Lab #1:

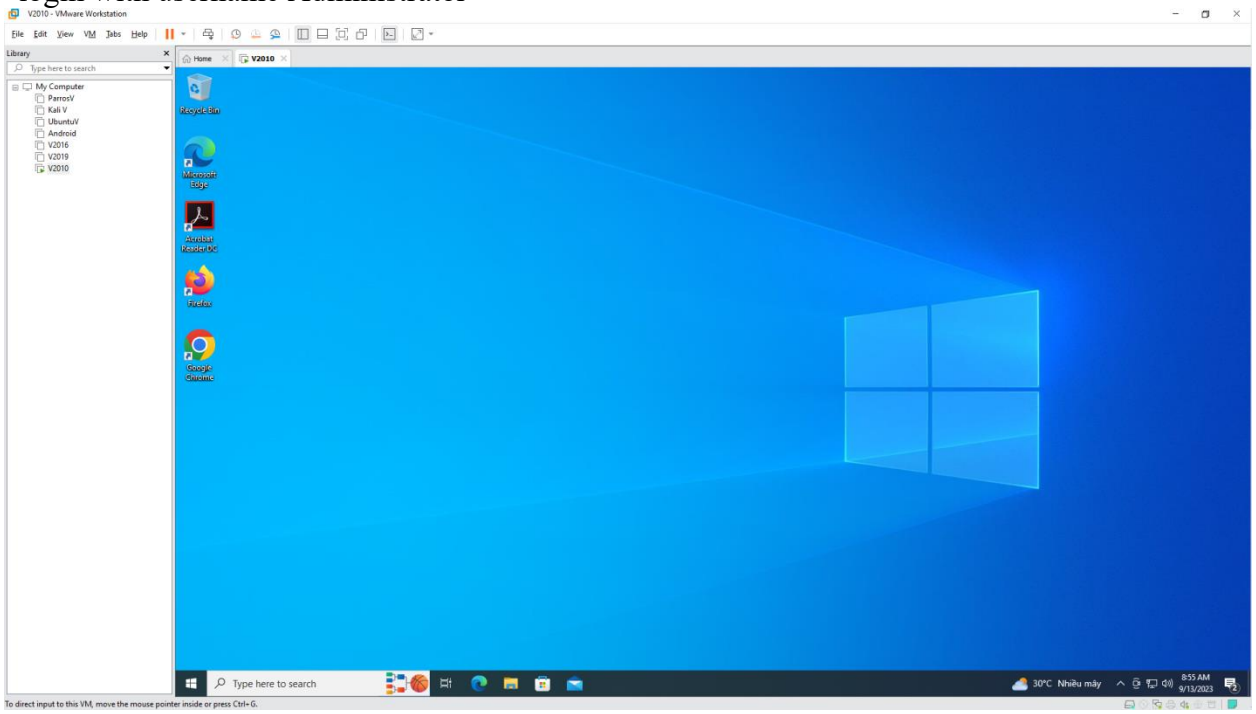
Course Name: Ethical Hacking and Offensive Security(HOD401)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 13/09/2023

Lab Tasks:

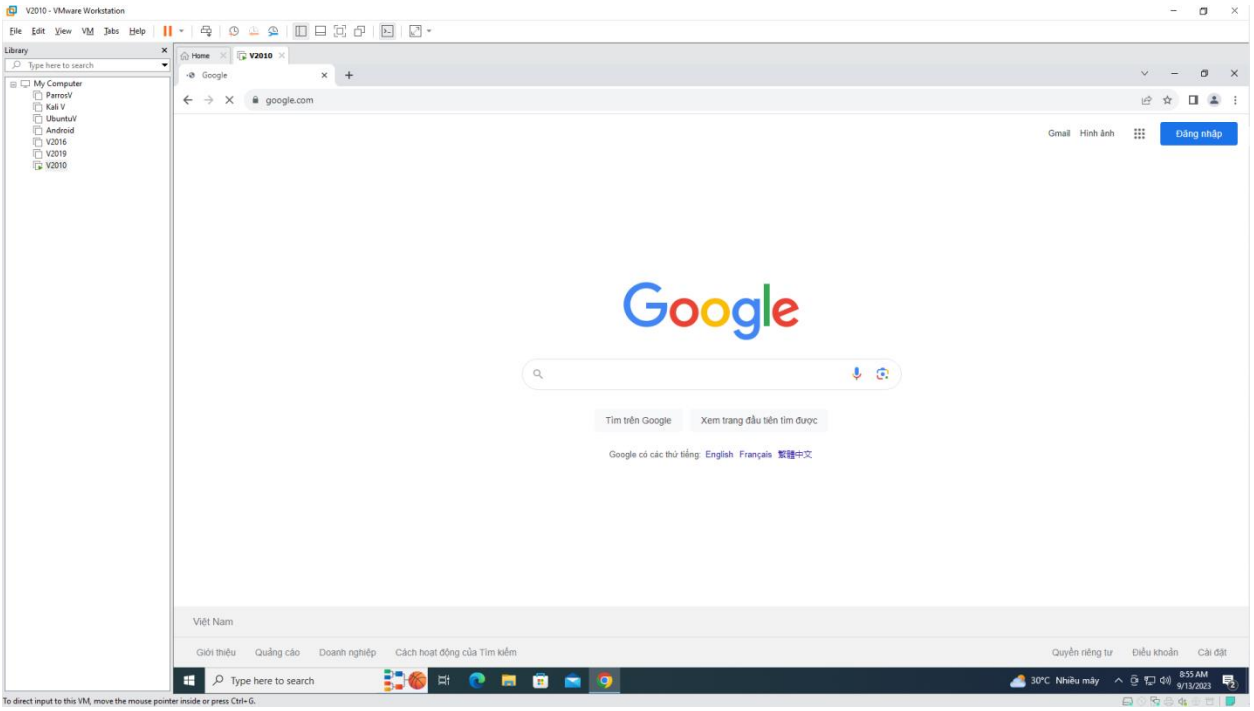
1. Perform Footprinting Through Search Engines

- Gather Information using Advanced Google Hacking Techniques

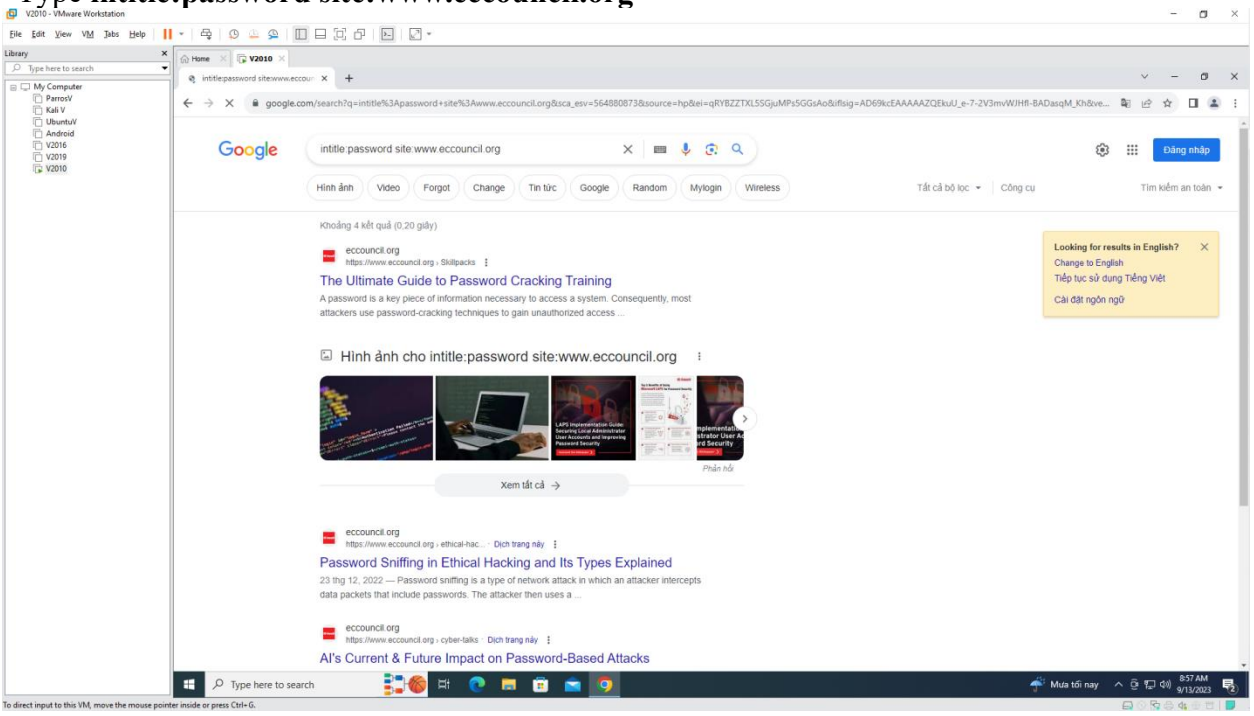
- using Windows 10
- login with username Administrator



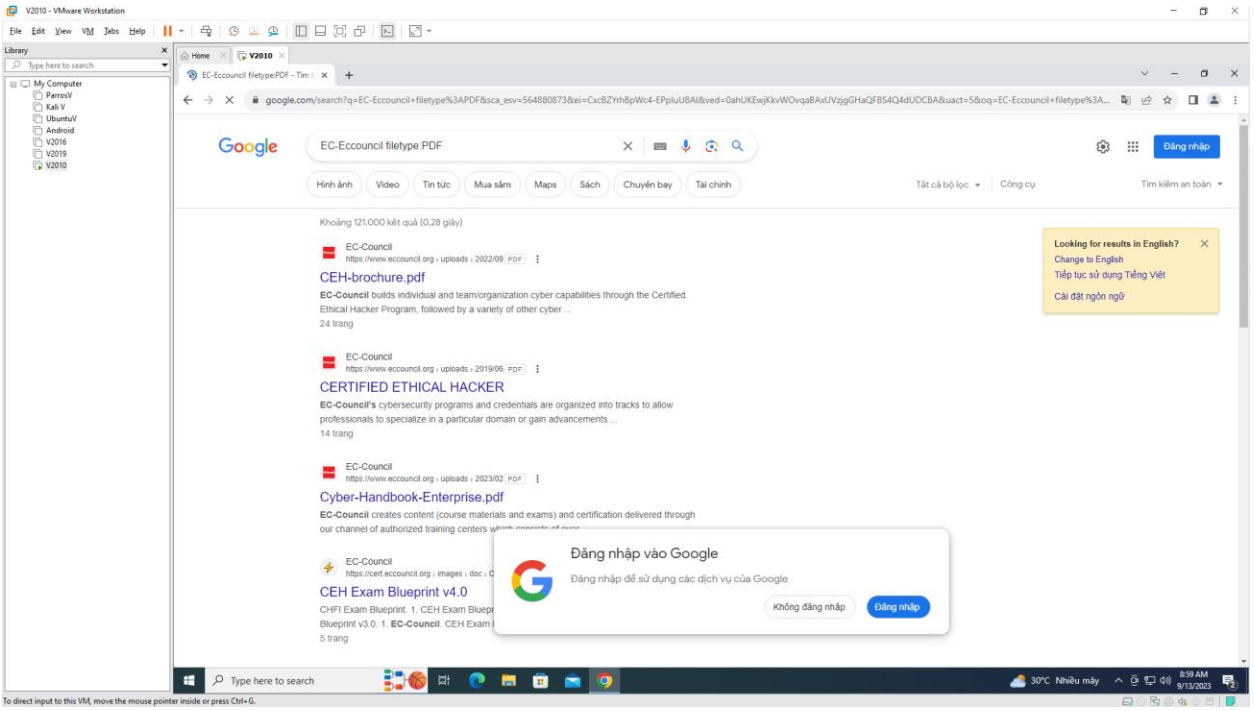
- Open website



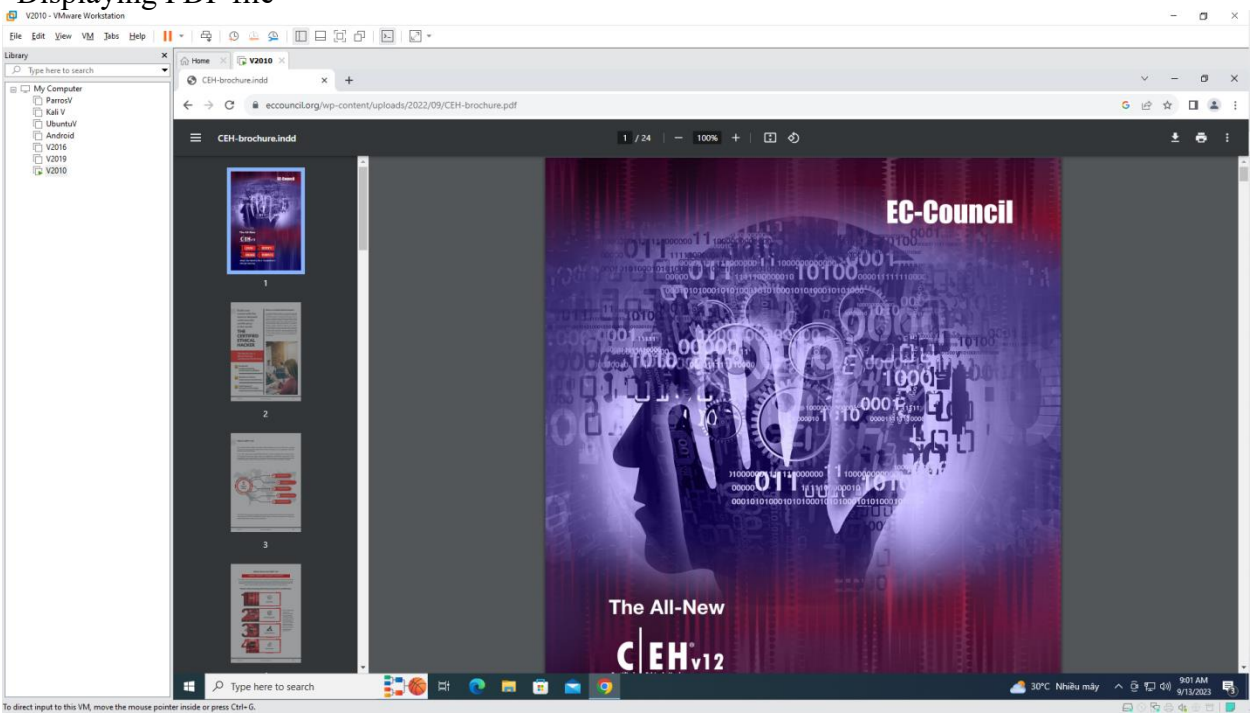
- Type **intitle:password site:www.eccouncil.org**



