the link, it redirects the user to a fake webpage that looks like an official website. For example, the recipient may be redirected to a fake bank webpage that then asks for sensitive information. Similarly, clicking on the link may download a malicious script onto the recipient's system to fetch information.

Shoulder Surfing

In Shoulder Surfing, information is collected by standing behind a target when he is dealing with sensitive information. By using this technique, passwords, account numbers, or other secret information can be gathered, depending upon the carelessness of the target.

Dumpster Diving

Dumpster Diving is the process of looking for treasure in trash. This technique is old but still effective. It includes accessing the target's trash such as printer trash, user desk, company trash to find phone bills, contact information, financial information, source codes, and other helpful material.

Footprinting Tool
Maltego

Maltego is a data mining tool that is powered by Paterva. This interactive tool gathers data and shows the results in graphs for analysis. The major purpose of this data mining tool is an online investigation of relationships among different pieces of information obtained from various sources over the internet. By using Transform, Maltego automates the process of gathering information from different data sources. A nodebased graph represents this information. There are three versions of Maltego client software, and they are mentioned below:

- Maltego CE
- Maltego Classic
- Maltego XL

Lab 02- 1: Maltego Tool Overview Procedure:

You can download Maltego from the Paterva website (i.e., https://www.paterva.com). Registration is required to download the software. After downloading, installing it requires a license key to run the application with complete features.

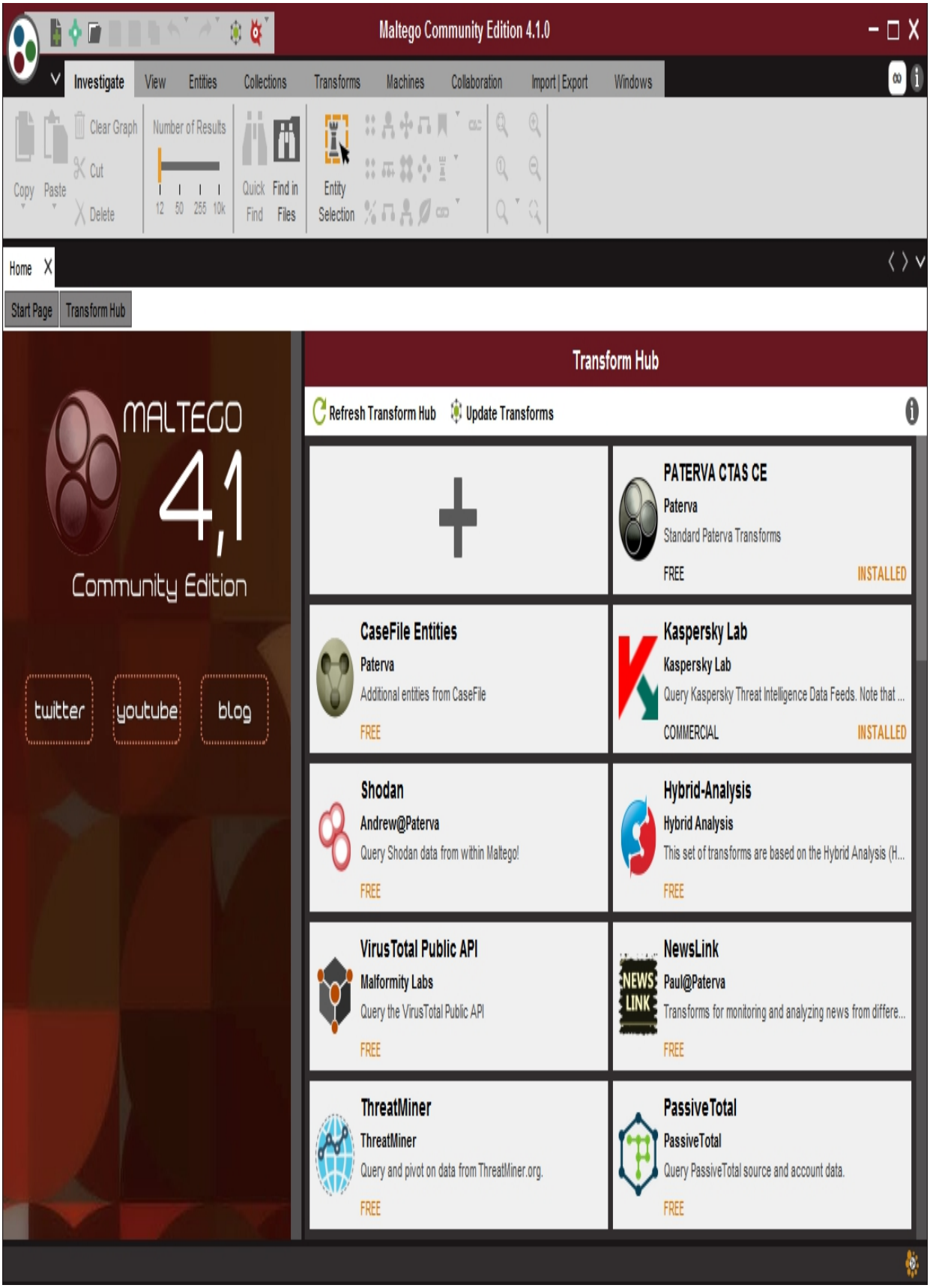


Figure 2.44: Maltego Home Page

Figure 2-44: Maltego Home Page

Above is the Home page of Maltego Community Edition (CE). On top of the first column, click on the "create new graph" icon  .

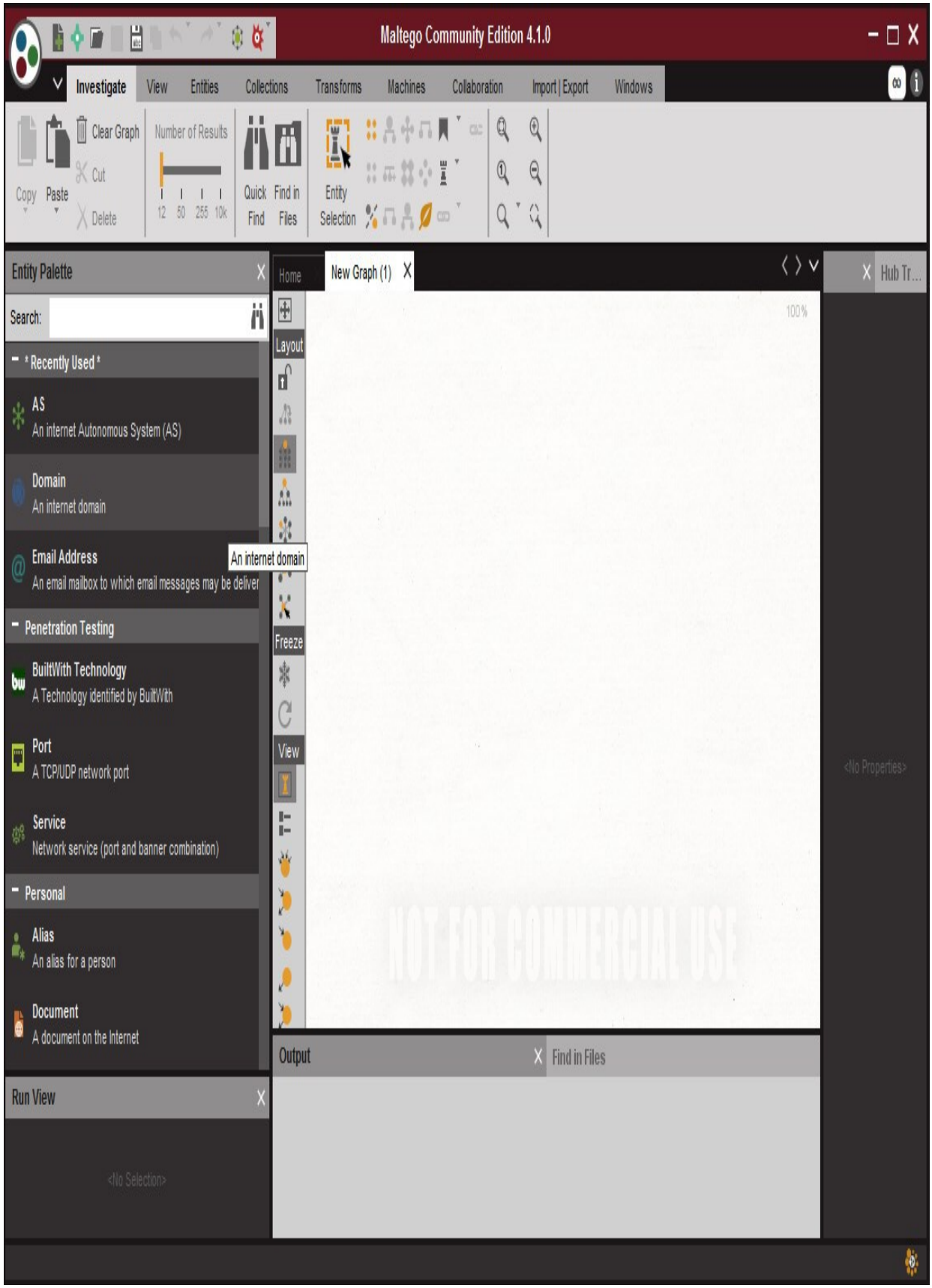

Maltego Community Edition 4.1.0
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Clear Graph
Cut
Delete
Copy
Paste
Number of Results
12
50
255
10k
Quick Find
Find in Files
Entity Selection
Entity Palette
Search:
* Recently Used *
AS
An internet Autonomous System (AS)
Domain
An internet domain
Email Address
An email mailbox to which email messages may be deliver
Penetration Testing
BuiltWith Technology
A Technology identified by BuiltWith
Port
A TCP/UDP network port
Service
Network service (port and banner combination)
Personal
Alias
An alias for a person
Document
A document on the Internet
Run View
<No Selection>
Home
New Graph (1)
Layout
Freeze
View
An internet domain
100%
NOT FOR COMMERCIAL USE
Output
Find in Files
Hub Tr...
<No Properties>

Figure 2-45: Maltego

You can select "*Entity Palette*" depending on your type of query. In our case, for example, "*Domain*" is selected.

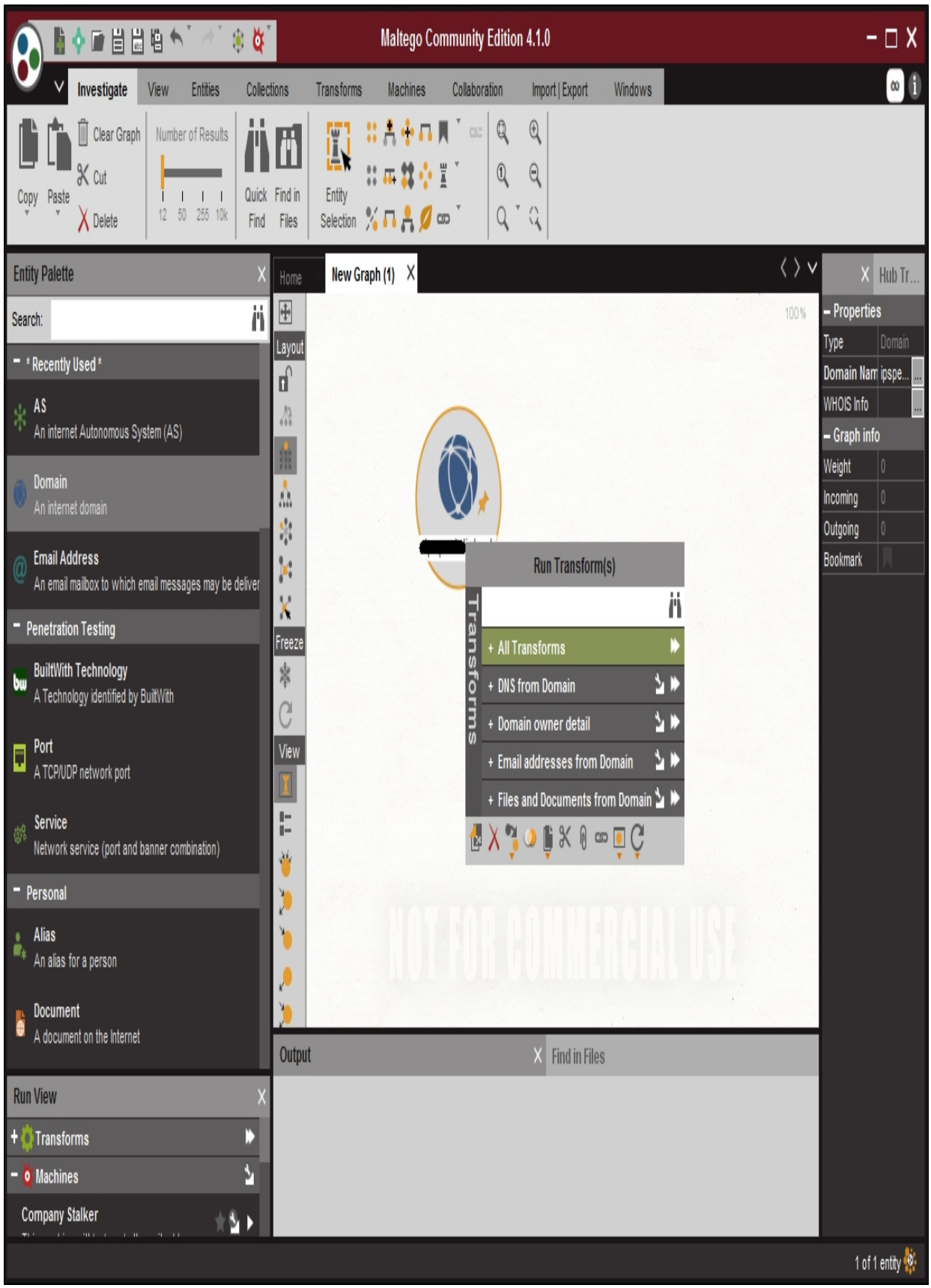

Maltego Community Edition 4.1.0
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Clear Graph
Cut
Delete
Copy
Paste
Number of Results
12
50
255
10k
Quick Find
Find in Files
Entity Selection
Entity Palette
Search:
* Recently Used *
AS
An internet Autonomous System (AS)
Domain
An internet domain
Email Address
An email mailbox to which email messages may be deliver
Penetration Testing
BuiltWith Technology
A Technology identified by BuiltWith
Port
A TCP/UDP network port
Service
Network service (port and banner combination)
Personal
Alias
An alias for a person
Document
A document on the Internet
Run View
Transforms
Machines
Company Stalker
Home
New Graph (1)
Layout
Freeze
View
100%
Run Transform(s)
Transforms
+ All Transforms
+ DNS from Domain
+ Domain owner detail
+ Email addresses from Domain
+ Files and Documents from Domain
NOT FOR COMMERCIAL USE
Output
Find in Files
Hub Tr...
Properties
Type
Domain
Domain Nam
ipspe...
WHOIS Info
Graph info
Weight
0
Incoming
0
Outgoing
0
Bookmark
1 of 1 entity

Figure 2-46: Maltego

Edit the domain and right click on the domain icon and select “ *Run Transform* ” . Select the option and observe the generated results. Available options will be: • All Transforms

- DNS from Domain
- Domain Owner Detail
- Email Addresses from Domain
- Files and Documents from Domain

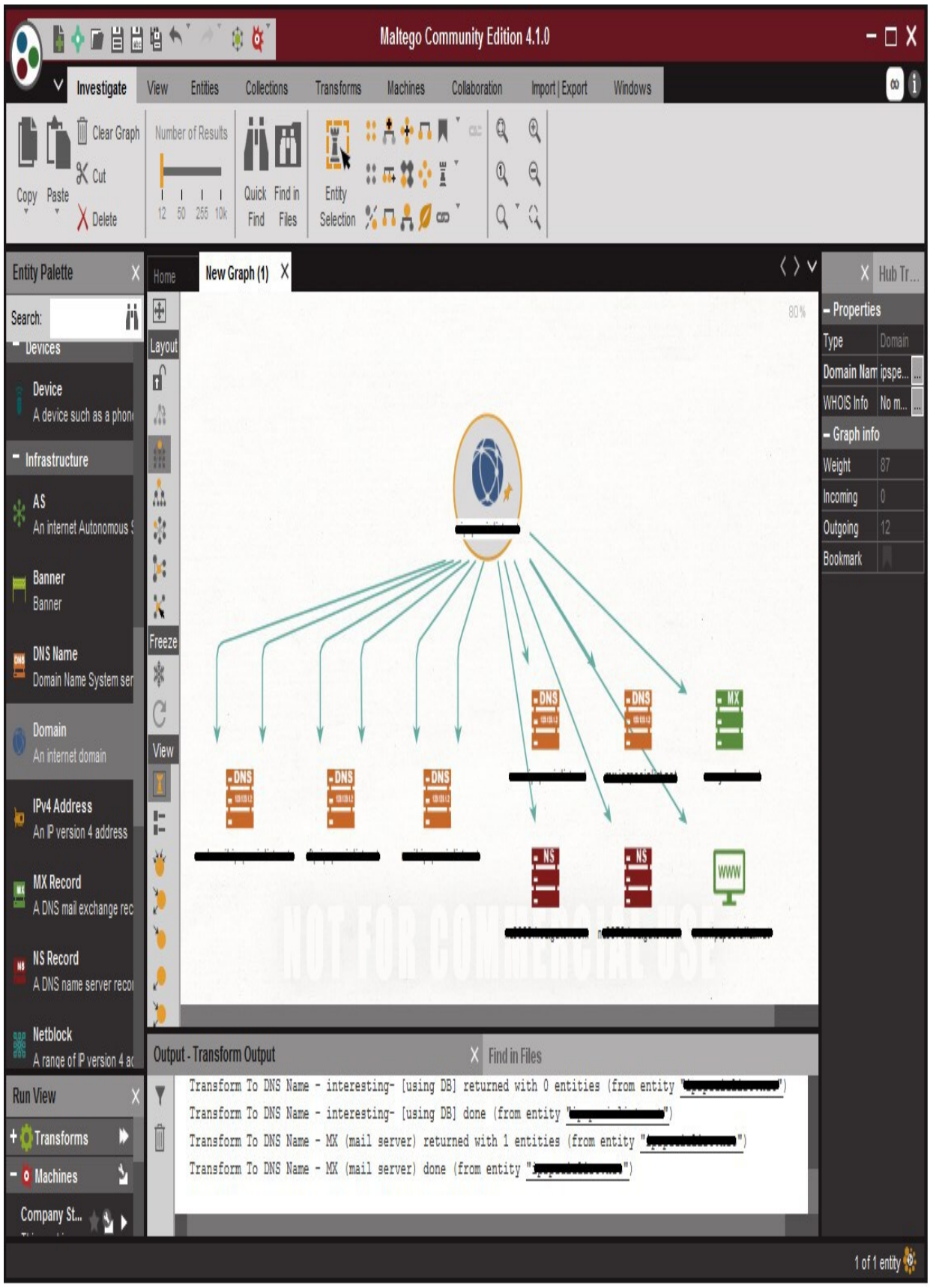


Figure 2 - 43: Maltego

Figure 2-47: Maltego

Recon-ng Recon-ng is a full feature Web Reconnaissance framework used for gathering

information as well as network detection. This tool is written in python and has independent modules, database interaction, and other features. You can download the software from www.bitbucket.org. This Open Source Web Reconnaissance tool requires the Kali Linux Operating system.

Lab 02-2: Recon-ng Overview Procedure:

Open Kali Linux and run Recon-ng.

