InternsElite

"Rule the world with elite"

InternsElite

MAJOR PROJECT

Cyber Security program

Name:- Dharmendra Kumar
Program Name:-CYBER SECURITY PROGRAM
Roll no:- 24/CS/J1456
Submission Date:- 21/07/2024

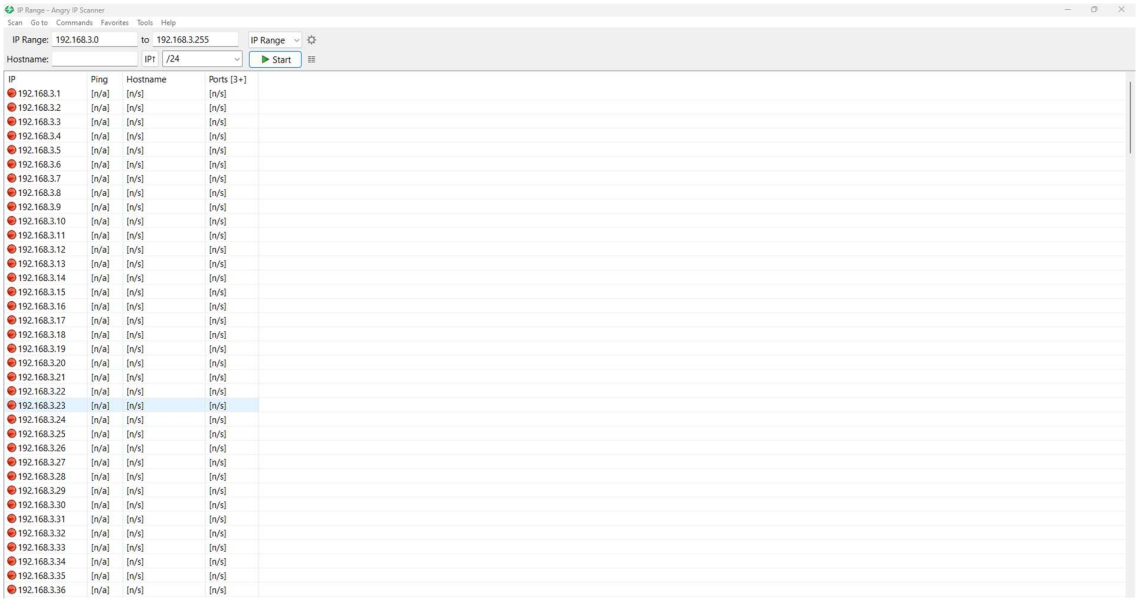
CYBER SECURITY – MAJOR PROJECT

TASK:-1 Use Angry IP Scanner for Network Scanning.

Network scanning refers to the process of identifying active devices on a network and gathering information about them. This activity is crucial for network administrators to manage and secure their networks effectively.

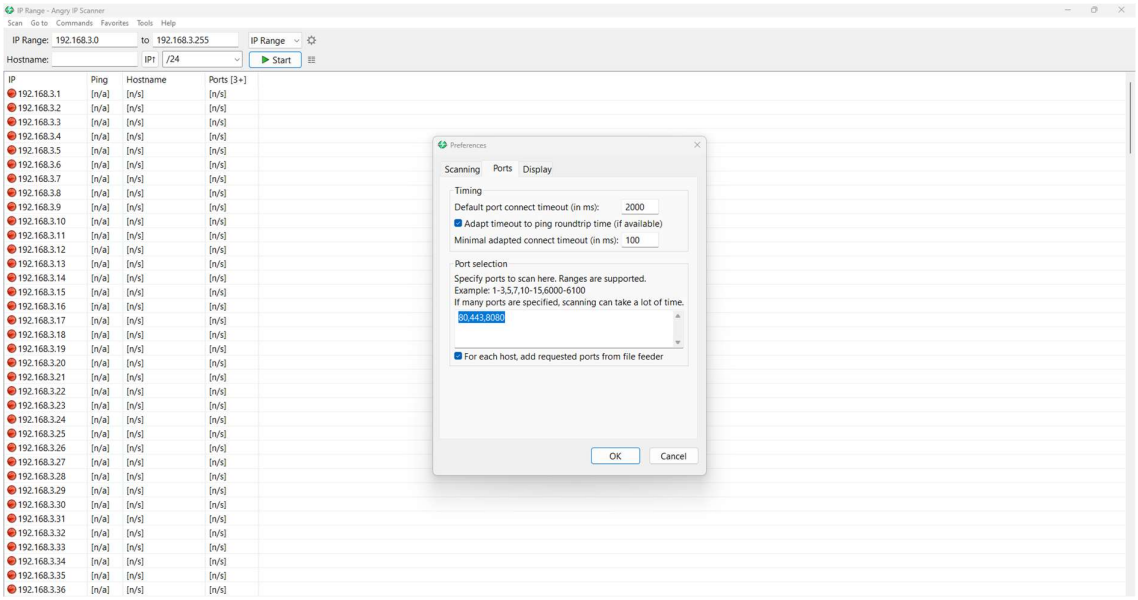
Angry IP Scanner: A lightweight tool for fast IP address and port scanning.

Step:- 1 Firstly, I use a Network IP address and set an IP range in the network, then I set the netmask. then click to start button.



The second step is to click on "Ports" and then navigate to "Ports Preferences."

Then If many ports are specified, scanning can take a lot of time



Finally, I conduct a scan of all ports.

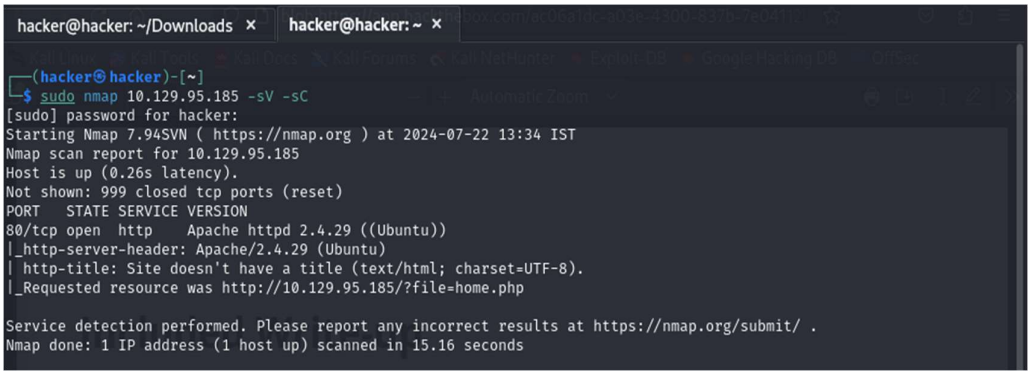
The first task is end

TASK:-2 Use Nmap/Zenmap Tool for Network Reconnaissance

One of the most renowned open-source network security scanning tools among pentesters is Network Mapper (Nmap). Nmap, a command-line utility, leverages multiple network protocols and advanced functionalities to scan hosts for open TCP and UDP ports, identify operating systems, extract service banners, and perform other detailed assessments. Enumeration involves actively establishing connections to target systems to uncover potential attack vectors, including discovering hosts, services, domains, URLs, and valid user accounts for potential exploitation.

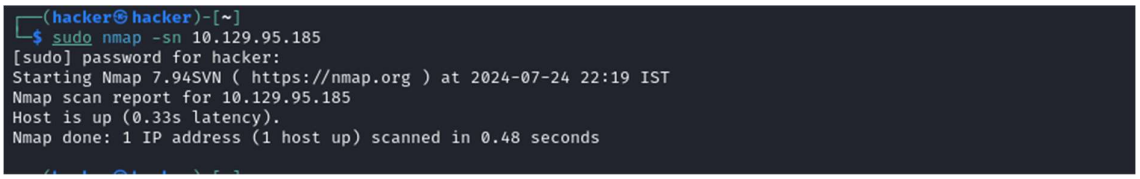
Step:-1 For Examples :-

This command, sudo nmap 10.129.95.185 -sV -sC , conducts a comprehensive scan that identifies live hosts within the specified IP range, while also performing service version detection (-sV) and running default scripts (-sC).



Then the next uses is

The command sudo nmap -sn 10.129.95.185 is shortened to perform a ping scan (-sn) on the IP address 10.129.95.185. This scan is used to identify which hosts are up on the network without performing detailed port scanning.



