

Lab #1:

Course Name: Ethical Hacking and Offensive Security(HOD401)

Student Name: Nguyễn Trần Vinh – SE160258

Instructor Name: Mai Hoàng Đỉnh

Lab Due Date: 13/09/2023

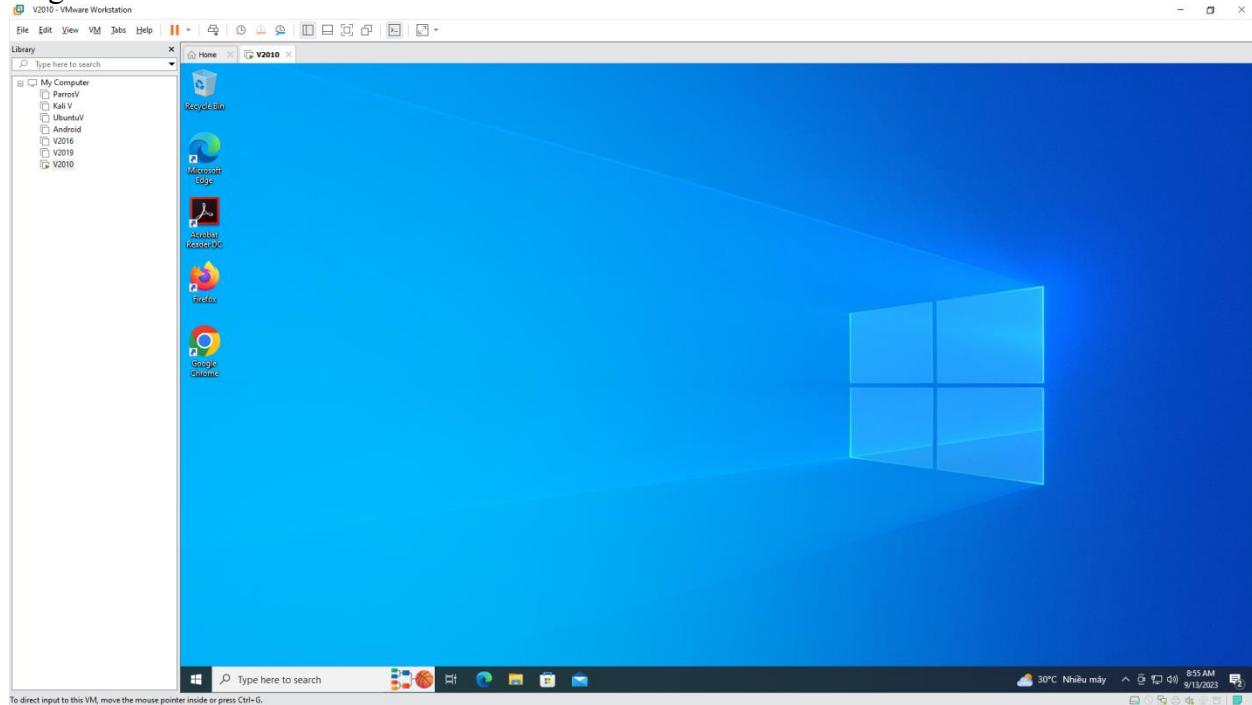
Lab Tasks:

1. Perform Footprinting Through Search Engines

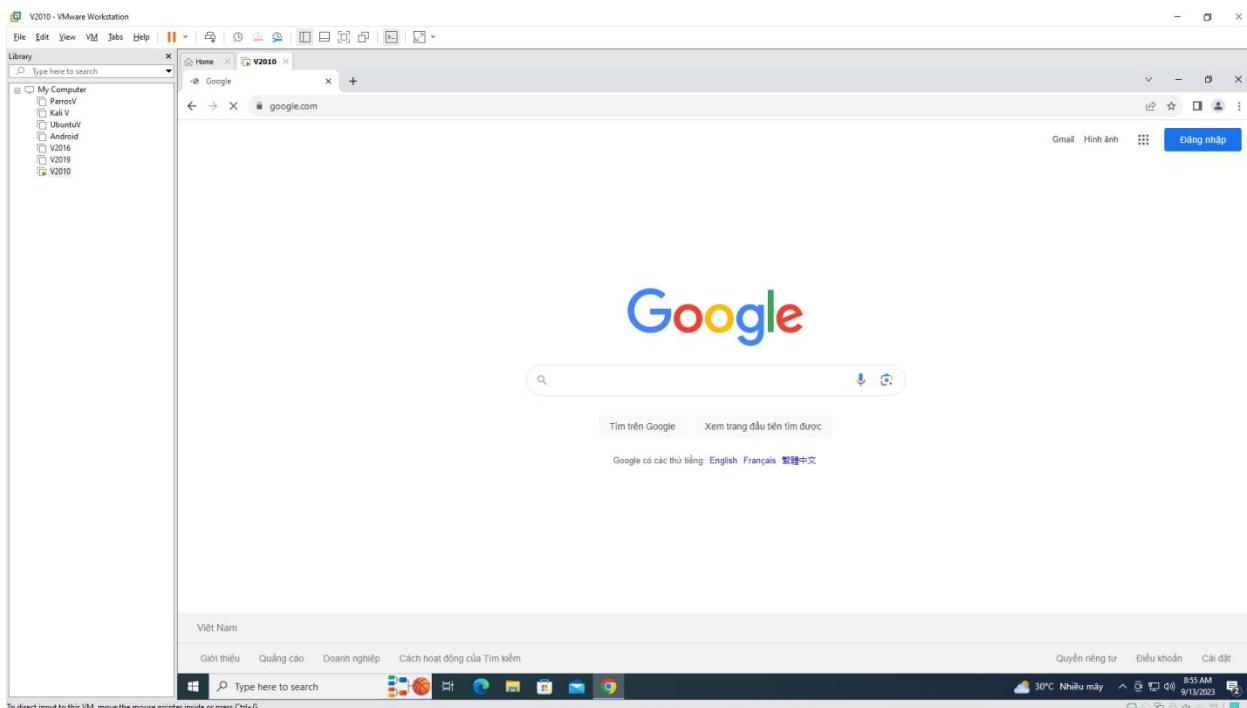
- Gather Information using Advanced Google Hacking Techniques

- using Windows 10

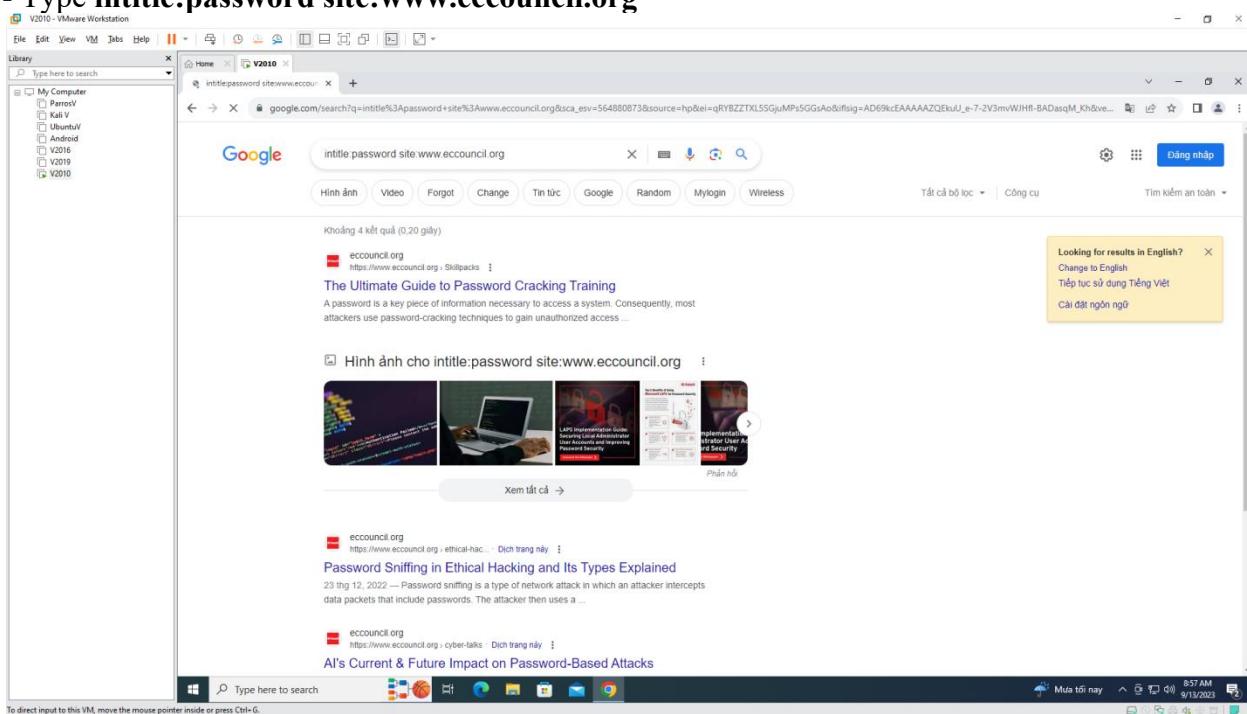
- login with username Administrator



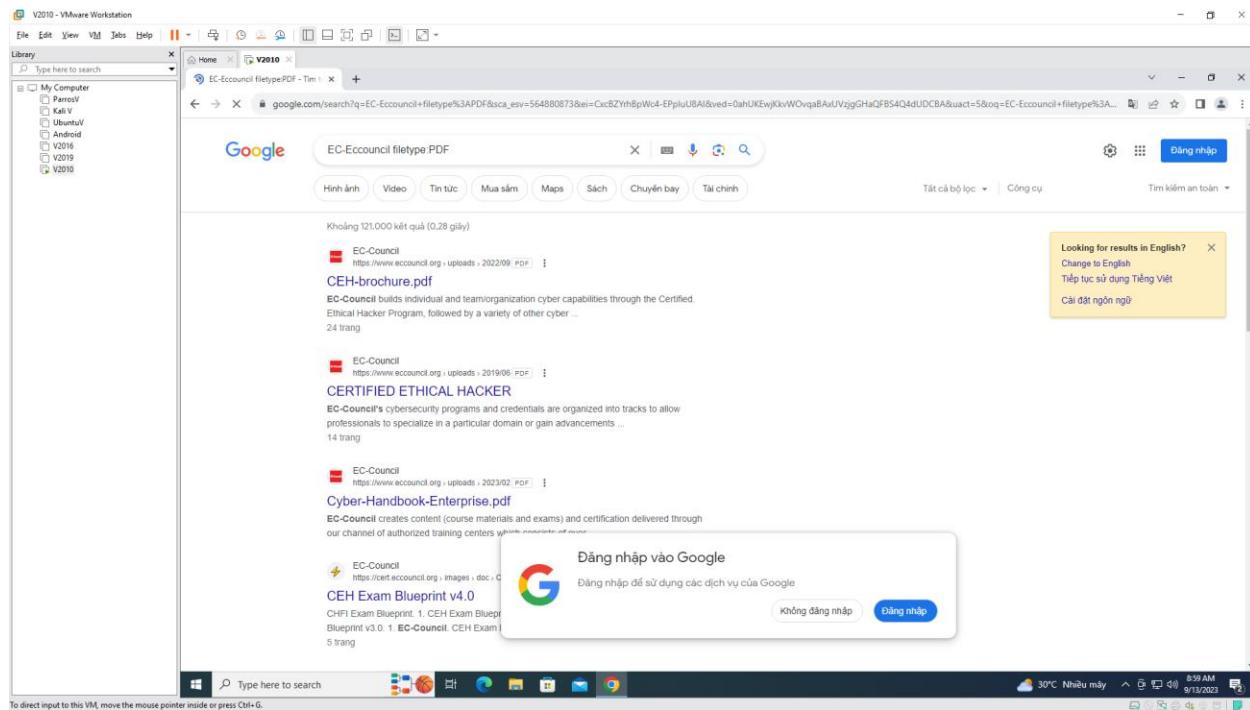
- Open website



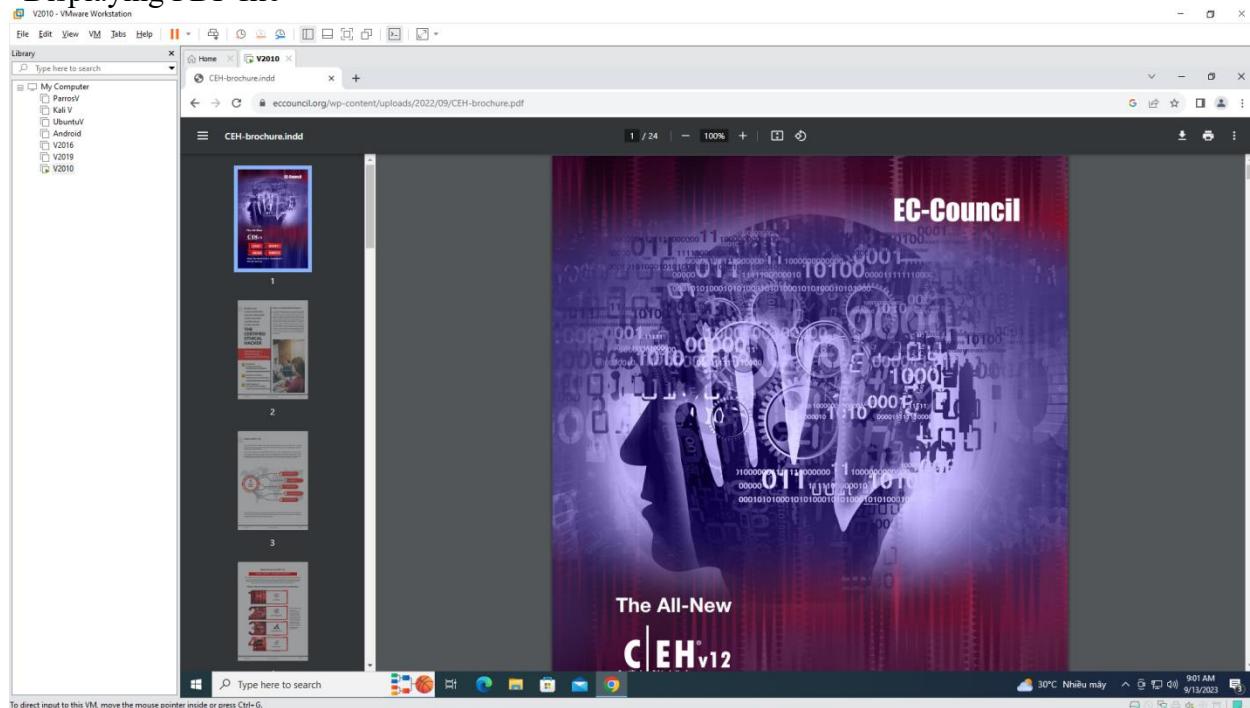
- Type intitle:password site:www.eccouncil.org



