Security Scanning Tools Overview

An introduction to the tools

Lead Consultant: Peter
Contact: info@hackertarget.com

Published: August 2009

Summary: This white paper describes features of the Open Source Vulnerability Assessment tools that are provided on line by HackerTarget.com. Vulnerability Analysis is an important part of the security process, it allows you to quickly gauge the current security posture of your Internet facing server or web site.

Table of Contents

1. Introduction.....1
2. The Process.....2
3. The Scanning Tools.....3
3.1 Nmap Port Scanner.....3
3.2 Fierce.pl Subdomain Scanner.....4
3.3 OpenVAS Vulnerability Scanner.....5
3.4 Nikto Web Scanner.....6
3.5 SQL Injection Scan.....7
3.5 JoomlaScan.....9
5. Conclusion.....10
7. Contact HackerTarget.com.....10

1. Introduction

http://www.HackerTarget.com has made available a number of open source security assessment tools online. These are hosted remotely on HackerTarget.com servers and allow a server operator or web-master to launch these tools remotely against servers and web sites that they manage to test the security status of these systems.

These tests allow you to get an idea of how secure your systems are before the attackers do.

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

New security breaches are constantly in the media, and there are thousands that go unreported. These attacks are performed by skilled attackers who are motivated by profit, intelligence gathering, political reasons or script kids having “fun”.

It does not matter if you are government, commercial, nonprofit or just a hobbyist – you will be probed and attacked and when you do it is good to know your systems are safe.

An on line vulnerability assessment is a great way to asses your current security.

Managing a secure system requires a layered approach, vulnerability assessment is an important layer and should be performed on a regular basis as systems change and new exploits and attacks surface.

2. The Process

The process of performing a vulnerability assessment is comparable to the process that would be undertaken by an attacker performing a targeted attack against your organisation. As the vulnerability assessment process does simulate in some ways an attack against your systems.

These tools are all open source and freely available for testing and download from the various web sites. HackerTarget.com host these tools on remote scanning servers allowing you to perform remote online scanning against your servers.

Our online option allows Free Scanning with a limit of for 4 scans / day. We also have an unlimited scanning subscription that removes the limit and also allows the use of Free Web Mail email address for the delivery of the results.

http://hackertarget.com/free-security-vulnerability-scans/
http://hackertarget.com/vulnerability-scan-subscription/

1. **Reconnaissance** is the first step, this is to pinpoint systems to attack, gain an idea of the technologies involved and a general first look at the attack surface.

   The tools used for reconnaissance in the HackerTarget.com tool kit are the world famous Nmap Port scanner and the Fierce.pl sub domain brute force tool.

2. After reconnaissance a general **vulnerability scan** against the targets discovered in Phase 1 would be launched using OpenVAS.

3. The final step in the tool kit is to use the **web assessment tools** Nikto, SQL Injection scanners and Joomla tools to assess specific web site urls and web servers.

4. This phase involves the **Review of results** from the earlier testing.

5. Reconfigure and fix any problems found to reduce the chance of the system becoming a new trophy for an attacker.

3. The Scanning Tools

3.1 Nmap Port Scanner

HackerTarget Scan: http://hackertarget.com/nmap-scan/

Project Web Site: http://www.insecure.org/

Documentation: http://nmap.org/book/man.html

The Nmap port scanner probes the IP you specified for open ports. These open ports are services that are running on your server that are open to the Internet. A host or network based firewall can block access to these ports and they will show up as filtered in the nmap results.

This is a good way to see what services your server is listening on and what is or is not being blocked by your firewall.