Then the next use is

The command sudo nmap -sF 10.129.95.185 is used to conduct a FIN scan (-sF) on the IP address 10.129.95.185.

```
┌──(hacker㉿hacker)-[~]
└─$ sudo nmap -sF 10.129.95.185
[sudo] password for hacker:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-24 22:19 IST
Nmap scan report for 10.129.95.185
Host is up (0.24s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE         SERVICE
80/tcp open|filtered http

Nmap done: 1 IP address (1 host up) scanned in 9.72 seconds
```

Then the next use is

The command sudo nmap -sU 10.129.95.185 is used to perform a UDP scan on the specified IP address (10.129.95.185)

```
┌──(hacker㉿hacker)-[~]
└─$ sudo nmap -sU 10.129.95.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-24 22:18 IST
Nmap scan report for 10.129.95.185
Host is up (0.32s latency).
Not shown: 998 closed udp ports (port-unreach)
PORT   STATE         SERVICE
68/udp open|filtered dhcpc
69/udp open|filtered tftp

Nmap done: 1 IP address (1 host up) scanned in 1022.78 seconds
```

Then the different command is nmap tool like as uses :-

```
┌──(hacker㉿hacker)-[~]
└─$ nmap -h
Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
```

```
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --noninteractive: Disable runtime interactions via keyboard
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
```

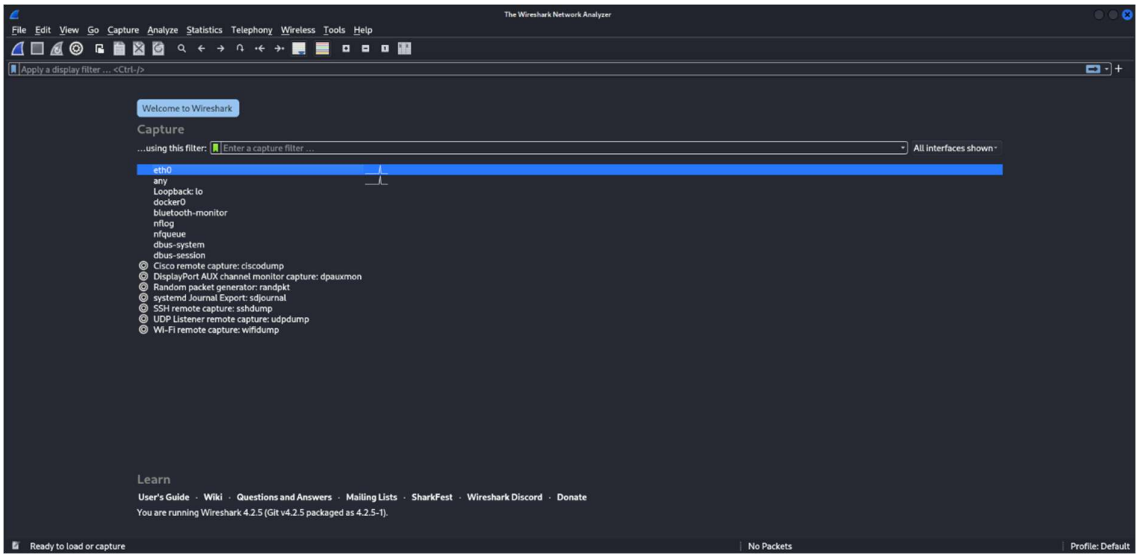
```
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
```

The Second Task is end

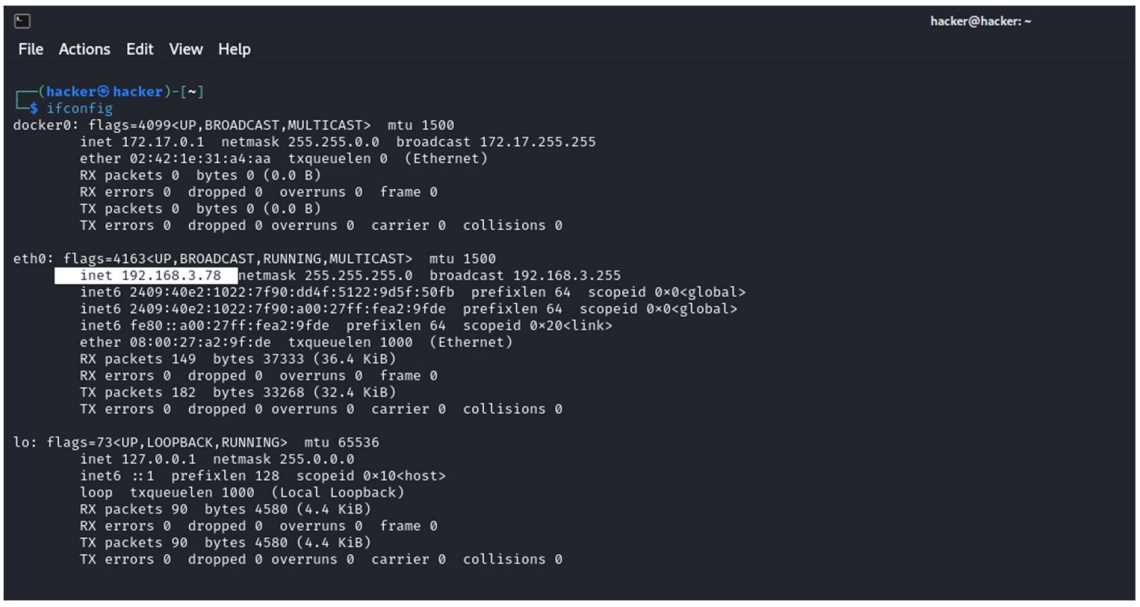
TASK:-3 Perform Sniffing for capturing the Passwords by wireshark

I am going to wireshark tool

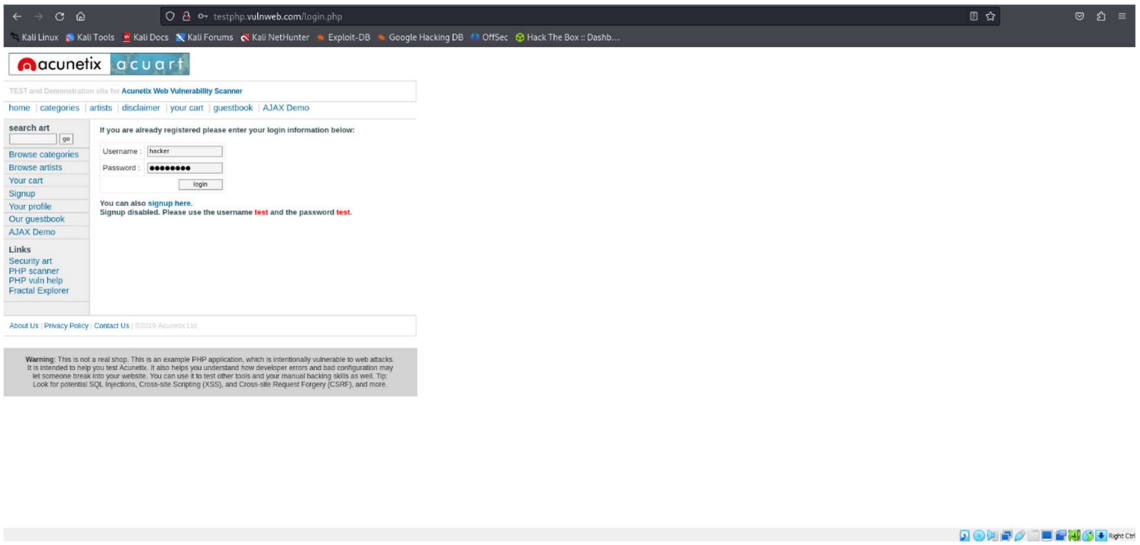
Step:-1 After opening Wireshark, the interface appears as follows:



Step:- 2 I am see the internet IP and then copying it to the internet IP." and then go to wireshark.

