Практикалық сабақ №6: Қауіпсіздікті тестілеу әдістемесі

Linux: curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && chmod 755 msfinstall && ./msfinstall

Windows: http://windows.metasploit.com/metasploitframework-latest.msi

Metasploit-framework бағдарламасының көмегімен тестілеу әдістемесін төмендегі суреттерге мысалында жасаңыз:

```
gulzinat@gulzinat-VirtualBox:~$ msfconsole
```

```
msf6 > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    color         Toggle color
    connect       Communicate with a host
    debug         Display information useful for debugging
    exit          Exit the console
```

```
msf6 > search wordpress
```

```
No     WordPress XMLRPC GHOST Vulnerability Scanner
15  auxiliary/scanner/http/wordpress_login_enum
No     WordPress Brute Force and User Enumeration Utility
```

```
msf6 > use auxiliary/scanner/http/wordpress_login_enum
msf6 auxiliary(scanner/http/wordpress_login_enum) >
```

```
msf6 auxiliary(scanner/http/wordpress_login_enum) > info

       Name: WordPress Brute Force and User Enumeration Utility
     Module: auxiliary/scanner/http/wordpress_login_enum
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Tiago Ferreira <tiago.ccna@gmail.com>
  Zach Grace <zgrace@404labs.com>
  Christian Mehlmauer <FireFart@gmail.com>
```

```
msf6 auxiliary(scanner/http/wordpress_login_enum) > set RHOSTS 192.168.33.10
RHOSTS => 192.168.33.10
msf6 auxiliary(scanner/http/wordpress_login_enum) >
```

Өзіндік жұмыс

1) Қосымшаны орнату;

2) Metasploit-framework бағдарламасының командаларымен жұмыс жасау.