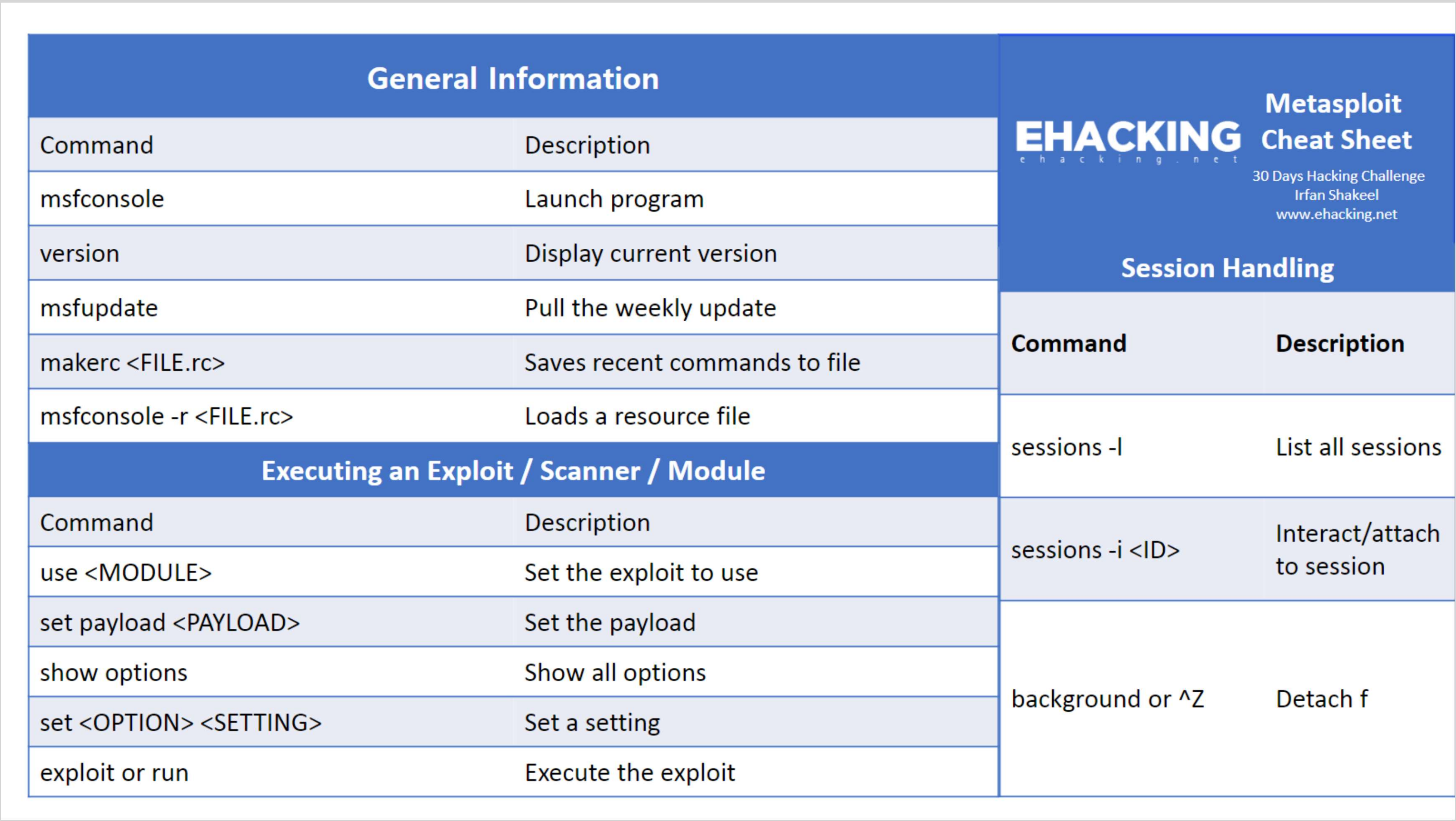


EHACKING
ehacking.net

Metasploit Cheat Sheet

30 Days Hacking Challenge
Irfan Shakeel
www.ehacking.net

General Information

Command	Description
msfconsole	Launch program
version	Display current version
msfupdate	Pull the weekly update
makerc <FILE.rc>	Saves recent commands to file
msfconsole -r <FILE.rc>	Loads a resource file

Executing an Exploit / Scanner / Module

Command	Description
use <MODULE>	Set the exploit to use
set payload <PAYLOAD>	Set the payload
show options	Show all options
set <OPTION> <SETTING>	Set a setting
exploit or run	Execute the exploit

Session Handling

Command	Description
sessions -l	List all sessions
sessions -i <ID>	Interact/attach to session
background or ^Z	Detach f

Using the Database

The DB saves data found during exploitation. Auxiliary scan results, hashdumps, and credentials show up in the DB.

- First Time Setup (Run from linux command line.)