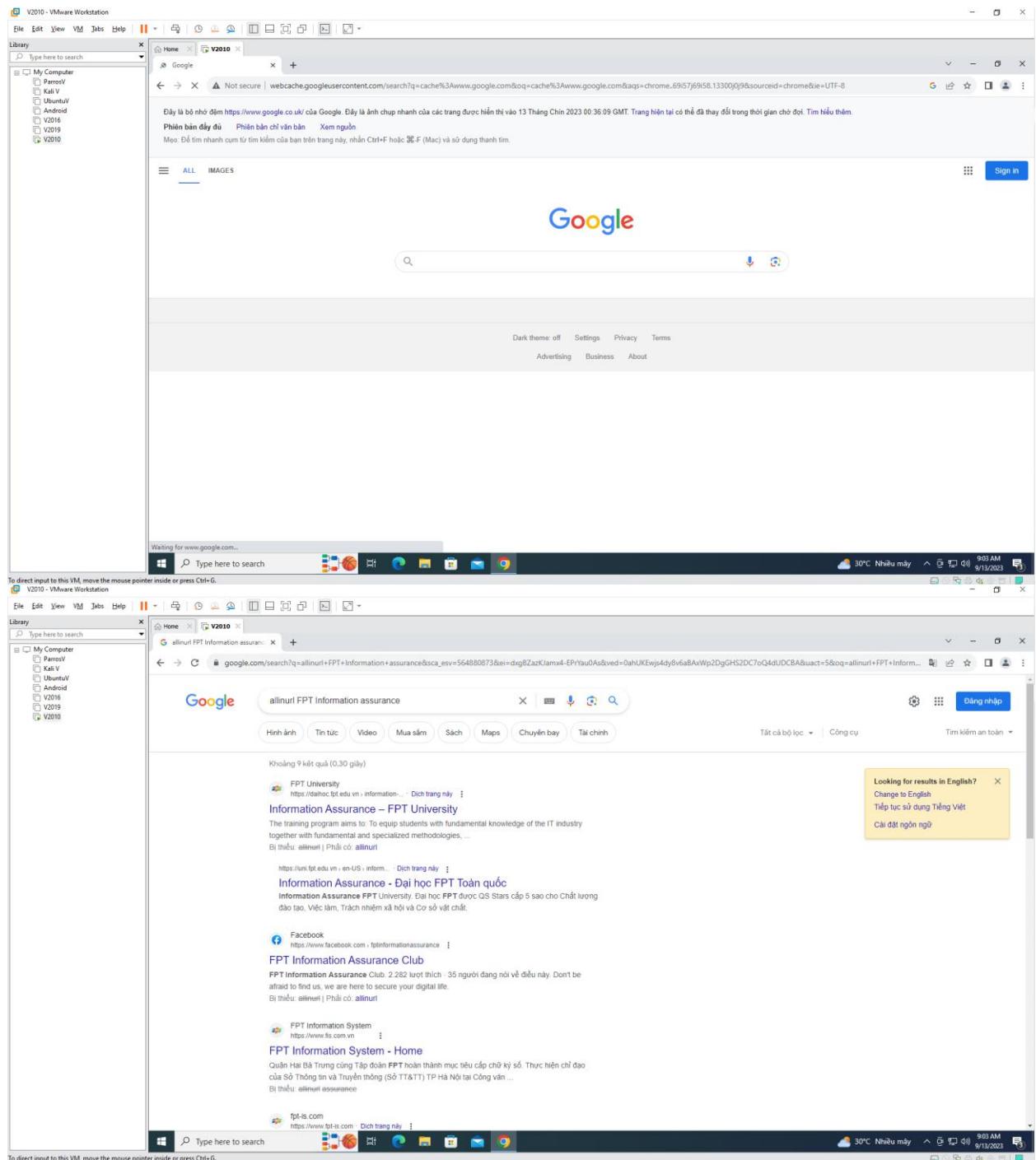
- EC-Council filetype:PDF

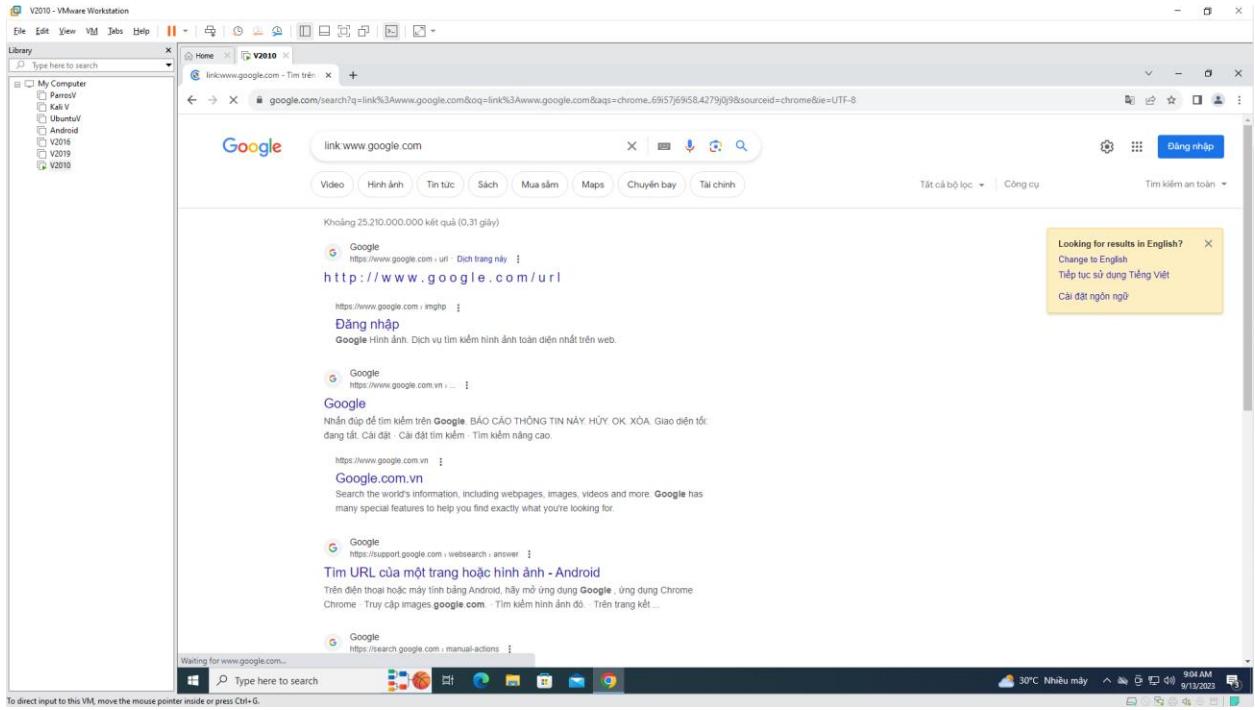


- Click on any link from result
- Displaying PDF file



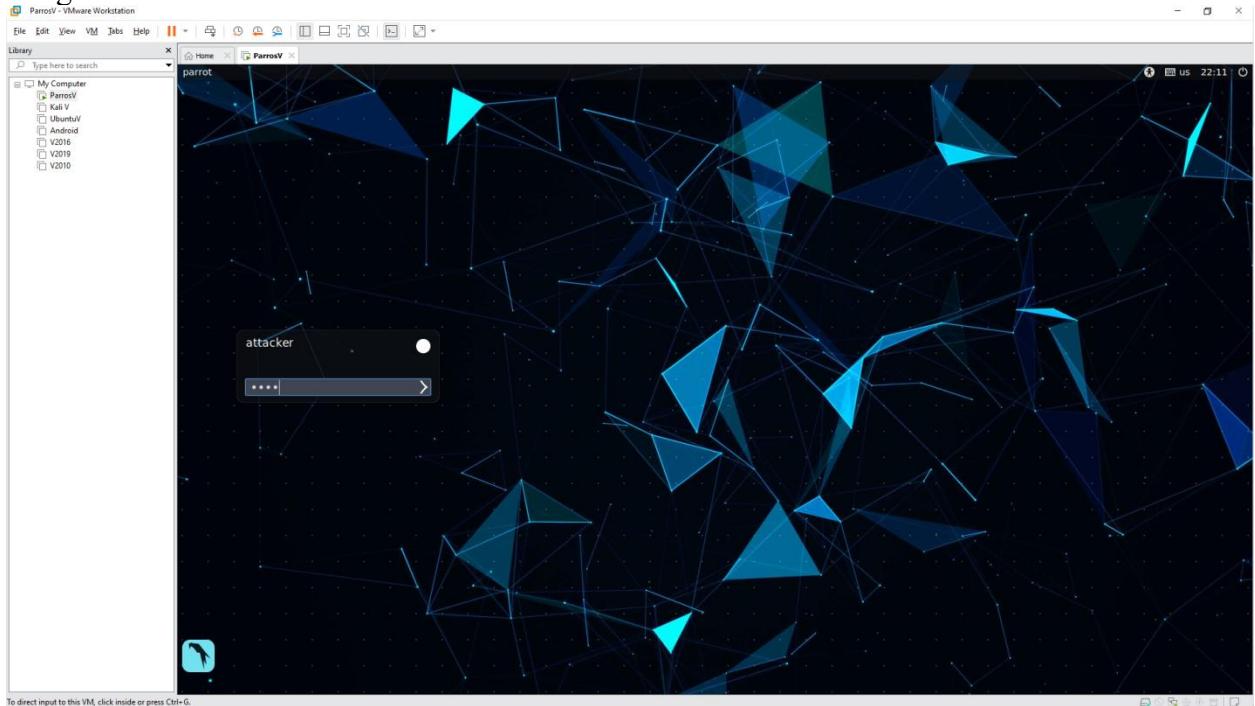
- Another advanced search



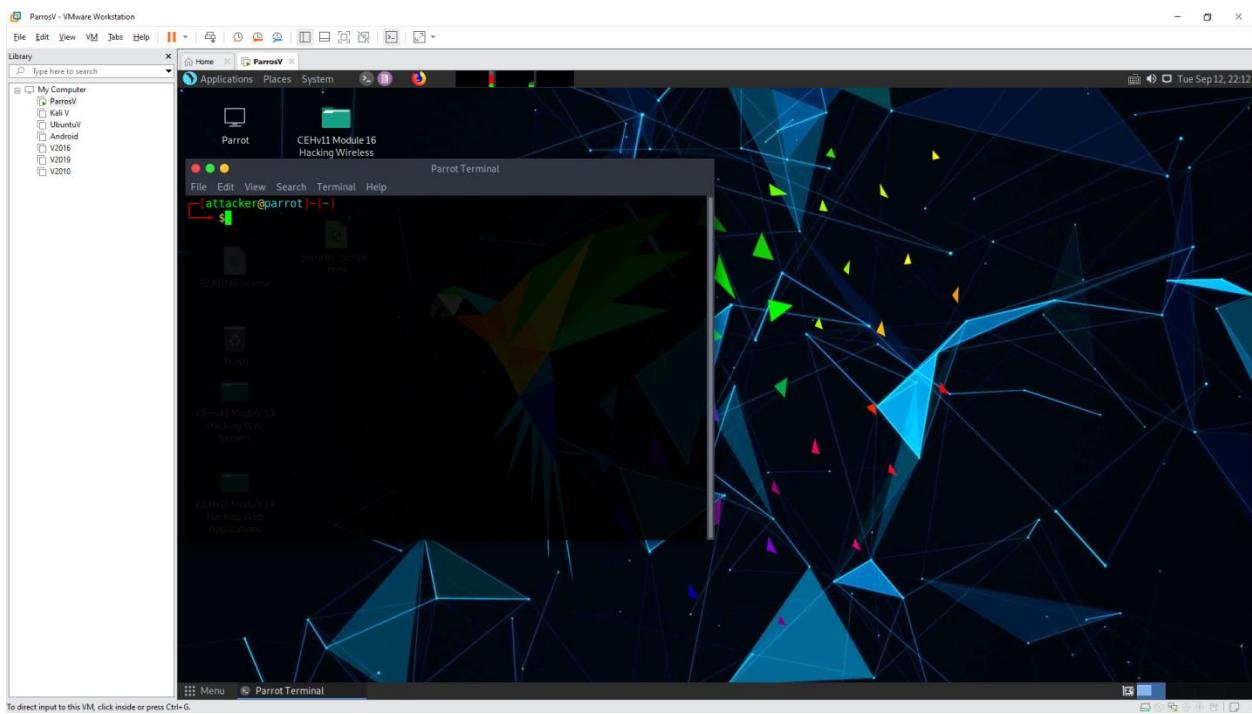


2. Perform Footprinting Through Web Services

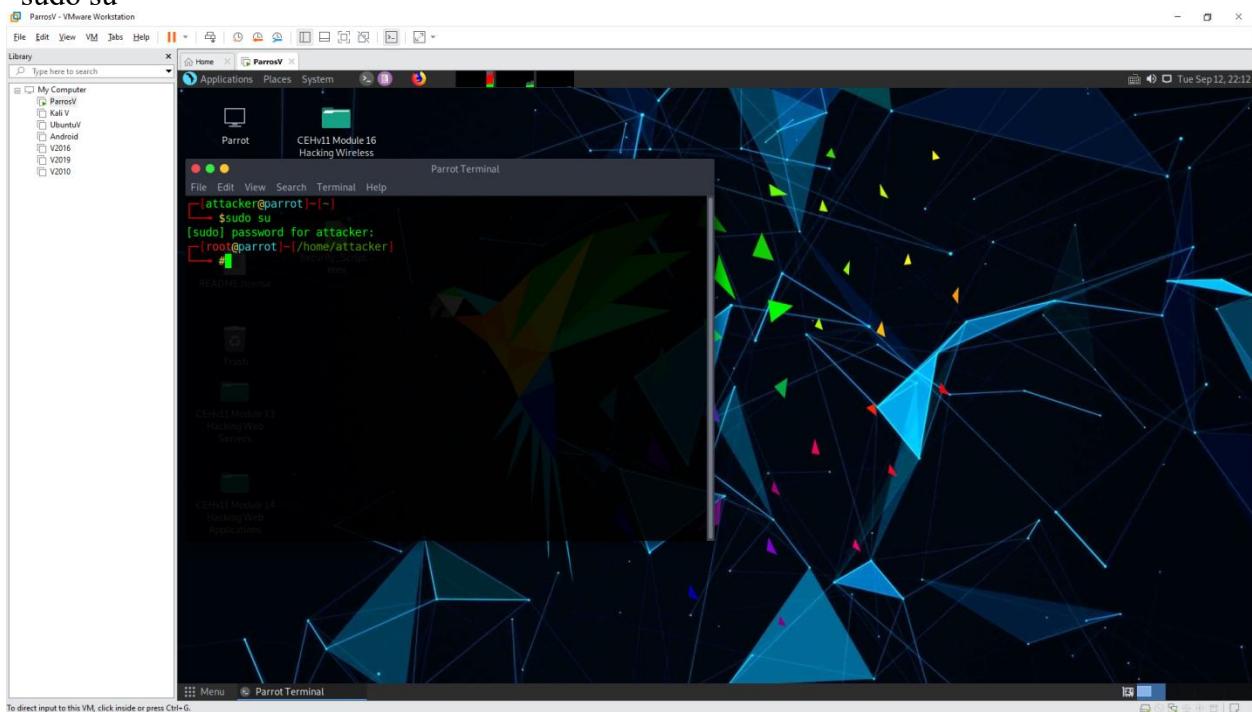
- Gather an Email List using the Harvester
 - Using Parrot
 - Login with user Attacker



