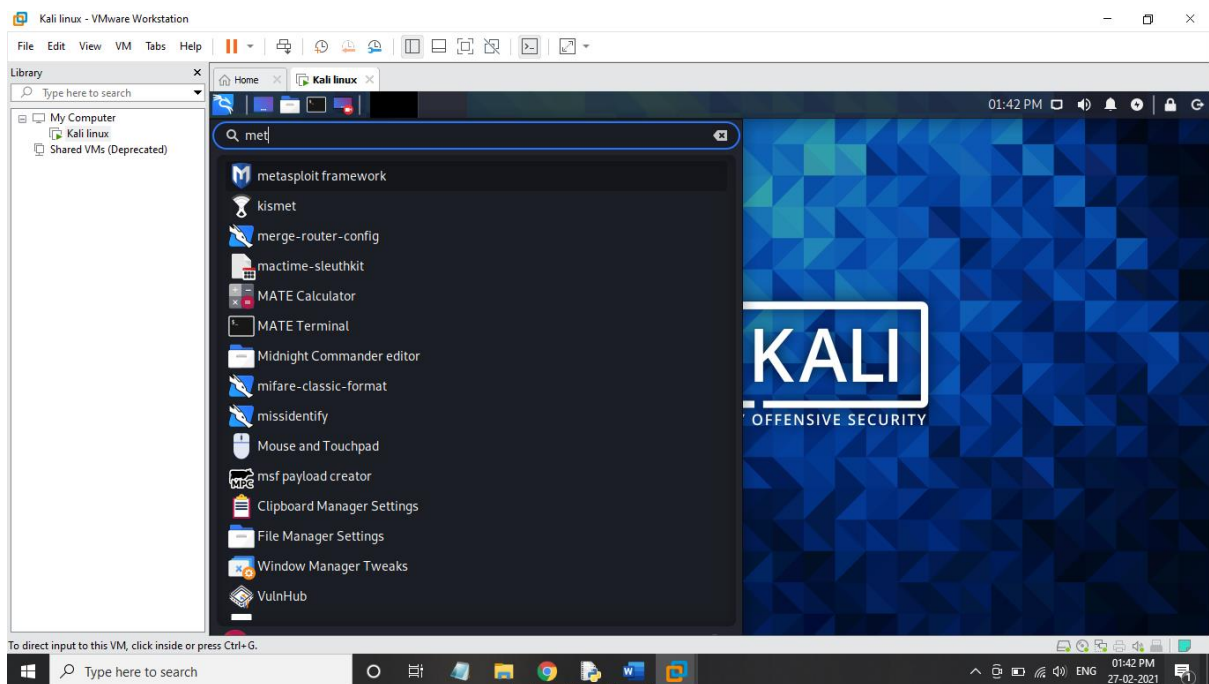
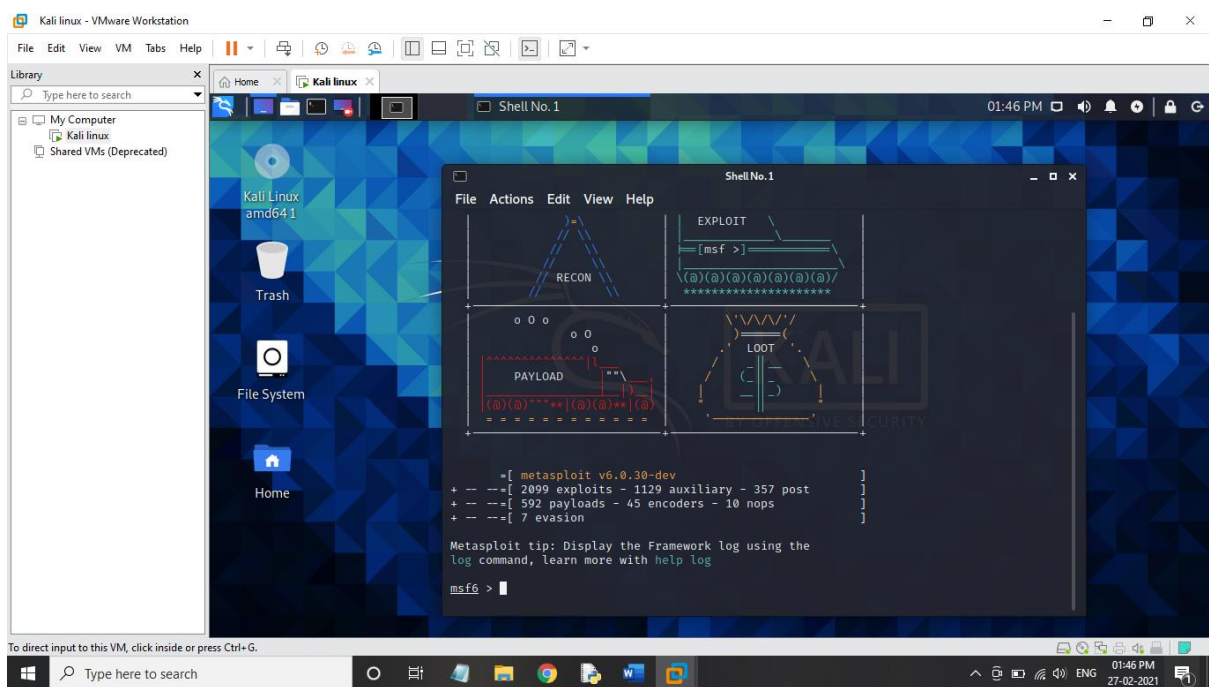