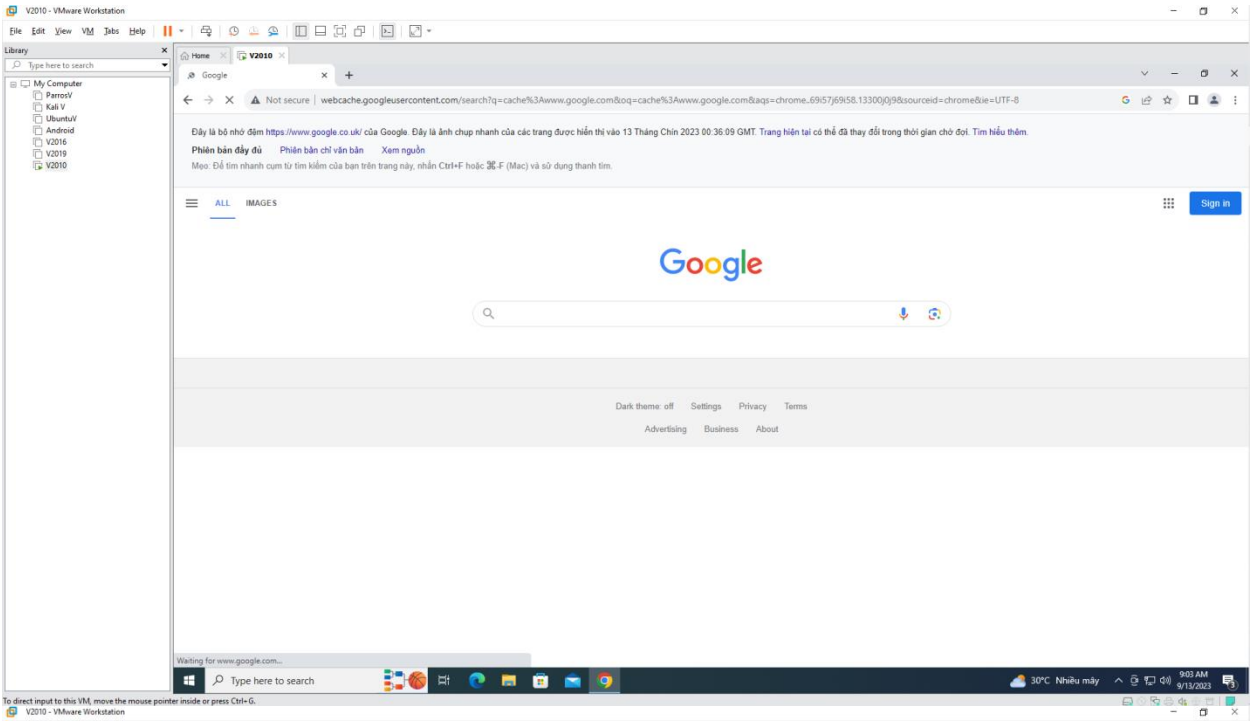
- EC-Council filetype:PDF

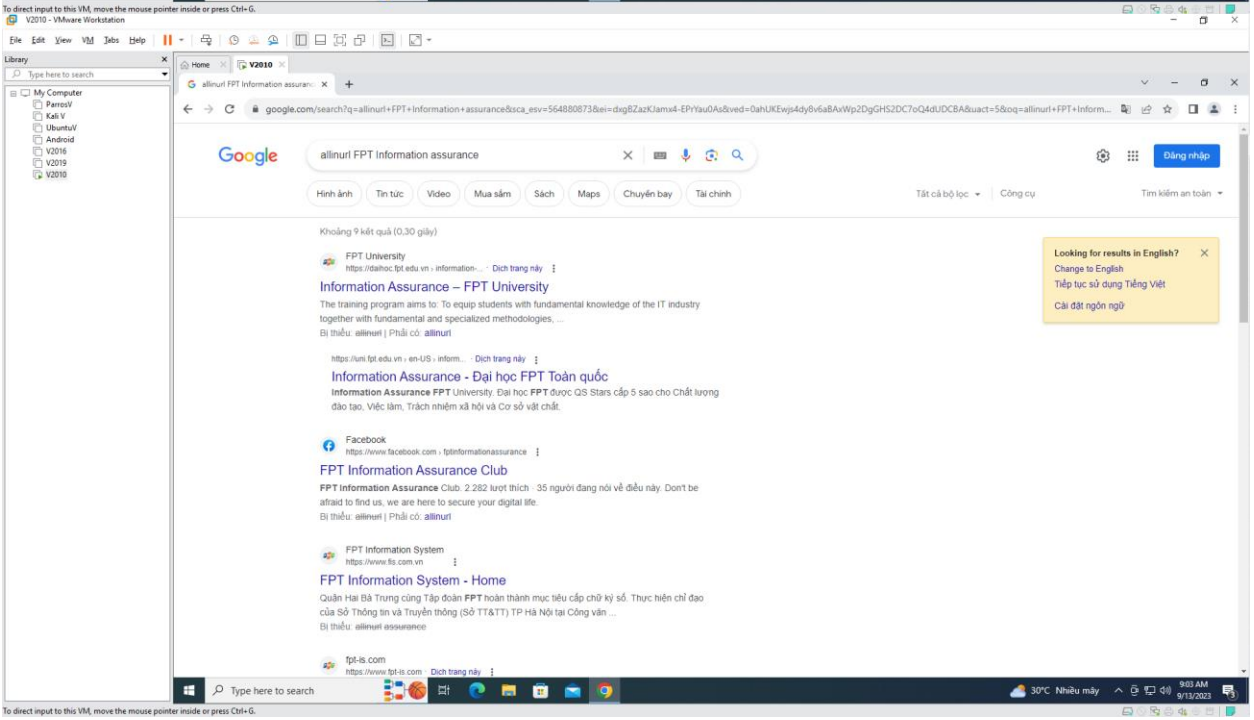


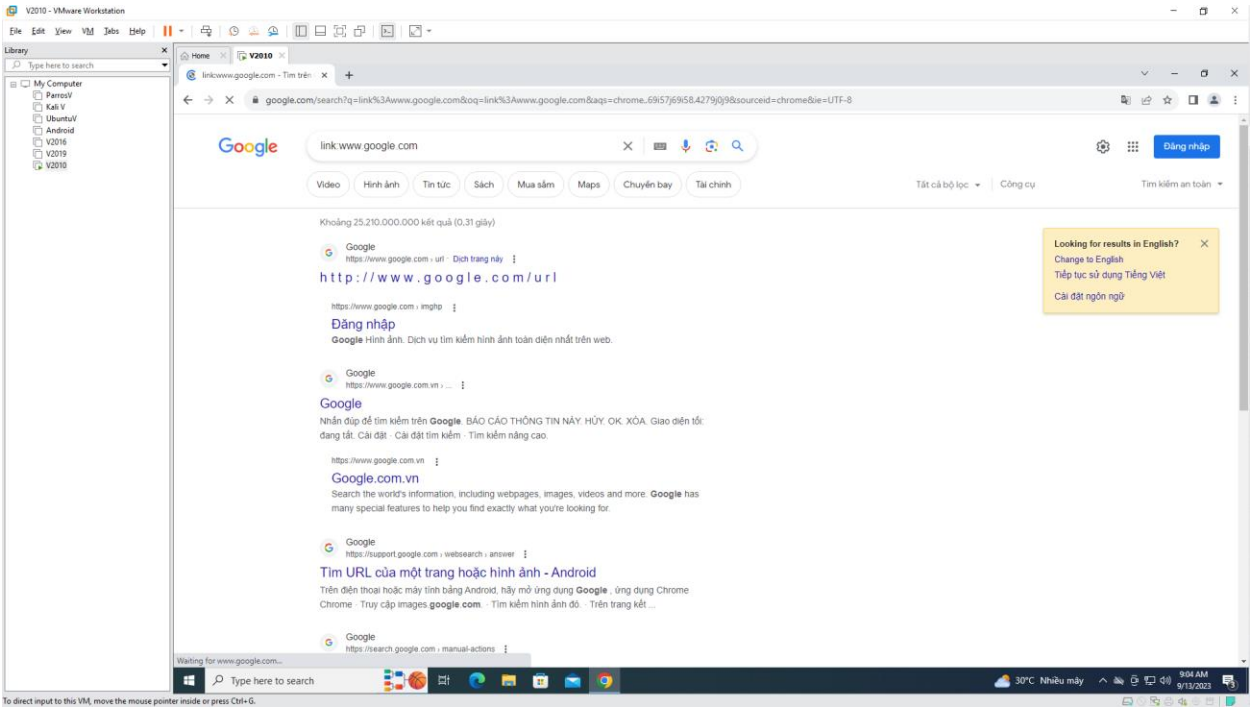
- Click on any link from result
- Displaying PDF file



- Another advanced search


V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
Google
Not secure | webcache.googleusercontent.com/search?q=cache%3Awww.google.com&oq=cache%3Awww.google.com&aqs=chrome..69i57j69i58.13300j0j9&sourceid=chrome&ie=UTF-8
Đây là bộ nhớ đệm https://www.google.co.uk/ của Google. Đây là ảnh chụp nhanh của các trang được hiển thị vào 13 Tháng Chín 2023 00:36:09 GMT. Trang hiện tại có thể đã thay đổi trong thời gian chờ đợi. Tìm hiểu thêm.
Phiên bản đầy đủ Phiên bản chỉ văn bản Xem nguồn
Mẹo: Để tìm nhanh cụm từ tìm kiếm của bạn trên trang này, nhấn Ctrl+F hoặc ⌘-F (Mac) và sử dụng thanh tìm.
ALL IMAGES
Sign in
Google
Dark theme: off Settings Privacy Terms
Advertising Business About
Waiting for www.google.com...
Type here to search
30°C Nhiều mây
9:03 AM
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 Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
allinurl FPT Information assuranc
google.com/search?q=allinurl+FPT+Information+assurance&sca_esv=564880873&ei=dxgBZazKJamx4-EPrYau0As&ved=0ahUKEwjs4dy8v6aBAxWp2DgGHS2DC7oQ4dUDCBA&uact=5&oq=allinurl+FPT+Inform...
Google
allinurl FPT Information assurance
Đăng nhập
Hình ảnh Tin tức Video Mua sắm Sách Maps Chuyến bay Tài chính
Tất cả bộ lọc Công cụ Tìm kiếm an toàn
Khoảng 9 kết quả (0,30 giây)
FPT University
https://daihoc.fpt.edu.vn › information-... · Dịch trang này
Information Assurance – FPT University
The training program aims to: To equip students with fundamental knowledge of the IT industry together with fundamental and specialized methodologies, ...
Bị thiếu: allinurl | Phải có: allinurl
https://uni.fpt.edu.vn › en-US › inform... · Dịch trang này
Information Assurance - Đại học FPT Toàn quốc
Information Assurance FPT University. Đại học FPT được QS Stars cấp 5 sao cho Chất lượng đào tạo, Việc làm, Trách nhiệm xã hội và Cơ sở vật chất.
Facebook
https://www.facebook.com › fptinformationassurance
FPT Information Assurance Club
FPT Information Assurance Club. 2.282 lượt thích · 35 người đang nói về điều này. Don't be afraid to find us, we are here to secure your digital life.
Bị thiếu: allinurl | Phải có: allinurl
FPT Information System
https://www.fis.com.vn
FPT Information System - Home
Quận Hai Bà Trưng cùng Tập đoàn FPT hoàn thành mục tiêu cấp chữ ký số. Thực hiện chỉ đạo của Sở Thông tin và Truyền thông (Sở TT&TT) TP Hà Nội tại Công văn ...
Bị thiếu: allinurl assurance
fpt-is.com
https://www.fpt-is.com · Dịch trang này
Looking for results in English?
Change to English
Tiếp tục sử dụng Tiếng Việt
Cài đặt ngôn ngữ
Type here to search
30°C Nhiều mây
9:03 AM
9/13/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

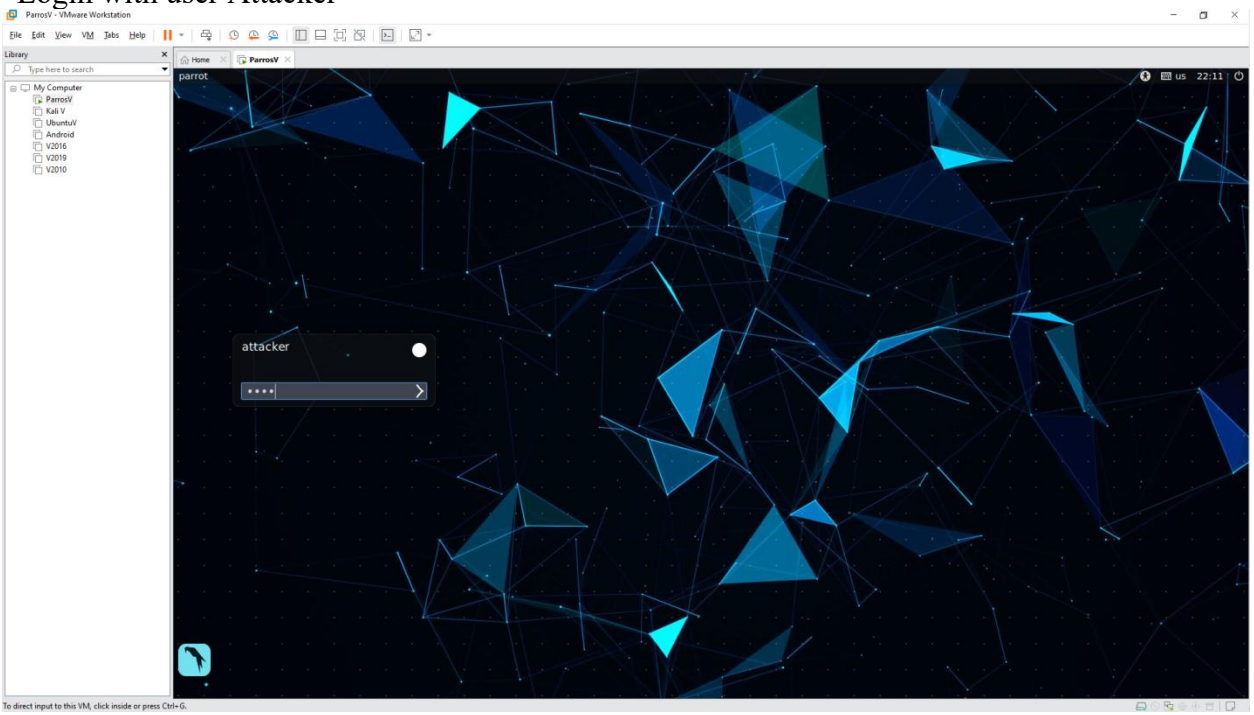


2. Perform Footprinting Through Web Services

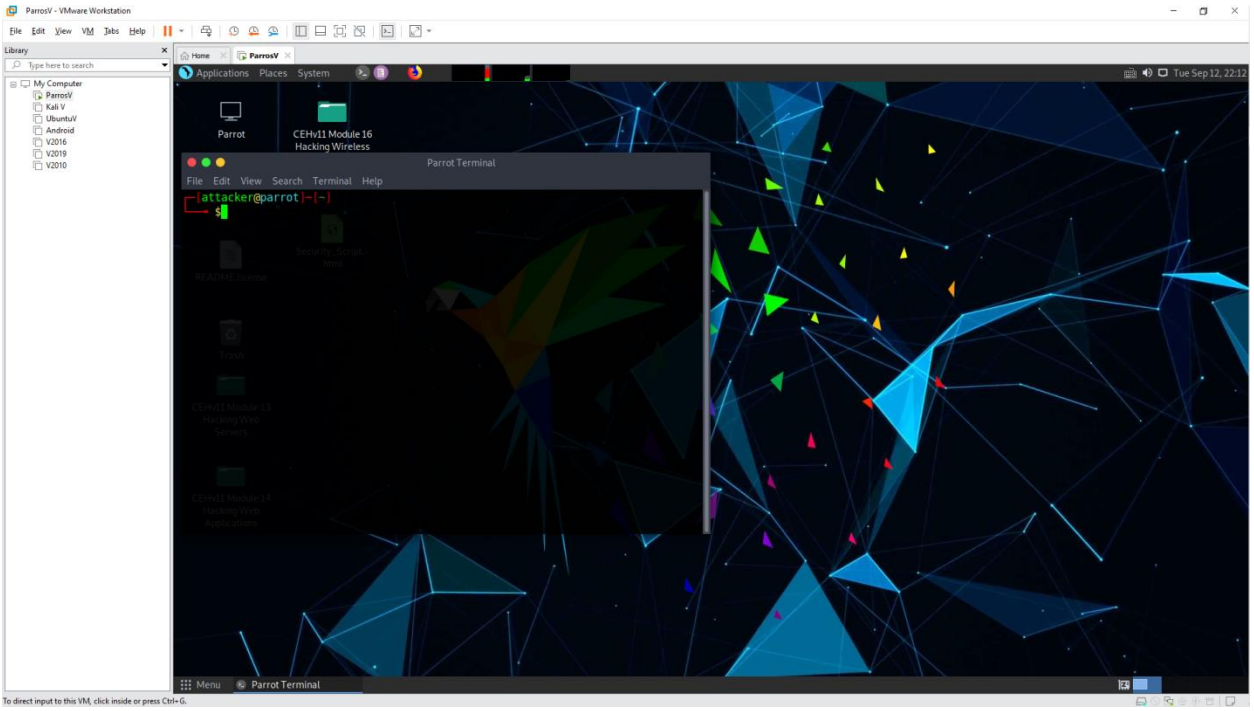
- Gather an Email List using the Harvester

- Using Parrot

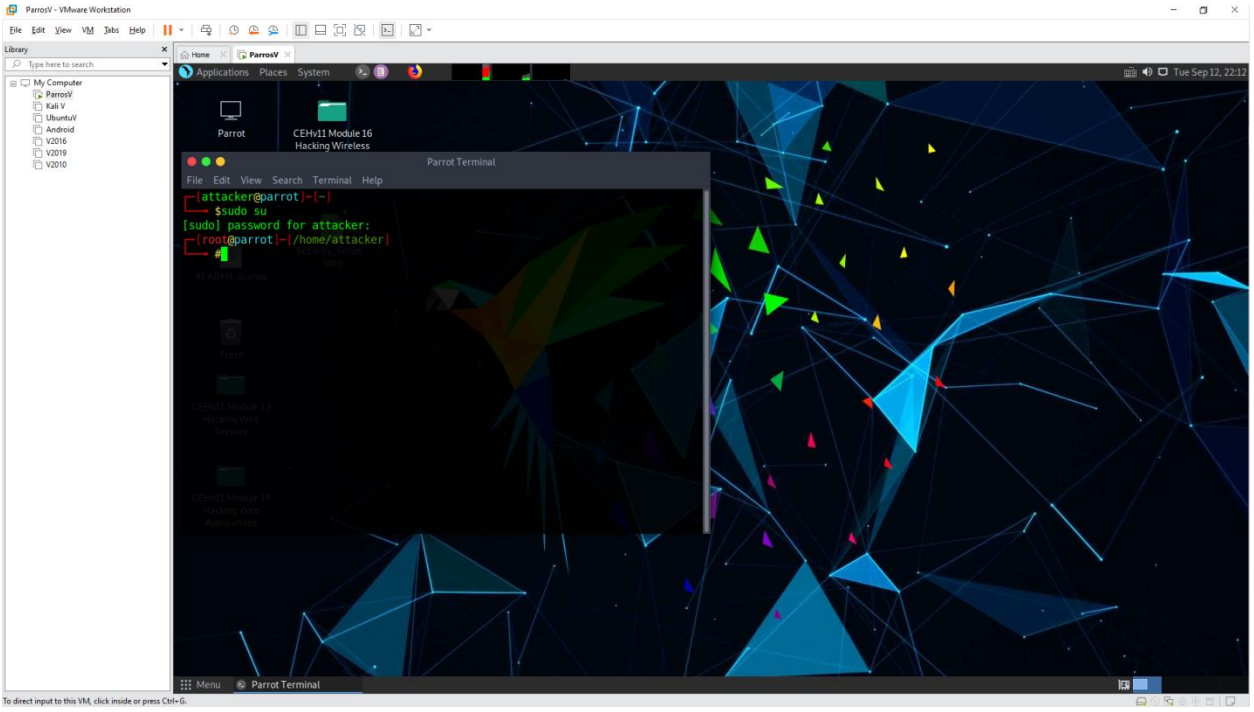
- Login with user Attacker



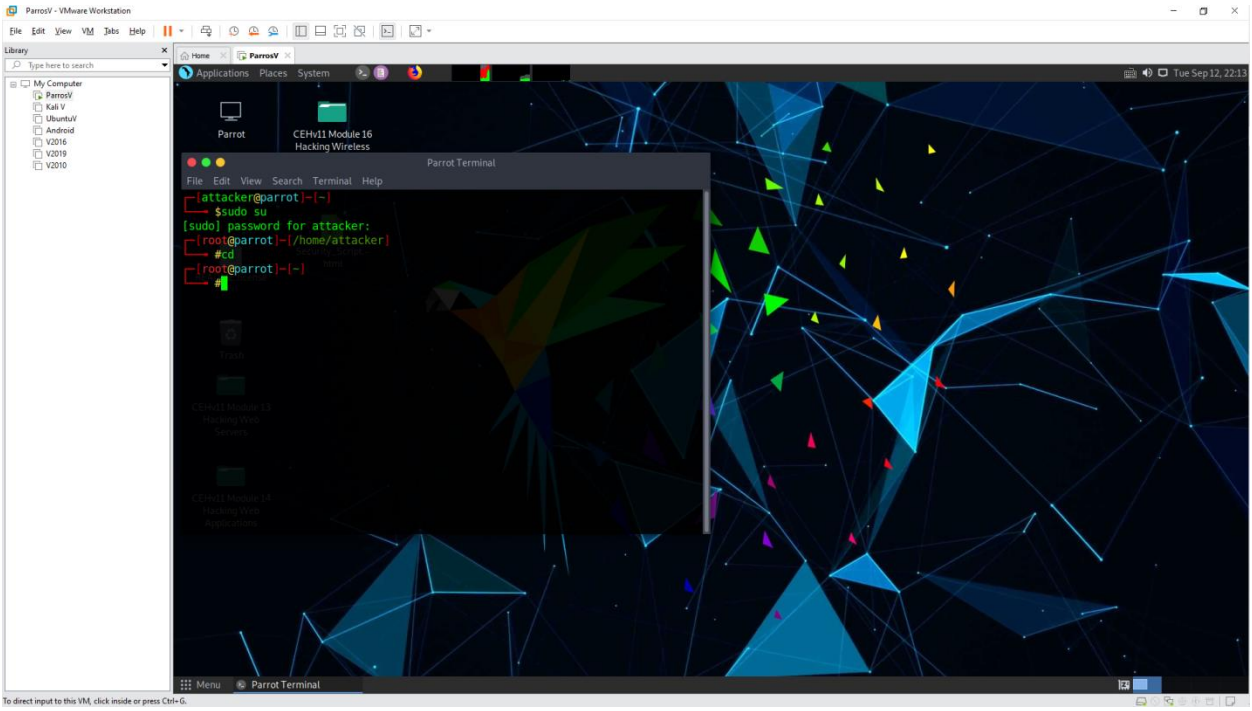
- Open terminal


ParrosV - VMware Workstation
Parrot
CEHv11 Module 16
Hacking Wireless
Parrot Terminal
[attacker@parrot]-[~]
$

