Metasploit – Storing Pen Test Results

pentestlab.blog/category/general-lab-notes/page/5

February 17, 2013

Penetration testers are using different tools and methods in order to keep their penetration testing results.If our preference is to use Metasploit Framework for our activities then we can use the store our results in its database as Metasploit is already integrated with postgresql.This can prove very handy as many penetration tests can run for several days and we will need to have our results in a centralized environment for later use.This will help us not only in the reporting stage but and in the exploitation stage as we constructing our attack path.

If we want to check our database settings we need to type the following commands as the image below indicates:

```
root@bt:~# cd /opt/metasploit/config/
root@bt:/opt/metasploit/config# cat database.yml

#
# These settings are for the database used by the Metasploit Framework
# unstable tree included in this installer, not the commercial editions.
#
development:
  adapter: "postgresql"
  database: "msf3dev"
  username: "msf3"
  password: "4bfedfc2"
  port: 7337
  host: "localhost"
  pool: 256
  timeout: 5

production:
  adapter: "postgresql"
  database: "msf3dev"
  username: "msf3"
  password: "4bfedfc2"
  port: 7337
  host: "localhost"
```

Database Settings

The information that we have obtained above it can be used for connection with the database through the metasploit framework.if we want to check the available database commands we can run the command **help** in the metasploit console.

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

    Command           Description
    -------           -----------
    creds             List all credentials in the database
    db_connect        Connect to an existing database
    db_disconnect     Disconnect from the current database instance
    db_export         Export a file containing the contents of the database
    db_import         Import a scan result file (filetype will be auto-detected)
    db_nmap           Executes nmap and records the output automatically
    db_rebuild_cache  Rebuilds the database-stored module cache
    db_status         Show the current database status
    hosts             List all hosts in the database
    loot              List all loot in the database
    notes             List all notes in the database
    services          List all services in the database
    vulns             List all vulnerabilities in the database
    workspace         Switch between database workspaces
```

Metasploit – Database Commands

Now if we want to connect with the existing database or with another database that we have created we can use the following command:

db_connect username:password@IP:Port/database_name

Now lets say that we have to perform a scan in an IP address.We can use directly the command db_nmap IP from the metasploit console which it will scan the target and automatically it will store the results in the database.

```
msf > db_nmap 192.168.1.84
[*] Nmap: Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2013-02-17 07:20 EST
[*] Nmap: Nmap scan report for 192.168.1.84
[*] Nmap: Host is up (0.00098s latency).
[*] Nmap: Not shown: 995 closed ports
[*] Nmap: PORT     STATE SERVICE
[*] Nmap: 135/tcp  open  msrpc
[*] Nmap: 139/tcp  open  netbios-ssn
[*] Nmap: 445/tcp  open  microsoft-ds
[*] Nmap: 1025/tcp open  NFS-or-IIS
[*] Nmap: 1026/tcp open  LSA-or-nterm
[*] Nmap: MAC Address: 00:50:56:BB:00:86 (VMware)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
```

Metasploit – Nmap Scan

Now if want to check the results in the database we can use the following commands:

- creds
- loot
- hosts
- services
- vulns
- notes

The following two pictures are just a sample of the commands hosts and services.

```
msf > hosts

Hosts
=====

address         mac                name  os_name  os_flavor  os_sp  purpose  in
  comments
-------         ---                ----  -------  ---------  -----  -------  --
  --------
172.16.36.136                            Unknown                    device

192.168.1.84    00:50:56:BB:00:86        Unknown                    device
```

List Hosts – Metasploit Database

```
msf > services

Services
========

host            port  proto  name          state  info
----            ----  -----  ----          -----  ----
172.16.36.136   1521  tcp    oracle        open   Linux: Version 10.2.0.1.0 - P
duction
192.168.1.84    445   tcp    microsoft-ds  open
192.168.1.84    139   tcp    netbios-ssn   open
192.168.1.84    135   tcp    msrpc         open
192.168.1.84    1025  tcp    nfs-or-iis    open
192.168.1.84    1026  tcp    lsa-or-nterm  open
```

List Services – Metasploit Database

Another thing that we can do here is to export the results in an XML format in order to use it with other tools like Dradis Framework.

```
msf > db_export /root/Desktop/pentestlab.txt
[*] Starting export of workspace default to /root/Desktop/pentestlab.txt [ xml
 ]...
[*]     >> Starting export of report
[*]     >> Starting export of hosts
[*]     >> Starting export of events
[*]     >> Starting export of services
[*]     >> Starting export of credentials
[*]     >> Starting export of web sites
[*]     >> Starting export of web pages
[*]     >> Starting export of web forms
[*]     >> Starting export of web vulns
[*]     >> Starting export of module details
[*]     >> Finished export of report
[*] Finished export of workspace default to /root/Desktop/pentestlab.txt [ xml
 ]...
```

Export Results From Metasploit Database

Conclusion

In this article we saw how we can use the database with metasploit in order to store information from a port scan that we performed.We can use this functionality as well in order to import results from other tools like Nessus or to export the results for integration with Dradis.This function of Metasploit Framework offers the penetration tester the ability to manage his results in an efficient way.