## PRACTICAL NO.9: VULNERABILITY TESTING.

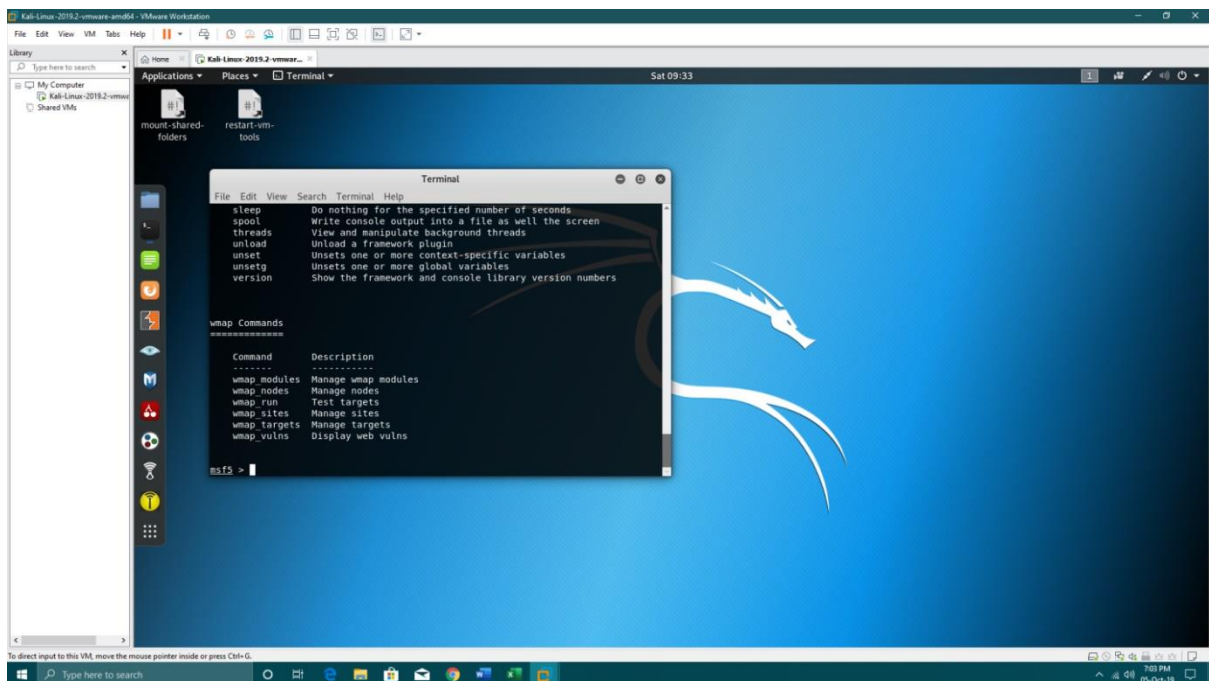
Step 1:- open metasploit.



