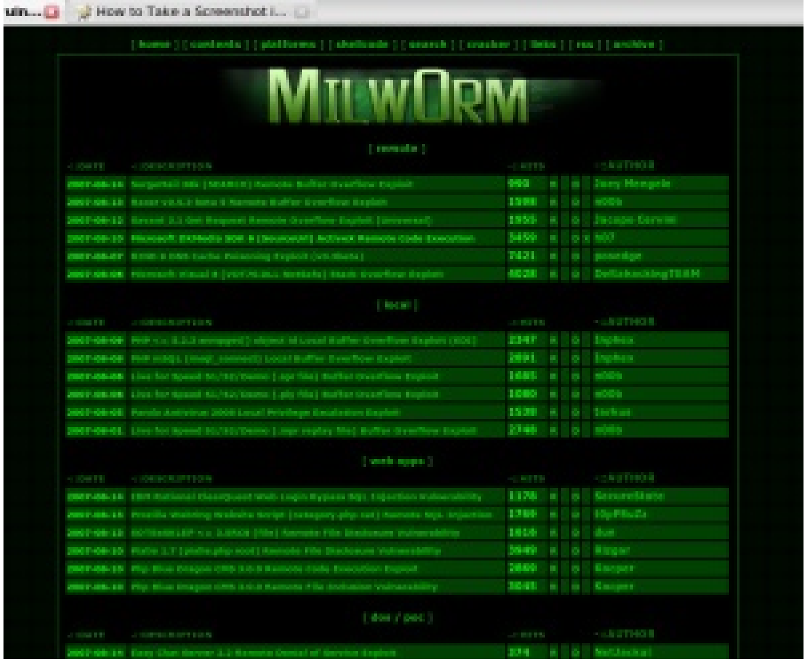
The spate of recent compromised hosts is more a matter of laziness and priorities rather than highly skilled attacks.

The smaller web hosts and organizations may not pick up the compromise immediately and here at HackerTarget we have investigated systems that were under the control of an attacker for up to 6 months before the breach was noticed.

An online vulnerability assessment is an efficient way to increase your internet security posture and stay secure.

2. Reasons for 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. I would advise you not to go any further than this, without consulting your lawyer!!


How to Take a Screenshot i...
[home] [contents] [platforms] [shellcode] [search] [cracker] [links] [rss] [archive]
MILW0RM
[remote]
[local]
[web apps]
[dos / poc]

Please note that we have nothing personal against the service provided by Milw0rm, it is merely the most well known and accessible place to get working exploits.

3. Common areas that are attacked

3.1 Poorly Configured Servers

Whether it is bad 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.

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 ssh password security

The use of strong passwords on all internet facing hosts is essential. It is a simple matter to view the ssh log for any internet facing host and see how often the system is being hit by brute force ssh attacks.

3.5 Password Reuse

Let say you pay close attention to your server and are confident there are no holes available to an external attacker. In fact you regularly post on forums around the web about how good your servers are. It just so happens that one of the forums you are posting to is not as vigilant as yourself. One day you wake up to find your main page has been defaced and you are losing sales every minute - not only that but your PayPal account has been emptied! How did this happen? Investigation has revealed the forum you use had its user database hacked and you used the same password on the forum as the one you use on your web mail. In your web mail an attacker has found your servers logon details. oops.

4. Uses of a compromised host

4.1 Spamming host

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. Do you really need a reason to stay secure?

- Prevent costly downtime in the event of a security breach
- Provides assurance to your customers that you value information security
- Avoids loss of reputation in the event of a security breach

6. Why you should use HackerTarget.com

* non-intrusive scan of your network / host perimeter

* identify security problems on your internet server and web sites

* results delivered to you weekly

* security is an ongoing process so we give you an ongoing helping hand

* detailed technical reports delivered to you by email for further investigation

* Technical Security Intelligence that will allow follow up remediation by your staff, consultants or HackerTarget.com

* allows you to concentrate on doing what you do best - getting on with business

* best of all its affordable - security shouldn't cost the earth

6.1 Other Options

* Conduct the scan yourself

Using the freely available scanners such as Nessus, Nmap, Nikto and SQLiX you can run the scans yourself. While familiarization with Linux will be a help, it is a great way to get some technical understanding of these excellent tools and the theory behind them.

* Use other more corporate services that will give you much more polished reports for a much higher price but essentially contain the same results data.

* Not worry about security and just cross your fingers and hope for the best. :)

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