Sample Output:

```
Starting Nmap 5.00 ( http://nmap.org ) at 2009-07-16 23:12 UTC
Interesting ports on lvps87-230-87-158.dedicated.hosteurope.de (87.230.87.158):
Not shown: 997 filtered ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 4.2p1 Debian 7ubuntu3.2 (protocol 2.0)
80/tcp   open  http     Apache httpd 2.0.55 ((Ubuntu) mod_python/3.1.4 Python/2.4.3
PHP/5.1.2 mod_ssl/2.0.55 OpenSSL/0.9.8a mod_perl/2.0.2 Perl/v5.8.7)
8443/tcp open  ssl/http Apache httpd 2.0.46 ((Red Hat) mod_ssl/2.0.46 OpenSSL/0.9.7a)
Service Info: OS: Linux

Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.27 seconds

We have scanned the IP Address: test.acunetix.com
```

3.2 Fierce.pl Subdomain Scanner

HackerTarget Scan: http://hackertarget.com/free-domain-scan/

Project Web Site: http://ha.ckers.org/fierce/

Documentation: http://ha.ckers.org/fierce/

You will often think of your www.yourdomain.com when testing your security, but what about if you have other domains (webdev.yourdomain.com, or www-test.yourdomain.com) these development web servers, mail servers, vpn gateways and other servers can be found with a sub domain search. The fierce domain scanner tests your DNS for a zone transfer and then goes ahead and performs a brute force against your domain. Testing a list of sub domains against your domain to attempt to find other servers and IP addresses. An attacker would use this to increase his attack surface. Note that attackers love to find servers such as development servers as they have more untested code and may not be as secure. A compromise of one system often leads to access to the production environments.

Sample Output:

```
DNS Servers for hackertarget.com:
        ns52.domaincontrol.com
        ns51.domaincontrol.com

Trying zone transfer first...
        Testing ns52.domaincontrol.com
                Request timed out or transfer not allowed.
        Testing ns51.domaincontrol.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 1875 test(s)...
e.hackertarget.com              alias           email.secureserver.net
email.secureserver.net  address 64.202.189.148
email.hackertarget.com          alias           email.secureserver.net
email.secureserver.net  address 64.202.189.148
ftp.hackertarget.com            alias           hackertarget.com
hackertarget.com        address 67.207.143.162
67.207.143.162  ftp.hackertarget.com
pop.secureserver.net    address 72.167.82.11
smtp.hackertarget.com           alias           smtp.secureserver.net
webmail.hackertarget.com                alias           webmail.secureserver.net
webmail.secureserver.net        address 64.202.189.148
www.hackertarget.com            alias           hackertarget.com
hackertarget.com        address 67.207.143.162
67.207.143.162  www.hackertarget.com

Subnets found (may want to probe here using nmap or unicornscan):
        67.207.143.0-255 : 2 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 13 entries.

Have a nice day.

We have scanned the domain: hackertarget.com
```

3.3 OpenVAS Vulnerability Scanner

HackerTarget Scan: http://hackertarget.com/openvas-scan/

Project Web Site: http://openvas.org/

Documentation: http://wald.intevation.org/frs/download.php/558/openvas-compendium-1.0.1.pdf

When Nessus moved away from being an open source project, a team of dedicated individuals started work on forking the Nessus project into a new Open Source Project.

Since those early days the OpenVAS scanner has been through some major code changes. Now the plugins are excellent and it is truly a competing scanning solution to other commercial products.

The output from OpenVAS is comprehensive and the emailed results from HackerTarget.com will have a html attachment that is the raw output from the scan similar to the linked samples below.

How does it work? The OpenVAS scanner will test your servers IP for open ports, and then using its database of over 10'000 plugins will test any open ports for security vulnerabilities.

The tests are wide ranging and comprehensive.

Sample output:
http://hackertarget.com/sample/sample-openvas-scan-centos.html
http://hackertarget.com/sample/sample-openvas-scan-win2003.html

3.4 Nikto Web Scanner

HackerTarget Scan: http://hackertarget.com/website-scan/

Project Web Site: http://www.cirt.net

Documentation: http://cirt.net/nikto2-docs/

The Nikto web scanner uses a database of known web vulnerabilities and web server misconfigurations to check against your website. This will fill up your web logs with many errors as it tests each of the checks against your website. Most of them will be 404 errors (page not found) as it runs through. However it just may find a forgotten script that you installed and had forgotten about. Maybe a new exploit came out for that script and that makes your server vulnerable.