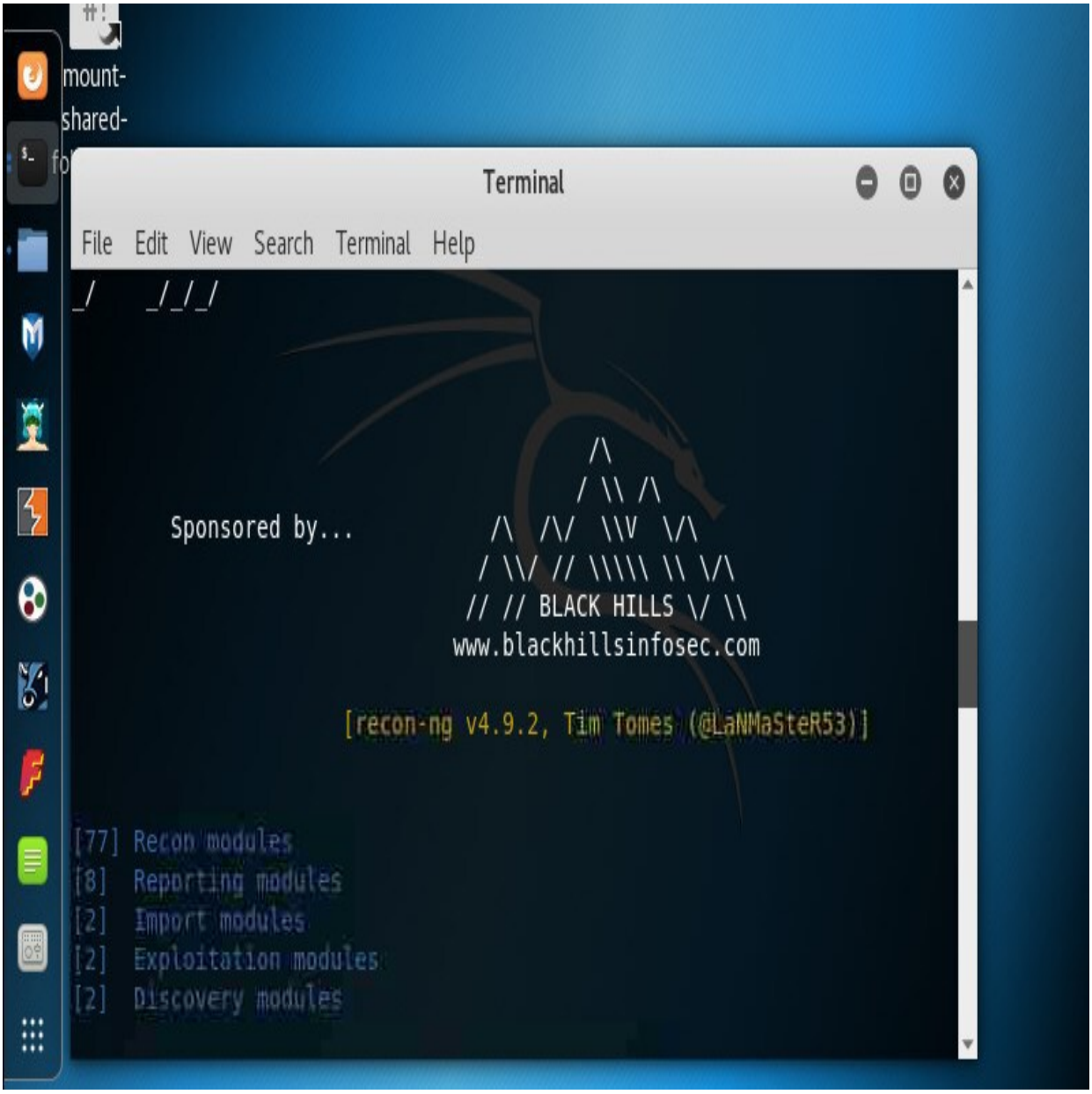


Figure 2-48: Recon-ng

Run the application Recon-ng or open the terminal of Kali Linux and type recon-ng and hit "Enter".

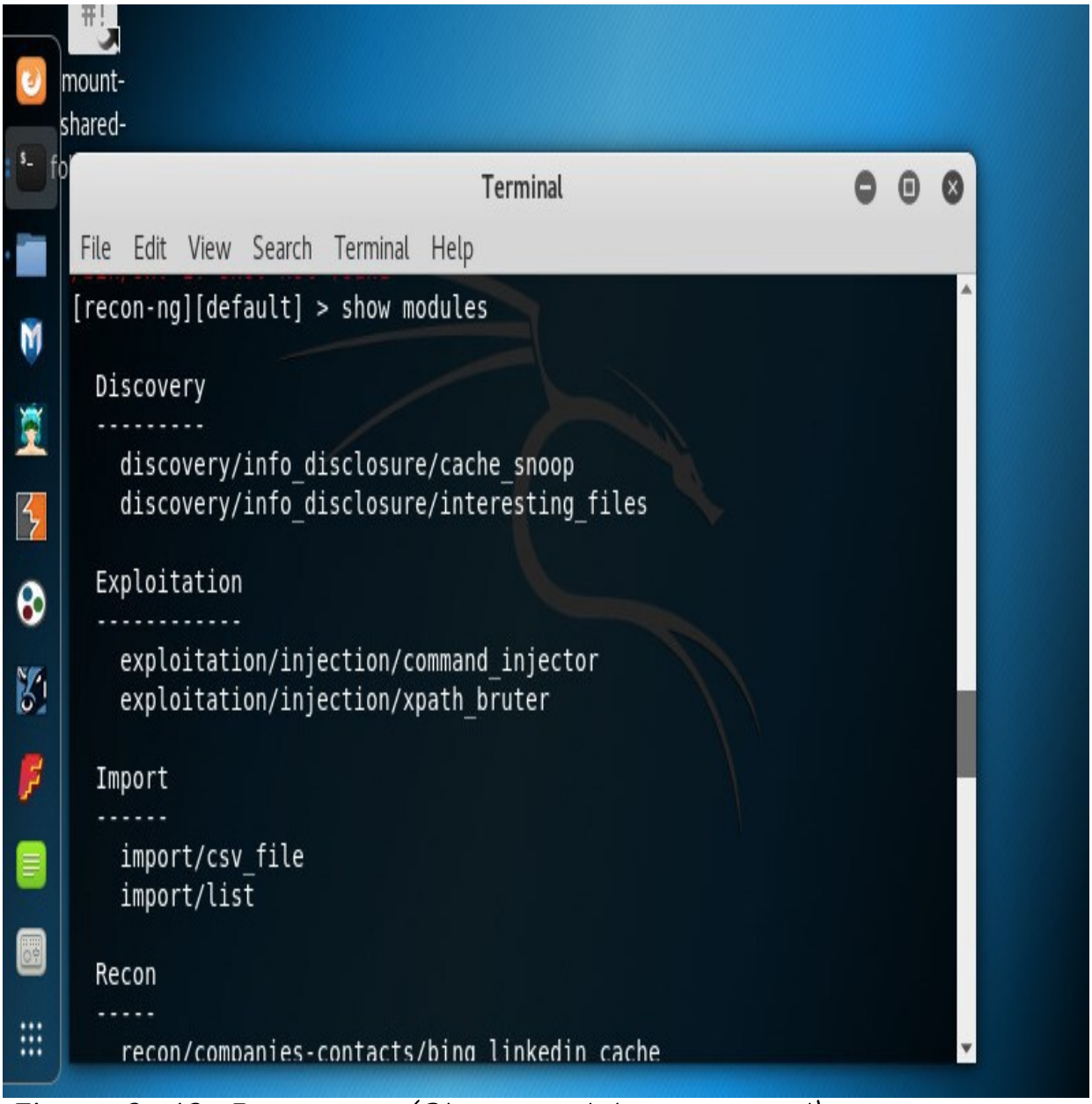


Figure 2-49: Recon-ng (Show module command)

Enter the command "***show modules***" to show all the available independent modules.

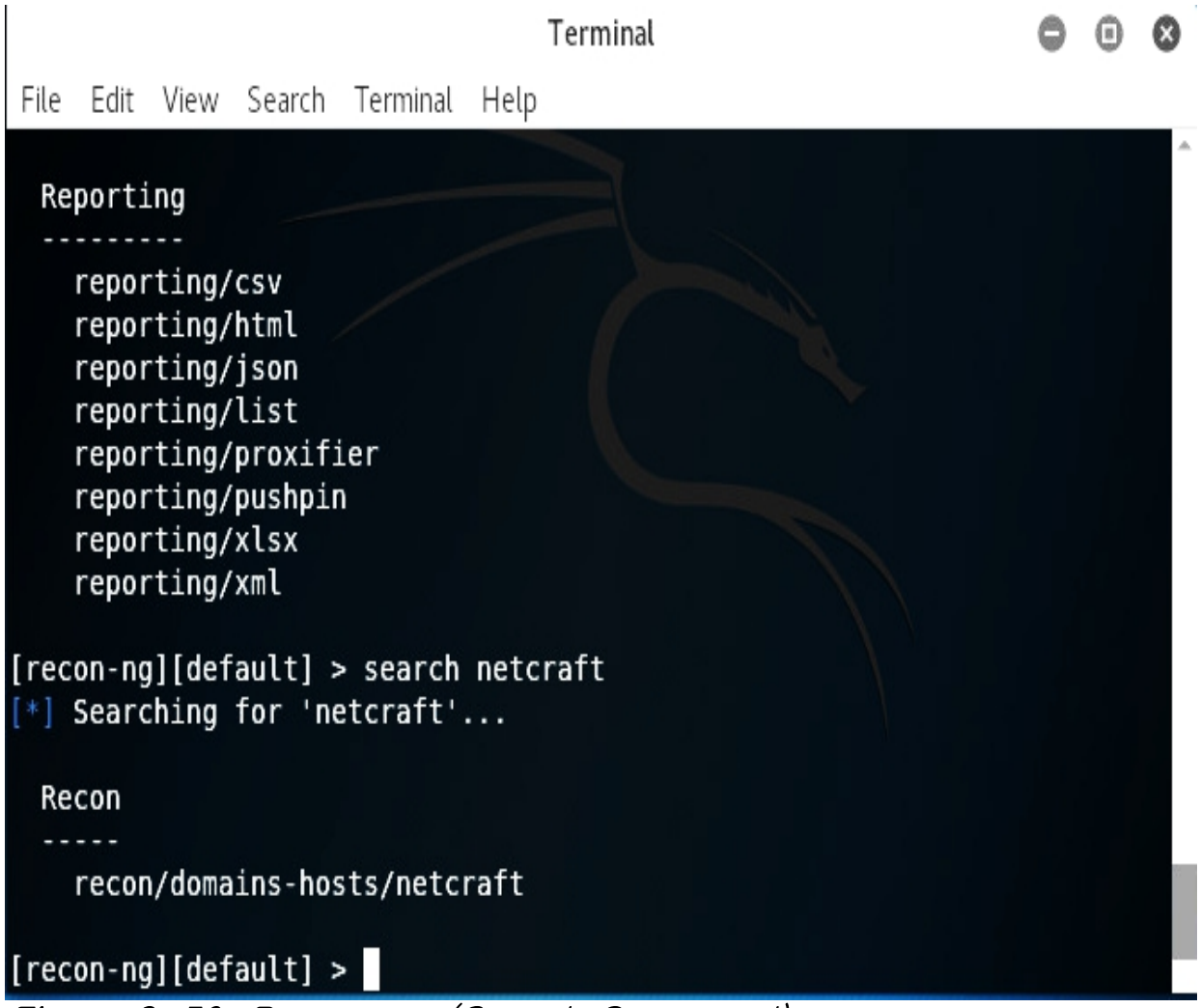


Figure 2-50: Recon-ng (Search Command)

You can search for any entity within a module. For example, in the above figure, the command "*search netcraft*" has been used.

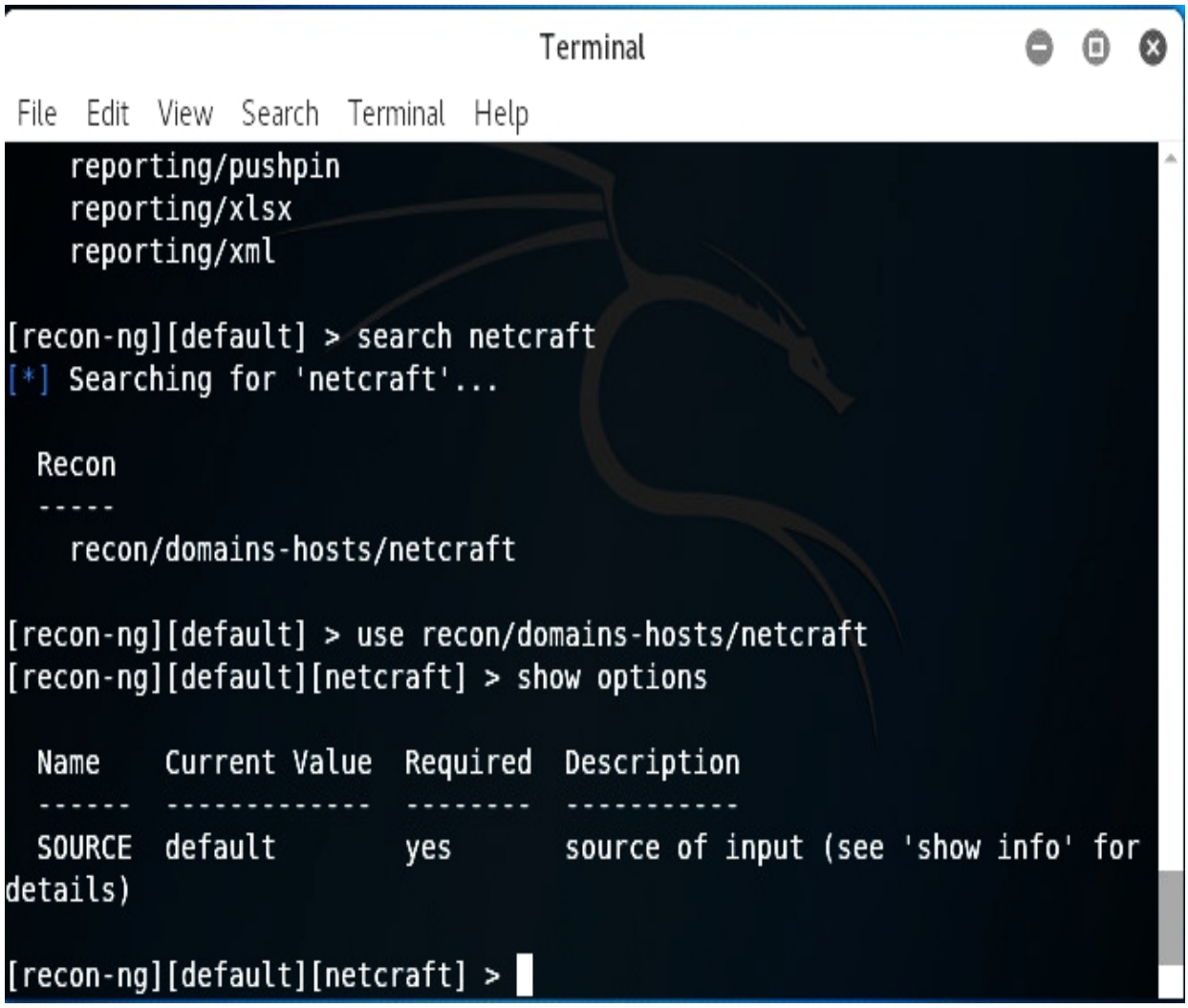


Figure 2-51: Using Netcraft through Recon-ng

To use the Netcraft module, use the command syntax "*use recon/domainhosts/netcraft*" and hit "Enter".

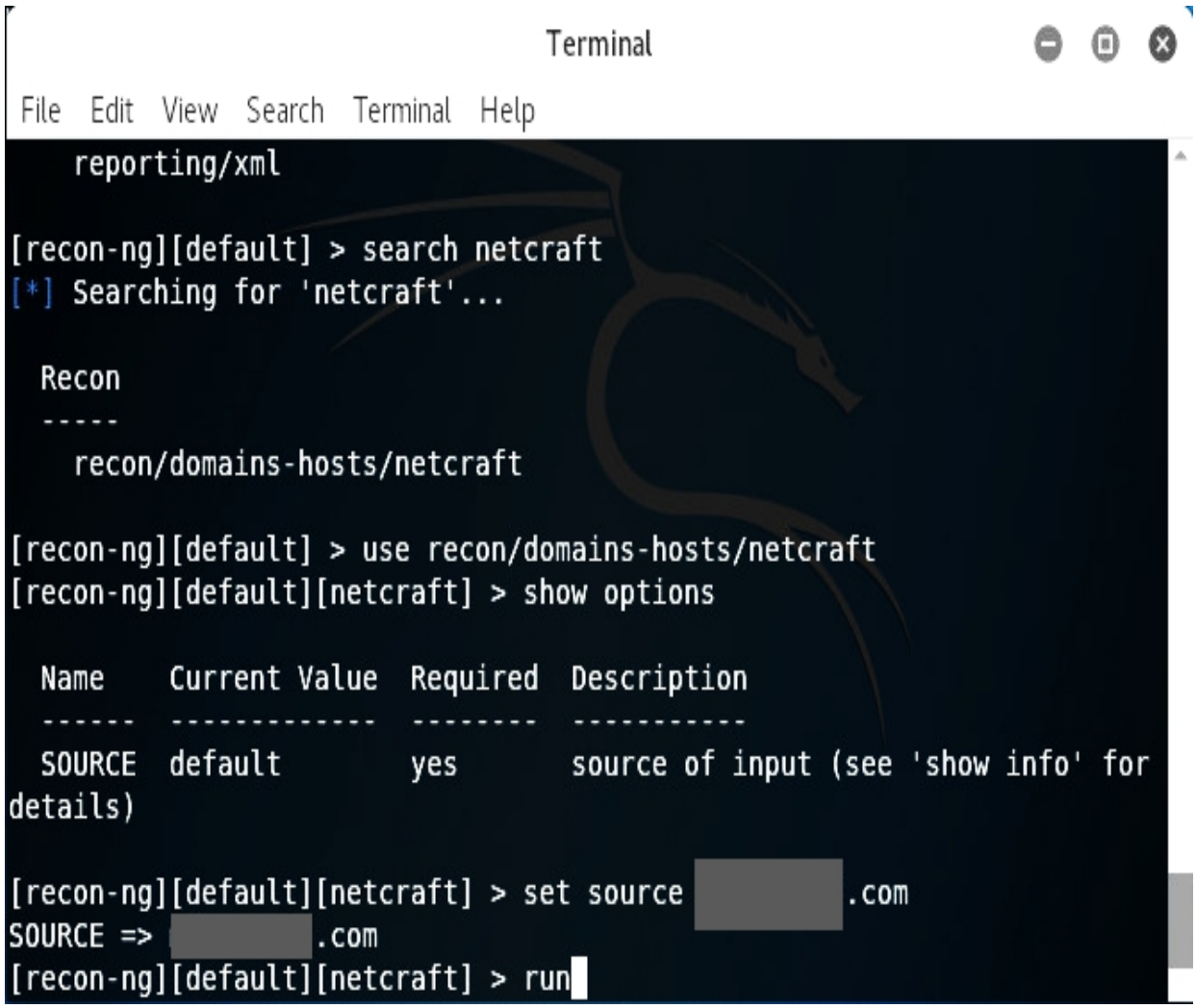


Figure 2-52: Searching for Target Domain

Set the source by the command "***set source*** *[domain]*". Press "Enter" to continue. Type "***Run***" to execute and press "Enter".

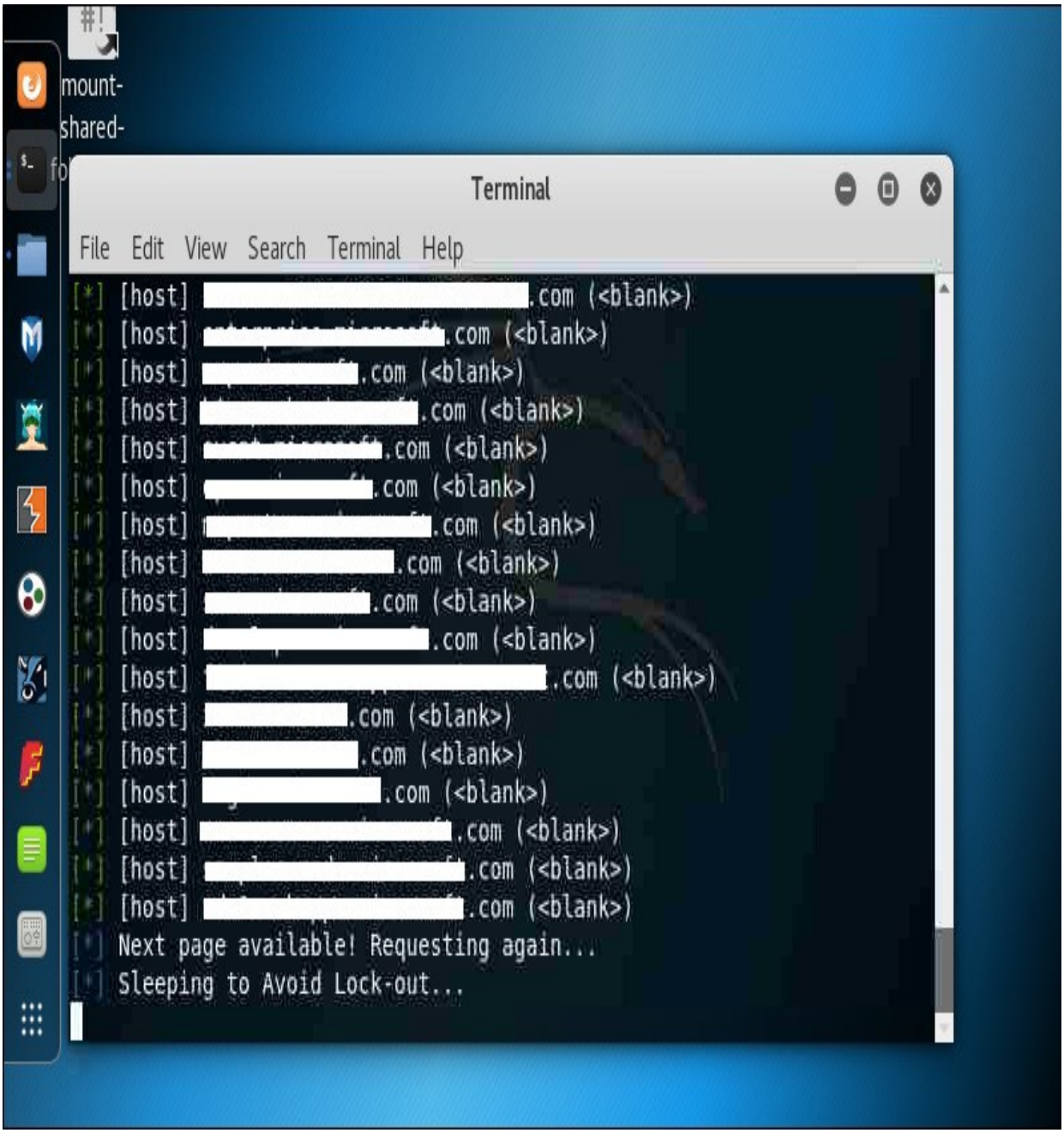


Figure 2-53: Search Result of Target Domain

Recon-ng gathers information about the target domain.

