Cybersecurity workshop

#todo #tools :

1. VirtualBox
2. Install kali linux for vb.
3. install maltego
4. install burpsuite
5. install foxyproxy on firefox

#reference : http://tinyurl.com/vitsep1722

KALI LINUX

1. ping website : to check connectivity

2. man any-command : to know about any commands

3. **Basic Commands :**

   #commands
   #APT: to download from internet

   1. apt -> sudo
   2. search : "sudo apt-cache search [app]" .
   3. show : "sudo apt-cache show vlc" to show the size and deets of the [app].
   4. install : "sudo apt-get install [app]"
   5. uninstall : "sudo apt-get remove [app]"
   6. update : "sudo apt-get update [app]"
   7. upgrade : "sudo apt-get upgrade [app]"
   8. uname -an : to check the kali linux version

   #DPKG: .deb is the extension for all Debian based applications and to install such files, we need DPKG package.

   1. install : "sudo dpkg -i [app.deb]"
   2. remove : "sudo dpkg -r [app.deb]"
   3. list : "dpkg -l"
   4. list specific tool : "dpkg -l [app]"

4. 1)VOIP : Voice Over Internet Protocol.
   2) TG : Tickegram.
   3) CDR : Call Data Record.

5. https://whois.domaintools.com/ : to find the domain details of a website. #tools

6. https://digital.com/best-web-hosting/who-is/](https://digital.com/best-web-hosting/who-is/) : to find the hosting details. #tools

7. https://builtwith.com/ : to find the list of websites in the server #tools

8. Wappalyzer : to find the development tools. #tools

9. http://virustotal.com/ : to find the sub-domains of the site. #tools

10. Maltego : a single tool to do all the above mentioned services. #tools

11. #commands nmap [website] : give details of open ports.

12. Maltego : Open → Machines → Run Machine → Footprinting L1 → type Domain name.

13. Dingtone or actionvoip : for voip #tools

14. Google working process (to find vulnerability):

    1. irurl admin.php
    2. intitle
    3. intext
    4. index of [keyword]
    5. filetype:[type] [keyword]
    6. site:[region]

15. finding Vulnerability :

    ### Sensitive Data Exposure:

    ```
    1) filetype:inc intext:mysql_connect
    2) Directory traversal :  intitle:backup+index of :
    3) wp-admin is the backup of the entire file.
    ```

16. Google Hacking Database : 1) https://www.exploit-db.com/google-hacking-database #tools

17. **SQL Injection :**

    1. inurl admin.php / adminlogin.php
    2. > *' or 1-1#* *#query*
    3. use this query as username and password for admin.php page and out of 50, you might be able to find 2 vulnerable sites.
    4. search "[website] responsible disclosure" to find the bugs. Do this to find the scope (/sub-domains) and find vulnerabilities only in that scope to get bounty.
    5. Configuring Burpsuite and browser :
        1. goto display and change fint size to 18.
        2. goto proxy , goto options and in VMWare or others, you won't find a port.
        3. Add port in that case. Use 8080 or 8081 port.
        4. Then goto browser and search foxyproxy and use addons.
        5. Click the addon and goto options, click add and type name , localhost as IP and port number.
        6. now select it.
        7. try https://demo.testfire.net.
        8. Goto burpsuite and goto intercept and check the logs, the website will be still loading.
        9. Goto burpsuite and click forward.
        10. Adding certificate : burp:8080 and click on CA certificate to download.
        11. preferences/settings in browser -> search certificates -> authorities -> import certificates.
        12. userrecon : get it from github, clone the git url
        13. Execute userrecon.sh using "bash userrecon.sh"
        14. zphisher tool -> use it.

18. **Pentmenu:** #tools

    ```
    1) pentmenu -> download from github (git clone)
    2) open terminal and redirect to pentmenu folder.
    3) to execute ./pentmenu and choose dos attack (2)
    4) choose slowloris (9)
    ```

```
5) type target site
6) type port number : 80
7) type default connect : 2000
```

19. privacy tools : privacy dashboard android app #tools

20. **Email spoofing: https://emkei.cz/** #tools

21. #command nslookup -q=mx [mail-domain] : to see the server of the domain

22. to check for the authenticity of the mail id, copy the header and use header analysis tools. https://mxtoolbox.com/EmailHeaders.aspx #tools

23. Hosting a site in TOR: we can use xamp/wamp server to host a site.

24. Run the xamp server -> write a php code in notepad -> then check the internet for deets of it. #hosting

25. Malware analysis : https://www.hybrid-analysis.com/ #tools

26. Upload a apk to https://builtwith.com/ and check for vulnerabilities #tools

27. Wifi Hacking : wifi pineapple #tools

28. OMG cable is a hardware used as USB cable and can hack

29. Hack RF one , aplha device, infection moneky #tools

30. Nessus is a vulnerability testing tool. #tools

31. Grabify to find IP adrress #tools

32. Google Go / Rust / Shell for cyber security. #languages

33. CTF, Hackthebox, picoctf, pentester lab, post swigger lab for ethical hacking #resources