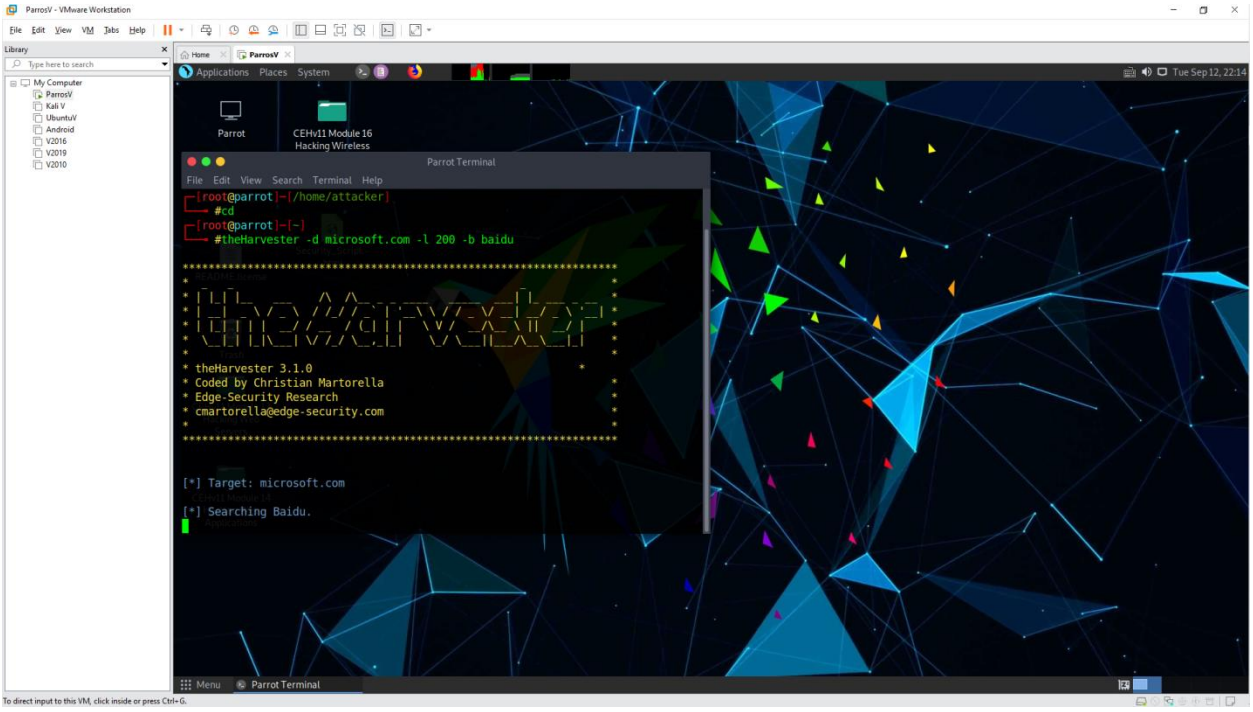
- sudo su

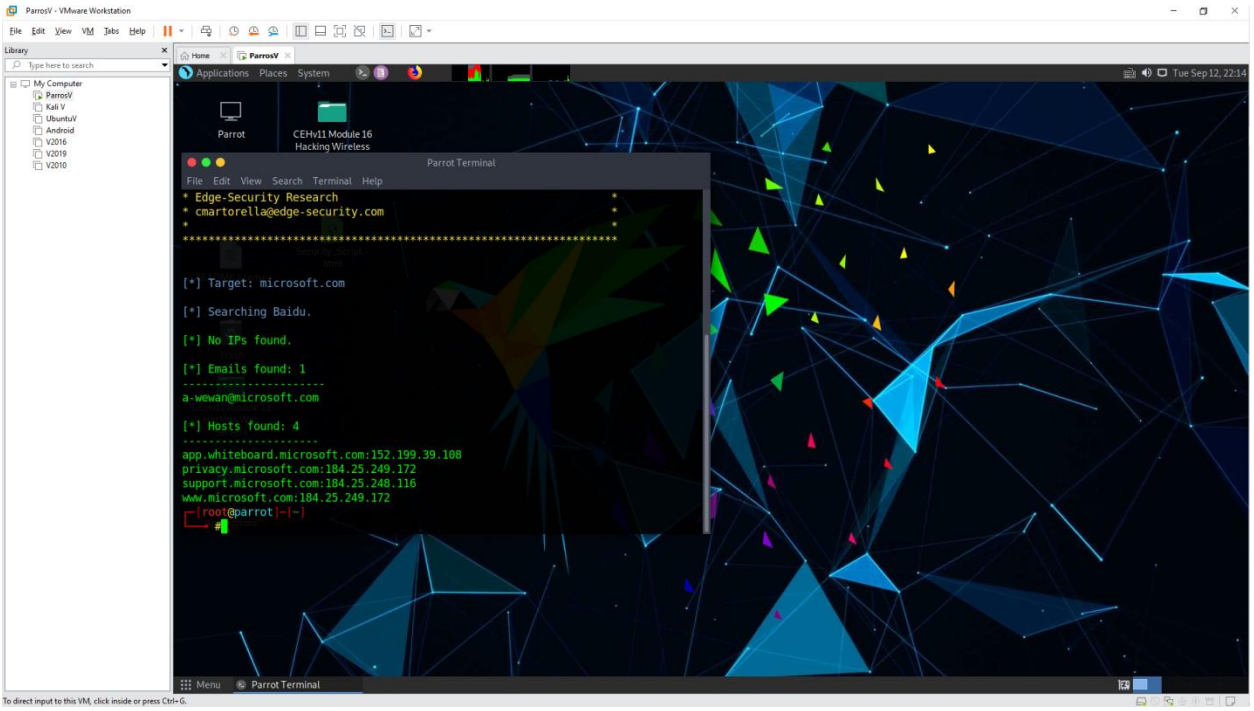

ParrosV - VMware Workstation
Parrot
CEHv11 Module 16
Hacking Wireless
Parrot Terminal
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#

- cd



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



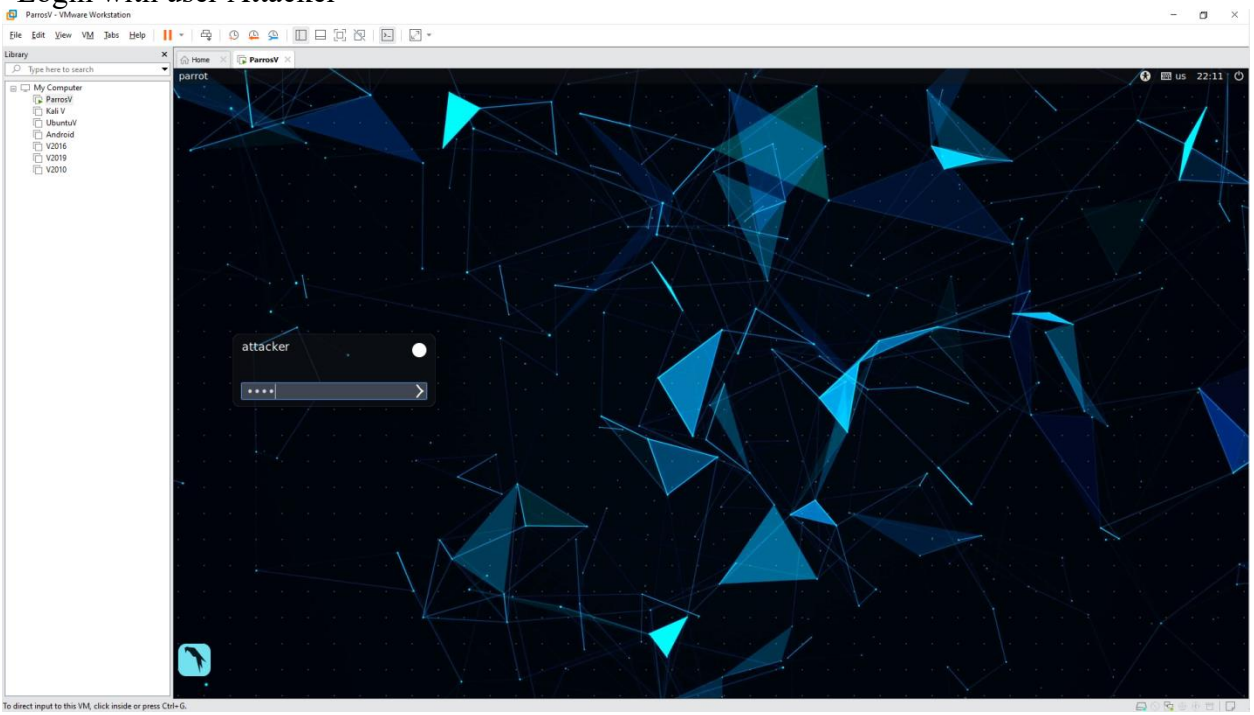


3. Perform Footprinting Social Networking Sites

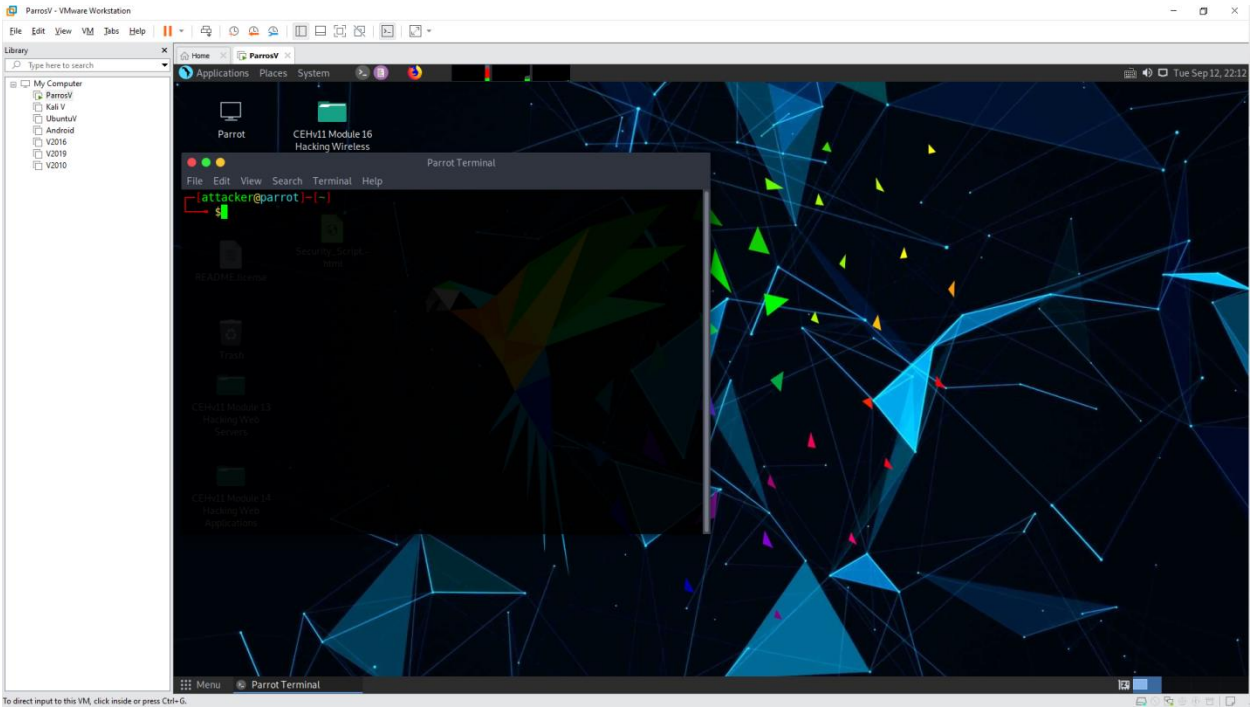
- Gather Employees' Information from LinkedIn using theHavester

- Using Parrot

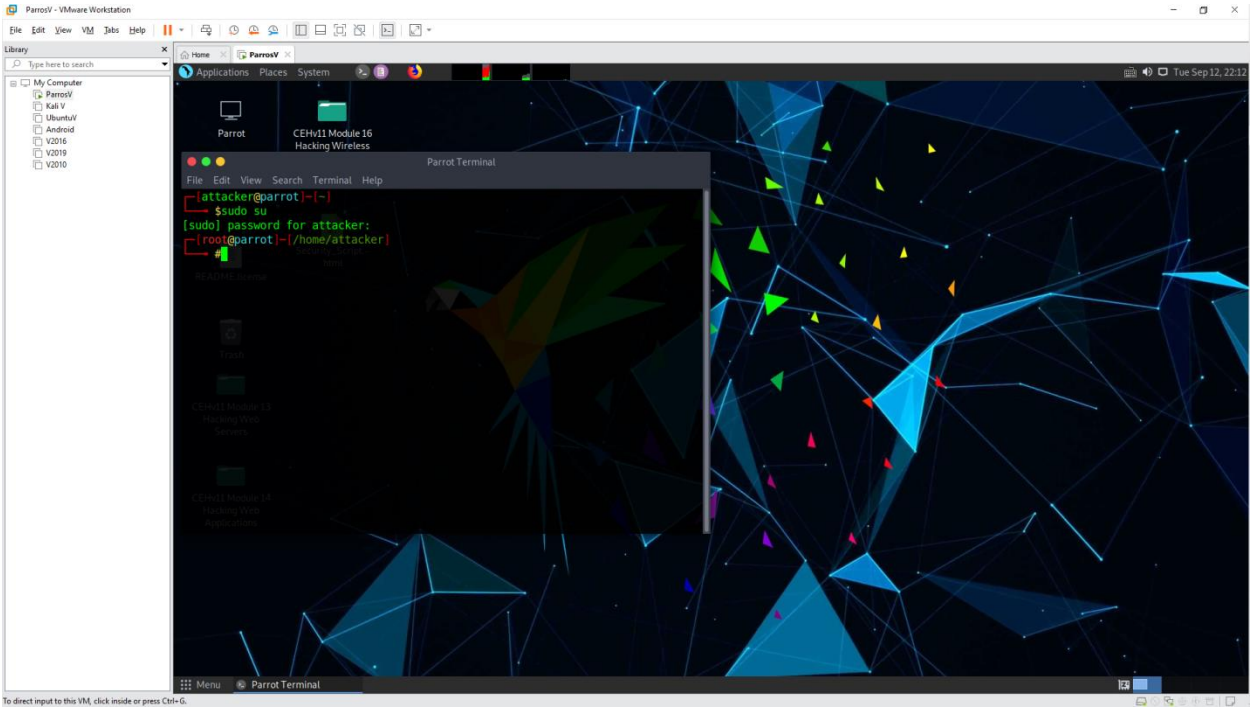
- Login with user Attacker



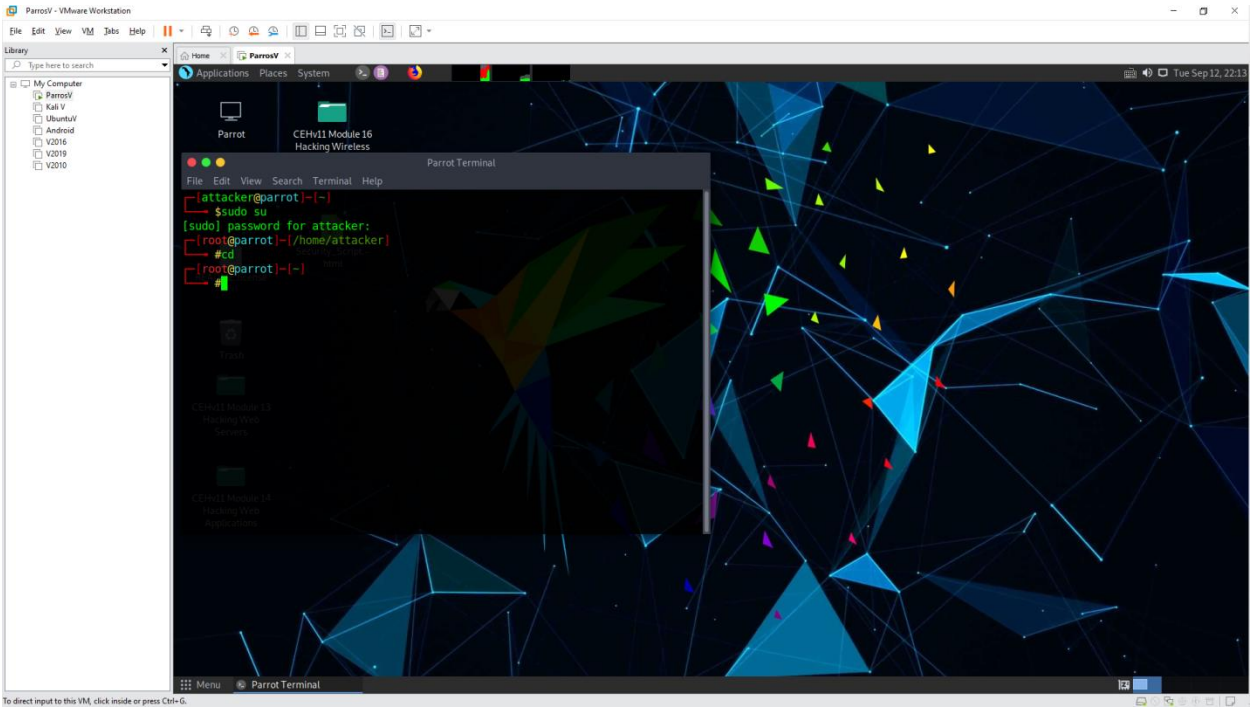
- Open terminal


ParrosV - VMware Workstation
Parrot
CEHv11 Module 16
Hacking Wireless
Parrot Terminal
[attacker@parrot]-[~]
$