Sample Output:

```
HackerTarget.com - Nikto Web Scan Sample Report

---------------------------------------------------------------------------
- Nikto 1.36/1.39 - www.cirt.net
+ Target IP: xx.126.xx.110
+ Target Hostname: www.testsite.com
+ Target Port: 80
+ Start Time: Sun Jul 29 14:48:24 2007
---------------------------------------------------------------------------
- Scan is dependent on "Server" string which can be faked, use -g to override
+ Server: Apache
+ Server: Apache/1.3.29 (Unix) mod_perl/1.28 PHP/4.3.4
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt - contains 19 'disallow' entries which should be manually
viewed (added to mutation file lists) (GET).
+ Apache/1.3.29 appears to be outdated (current is at least
Apache/2.0.47). Apache 1.3.28 is still maintained and considered secure.
+ mod_perl/1.28 appears to be outdated (current is at least 1.99_10)
+ PHP/4.3.4 appears to be outdated (current is at least 4.3.4RC2)
+ /.htaccess - Contains authorization information (GET)
+ /.htpasswd - Contains authorization information (GET)
+ /phpBB2/includes/db.php - Some versions of db.php from phpBB2 allow
remote file inclusions. Verify the current version is running. See
http://www.securiteam.com/securitynews/5BP0F2A6KC.html for more info (GET)
+ /\">
```

3.5 SQL Injection Scan

HackerTarget Scan: http://hackertarget.com/free-sql-scan/

Project Web Site: http://www.owasp.org/index.php/Category:OWASP_SQLiX_Project

Project Web Site: http://sqlmap.sourceforge.net/

Documentation: http://sqlmap.sourceforge.net/doc/README.html

SQL Injection is currently the leading attack vector against web based applications. Through poorly configured dynamic web pages an attacker can gain access to your database and from that either your data or it can be used to gain full access to your server.

We use two of the leading open source sql injection tools for our test, SQLiX and Sqlmap. Note that these tests are configured to only perform a HTTP GET test against url parameters. See the parameter below at the end of the url (artist=1). This is the type of url that can be tested, usually it would be php, asp, cfm or jsp – although other types are able to be tested.