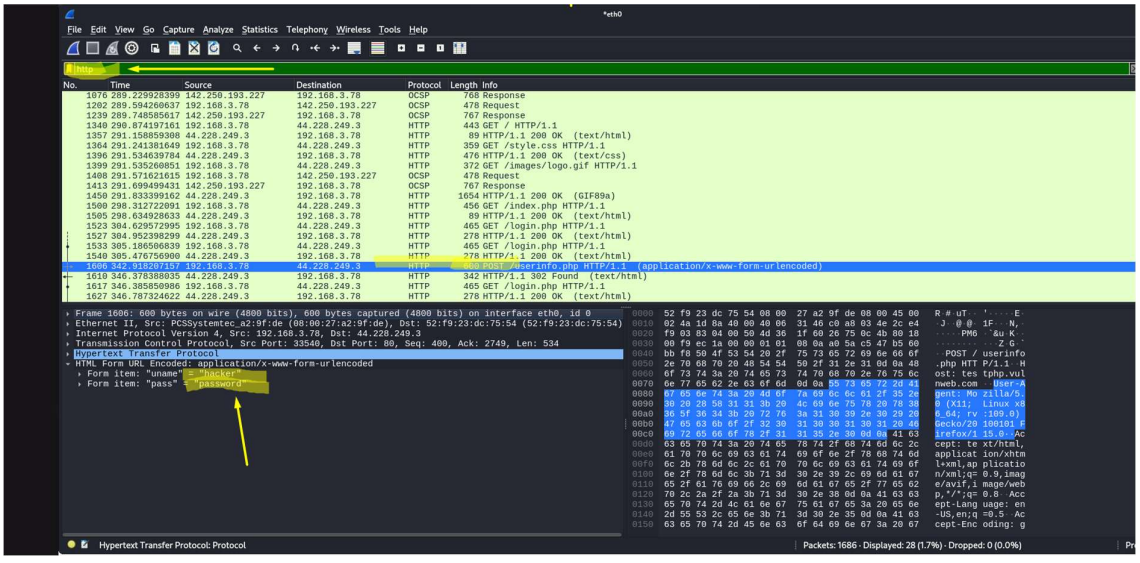


Step:-3 I am going to the website, filling in the username and password, and then clicking the login button. And Then go to the wireshark.



Step:-4 Then, filter for HTTP and proceed to the POST method in Hypertext Transfer Protocol.

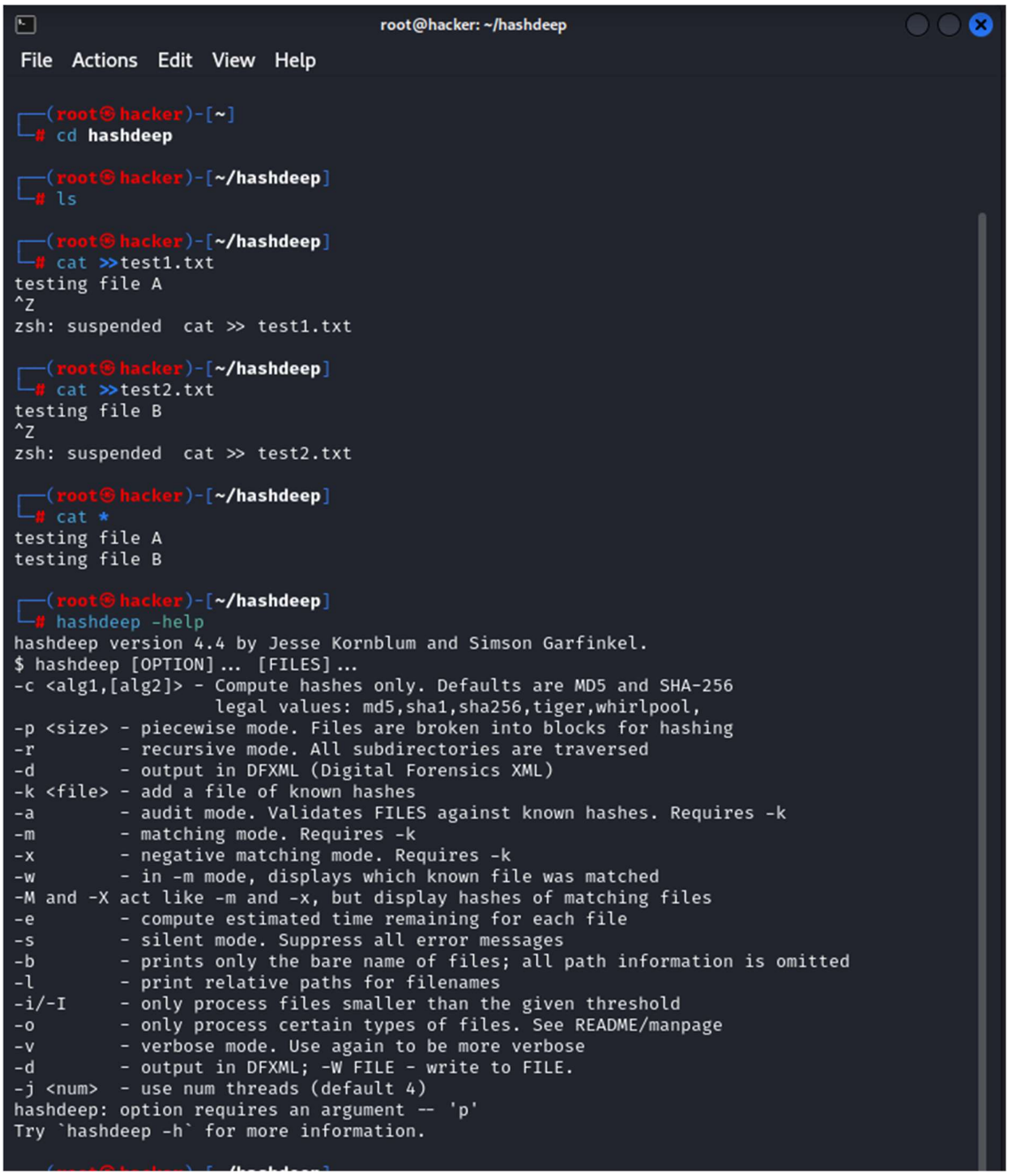
And then click to the HTML Form URL Encoded.



The Third Task is End

TASK:-4 Perform Data Auditing with Hashdeep.

Then follow the steps



```
┌──(root㉿hacker)-[~/dharm2]
└─# hashdeep test1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /root/dharm2
## # hashdeep test1.txt
##
14,997a9f00e25f85b73ffb1898376b7186,76d793c71e4f153583c2687898468b4068db96782fcc793a2282abdf684a52c3,/root/dharm2/test1.txt

┌──(root㉿hacker)-[~/dharm2]
└─# hashdeep test1.txt>test1_hash.txt

┌──(root㉿hacker)-[~/dharm2]
└─# ls
test1.txt  test1_hash.txt  test2.txt

┌──(root㉿hacker)-[~/dharm2]
└─# cat test1_hash.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /root/dharm2
## # hashdeep test1.txt
##
14,997a9f00e25f85b73ffb1898376b7186,76d793c71e4f153583c2687898468b4068db96782fcc793a2282abdf684a52c3,/root/dharm2/test1.txt
```

```
┌──(root㉿hacker)-[~/dharm2]
└─# hashdeep -a test1.txt -k test1_hash.txt
hashdeep: Audit passed

┌──(root㉿hacker)-[~/dharm2]
└─# vi test1.txt
```


```
┌──(root㉿hacker)-[~/dharm2]
└─# cat test1.txt
testing file1 this is file
```

THE END TASK

6. Give command of windows and Linux for Network/Server Details gathering

Windows Commands

1. **Get IP Configuration:**

ipconfig

```
Microsoft Windows [Version 10.0.22631.3958]
(c) Microsoft Corporation. All rights reserved.

C:\Users\dharm>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d58c:4482:a0eb:21c8%5
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:40e2:1022:7f90:a2e2:f480:1fb0:9c43
   Temporary IPv6 Address. . . . . . : 2409:40e2:1022:7f90:b099:46a:2d7:bc68
   Link-local IPv6 Address . . . . . : fe80::521:38d4:6be3:9516%20
   IPv4 Address. . . . . . . . . . . : 192.168.3.39
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::50f9:23ff:fedc:7554%20
                                       192.168.3.165

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : bbrouter
```