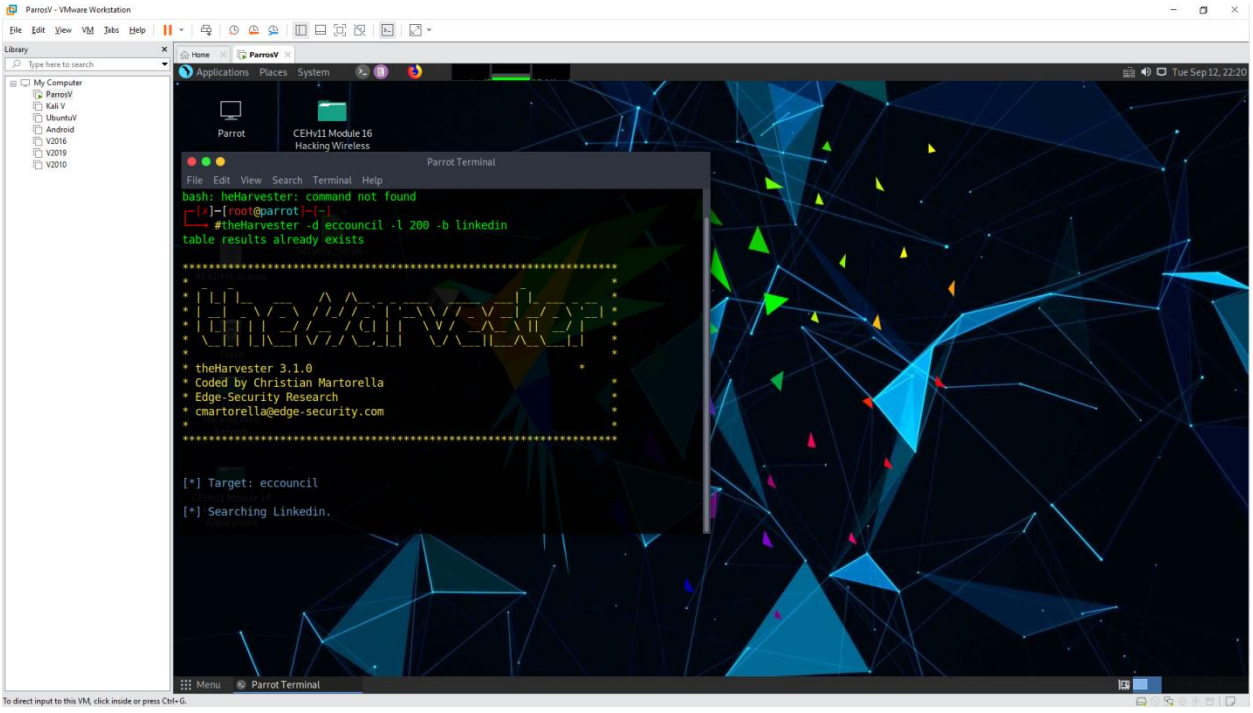
- sudo su

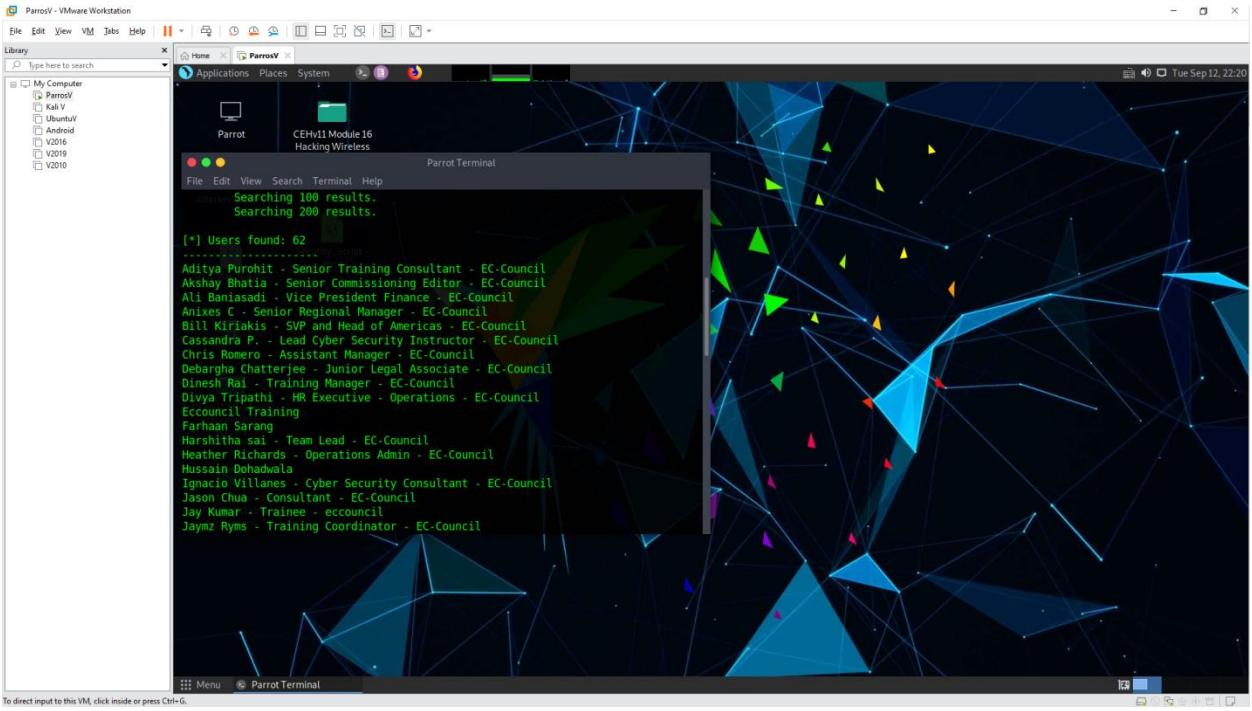

ParrosV - VMware Workstation
Parrot
CEHv11 Module 16
Hacking Wireless
Parrot Terminal
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#

- cd



- theHarvester-d eccouncil -l 200 -b linkedin

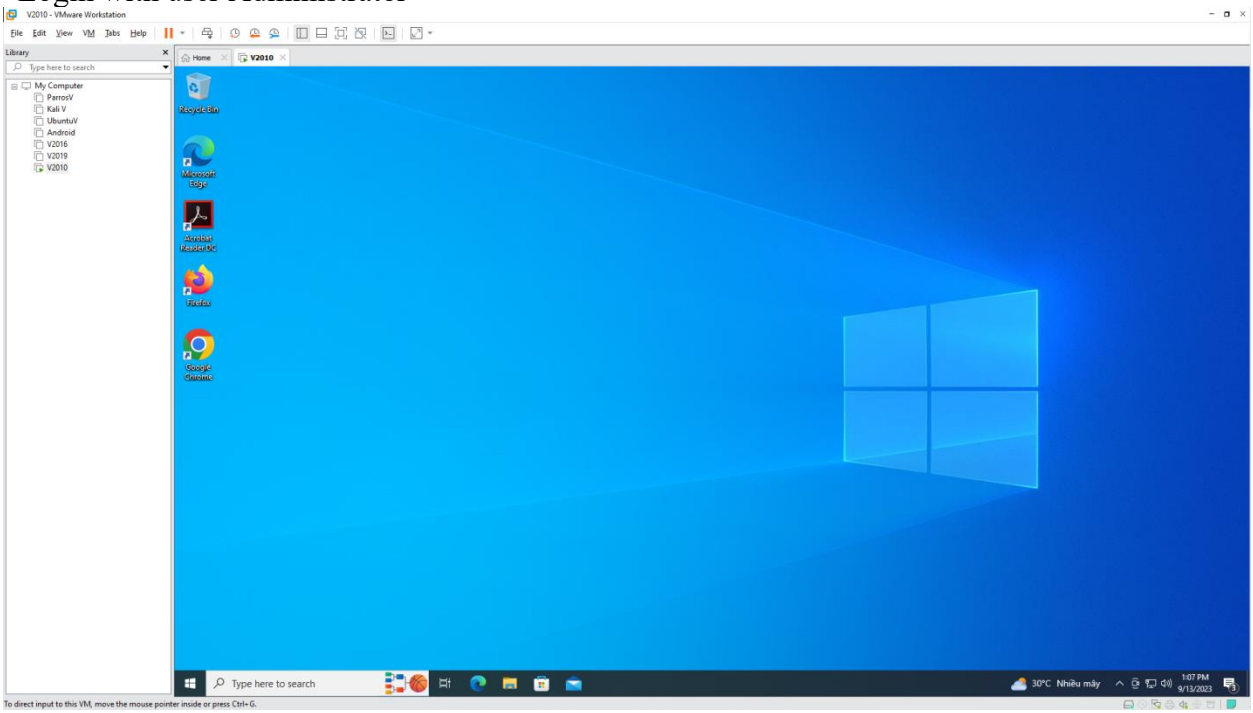




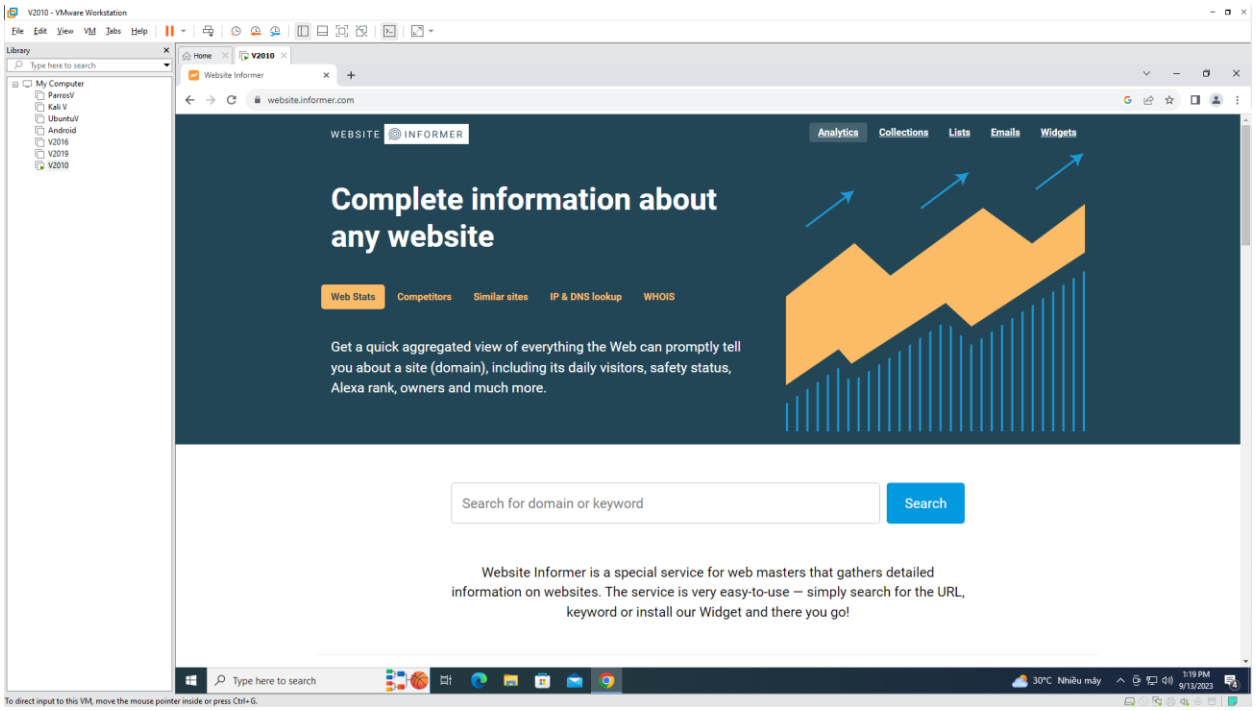
4. Perform Web Footprinting

- Gather Information about a Target Website using Website Informer

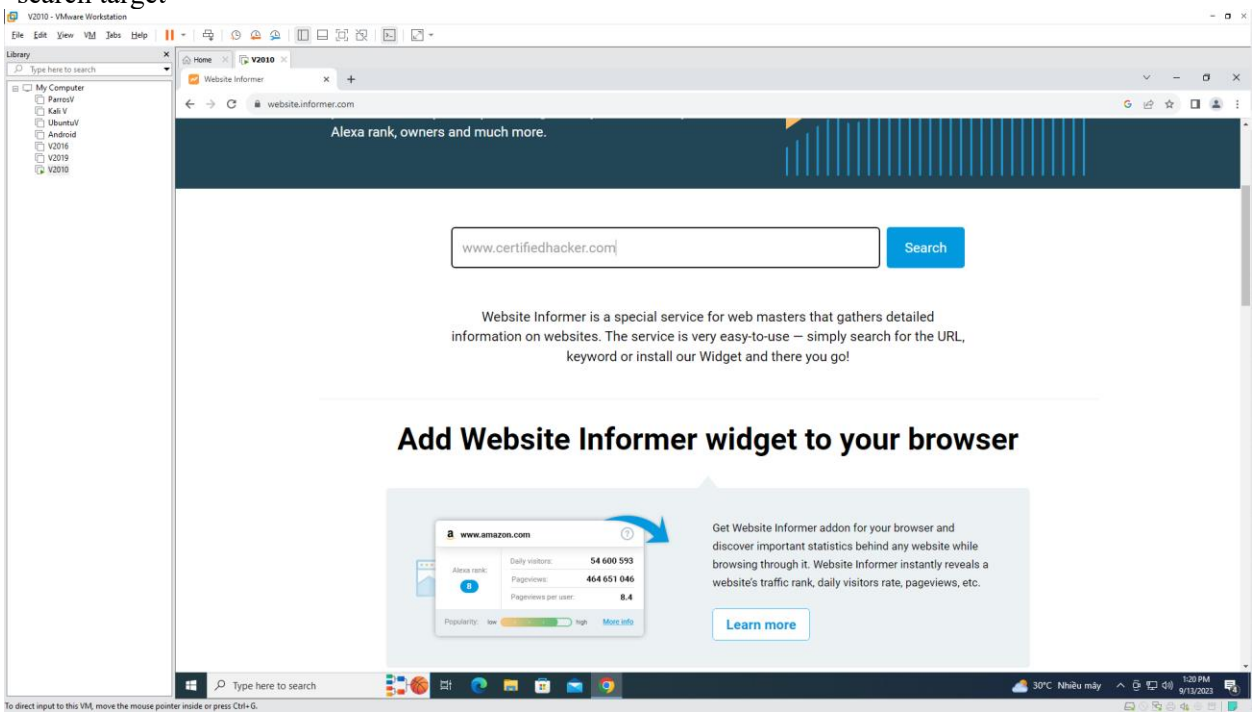
- Using Windows 10
- Login with user Administrator