Additional Footprinting Tools

FOCA stands for Fingerprinting Organizations with Collected Archives. The FOCA tool finds metadata and other hidden information within a document on a website. Scanned searches can be downloaded and analyzed. FOCA is a powerful tool that can support various types of documents including Open Office, Microsoft Office, Adobe InDesign,

PDF, SVG, etc. Search uses three search engines: Google, Bing, and DuckDuckGo.

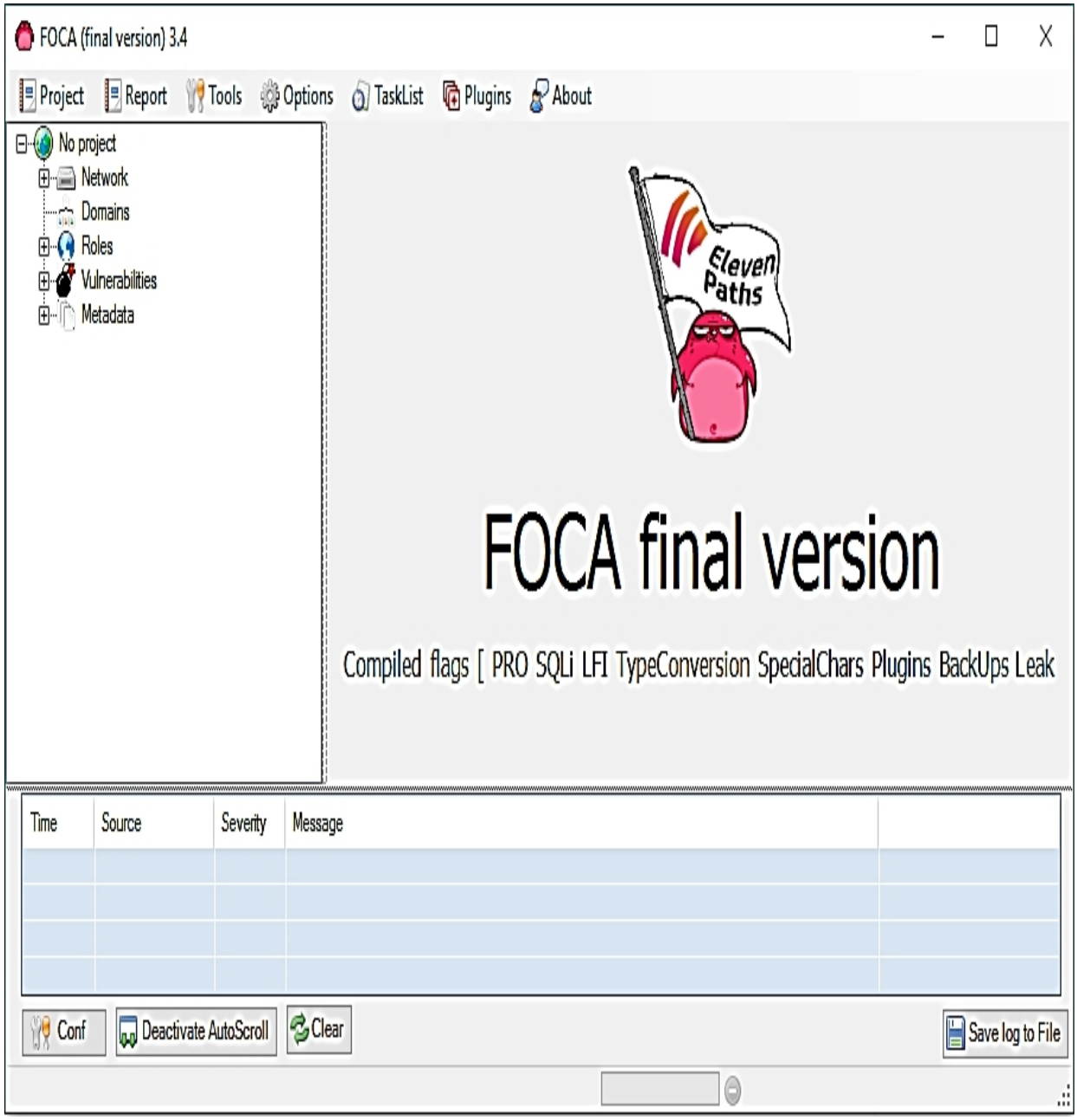


Figure 2-54: FOCA Dashboard

Lab 02-3: FOCA Tool Overview

Procedure:

Download the software *FOCA* from https://www.elevenpaths.com. Now, go to "*Project*" > "*New Project*".

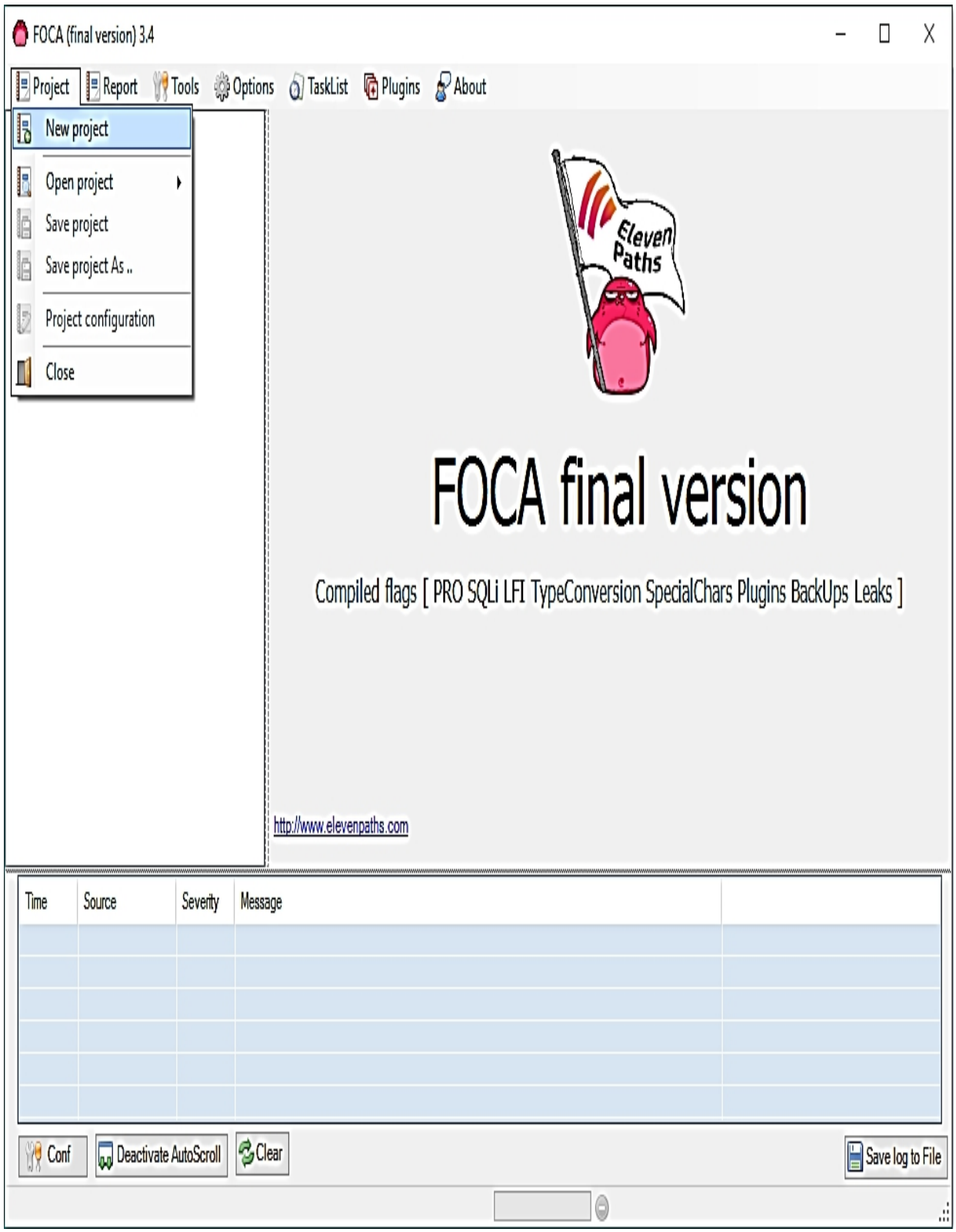


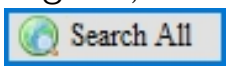
Figure 2–55: Creating a New Project Using FOCA

Now, enter the Project Name, Domain Website, and Alternate Website (if required). Select the directory to save the results and enter the

project date. Click “Create”


to proceed.

Figure 2-56: Creating a New Project Using FOCA

Select the Search engines, Extensions, and other parameters as per your requirements. 

Click on the “Search All” button.

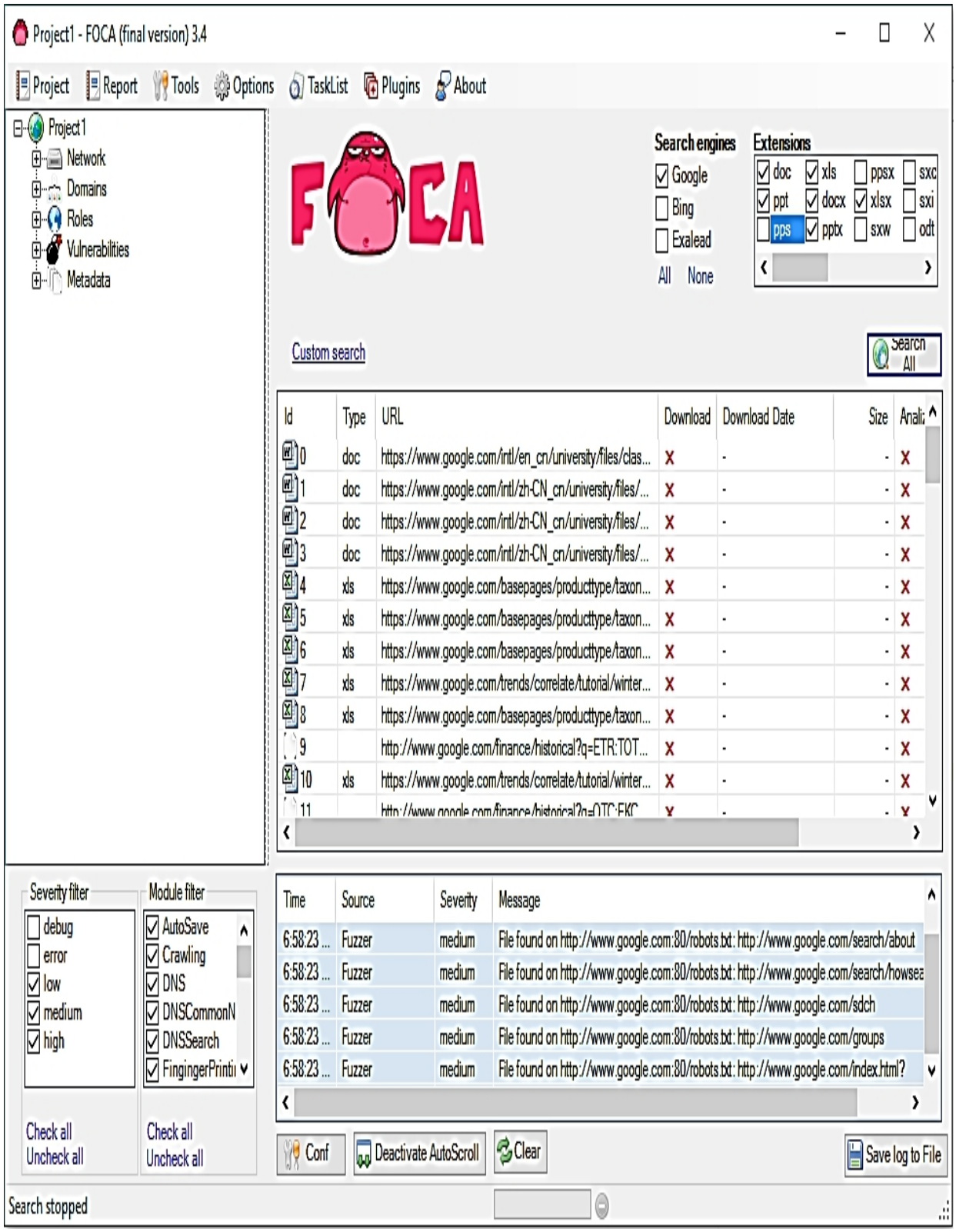


Figure 2–57: Search Using FOCA

Once the search completes, the search box shows multiple files. You can select a file, download it, extract metadata, and gather other information like username, file creation date, and modification.

Figure 2-58: Analyzing Options with FOCA

Some other footprinting tools are:

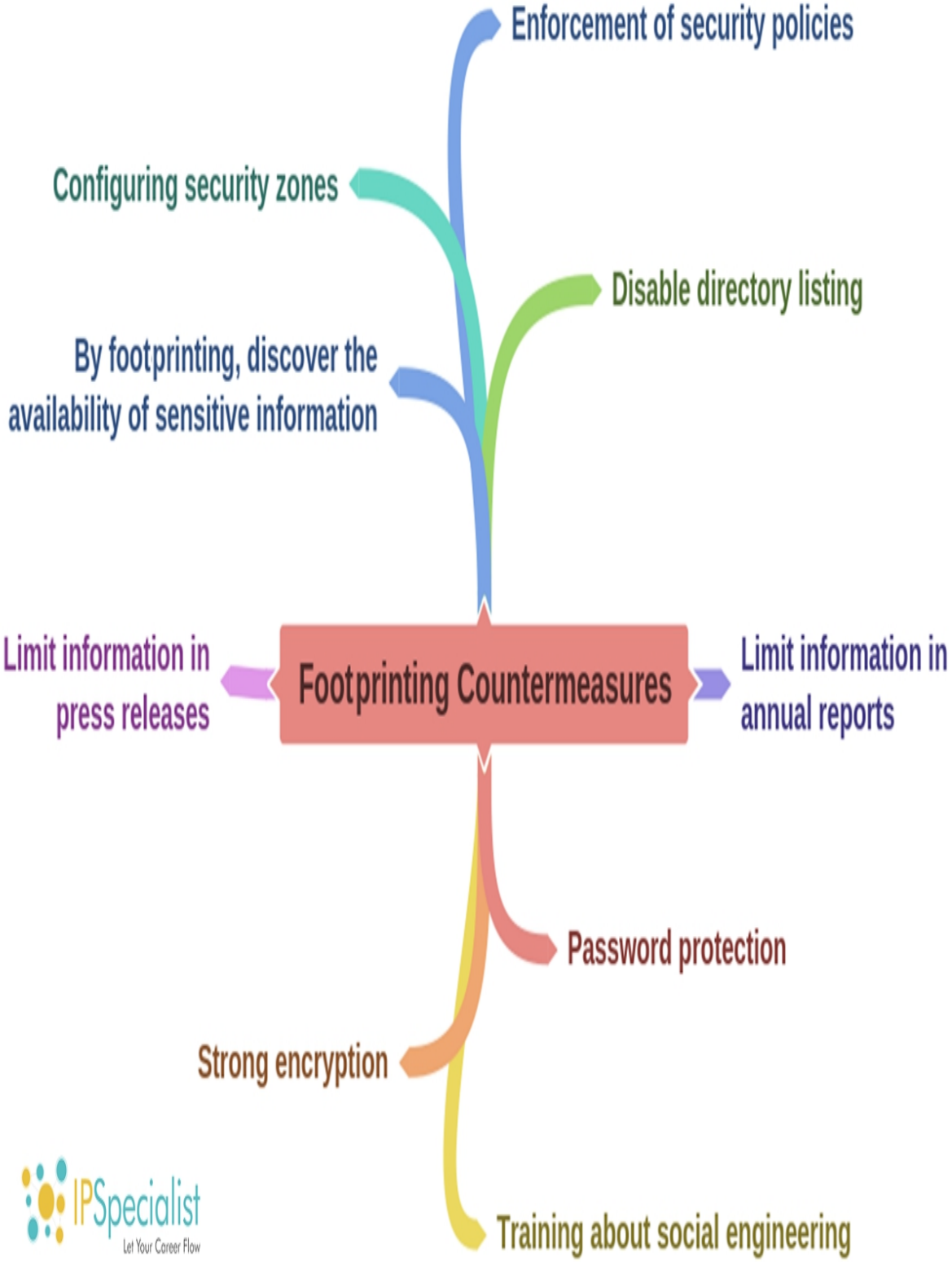
Tools Websites Prefix WhoIs http://pwhois.org Netmask http://www.phenoelit.org DNS-Digger http://www.dnsdigger.com Email Tracking Tool http://www.filley.com Ping-Probe http://www.ping-probe.com Google Hacks http://code.google.com *Table 2-11: Additional Footprinting Tools*

Countermeasures of Footprinting

Footprinting countermeasures include the following:

- An organization's employees' access to social networking sites from the corporate network must be restricted
- Devices and servers should be configured to avoid data leakage
- Education, training, and awareness regarding footprinting, its impact, methodologies, and countermeasures should be provided to employees
- Revealing sensitive information in annual reports, press releases, etc. should be avoided
- Prevent search engines from caching web pages

Mind Map


Enforcement of security policies
Configuring security zones
Disable directory listing
By footprinting, discover the availability of sensitive information
Limit information in press releases
Footprinting Countermeasures
Limit information in annual reports
Password protection
Strong encryption
Training about social engineering
IPSpecialist
Let Your Career Flow

Lab 2-4: Gathering Information Using Windows Command Line Utilities

Case Study: Consider a network where you have access to a Windows PC connected to the internet. Using Windows-based tools, let's gather some information about the target. You can assume any target domain or IP address, in our case we are using **example.com** as a target.