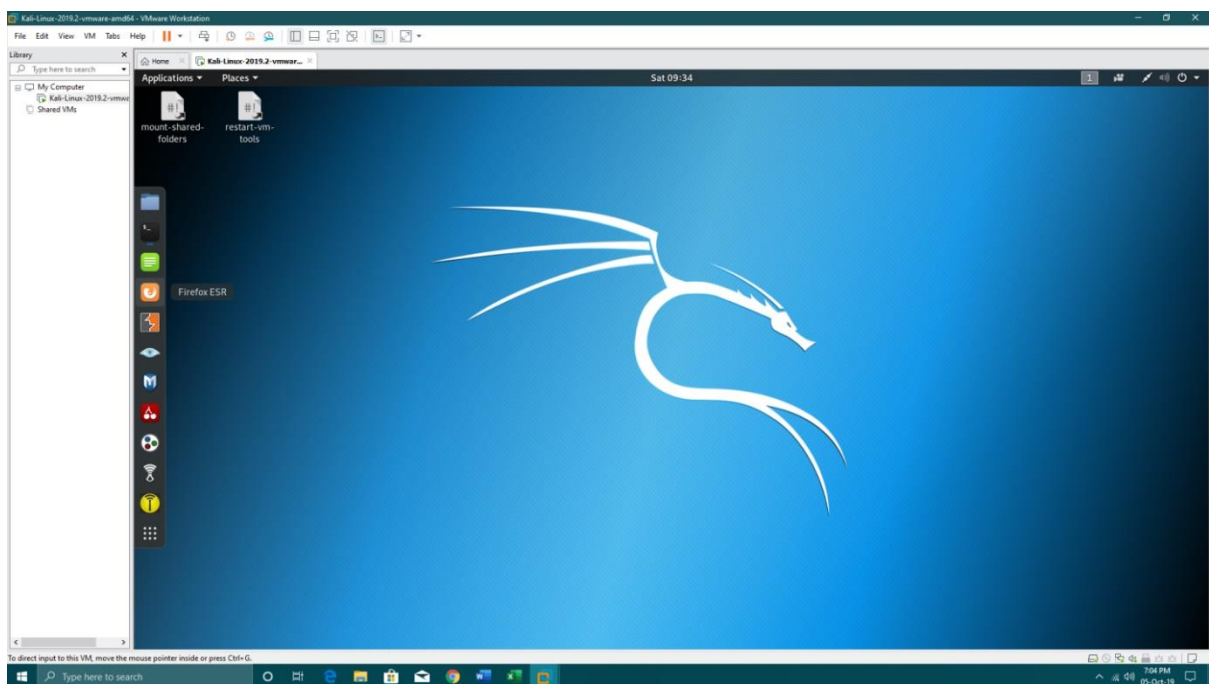
Step 2:- write load wmap.



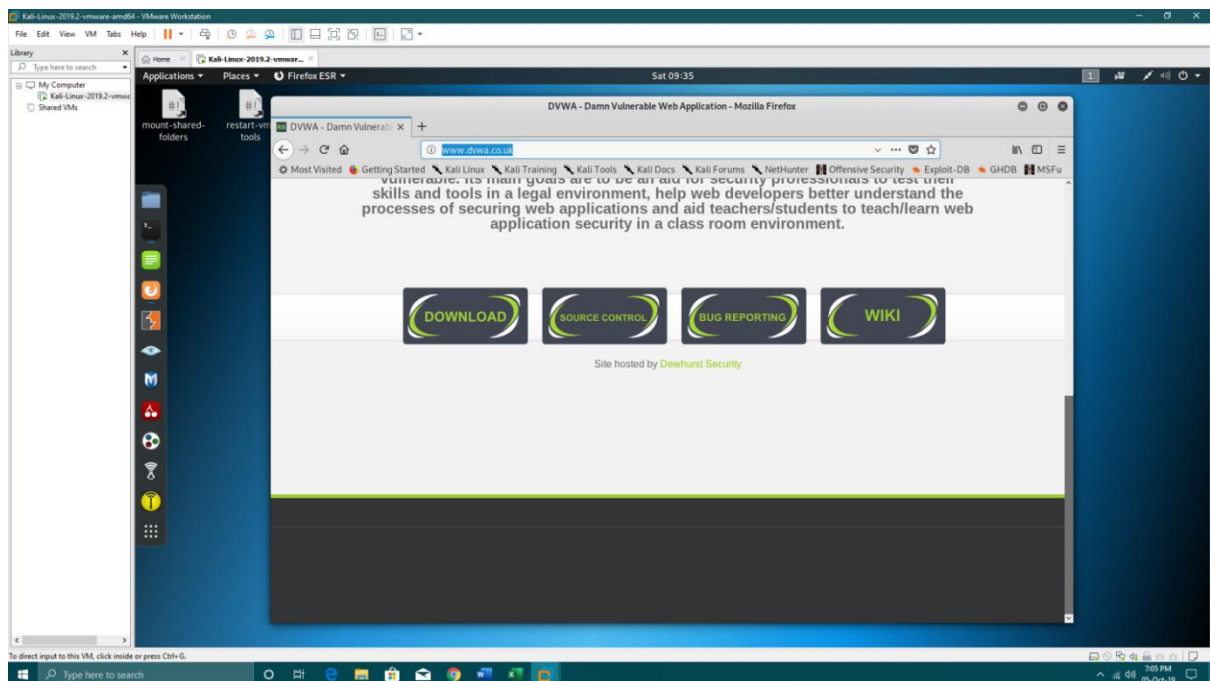
Step 3:- write help | less to know wmap commands.



