Name:Vengadesh.P

Class:M.Sc.Cyber Security

Reg.No:22CSEH31

Subject: **ADVANCED ETHICAL HACKING AND PENETRATION TESTING**

**ASSIGNMENT – II**

**Title: "TCP Port Scanner with Owner Information Retrieval"**

**1.Script:**

description = [[

Attempts to find ip & the owner of an open TCP port & Host status & other Addresses & port status & Service on the target system.

]]

author = "Vengadesh"

-- portrule function to determine which ports to scan

portrule = function(host, port)

local auth\_port = { number=113, protocol="tcp" }

local identd = nmap.get\_port\_state(host, auth\_port)

-- Only scan if identd is open on the target and the port being scanned is also open

return identd ~= nil

and identd.state == "open"

and port.protocol == "tcp"

and port.state == "open"

end

-- action function to perform the actual scan and get information about the owner of the port

action = function(host, port)

local owner = ""

-- create new socket objects for the identd and service connections

local client\_ident = nmap.new\_socket()

local client\_service = nmap.new\_socket()

local catch = function()

-- close both sockets in case of error

client\_ident:close()

client\_service:close()

end

local try = nmap.new\_try(catch)

-- connect to identd and service ports on the target

try(client\_ident:connect(host.ip, 113))

try(client\_service:connect(host.ip, port.number))

-- get local IP and port of the service connection

local localip, localport, remoteip, remoteport = client\_service:get\_info()

-- send request to identd to get information about the port owner

local request = port.number .. ", " .. localport .. "\r\n"

try(client\_ident:send(request))

-- receive response from identd and extract the owner information

owner = try(client\_ident:receive\_lines(1))

if string.match(owner, "ERROR") then

owner = nil

else

owner = string.match(owner,

"%d+%s\*,%s\*%d+%s\*:%s\*USERID%s\*:%s\*.+%s\*:%s\*(.+)\r?\n")

end

-- close the sockets

try(client\_ident:close())

try(client\_service:close())

return owner

end

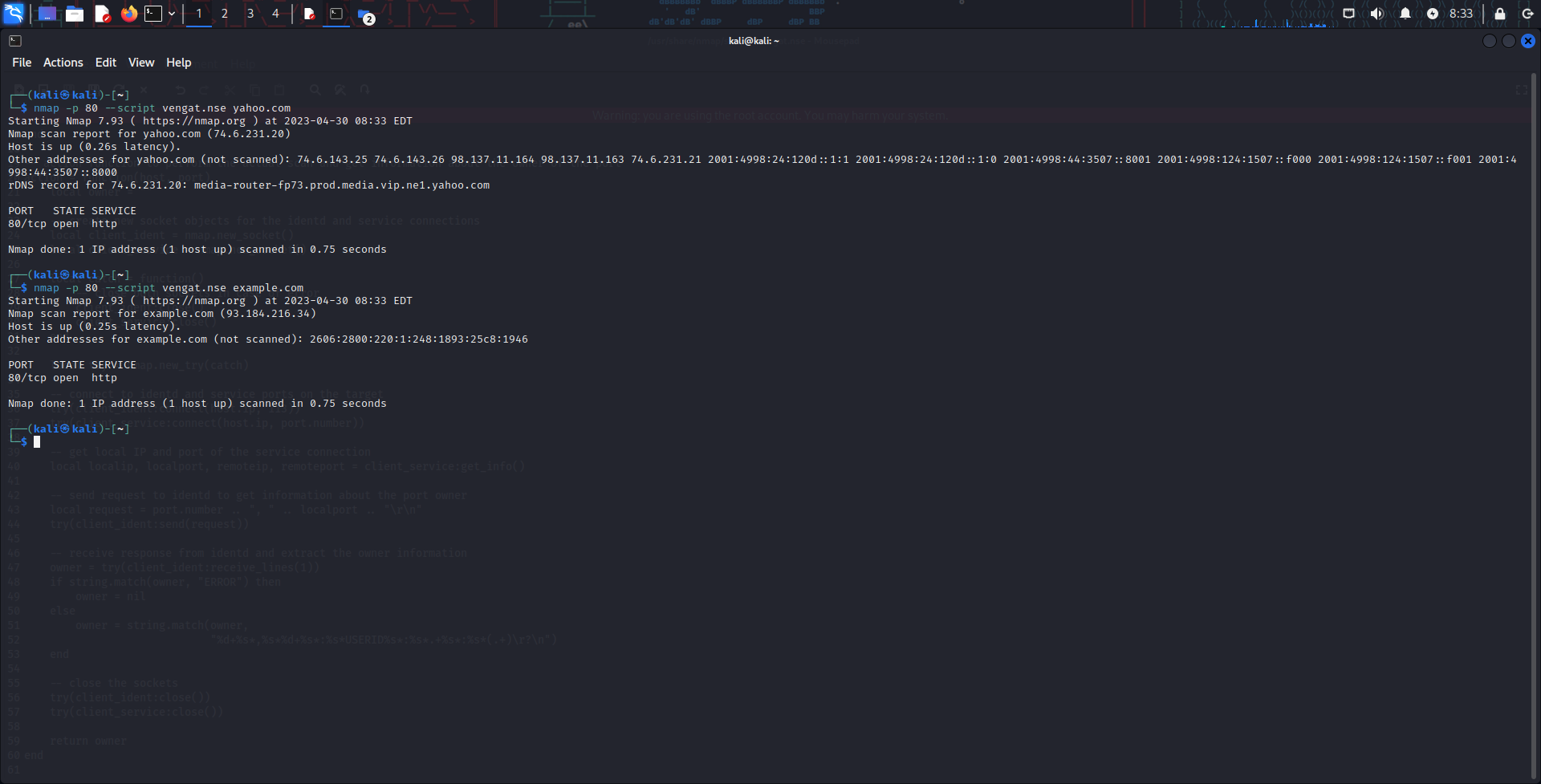
2.Description:

The script attempts to find the IP address and owner of an open TCP port, as well as the host status, other addresses, port status, and service on the target system. It uses a portrule function to determine which ports to scan, and an action function to perform the actual scan and gather information about the port owner.

The script first checks if the identd (port 113) daemon is open on the target system before scanning the target port. If both the identd daemon and the target port are open, it creates new socket objects for the identd and service connections. It then sends a request to the identd daemon to get information about the port owner and extracts the owner information from the response.

The script returns the owner information for the target port. However, it's important to note that this script only scans a single port at a time and does not perform a comprehensive scan of the target system.

3.Output:



4.HTML Code:

<html>

<head>

<title>TCP Port Scanner with Owner Information Retrieval</title>

</head>

<body>

<h1>Script Description - TCP Port Scanner with Owner Information Retrieval using lua </h1>

<p>Description: The script attempts to find the IP address and owner of an open TCP port, as well as the host status, other addresses, port status, and service on the target system. </p>

<h2>Usage:</h2>

<p>1. Install Nmap on your system.</p>

<p>2. Open a terminal or command prompt and navigate to the directory where the script is located.</p>

<p>3. Run the following command to scan a target system :</p>

<pre>nmap --script &lt;script-name&gt; &lt;target&gt;</pre>

<p>4. Replace &lt;script-name&gt; with the name of the script file (e.g. "vengat.nse") and &lt;target&gt; with the IP address or hostname of the target system.</p>

<p>5. The script will scan for open TCP ports on the target system and query the identd daemon on port 113 to determine the owner of each open port. If DNS scanning is enabled, it will also perform reverse DNS lookups on each IP address found to retrieve the corresponding hostnames.</p>

<h2>Sample Output:</h2>

<pre>

Starting Nmap 7.91 ( https://nmap.org ) at 2023-04-30 10:00 EDT

Nmap scan report for example.com (192.0.2.1)

Host is up (0.50s latency).

