[root@Project-11-Task-01 ~]# nmap -sV -O 10.10.2.105

Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-16 00:17 CST

Nmap scan report for 10.10.2.105

Host is up (0.00038s latency).

Not shown: 997 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.0 (protocol 2.0)

80/tcp open http Apache httpd 2.4.37 ((centos))

3306/tcp open mysql MySQL 5.5.5-10.3.17-MariaDB

MAC Address: 08:00:27:9C:31:3B (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 3.X|4.X

OS CPE: cpe:/o:linux:linux\_kernel:3 cpe:/o:linux:linux\_kernel:4

OS details: Linux 3.2 - 4.9

Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 11.35 seconds

[root@Project-11-Task-01 ~]# nmap --script=http-methods --script=http-enum --script=http-vuln\* 10.10.2.105

Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-16 00:18 CST

Nmap scan report for 10.10.2.105

Host is up (0.00020s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

| http-enum:

| /wp-login.php: Possible admin folder

| /: WordPress version: 5.3.2

| /wp-includes/images/rss.png: Wordpress version 2.2 found.

| /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.

| /wp-includes/images/blank.gif: Wordpress version 2.6 found.

| /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.

| /wp-login.php: Wordpress login page.

| /wp-admin/upgrade.php: Wordpress login page.

| /readme.html: Interesting, a readme.

|\_ /icons/: Potentially interesting folder w/ directory listing

| http-methods:

|\_ Supported Methods: GET HEAD POST OPTIONS

3306/tcp open mysql

MAC Address: 08:00:27:9C:31:3B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 10.86 seconds

[root@Project-11-Task-01 ~]# nmap --script=http-php-version --script=http-phpmyadmin-dir-traversal --script=http-phpself-xss --script=http-vuln-cve2012-1823 10.10.2.105

Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-16 00:19 CST

Nmap scan report for 10.10.2.105

Host is up (0.00025s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

|\_http-php-version: Version from header x-powered-by: PHP/7.3.5

3306/tcp open mysql

MAC Address: 08:00:27:9C:31:3B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 8.52 seconds

[root@Project-11-Task-01 ~]# nmap --script=mysql-info --script=mysql-empty-password --script=mysql-enum --script=mysql-vuln\* 10.10.2.105

Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-16 00:21 CST

Nmap scan report for 10.10.2.105

Host is up (0.00030s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

3306/tcp open mysql

| mysql-enum:

| Valid usernames:

| root:<empty> - Valid credentials

| netadmin:<empty> - Valid credentials

| user:<empty> - Valid credentials

| web:<empty> - Valid credentials

| test:<empty> - Valid credentials

| sysadmin:<empty> - Valid credentials

| administrator:<empty> - Valid credentials

| webadmin:<empty> - Valid credentials

| admin:<empty> - Valid credentials

| guest:<empty> - Valid credentials

|\_ Statistics: Performed 10 guesses in 1 seconds, average tps: 10.0

| mysql-info:

| Protocol: 10

| Version: 5.5.5-10.3.17-MariaDB

| Thread ID: 106

| Capabilities flags: 63486

| Some Capabilities: ODBCClient, Support41Auth, SupportsTransactions, IgnoreSigpipes, LongColumnFlag, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, InteractiveClient, SupportsCompression, IgnoreSpaceBeforeParenthesis, ConnectWithDatabase, SupportsLoadDataLocal, Speaks41ProtocolOld, FoundRows, SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleStatments

| Status: Autocommit

| Salt: :'SNmZ[;Tsg+=1{=[41:

|\_ Auth Plugin Name: 94

MAC Address: 08:00:27:9C:31:3B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.80 seconds

[root@Project-11-Task-01 ~]# nmap --script=http-wordpress-enum --script=http-wordpress-users --script=http-wordpress-brute --script=http-vuln-cve2014-8877 --script=http-vuln-cve2017-1001000 10.10.2.105

Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-16 00:25 CST

Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 70.00% done; ETC: 00:25 (0:00:12 remaining)

Stats: 0:02:59 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 70.00% done; ETC: 00:29 (0:01:16 remaining)

Nmap scan report for 10.10.2.105

Host is up (0.00033s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

| http-wordpress-brute:

| Accounts: No valid accounts found

|\_ Statistics: Performed 3240 guesses in 599 seconds, average tps: 5.3

| http-wordpress-enum:

| Search limited to top 100 themes/plugins

| themes

| twentyseventeen 2.2

| plugins

|\_ akismet 4.1.3

| http-wordpress-users:

| Username found: ruanxiaolong

|\_Search stopped at ID #25. Increase the upper limit if necessary with 'http-wordpress-users.limit'

3306/tcp open mysql

MAC Address: 08:00:27:9C:31:3B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 601.71 seconds