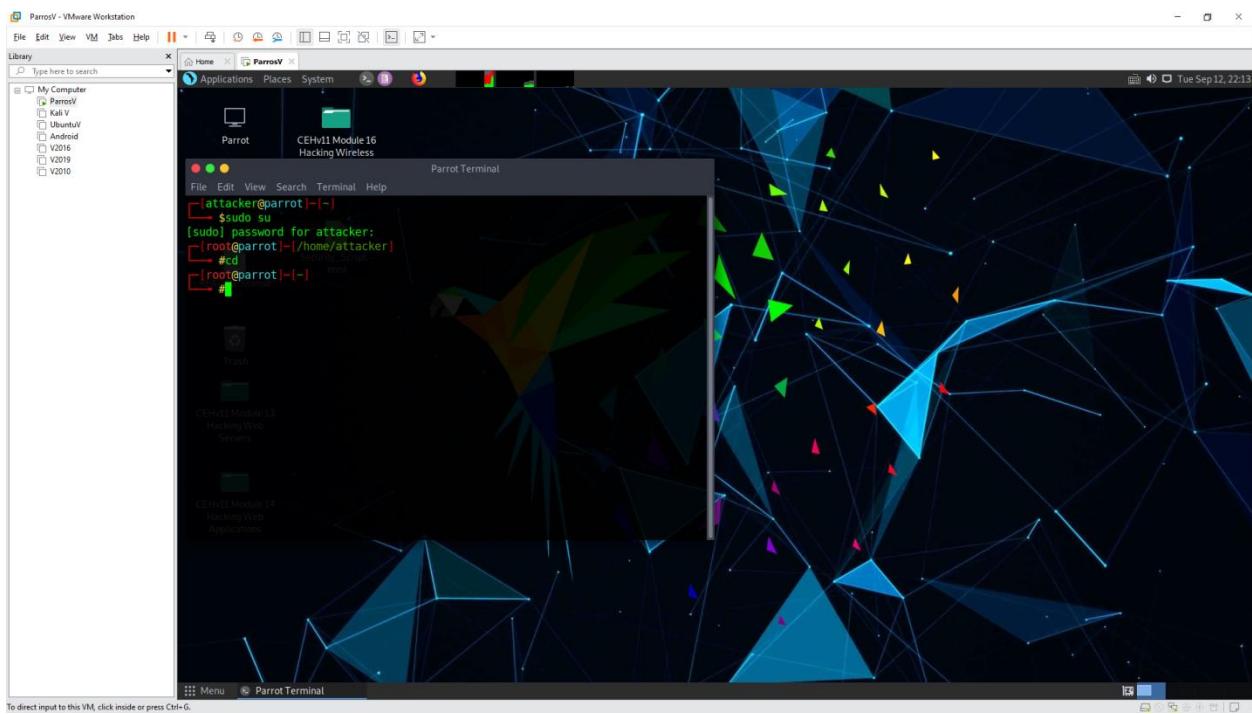
- Open terminal



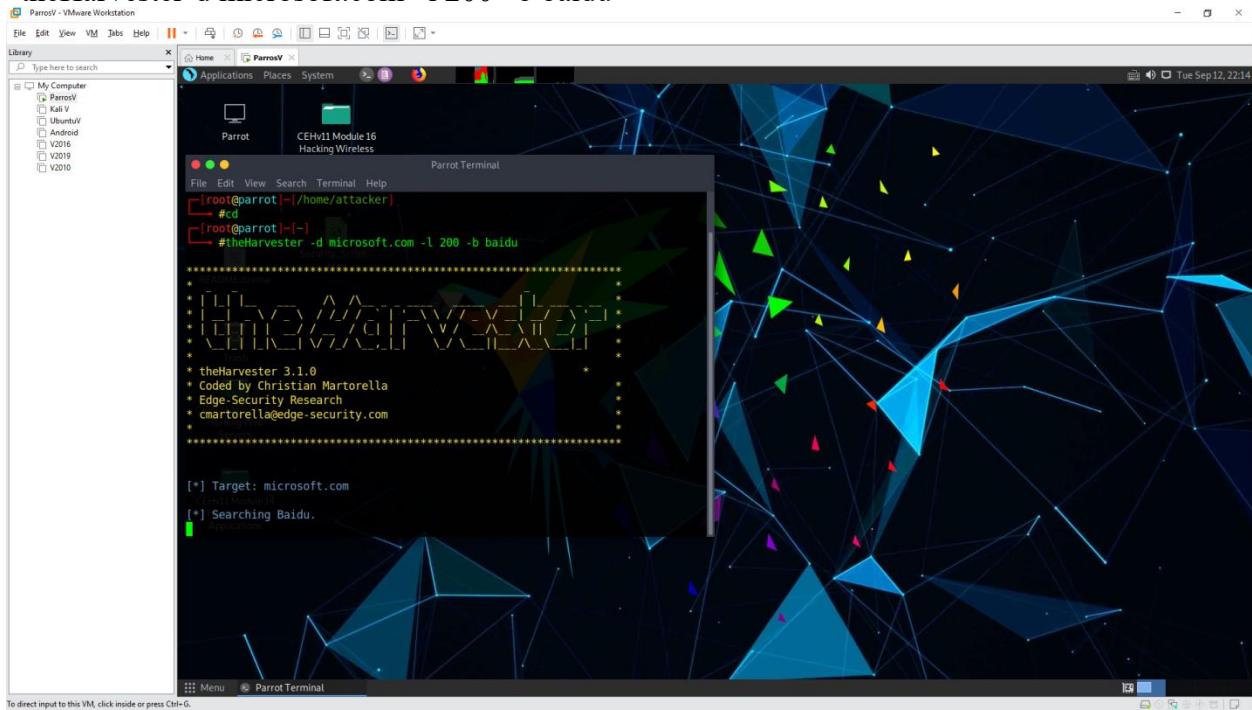
- sudo su

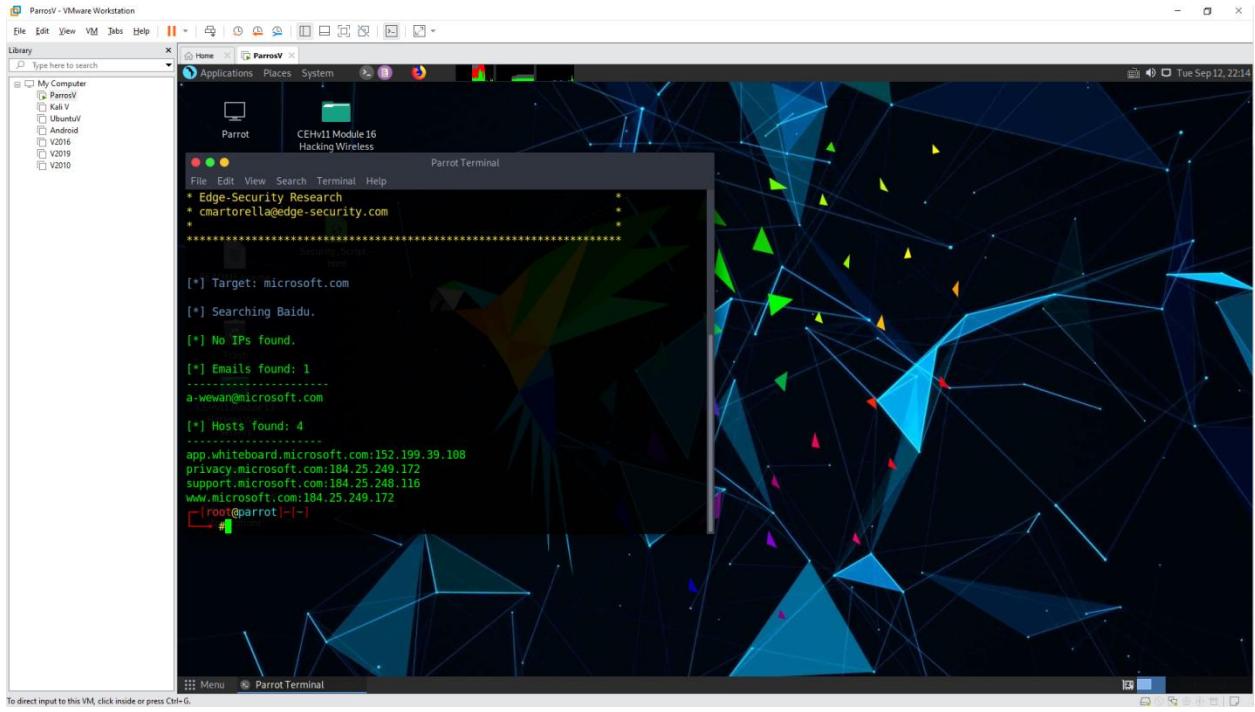


- cd



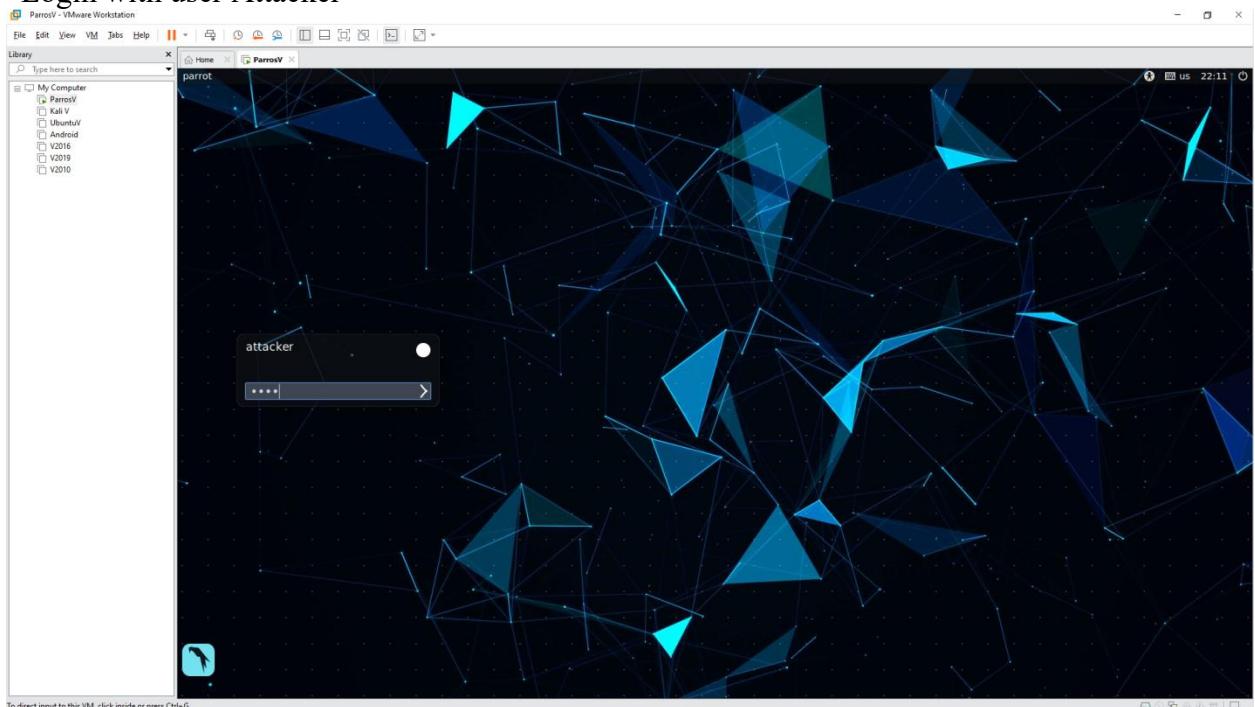
- theHarvester-d microsoft.com -l 200 -b baidu



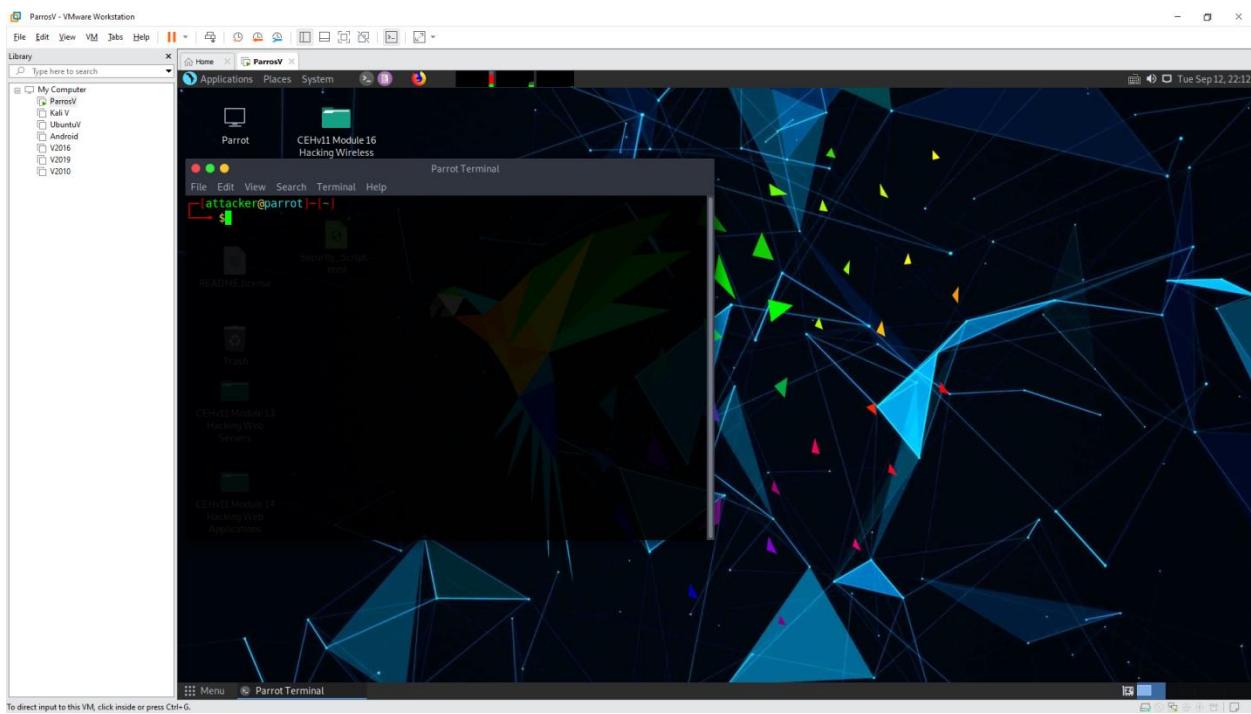


3. Perform Footprinting Social Networking Sites

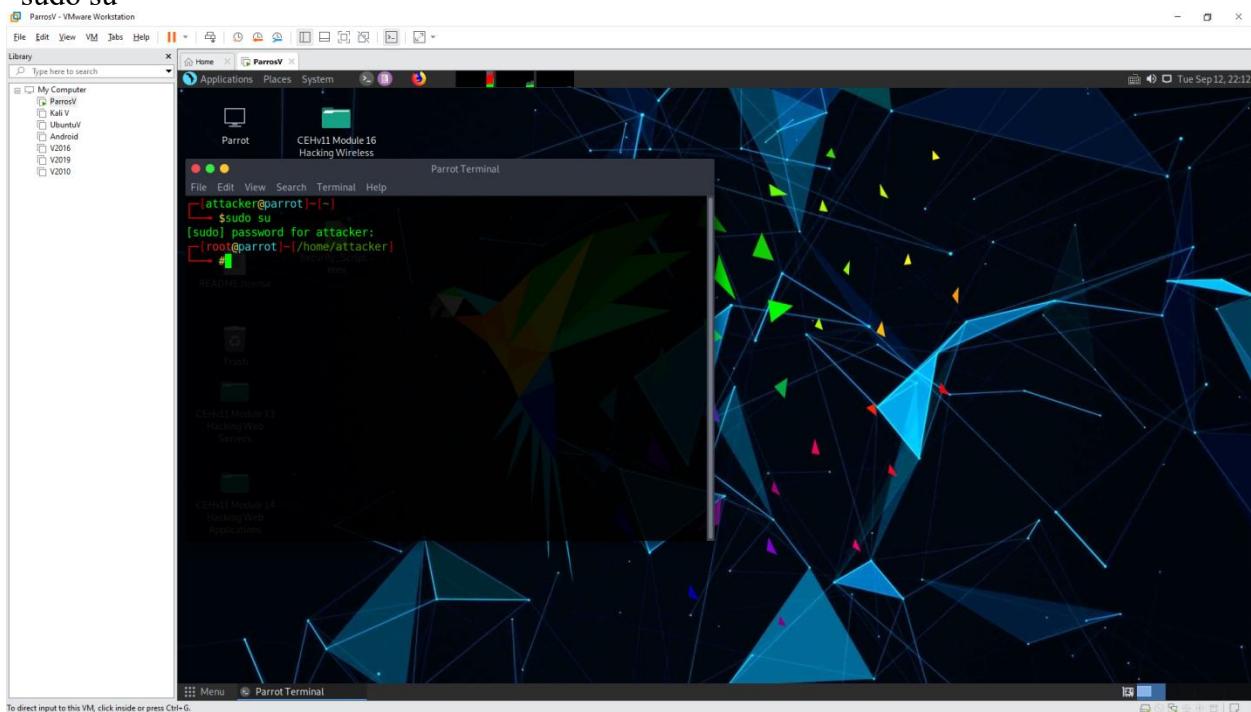
- Gather Employees' Information from LinkedIn using theHavester
- Using Parrot
- Login with user Attacker