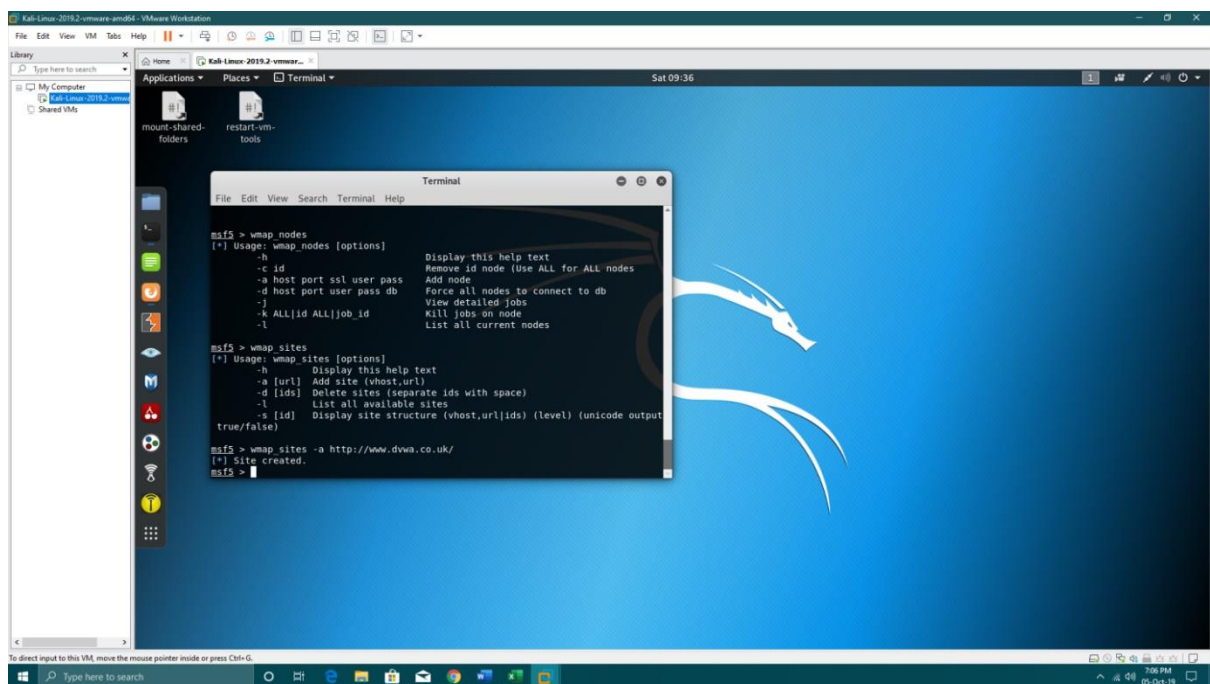
Step 4:- open firefox.



Step 5:- search a website of your own to initiate the attack.