Topology Diagram:

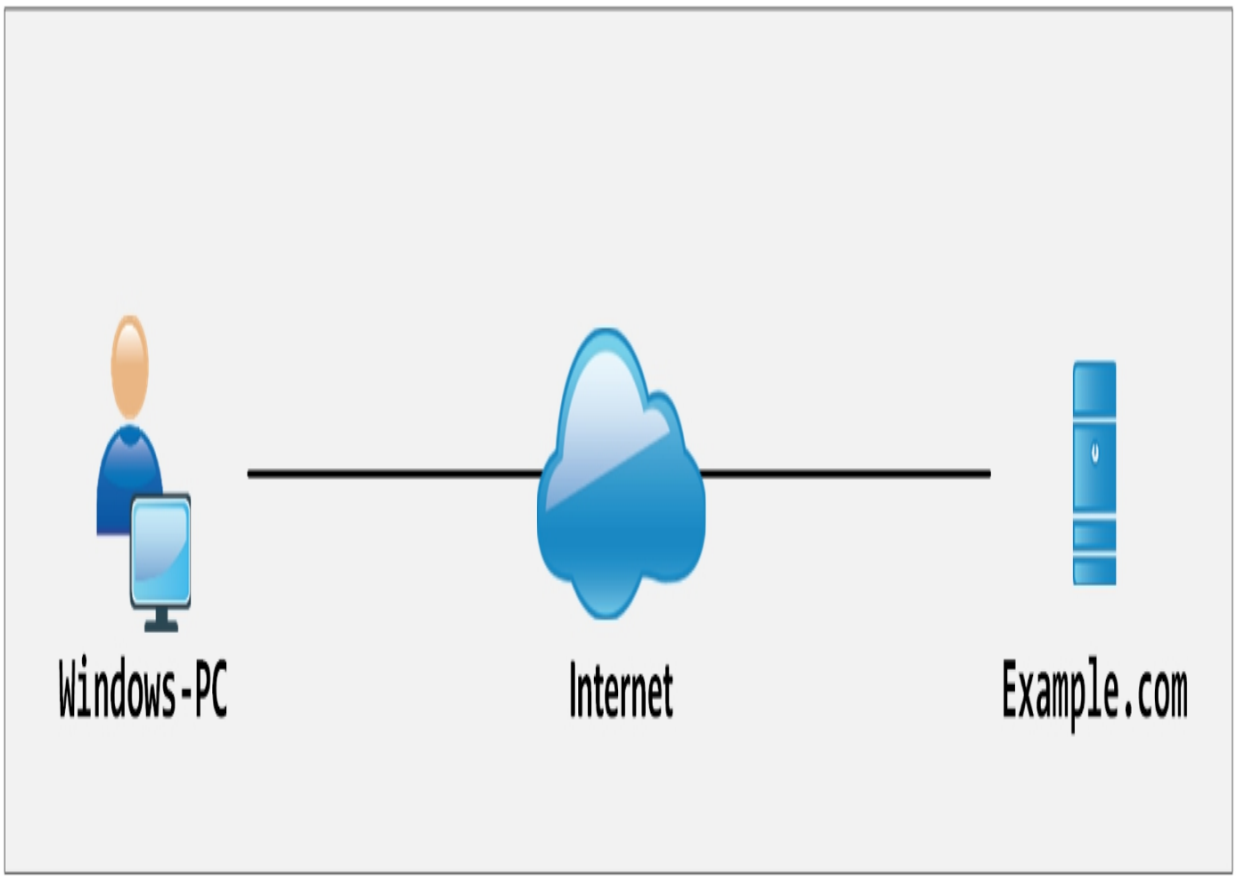


Figure 2-59: Topology Diagram

Procedure:

Open "Windows Command Line (cmd)" from the Windows PC.

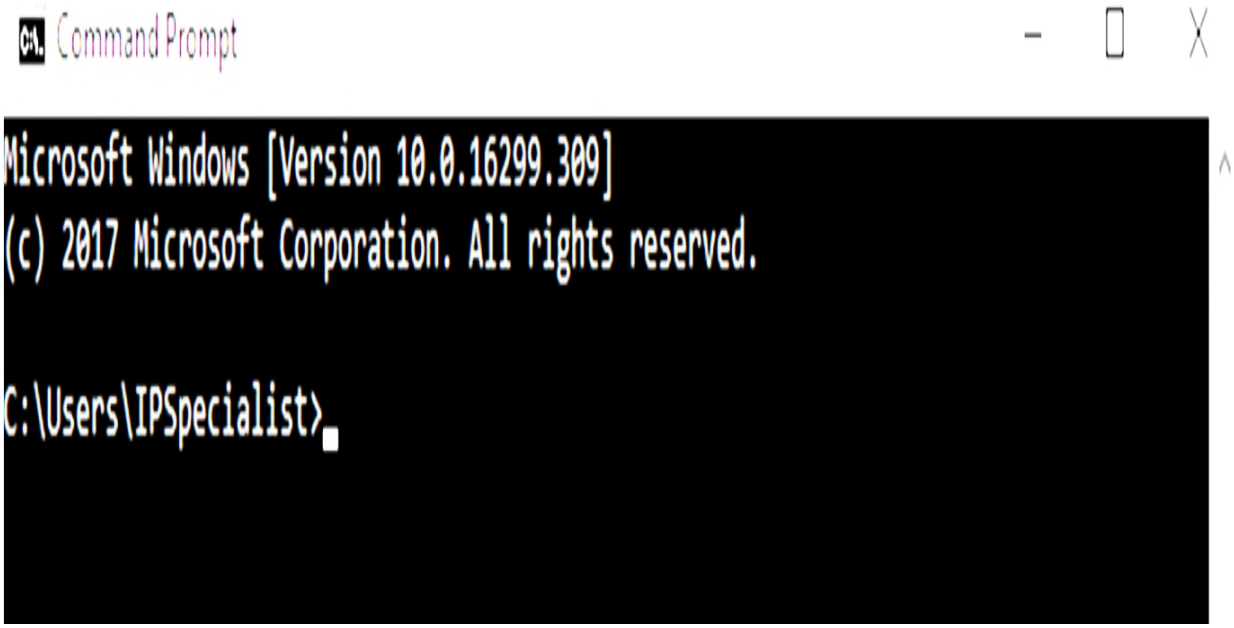


Figure 2-60: Windows Command Prompt

Enter the command "*ping example.com*" to ping.

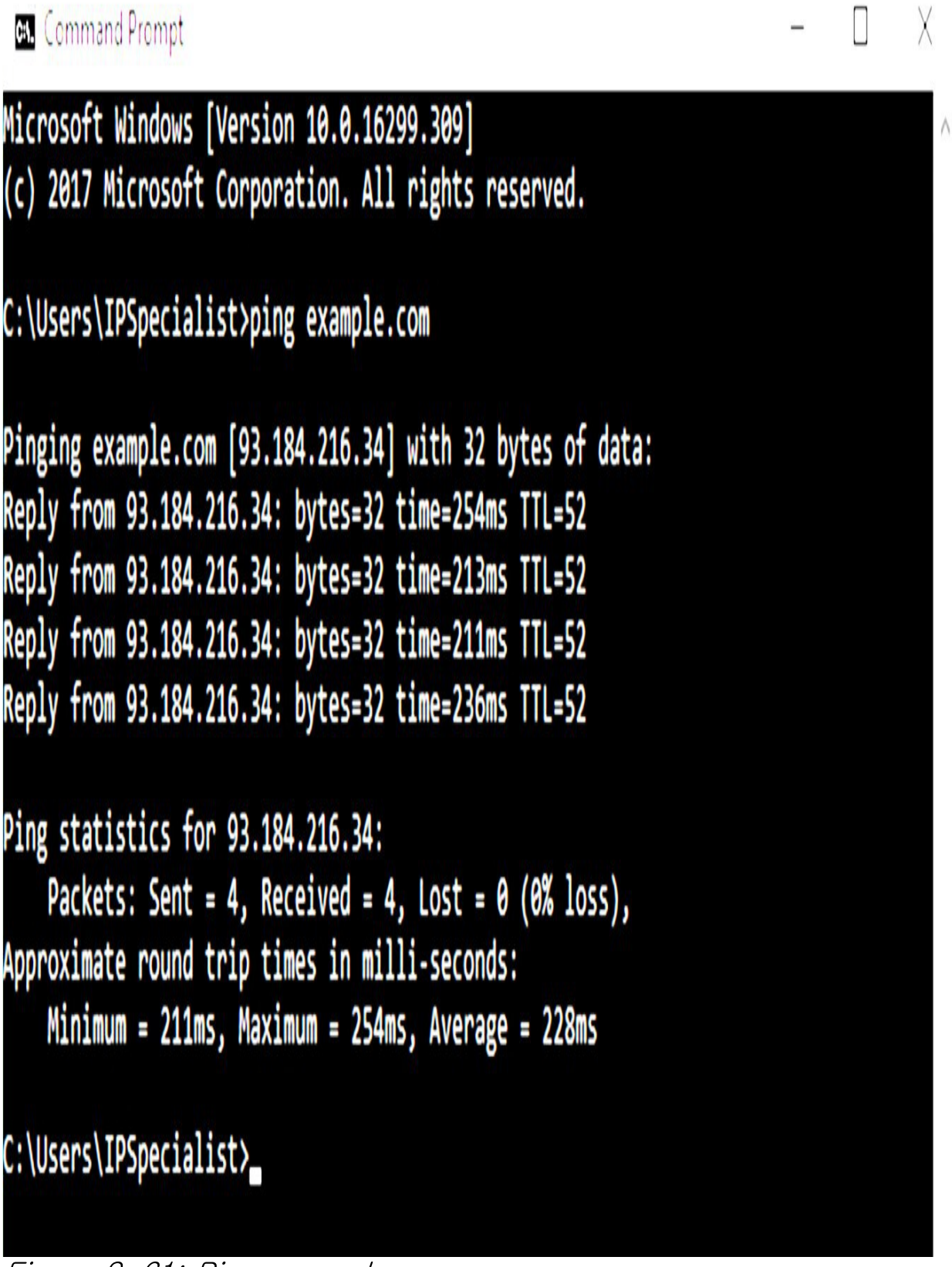


Figure 2-61: Ping example.com

From the output, you can observe and extract the following information:
1. example.com is live
2. The IP address of example.com
3. The Round Trip Time
4. The TTL value
5. The Packet loss statistics

Now, enter the command "*ping example.com -f -l 1500*" to check the value of fragmentation.

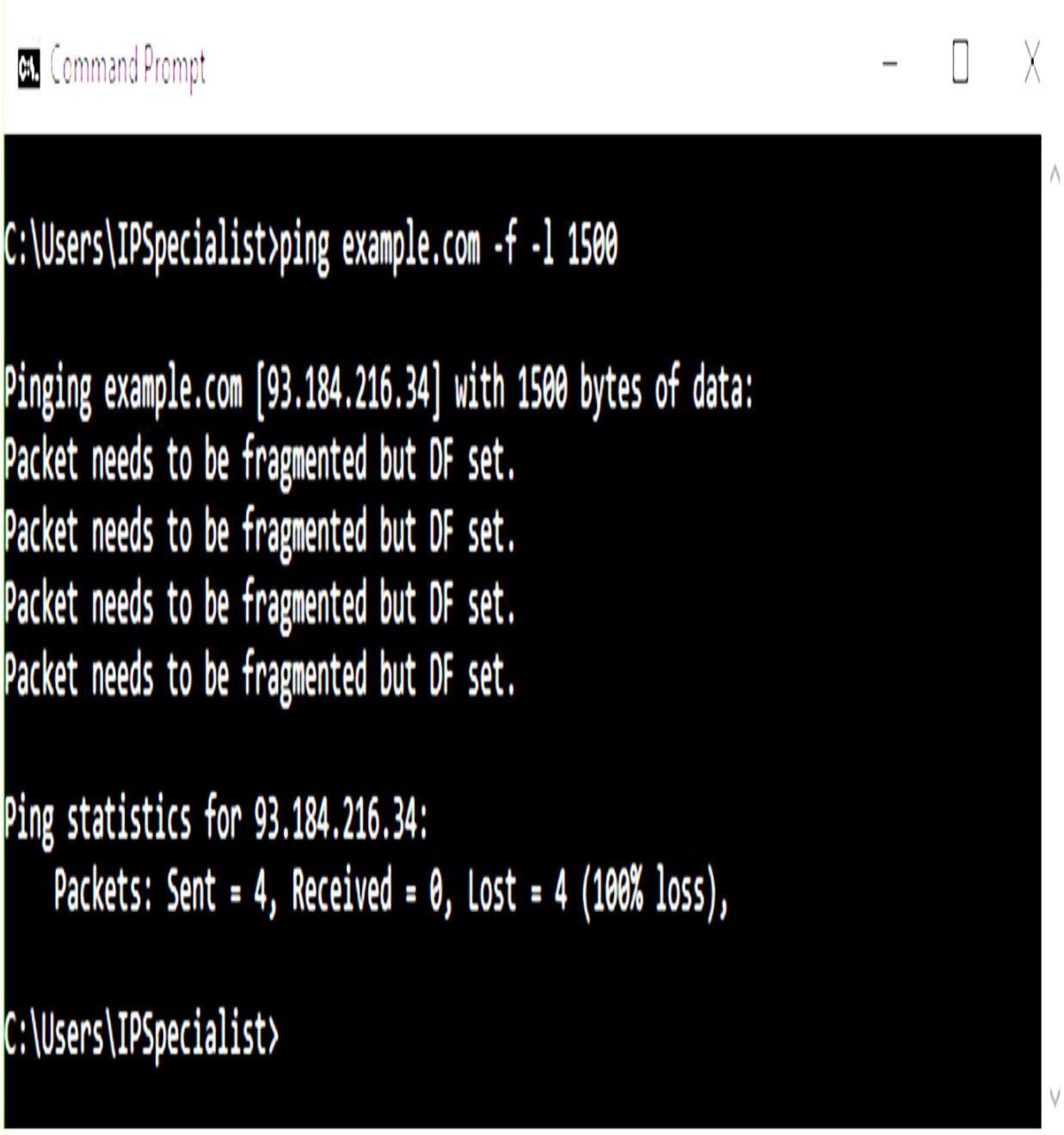


Figure 2-62: Ping example.com with DF Bit Set

The output shows "***Packet needs to be fragmented but DF set***", which means 150o bits will require being fragmented. Let's try again with a smaller value:

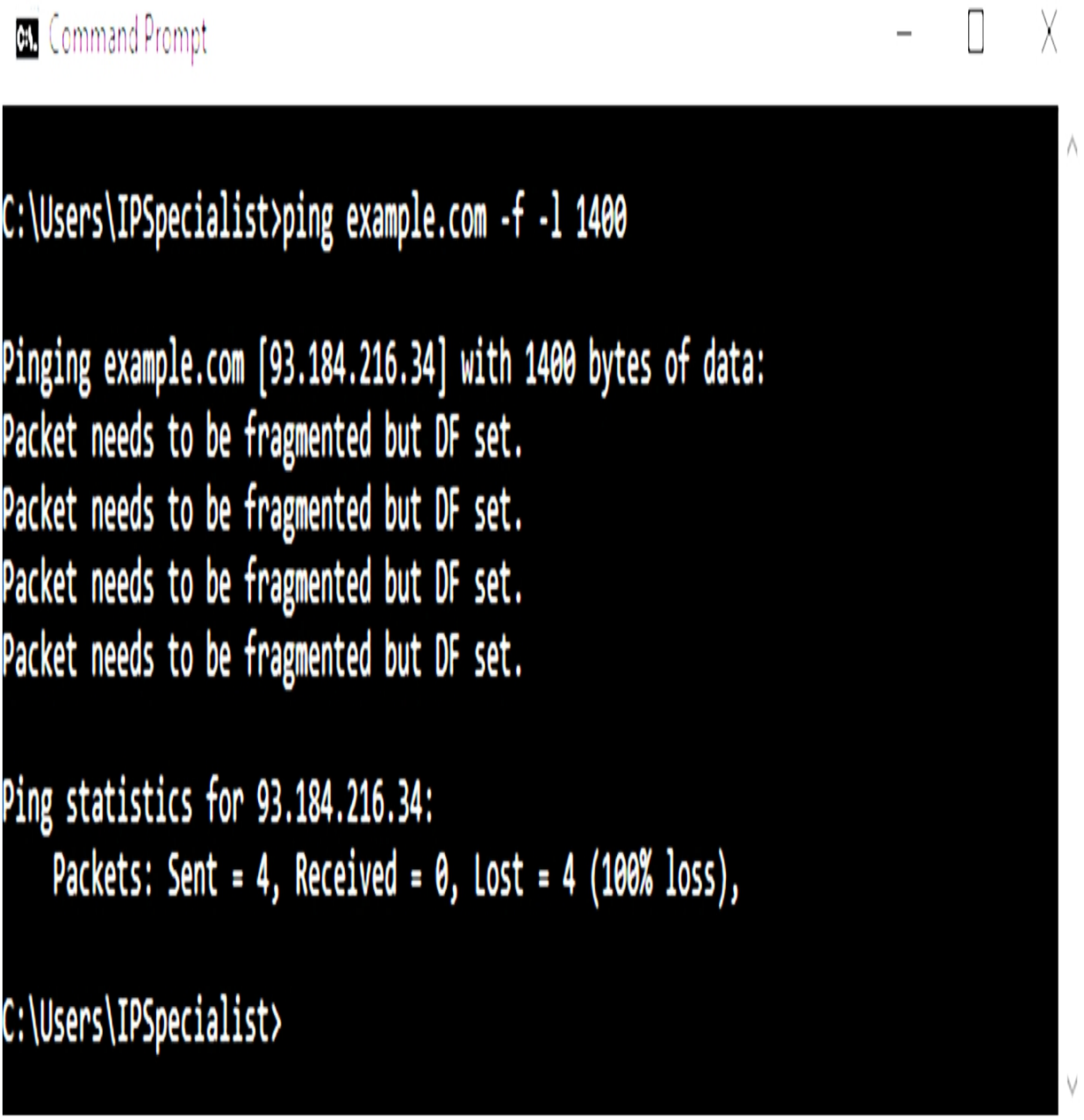


Figure 2-63: Ping example.com with DF Bit Set

The output again shows "***Packet needs to be fragmented but DF set***", which means 140o bits will require being fragmented. Let's try again with another smaller value:

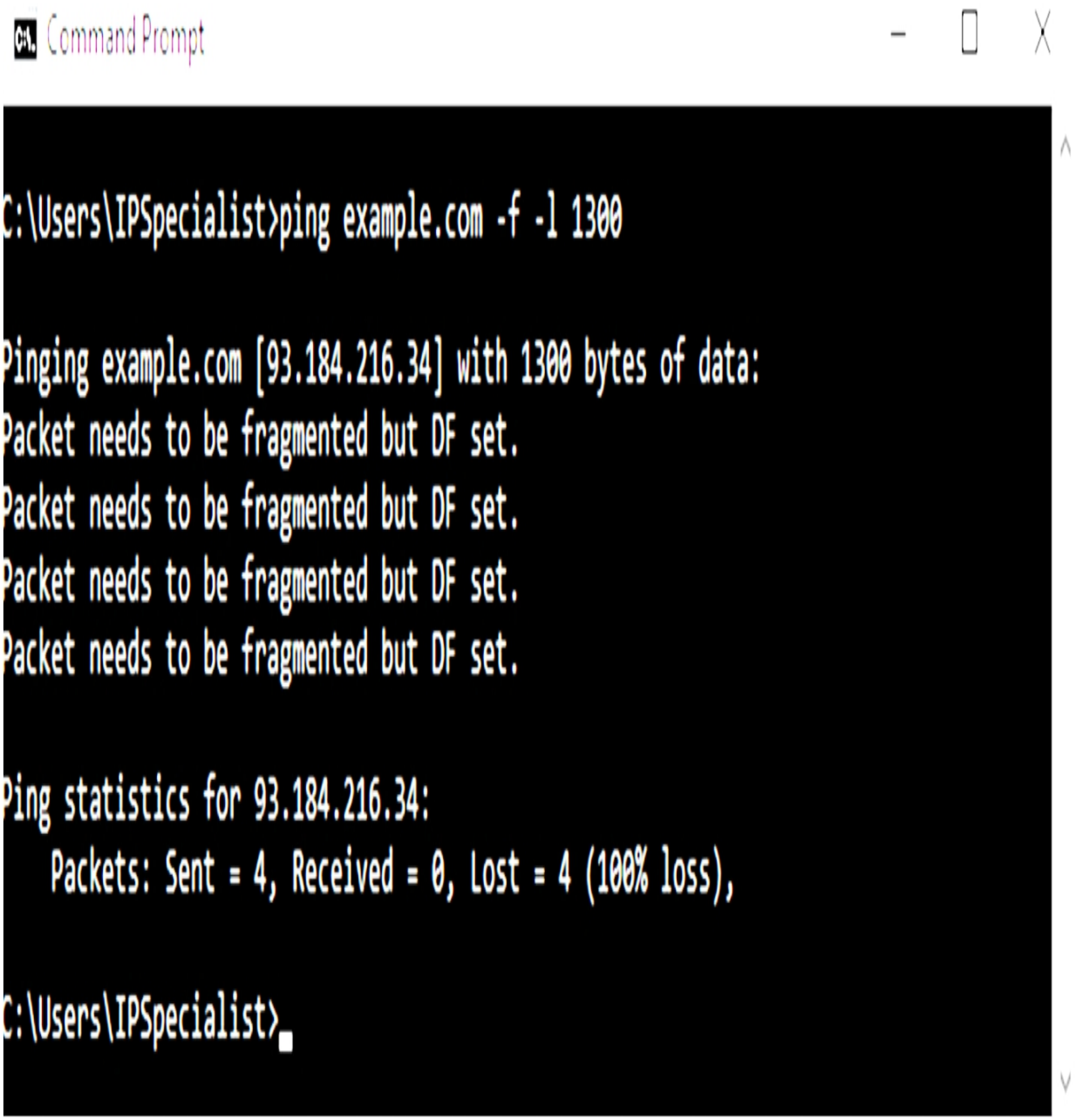


Figure 2-64: Ping example.com with DF Bit Set

The output again shows "***Packet needs to be fragmented but DF set***", which means 130o bits will require being fragmented. Let's try again with an even smaller value:

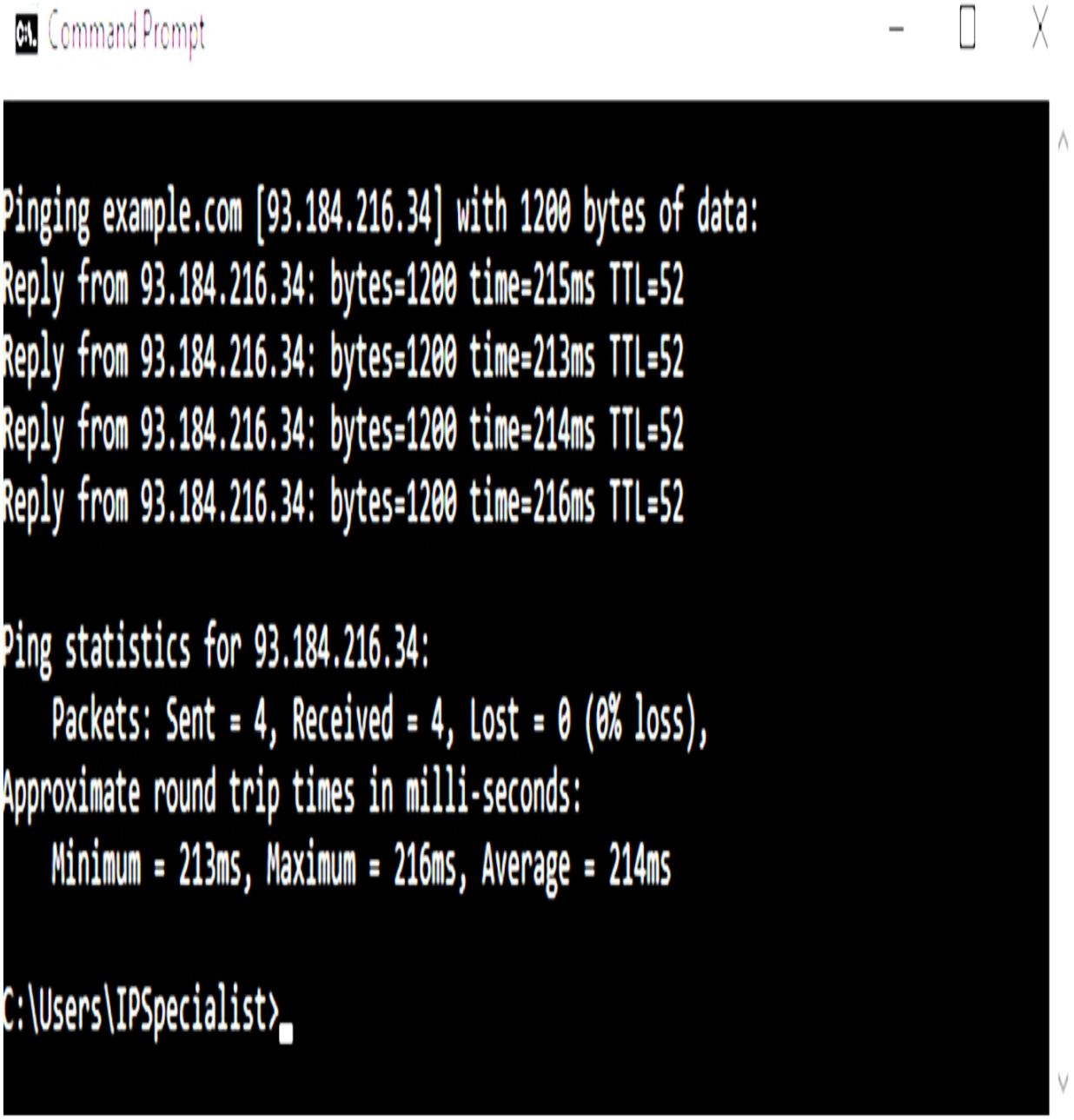


Figure 2-65: Ping example.com with DF Bit Set

The output now shows the reply, which means 120o bits will not require being fragmented. You can try again to get a more appropriate fragment value. Now, enter the command "*Tracert example.com*" to trace the target.

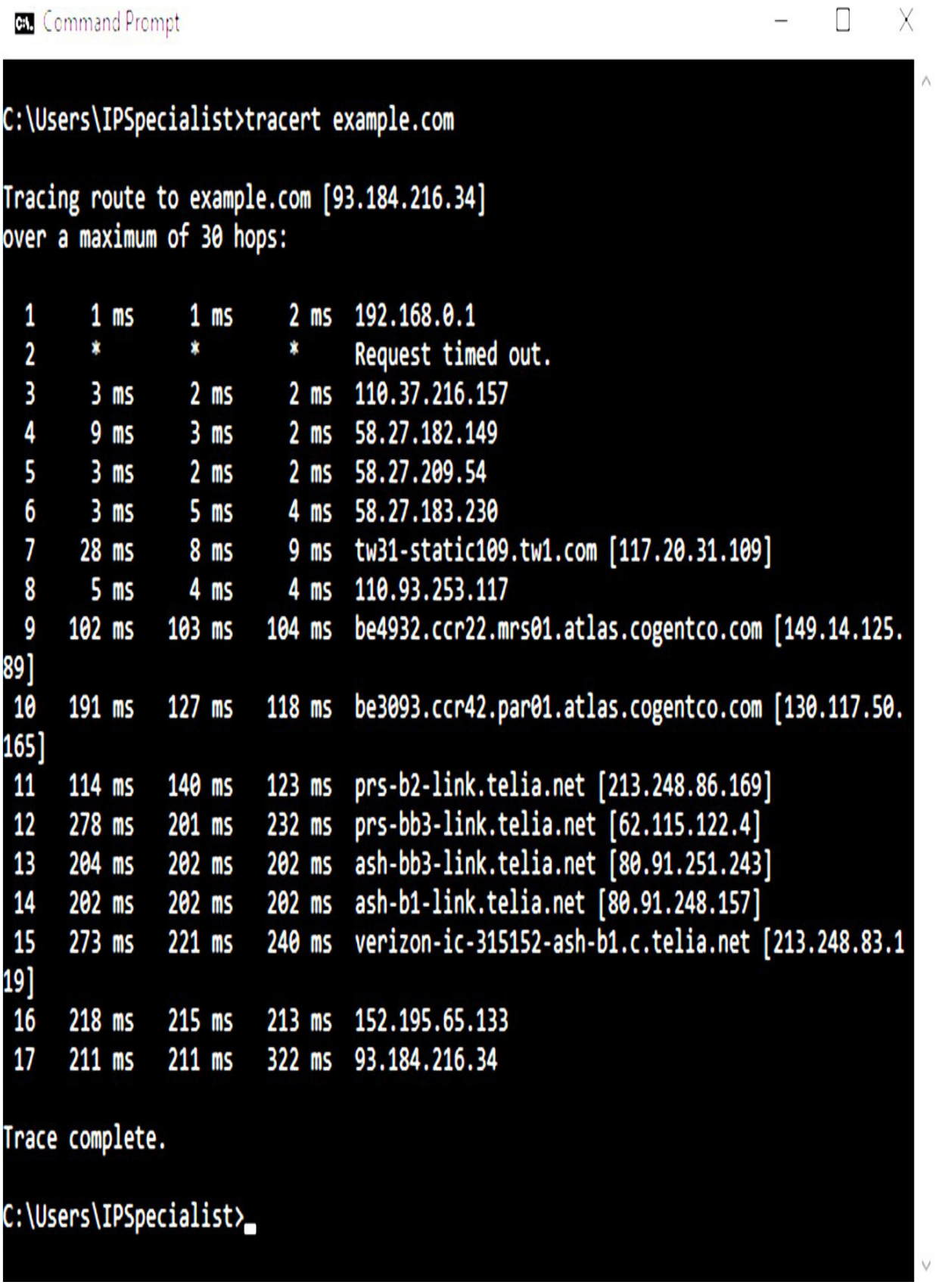

Command Prompt
C:\Users\IPSpecialist>tracert example.com
Tracing route to example.com [93.184.216.34]
over a maximum of 30 hops:
1 1 ms 1 ms 2 ms 192.168.0.1
2 * * * Request timed out.
3 3 ms 2 ms 2 ms 110.37.216.157
4 9 ms 3 ms 2 ms 58.27.182.149
5 3 ms 2 ms 2 ms 58.27.209.54
6 3 ms 5 ms 4 ms 58.27.183.230
7 28 ms 8 ms 9 ms tw31-static109.tw1.com [117.20.31.109]
8 5 ms 4 ms 4 ms 110.93.253.117
9 102 ms 103 ms 104 ms be4932.ccr22.mrs01.atlas.cogentco.com [149.14.125.89]
10 191 ms 127 ms 118 ms be3093.ccr42.par01.atlas.cogentco.com [130.117.50.165]
11 114 ms 140 ms 123 ms prs-b2-link.telia.net [213.248.86.169]
12 278 ms 201 ms 232 ms prs-bb3-link.telia.net [62.115.122.4]
13 204 ms 202 ms 202 ms ash-bb3-link.telia.net [80.91.251.243]
14 202 ms 202 ms 202 ms ash-b1-link.telia.net [80.91.248.157]
15 273 ms 221 ms 240 ms verizon-ic-315152-ash-b1.c.telia.net [213.248.83.119]
16 218 ms 215 ms 213 ms 152.195.65.133
17 211 ms 211 ms 322 ms 93.184.216.34
Trace complete.
C:\Users\IPSpecialist>

Figure 2-66: Ping example.com with DF Bit Set

From the output, you can get information about the hops between the source (your PC) and the destination (example.com), response times, and other information.

Lab 2-5: Downloading a Website Using a Website Copier tool (HTTrack)

Case Study: We are using Windows Server 20 16 for this lab. You can check the compatibility of the HTTrack Website copier tool on different platforms such as Windows, Linux, and Android from the website http://www.httrack.com . Download and install the HTTrack tool. In this lab, we are going to copy a website into our local directory and browse it from there in an offline environment.

Procedure:

Download and install the WinHTTrack Website Copier Tool.


Setup - WinHTTrack Website Copier
Welcome to the WinHTTrack Website Copier Setup Wizard
This will install WinHTTrack Website Copier 3.49-2 (x64) on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel

Figure 2-67: WinHTTrack Website Copier
HTTrack Website Copier tool installation.

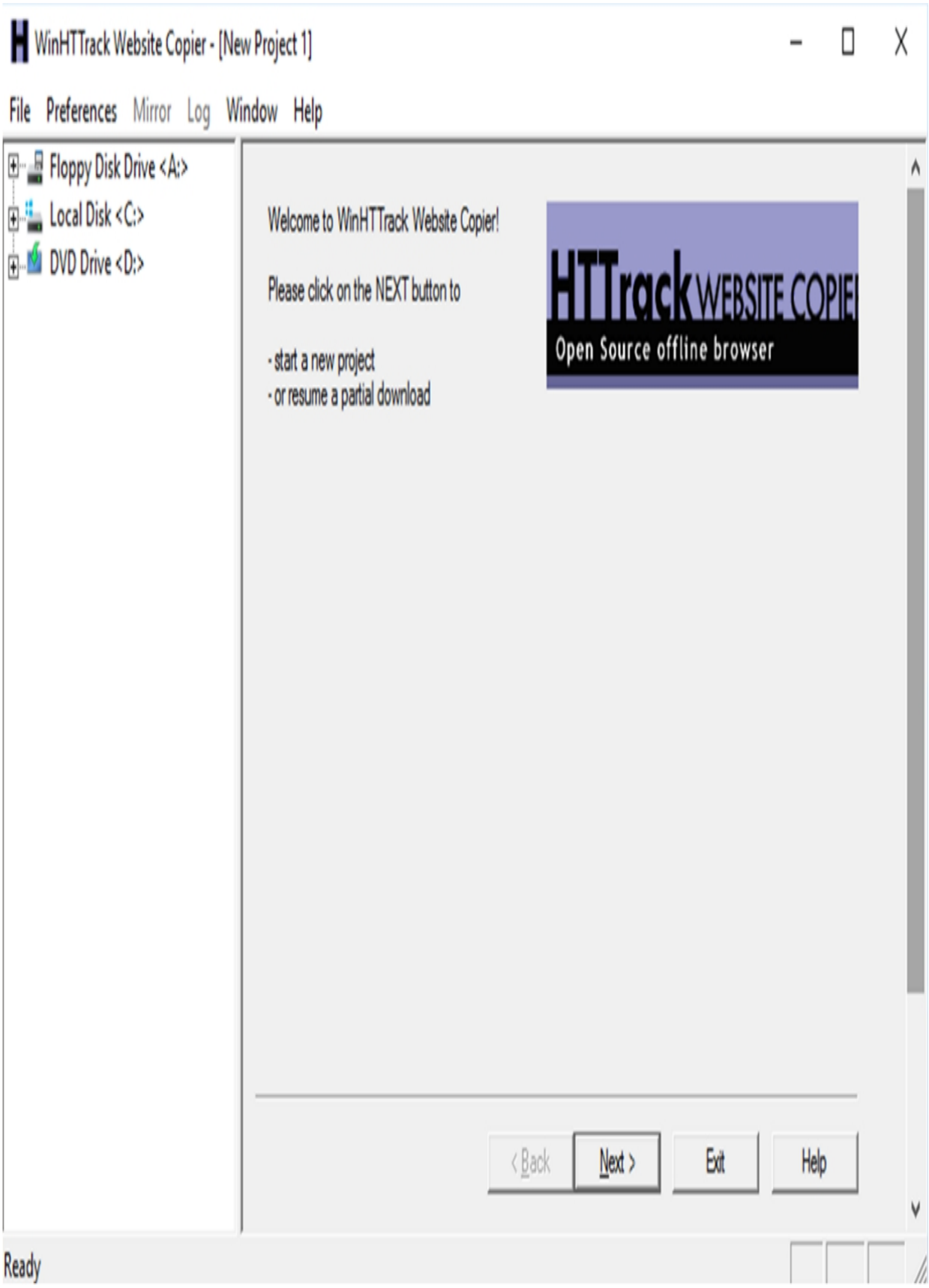

WinHTTrack Website Copier - [New Project 1]
File Preferences Mirror Log Window Help
Floppy Disk Drive <A:>
Local Disk <C:>
DVD Drive <D:>
Welcome to WinHTTrack Website Copier!
Please click on the NEXT button to
- start a new project
- or resume a partial download
HTTrack WEBSITE COPIER
Open Source offline browser
< Back
Next >
Exit
Help
Ready

Figure 2-68: WinHTTrack Website Copier

Click “Next”.

Figure 2-69: Creating a new project

Enter a project name. For example, Testing_Project.

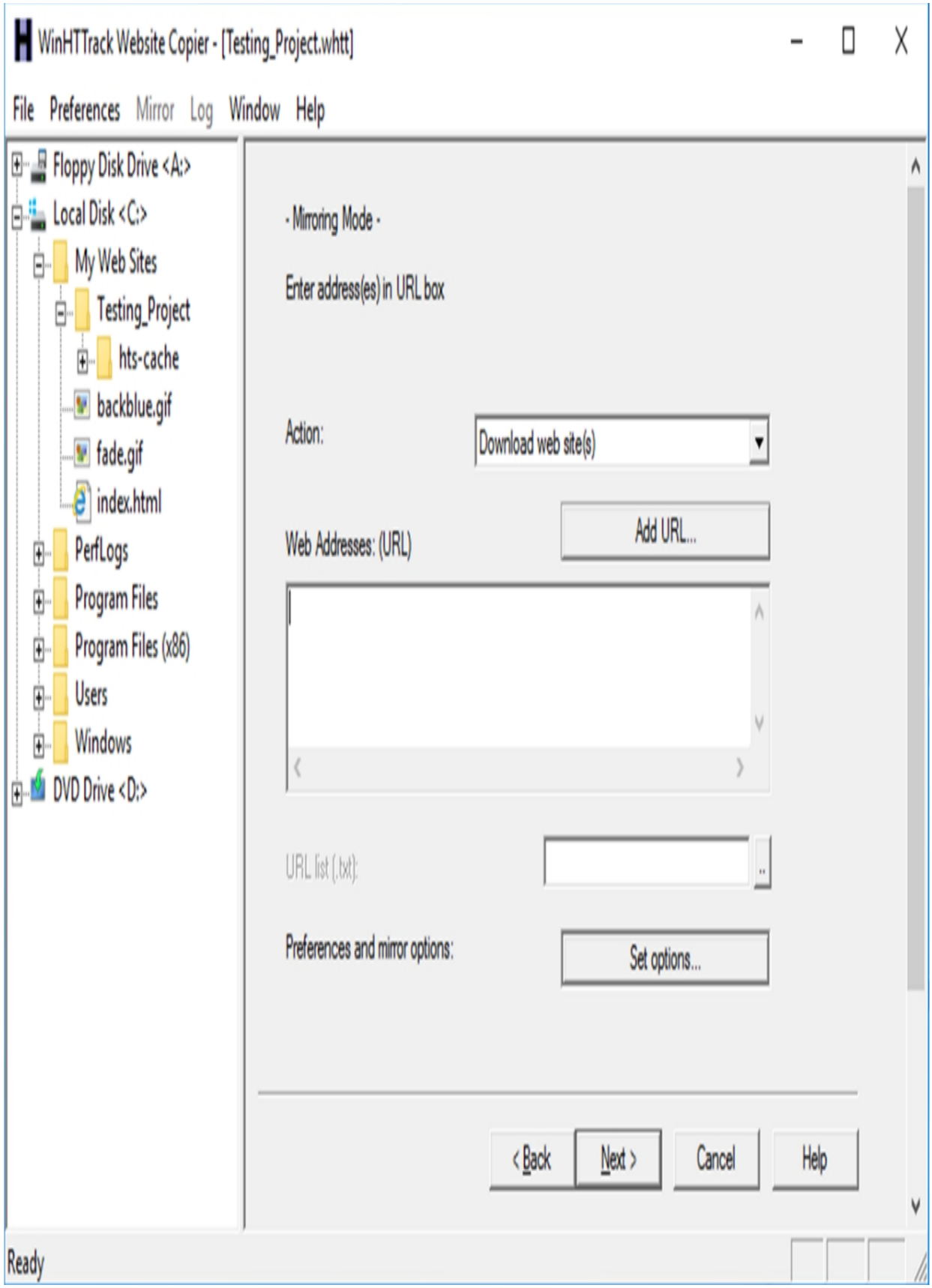

WinHTTrack Website Copier - [Testing_Project.whtt]
File Preferences Mirror Log Window Help
Floppy Disk Drive <A:>
Local Disk <C:>
My Web Sites
Testing_Project
hts-cache
backblue.gif
fade.gif
index.html
PerfLogs
Program Files
Program Files (x86)
Users
Windows
DVD Drive <D:>
- Mirroring Mode -
Enter address(es) in URL box
Action:
Download web site(s)
Web Addresses: (URL)
Add URL...
URL list (.txt):
Preferences and mirror options:
Set options...
< Back
Next >
Cancel
Help
Ready

Figure 2-70: Setting Target

Click on the "Set Options" button.

Figure 2-71: Configuring Options

Go to the "***Scan Rules***" tab and select options as per your requirements.