Windows Commands

2. **View Routing Table:**

route print

```
C:\Users\dharm>route print
===========================================================================
Interface List
  5...0a 00 27 00 00 05 ......VirtualBox Host-Only Ethernet Adapter
 12...28 c5 d2 cc 24 79 ......Microsoft Wi-Fi Direct Virtual Adapter
  8...2a c5 d2 cc 24 78 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 20...28 c5 d2 cc 24 78 ......Intel(R) Wi-Fi 6E AX211 160MHz
 13...d0 ad 08 a7 18 e1 ......Realtek Gaming GbE Family Controller
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.3.165    192.168.3.39     35
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.3.0    255.255.255.0         On-link      192.168.3.39    291
     192.168.3.39  255.255.255.255         On-link      192.168.3.39    291
    192.168.3.255  255.255.255.255         On-link      192.168.3.39    291
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link      192.168.3.39    291
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link      192.168.3.39    291
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 20     51 ::/0                     fe80::50f9:23ff:fedc:7554
  1    331 ::1/128                  On-link
 20     51 2409:40e2:1022:7f90::/64 On-link
 20    291 2409:40e2:1022:7f90:a2e2:f480:1fb0:9c43/128
                                    On-link
 20    291 2409:40e2:1022:7f90:b099:46a:2d7:bc68/128
                                    On-link
  5    281 fe80::/64                On-link
 20    291 fe80::/64                On-link
 20    291 fe80::521:38d4:6be3:9516/128
                                    On-link
```

```
  5    281 fe80::d58c:4482:a0eb:21c8/128
                                    On-link
  1    331 ff00::/8                 On-link
  5    281 ff00::/8                 On-link
 20    291 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

3. Display Active Network Connections:

netstat -an

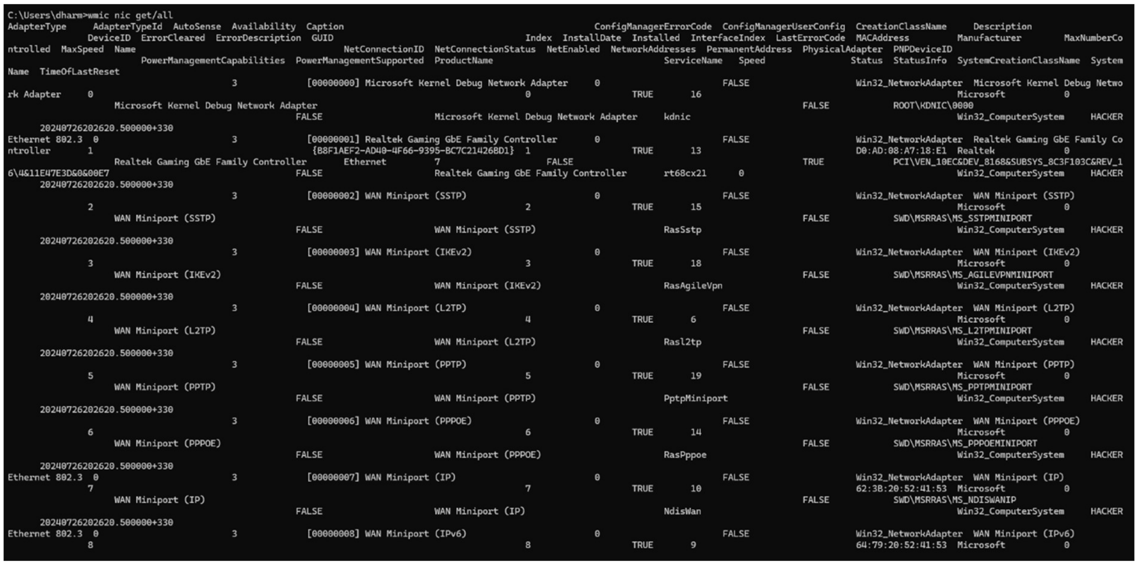
```
C:\Users\dharm>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49694        127.0.0.1:49695        ESTABLISHED
  TCP    127.0.0.1:49695        127.0.0.1:49694        ESTABLISHED
  TCP    127.0.0.1:49696        127.0.0.1:49697        ESTABLISHED
  TCP    127.0.0.1:49697        127.0.0.1:49696        ESTABLISHED
  TCP    192.168.3.39:139       0.0.0.0:0              LISTENING
  TCP    192.168.3.39:60853     192.168.3.165:53       TIME_WAIT
  TCP    192.168.3.39:60854     192.168.3.165:53       TIME_WAIT
  TCP    192.168.3.39:60855     192.168.3.165:53       TIME_WAIT
  TCP    192.168.3.39:60856     192.168.3.165:53       TIME_WAIT
  TCP    192.168.3.39:60857     192.168.3.165:53       TIME_WAIT
  TCP    192.168.3.39:60858     192.168.3.165:53       TIME_WAIT
  TCP    192.168.3.39:60875     192.168.3.165:53       TIME_WAIT
  TCP    192.168.3.39:60876     192.168.3.165:53       TIME_WAIT
  TCP    192.168.3.39:60877     192.168.3.165:53       TIME_WAIT
  TCP    192.168.3.39:60878     192.168.3.165:53       TIME_WAIT
  TCP    192.168.3.39:60879     192.168.3.165:53       TIME_WAIT
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:49664             [::]:0                 LISTENING
  TCP    [::]:49665             [::]:0                 LISTENING
  TCP    [::]:49666             [::]:0                 LISTENING
  TCP    [::]:49667             [::]:0                 LISTENING
  TCP    [::]:49668             [::]:0                 LISTENING
  TCP    [::]:49670             [::]:0                 LISTENING
  TCP    [::1]:49669            [::]:0                 LISTENING
  TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:49409  [2603:1040:a06:6::]:443  ESTABLISHED
  TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:57712  [2603:1063:2202:14::3]:443  ESTABLISHED
  TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:58819  [64:ff9b::14d4:5875]:443  ESTABLISHED
  TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:58822  [2404:6800:4003:c03::bc]:5228  ESTABLISHED
  TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:58844  [2405:200:1630:18a::1011]:443  CLOSE_WAIT
  TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:58946  [2603:1063:2202:14::3]:443  ESTABLISHED
  TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:59199  [2a03:2880:f26b:c8:face:b00c:0:7260]:80  ESTABLISHED
  TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:60585  [2620:1ec:21::14]:443  ESTABLISHED
  TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:60827  [64:ff9b::14bd:ad1a]:443  TIME_WAIT
  TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:60828  [64:ff9b::d6b:2a0c]:443  ESTABLISHED
  TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:60852  [2603:1046:1406::5]:443  TIME_WAIT
```

```
TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:60827  [64:ff9b::14bd:ad1a]:443  TIME_WAIT
TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:60828  [64:ff9b::d6b:2a0c]:443  ESTABLISHED
TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:60852  [2603:1046:1406::5]:443  TIME_WAIT
TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:60859  [2603:1046:1400::7]:443  TIME_WAIT
TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:60860  [2603:1046:1400::1]:443  ESTABLISHED
TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:60861  [2405:200:160b:1731::312c:b752]:443  ESTABLISHED
TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:60863  [2405:200:160b:1731::312c:b74b]:443  ESTABLISHED
TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:60868  [2603:1046:900:54::2]:443  ESTABLISHED
TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:60869  [2620:1ec:33::254]:443  ESTABLISHED
TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:60870  [2a01:111:202c::254]:443  ESTABLISHED
TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:60871  [2606:2800:147:120f:30c:1ba0:fc6:265a]:443  ESTABLISHED
TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:60872  [64:ff9b::98c3:264c]:80  ESTABLISHED
TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:60873  [64:ff9b::cc4f:c5de]:443  ESTABLISHED
TCP    [2409:40e2:1022:7f90:b099:46a:2d7:bc68]:60874  [2603:1046:1400::7]:443  TIME_WAIT
UDP    0.0.0.0:500            *:*
UDP    0.0.0.0:4500           *:*
UDP    0.0.0.0:5050           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5355           *:*
UDP    0.0.0.0:49244          0.0.32.10:443
UDP    0.0.0.0:54108          0.0.32.14:443
UDP    0.0.0.0:56586          *:*
UDP    0.0.0.0:57486          *:*
UDP    127.0.0.1:1900         *:*
UDP    127.0.0.1:51705        *:*
UDP    127.0.0.1:62435        127.0.0.1:62435
UDP    192.168.3.39:137       *:*
UDP    192.168.3.39:138       *:*
UDP    192.168.3.39:1900      *:*
UDP    192.168.3.39:51704     *:*
UDP    192.168.56.1:137       *:*
UDP    192.168.56.1:138       *:*
UDP    192.168.56.1:1900      *:*
UDP    192.168.56.1:51703     *:*
UDP    [::]:500               *:*
UDP    [::]:4500              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
```