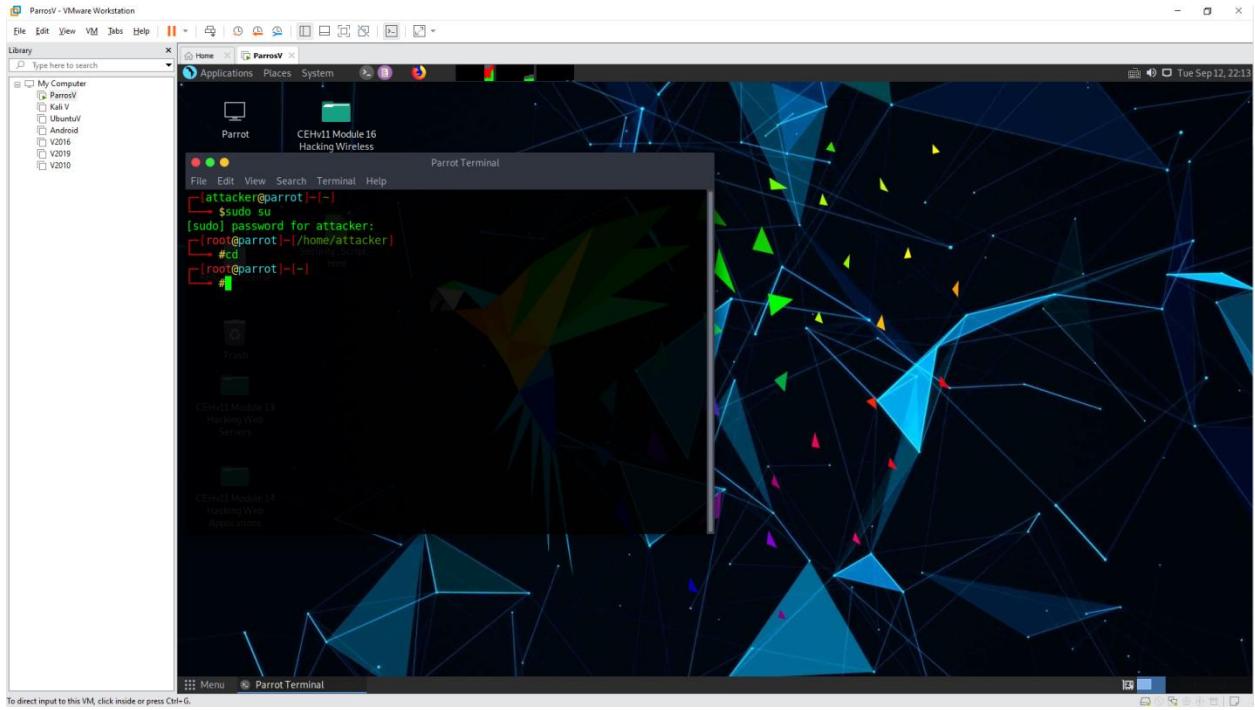
- Open terminal



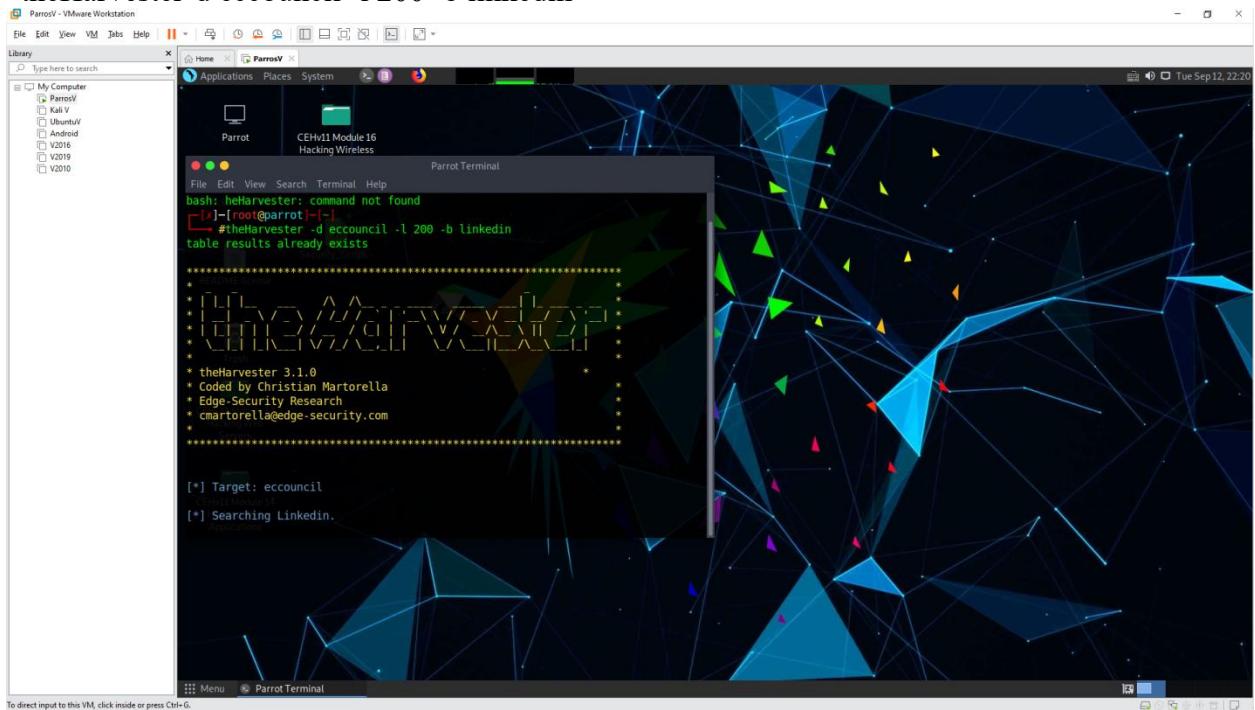
- sudo su

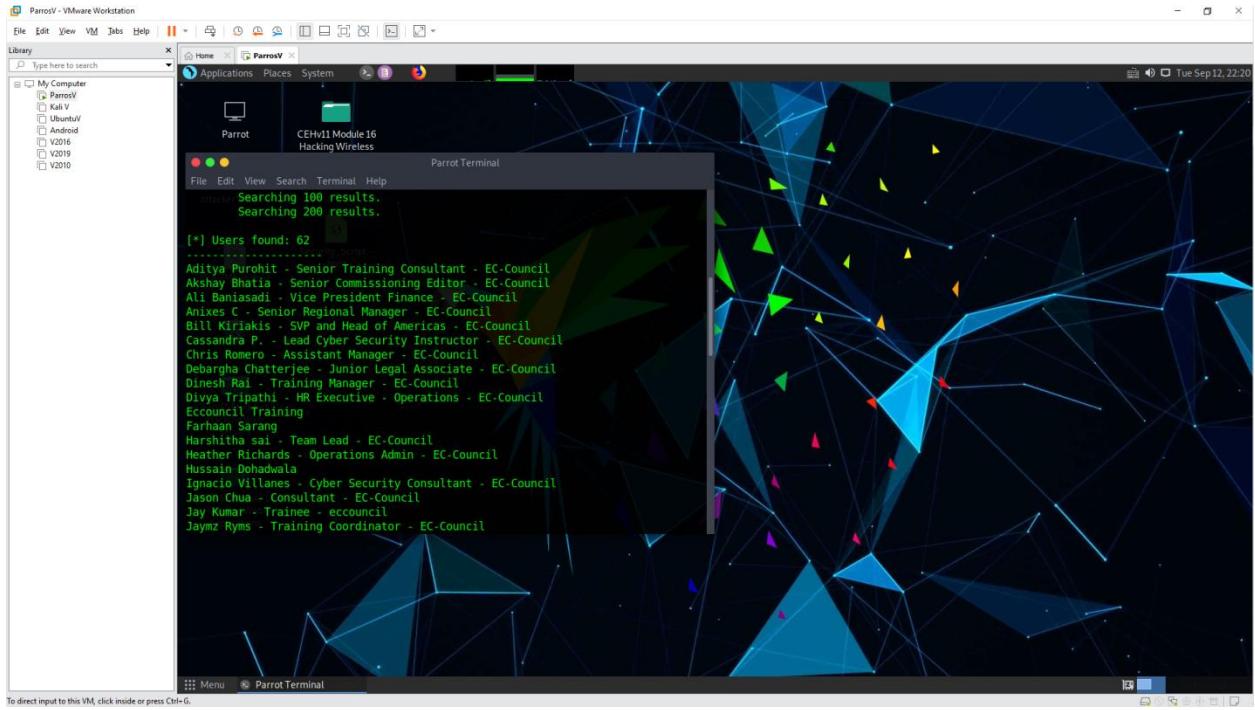


- cd



- theHarvester -d eccouncil -l 200 -b linkedin



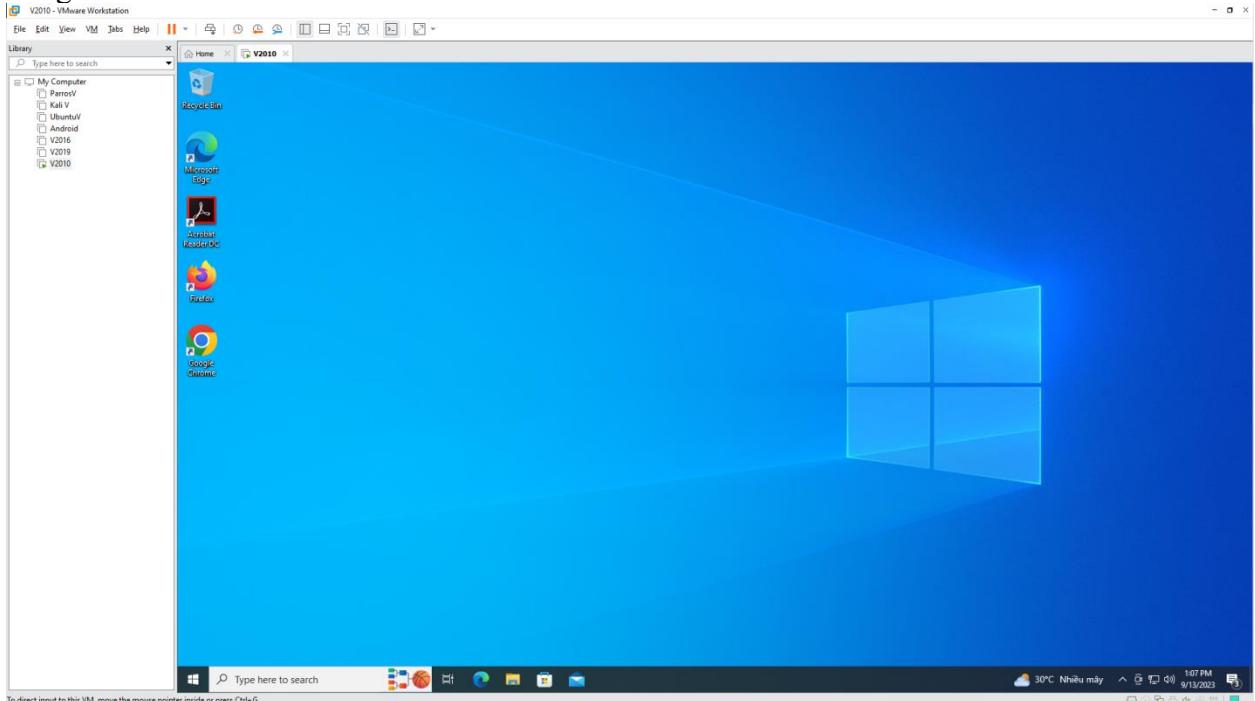


4. Perform Web Footprinting

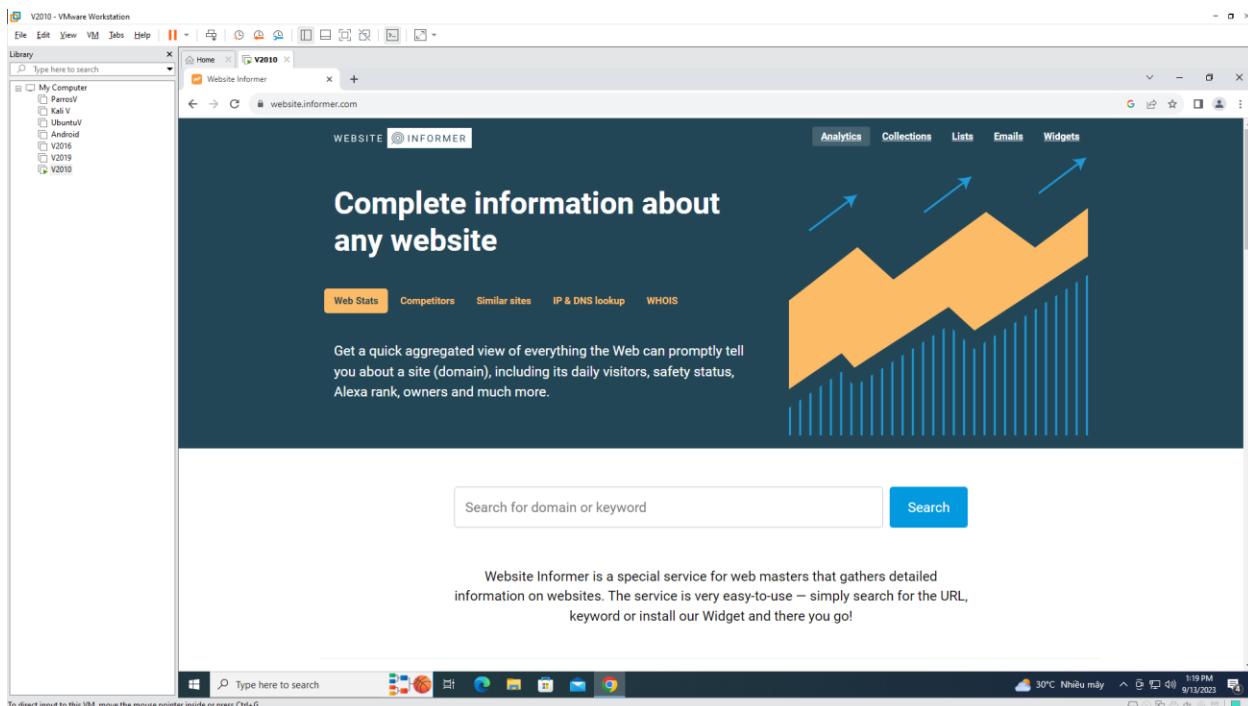
- Gather Information about a Target Website using Website Informer

- Using Windows 10

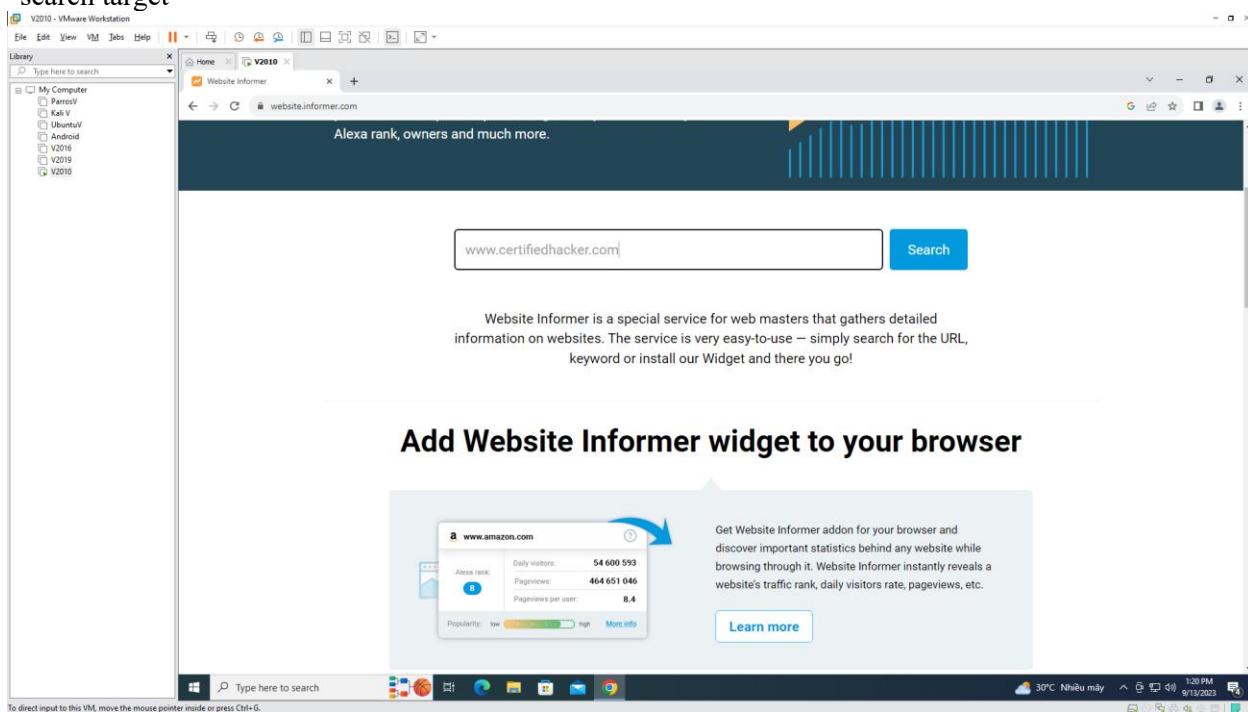
- Login with user Administrator



- open browser



- search target



- Information of target

V2010 - VMware Workstation

File Edit View VM Help

Type here to search

Library

- My Computer
 - PanosV
 - Kali V
 - UbuntuV
 - Android
 - V2016
 - V2019
 - V2019

certifiedhacker.com at WI Certi... +

website.informer.com/certifiedhacker.com

website.informer.com

Search for domain or keyword: certifiedhacker.com Search

// WWW.CERTIFIEDHACKER.COM

Visit www.certifiedhacker.com

Sponsored links

General Info Stats & Details Whois IP Whois Expand all blocks

Certified Hacker

A brief description of this website or your business.

Keywords: associated, Keywords, or phrases, hacker.com, with each page, shodan, are best, Certified Hacker, certifiedhacker.com

Last scanned Sep 3, 2023

Daily visitors: 534 Daily pageviews: 534

Created: 2002-07-30 Expires: 2024-07-30 Owner: PERFECT PRIVACY, LLC Hosting company: Unified Layer Registrar: Network Solutions, LLC IPs: 162.241.216.11 DNS: ns1.bluehost.com ns2.bluehost.com Email: See owner's emails

★★★★★

Sponsored links

OVCloud OPEN

30°C Nhiều mây 1:21 PM 9/13/2023

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

V2010 - VMware Workstation

File Edit View VM Help

Type here to search

Library

- My Computer
 - PanosV
 - Kali V
 - UbuntuV
 - Android
 - V2016
 - V2019
 - V2019

certifiedhacker.com at WI Certi... +

website.informer.com/certifiedhacker.com

Keywords: associated, Keywords, or phrases, hacker.com, with each page, shodan, are best, Certified Hacker, certifiedhacker.com

Last scanned Sep 3, 2023

Sponsored links

Daily visitors: 534 Daily pageviews: 534

Created: 2002-07-30 Expires: 2024-07-30 Owner: PERFECT PRIVACY, LLC Hosting company: Unified Layer Registrar: Network Solutions, LLC IPs: 162.241.216.11 DNS: ns1.bluehost.com ns2.bluehost.com Email: See owner's emails

★★★★★

Sponsored links

Stats & Details

Whois

IP Whois

Similar sites

- japanincinema.net
- Loadimg...
- gigazine.com
- Flashy - Changing the way photography works
- bayabay.com.ua
- BUYnBay.com.ua - доставка товаров в Украину со всего мира
- mensguide.co.uk
- mensguide.co.uk
- slubujecimosc.pl
- Slubuję Ci Miłość | Strona w budowie

30°C Nhiều mây 1:21 PM 9/13/2023

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- WHOIS

- Whois

Domain Name: CERTIFIEDHACKER.COM
 Registry Domain ID: 88849376_DOMAIN_COM-VRSN
 Registrar WHOIS Server: whois.networksolutions.com
 Registrar URL: http://networksolutions.com
 Updated Date: 2023-08-22T07:58:34Z
 Creation Date: 2002-07-30T00:32:00Z
 Registrar Registration Expiration Date: 2024-07-30T00:32:00Z
 Registrant: Network Solutions, LLC
 Registrar IANA ID: 2
 Reseller:
 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
 Registry Registrant ID:
 Registrant Name: PERFECT PRIVACY, LLC
 Registrant Organization:
 Registrant Street: 5335 Gate Parkway care of Network Solutions PO Box 459
 Registrant City: Jacksonville
 Registrant State/Province: FL
 Registrant Postal Code: 32256
 Registrant Country: US
 Registrant Phone: +1.5707088622
 Registrant Phone Ext:
 Registrant Fax:
 Registrant Fax Ext:
 Registrant Email: kqpt994x73@networksolutionsprivateregistration.com
 Registry Admin ID:
 Admin Name: PERFECT PRIVACY, LLC
 Admin Organization:
 Admin Street: 5335 Gate Parkway care of Network Solutions PO Box 459
 Admin City: Jacksonville
 Admin State/Province: FL
 Admin Postal Code: 32256
 Admin Country: US
 Admin Phone: +1.5707088622
 Admin Phone Ext:
 Admin Fax:
 Admin Fax Ext:
 Admin Email: kqpt994x73@networksolutionsprivateregistration.com
 Registry Tech ID:
 Tech Name: PERFECT PRIVACY, LLC
 Tech Organization:
 Tech Street: 5335 Gate Parkway care of Network Solutions PO Box 459
 Tech City: Jacksonville
 Tech State/Prov:

- Stats & details

- Stats & Details

Hosting company: Unified Layer
 Registrar: Network Solutions, LLC
 IPs: 162.24.2.16.11
 DNS: ns1.bluehost.com
 ns2.bluehost.com ★★★★!
 Email: See owner's emails

Sponsored links

Alexa.com Traffic Rank Search %

Month Average Daily Reach	0.00002	+300% ↑
Month Average Daily Pageviews	0.000001	+200% ↑
Month Average Pageviews per user	1	34.21% ↓

Mywot.com - Reputation rating 72

- Trustworthiness: 72
- Vendor reliability: 72
- Privacy: 72

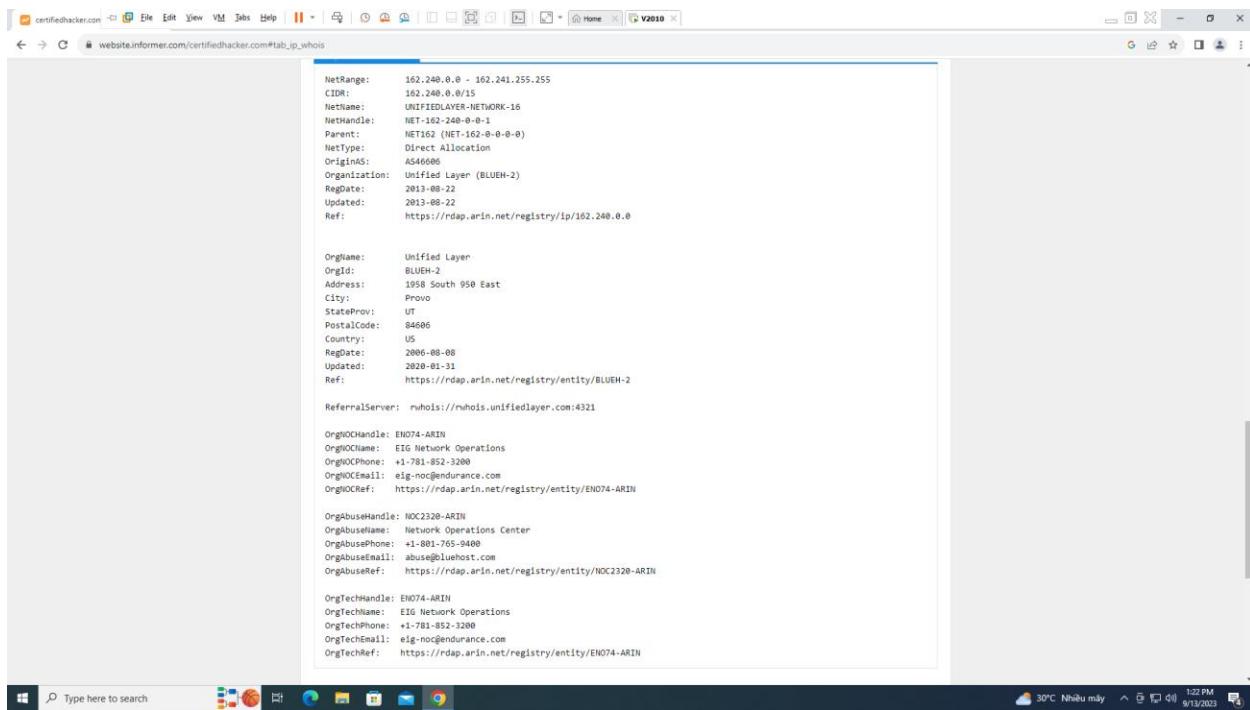
Siteadvisor.com Status: good

Compete.com Visits: 1454

- Whois

Domain Name: CERTIFIEDHACKER.COM
 Registry Domain ID: 88849376_DOMAIN_COM-VRSN
 Registrar WHOIS Server: whois.networksolutions.com
 Registrar URL: http://networksolutions.com
 Updated Date: 2023-08-22T07:58:34Z
 Creation Date: 2002-07-30T00:32:00Z
 Registrar Registration Expiration Date: 2024-07-30T00:32:00Z
 Registrant: Network Solutions, LLC
 Registrar IANA ID: 2
 Reseller:
 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
 Registry Registrant ID:
 Registrant Name: PERFECT PRIVACY, LLC
 Registrant Organization:
 Registrant Street: 5335 Gate Parkway care of Network Solutions PO Box 459
 Registrant City: Jacksonville
 Registrant State/Province: FL
 Registrant Postal Code: 32256

- IP Whois



```

NetRange: 162.240.0.0 - 162.241.255.255
CIDR: 162.240.0.0/15
NetName: UNIFIEDLAYER-NETWORK-16
NetHandle: NET-162-240-0-0-1
Parent: NET162 (NET-162-0-0-0-0)
NetType: Direct Allocation
OrgInfoS: AS46606
Organization: Unified Layer (BLUEH-2)
RegDate: 2013-08-22
Updated: 2013-08-22
Ref: https://rdap.arin.net/registry/ip/162.240.0.0

OrgName: Unified Layer
OrgId: BLUEH-2
Address: 1958 South 950 East
City: Provo
StateProv: UT
PostalCode: 84606
Country: US
RegDate: 2006-08-08
Updated: 2020-01-31
Ref: https://rdap.arin.net/registry/entity/BLEUH-2

ReferralServer: ruwhois://ruwhois.unifiedlayer.com:4321

OrgInfoHandle: EN074-ARIN
OrgInfoName: EIG Network Operations
OrgInfoPhone: +1-781-852-3200
OrgInfoEmail: eig-noc@endurance.com
OrgInfoRef: https://rdap.arin.net/registry/entity/EN074-ARIN

OrgAbuseHandle: NOC2320-ARIN
OrgAbuseName: Network Operations Center
OrgAbusePhone: +1-801-765-9440
OrgAbuseEmail: abuse@uehost.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/NOC2320-ARIN

OrgTechHandle: EN074-ARIN
OrgTechName: EIG Network Operations
OrgTechPhone: +1-781-852-3200
OrgTechEmail: eig-noc@endurance.com
OrgTechRef: https://rdap.arin.net/registry/entity/EN074-ARIN

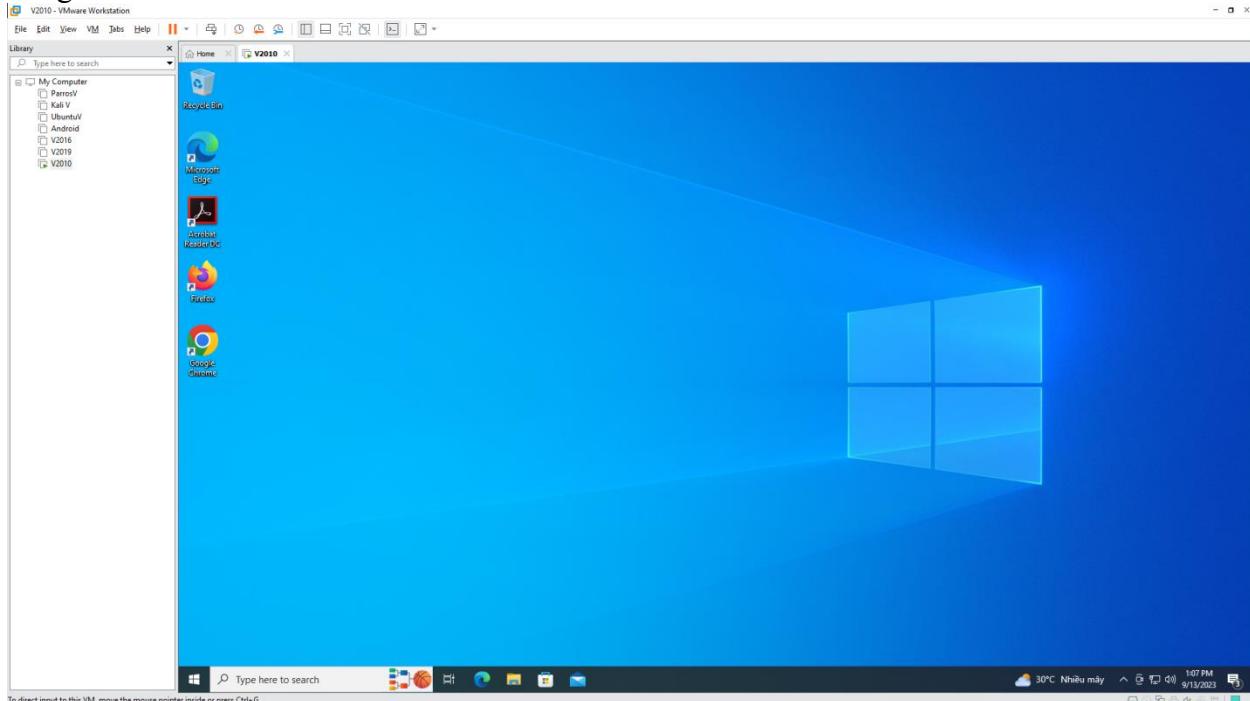
```

5. Perform Email Footprinting

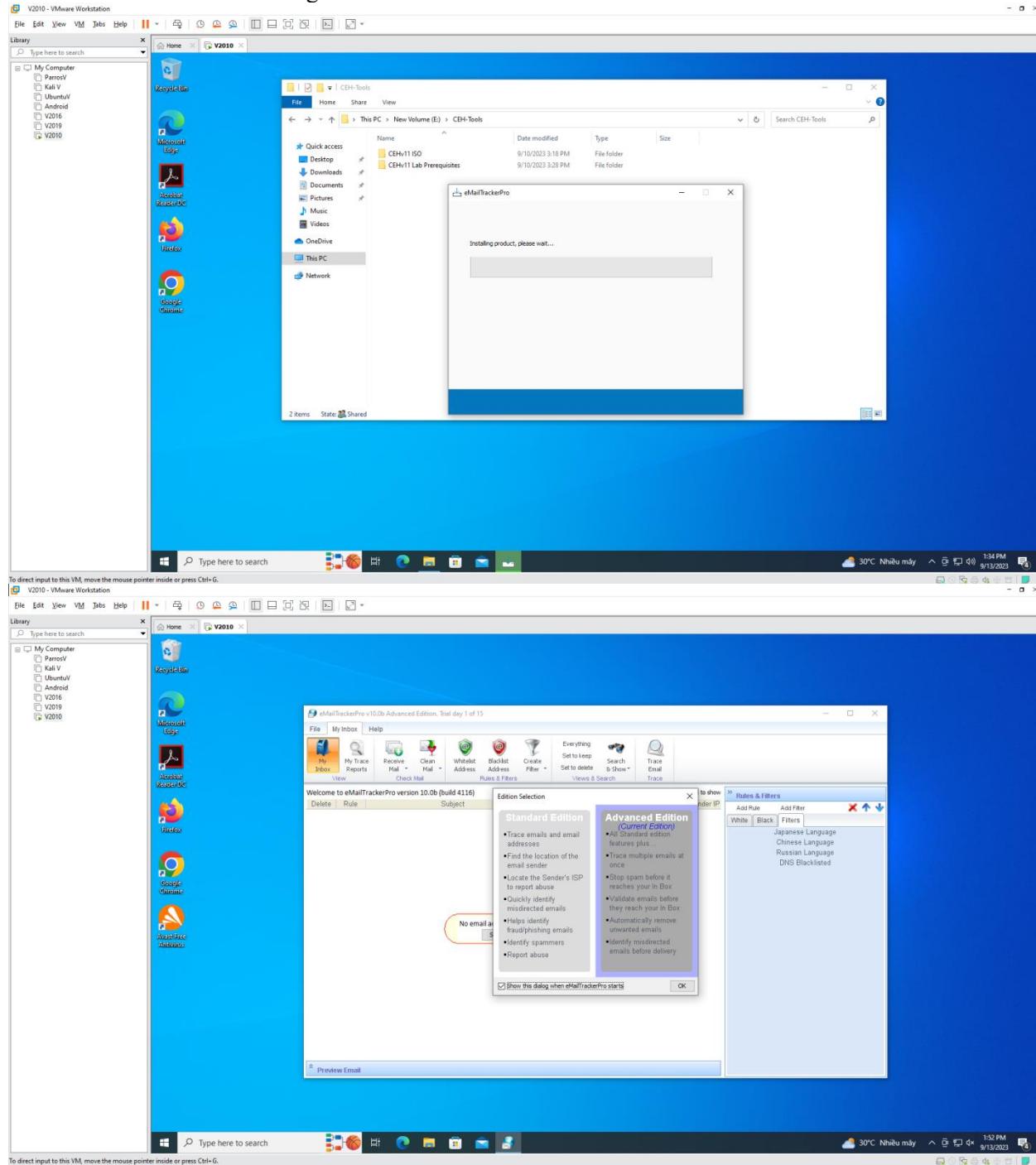
- Gather Information About a Target by Tracing Emails using eMail TrackerPro

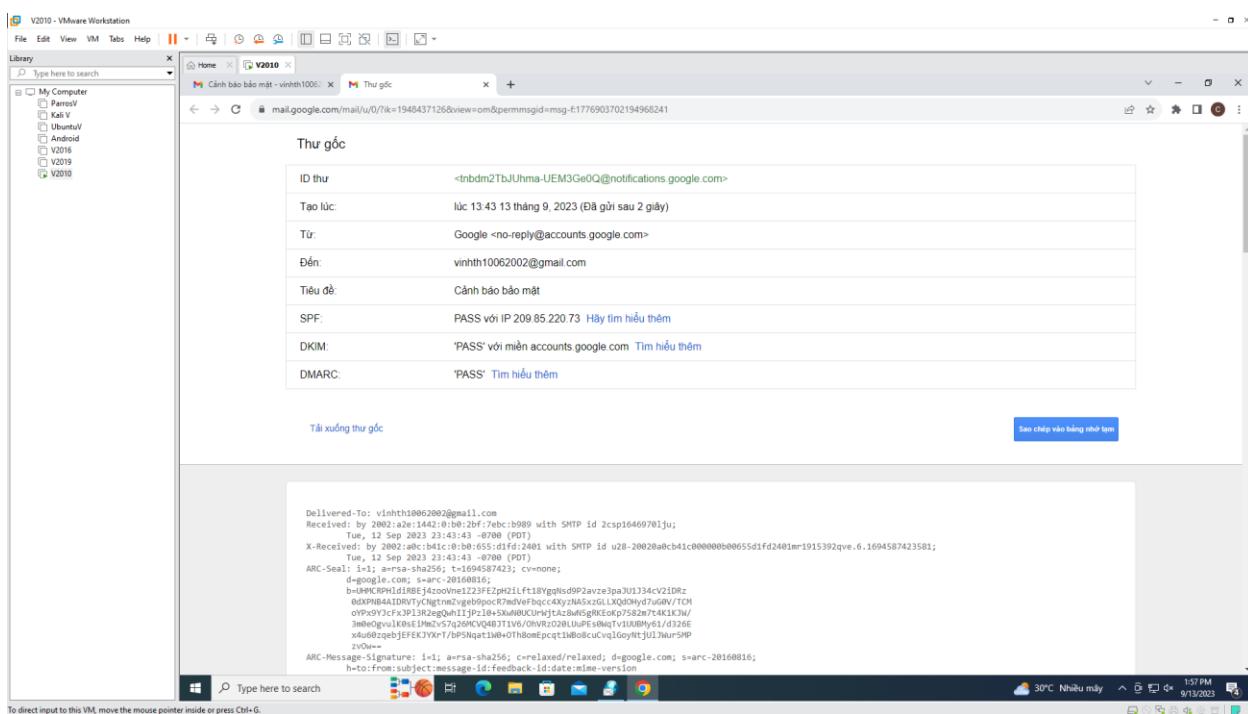
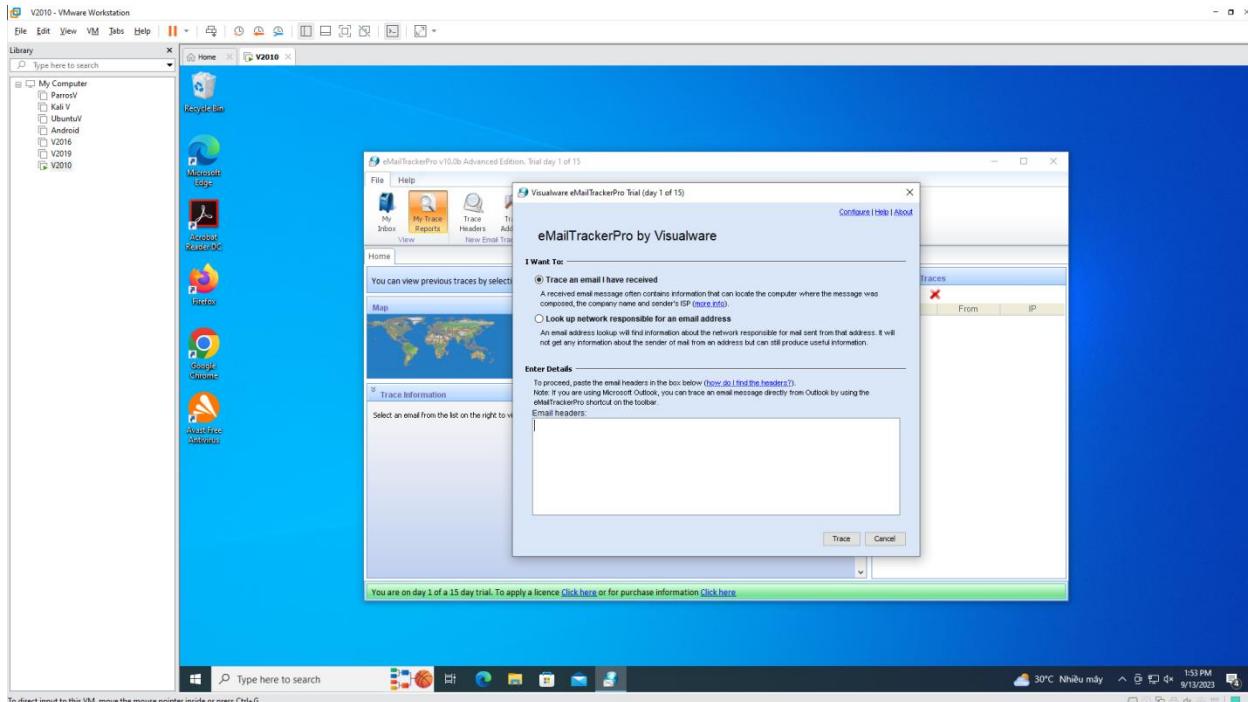
- Using Windows 10

