WMAP Web Scanner a11y.text WMAP Web Scanner What is WMAP? a11y.text What is WMAP? WMAP is a feature-rich web application vulnerability scanner that was originally created from a tool named SQLMap . This tool is integrated with Metasploit and allows us to conduct web application scanning from within the Metasploit Framework. Vulnerability Scanning with WMAP a11y.text Vulnerability Scanning with WMAP We begin by first creating a new database to store our WMAPÂ scan results in, load the wmap plugin, and run help to see what new commands are available to us. msf > load wmap

```
.-.-.-..-.-.-..---..---.
| | | || | | || | || |-'
`-----'`-'-'-'`-^-'`-'
[WMAP 1.5.1] ===  et [  ] metasploit.com 2012
[*] Successfully loaded plugin: wmap

msf >  help

wmap Commands
=============

    Command       Description
    -------       -----------
    wmap_modules  Manage wmap modules
    wmap_nodes    Manage nodes
    wmap_run      Test targets
    wmap_sites    Manage sites
    wmap_targets  Manage targets
    wmap_vulns    Display web vulns
```

...snip... Prior to running a web app scan, we first need to add a new target URL by passing the -a switch to wmap_sites . Afterwards, running wmap_sites -l will print out the available targets.

```
msf > wmap_sites -h
[*]  Usage: wmap_targets [options]
 -h        Display this help text
 -a [url]  Add site (vhost,url)
 -l        List all available sites
 -s [id]   Display site structure (vhost,url|ids) (level)



msf > wmap_sites -a http://172.16.194.172
[*] Site created.
msf > wmap_sites -l
[*] Available sites
===============

     Id  Host            Vhost           Port  Proto  # Pages  # Forms
     --  ----            -----           ----  -----  -------  -------
     0   172.16.194.172  172.16.194.172  80    http   0        0
```

Next, we add the site as a target with wmap_targets .

```
msf > wmap_targets -h
[*] Usage: wmap_targets [options]
 -h   Display this help text
 -t [urls] Define target sites (vhost1,url[space]vhost2,url)
 -d [ids] Define target sites (id1, id2, id3 ...)
 -c   Clean target sites list
 -l    List all target sites
```

```
msf > wmap_targets -t http://172.16.194.172/mutillidae/index.php Once added, we can view our list
of targets by using the -l switch from the console. msf > wmap_targets -l
[*] Defined targets
===============

     Id  Vhost           Host            Port  SSL    Path
     --  -----           ----            ----  ---    ----
     0   172.16.194.172  172.16.194.172  80    false /mutillidae/index.php Using the wmap_run
command will scan the target system. msf > wmap_run -h
[*] Usage: wmap_run [options]
 -h                        Display this help text
 -t                        Show all enabled modules
 -m [regex]                Launch only modules that name match provided regex.
 -p [regex]                Only test path defined by regex.
 -e [/path/to/profile]     Launch profile modules against all matched targets.
                           (No profile file runs all enabled modules.) We first use the -t switch to list the
modules that will be used to scan the remote system. msf > wmap_run -t

[*] Testing target:
[*]  Site: 192.168.1.100 (192.168.1.100)
[*]  Port: 80 SSL: false
[*] ============================================================
[*] Testing started. 2012-01-16 15:46:42 -0500
```

```
[*]
=[ SSL testing ]=
[*] =============================================================
[*] Target is not SSL. SSL modules disabled.
[*]
=[ Web Server testing ]=
[*] =============================================================
[*] Loaded auxiliary/admin/http/contentkeeper_fileaccess ...
[*] Loaded auxiliary/admin/http/tomcat_administration ...
[*] Loaded auxiliary/admin/http/tomcat_utf8_traversal ...
[*] Loaded auxiliary/admin/http/trendmicro_dlp_traversal ...
...snip...

msf > All that remains now is to actually run the WMAP scan against our target URL. msf >
wmap_run -e
[*] Using ALL wmap enabled modules.
[-] NO WMAP NODES DEFINED. Executing local modules
[*] Testing target:
[*]  Site: 172.16.194.172 (172.16.194.172)
[*]  Port: 80 SSL: false
=============================================================
[*] Testing started. 2012-06-27 09:29:13 -0400
[*]
=[ SSL testing ]=
=============================================================
[*] Target is not SSL. SSL modules disabled.
```

```
[*]
=[ Web Server testing ]=
============================================================
[*] Module auxiliary/scanner/http/http_version


[*] 172.16.194.172:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/scanner/http/robots_txt


...snip...
...snip...
...snip...


[*] Module auxiliary/scanner/http/soap_xml
[*] Path: /
[*] Server 172.16.194.172:80 returned HTTP 404 for /.  Use a different one.
[*] Module auxiliary/scanner/http/trace_axd
[*] Path: /
[*] Module auxiliary/scanner/http/verb_auth_bypass
[*]
=[ Unique Query testing ]=
============================================================
[*] Module auxiliary/scanner/http/blind_sql_query
[*] Module auxiliary/scanner/http/error_sql_injection
[*] Module auxiliary/scanner/http/http_traversal
[*] Module auxiliary/scanner/http/rails_mass_assignment
[*] Module exploit/multi/http/lcms_php_exec

[*]

=[ Query testing ]=

======================================================================

[*]

=[ General testing ]=

======================================================================

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

Launch completed in 212.01512002944946 seconds.

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

[*] Done. Once the scan has finished executing, we take a look at the database to see if WMAP found anything of interest. msf > wmap_vulns -l

```
[*] + [172.16.194.172] (172.16.194.172): scraper /

[*]  scraper Scraper

[*]  GET Metasploitable2 - Linux

[*] + [172.16.194.172] (172.16.194.172): directory /dav/

[*]  directory Directory found.

[*]  GET Res code: 200

[*] + [172.16.194.172] (172.16.194.172): directory /cgi-bin/

[*]  directory Directoy found.

[*]  GET Res code: 403


...snip...
```

msf > Looking at the above output, we can see that WMAP has reported one vulnerability. Running vulns will list the details for us. msf > vulns

```
[*] Time: 2012-01-16 20:58:49 UTC Vuln: host=172.16.2.207 port=80 proto=tcp
name=auxiliary/scanner/http/options
refs=CVE-2005-3398,CVE-2005-3498,OSVDB-877,BID-11604,BID-9506,BID-9561
```

msf > Because of our vulnerability scanning with WMAP, we can now use these results to gather further information on the reported vulnerability. As pentesters, we would want to investigate each finding further and identify if there are potential methods for attack. Next Working with NeXpose Prev VNC Authentication