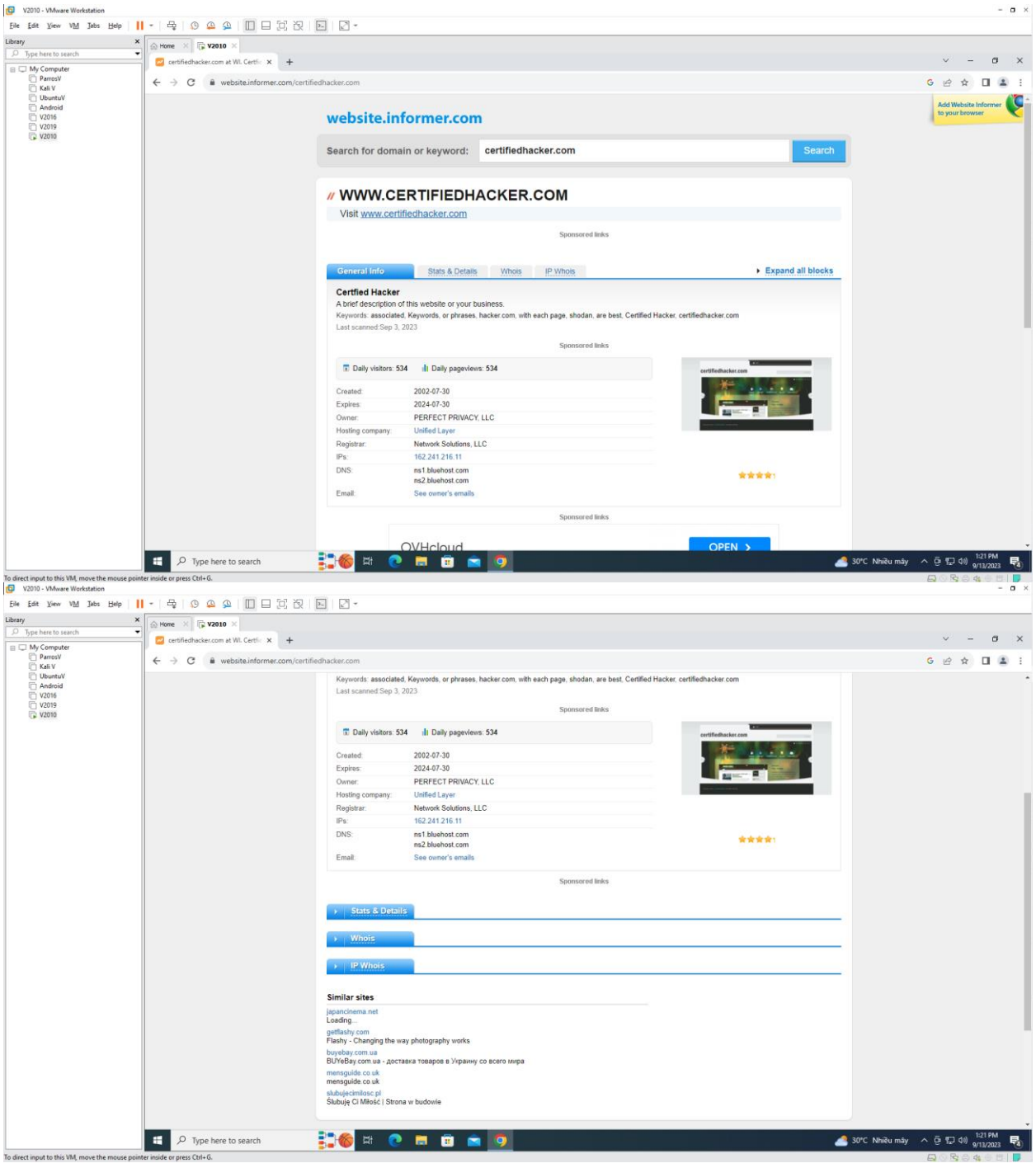
- open browser



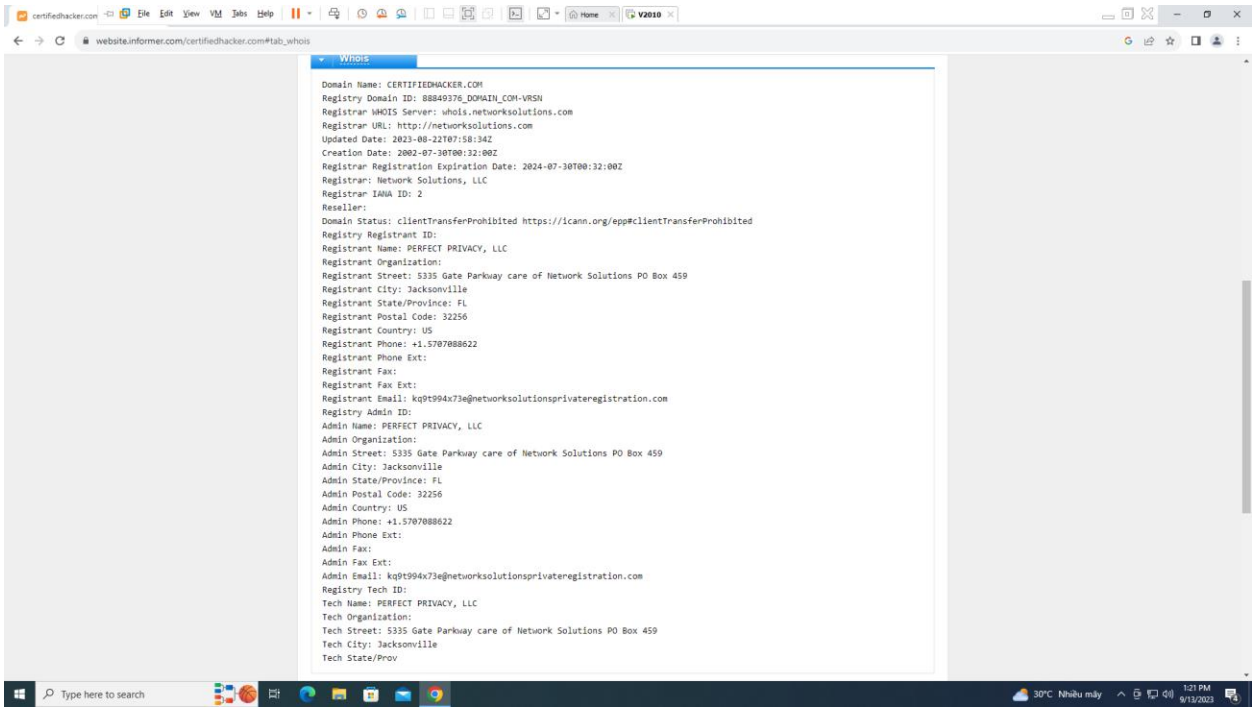
- search target



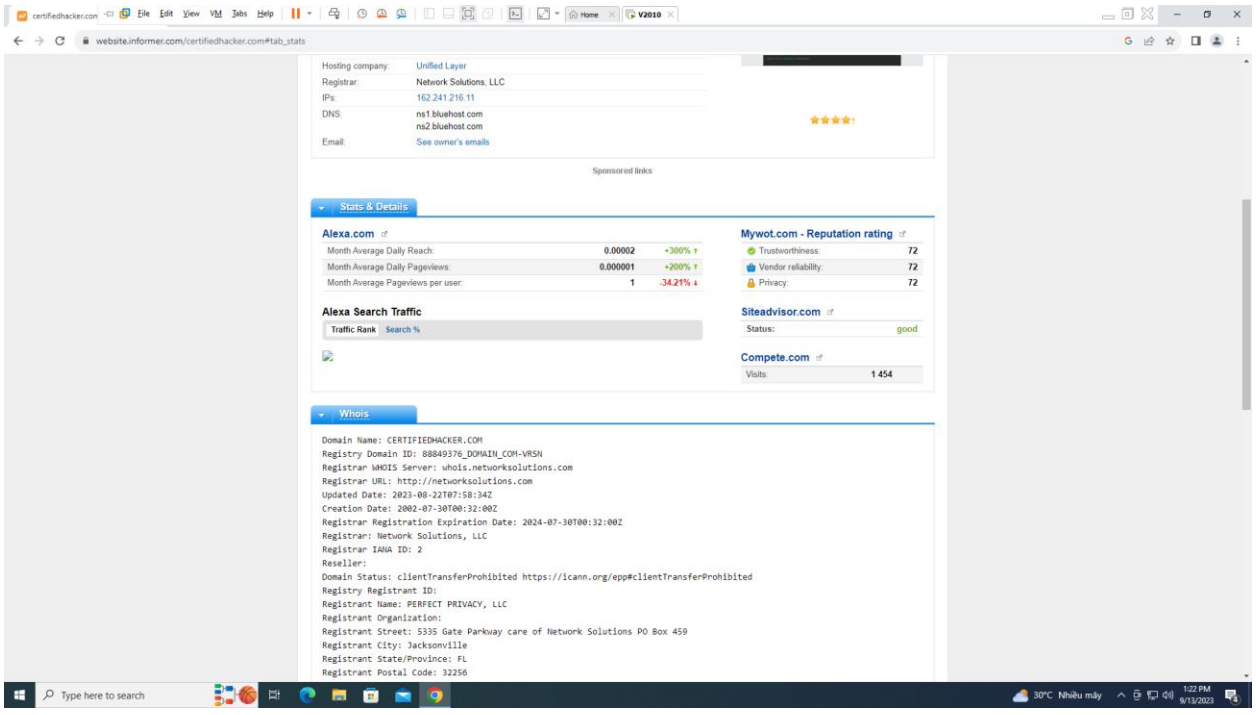
- Information of taget


website.informer.com
Search for domain or keyword:
certifiedhacker.com
Search
WWW.CERTIFIEDHACKER.COM
Visit www.certifiedhacker.com
General Info
Stats & Details
Whois
IP Whois
Expand all blocks
Certfied 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
Stats & Details
Whois
IP Whois
Similar sites
japancinema.net
Loading...
getflashy.com
Flashy - Changing the way photography works
buyebay.com.ua
BUYeBay.com.ua - доставка товаров в Украину со всего мира
mensguide.co.uk
mensguide.co.uk
slubujecimilosc.pl
Slubuję Ci Miłość | Strona w budowie

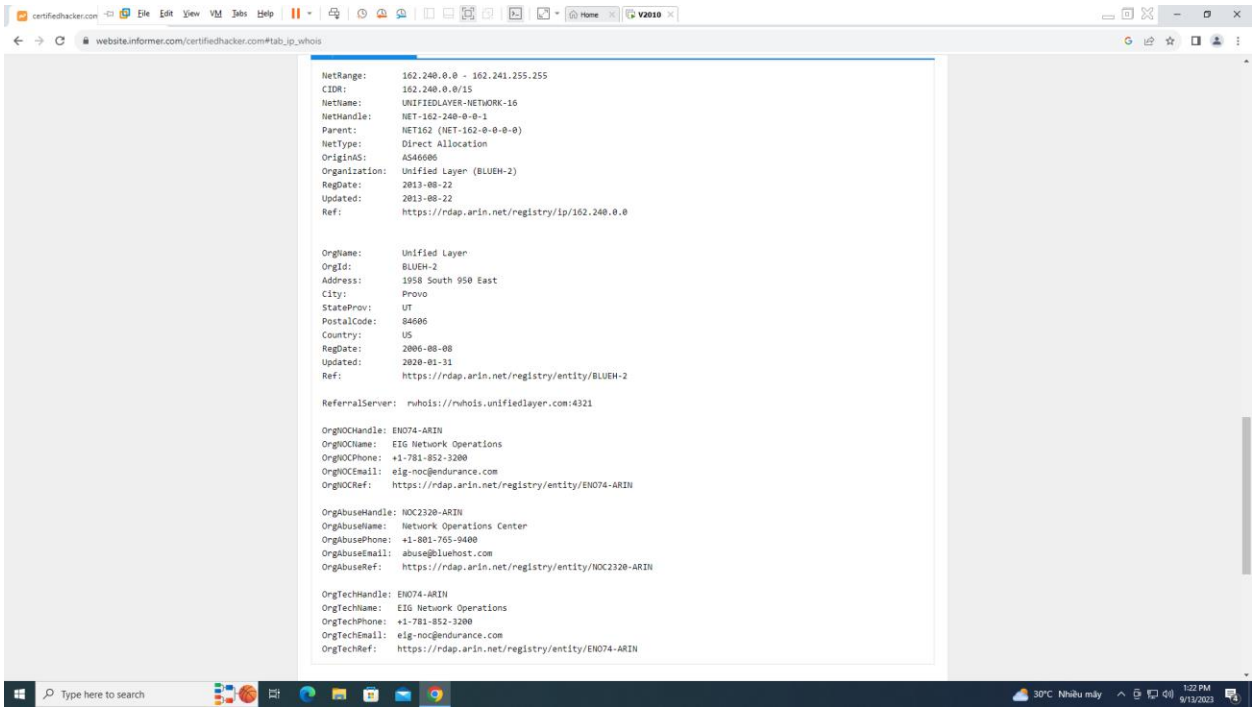
- WHOIS



- Stats & details



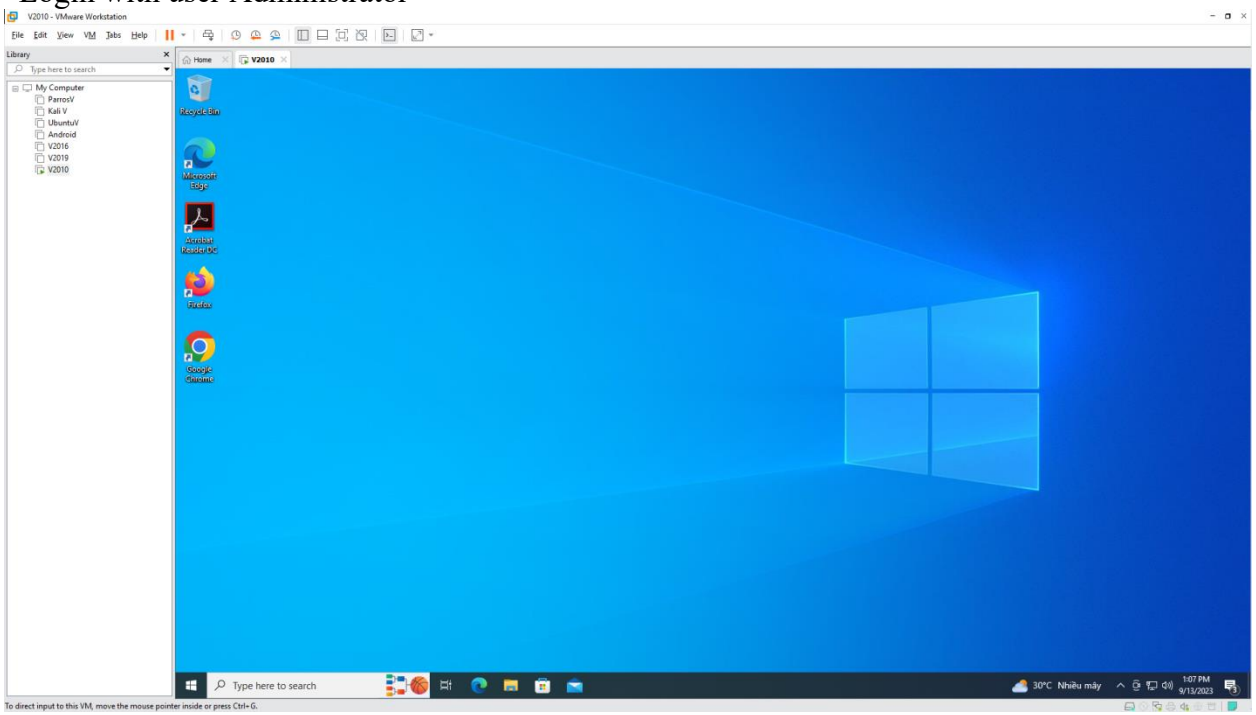
- IP Whois



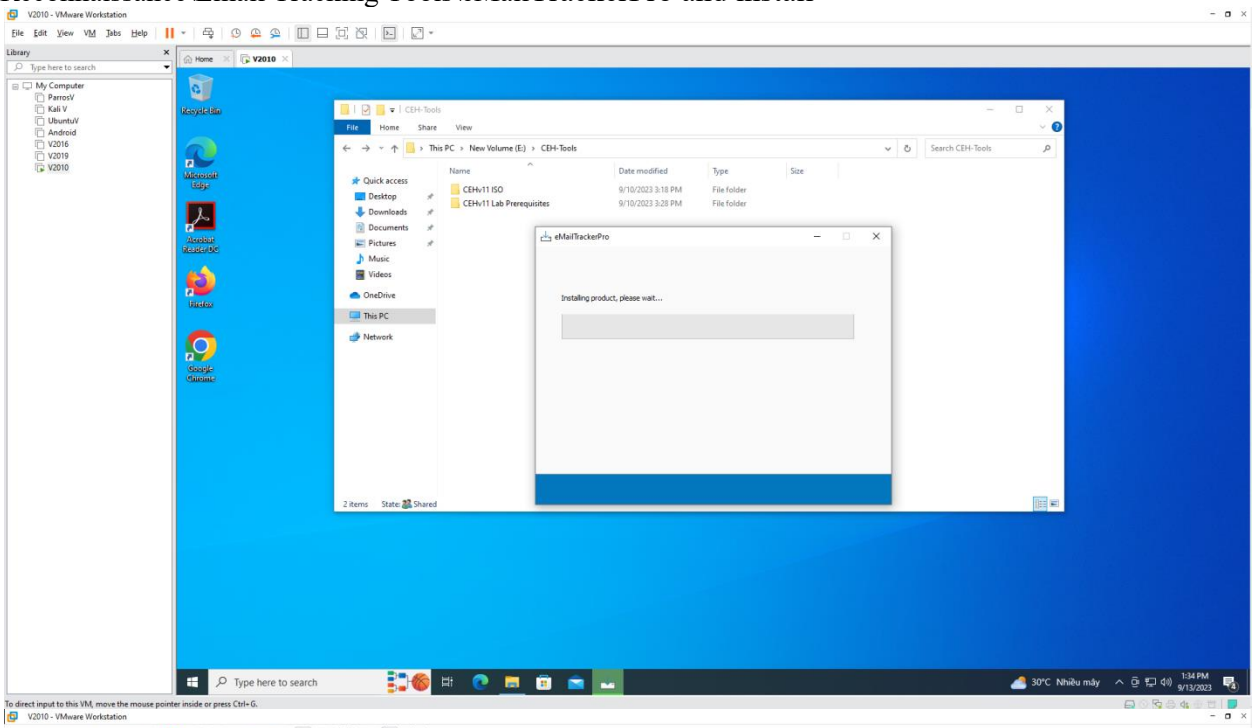
5. Perform Email Footprinting

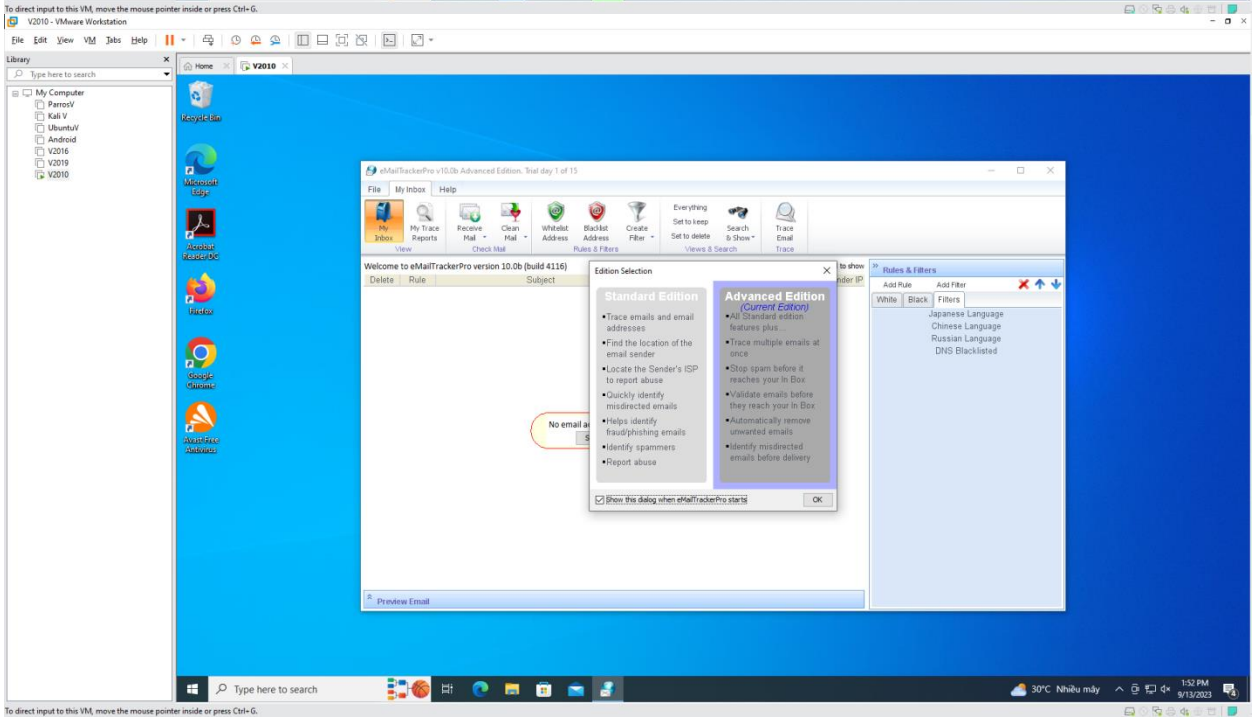
- Gather Information About a Target by Tracing Emails using eMail TrackerPro

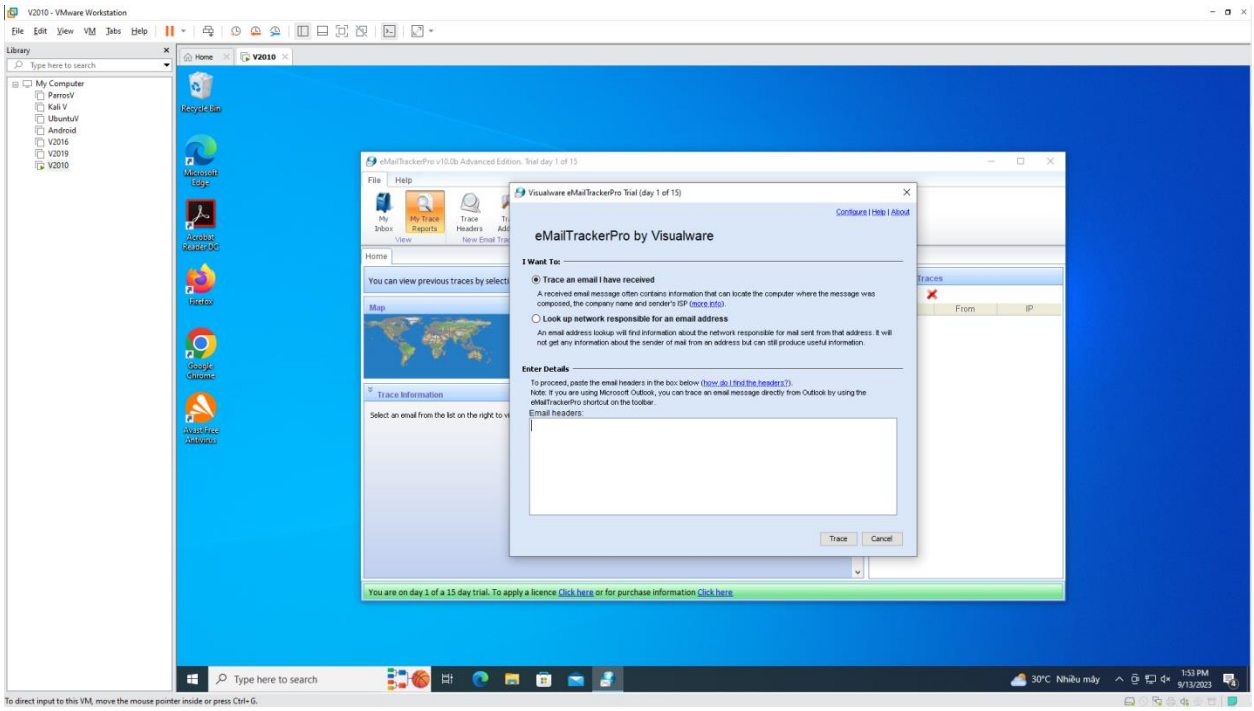
- Using Windows 10
- Login with user Administrator