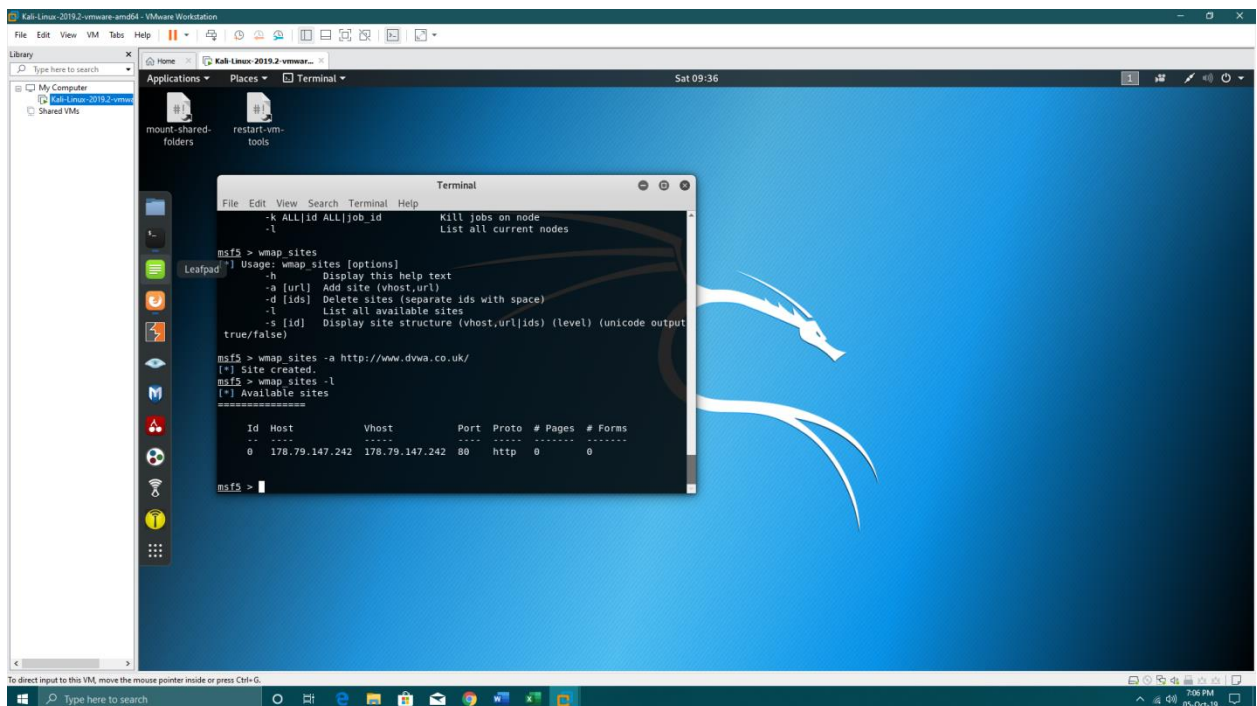


Step 6:- write wmap\_sites -a (url of your site).





Step 7:- to check if its added write wmap\_sites -l.

