**ASSIGNMENT NO.- 1**

Name: Pratik Patil

Roll No.: 469

Write a socket program to scan host vulnerabilities

**CODE:**

**import socket # Importing socket**

**def isVulnerable(banner,vulne): # Checking if the running service is vulnerable**

**f = open(vulne,'r')**

**for vulnerability in f.readlines():**

**if vulnerability in banner:**

**return True**

**return False**

**if \_\_name\_\_ == "\_\_main\_\_":**

**# Scanning the IP**

**ip = raw\_input("Enter the IP Address: ")**

**# Scanning the following ports**

**portList = [20, 21, 23, 22, 53, 80, 443, 143]**

**# Setting timeout to 2 seconds incase socket not able to connect**

**socket.setdefaulttimeout(2)**

**count = 0**

**vulne = raw\_input(“Enter the variability file name: “)**

**print ip**

**# Iterating through the ports**

**for port in portList:**

**try:**

**# Initialize Socket**

**s = socket.socket()**

**# Attempt to connect with socket, exception if fails to connect**

**s.connect((ip, port))**

**# Receive banner of running service**

**banner = s.recv(1024)**

**# Checks if vulnerable**

**if isVulnerable(banner,vulne):**

**print "[+]Vulnerability Found on Port", port, ":", banner**

**count += 1**

**except:**

**# Continue the loop in case of port not connecting or down**

**continue**

**# If count is more than 0, the machine is vulnerable**

**if count:**

**print "========================\nMachine is Vulnerable\n========================\n"**

**else:**

**print "========================\nMachine is Not Vulnerable\n========================\n"**