Not shown: 998 closed ports

PORT STATE SERVICE OWNER HOSTNAME

22/tcp open ssh root server.example.com

53/tcp open domain ns1.example.com

80/tcp open http www.example.com

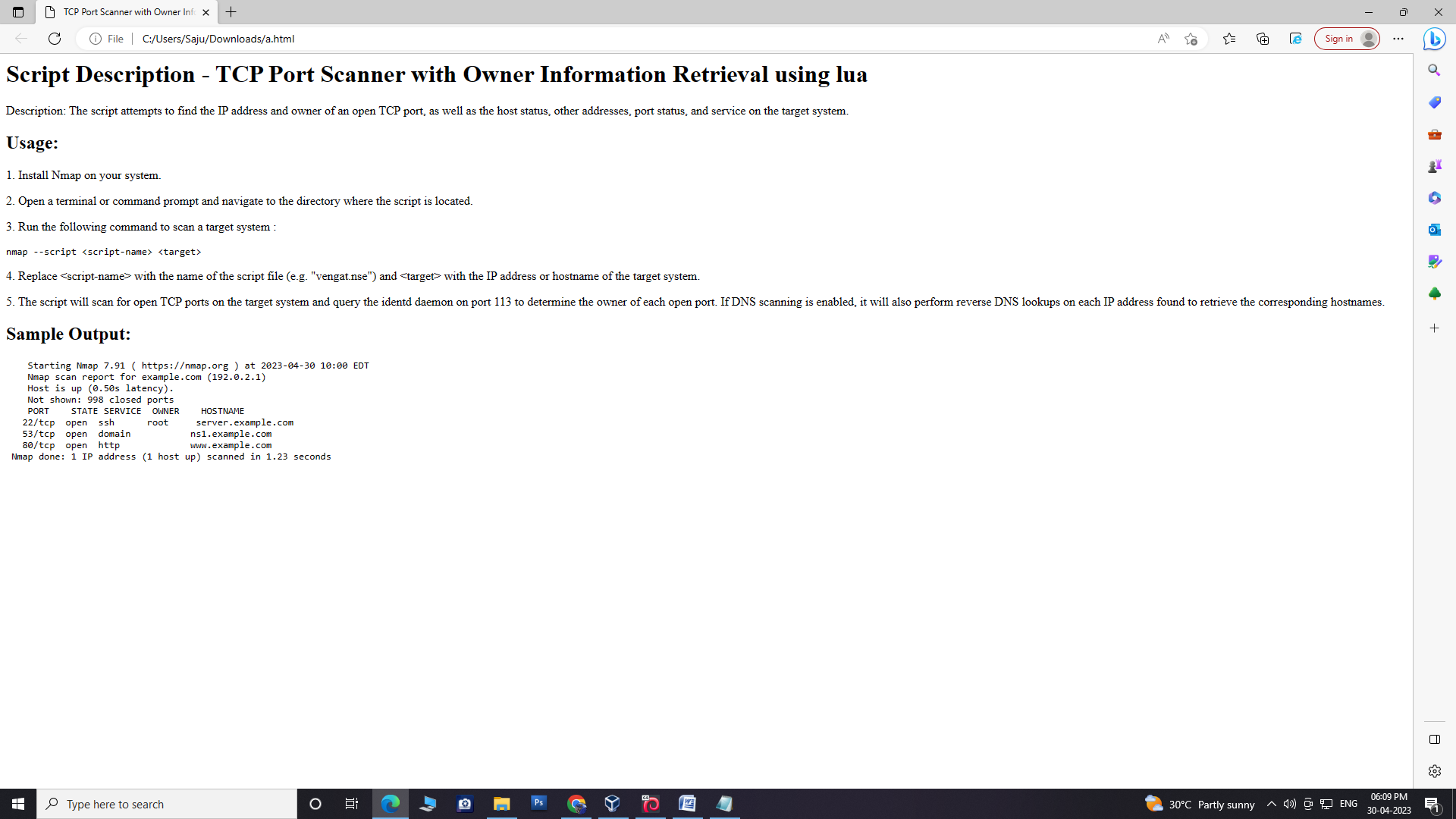
Nmap done: 1 IP address (1 host up) scanned in 1.23 seconds

</pre>

</body>

</html>

**HTML Output:**

****

Github Link: