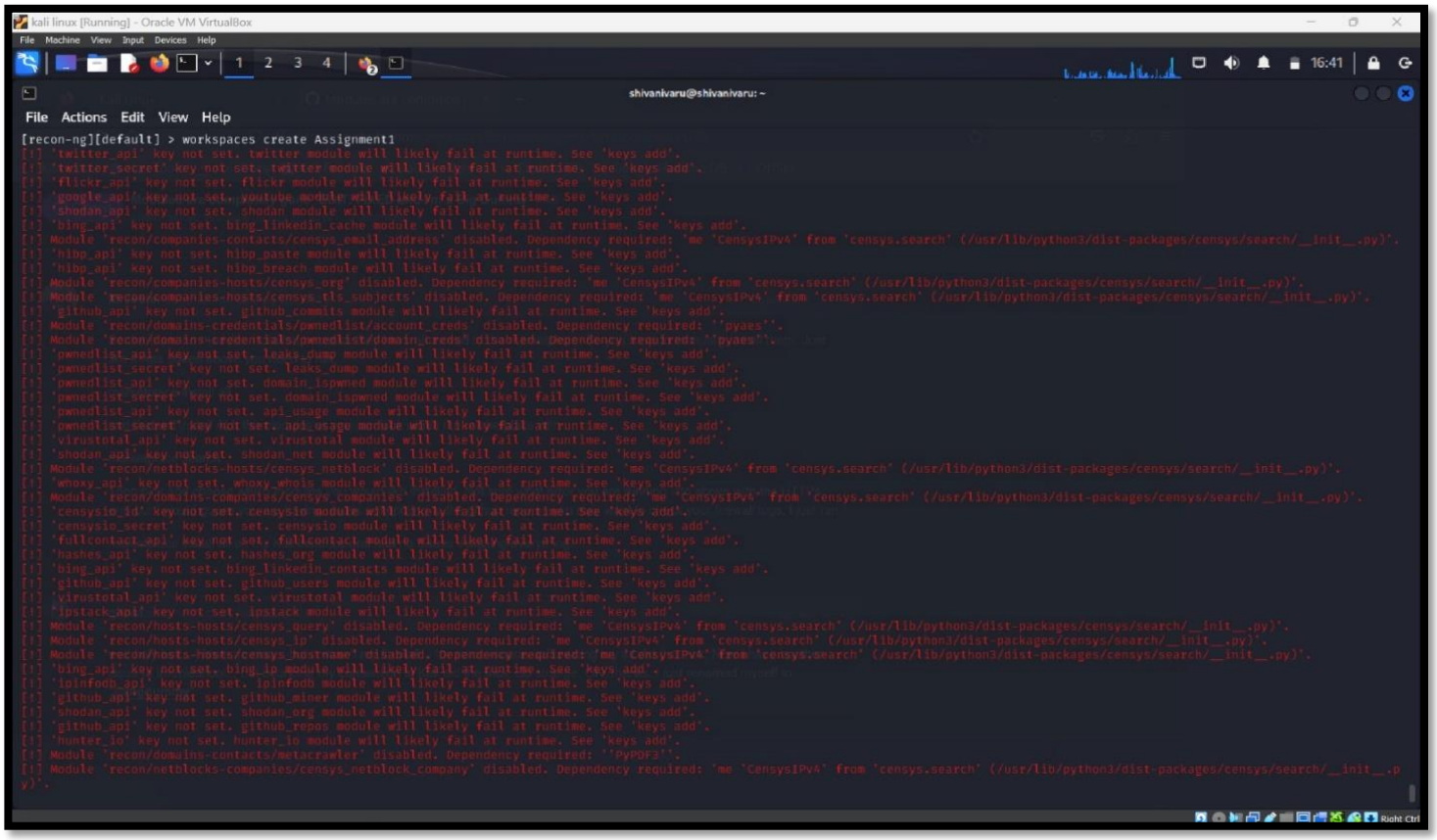
Subject: Security Testing

SENG 8061

ASSIGNMENT - 1

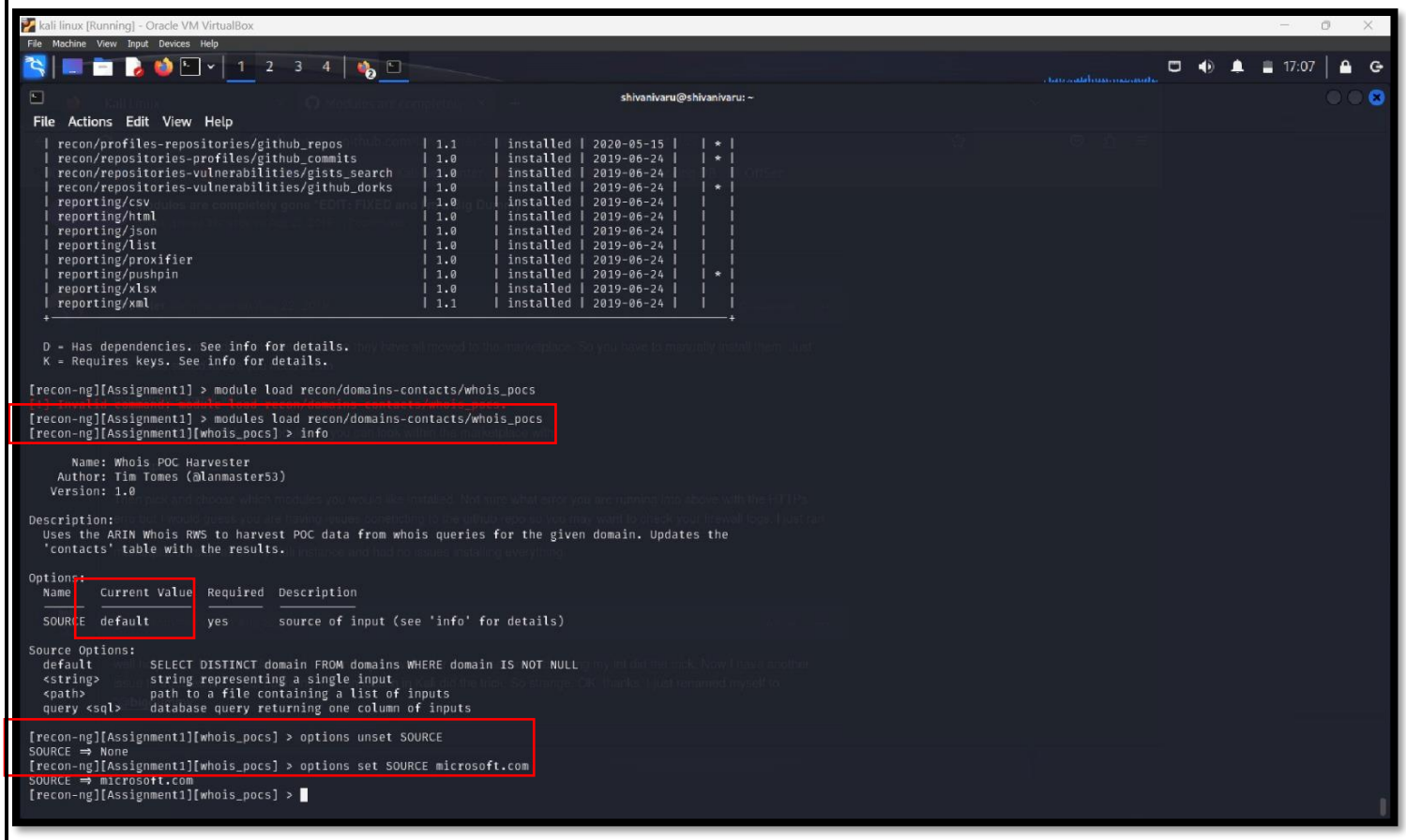
Name	Student ID
Shivani Varu	8941914
Mohammed Rafique	8954785

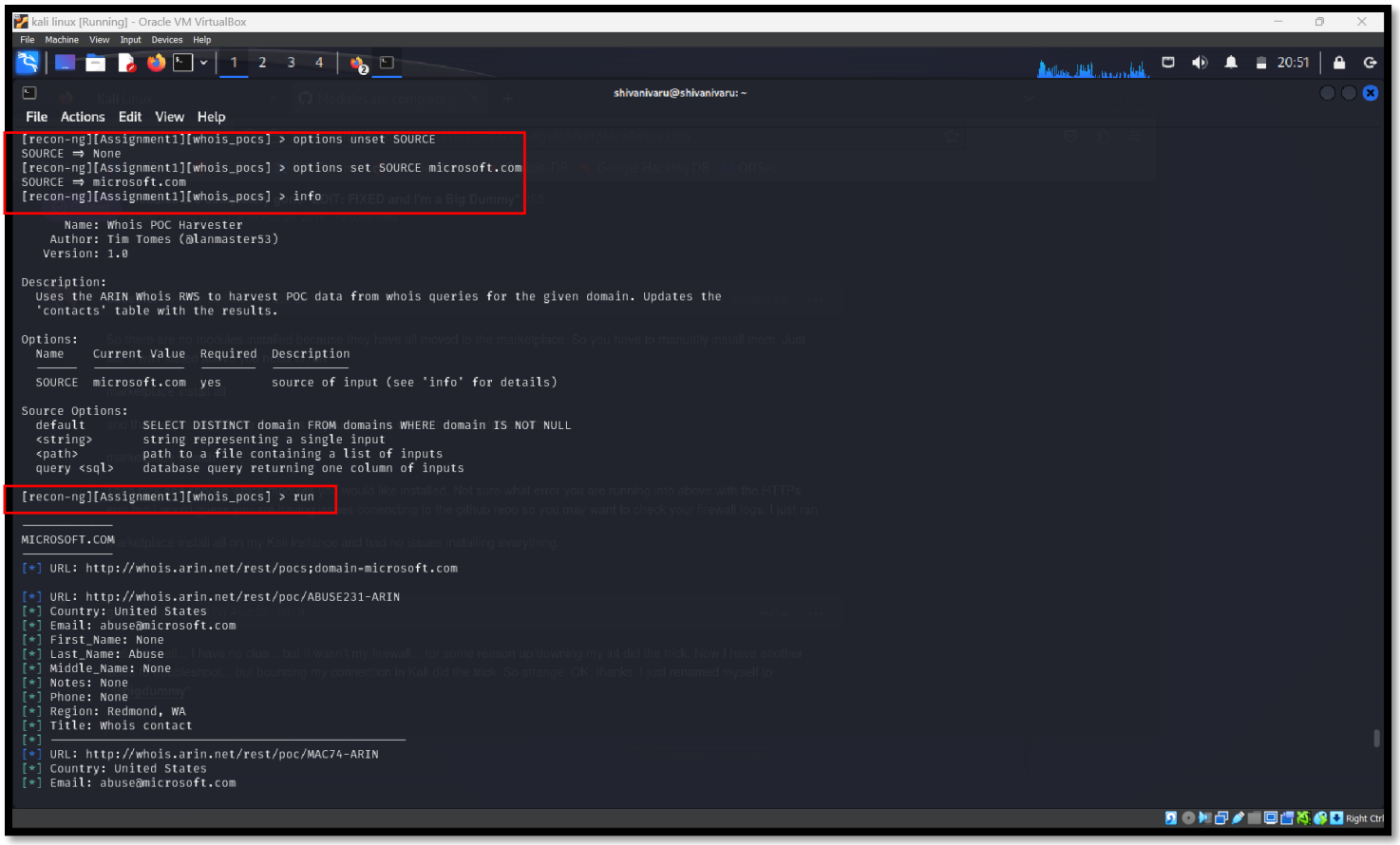
Tools Used	**Recon-ng**
Target Website	**Microsoft.com**
Command Used	**Workspaces create Assignment1**

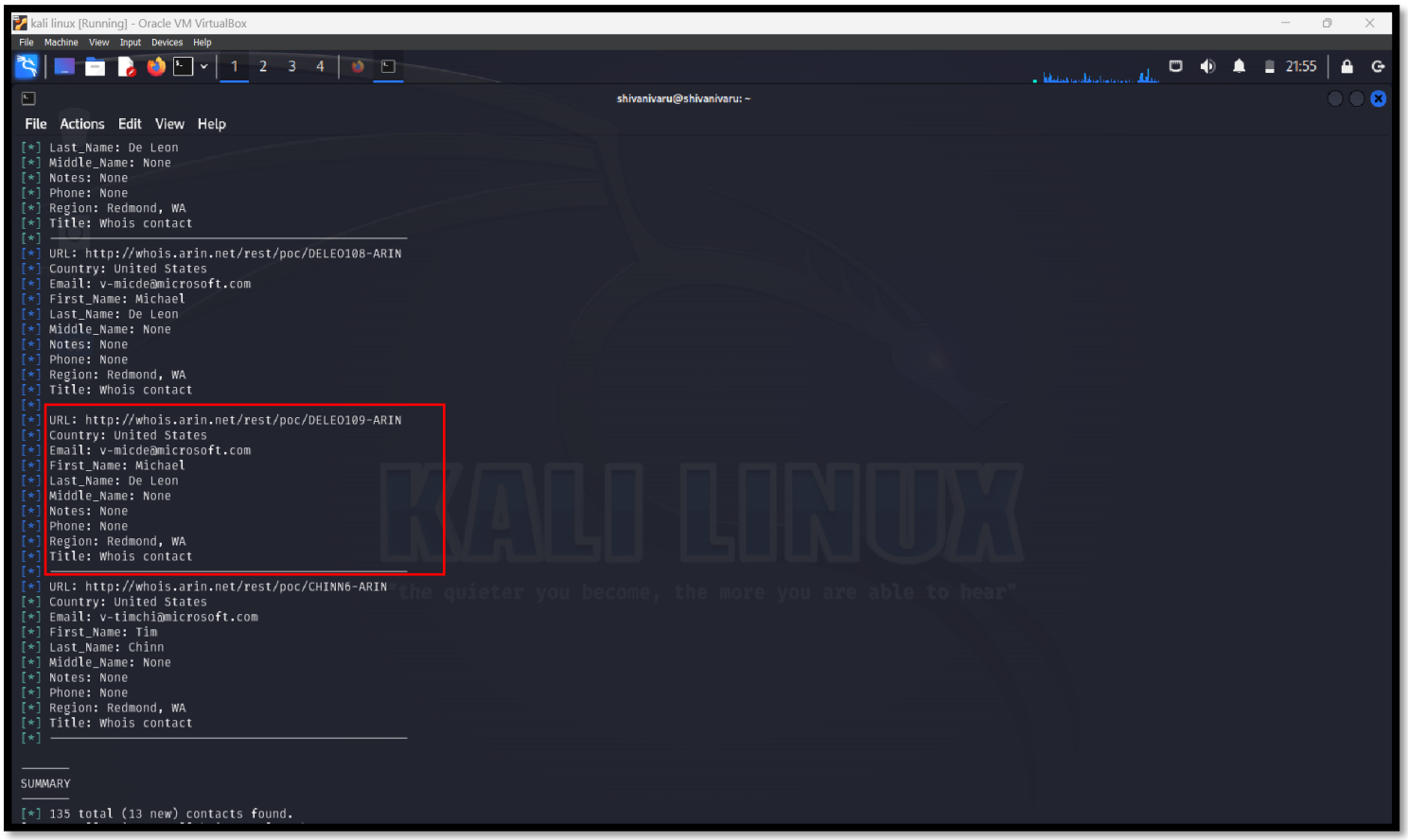


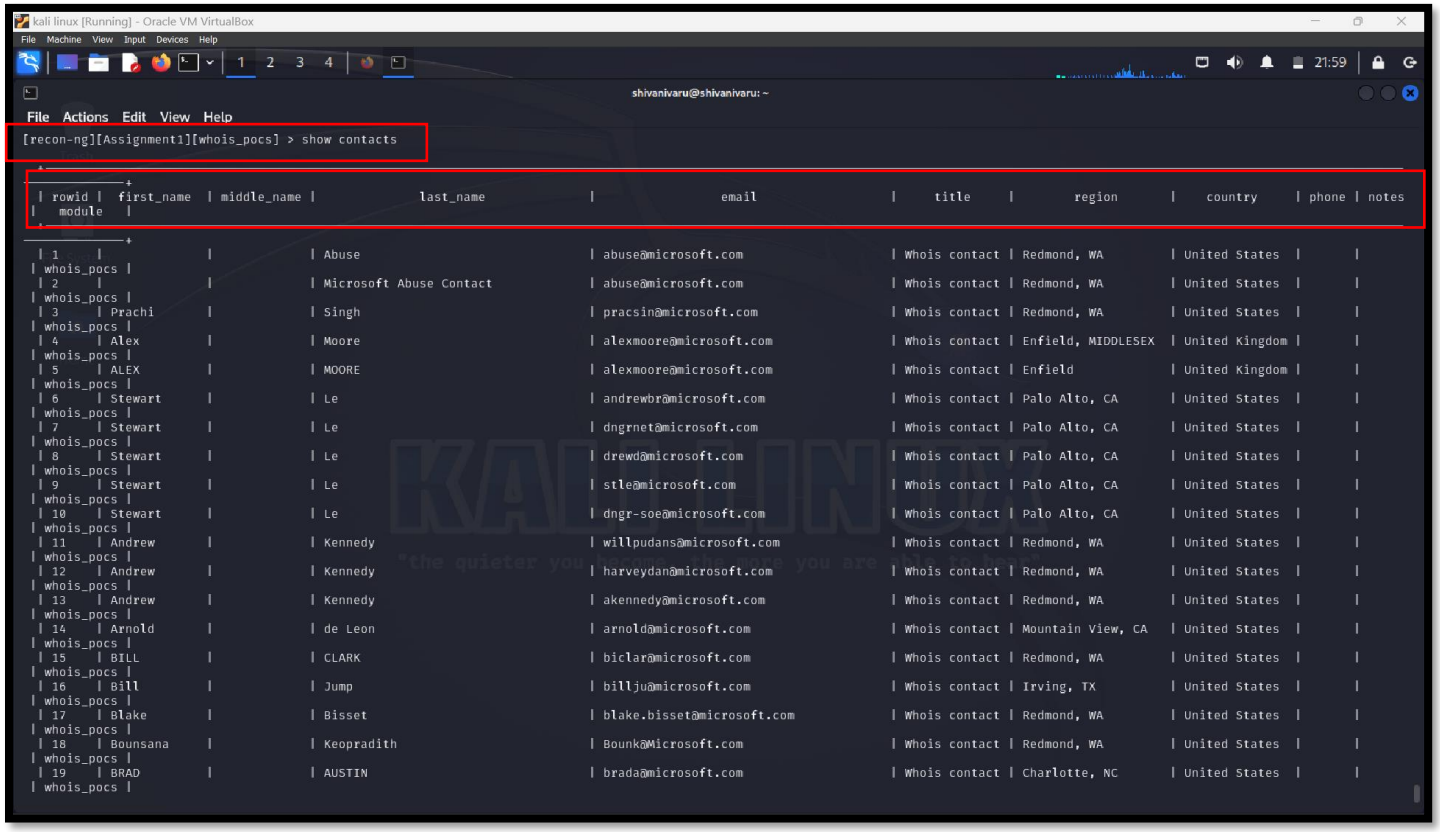
Modules Used	**modules load recon/domains-contacts/whois_pocs**
Command Used	**Show Contacts**

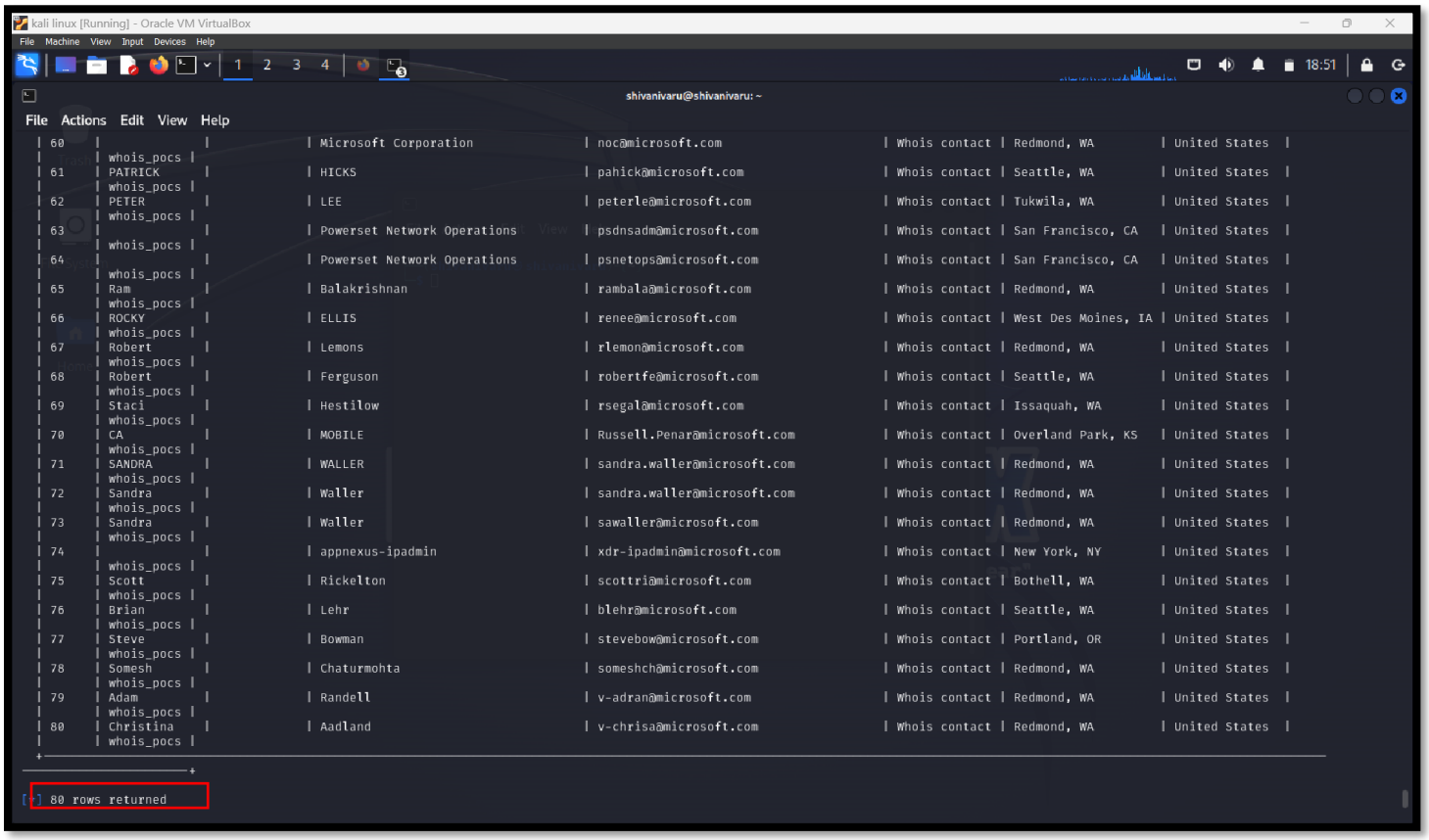
- The "modules load/recon/domains-contacts/whois_pocs" command in Recon-ng is used to load the "whois_pocs" module from the "domains-contacts" category.
- This module is designed to gather and display the Point of Contacts (POCs) obtained from Whois records for a given domain.
- Recon-ng, being a modular framework, allows users to load specific modules for different purposes, such as information gathering, and the "whois_pocs" module is one of the many modules available in Recon-ng for this purpose.
- The tool provides a variety of modules, including geoip lookup, banner grabbing, DNS lookup, and port scanning, making it a powerful asset for reconnaissance and open source intelligence gathering




kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
shivanivaru@shivanivaru: ~
File Actions Edit View Help
[recon-ng][Assignment1][whois_pocs] > options unset SOURCE
SOURCE => None
[recon-ng][Assignment1][whois_pocs] > options set SOURCE microsoft.com
SOURCE => microsoft.com
[recon-ng][Assignment1][whois_pocs] > info
Name: Whois POC Harvester
Author: Tim Tomes (@lanmaster53)
Version: 1.0
Description:
Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the 'contacts' table with the results.
Options:
Name Current Value Required Description
SOURCE microsoft.com yes source of input (see 'info' for details)
Source Options:
default SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
<string> string representing a single input
<path> path to a file containing a list of inputs
query <sql> database query returning one column of inputs
[recon-ng][Assignment1][whois_pocs] > run
MICROSOFT.COM
[*] URL: http://whois.arin.net/rest/pocs;domain=microsoft.com
[*] URL: http://whois.arin.net/rest/poc/ABUSE231-ARIN
[*] Country: United States
[*] Email: abuse@microsoft.com
[*] First_Name: None
[*] Last_Name: Abuse
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Redmond, WA
[*] Title: Whois contact
[*] URL: http://whois.arin.net/rest/poc/MAC74-ARIN
[*] Country: United States
[*] Email: abuse@microsoft.com

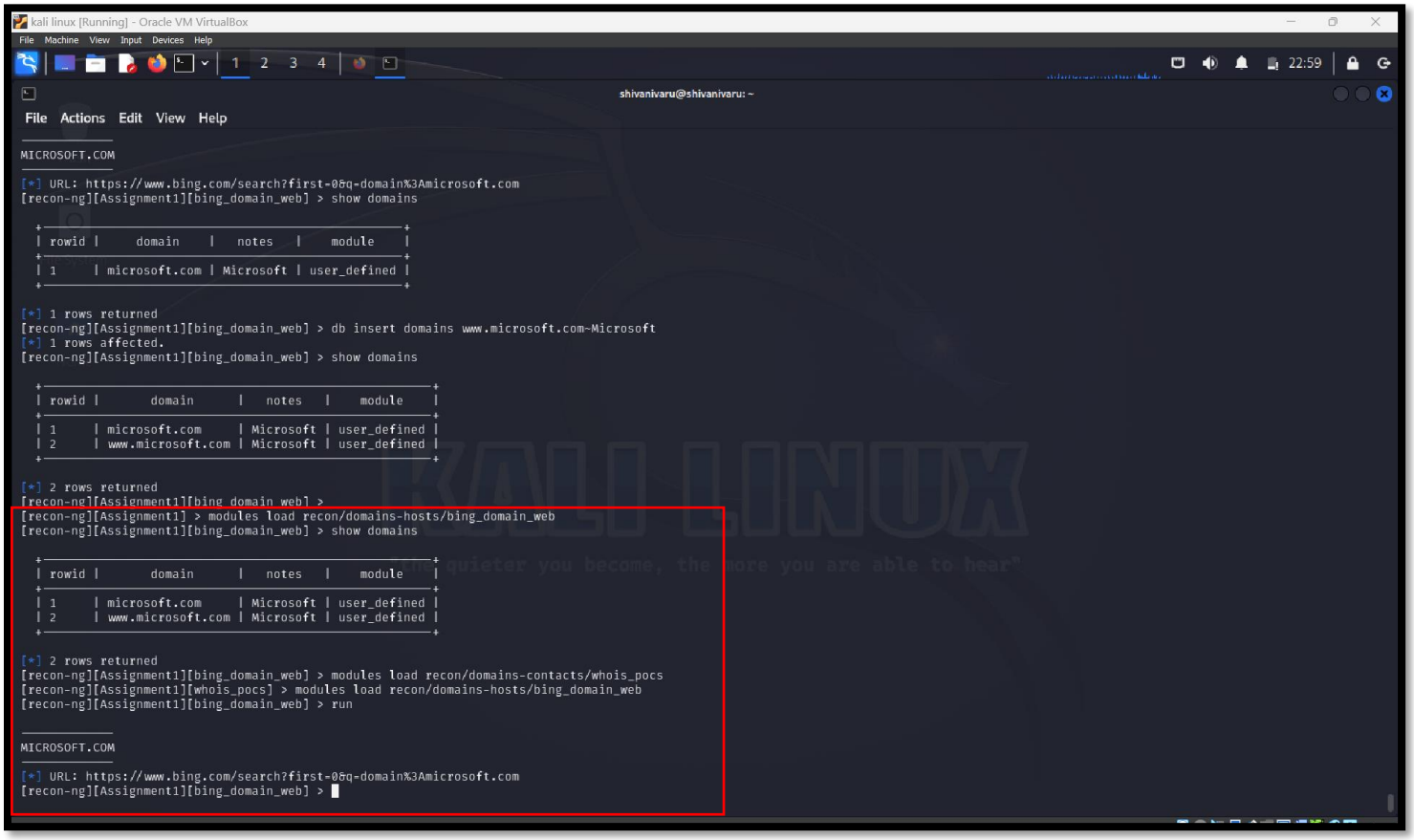

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
shivanivaru@shivanivaru: ~
File Actions Edit View Help
[*] Last_Name: De Leon
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Redmond, WA
[*] Title: Whois contact
[*] URL: http://whois.arin.net/rest/poc/DELEO108-ARIN
[*] Country: United States
[*] Email: v-micde@microsoft.com
[*] First_Name: Michael
[*] Last_Name: De Leon
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Redmond, WA
[*] Title: Whois contact
[*] URL: http://whois.arin.net/rest/poc/DELEO109-ARIN
[*] Country: United States
[*] Email: v-micde@microsoft.com
[*] First_Name: Michael
[*] Last_Name: De Leon
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Redmond, WA
[*] Title: Whois contact
[*] URL: http://whois.arin.net/rest/poc/CHINN6-ARIN
[*] Country: United States
[*] Email: v-timchi@microsoft.com
[*] First_Name: Tim
[*] Last_Name: Chinn
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Redmond, WA
[*] Title: Whois contact
SUMMARY
[*] 135 total (13 new) contacts found.



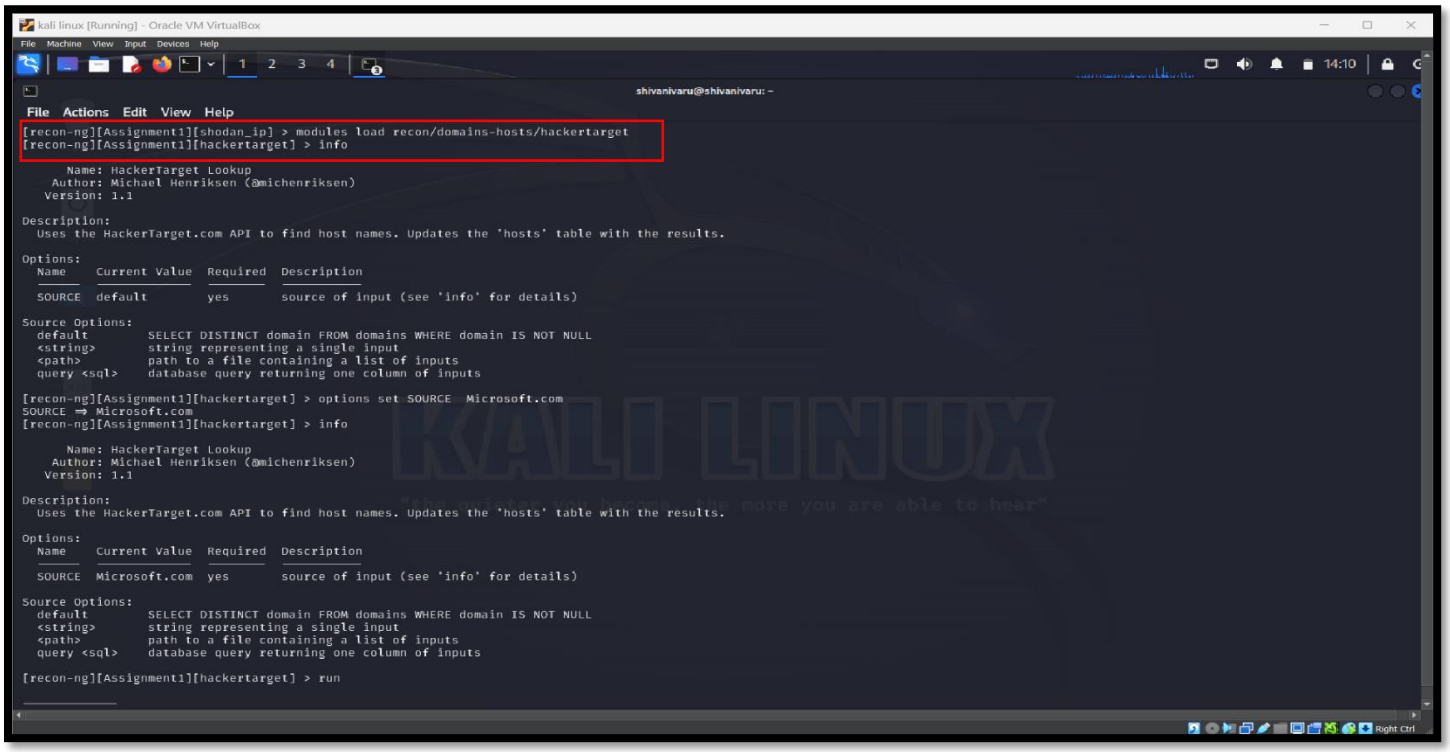


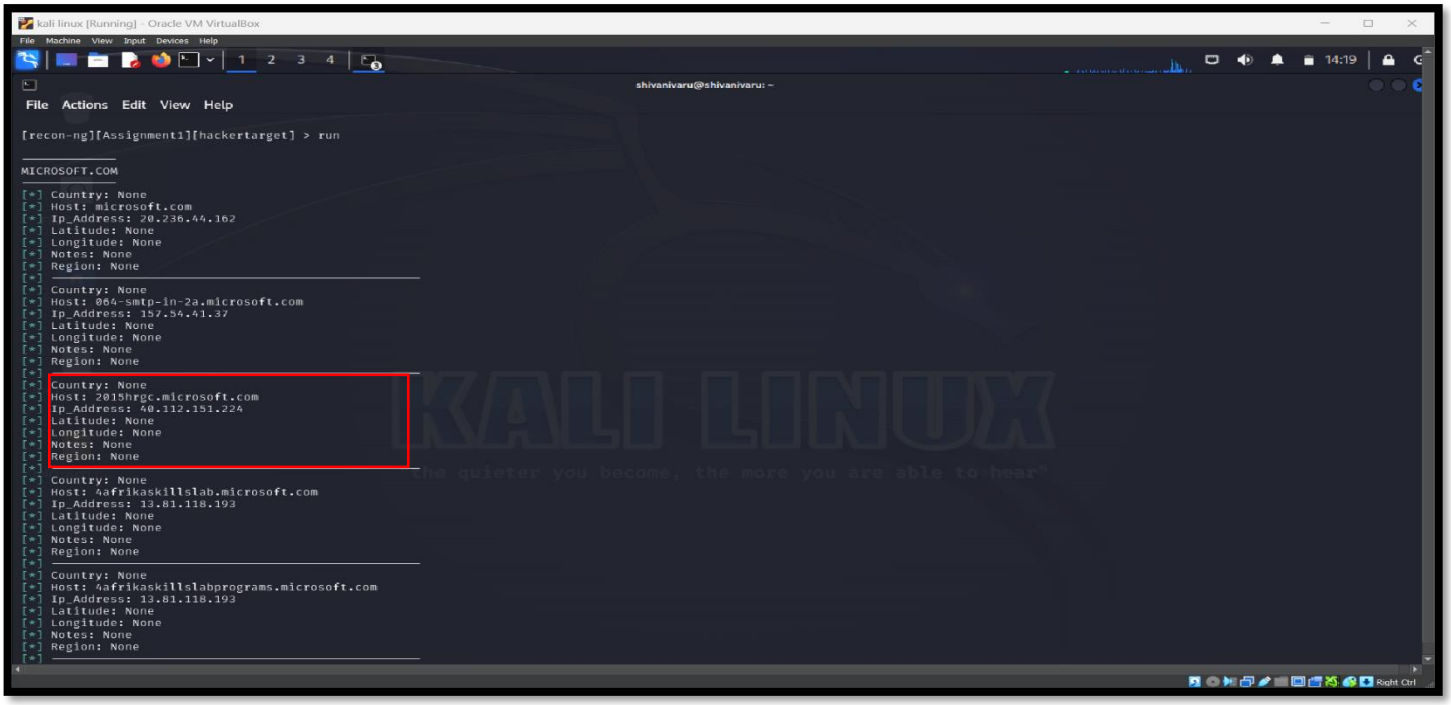
Here, we got information about company's URL, where the servers are located email address of employees of company, employee's first name,last name,server's region etc

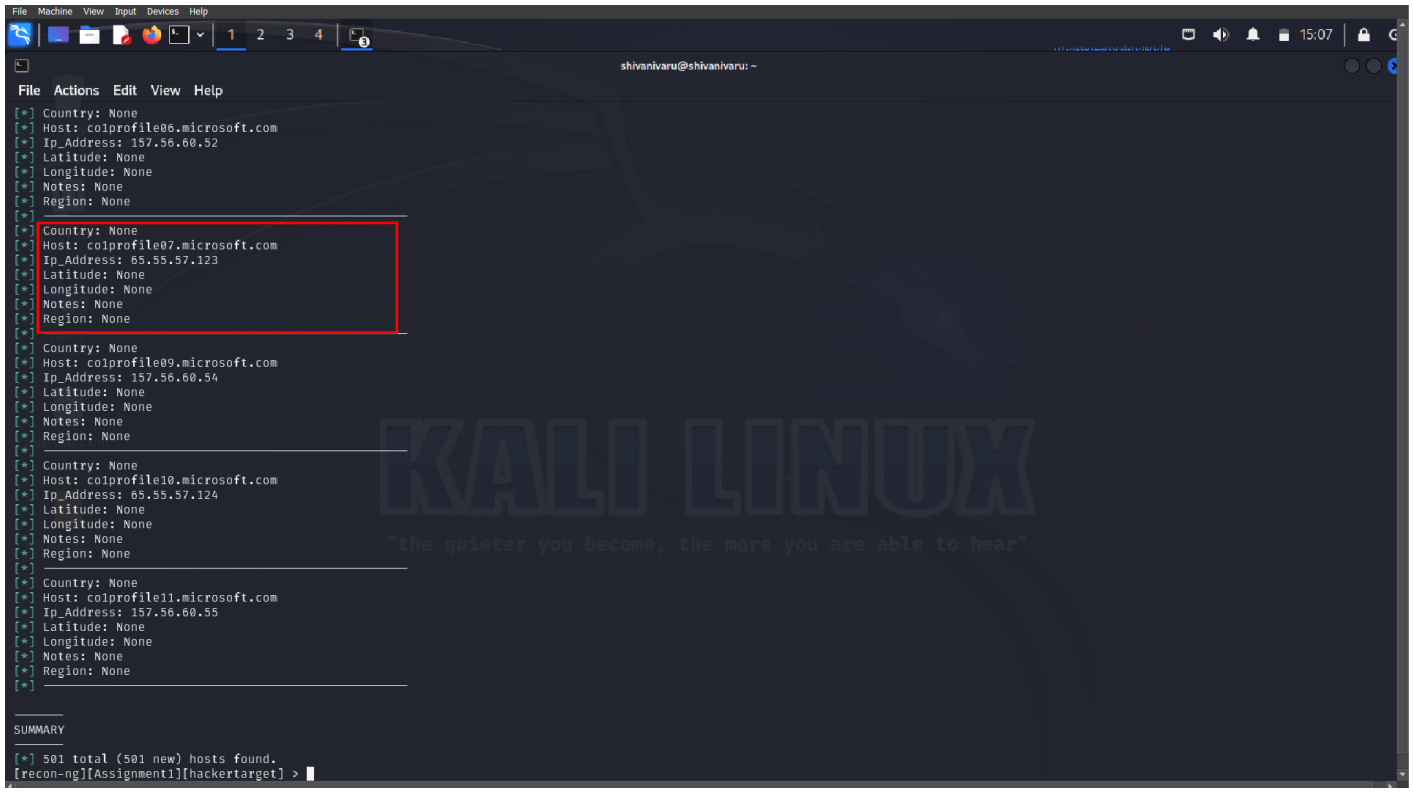
Modules Used	**modules load recon/domains-hosts/bing_domain_web**
Command Used	**Show Domains**



Modules Used	**modules load recon/domains-hosts/hackertarget**
Command Used	**Info** **Options set SOURCE Microsoft.com** **Run**

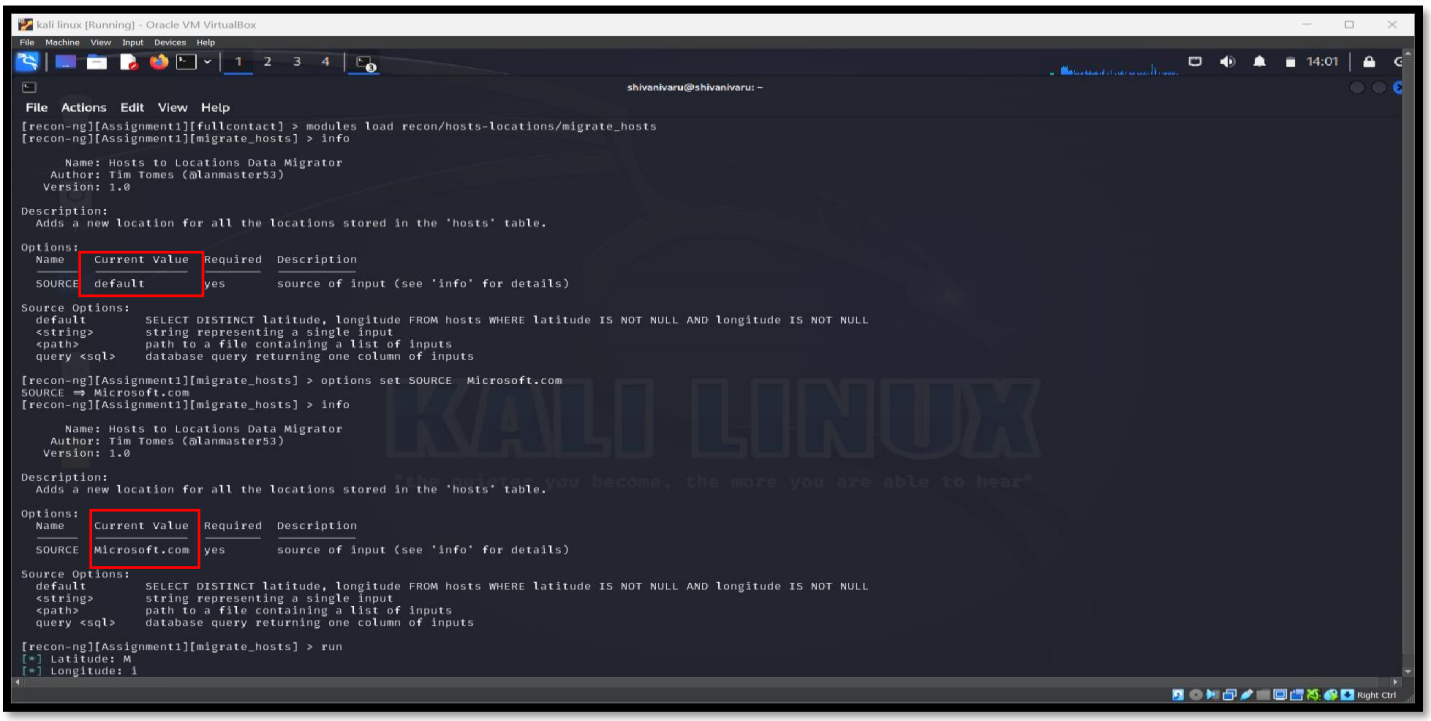


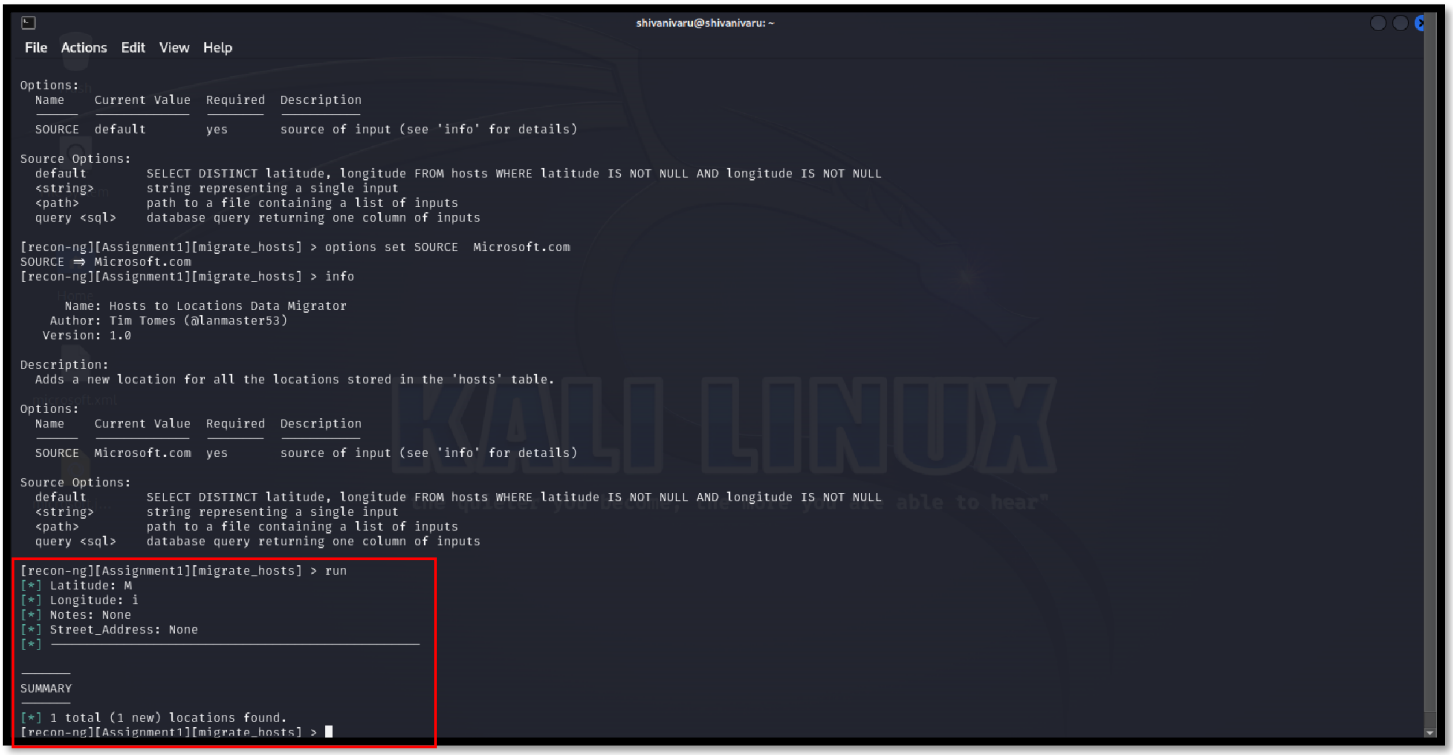




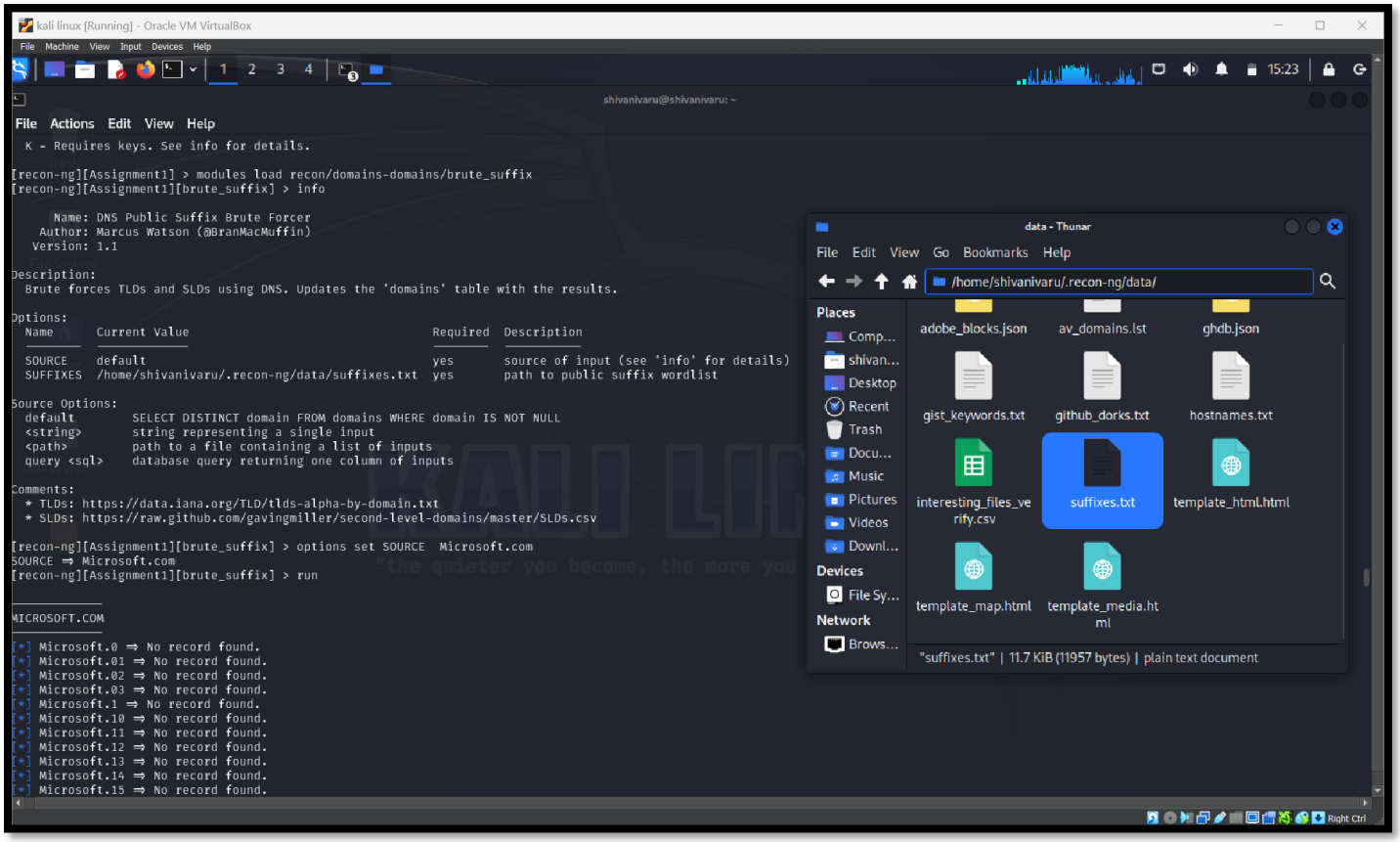
Here, we obtained 501 total hosts after running the "hackertarget" module with the source set to "Microsoft.com," it indicates that the module has successfully gathered information on 501 hosts related to Microsoft.com. Along with hostname, we retrieved different IP Address as well.

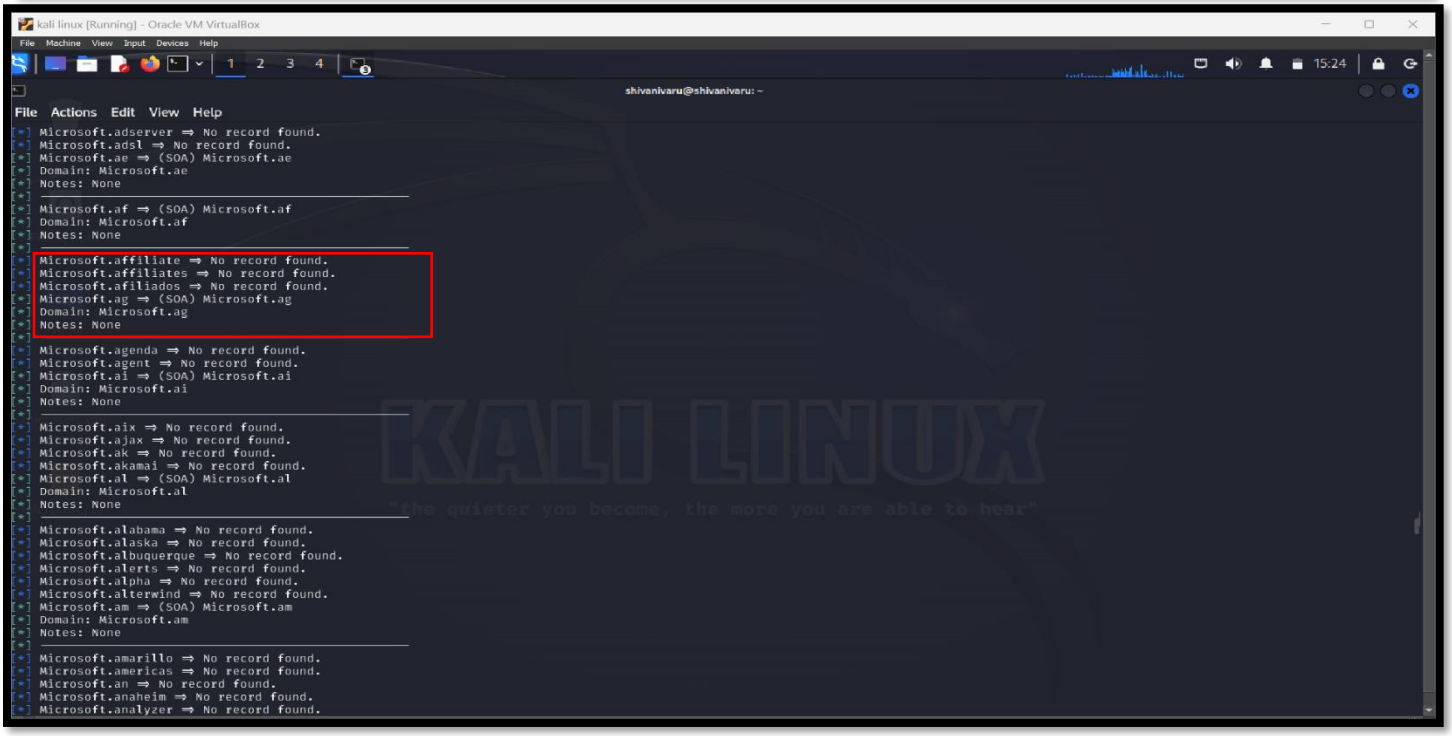
Modules Used	**modules load recon/hosts-locations/migrate_hosts**
Command Used	**Info** **Run** **Options set SOURCE Microsoft.com**

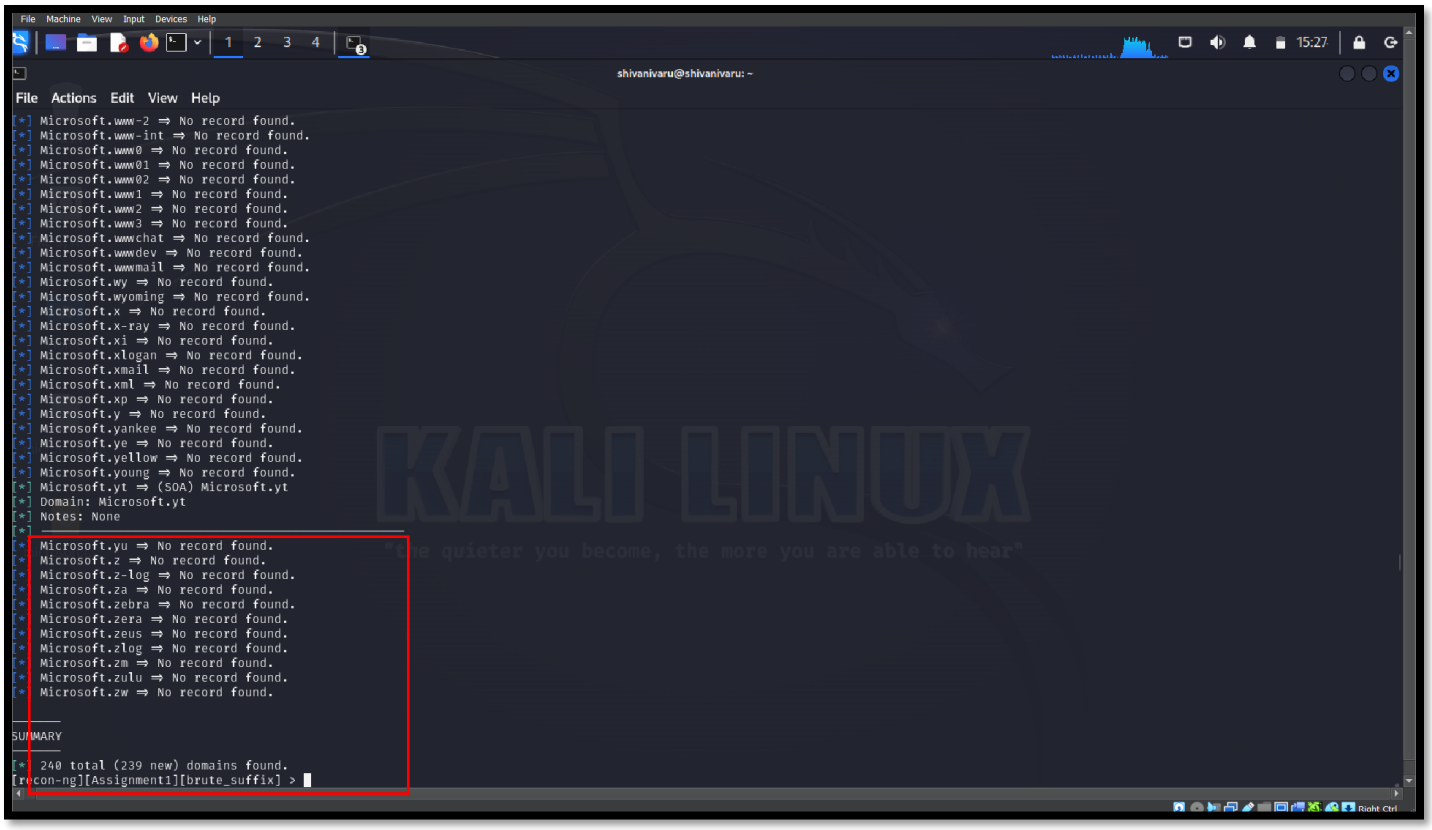




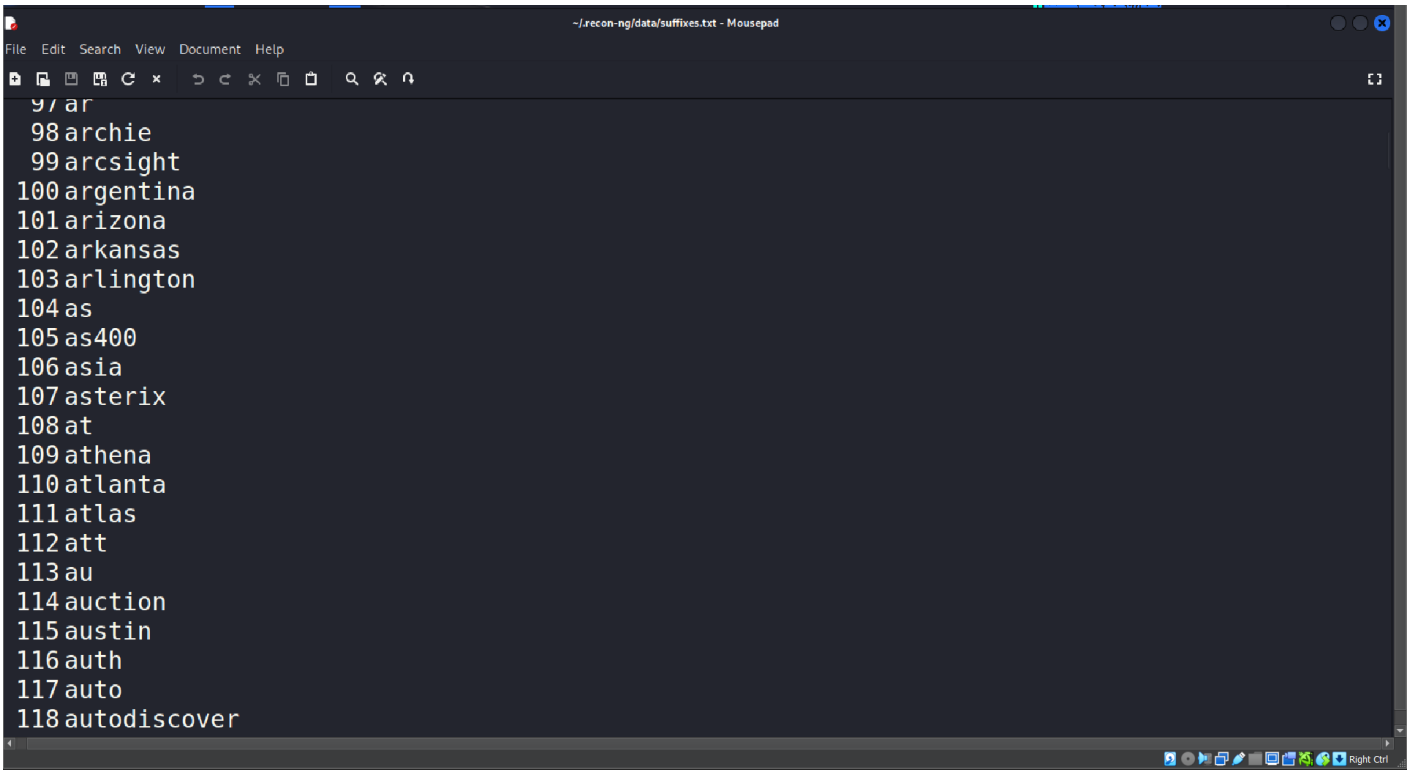
Modules Used	**modules load recon/domans-domains/brute_suffix**
Command Used	➢ **Info** ➢ **Options set SOURCE Microsoft.com** ➢ **Run**





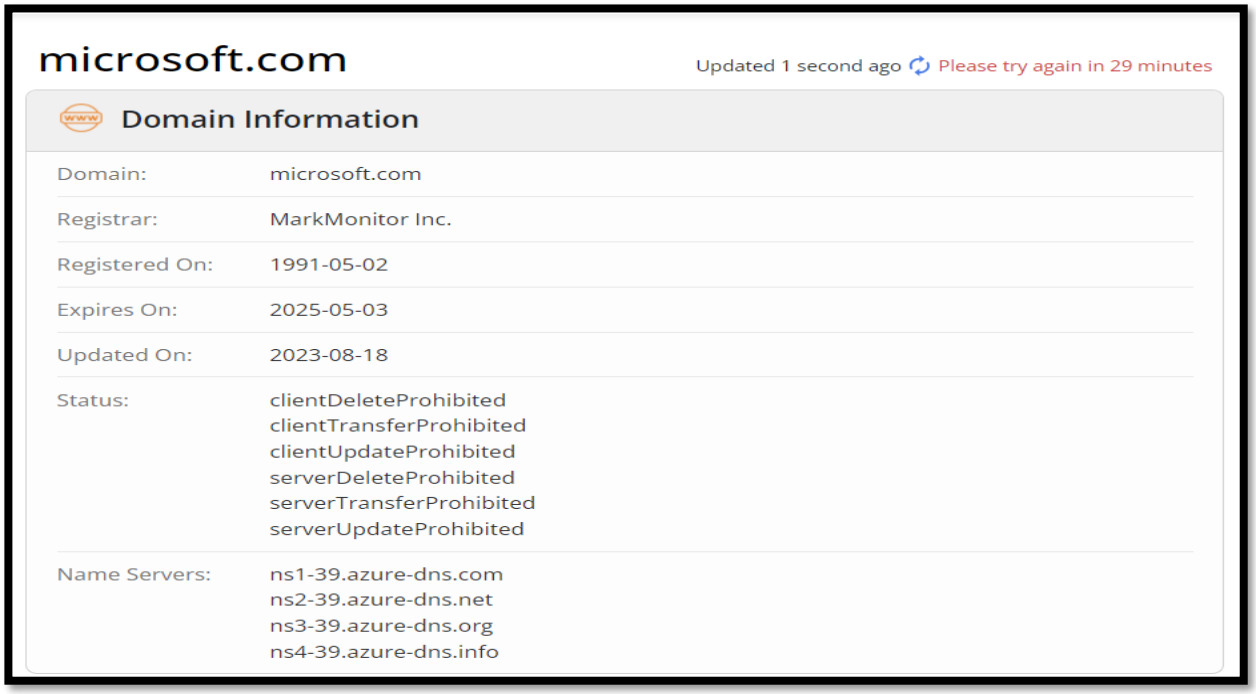


Suffixes.txt file generate.



Tools Used	**Whois**
Target Website	**Microsoft.com**

Utilized WHOIS databases to extract information about Microsoft's domain registration, including the registrant contact, administrative contact, technical contact, registration date, and contact details.

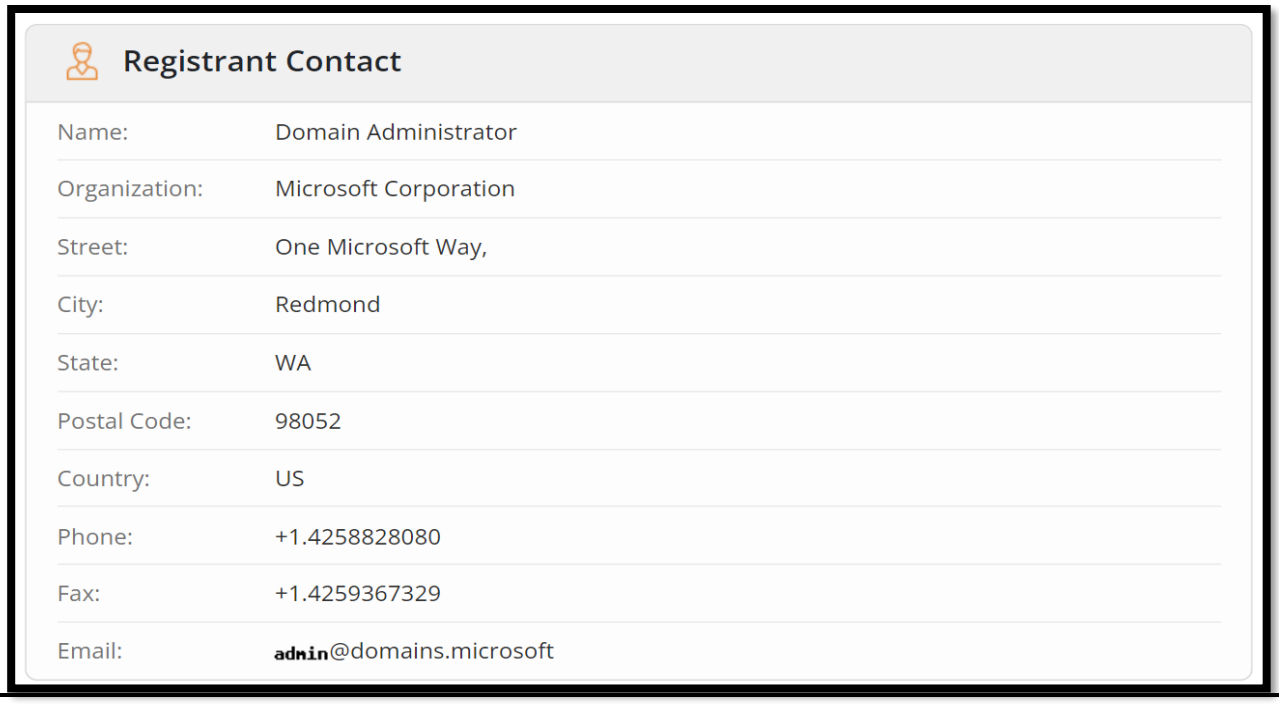


microsoft.com

Updated 1 second ago Please try again in 29 minutes

Domain Information

Domain:	microsoft.com
Registrar:	MarkMonitor Inc.
Registered On:	1991-05-02
Expires On:	2025-05-03
Updated On:	2023-08-18
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	ns1-39.azure-dns.com ns2-39.azure-dns.net ns3-39.azure-dns.org ns4-39.azure-dns.info



Registrant Contact

Name:	Domain Administrator
Organization:	Microsoft Corporation
Street:	One Microsoft Way,
City:	Redmond
State:	WA
Postal Code:	98052
Country:	US
Phone:	+1.4258828080
Fax:	+1.4259367329
Email:	admin@domains.microsoft

Technical Contact

Name:	MSN Hostmaster
Organization:	Microsoft Corporation
Street:	One Microsoft Way,
City:	Redmond
State:	WA
Postal Code:	98052
Country:	US
Phone:	+1.4258828080
Fax:	+1.4259367329
Email:	msnhst@microsoft.com

Administrative Contact

Name:	Domain Administrator
Organization:	Microsoft Corporation
Street:	One Microsoft Way,
City:	Redmond
State:	WA
Postal Code:	98052
Country:	US
Phone:	+1.4258828080
Fax:	+1.4259367329
Email:	admin@domains.microsoft

Raw Whois Data

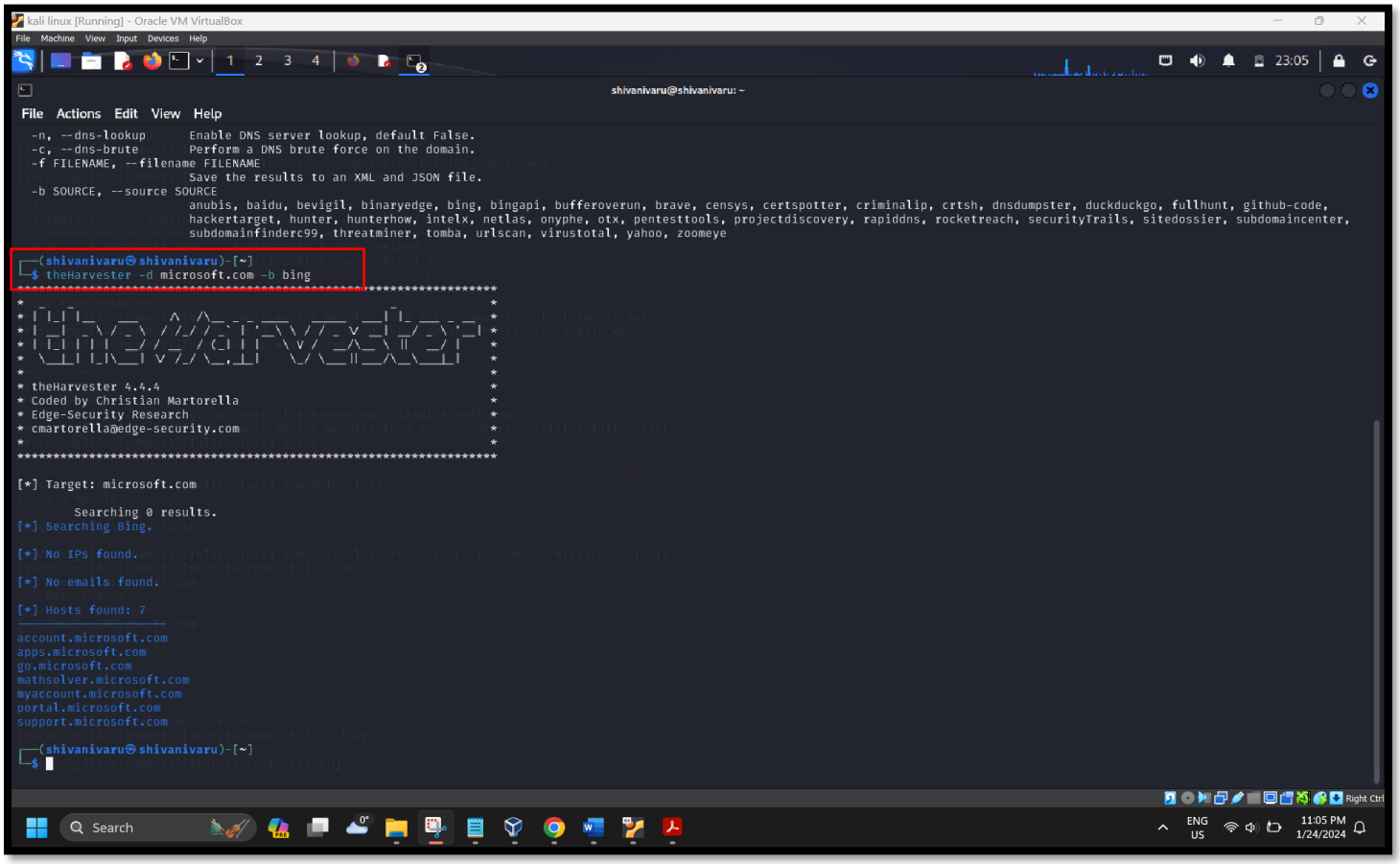
```
Domain Name: microsoft.com
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2023-08-18T16:15:54+0000
Creation Date: 1991-05-02T04:00:00+0000
Registrar Registration Expiration Date: 2025-05-03T00:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Microsoft Corporation
Registrant Street: One Microsoft Way,
Registrant City: Redmond
Registrant State/Province: WA
Registrant Postal Code: 98052
Registrant Country: US
Registrant Phone: +1.4258828080
Registrant Phone Ext:
Registrant Fax: +1.4259367329
Registrant Fax Ext:
Registrant Email: admin@domains.microsoft
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Microsoft Corporation
Admin Street: One Microsoft Way,
Admin City: Redmond
Admin State/Province: WA
Admin Postal Code: 98052
Admin Country: US
Admin Phone: +1.4258828080
Admin Phone Ext:
Admin Fax: +1.4259367329
Admin Fax Ext:
Admin Email: admin@domains.microsoft
Registry Tech ID:
Tech Name: MSN Hostmaster
Tech Organization: Microsoft Corporation
Tech Street: One Microsoft Way,
Tech City: Redmond
Tech State/Province: WA
Tech Postal Code: 98052
```

Company Contact Details

- We are looking for the organization's domain information, administration, registrant, and technical contact information.
- We have identified the contact information by using "Whois." The Internet Assigned Number Authority (IANA) is responsible for managing the root zone in the Domain Name System (DNS), media types, autonomous system numbers, and other symbols and Internet numbers linked to Internet Protocol.
- All the passive information we've acquired will assist us in obtaining the organization's employee information. We can access all systems connected to the same domain by using the organization's registrar domain and IANA number.
- We have registrar servers that connect URLs with webserver IP addresses.

Tools Used	**Harvester**
Target Website	**Microsoft.com**
Command Used	**theHarvester -d microsoft.com -b bing**

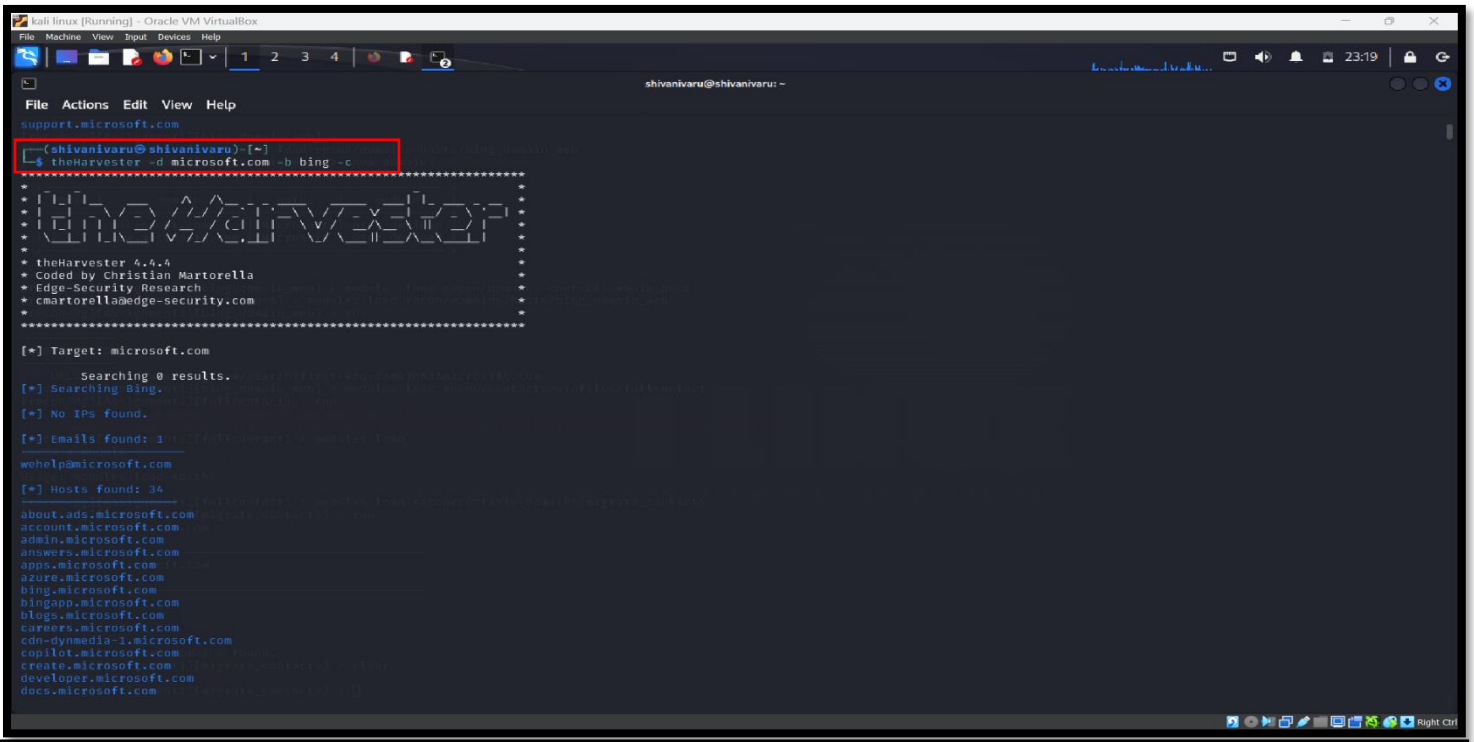
- The command "theHarvester -d microsoft.com -b bing" is used to extract information about the domain "microsoft.com" from the Bing search engine using theHarvester tool.
- theHarvester is an open-source tool for gathering email accounts, subdomain names, virtual hosts, open ports, banners, and employee names from various public sources. **(MaxiSoler, 2012)**
- It supports multiple public sources, including Bing, Google, Censys, and others.
- The tool is commonly used for open-source intelligence (OSINT) gathering to help determine an organization's external threat posture. **(Nmmapper.com)**
- It can be an asset for penetration testers and system administrators in the early stages of a security assessment.

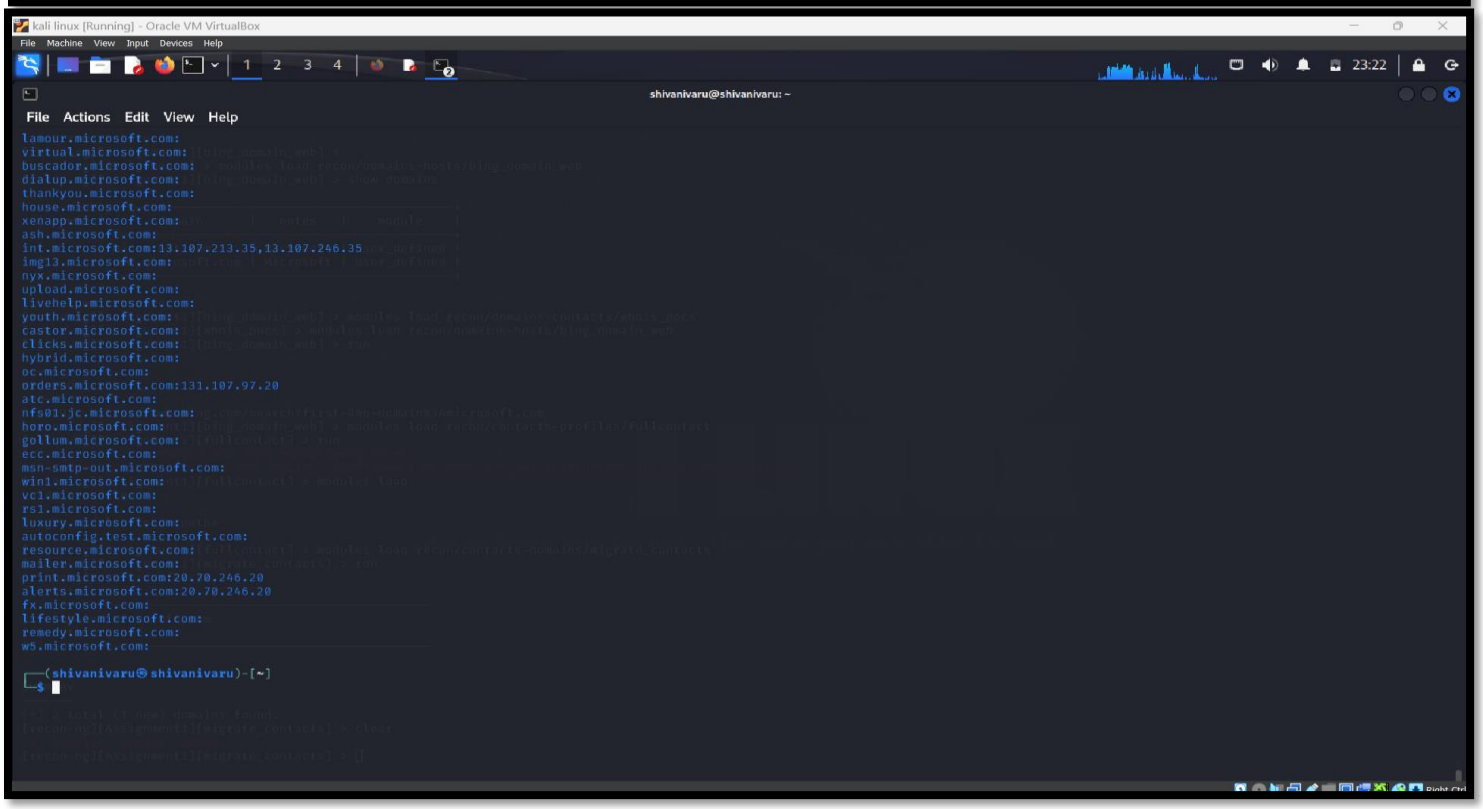


As a result, we have found above open ports/ IP addresses, email accounts, and 7 host of different websites they use. we found 16 emails.

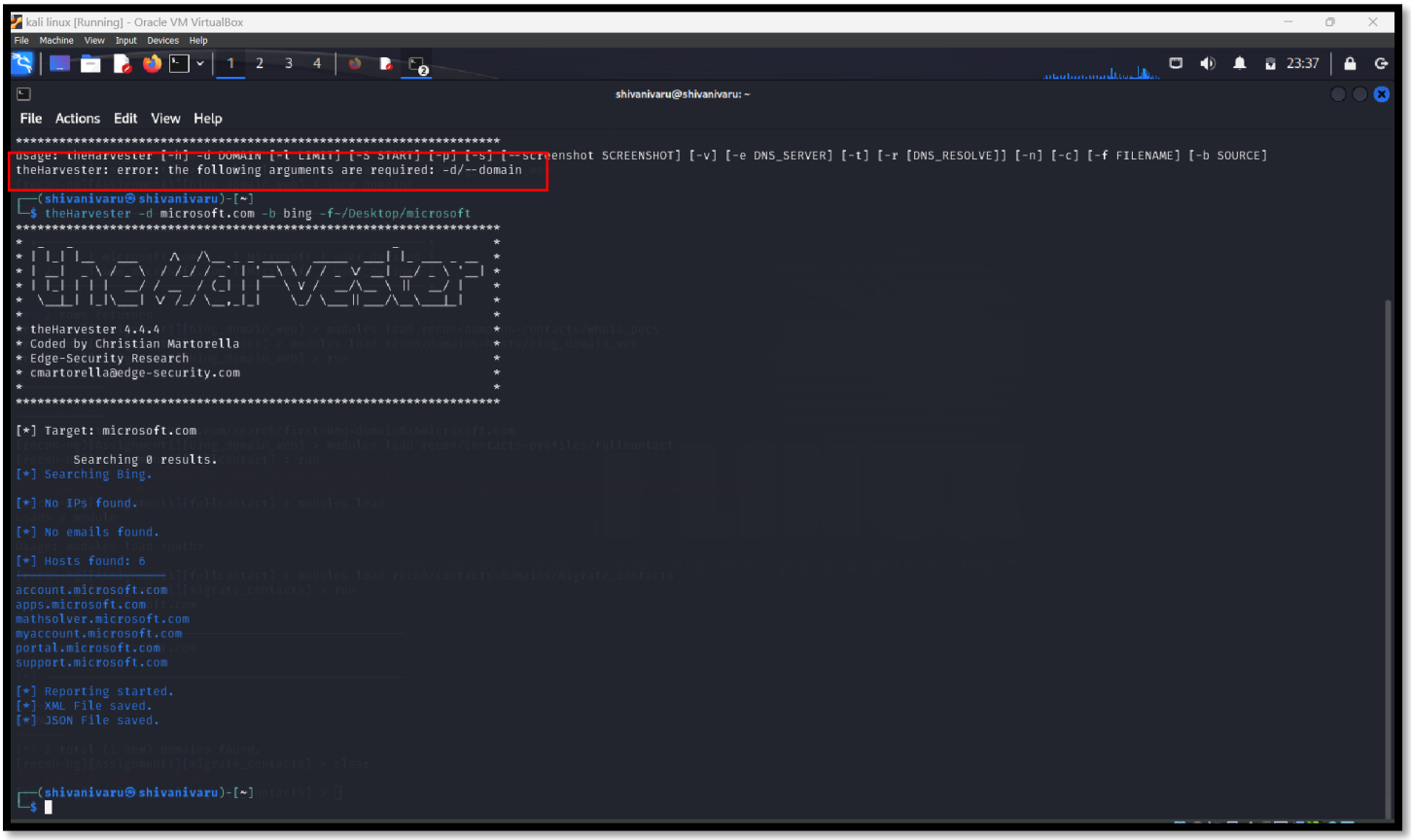
Command Used	**TheHarvester -d microsoft.com -b bing -c**

The "-c" flag is used to activate the DNS brute force plugin, which runs a dictionary brute force enumeration. This can be helpful in identifying additional subdomains associated with the target domain.



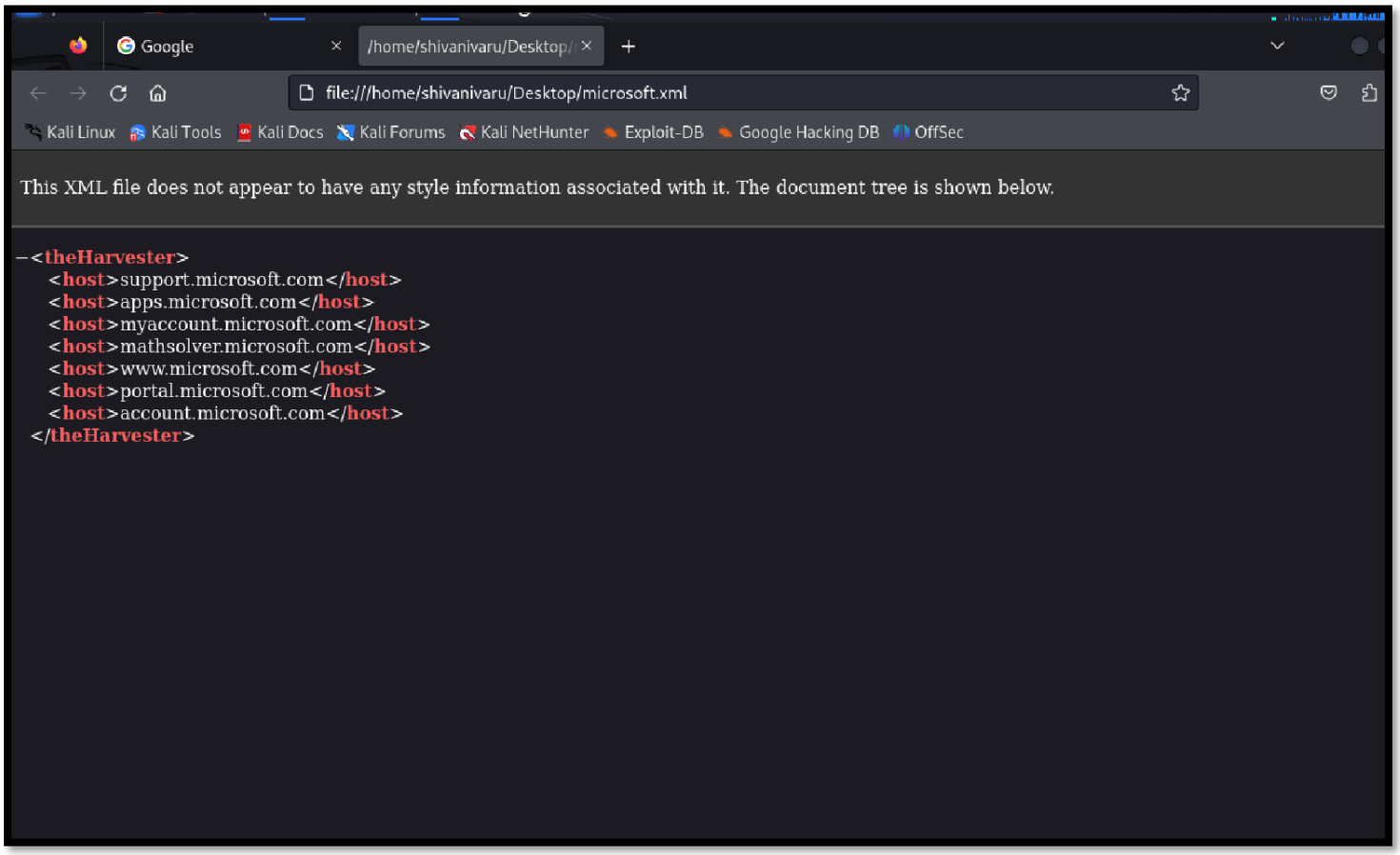


Command Used	**TheHarvester -d microsoft.com -b bing -f~/Desktop/Microsoft**

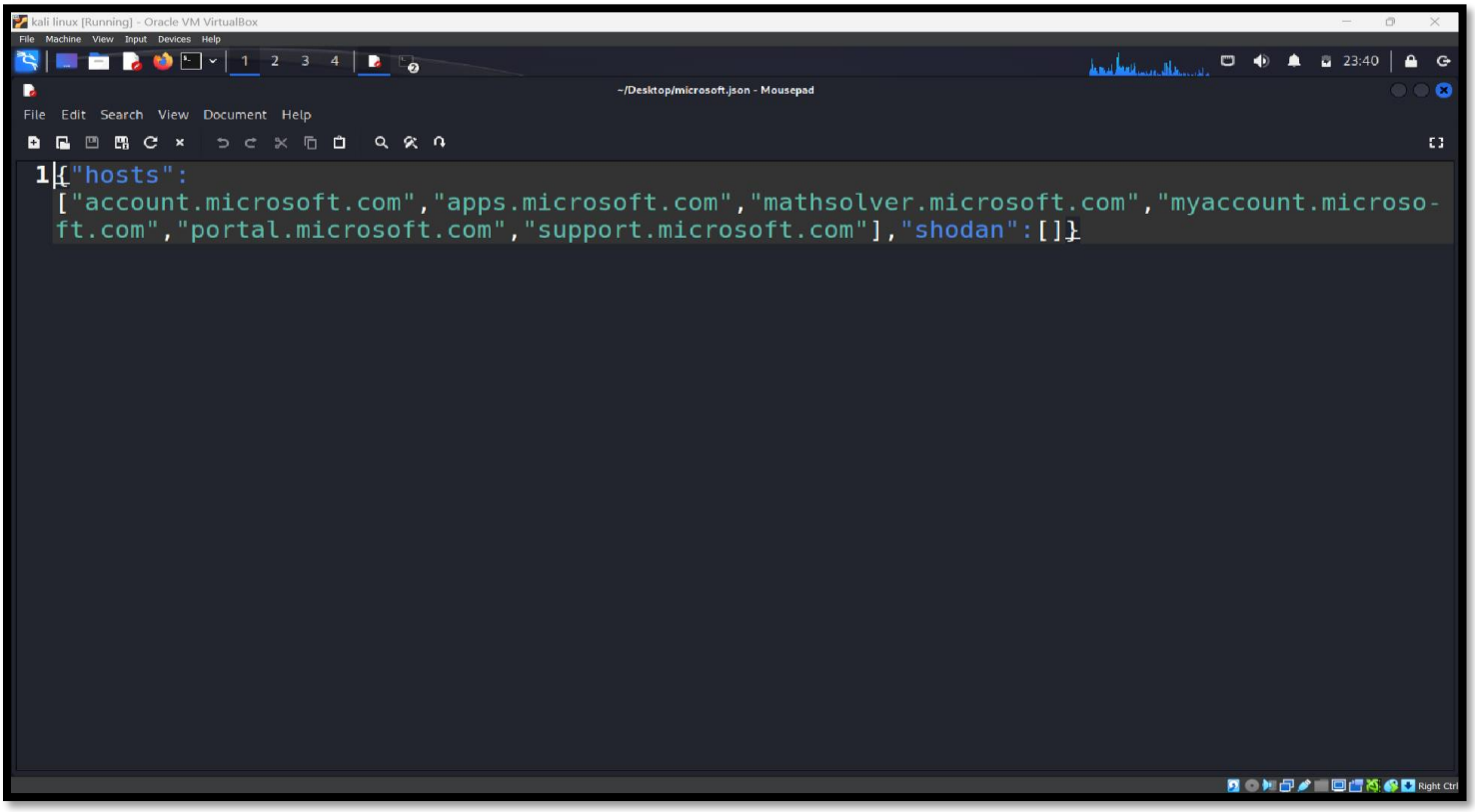


The **-d** flag specifies the domain to scan, the **-b** flag specifies the search engine to use, and the **-f** flag specifies an output file for the found results, which will be saved on the Desktop with the name "**microsoft**".

❖ **XML Format**



❖ **Json format**



References

1) Admin, T. (2024, January 5). Recon-ng tutorial. HackerTarget.com. https://hackertarget.com/recon-ng-tutorial/
2) Moulik. (2023, December 30). Recon-ng: A full tutorial from NOOB to pro [updated 2024]. TECHYRICK. https://techyrick.com/recon-ng/
3) GeeksforGeeks. (2021, April 16). Recon-ng information gathering tool in Kali Linux. GeeksforGeeks. https://www.geeksforgeeks.org/recon-ng-installation-on-kali-linux/
4) Recon-NG: Kali linux tools. Kali Linux. (2022, November 16). https://www.kali.org/tools/recon-ng/
5) Recon-ng information gathering tool in Kali Linux - javatpoint. www.javatpoint.com. (n.d.). https://www.javatpoint.com/recon-ng-information-gathering-tool-in-kali-linux
6) Securitytrails. (n.d.). https://securitytrails.com/blog/recon-ng
7) MaxiSoler. (2012, April 17). *Home*. ToolsWatch Cyber Security Tools Events. https://toolswatch.org/2012/04/theharvester-v2-2-released/
8) Nmmapper.com. (n.d.). *Online platform for network pentesting and mapping tool for penetration testers and system administrators*. nmmapper.com. https://www.nmmapper.com/sys/theharvester/email-harvester-tool/online/

Video Recording Link:

https://conestogac.zoom.us/rec/share/-WaUywpUeU5kQlxDhKMgB6ABiR7DmlQRgqMVH1tVC4-xGRZgrUTQ2i0zYi6dqnAg.qCPAoPKJTclM5GeI?startTime=1706314693000