```
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5355              *:*
UDP    [::]:49244             [2404:6800:4002:80a::200a]:443
UDP    [::]:54108             [2404:6800:4002:813::200e]:443
UDP    [::]:56586             *:*
UDP    [::]:57486             *:*
UDP    [::1]:1900             *:*
UDP    [::1]:51702            *:*
UDP    [fe80::521:38d4:6be3:9516%20]:1900  *:*
UDP    [fe80::521:38d4:6be3:9516%20]:51701  *:*
UDP    [fe80::d58c:4482:a0eb:21c8%5]:1900  *:*
UDP    [fe80::d58c:4482:a0eb:21c8%5]:51700  *:*
```

4. **Get Network Adapter Details:**

wmic nic get /all



5. **View Network Shares:**

net share

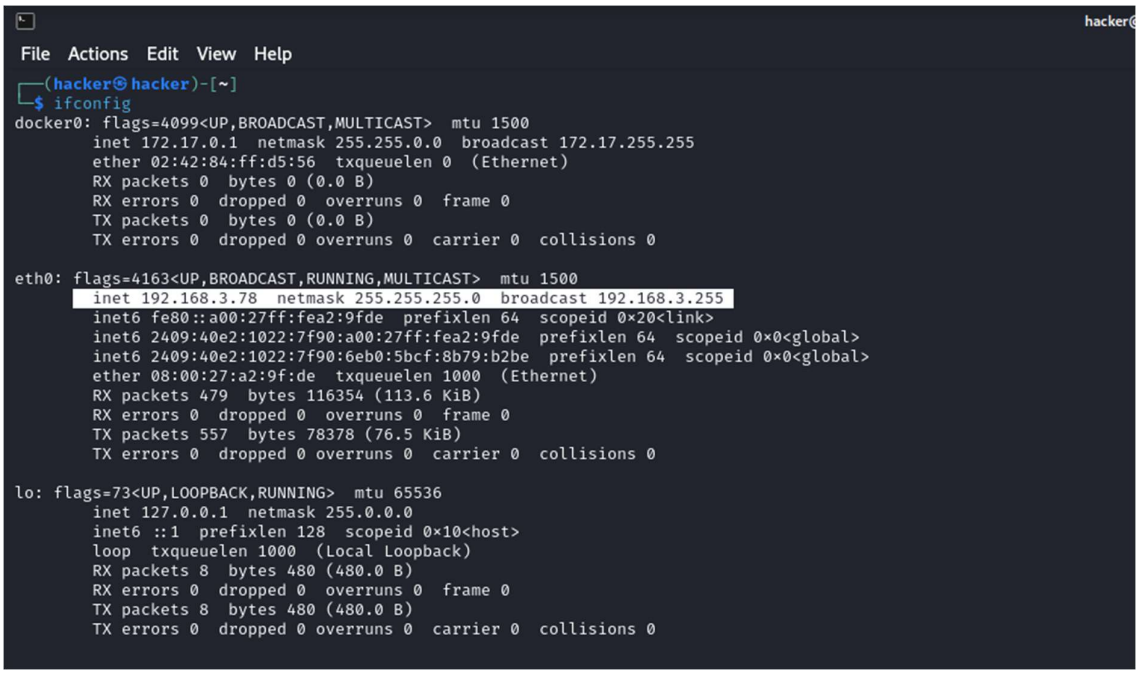
6. **Check DNS Configuration:**
   nslookup

```
C:\Users\dharm>net share

Share name   Resource                        Remark

------------------------------------------------------------------------------
C$           C:\                             Default share
D$           D:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\Windows                      Remote Admin
The command completed successfully.