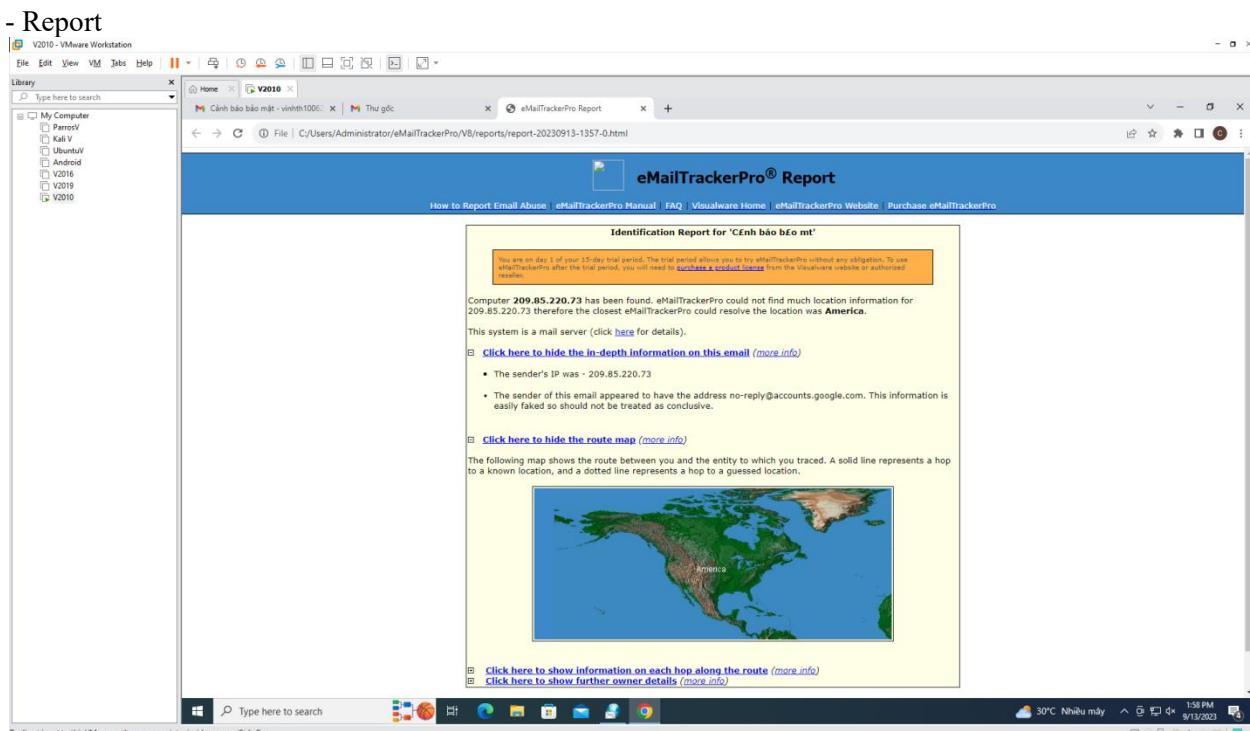
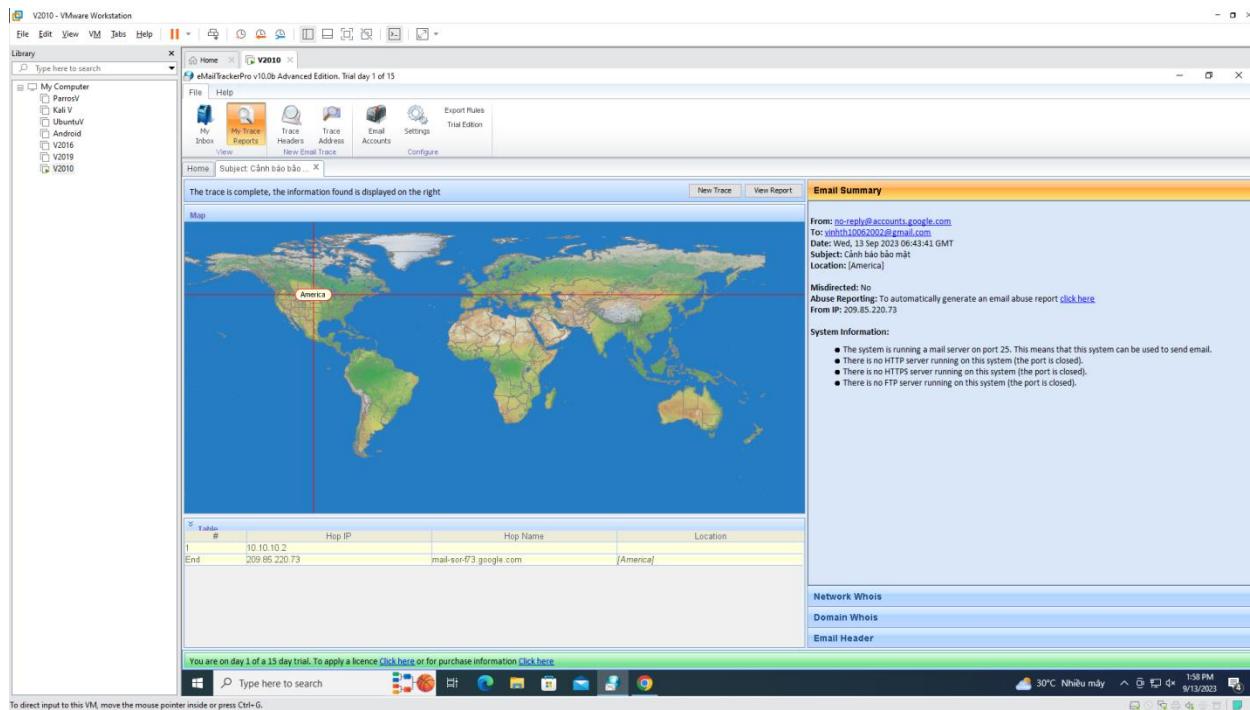
- Login with user Administrator



- Open File Explorer, navigate to E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro and install



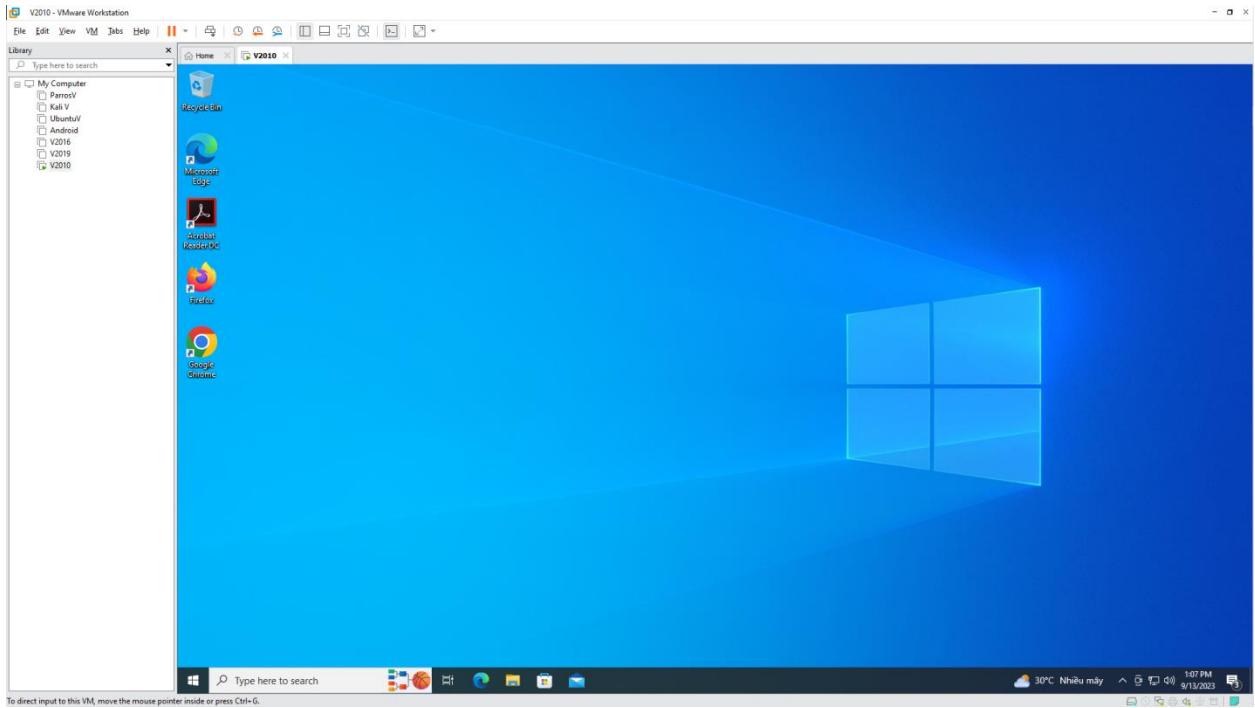




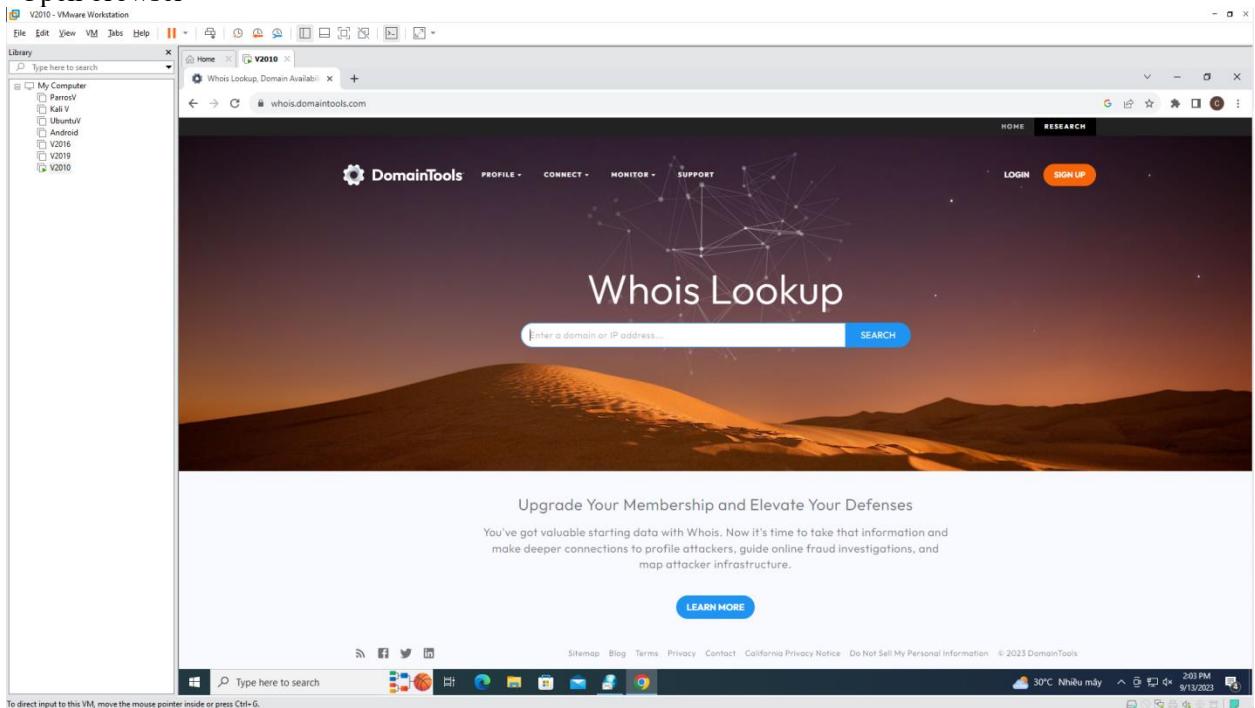
6. Perform Whois Footprinting

- Perform Whois lookup using DomainTools

- Using Windows 10
- Login with user Administrator



- Open browser



- search www.certifiedhacker.com

The image consists of three vertically stacked screenshots of the DomainTools website, specifically the Whois lookup page for the domain 'certifiedhacker.com'. Each screenshot shows a different view of the same information.

Screenshot 1 (Top): This view displays the main Whois Record for 'certifiedhacker.com'. It includes sections for Domain Profile, Registrar, Registrar Status, Name Servers, IP Address, IP Location, ASN, Domain Status, IP History, Registrar History, and Hosting History. A note at the bottom states 'Whois Record last updated on 2023-09-13'.

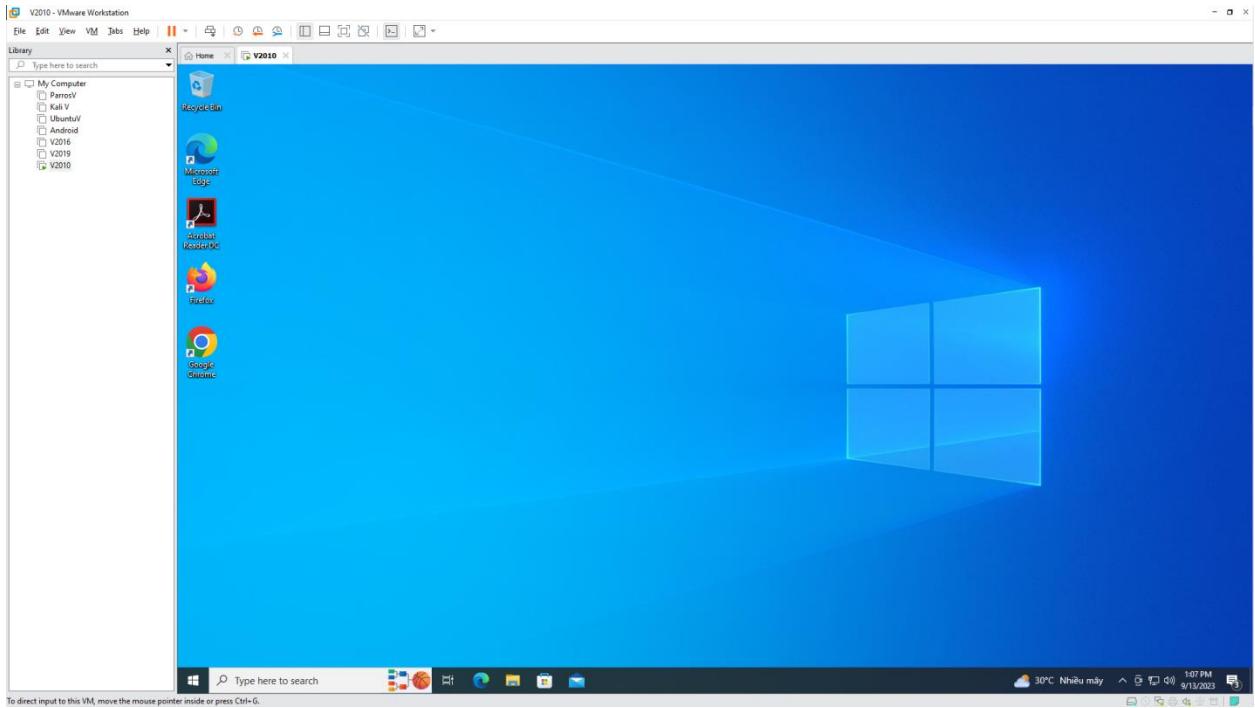
Screenshot 2 (Middle): This view provides a detailed breakdown of the Whois record, listing numerous specific fields such as Registry Domain ID, Registrant Name, Admin Name, Tech Name, and various contact details for Network Solutions, LLC. It also includes sections for 'Available TLDs' and a list of related domains.

Screenshot 3 (Bottom): This view is similar to Screenshot 2 but includes a sidebar on the right side. The sidebar contains links for 'View Whois' and 'Buy Domain' next to a list of related domains: 'CertifiedHacker.com', 'CertifiedHacker.net', 'CertifiedHacker.org', 'CertifiedHacker.info', 'CertifiedHacker.biz', and 'CertifiedHacker.tel'. The status of each domain is indicated by a colored square: green for 'Taken domain.', orange for 'Available domain.', and red for 'Deleted previously owned domain.'