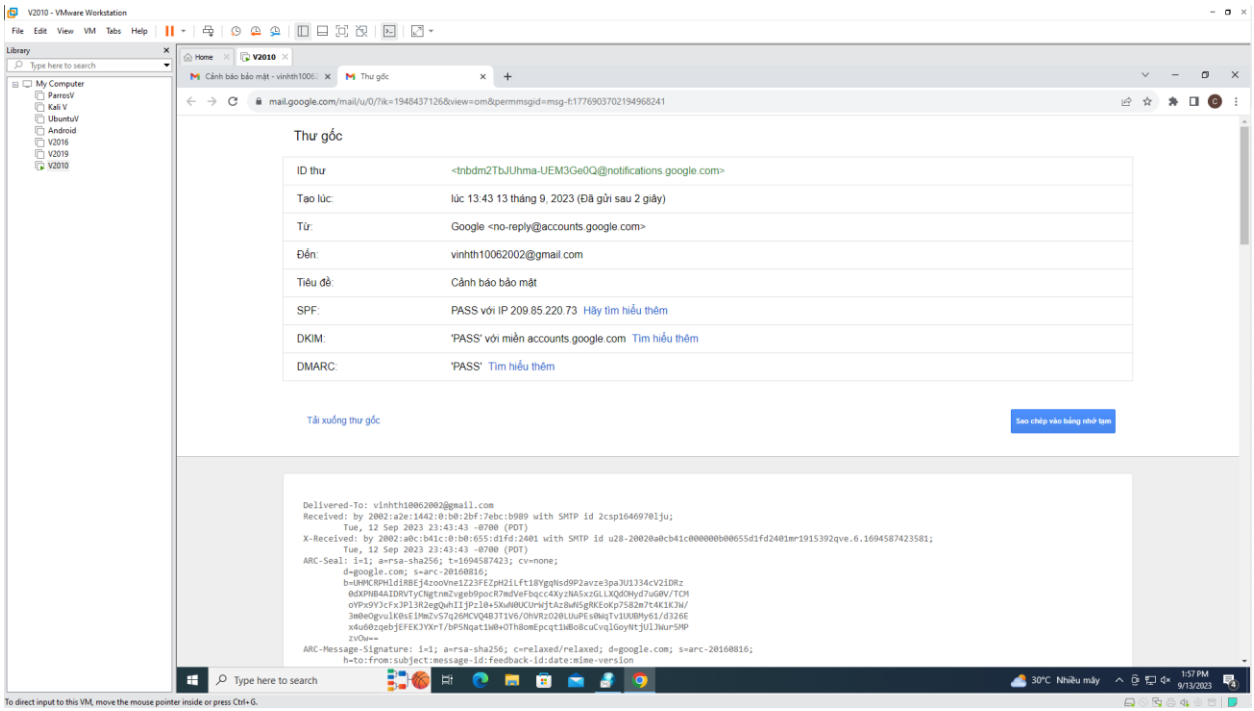


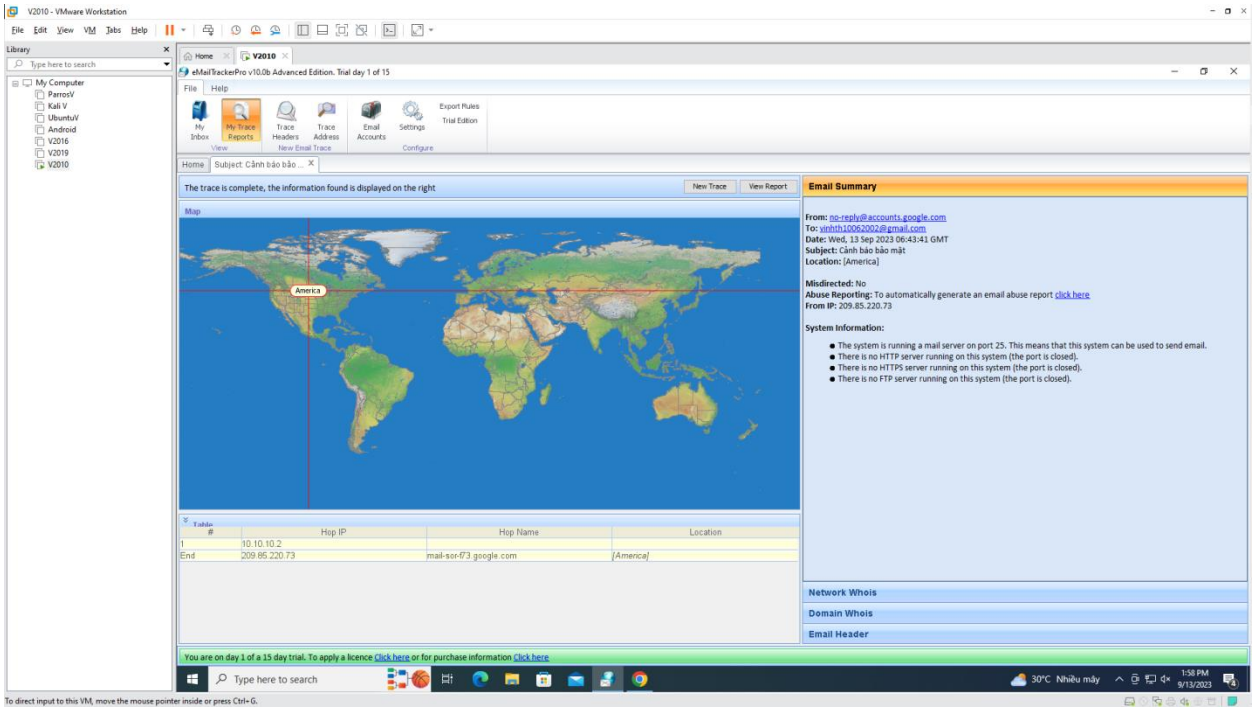
- Open File Explorer, navigate to E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro and install



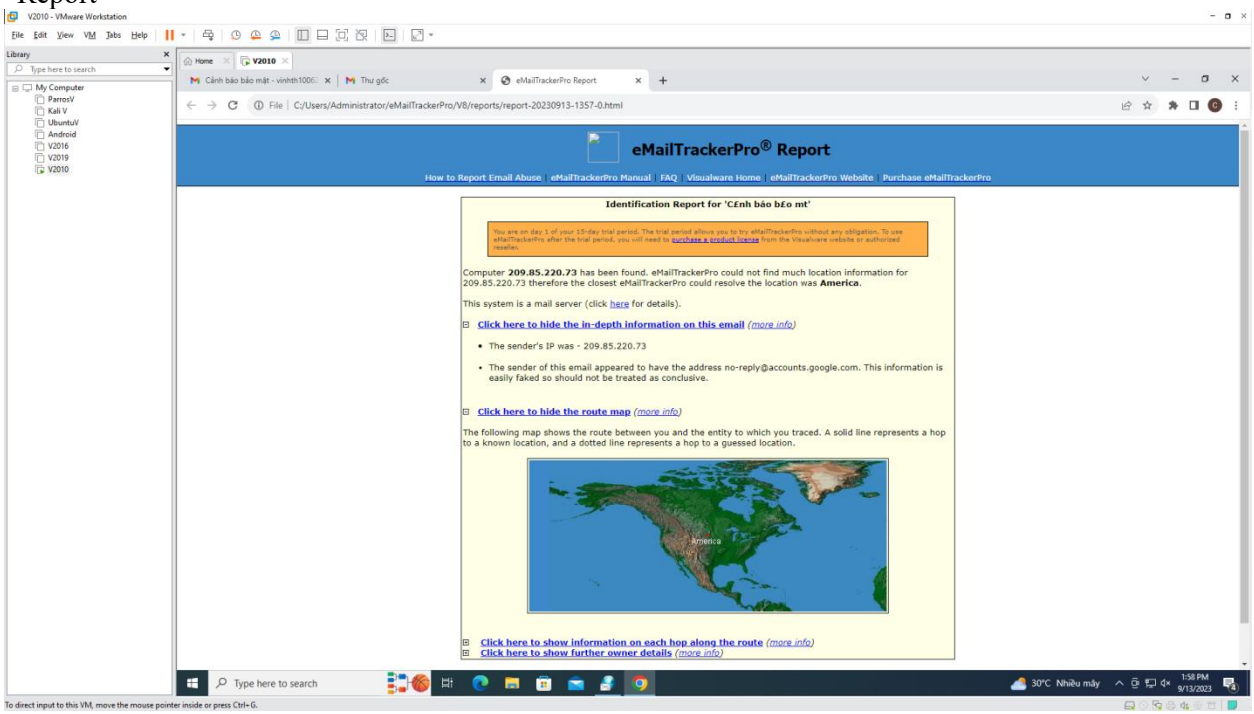



V2010 - VMware Workstation
eMailTrackerPro by Visualware
Trace an email I have received
Look up network responsible for an email address
Trace
Cancel
You are on day 1 of a 15 day trial. To apply a licence Click here or for purchase information Click here


V2010 - VMware Workstation
Thư gốc
ID thư <tnbdm2TbJUhma-UEM3Ge0Q@notifications.google.com>
Tạo lúc: lúc 13:43 13 tháng 9, 2023 (Đã gửi sau 2 giây)
Từ: Google <no-reply@accounts.google.com>
Đến: vinhth10062002@gmail.com
Tiêu đề: Cảnh báo bảo mật
SPF: PASS với IP 209.85.220.73 Hãy tìm hiểu thêm
DKIM: 'PASS' với miền accounts.google.com Tìm hiểu thêm
DMARC: 'PASS' Tìm hiểu thêm
Tải xuống thư gốc
Sao chép vào bảng nhớ tạm



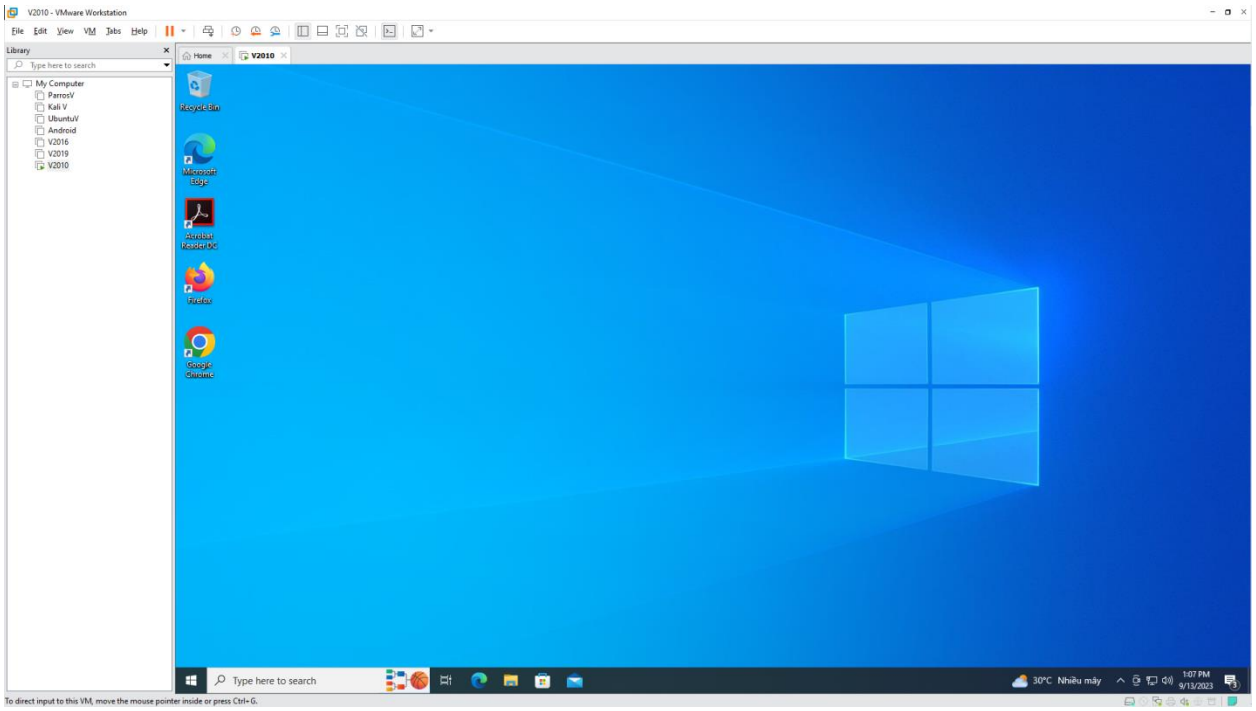
- Report



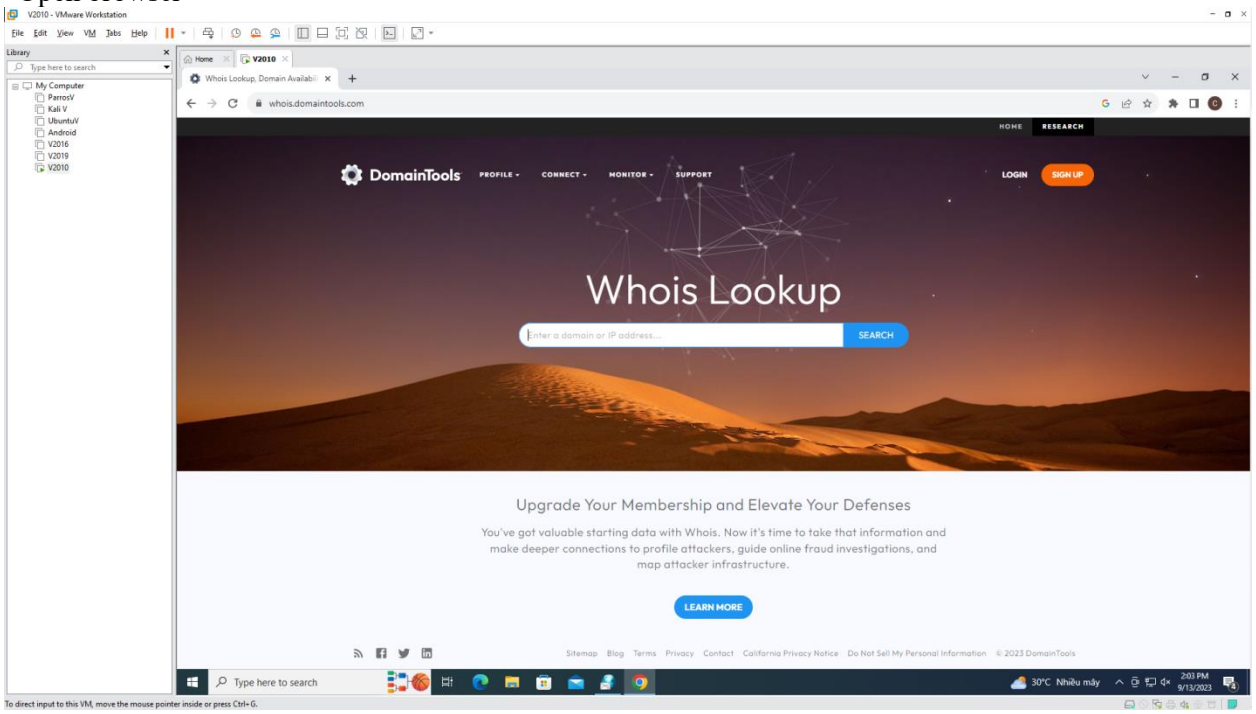
6. Perform Whois Footprinting

- Perform Whois lookup using DomainTools

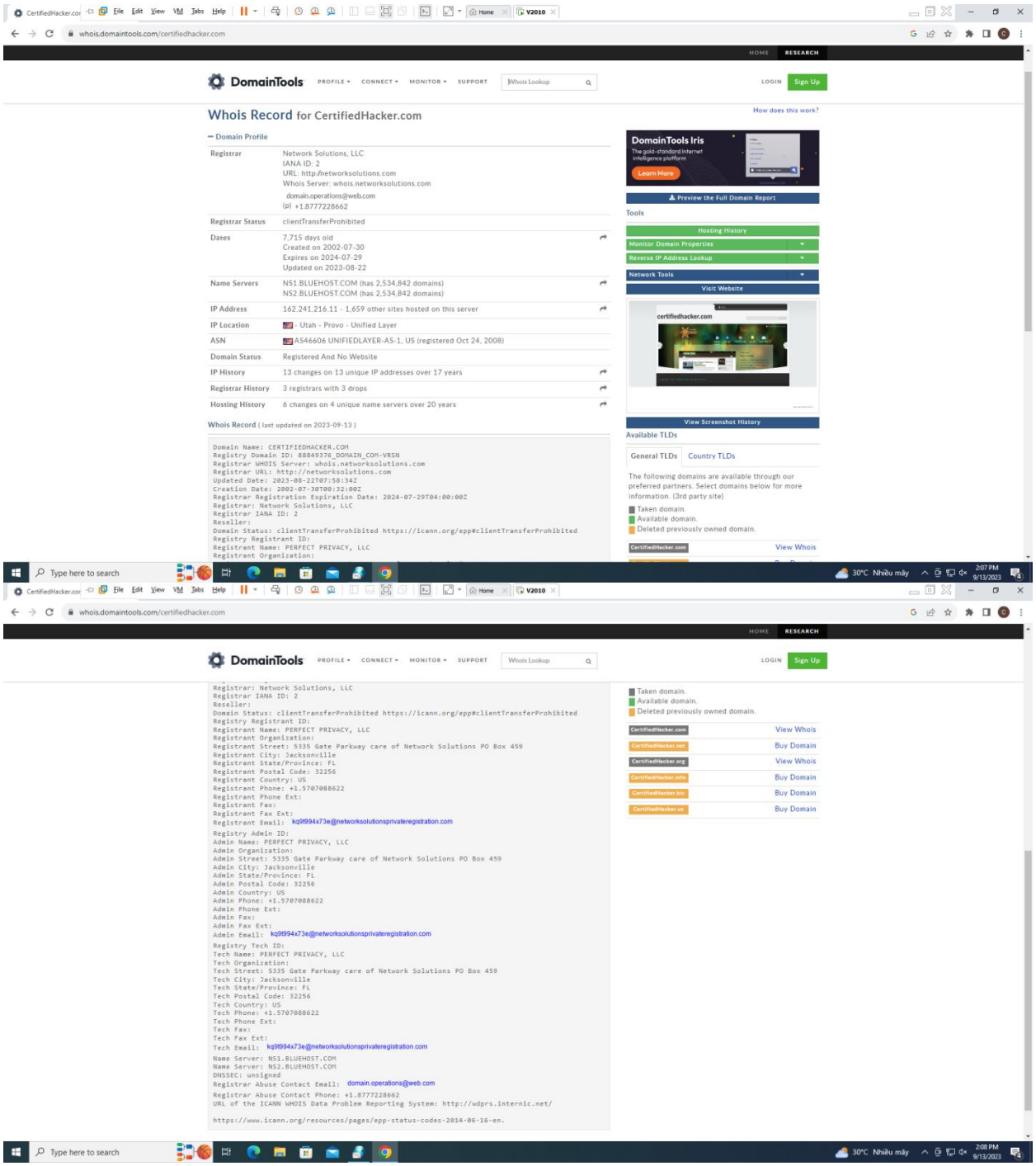
- Using Windows 10
- Login with user Administrator