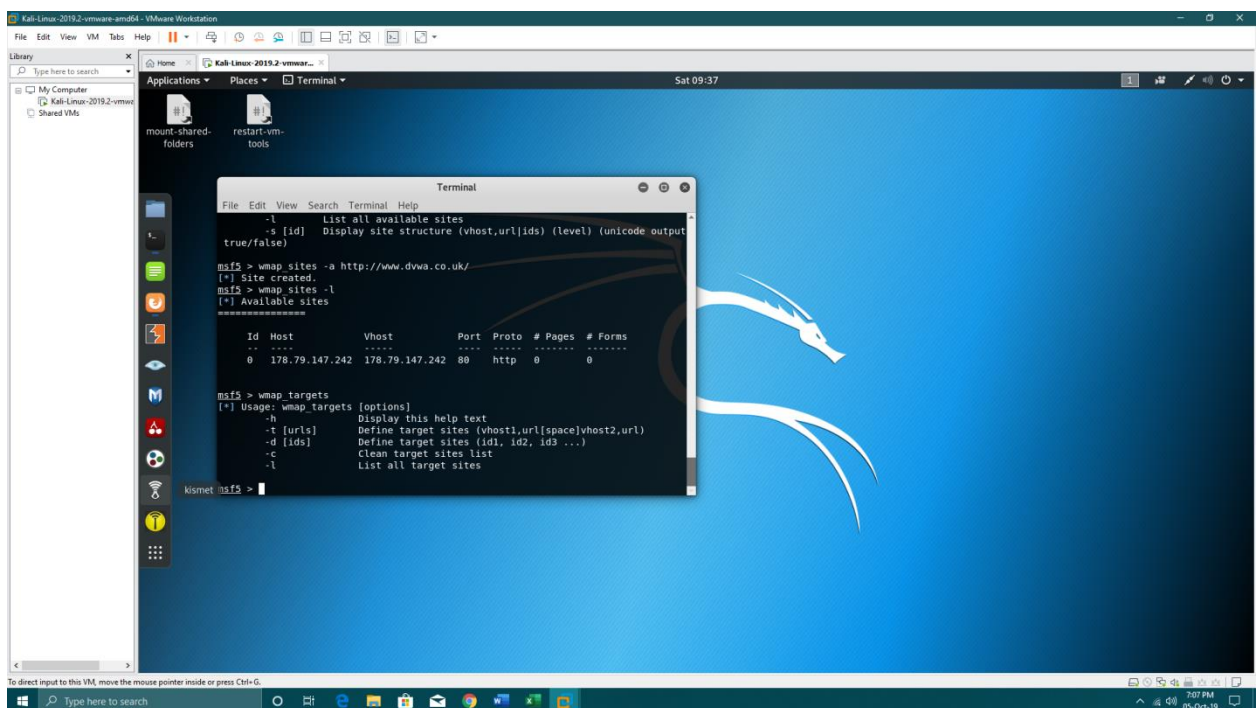


The screenshot shows a Kali Linux virtual machine window. A terminal window is open, displaying the following commands and output:

```
msf5 > wmap_sites
[*] Usage: wmap_sites [options]
-h          Display this help text
-a [url]    Add site (vhost,url)
-d [ids]    Delete sites (separate ids with space)
-l          List all available sites
-s [id]     Display site structure (vhost,url|ids) (level) (unicode output true/false)

msf5 > wmap_sites -a http://www.dvwa.co.uk/
[*] Site created.
msf5 > wmap_sites -l
[*] Available sites
=====
Id  Host          Vhost          Port  Proto  # Pages  # Forms
--  --          -
0   178.79.147.242 178.79.147.242 80    http   0        0
msf5 >
```

Step 8:- write wmap\_targets



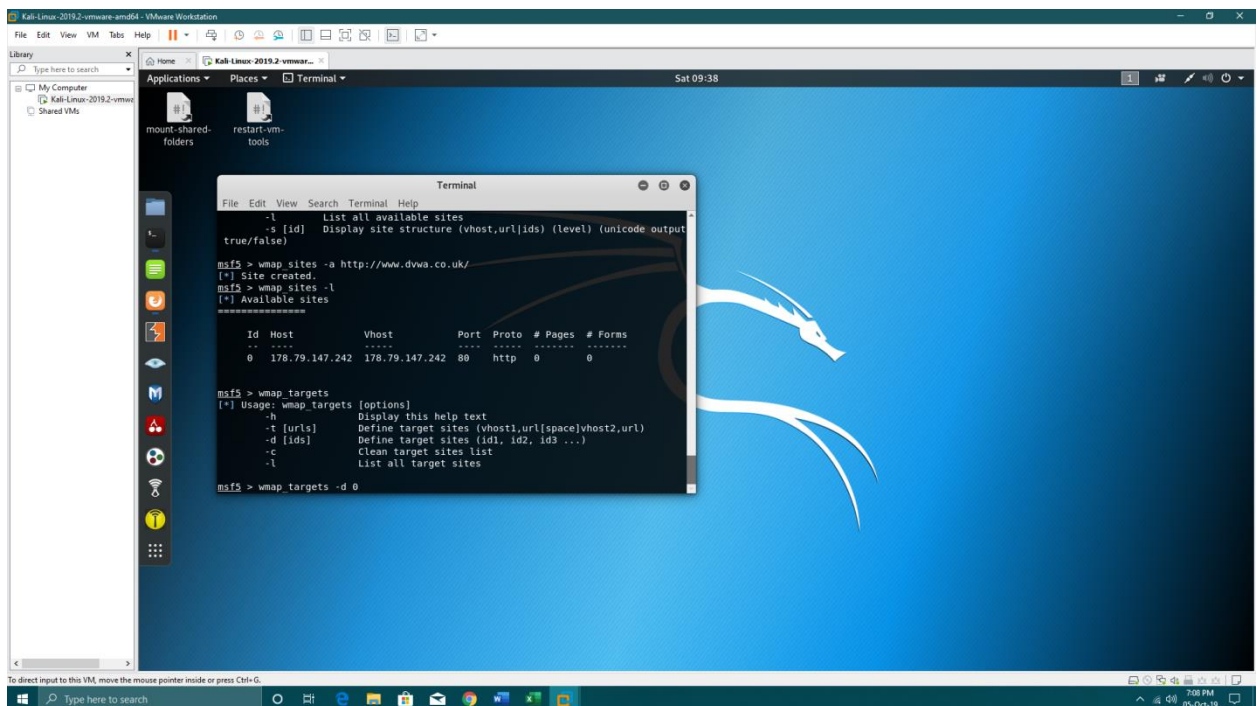
The screenshot shows the same Kali Linux virtual machine window. The terminal window now displays the following commands and output:

```
msf5 > wmap_sites -l
[*] Available sites
=====
Id  Host          Vhost          Port  Proto  # Pages  # Forms
--  --          -
0   178.79.147.242 178.79.147.242 80    http   0        0

msf5 > wmap_targets
[*] 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

msf5 >
```