Sample url to test: test.acunetix.com/artists.php?artist=1

Sample output:

```
======================================================
                  -- SQLiX --
 Â© Copyright 2006 Cedric COCHIN, All Rights Reserved.
======================================================

Analysing URL [http://test.acunetix.com/artists.php?artist=1]
 http://test.acunetix.com/artists.php?artist=1
        [+] working on artist
                [+] Method: MS-SQL error message
                [+] Method: SQL error message
                [+] Method: MySQL comment injection
                        [ERROR] Parameter doesn't impact content
                [+] Method: SQL Blind Integer Injection
                        [FOUND] Blind SQL Injection: Integer based
                        [FOUND] Database type: MySQL Server
                        [INFO] Current function: version()
                        [INFO] length: 31

                                5.0_____________________________
                                5.0_____________________________-log
                                5.0____Debian_______________-log
                                5.0.___Debian_______________-log
                                5.0.2__Debian_______________-log
                                5.0.22_Debian_______________-log
                                5.0.22-Debian_______________-log
                                5.0.22-Debian_______________-log
                                5.0.22-Debian_0_____________-log
                                5.0.22-Debian_0u____________-log
```


```
                                5.0.22-Debian_0ub__________-log
                                5.0.22-Debian_0ubu_________-log
                                5.0.22-Debian_0ubun________-log
                                5.0.22-Debian_0ubunt_______-log
                                5.0.22-Debian_0ubuntu______-log
                                5.0.22-Debian_0ubuntu6_____-log
                                5.0.22-Debian_0ubuntu6.____-log
                                5.0.22-Debian_0ubuntu6.0___-log
                                5.0.22-Debian_0ubuntu6.06__-log
                                5.0.22-Debian_0ubuntu6.06._-log
                                5.0.22-Debian_0ubuntu6.06.6-log

                        [FOUND] SQL Blind Integer Injection
---  No results here means that SQLiX found no injection point  ---


--- Now sqlmap will test your url ---

   sqlmap/0.7rc1
   by Bernardo Damele A. G. <bernardo.damele@gmail.com>

[*] starting at: 04:55:14

[04:55:14] [INFO] testing connection to the target url
[04:55:15] [INFO] testing if the url is stable, wait a few seconds
[04:55:16] [INFO] url is stable
[04:55:16] [INFO] testing if User-Agent parameter 'User-Agent' is dynamic
[04:55:17] [WARNING] User-Agent parameter 'User-Agent' is not dynamic
[04:55:17] [INFO] testing if GET parameter 'artist' is dynamic
[04:55:18] [INFO] confirming that GET parameter 'artist' is dynamic
[04:55:19] [INFO] GET parameter 'artist' is dynamic
[04:55:19] [INFO] testing sql injection on GET parameter 'artist' with 0 parenthesis
[04:55:19] [INFO] testing unescaped numeric injection on GET parameter 'artist'
[04:55:20] [INFO] confirming unescaped numeric injection on GET parameter 'artist'
[04:55:20] [INFO] GET parameter 'artist' is unescaped numeric injectable with 0 parenthesis
[04:55:20] [INFO] testing for parenthesis on injectable parameter
[04:55:22] [INFO] the injectable parameter requires 0 parenthesis
[04:55:22] [ERROR] unhandled exception in sqlmap/0.7rc1, please copy the command line and
the following text and send by e-mail to sqlmap-users@lists.sourceforge.net. The developer
will fix it as soon as possible:
sqlmap version: 0.7rc1
Python version: 2.5.2
Operating system: linux2

[*] shutting down at: 04:55:22
```

3.5 JoomlaScan

HackerTarget Scan: http://hackertarget.com/joomla-security-scan/

Project Web Site: http://yehg.org

Documentation: http://www.owasp.org/index.php/Category:OWASP_Joomla_Vulnerability_Scanner_Project

The final scan in our tool kit is specific to the Joomla content management system. A widely used open source content management solution that allows creation and updating of a portal like website easy to manage. Joomla however is well known for its security vulnerabilities – often this is due to poorly written plugins rather than the core components of the system. This JoomlaScan tests a Joomla based website against a database of known vulnerabilities – this is similar to Nikto however it is more focused being a test for a single product.

To test enter the full url of your Joomla Site like so:

www.mywebsite.com/pathtojoomla/

5. Conclusion

The benefits are obvious:

- **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**

As you can see we provide a variety of tools for online security testing, and they each perform a different function. The output from these tools is technical in nature, however the fact that they are open source means there is a great deal of support and information available from the online security community if you are happy to sit down and do some research.

We know that not everyone has the time to become a security expert so at we do offer a full vulnerability assessment service here at http://www.HackerTarget.com.

The outline of our full assessment is a full security test against a server or web site using all of the above tools; along with manual testing by an experienced security professional. After the automated scans are run, the assessment runs to 3 hours of consulting time, in that time manual testing is performed to confirm any discovered vulnerabilities; additional testing may be performed if required and then a full report is compiled. This report provides a summary of the issues found and recommendations for mitigating the risk that these issues pose to your organisation.

This assessment is $150 USD for a single server, contact us for further details or a quote for bulk orders.

http://hackertarget.com/assessment-request/

7. Contact HackerTarget.com

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

Email: info@hackertarget.com
web: http://www.hackertarget.com