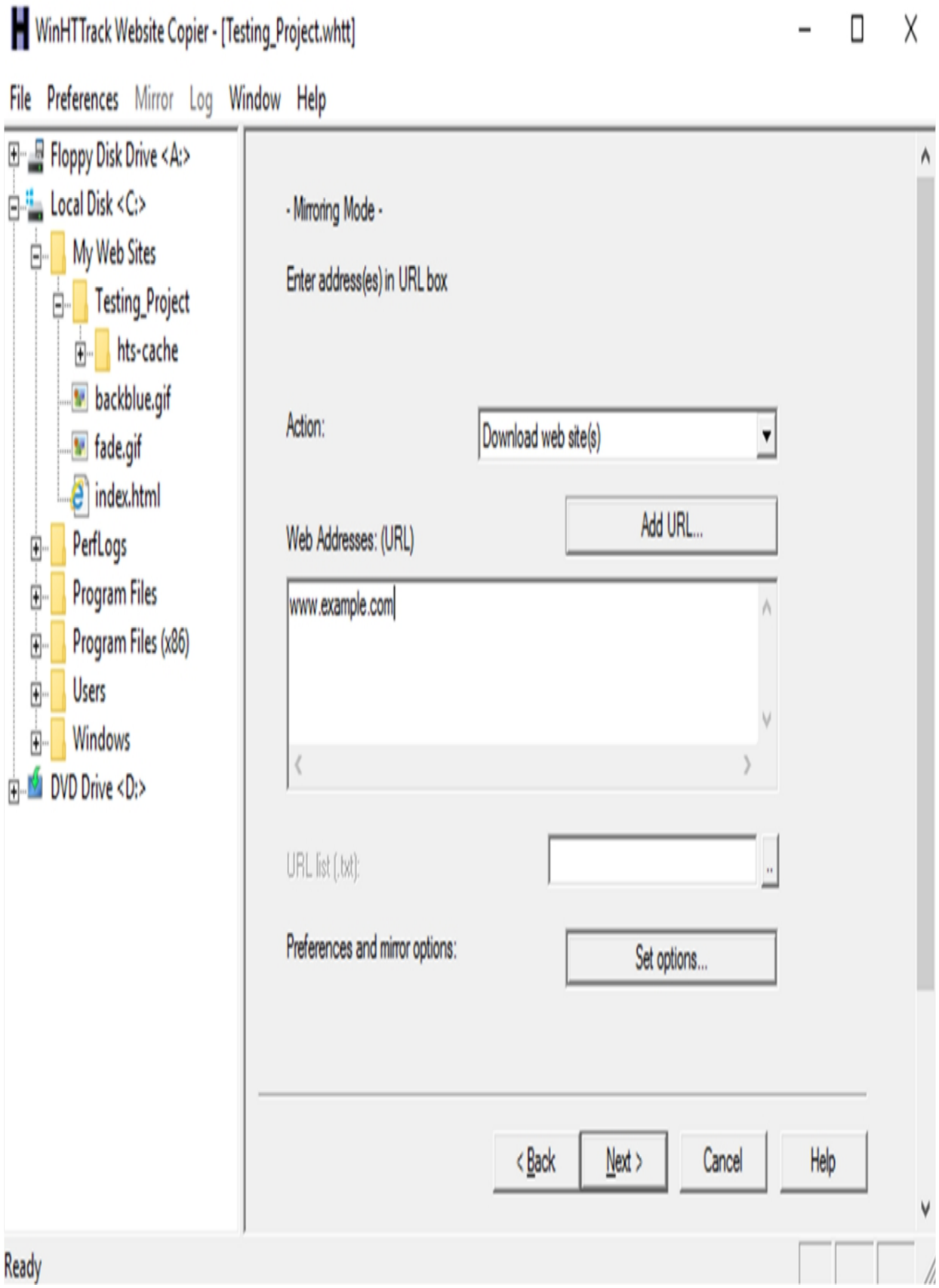

WinHTTrack Website Copier - [Testing_Project.whtt]
File Preferences Mirror Log Window Help
Floppy Disk Drive <A:>
Local Disk <C:>
My Web Sites
Testing_Project
hts-cache
backblue.gif
fade.gif
index.html
PerfLogs
Program Files
Program Files (x86)
Users
Windows
DVD Drive <D:>
- Mirroring Mode -
Enter address(es) in URL box
Action:
Download web site(s)
Web Addresses: (URL)
Add URL...
www.example.com
URL list (.txt):
Preferences and mirror options:
Set options...
< Back
Next >
Cancel
Help
Ready

Figure 2-72: Configuring Options

Enter the Web Address in the field and click “Next”.

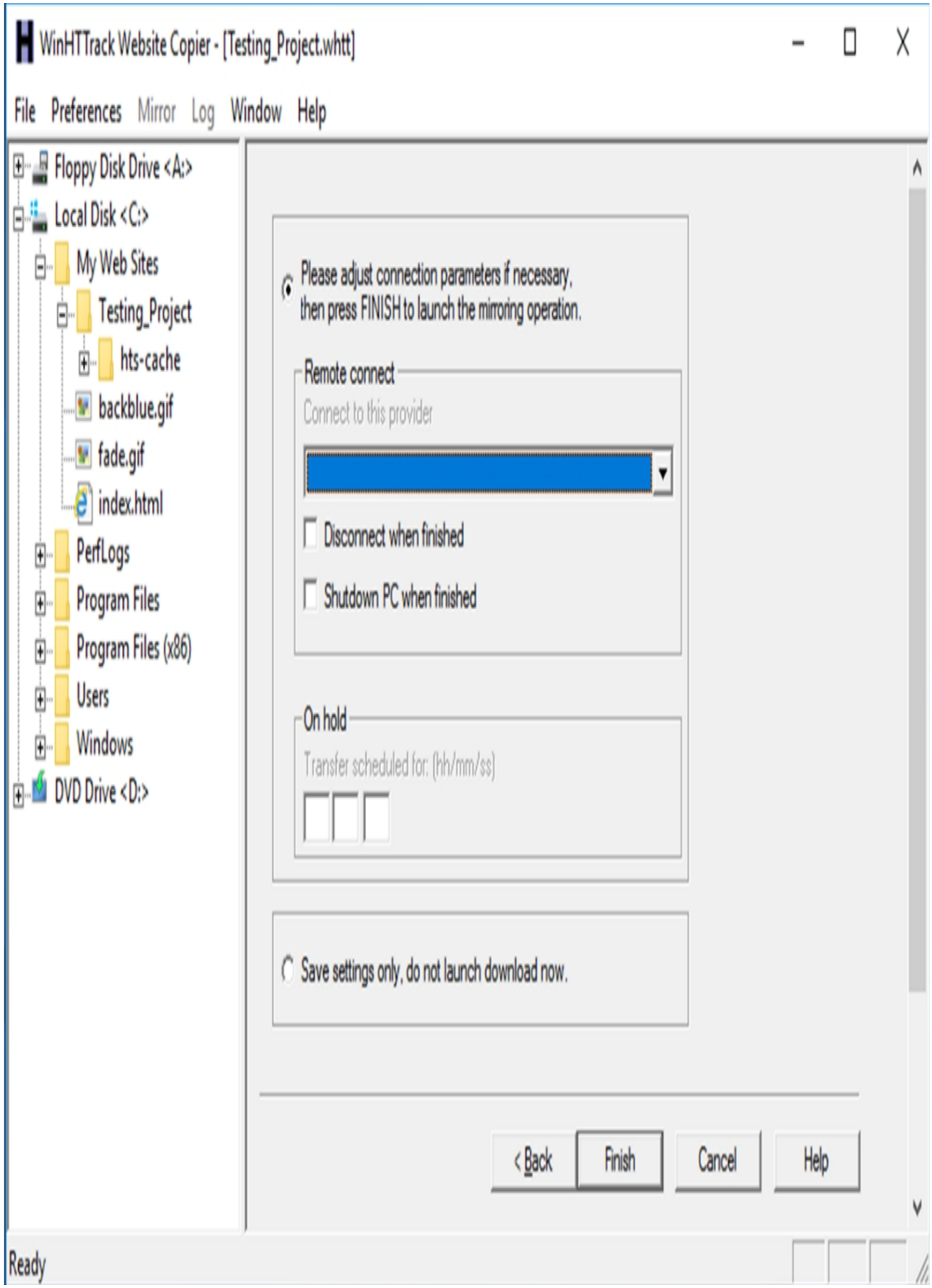

WinHTTrack Website Copier - [Testing_Project.whtt]
File Preferences Mirror Log Window Help
Floppy Disk Drive <A:>
Local Disk <C:>
My Web Sites
Testing_Project
hts-cache
backblue.gif
fade.gif
index.html
PerfLogs
Program Files
Program Files (x86)
Users
Windows
DVD Drive <D:>
Please adjust connection parameters if necessary,
then press FINISH to launch the mirroring operation.
Remote connect
Connect to this provider
Disconnect when finished
Shutdown PC when finished
On hold
Transfer scheduled for: (hh/mm/ss)
Save settings only, do not launch download now.
< Back
Finish
Cancel
Help
Ready

Figure 2-73: Configuring Options

Click “Next”.

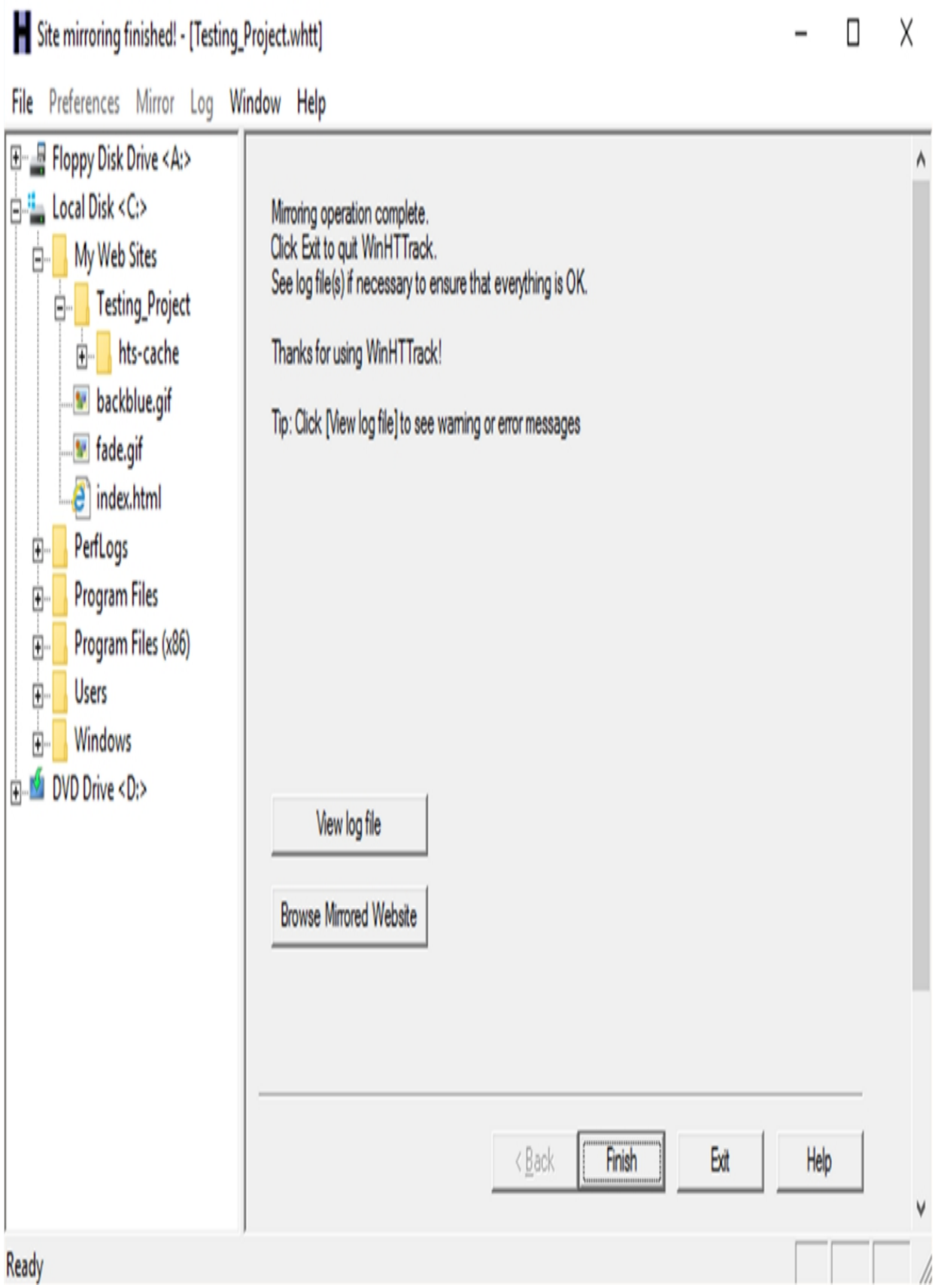

Site mirroring finished! - [Testing_Project.whtt]
File Preferences Mirror Log Window Help
Floppy Disk Drive <A:>
Local Disk <C:>
My Web Sites
Testing_Project
hts-cache
backblue.gif
fade.gif
index.html
PerfLogs
Program Files
Program Files (x86)
Users
Windows
DVD Drive <D:>
Mirroring operation complete.
Click Exit to quit WinHTTrack.
See log file(s) if necessary to ensure that everything is OK.
Thanks for using WinHTTrack!
Tip: Click [View log file] to see warning or error messages
View log file
Browse Mirrored Website
< Back
Finish
Exit
Help
Ready

Figure 2-74: Copying Complete

Click “Browse Mirrored Website”.

Figure 2-75: Browsing Copied Website

Select your favorite web browser.

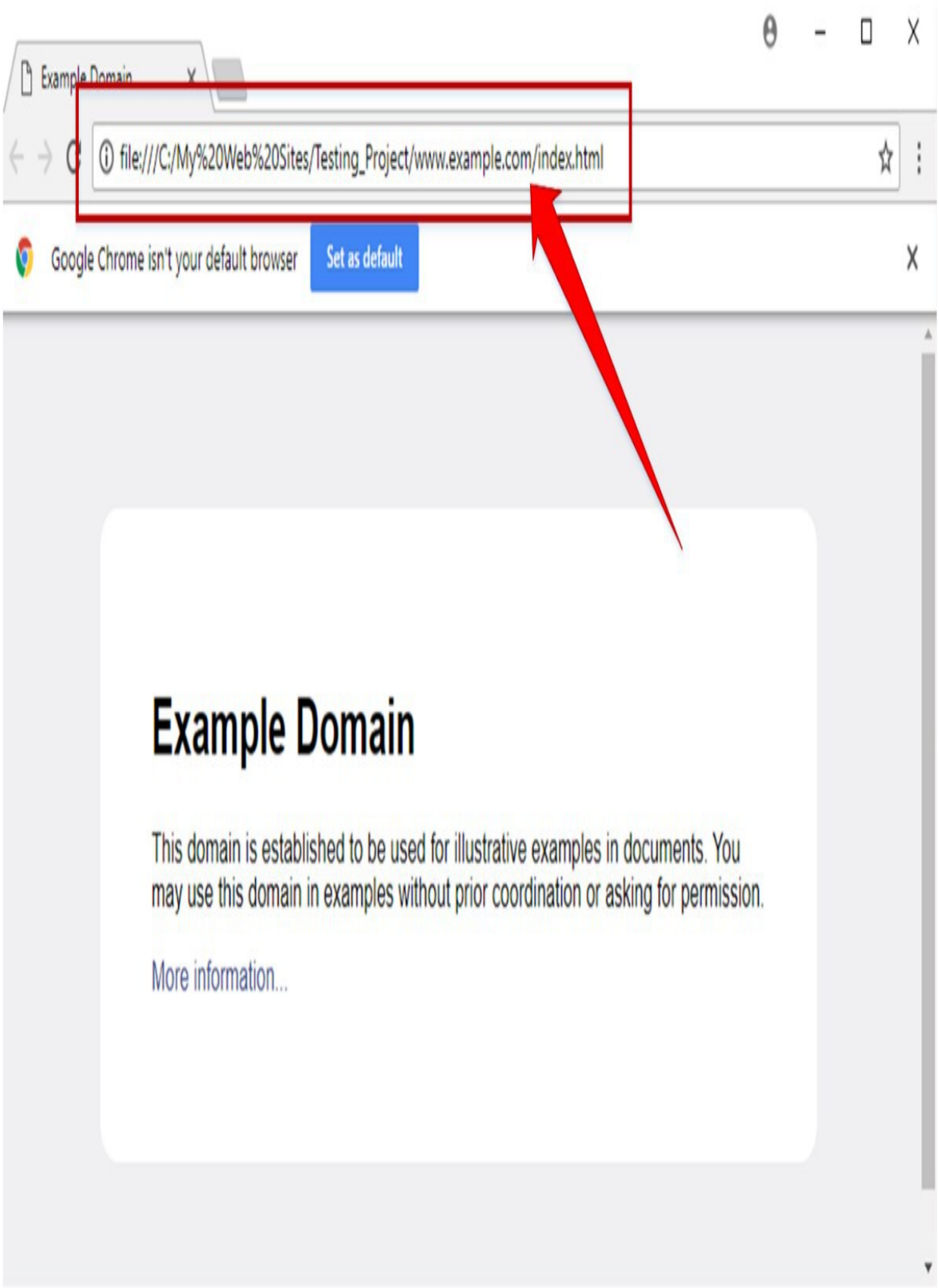

Example Domain
file:///C:/My%20Web%20Sites/Testing_Project/www.example.com/index.html
Google Chrome isn't your default browser
Set as default
Example Domain
This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission.
More information...

Figure 2-76: Website browsed from a local directory

Observe the above output. The website example.com is copied into a local directory and browsed from there. Now you can explore the website in an offline environment for accessing the structure of the website and other parameters.

Figure 2-77: Original Website

To be sure, compare the website to the original website. Open a new tab and go to the URL example.com.

Lab 2-6: Gathering Information Using Metasploit

Case Study: In this lab, we are using Metasploit Framework, a default application in Kali Linux for gathering more information about the host in a network. A Metasploit Framework is a powerful tool, popularly used for scanning and gathering information in the hacking environment. Metasploit Pro enables you to automate the process of discovery and exploitation and provides you with the necessary tools to perform the manual testing phase of a penetration test. You can use Metasploit Pro to scan for open ports and services, exploit vulnerabilities, pivot further into a network, collect evidence, and create a report of the test results.

Note: Metasploit is a penetration testing system that makes hacking way easier than it used to be. It is an essential tool for many attackers and defenders.

Topology Information: In this lab, we are going run Metasploit Framework on a private network 10. 10.50.0/24 where different hosts are live including Windows 7, Kali Linux, Windows Server 20 16 and others.

Procedure:

Open Kali Linux and run Metasploit Framework.

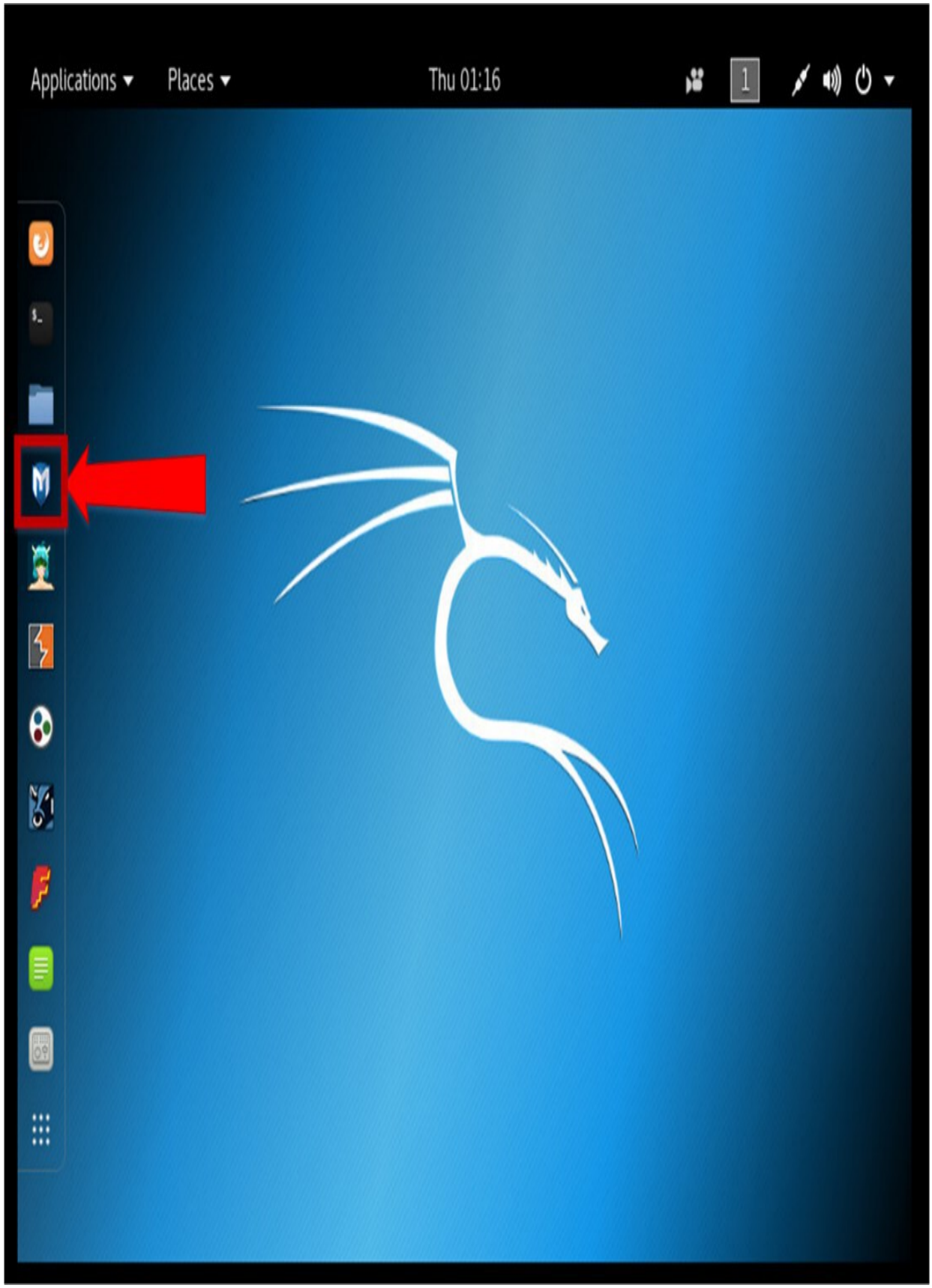

Applications
Places
Thu 01:16
1

Figure 2-78: Kali Linux Desktop

Metasploit Framework initialization as shown in the figure below.