Step 9:- write wmap\_targets -d 0 ( 0 is the id of our site) .



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the following commands and output:

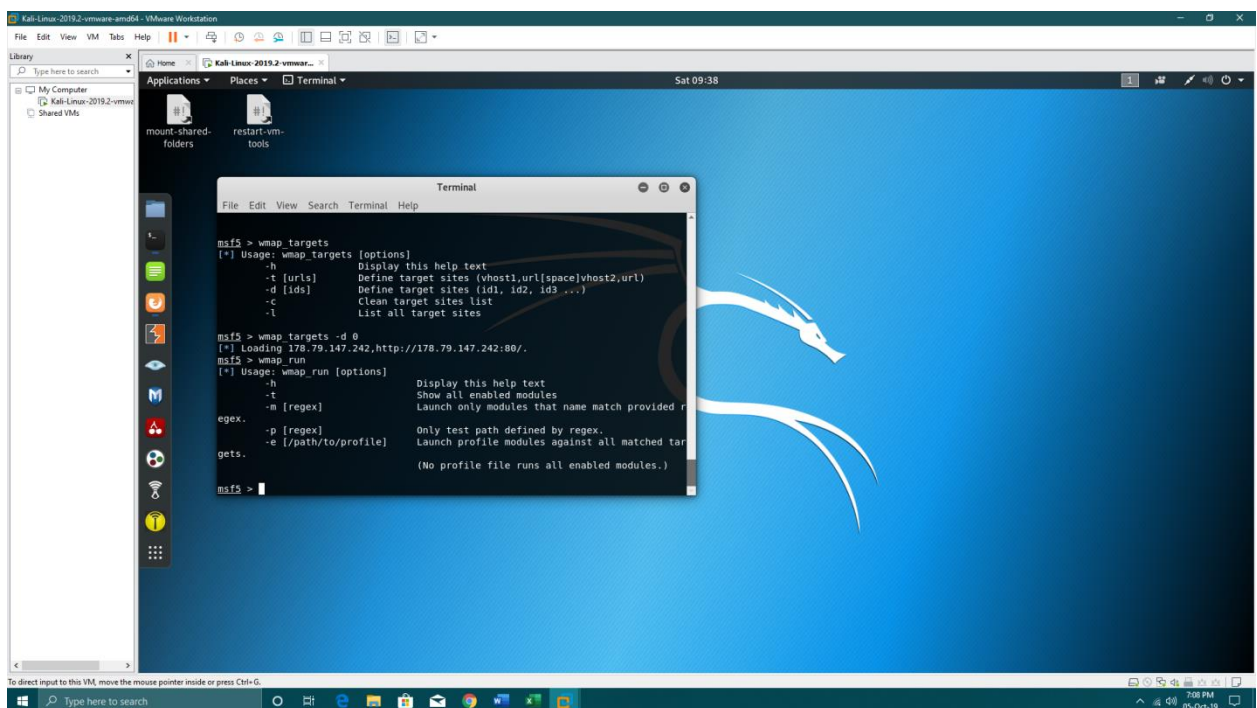
```
msf5 > wmap sites -a http://www.dvwa.co.uk/
[*] site created.
msf5 > wmap sites -l
[*] Available sites

=====
Id  Host          Vhost          Port  Proto  # Pages  # Forms
--  -
0   178.79.147.242 178.79.147.242 80    http   0        0

msf5 > wmap_targets
[*] 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

msf5 > wmap_targets -d 0
```

Step 10:- write wmap\_run.