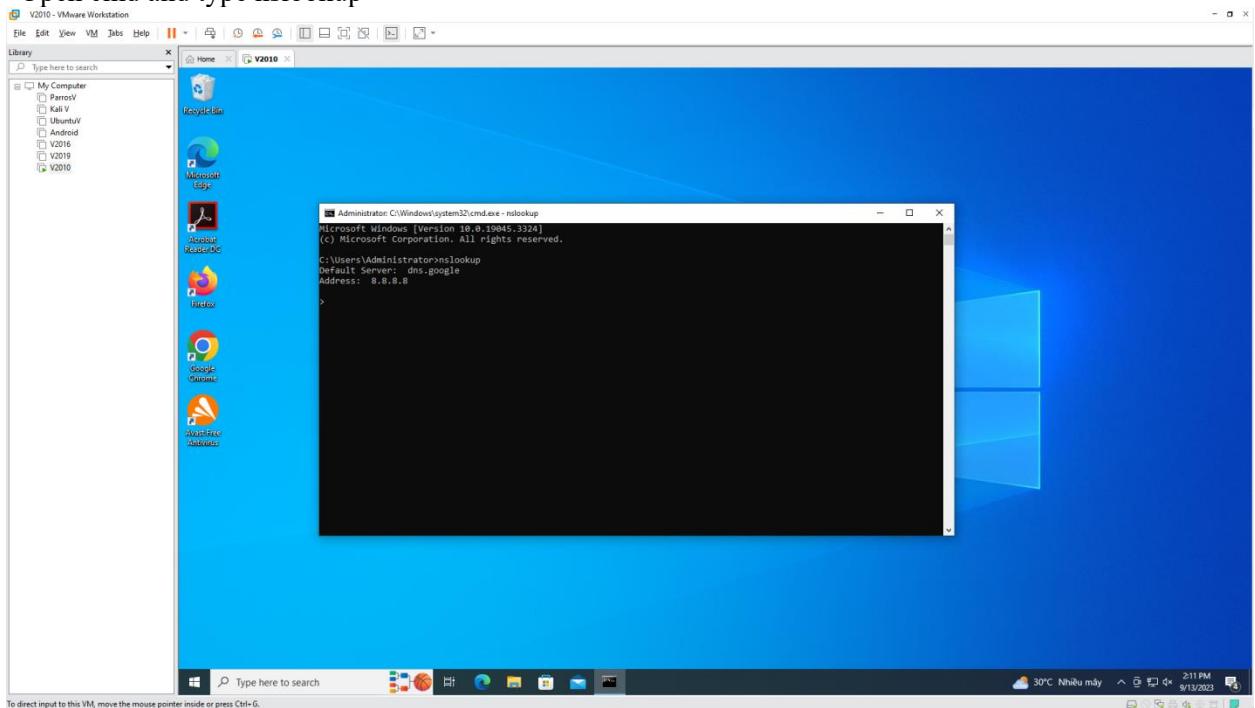
7. Perform DNS Footprinting

- Perform Whois lookup using DomainTools

- Using Windows 10
- Login with user Administrator

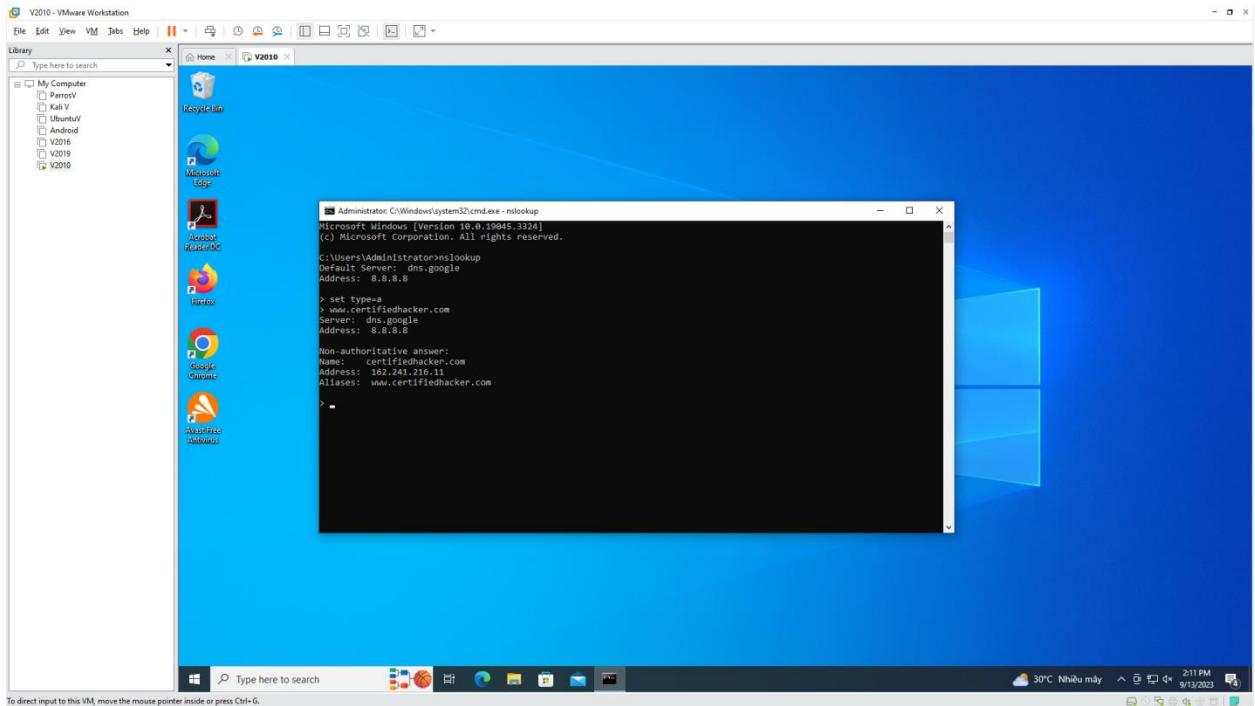


- Open cmd and type nslookup



- set type=a

- www.certifiedhacker.com



- set type cname
- www.certifiedhacker.com

The image shows two screenshots of a Windows 10 desktop environment within a VMware Workstation window. Both screenshots feature a blue Windows 10 desktop background with a taskbar at the bottom containing icons for File Explorer, Task View, Start, Action Center, and system status.

In the top screenshot, a Command Prompt window is open with the following command and output:

```
Administrator: C:\Windows\system32\cmd.exe - nslookup  
Microsoft Windows [Version 10.0.19045.3324]  
(c) Microsoft Corporation. All rights reserved.  
C:\Users\Administrator>nslookup  
Default Server: dns.google  
Address: 8.8.8.8  
  
> set type=a  
> www.certifiedhacker.com  
Server: dns.google  
Address: 8.8.8.8  
  
Non-authoritative answer:  
Name: certifiedhacker.com  
Address: 162.241.216.11  
Aliases: www.certifiedhacker.com  
  
> set type=cname  
> www.certifiedhacker.com  
Server: dns.google  
Address: 8.8.8.8  
  
Non-authoritative answer:  
www.certifiedhacker.com canonical name = certifiedhacker.com  
>
```

In the bottom screenshot, another Command Prompt window is open with the following command and output:

```
Administrator: C:\Windows\system32\cmd.exe - nslookup  
Key  
*** dns.google can't find cts: Non-existent domain  
> set type=a  
> ns1.bluehost.com  
Server: dns.google  
Address: 8.8.8.8  
  
Non-authoritative answer:  
Name: ns1.bluehost.com  
Address: 162.159.24.80
```

- open web browser

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

NSLOOKUP is a service to look up information in the DNS (Domain Name System [RFC1034, RFC1035, RFC1033]). The NSLOOKUP utility is a unix tool. If you want to learn more, here is the nslookup manual (man page).
 Basically, DNS maps domain names to IP addresses.
 Although this web online service can query a specific DNS server, in most cases it may be sufficient and convenient just to use the KLOTH.NET default nameserver "localhost"!127.0.0.1.
 To resolve an IP address by reverse lookup (get a computer's name if you only have its IP address), try to perform a PTR query instead of A query. This reverse lookup will only work if the IP address owner has inserted a PTR record in the DNS. The PTR information is informal only and it may mostly be true, but sometimes not. If you don't get a PTR information about a specific computer from a NSLOOKUP query, you may want to try our whois service to find out the owner of this IP address.
 Like the PTR, other records are also not mandatory: LOG, RP, TXT. They are not strictly required in the DNS and their content may be true or not.
 You can't trust on the LOC to locate a host, because most hosts don't have this record defined.

If you prefer dig over nslookup, you may try our dig service
 This page is also available in German, French and Portuguese. Enjoy.
 >>> If you would like to see this service in your or any other language, please send a translation.

PayPal donate If you like this service, please, consider to make a small donation to fund and continue this site. Thank you.

Link to www.kloth.net

Recommended books about Networking

Document URL: <http://www.kloth.net/services/nslookup.php>
 Copyright © 1999-2023 Raft D. Kloth, Ludwigsburg, DE (GRG software). <- hostmaster@kloth.net > (don't send spam)
 Created 1999-09-13 Last modified 2011-01-30 Your visit: 2023-09-13 (Wed) 07:19:05. It is the 256th day of this year.
 [Go to the top of this page] [...], to the index page]

30°C, Nhiều mây 2:19 PM 9/13/2023

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

NSLOOKUP is a service to look up information in the DNS (Domain Name System [RFC1034, RFC1035, RFC1033]). The NSLOOKUP utility is a unix tool. If you want to learn more, here is the nslookup manual (man page).
 Basically, DNS maps domain names to IP addresses.
 Although this web online service can query a specific DNS server, in most cases it may be sufficient and convenient just to use the KLOTH.NET default nameserver "localhost"!127.0.0.1.
 To resolve an IP address by reverse lookup (get a computer's name if you only have its IP address), try to perform a PTR query instead of A query. This reverse lookup will only work if the IP address owner has inserted a PTR record in the DNS. The PTR information is informal only and it may mostly be true, but sometimes not. If you don't get a PTR information about a specific computer from a NSLOOKUP query, you may want to try our whois service to find out the owner of this IP address.
 Like the PTR, other records are also not mandatory: LOG, RP, TXT. They are not strictly required in the DNS and their content may be true or not.
 You can't trust on the LOC to locate a host, because most hosts don't have this record defined.

If you prefer dig over nslookup, you may try our dig service
 This page is also available in German, French and Portuguese. Enjoy.
 >>> If you would like to see this service in your or any other language, please send a translation.

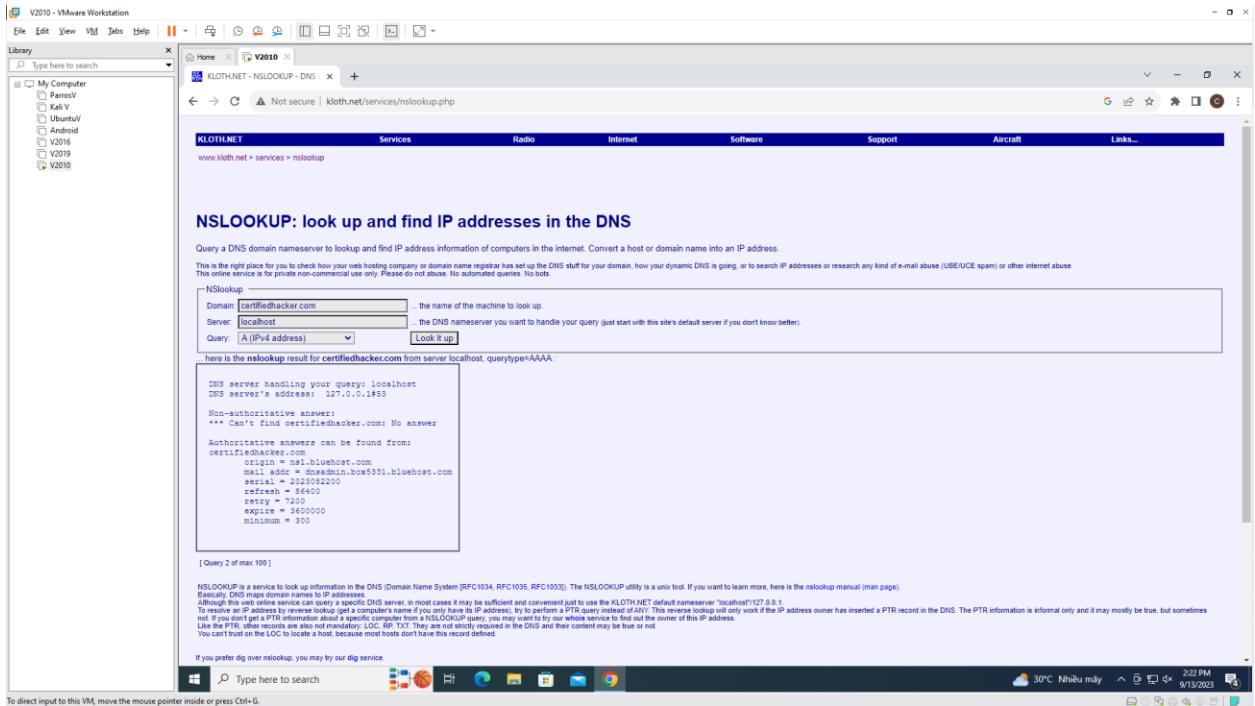
PayPal donate If you like this service, please, consider to make a small donation to fund and continue this site. Thank you.

Link to www.kloth.net

Recommended books about Networking

Document URL: <http://www.kloth.net/services/nslookup.php>
 Copyright © 1999-2023 Raft D. Kloth, Ludwigsburg, DE (GRG software). <- hostmaster@kloth.net > (don't send spam)
 Created 1999-09-13 Last modified 2011-01-30 Your visit: 2023-09-13 (Wed) 07:19:05. It is the 256th day of this year.
 [Go to the top of this page] [...], to the index page]

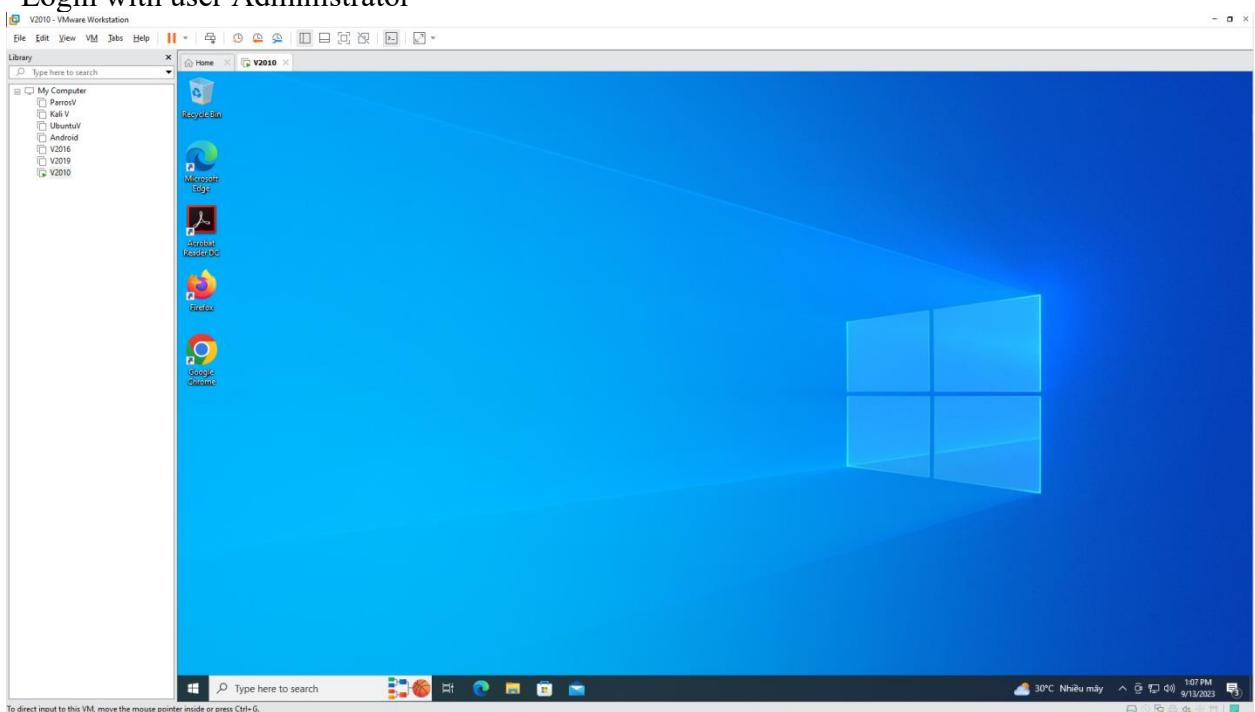
30°C, Nhiều mây 2:20 PM 9/13/2023



8. Perform Network Footprinting

- Locate network range

- Using Windows 10
- Login with user Administrator



- open browser

V2010 - VMware Workstation

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- search 162.241.216.11

V2010 - VMware Workstation

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

V2010 - VMware Workstation

File Edit View VM Help

Library Type here to search

My Computer

- PanosV
- Kali V
- UbuntuV
- Android
- V2016
- V2019
- V2019

ARIN Whois/RDAP - American Registry for Internet Numbers

Your IPv4 address is 42.119.149.96

Port 43 Whois whois.arin.net

Log in

Related Entities 1 Entity

Source Registry ARIN

Kind Org

Full Name Unified Layer

Handle BLUEH-2

Address 1958 South 950 East
Provo
UT
84606
United States

Roles Registrant

Registration Tue, 08 Aug 2006 17:53:22 GMT (Wed Aug 09 2006 local time)

Last Changed Fri, 31 Jan 2020 15:18:54 GMT (Fri Jan 31 2020 local time)

Self https://dap.arin.net/registry/entity/BLUEH-2

Alternate https://whois.arin.net/rest/org/BLUEH-2

Port 43 Whois whois.arin.net

Related Entities 2 Entities

Source Registry ARIN

Kind Group

Full Name Network Operations Center

Handle NOC2320-ARIN

Email abuse@bluehost.com

Telephone +1-801-765-9400

Organization Network Operations Center

Address 1958 South 950 East

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

V2010 - VMware Workstation

File Edit View VM Help

Library Type here to search

My Computer

- PanosV
- Kali V
- UbuntuV
- Android
- V2016
- V2019
- V2019

ARIN Whois/RDAP - American Registry for Internet Numbers

Your IPv4 address is 42.119.149.96

Port 43 Whois whois.arin.net

Log in

Related Entities 2 Entities

Source Registry ARIN

Kind Group

Full Name Network Operations Center

Handle NOC2320-ARIN

Email abuse@bluehost.com

Telephone +1-801-765-9400

Organization Network Operations Center

Address 1958 South 950 East
Provo
UT
84606
United States

Roles Abuse

Registration Wed, 01 Nov 2006 21:36:06 GMT (Thu Nov 02 2006 local time)

Last Changed Thu, 16 Mar 2023 13:33:35 GMT (Thu Mar 16 2023 local time)