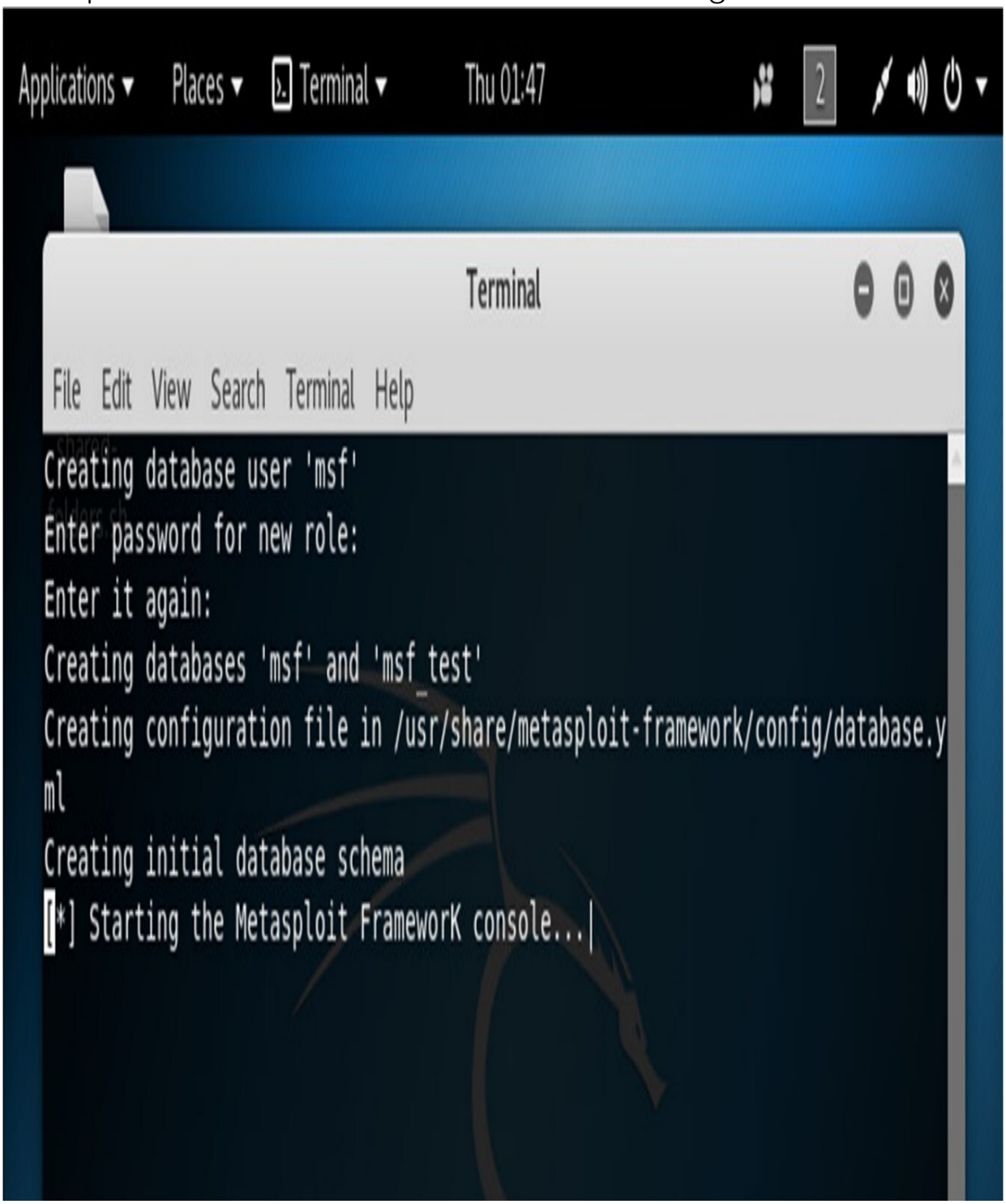


Figure 2-79: Metasploit Framework

msf > db_status

[*] postgresql connected to msf

// If your database is not connected, it means your database is not initiated. You will need to exit msfconsole and restart the postgresql service.

// Performing nmap Scan for ping sweep on the subnet 10. 10.50.0/24 msf > nmap -Pn -sS -A -oX Test 10. 10.50.0/24
[*] exec: nmap -Pn -sS -A -oX Test 10. 10.50.0/24
Starting Nmap 7.60 (https://nmap.org) at 20 18-04-26 0 1:49 EDT
Stats: 0:04:3 1 elapsed; 247 hosts completed (8 up), 8 undergoing Script Scan NSE
Timing: About 99.77% done; ETC: 0 1:53 (0:00:00 remaining)
Stats: 0:05:04 elapsed; 247 hosts completed (8 up), 8 undergoing Script Scan NSE
Timing: About 99.79% done; ETC: 0 1:54 (0:00:00 remaining)
Stats: 0:06:2 1 elapsed; 247 hosts completed (8 up), 8 undergoing Script Scan NSE
Timing: About 99.93% done; ETC: 0 1:55 (0:00:00 remaining)
Nmap scan report for 10. 10.50. 1
Host is up (0.00 12s latency).
Not shown: 996 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh Cisco SSH 1.25 (protocol 1.5)
| ssh-hostkey:
|_ 5 12 ca:9c:c7:d2:d4:b0:78:82:3e:34:8f:cf:00:9d:75:db (RSA 1)
|_sshv 1: Server supports SSHv 1
23/tcp open telnet Cisco router telnetd
5060/tcp open sip-proxy Cisco SIP Gateway (IOS 15.2.4.M4)

|_sip-methods: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER

506 1 /tcp open tcpwrapped
MAC Address: C0:67:AF:C7:D9:80 (Cisco Systems)

OS details: Cisco 836, 890, 175 1, 184 1, 2800, or 2900 router (IOS 12.4 15. 1), Cisco Aironet 1 14 1N (IOS 12.4) or 3602I (IOS 15.3) WAP, Cisco Aironet 2600-series WAP (IOS 15.2(2))

Network Distance: 1 hop
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios
Nmap scan report for 10. 10.50. 10 Host is up (0.00030s latency). Not shown: 990 filtered ports PORT STATE SERVICE 22/tcp open ssh | ssh-hostkey:
VERSION OpenSSH 5.6 (protocol 2.0)

TRACEROUTE
HOP RTT ADDRESS 1 1. 15 ms 10. 10.50. 1

| 1024 e3:93:64: 12:9c:c0:70:72:35:e 1:ac:6 1:af:cc:49:ec (DSA) 8300/tcp closed tmi
MAC Address: F8:72:EA:A4:A 1:CC (Cisco Systems)

|_ 2048 2a:0b:42:38:f4:ca:d6:07:95:aa:87:ed:52:de:d 1: 14 (RSA)
80/tcp open http VMware ESXi Server httpd
|_http-title: Did not follow redirect to https:// 10. 10.50. 10/
427/tcp open svrloc?
443/tcp open ssl/http VMware ESXi Server httpd
|_http-title: " + ID_EESX_Welcome + "

| ssl-cert: Subject:
commonName=localhost.localdomain/organizationName=VMware,
Inc/stateOrProvinceName=California/countryName=US

| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 20 14-0 1- 15T03:42:3 1
|_Not valid after: 2025-07- 16T03:42:3 1
|_ssl-date: 20 18-04-25T 19:58:24+00:00; 9h53m36s from scanner time. | vmware-
version:
| Server version: VMware ESXi 5. 1.0
| Build: 106549 1
| Locale version: INTL 000
| OS type: vmnix-x86
|_ Product Line ID: embeddedEsx
902/tcp open ssl/vmware-auth VMware Authentication Daemon 1. 10 (Uses VNC,
SOAP) 5988/tcp closed wbem-http
5989/tcp open ssl/wbem SBLIM Small Footprint CIM Broker

| ssl-cert: Subject:
commonName=localhost.localdomain/organizationName=VMware,
Inc/stateOrProvinceName=California/countryName=US

| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 20 14-0 1- 15T03:42:3 1
|_Not valid after: 2025-07- 16T03:42:3 1
|_ssl-date: 20 18-04-25T 19:58:23+00:00; 9h53m36s from scanner time. 8000/tcp
open http-alt?
8 100/tcp open tcpwrapped

Aggressive OS guesses: VMware ESXi 5.0 5.5 (96%), VMware ESXi 5.5 (96%),
VMware ESXi 4. 1 (95%), VMware ESXi 6.0.0 (93%), FreeBSD
(93%), VMware ESXi 4. 1.0 (93%), VMware ESX Server
7.0-RELEASE-p 1 10.0-CURRENT

4.0. 1 (9 1%), FreeBSD 5.2. 1- RELEASE (9 1%), FreeBSD 8.0-BETA2 10. 1-RELEASE
(90%), FreeBSD 5.3 5.5 (90%)

No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Service Info: Host: localhost.localdomain; CPE: cpe:/o:vmware:esxi,
cpe:/o:vmware:ESXi:5. 1.0

Host script results: |_clock-skew: mean: 9h53m36s, deviation: 0s, median: 9h53m36s
TRACEROUTE
HOP RTT ADDRESS 1 0.30 ms 10. 10.50. 10

Nmap scan report for 10. 10.50. 1 1 Host is up (0.00058s latency). Not shown: 990 filtered ports PORT STATE SERVICE 22/tcp open ssh | ssh-hostkey:
VERSION OpenSSH 5.6 (protocol 2.0) | vmware-version:
| Server version: VMware ESXi 5. 1.0
| Build: 106549 1
| Locale version: INTL 000
| OS type: vmnix-x86
|_ Product Line ID: embeddedEsx
902/tcp open ssl/vmware-auth VMware Authentication Daemon 1. 10 (Uses VNC, SOAP) 5988/tcp closed wbem-http
5989/tcp open ssl/wbem SBLIM Small Footprint CIM Broker

| 1024 6f:d3:3d:cb:54:0b:83:3e:bd:25: 1c:da:67:b6:92:fb (DSA)
|_ 2048 f9:bc:20:c5:6e:db:6a:86:ea:f5:24:06:57:c6:d9:6f (RSA)
80/tcp open http VMware ESXi Server httpd
|_http-title: Did not follow redirect to https:// 10. 10.50. 1 1/
427/tcp open svrloc?
443/tcp open ssl/http VMware ESXi Server httpd
|_http-title: " + ID_EESX_Welcome + "

| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=VMware, Inc/stateOrProvinceName=California/countryName=US

| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 20 14-0 1- 18T05:33:03
|_Not valid after: 2025-07- 19T05:33:03
|_ssl-date: 20 18-04-25T 19:50: 12+00:00; 10h0 1m33s from scanner time.

| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=VMware, Inc/stateOrProvinceName=California/countryName=US

| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 20 14-0 1- 18T05:33:03
|_Not valid after: 2025-07- 19T05:33:03
|_ssl-date: 20 18-04-25T 19:50:25+00:00; 10h0 1m35s from scanner time. 8000/tcp open http-alt?
8 100/tcp open tcpwrapped
8300/tcp closed tmi
MAC Address: F8:72:EA:A4:A 1:2C (Cisco Systems)
Device type: specialized
Running: VMware ESXi 5.X

OS CPE: cpe:/o:vmware:esxi:5
OS details: VMware ESXi 5.0 5.5
Network Distance: 1 hop

Service Info: Host: localhost.localdomain; CPE: cpe:/o:vmware:esxi,
cpe:/o:vmware:ESXi:5. 1.0
Host script results: |_clock-skew: mean: 10h0 1m34s, deviation: 1s, median: 10h0
1m35s
TRACEROUTE
HOP RTT ADDRESS

1 0.58 ms 10. 10.50. 1 1 Not shown: 998 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0) |
ssh-hostkey:
| 2048 8d:b4:b0:0 1:63:84:eb:c7:bf:cf:f7:b0:c3: 12:0e: 13 (RSA)
| 256 02:3 1:3e:d3:75:97:f2: 10:88:30:6a:c 1:ca:a4:82:bf (ECDSA)
|_ 256 c5:2 1:3a:a7:8 1:f5:a6:00:ee:5e:76:94:88:68:03: 1d (EdDSA)
80/tcp open http Apache httpd 2.4. 18 ((Ubuntu))
|_http-server-header: Apache/2.4. 18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:72:4A:C 1 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 4.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for vc.ooredoocloud.qa (10. 10.50.20) Host is up (0.00065s
latency).
TRACEROUTE
HOP RTT ADDRESS

1 0.65 ms 10. 10.50.20 | Build: 5528349 | Locale version: INTL | OS type: win32-x86
|_ Product Line ID: ws

Nmap scan report for 10. 10.50. 100
Host is up (0.00078s latency).
Not shown: 983 closed ports
PORT STATE SERVICE VERSION

135 /tcp open msrpc Microsoft Windows RPC 139/tcp open netbios-ssn Microsoft
Windows netbios-ssn 443/tcp open ssl/http VMware VirtualCenter Web service
|_http-title: Site doesn't have a title (text; charset=plain). | ssl-cert: Subject:
commonName=VMware/countryName=US | Not valid before: 20 17- 12- 19T 17:36:0 1
|_Not valid after: 20 18- 12- 19T 17:36:0 1
|_ssl-date: TLS randomness does not represent time

| vmware-version:
| Server version: VMware Workstation 12.5.6

445/tcp open microsoft-ds Windows 7 Professional 760 1 Service Pack 1
microsoftds (workgroup: WORKGROUP)

554 /tcp open rtsp?
902/tcp open ssl/vmware-auth VMware Authentication Daemon 1. 10 (Uses VNC,
SOAP)
9 12/tcp open vmware-auth VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1025/tcp open msrpc
1026/tcp open msrpc
1027/tcp open msrpc
1028/tcp open msrpc
1030/tcp open msrpc
103 1/tcp open msrpc
2869/tcp open http
3389/tcp open ms-wbt-server
Microsoft Windows RPC
Microsoft Windows RPC
Microsoft Windows RPC
Microsoft Windows RPC
Microsoft Windows RPC
Microsoft Windows RPC
Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) Microsoft Terminal Service

| ssl-cert: Subject: commonName=Win 7-PC
20 17- 12- 12T 19:55:25| Not valid before:
|_Not valid after: 20 18-06- 13T 19:55:25
|_ssl-date: 20 18-04-26T05:47:49+00:00; 3m54s from scanner time.
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) |_http-server-header:
Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable

10243 /tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) |_http-server-
header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
MAC Address: 00:0C:29:95:04:33 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8. 1

OS CPE: cpe:/o:microsoft:windows_7::cpe:/o:microsoft:windows_7::sp 1
cpe:/o:microsoft:windows_server_2008::sp 1
cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8
cpe:/o:microsoft:windows_8. 1

OS details: Microsoft Windows 7 SP0 - SP 1, Windows Server 2008 SP 1, Windows
Server 2008 R2, Windows 8, or Windows 8. 1 Update 1

Network Distance: 1 hop
Service Info: Host: WIN7-PC; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:vmware:Workstation: 12.5.6

Host script results: |_clock-skew: mean: 3m54s, deviation: 0s, median: 3m54s

|_nbstat: NetBIOS name: WIN7-PC, NetBIOS 00:0c:29:95:04:33 (VMware)
| smb-os-discovery:
| OS: Windows 7 Professional 760 1 Service Pack user: <unknown>, NetBIOS MAC:

1 (Windows 7 Professional 6. 1) | OS CPE: cpe:/o:microsoft:windows_7::sp 1:professional | Computer name: Win7-PC
| NetBIOS computer name: WIN7-PC₩x00
| Workgroup: WORKGROUP₩x00
|_ System time: 20 18-04-26T 10:47:56+05:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default) | smb2-security-mode:
| 2.02:
|_ Message signing enabled but not required | smb2-time:
| date: 20 18-04-26 0 1:48:04
|_ start_date: 20 18-03-27 07:26:43

TRACEROUTE HOP RTT ADDRESS
1 0.78 ms 10. 10.50. 100

Nmap scan report for 10. 10.50.202 445/tcp open microsoft-ds Windows 7 Professional 760 1 Service Pack 1 microsoftds (workgroup: WORKGROUP)

Host is up (0.00096s latency).
Not shown: 986 closed ports
PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC 139/tcp open netbios-ssn Microsoft Windows netbios-ssn

554 /tcp open rtsp?
2869/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp open ms-wbt-server Microsoft Terminal Service | ssl-cert: Subject: commonName=Win7- 1-PC
| Not valid before: 20 18-03-05T06: 10:47
|_Not valid after: 20 18-09-04T06: 10:47
|_ssl-date: 20 18-04-26T05:5 1:38+00:00; 28s from scanner time.
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) |_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable

10243/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) |_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49 152/tcp open msrpc
49 153/tcp open msrpc
49 154/tcp open msrpc
49 156/tcp open msrpc
49 157/tcp open msrpc
49 160/tcp open msrpc Microsoft Windows RPC Microsoft Windows RPC Microsoft Windows RPC Microsoft Windows RPC Microsoft Windows RPC Microsoft Windows RPC MAC Address: 00:0C:29:20:C4:A9 (VMware) Device type: general purpose
Running: Microsoft Windows 7|2008|8. 1

OS CPE: cpe:/o:microsoft:windows_7::cpe:/o:microsoft:windows_7::sp 1 cpe:/o:microsoft:windows_server_2008::sp 1
cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8. 1

OS details: Microsoft Windows 7 SP0 - SP 1, Windows Server 2008 SP 1, Windows Server 2008 R2, Windows 8, or Windows 8. 1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN7- 1-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results: | OS: Windows 7 Professional 760 1 Service Pack 1 (Windows 7 Professional 6. 1) | OS CPE: cpe:/o:microsoft:windows_7::sp 1:professional
| Computer name: Win7- 1-PC
| NetBIOS computer name: WIN7- 1-PC₩x00
| Workgroup: WORKGROUP₩x00
|_ System time: 20 18-04-25T22:5 1:33-07:00
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
| 2.02:
|_ Message signing enabled but not required
| smb2-time:
| date: 20 18-04-26 0 1:5 1:33
|_ start_date: 20 18-03-29 05:57:42

|_clock-skew: mean: 28s, deviation: 0s, median: 28s
|_nbstat: NetBIOS name: WIN7- 1-PC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:20:c4:a9 (VMware)
| smb-os-discovery:
TRACEROUTE
HOP RTT ADDRESS

1 0.96 ms 10. 10.50.202 Running: Linux 3.X|4.X OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 OS details: Linux 3.2 4.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10. 10.50.2 10
Host is up (0.00065s latency).
Not shown: 998 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2. 1 (Ubuntu Linux; protocol 2.0) |
ssh-hostkey:
| 2048 3c:9c:fb:cb:58:35:f9:d7:d7:32:6f:ad:6a:f8:c7:9b (RSA)
| 256 70:e7:d9:a2:6a:54:92:e6:07:c9:89:58:b5:99:7d:0d (ECDSA)
|_ 256 b 1:be:a6:62:96:69:76:64:aa:23:bb:ad:54:cc:c0:db (EdDSA)
80/tcp open http Apache httpd 2.4. 18 ((Ubuntu))
|_http-server-header: Apache/2.4. 18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:EA:BD:DF (VMware)
Device type: general purpose

TRACEROUTE HOP RTT ADDRESS
1 0.65 ms 10. 10.50.2 10

Nmap scan report for 10. 10.50.2 1 1 Host is up (0.00037s latency).
Not shown: 999 filtered ports
PORT STATE SERVICE VERSION
3389/tcp open ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WIN2HMGPM3UAD7
| Not valid before: 20 18-03-28T 12:23: 16
|_Not valid after: 20 18-09-27T 12:23: 16
|_ssl-date: 20 18-04-26T05:5 1:4 1+00:00; 5s from scanner time.
MAC Address: 00:0C:29:BA:AC:AA (VMware)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose
Running (JUST GUESSING): FreeBSD 6.X (85%)
OS CPE: cpe:/o:FreeBSD:FreeBSD:6.2
Aggressive OS guesses: FreeBSD 6.2-RELEASE (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:Microsoft:windows