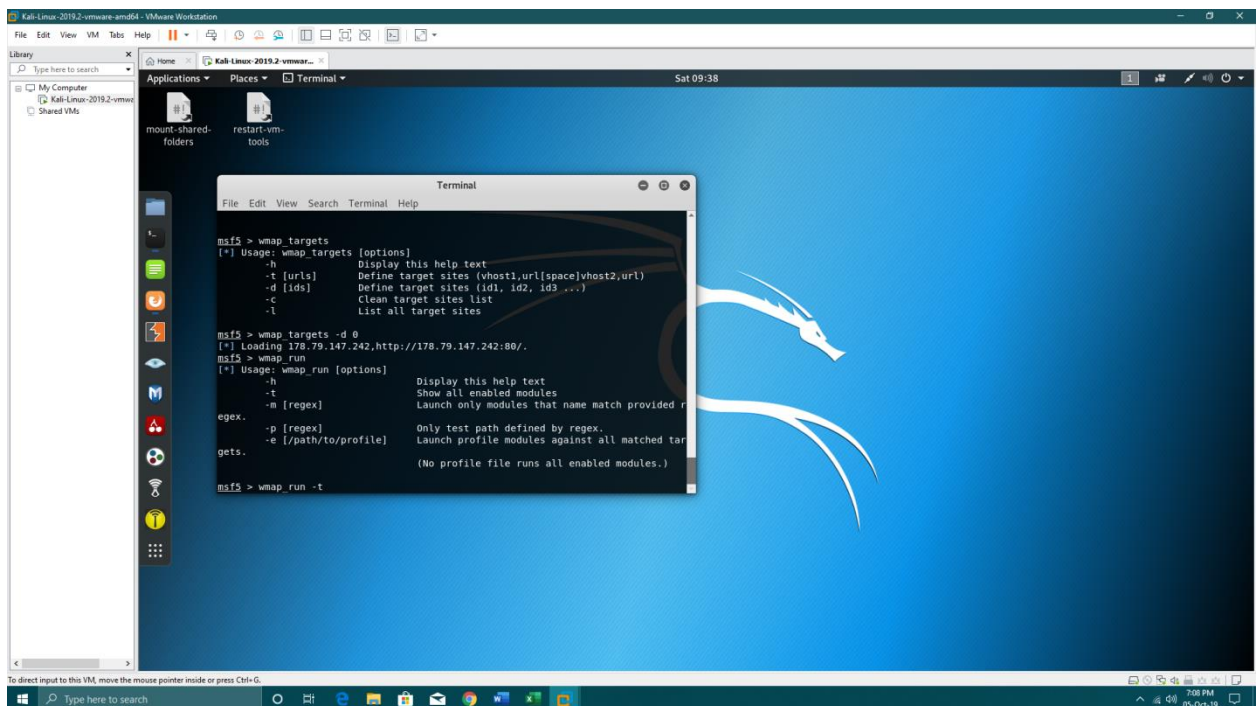
The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the following commands and output:

```
msf5 > wmap_targets
[*] 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

msf5 > wmap_targets -d 0
[*] Loading 178.79.147.242,http://178.79.147.242:80/.
msf5 > wmap_run
[*] Usage: wmap_run [options]
-h          Display this help text
-t          Show all enabled modules
-a [regex]  Launch only modules that name match provided r
egex.
-p [regex]  Only test path defined by regex.
-e [path/to/profile] Launch profile modules against all matched tar
gets.
             (No profile file runs all enabled modules.)

msf5 >
```

Step 11:- write wmap\_run -t to enable the modules.



The screenshot shows a Kali Linux virtual machine desktop. A terminal window is open, displaying the following commands and output:

```
msf5 > wmap_targets
[*] 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

msf5 > wmap_targets -d 0
[*] Loading 178.79.147.242,http://178.79.147.242:80/
msf5 > wmap_run
[*] Usage: wmap_run [options]
-h          Display this help text
-t          Show all enabled modules
-m [regex]  Launch only modules that name match provided r
egex.
-p [regex]  Only test path defined by regex.
-e [/path/to/profile] Launch profile modules against all matched tar
gets.
              (No profile file runs all enabled modules.)

msf5 > wmap_run -t
```

Step 12:- write wmap\_run -e to launch the modules against the selected site.