C:\Users\dharm>nslookup
Default Server:  UnKnown
Address:  192.168.3.165

> |
```

Give command of Linux for Network/Server Details gathering

1. **Get IP Configuration:**

ifconfig



or, on newer systems:

View Routing Table:

route -n

or, on newer systems:

ip route

Display Active Network Connections:

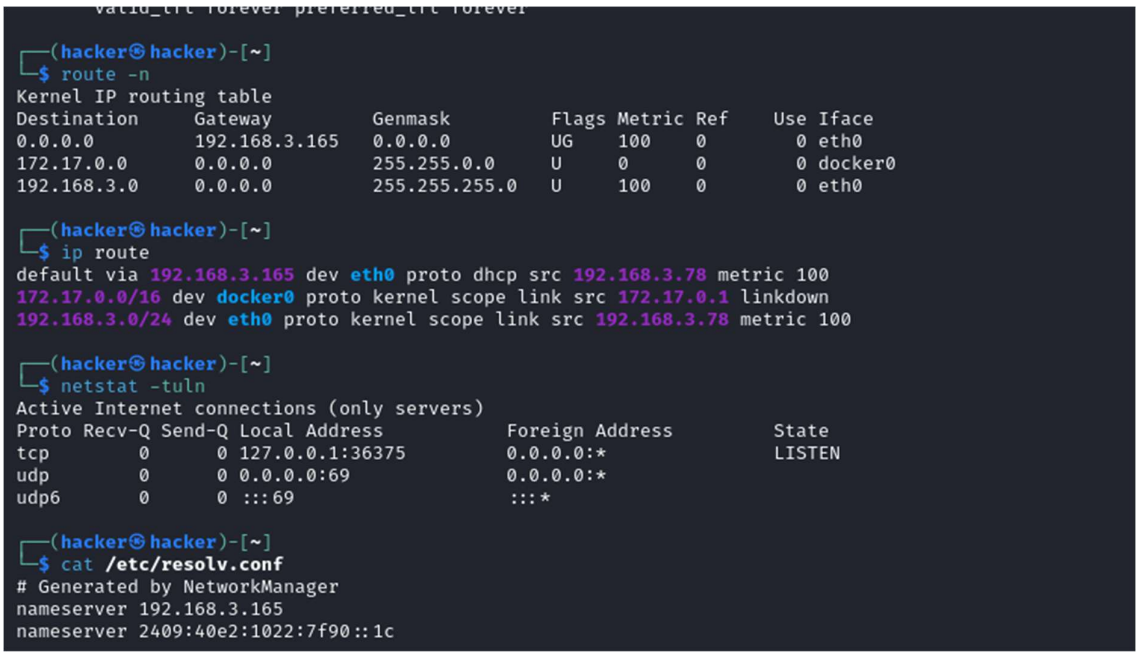
netstat -tuln

or, on newer systems:

ss -tuln

Check DNS Configuration:

cat /etc/resolv.conf



or, on newer systems:

ss -tuln

Get Network Adapter Details:

bash

Co

lshw -C network

or:

nmcli device

View Network Shares (Samba):

smbclient -L localhost

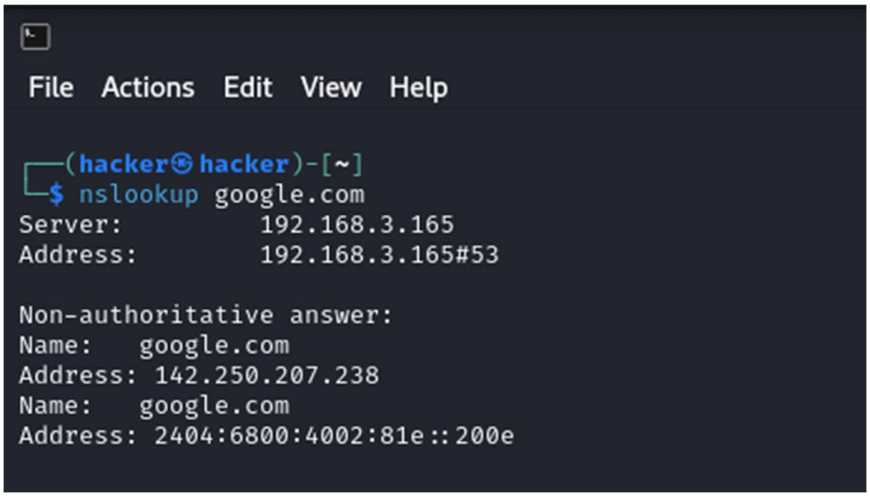
These commands will help you gather detailed information about the network and server configuration on both Windows and Linux systems.

THE TASK IS END

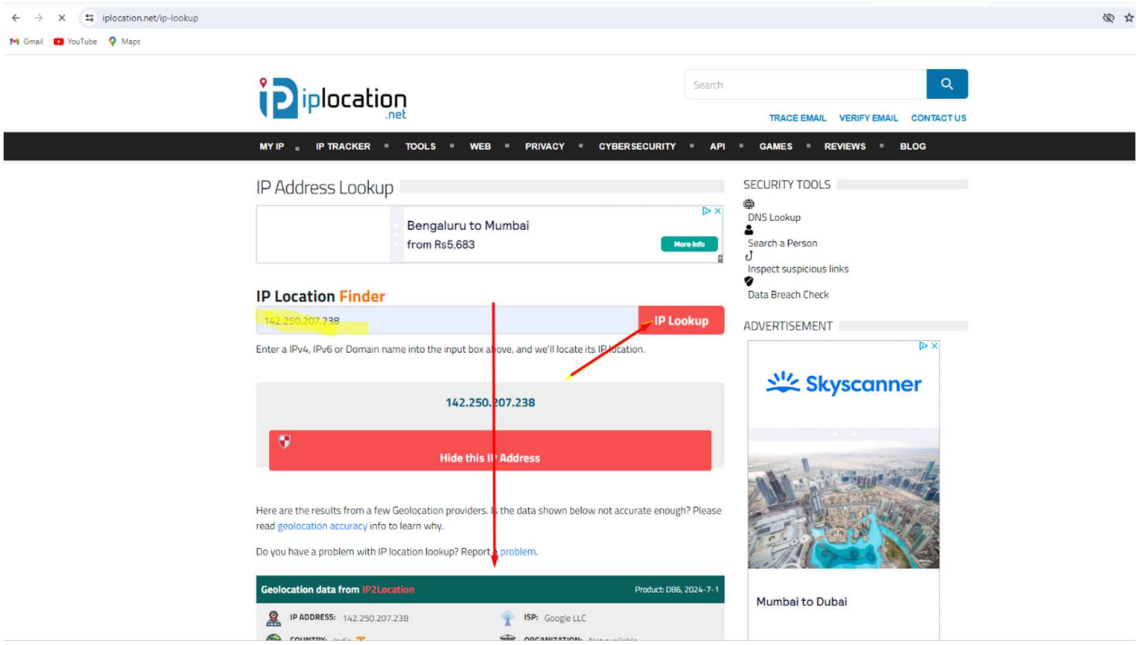
TASK:-6 Reconnaissance of any website/IP with the help of these tools(IP LOOKUP WEBSITE/WHOIS/WHAT IS MY IP ADDRESS)

Step 1: Find the IP address

This step I am used command is nslookup: **and then copy to the ip Address**