Host script results:
|_clock-skew: mean: 5s, deviation: 0s, median: 5s

TRACEROUTE Nmap scan report for 10. 10.50.200 Host is up (0.000042s latency).
All 1000 scanned ports on 10. 10.50.200 are closed

Too many fingerprints match this host to give specific OS details Network Distance: 0 hops

HOP RTT ADDRESS
1 0.37 ms 10. 10.50.2 1 1
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 256 IP addresses (9 hosts up) scanned in 384.48 seconds
//Importing Nmap XML file

msf > db_import Test
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v 1.8. 1' [*] Importing host 10. 10.50. 1
[*] Importing host 10. 10.50. 10
[*] Importing host 10. 10.50. 1 1
[*] Importing host 10. 10.50.20
[*] Importing host 10. 10.50. 100
[*] Importing host 10. 10.50.202
[*] Importing host 10. 10.50.2 10
[*] Importing host 10. 10.50.2 1 1
[*] Importing host 10. 10.50.200
[*] Successfully imported /root/Test

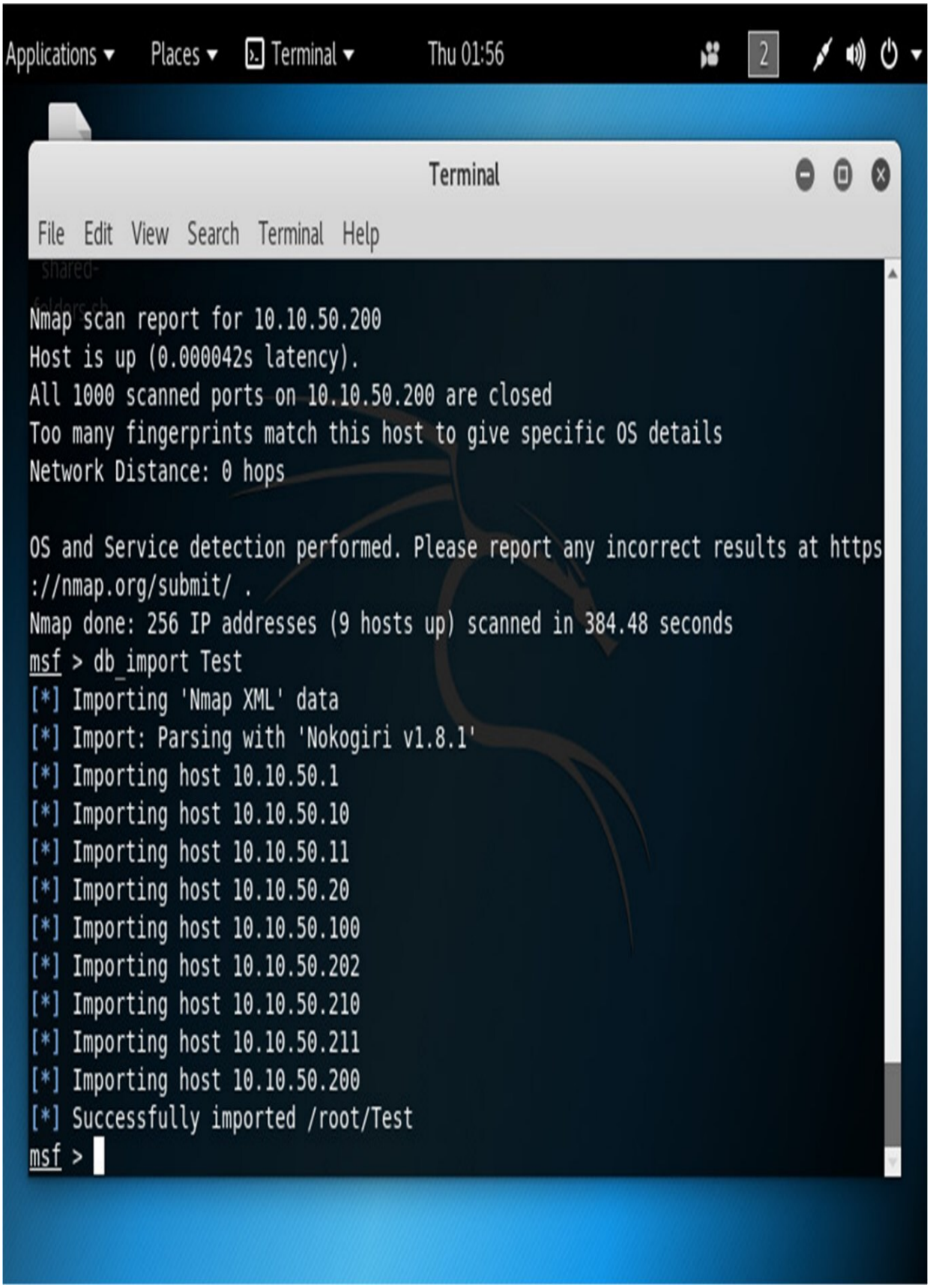


Figure 2. 80: Importing Results

Figure 2-80: Importing Results

msf > hosts
Hosts ═══

Address
info comments
———
——

10 . 10.50. 1
10. 10.50. 10
10. 10.50. 1 1
10. 10.50.20
10. 10.50. 100
10. 10.50.200
10. 10.50.202
10. 10.50.2 10
10. 10.50.2 1 1 mac name os_name os_flavor os_sp purpose

———————————— ———— ———

c 0:67:af:c7:d9:80 IOS 12.X device f8:72:ea:a4:a 1:cc ESXi 5.X device f8:72:ea:a4:a 1:2c ESXi 5.X device 00:0c:29:72:4a:c 1 Linux 3.X server 00:0c:29:95:04:33 Windows 7 client

Unknown device
00:0c:29:20:c4:a9 Windows 7 client
00:0c:29:ea:bd:df Linux 3.X server
00:0c:29:ba:ac:aa FreeBSD 6.X device

//Performing Services scan msf > db_nmap -sS -A 10. 10.50.2 1 1


Applications
Places
Terminal
Thu 02:02
Terminal
File Edit View Search Terminal Help
msf > db_nmap -sS -A 10.10.50.211
[*] Nmap: Starting Nmap 7.60 (https://nmap.org) at 2018-04-26 02:01 EDT
[*] Nmap: Nmap scan report for 10.10.50.211
[*] Nmap: Host is up (0.00032s latency).
[*] Nmap: Not shown: 999 filtered ports
[*] Nmap: PORT STATE SERVICE VERSION
[*] Nmap: 3389/tcp open ms-wbt-server Microsoft Terminal Services
[*] Nmap: | ssl-cert: Subject: commonName=WIN-2HMGPM3UAD7
[*] Nmap: | Not valid before: 2018-03-28T12:23:16
[*] Nmap: |_Not valid after: 2018-09-27T12:23:16
[*] Nmap: |_ssl-date: 2018-04-26T06:01:58+00:00; -4s from scanner time.
[*] Nmap: MAC Address: 00:0C:29:BA:AC:AA (VMware)
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
[*] Nmap: Device type: general purpose
[*] Nmap: Running (JUST GUESSING): FreeBSD 6.X (85%)
[*] Nmap: OS CPE: cpe:/o:freebsd:freebsd:6.2
[*] Nmap: Aggressive OS guesses: FreeBSD 6.2-RELEASE (85%)
[*] Nmap: No exact OS matches for host (test conditions non-ideal).
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Host script results:
[*] Nmap: |_clock-skew: mean: -4s, deviation: 0s, median: -4s
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT ADDRESS
[*] Nmap: 1 0.31 ms 10.10.50.211
[*] Nmap: OS and Service detection performed. Please report any incorrect results at ht

Figure 2-81: Service Scan

Observe the scan result showing different services, and the open and closed port information of live hosts.

msf > services

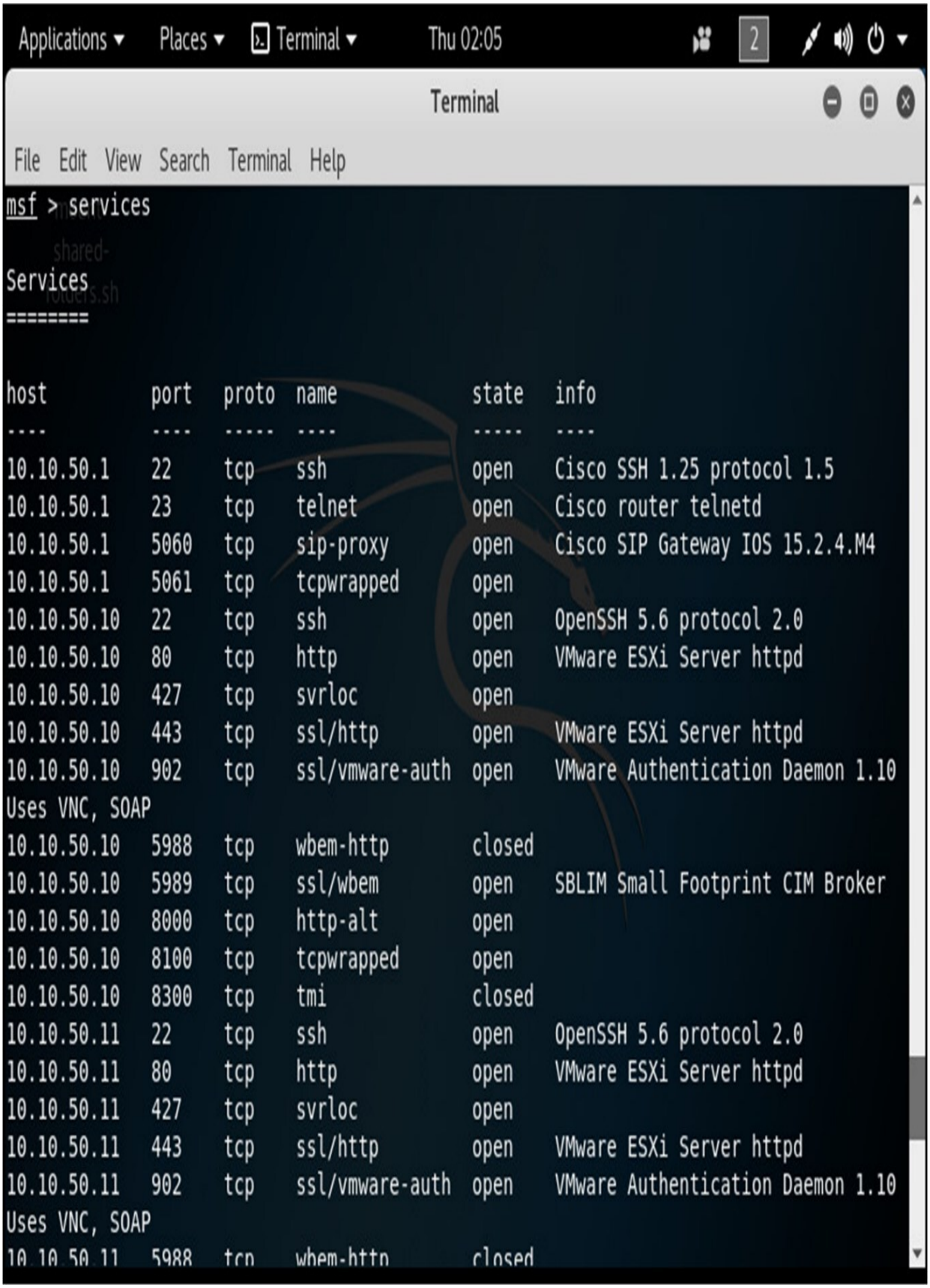

Applications
Places
Terminal
Thu 02:05
2
Terminal
File Edit View Search Terminal Help
msf > services
Services
========
host port proto name state info
---- ---- ----- ---- ----- ----
10.10.50.1 22 tcp ssh open Cisco SSH 1.25 protocol 1.5
10.10.50.1 23 tcp telnet open Cisco router telnetd
10.10.50.1 5060 tcp sip-proxy open Cisco SIP Gateway IOS 15.2.4.M4
10.10.50.1 5061 tcp tcpwrapped open
10.10.50.10 22 tcp ssh open OpenSSH 5.6 protocol 2.0
10.10.50.10 80 tcp http open VMware ESXi Server httpd
10.10.50.10 427 tcp svrloc open
10.10.50.10 443 tcp ssl/http open VMware ESXi Server httpd
10.10.50.10 902 tcp ssl/vmware-auth open VMware Authentication Daemon 1.10
Uses VNC, SOAP
10.10.50.10 5988 tcp wbem-http closed
10.10.50.10 5989 tcp ssl/wbem open SBLIM Small Footprint CIM Broker
10.10.50.10 8000 tcp http-alt open
10.10.50.10 8100 tcp tcpwrapped open
10.10.50.10 8300 tcp tmi closed
10.10.50.11 22 tcp ssh open OpenSSH 5.6 protocol 2.0
10.10.50.11 80 tcp http open VMware ESXi Server httpd
10.10.50.11 427 tcp svrloc open
10.10.50.11 443 tcp ssl/http open VMware ESXi Server httpd
10.10.50.11 902 tcp ssl/vmware-auth open VMware Authentication Daemon 1.10
Uses VNC, SOAP
10.10.50.11 5988 tcp wbem-http closed

Figure 2-82: Service Scan Results

msf > use scanner/smb/smb_version
msf auxiliary(scanner/smb/smb_version) > show options
Module options (auxiliary/scanner/smb/smb_version):

Name Current Setting Required Description
———————— ———— ————

RHOSTS
SMBDomain. SMBPass SMBUser THREADS 1 yes The target address range or CIDR identifier no The Windows domain to use for authentication

no The password for the specified username no The username to authenticate as yes The number of concurrent threads

msf auxiliary(scanner/smb/smb_version) > set RHOSTS 10. 10.50. 100-2 1 1 RHOSTS => 10. 10.50. 100-2 1 1
msf auxiliary(scanner/smb/smb_version) > set THREADS 100
THREADS => 100
msf auxiliary(scanner/smb/smb_version) > show options
Module options (auxiliary/scanner/smb/smb_version):

Name Current Setting Required Description
———————— ———— ————

RHOSTS 10. 10.50. 100-2 1 1 yes The target address range or CIDR identifier
SMBDomain.
SMBPass
SMBUser
THREADS 100
no The Windows domain to use for authentication

no The password for the specified username no The username to authenticate as yes The number of concurrent threads

Figure 2: 83: SMB Scan Results

Figure 2-83: SMB Scan Results

```
msf auxiliary(scanner/smb/smb_version) > run
```


Terminal
File Edit View Search Terminal Help
msf auxiliary(scanner/smb/smb_version) > run
[+] 10.10.50.100:445 - Host is running Windows 7 Professional SP1 (build:7601) (name:WIN7-PC) (workgroup:WORKGROUP)
[+] 10.10.50.202:445 - Host is running Windows 7 Professional SP1 (build:7601) (name:WIN7-1-PC) (workgroup:WORKGROUP)
[*] Scanned 24 of 112 hosts (21% complete)
[*] Scanned 28 of 112 hosts (25% complete)
[*] Scanned 76 of 112 hosts (67% complete)
[*] Scanned 79 of 112 hosts (70% complete)
[*] Scanned 81 of 112 hosts (72% complete)
[*] Scanned 103 of 112 hosts (91% complete)
[*] Scanned 110 of 112 hosts (98% complete)
[*] Scanned 111 of 112 hosts (99% complete)
[*] Scanned 112 of 112 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_version) >

Figure 2-84: Running SMB Scan

msf auxiliary(scanner/smb/smb_version) > hosts

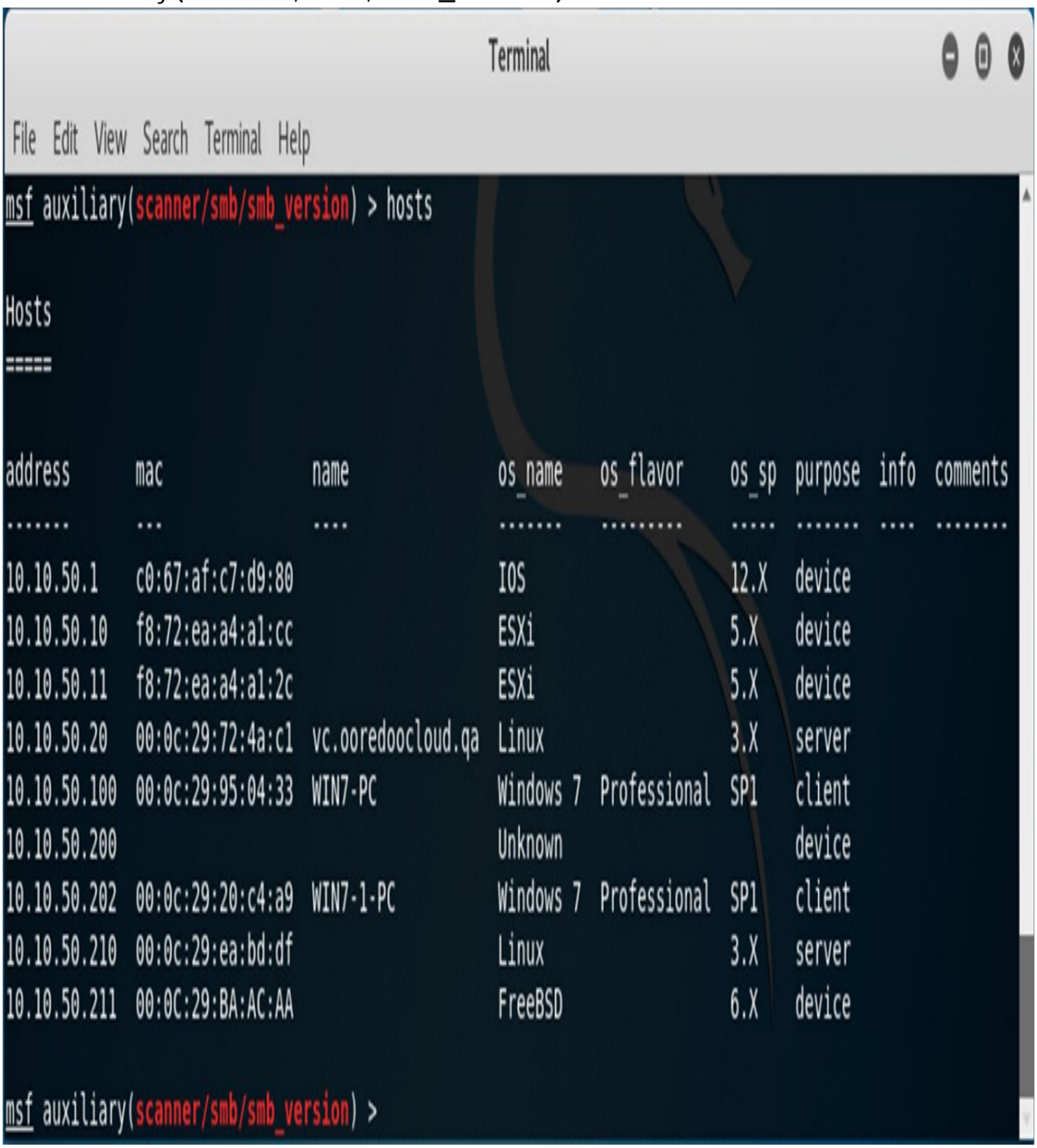


Figure 2-85: SMB Scan results

Observe the OS_Flavor field. SMB scanning scans for Operating System Flavor for the RHOST range configured.

Practice Questions:

1. What are the basic ways to perform Footprinting? A. Active & Passive Footprinting
B. Pseudonymous & Passive Footprinting C. Social & Internet Footprinting
D. Active & Social Footprinting

2. Which one of the following is the best meaning of Footprinting? A. Collection of information about a target
B. Monitoring target
C. Tracing a target
D. Scanning a target

3. What is the purpose of Social Engineering?
A. Reveal information from human beings
B. Extract information from compromised social networking sites C. Reveal information about social networking sites D. Compromising social accounts

4. Which feature is used to make a search more appropriate? A. Keywords
B. Operators
C. Google hacking database
D. Cache

5. Wayback Machine is used for: A. Backup a Website
B. Scan a Website
C. Archive a Website
D. Manage a Website

6. EDGAR, CNBC & LexisNexis are used for: A. Gathering financial information B. Gathering general information C. Gathering personal information D. Gathering network information

7. Which record type will reveal the information about Host IP address?
A. A
B. MX
C. NS
D. SRV