Command	Description
service postgresql Start	Start DB
msfdb Init	Init the DB

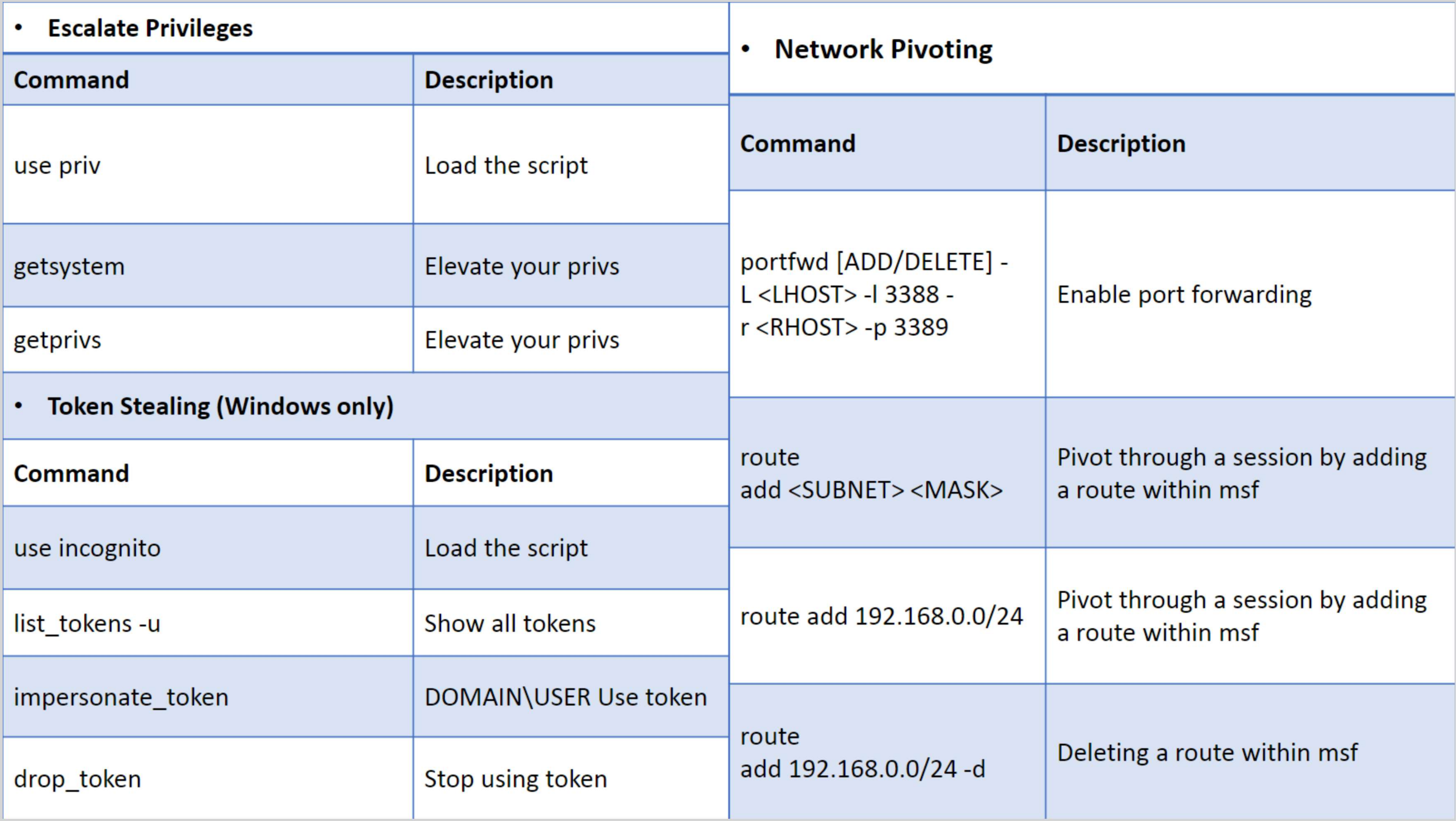
- Inside msfconsole

Command	Description
db_status	Should say connected
hosts	Show hosts in DB
services	Show ports in DB
vulns	Show all vulns found

Meterpreter Session Commands

The Meterpreter is a payload within the Metasploit Framework that provides control over an exploited target system, running as a DLL loaded inside of any process on a target machine.

Command	Description
sysinfo	Show system info
ps	Show running processes
kill <PID>	Terminate a process
getuid	Show your user ID
upload / download	Upload / download a file
pwd / lpwd	Print working directory (local / remote)
cd / lcd	Change directory (local / remote)
cat	Show contents of a file
edit <FILE>	Edit a file (vim)
shell	Drop into a shell on the target machine
migrate <PID>	Switch to another process
hashdump	Show all pw hashes (Windows only)
idletime	Display idle time of user
screenshot	Take a screenshot
clearev	Clear the logs



- **Escalate Privileges**

Command	**Description**
use priv	Load the script
getsystem	Elevate your privs
getprivs	Elevate your privs

- **Token Stealing (Windows only)**

Command	**Description**
use incognito	Load the script
list_tokens -u	Show all tokens
impersonate_token	DOMAIN\USER Use token
drop_token	Stop using token

- **Network Pivoting**

Command	**Description**
portfwd [ADD/DELETE] -L <LHOST> -l 3388 -r <RHOST> -p 3389	Enable port forwarding
route add <SUBNET> <MASK>	Pivot through a session by adding a route within msf
route add 192.168.0.0/24	Pivot through a session by adding a route within msf
route add 192.168.0.0/24 -d	Deleting a route within msf