Step:-2 I'll go to the iplocation.net website, enter the IP address, and click the "IP Lookup" button

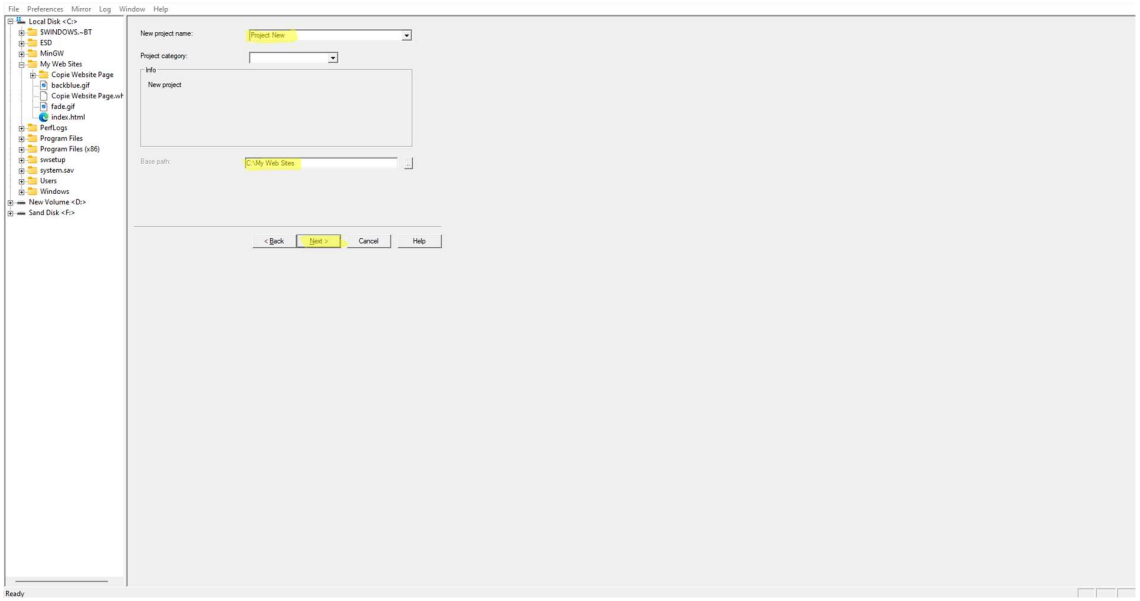


I would go to the iplocation.net website, enter the IP address, click the "IP Lookup" button, scroll down the website, and get to see the data in various formats

This task is end

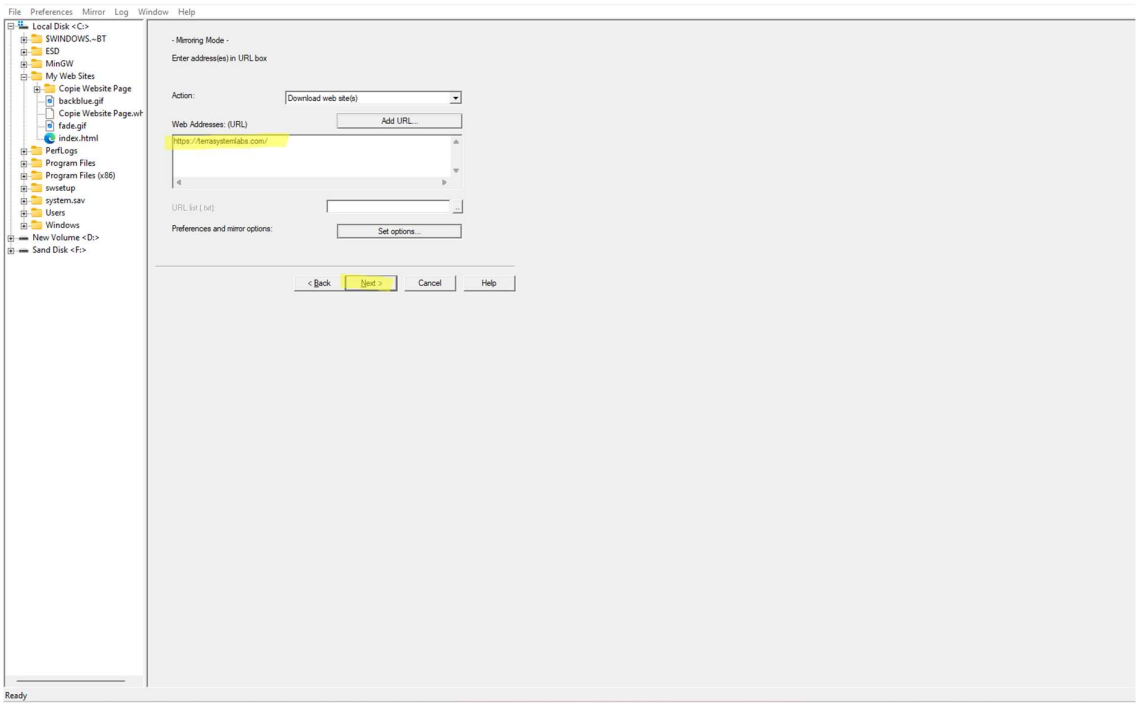
TASK:-7 Copy the website pages with the tools (HT-Track / site sucker / Get left)

Step:- 1. Open the HTTrack application, enter the project name, and then click the Next button.

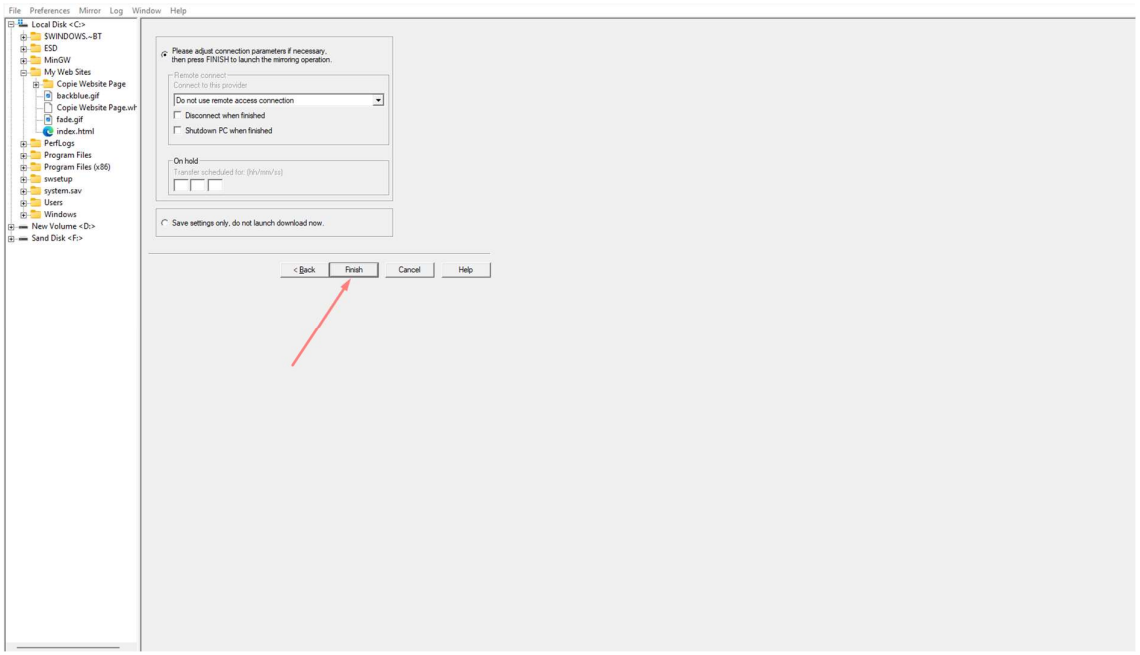


Step:- 2 Then, go to the target website and copy the link. Then go into the httrack application

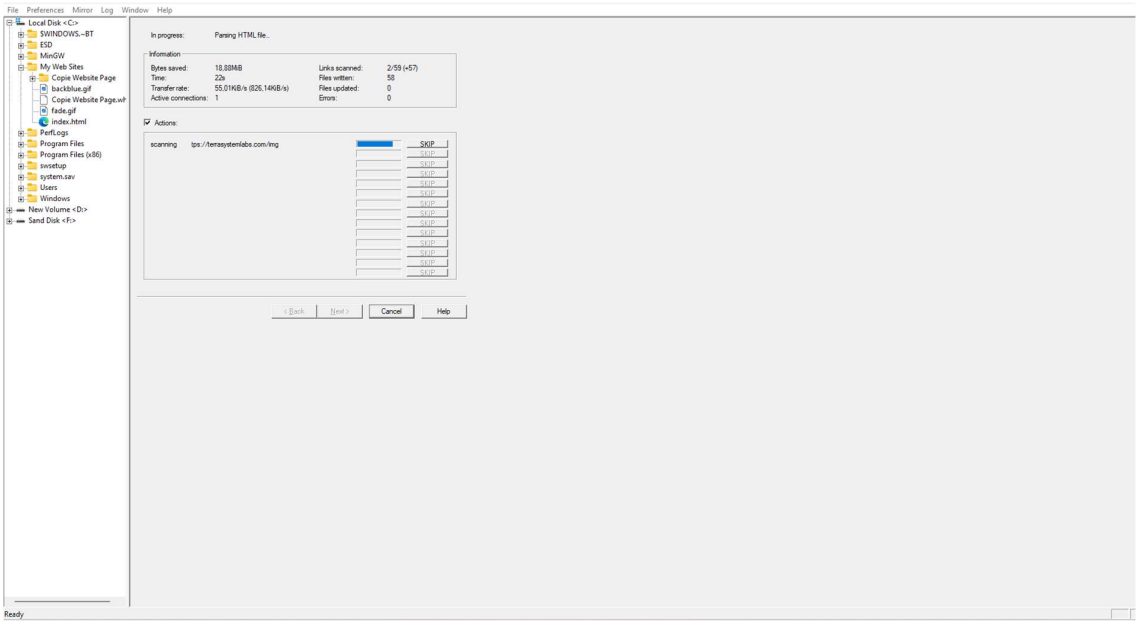
Step:-3 Next, paste the website link into the URL section and click the Next button.



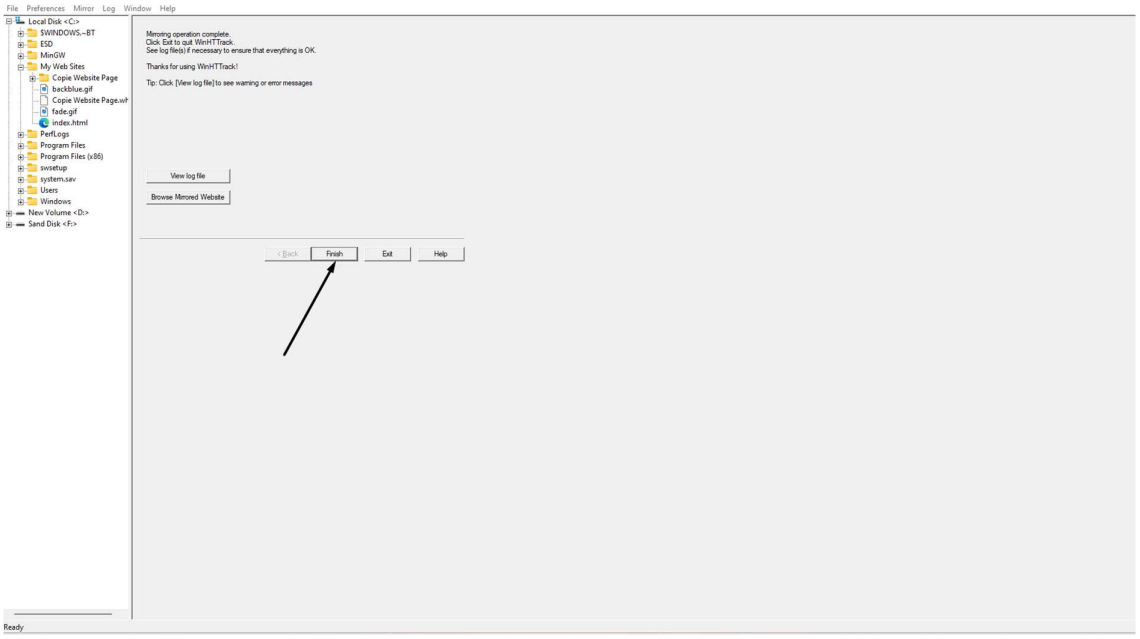
Step:- 4 Then Click to next button



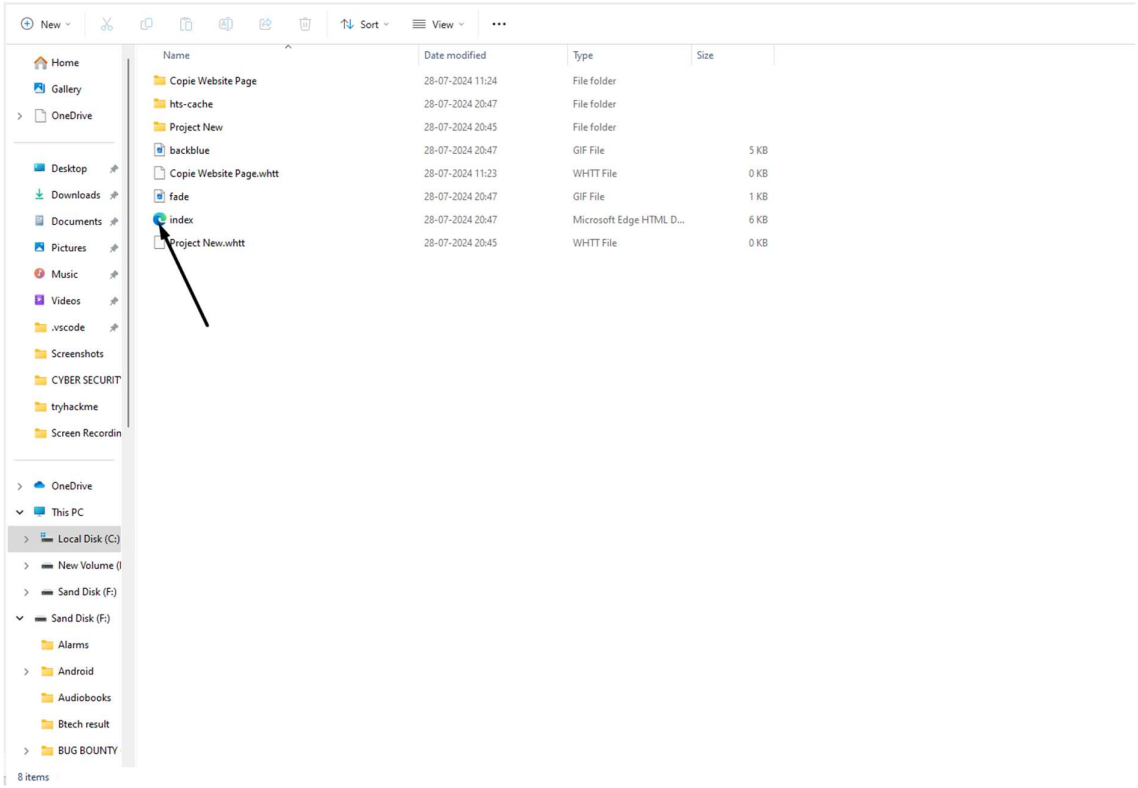
Step:- 5 The process will start. Please wait until it finishes



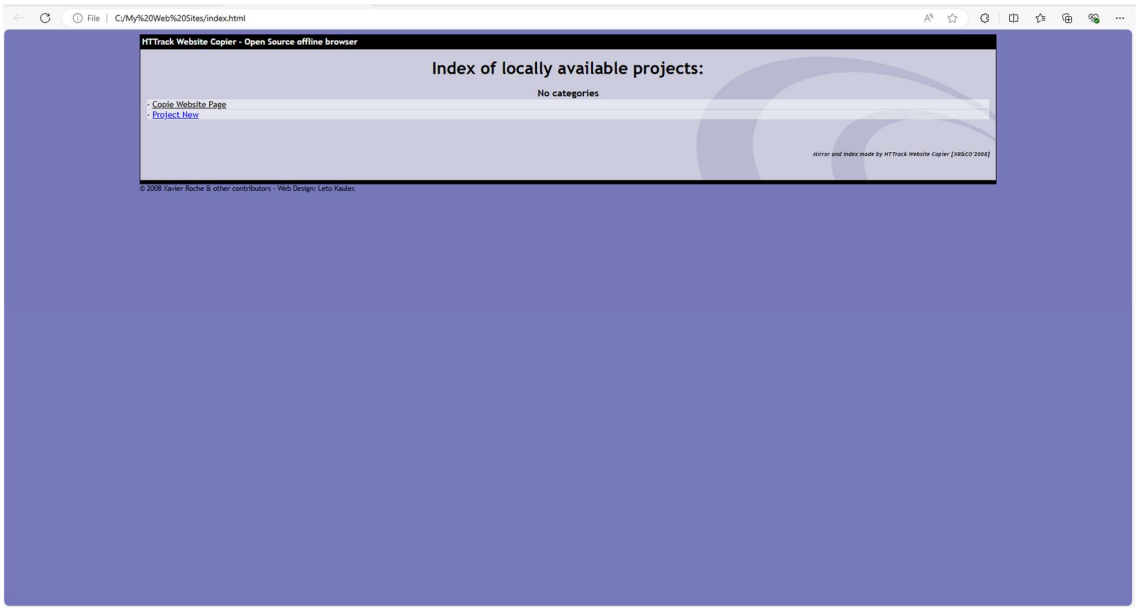
Step:- 6 Then, click the Finish button and go to the file manager.