Self https://dap.arin.net/registry/entity/NOC2320-ARIN

Alternate https://whois.arin.net/rest/poc/NOC2320-ARIN

Port 43 Whois whois.arin.net

Source Registry ARIN

Kind Group

Full Name EIG Network Operations

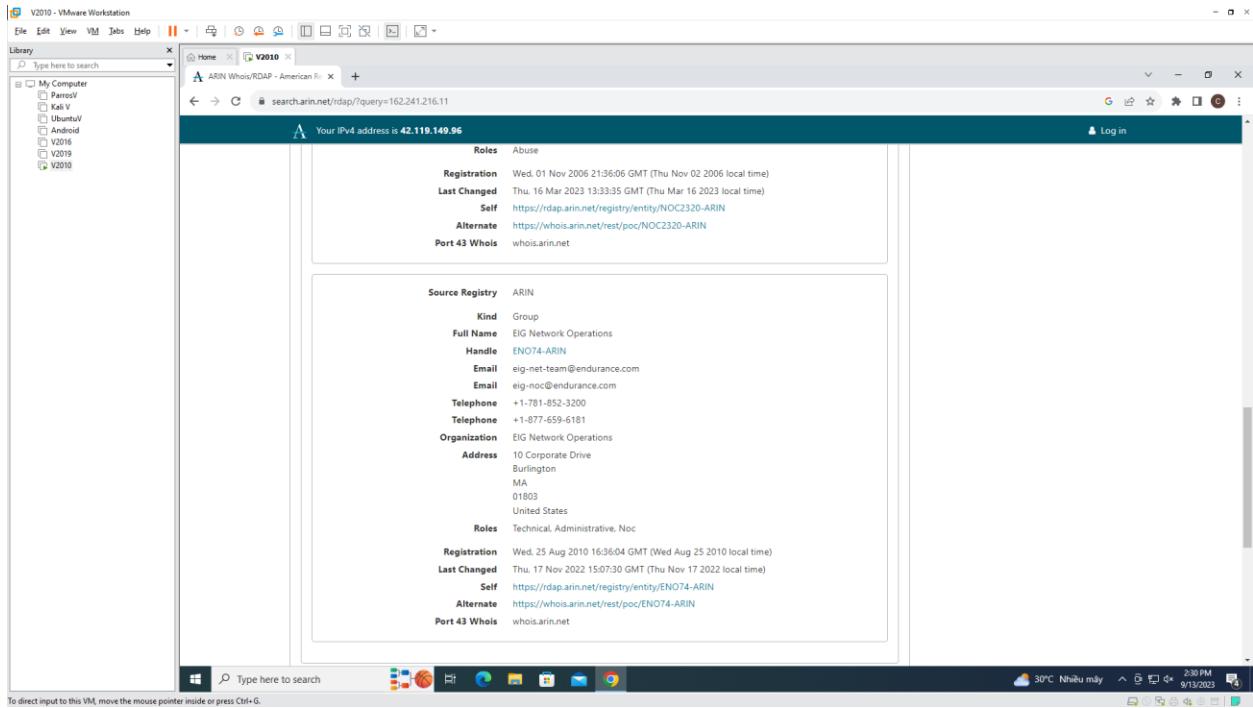
Handle EN074-ARIN

Email eig-net-team@endurance.com

Email eig-noc@endurance.com

Telephone +1-781-852-3200

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

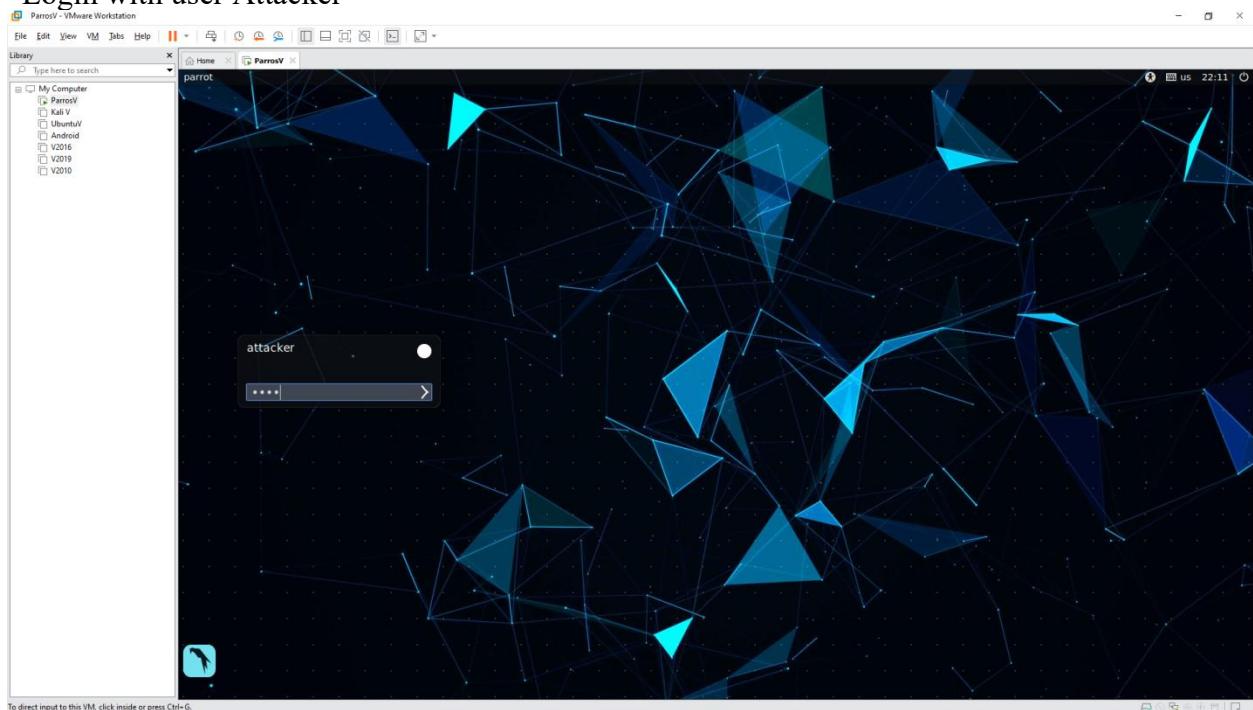


9. Perform Footprinting using Various Footprinting Tools

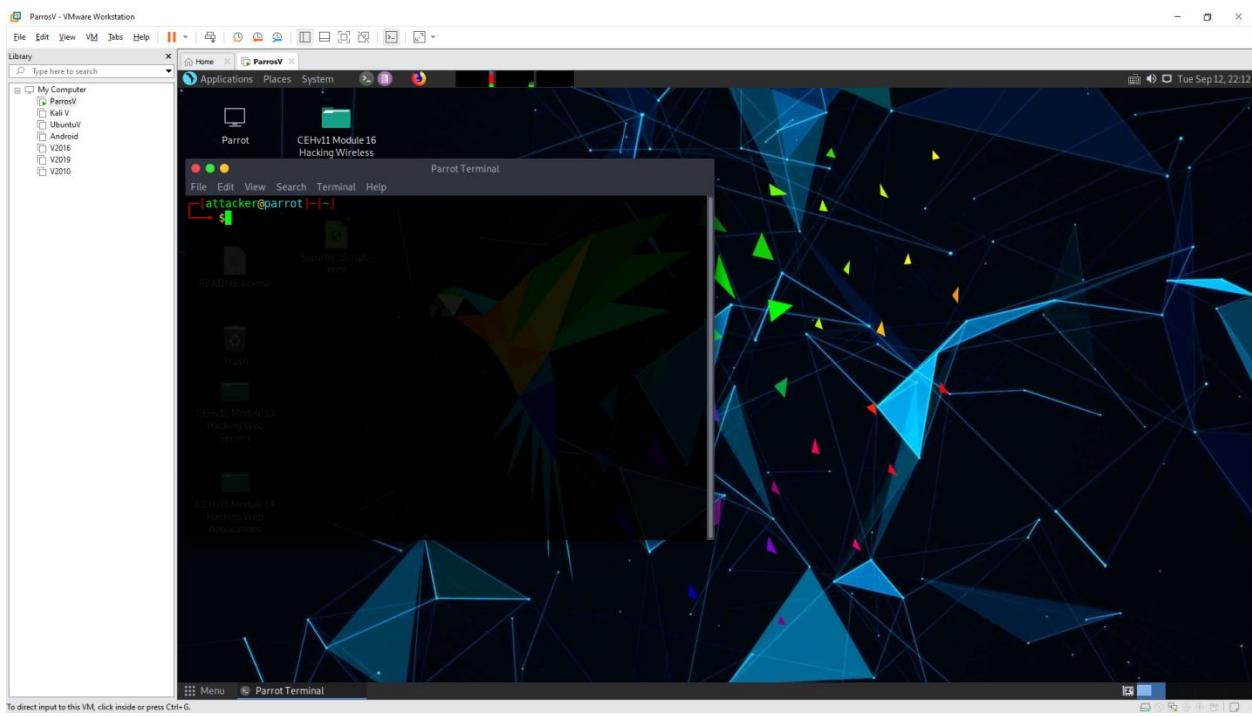
- Footprinting a Target using Recon-ng

- Using Parrot

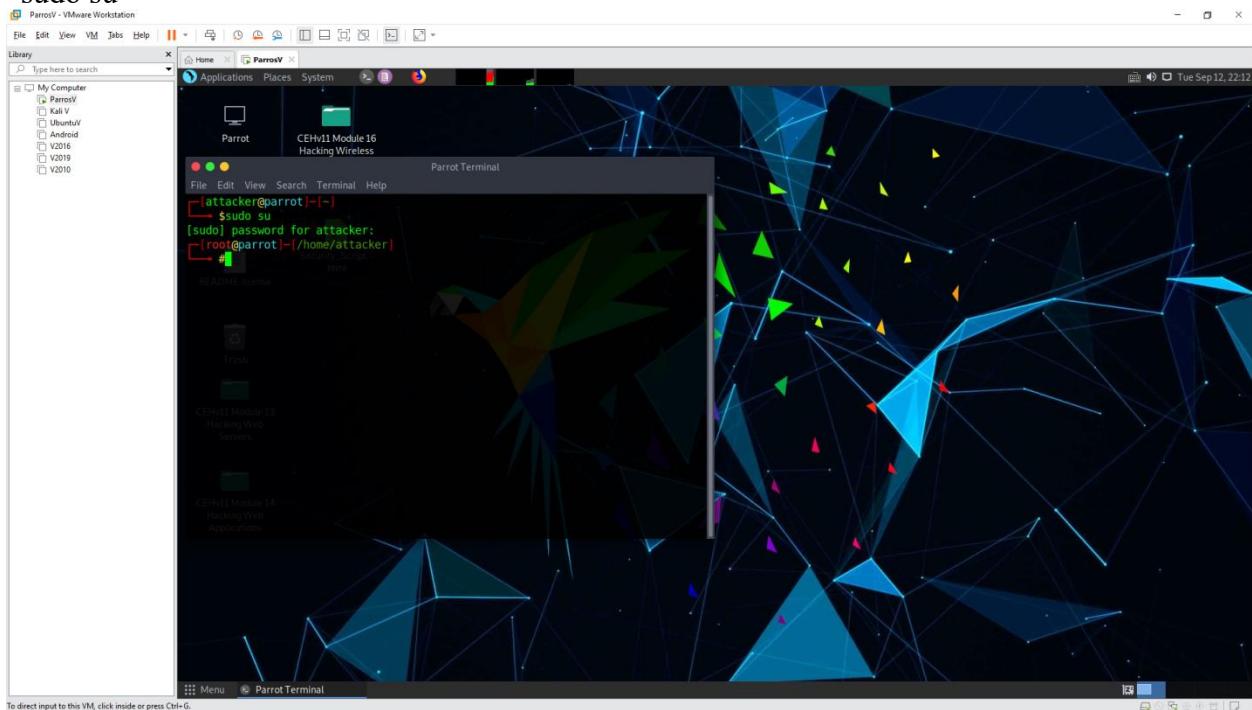
- Login with user Attacker



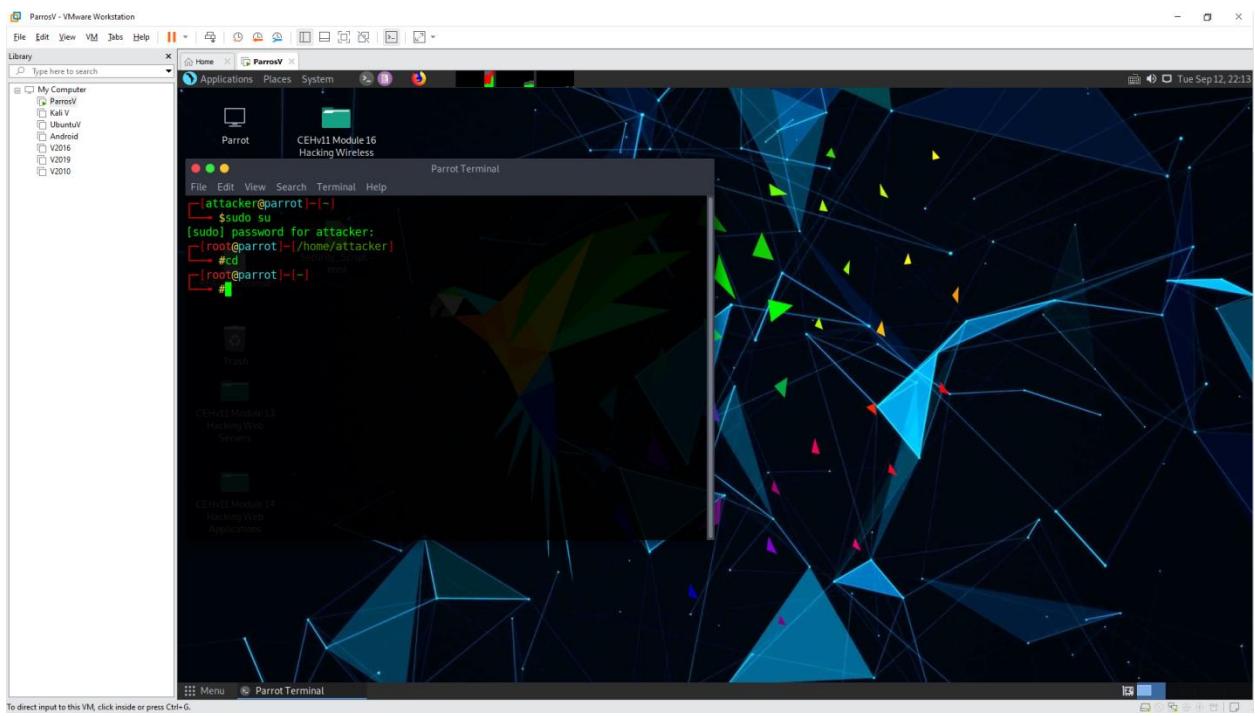
- Open terminal



- sudo su



- cd



- install osrframework

```

ParrotV - VMware Workstation
File Edit View VM Jobs Help || Application Places System Parrot Terminal
Library Type here to search
My Computer ParrotV Kali V UbuntuV Android V2016 V2019 V2010
File Edit View Search Terminal Help
[root@parrot ~]# pip3 install osrframework
Collecting osrframework
  Downloading osrframework-0.20.5.tar.gz (203 kB)
    |████████| 203 kB 1.6 MB/s
Collecting bs4
  Downloading bs4-0.0.1.tar.gz (1.1 kB)
Collecting cfscrape
  Downloading cfscrape-2.1.1-py3-none-any.whl (12 kB)
Requirement already satisfied: colorama in /usr/lib/python3/dist-packages (from osrframework) (0.4.3)
Collecting configparser
  Downloading configparser-0.0.0-py3-none-any.whl (19 kB)
Requirement already satisfied: decorator in /usr/lib/python3/dist-packages (from osrframework) (4.4.2)
Collecting ducky
  Downloading ducky-3.2.0-py3-none-any.whl (5.0 kB)
Requirement already satisfied: networkx in /usr/lib/python3/dist-packages (from osrframework) (2.4)
Collecting oauthlib
  Downloading oauthlib-3.2.2-py3-none-any.whl (151 kB)
    |████████| 151 kB 13.5 MB/s
Collecting pyexcel==0.2.1
  Downloading pyexcel-0.2.1.zip (63 kB)
    |████████| 63 kB 3.4 MB/s
Collecting pyexcel_ods==0.1.0
  Downloading pyexcel_ods-0.1.0.tar.gz (11 kB)
Collecting pyexcel_xls==0.1.0
  Downloading pyexcel_xls-0.1.0.zip (11 kB)
Collecting pyexcel_xlsx==0.1.0
  Downloading pyexcel_xlsx-0.1.0.tar.gz (5.8 kB)
Collecting python-emailahoy3
  Downloading python-emailahoy3-0.1.0.tar.gz (5.0 kB)
Collecting python-whois
  Downloading python-whois-0.8.0.tar.gz (109 kB)
    |████████| 109 kB 33.7 MB/s
Requirement already satisfied: pyyaml in /usr/lib/python3/dist-packages (from osrframework) (5.3.1)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from osrframework) (2.23.0)

To direct input to this VM, click inside or press Ctrl-G.
ParrotV - VMware Workstation
File Edit View VM Jobs Help || Application Places System Parrot Terminal
Library Type here to search
My Computer ParrotV Kali V UbuntuV Android V2016 V2019 V2010
File Edit View Search Terminal Help
[root@parrot ~]# CDE/1/Module 16
2023-09-13 04:16:27.382997      24 results obtained:
Sheet Name: Objects recovered (2023-9-13.4h16m).
+-----+-----+
| com.i3visio.Domain | com.i3visio.IPV4 |
+-----+-----+
| eccouncil.com       | 104.18.22.3   |
| eccouncil.org       | 104.18.8.180  |
| eccouncil.org.uk    | 3.64.163.50  |
| eccouncil.net       | 208.91.197.27 |
| eccouncil.us        | 208.91.197.27 |
| eccouncil.in        | 162.241.85.161|
| eccouncil.eu        | 91.195.241.232|
| eccouncil.tv        | 66.129.123.226|
| eccouncil.cn        | 129.226.173.83|
| eccouncil.pk        | 104.21.23.138 |
| eccouncil.ir        | 185.143.234.120|
| eccouncil.tn        | 104.21.8.104  |
| eccouncil.co        | 3.64.163.50  |
| eccouncil.me        | 34.102.136.180|
| eccouncil.exposed   | 208.91.197.27 |
| eccouncil.cz        | 89.185.225.244|
+-----+-----+
To direct input to this VM, click inside or press Ctrl-G.

```