- Open browser



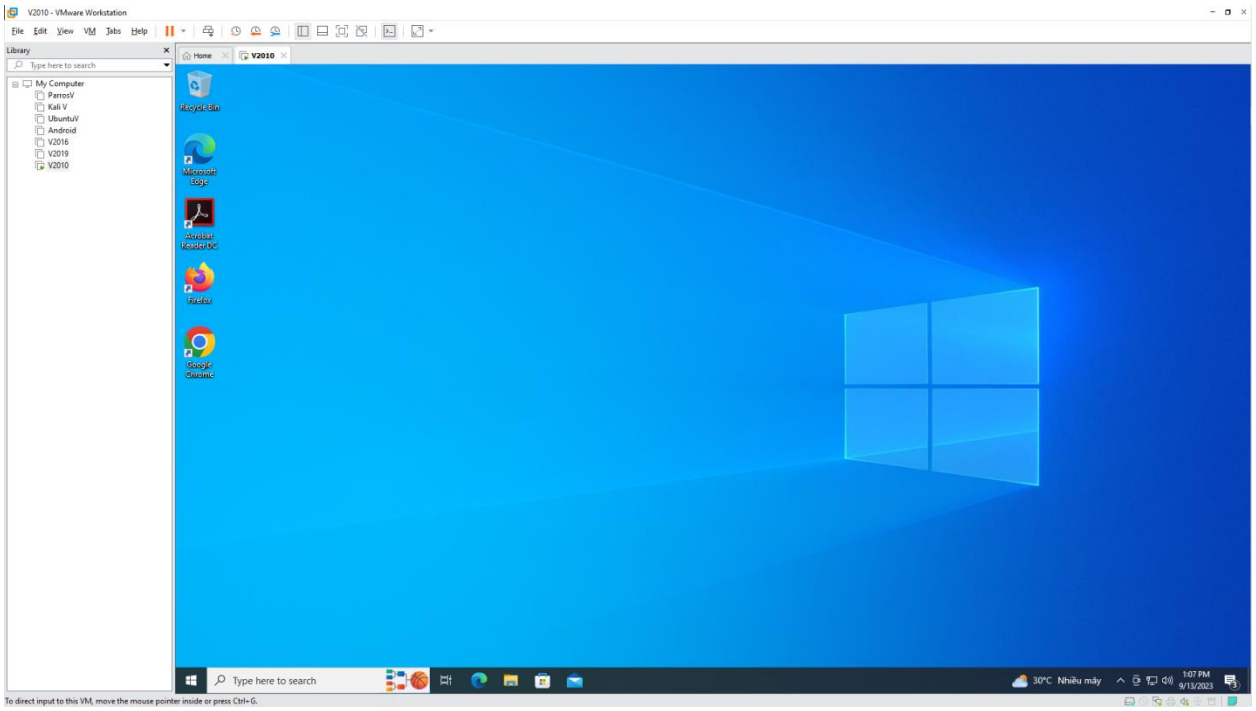
- search www.certifiedhacker.com



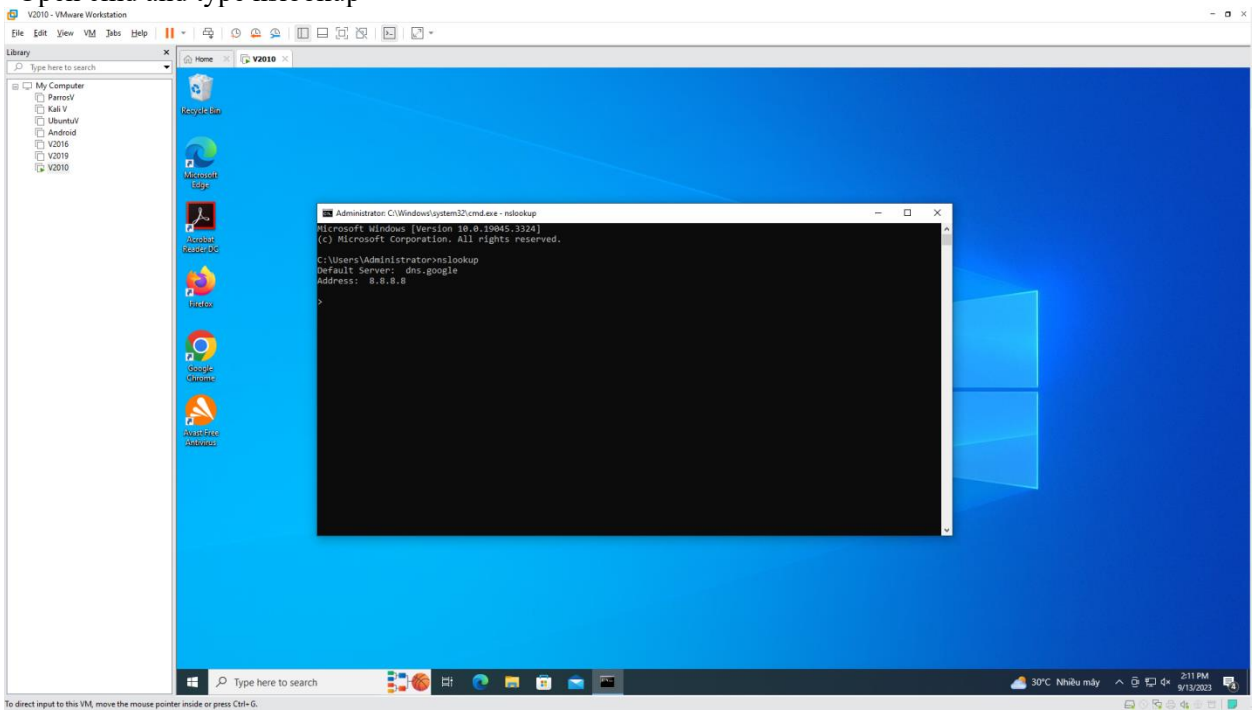
7. Perform DNS Footprinting

- Perform Whois lookup using DomainTools

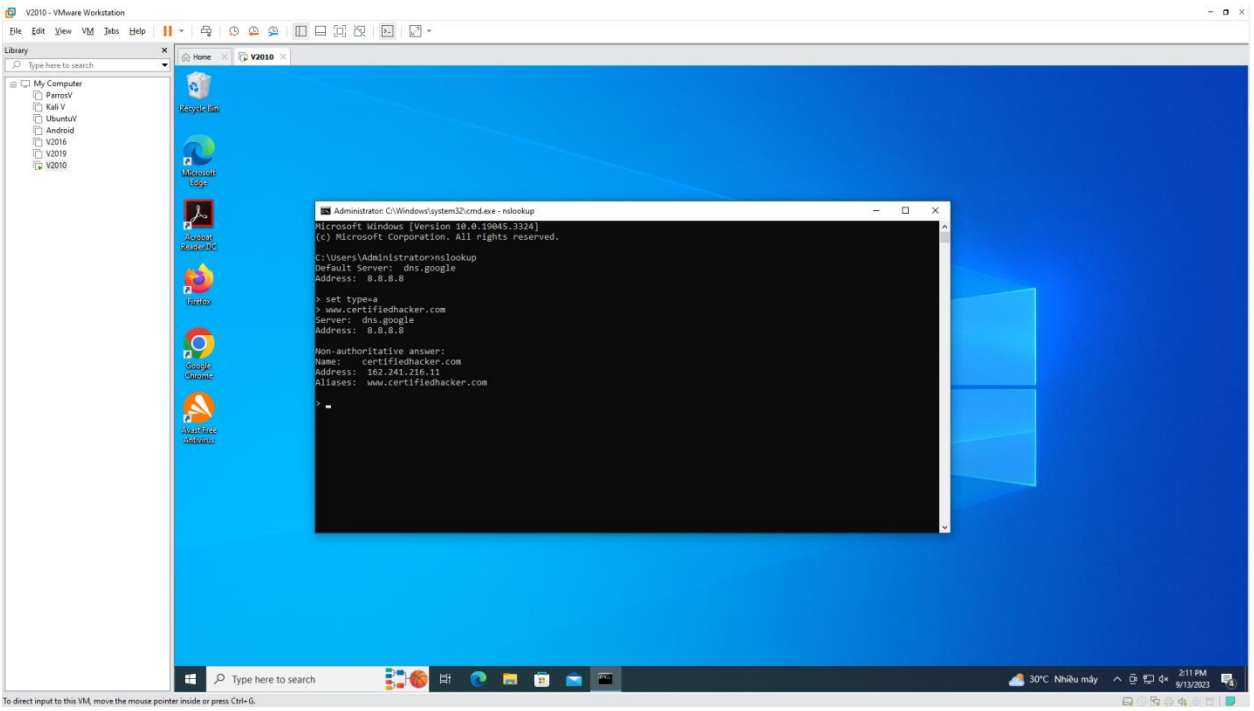
- Using Windows 10
- Login with user Administrator



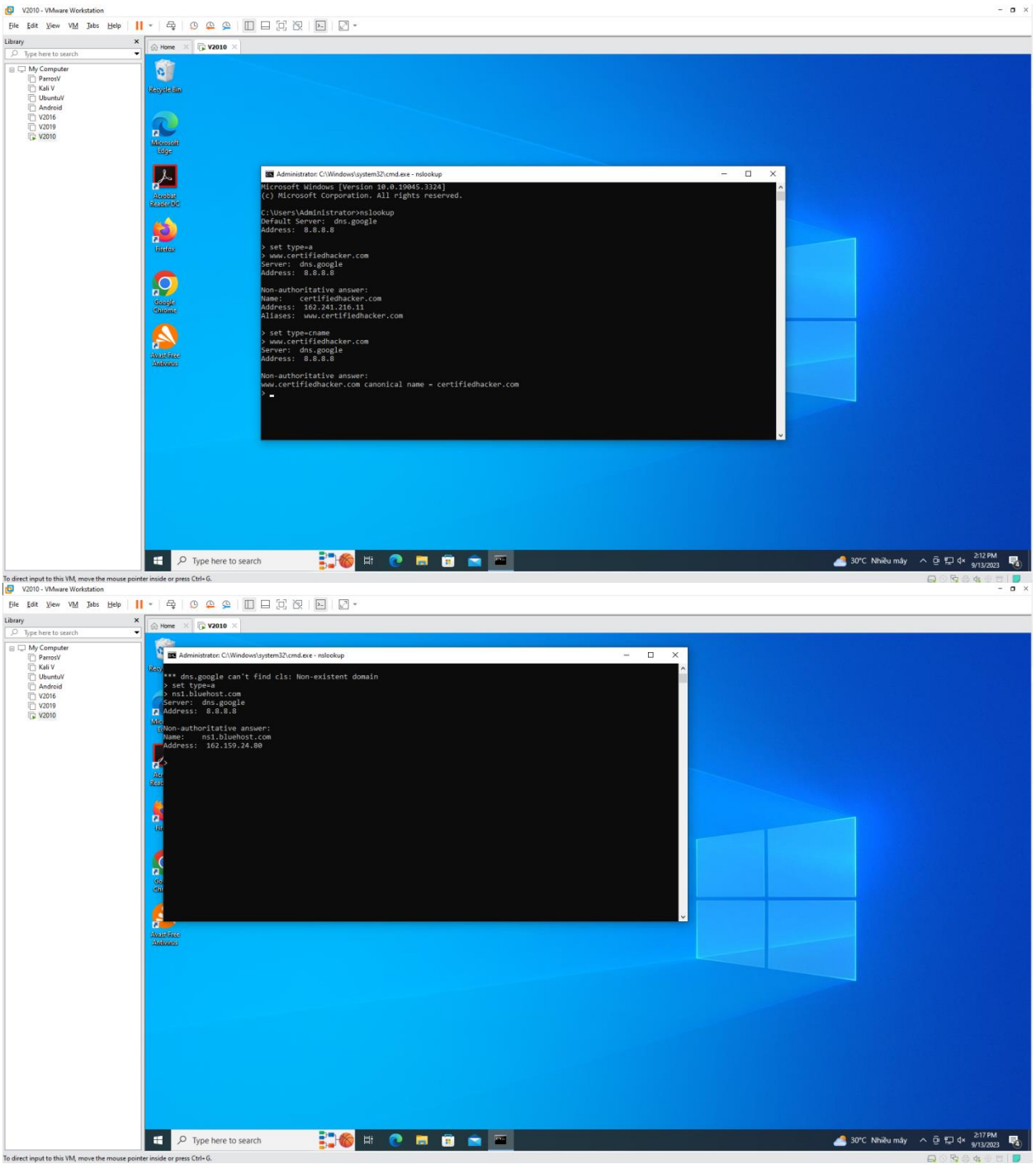
- Open cmd and type nslookup



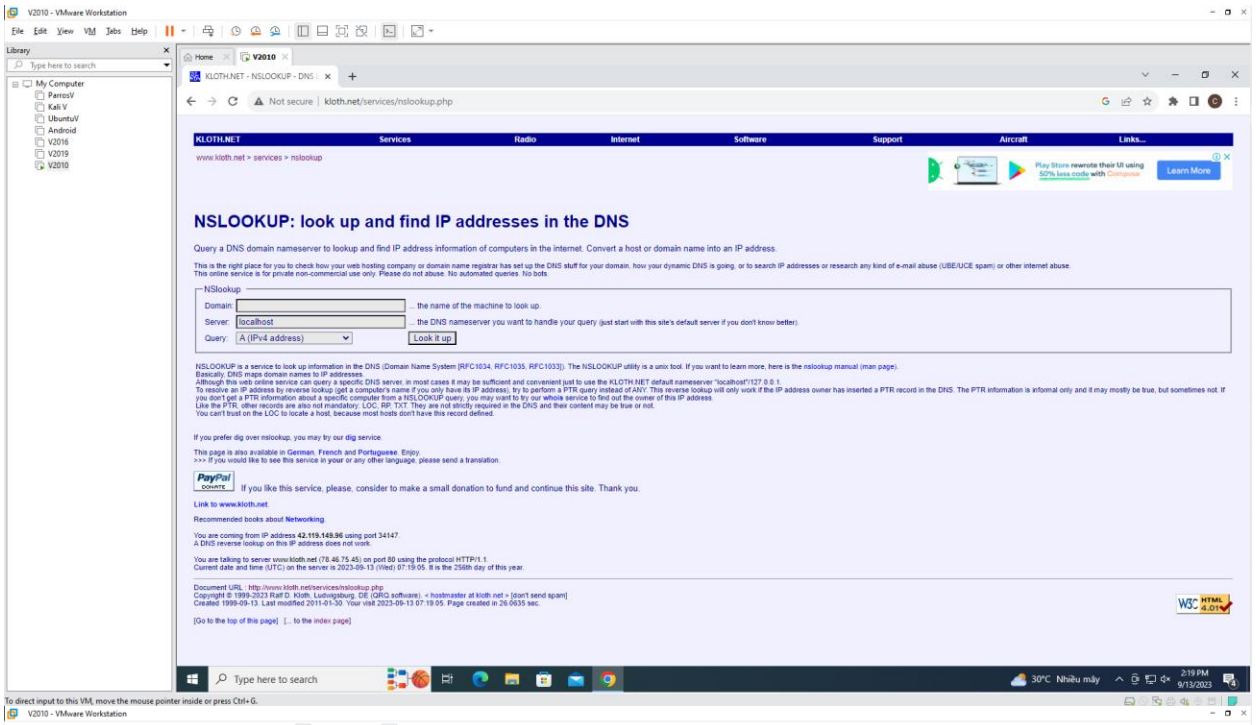
- set type=a
- www.certifiedhacker.com

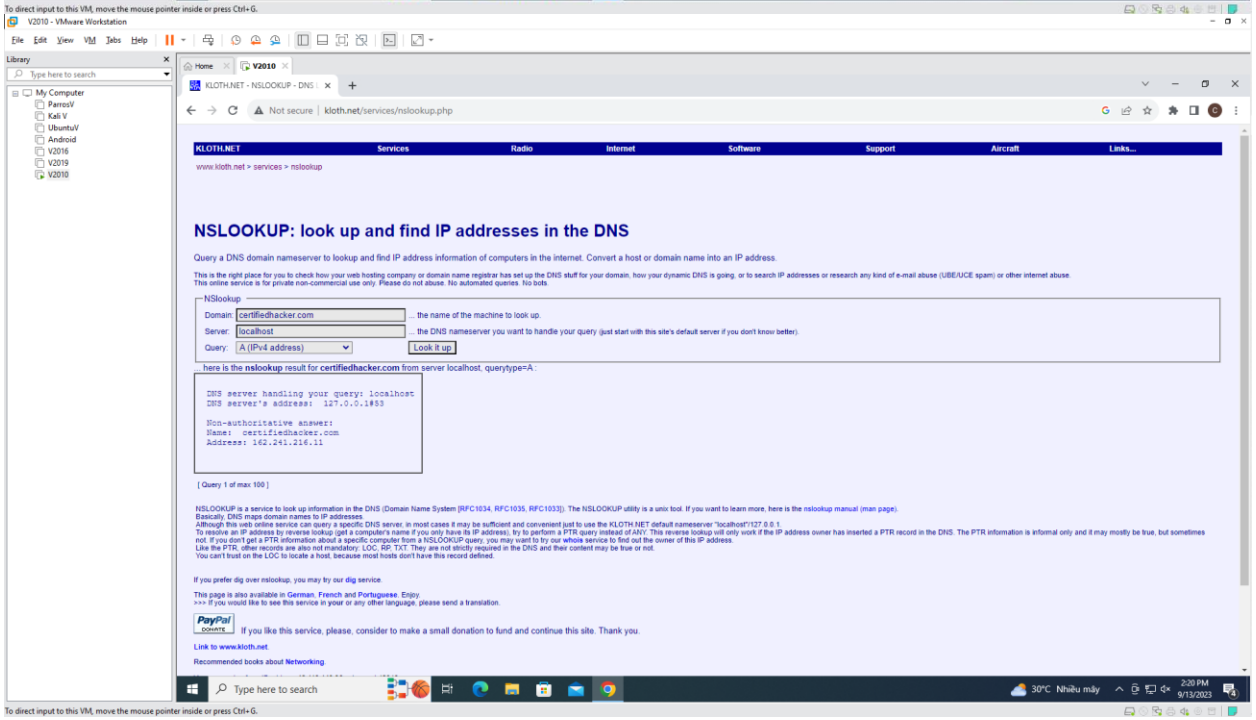


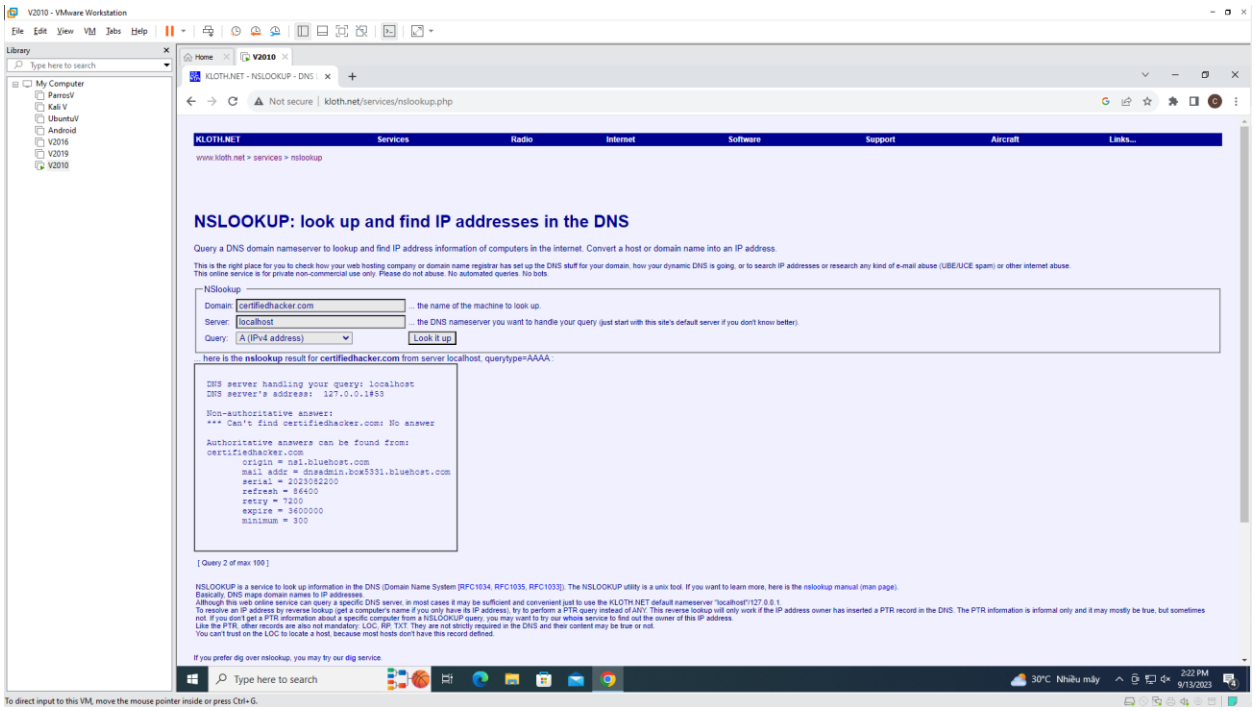
- set type=cname
- www.certifiedhacker.com