Step:-7 then click to the Index



Step:- 8 Then click the Copie Website Page



Step:-9 Then finally cope the website page

Task is end

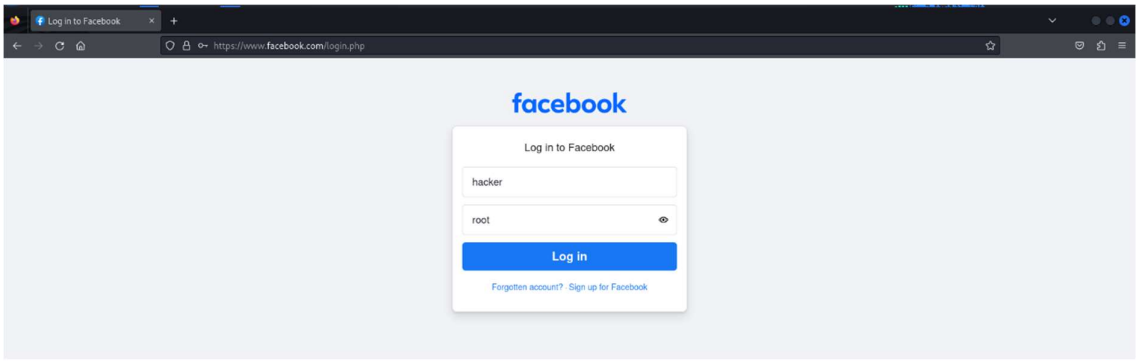
TASK:-8 Perform Phishing of any websites:

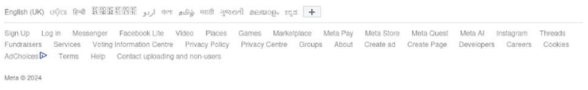
Phishing is a malicious activity that involves attempting to acquire sensitive information such as usernames, passwords, and credit card details by pretending to be a trustworthy entity in electronic communications. It is illegal and unethical to engage in or support phishing activities.

I am perform kali linux I am already setup the Zphiser

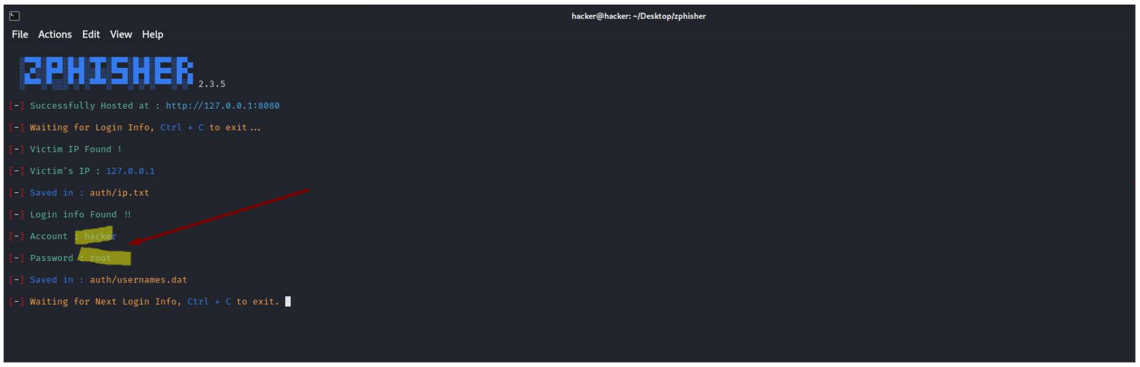
"Then, copy the link and send it to any user via email or messages." Then the user you are sending it to will enter his username and password and then he can view his details.

"Then the facebook login page will look like this." Then every person fill the data and then click to login page





"I checked the terminal and found the username and password." This is called as phishing attack



"All tasks are completed."

THANKYOU