

Databases a11y.text Databases Store Information in a Database Using Metasploit a11y.text Store Information in a Database Using Metasploit When conducting a penetration test, it is frequently a challenge to keep track of everything you have done on (or to) the target network. This is where having a database configured can be a great timesaver. Metasploit has built-in support for the PostgreSQL database system. The system allows quick and easy access to scan information and gives us the ability to import and export scan results from various third party tools. We can also use this information to configure module options rather quickly. Most importantly, it keeps our results clean and organized. msf > help database

Database Backend Commands

=====

Command	Description
-----	-----
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

msf > hosts

Hosts

=====

address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments
-----	---	----	-----	-----	----	-----	----	-----
172.16.194.134			Unknown			device		
172.16.194.163		172.16.194.163	Linux	Ubuntu		server		
172.16.194.172	00:0C:29:D1:62:80	172.16.194.172	Linux	Ubuntu		server		

msf > services -p 21

Services

=====

host	port	proto	name	state	info
----	----	-----	-----	-----	-----
172.16.194.172	21	tcp	ftp	open	vsftpd 2.3.4 In the next section of Metasploit Unleashed weâ€™ll take a look at setting up our Metasploit Database . Next Using the Database Prev

Generating Payloads