- open web browser


V2010 - VMware Workstation
KLOTH.NET - NSLOOKUP - DNS
Not secure | kloth.net/services/nslookup.php
NSLOOKUP: look up and find IP addresses in the DNS
Query a DNS domain nameserver to lookup and find IP address information of computers in the internet. Convert a host or domain name into an IP address.
Domain:
Server: localhost
Query: A (IPv4 address)
Look it up
Type here to search
30°C Nhiều mây
2:19 PM
9/13/2023

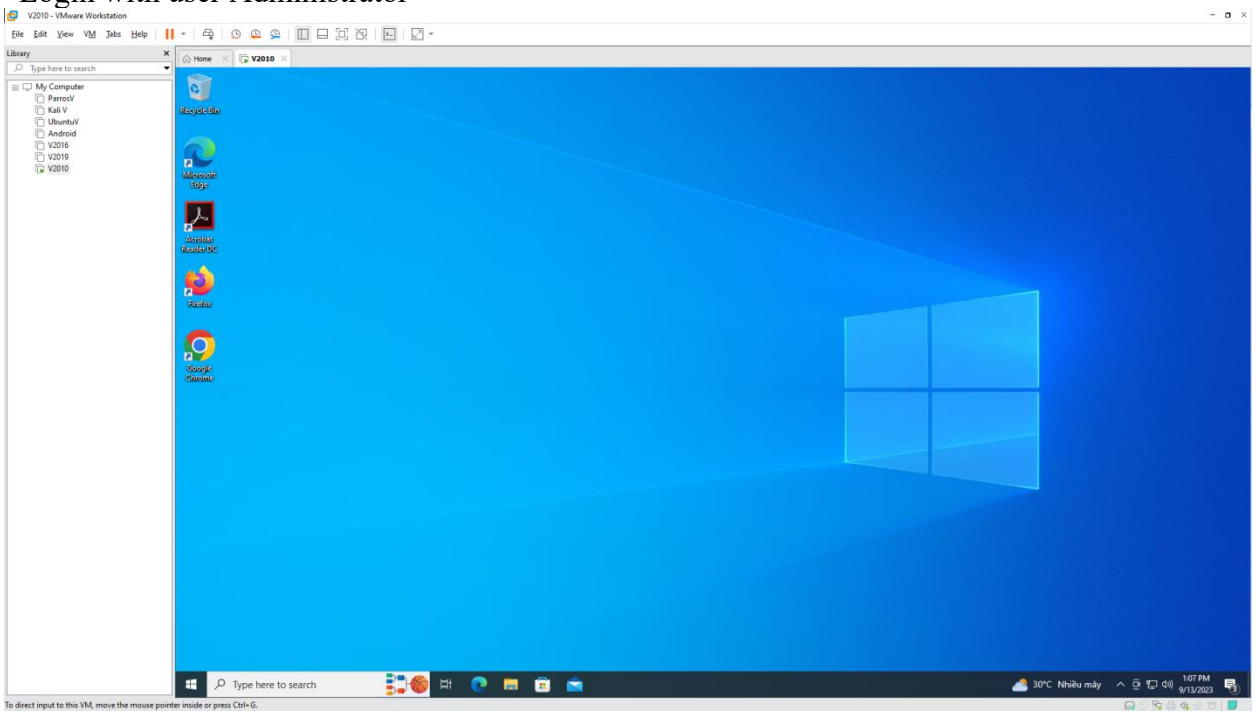

V2010 - VMware Workstation
KLOTH.NET - NSLOOKUP - DNS
Not secure | kloth.net/services/nslookup.php
NSLOOKUP: look up and find IP addresses in the DNS
Domain: certifiedhacker.com
Server: localhost
Query: A (IPv4 address)
Look it up
here is the nslookup result for certifiedhacker.com from server localhost, querytype=A :
DNS server handling your query: localhost
DNS server's address: 127.0.0.1#53
Non-authoritative answer:
Name: certifiedhacker.com
Address: 162.241.216.11
[Query 1 of max 100]
Type here to search
30°C Nhiều mây
2:20 PM
9/13/2023



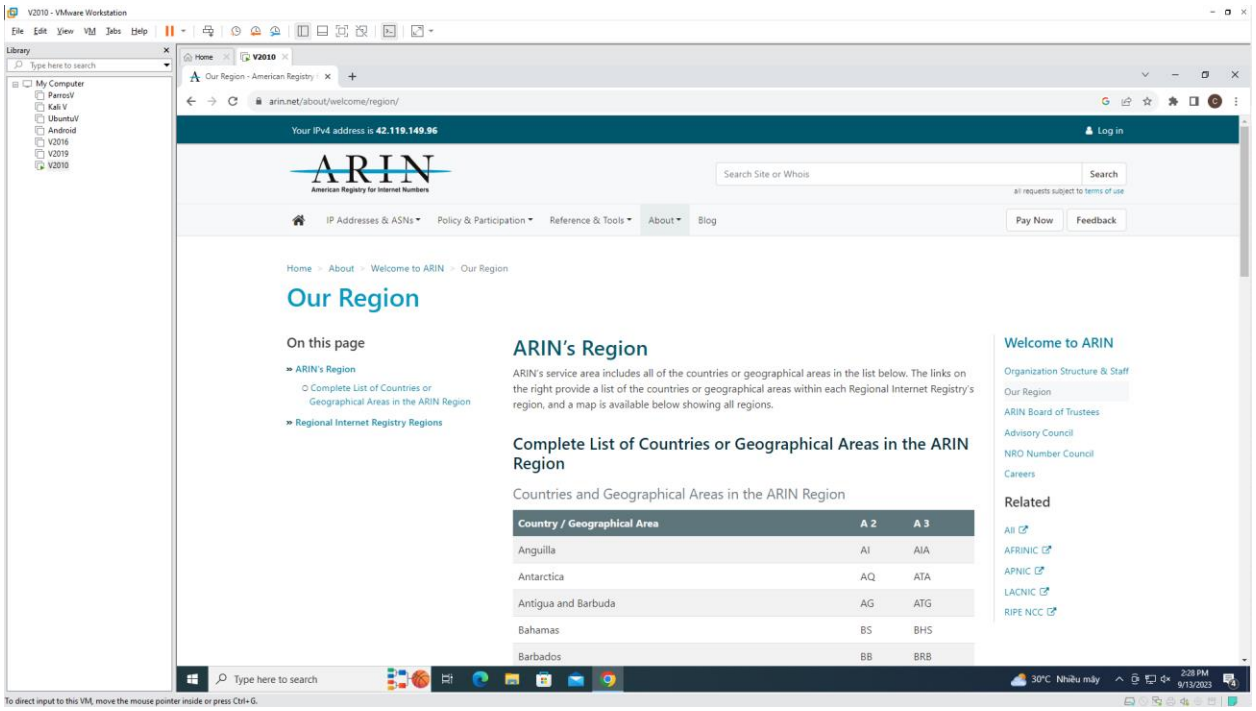
8. Perform Network Footprinting

- Locate network range

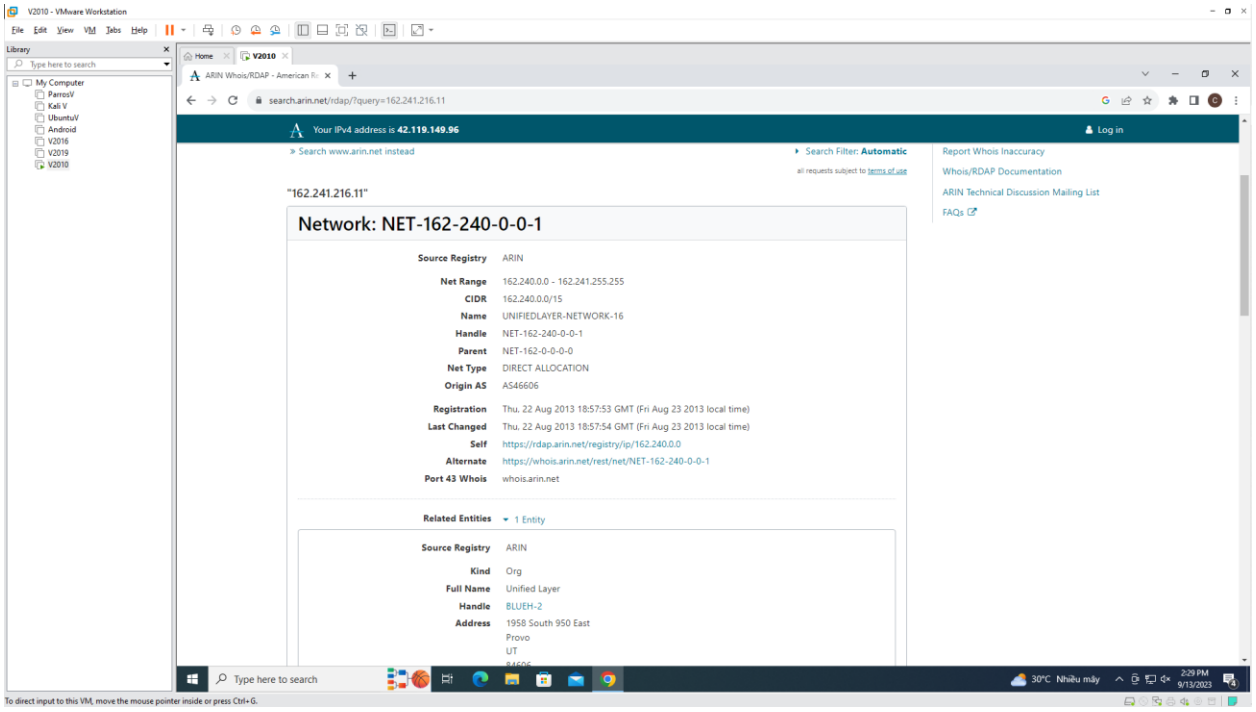
- Using Windows 10
- Login with user Administrator

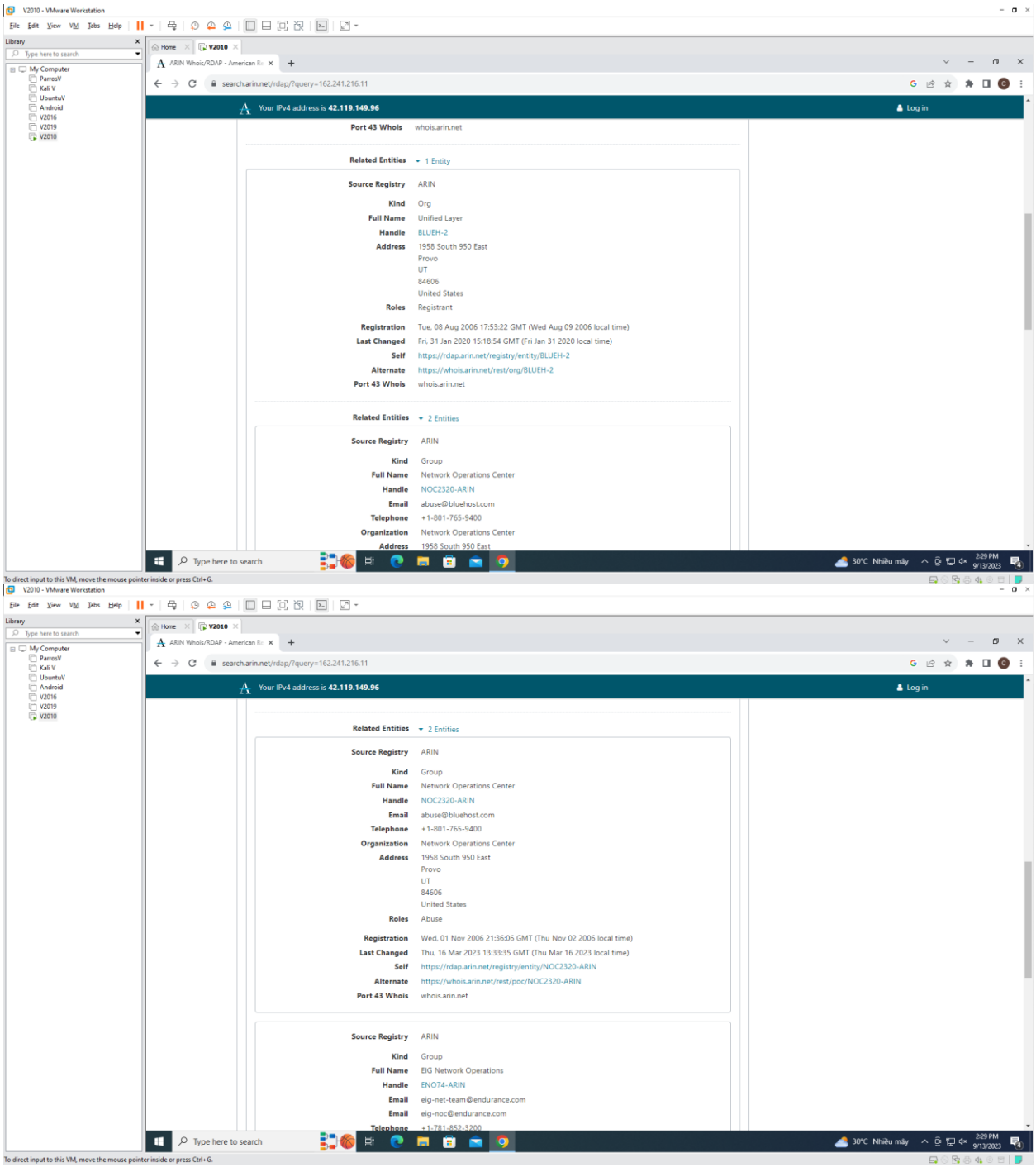


- open browser

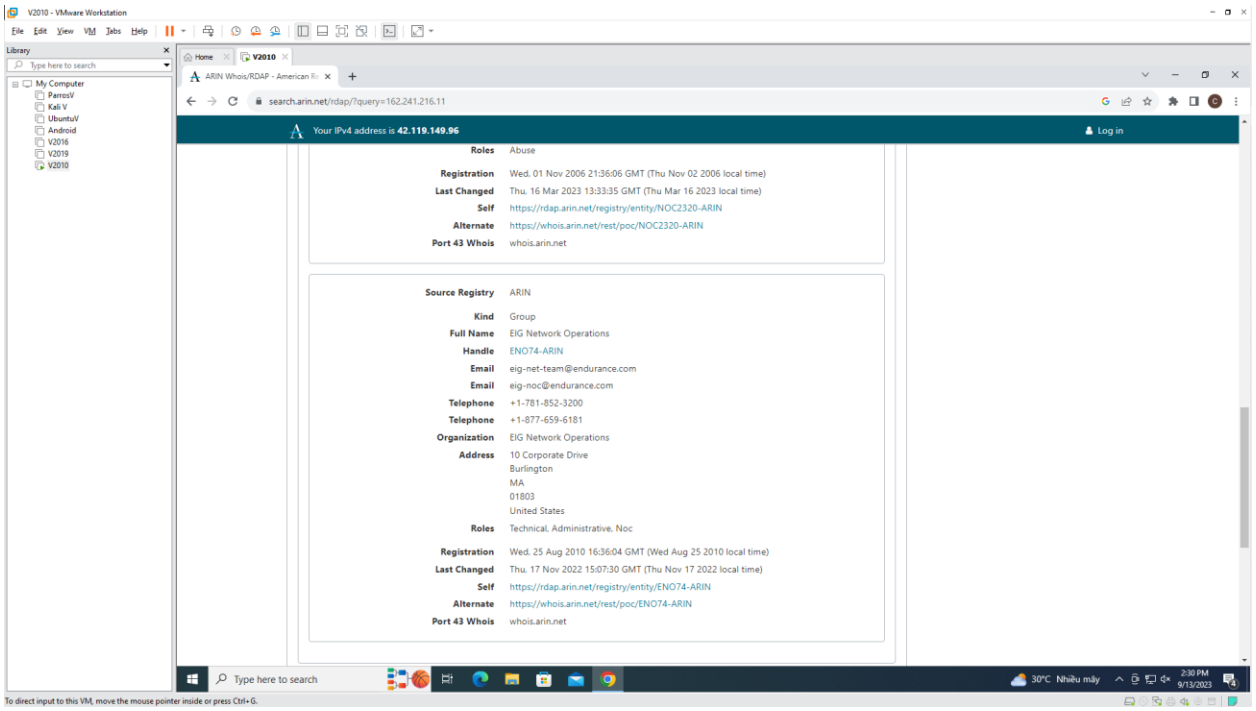


- search 162.241.216.11




V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
ARIN Whois/RDAP - American Re
search.arin.net/rdap/?query=162.241.216.11
Your IPv4 address is 42.119.149.96
Log in
Port 43 Whois whois.arin.net
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://rdap.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
Type here to search
30°C Nhiều mây
2:29 PM
9/13/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

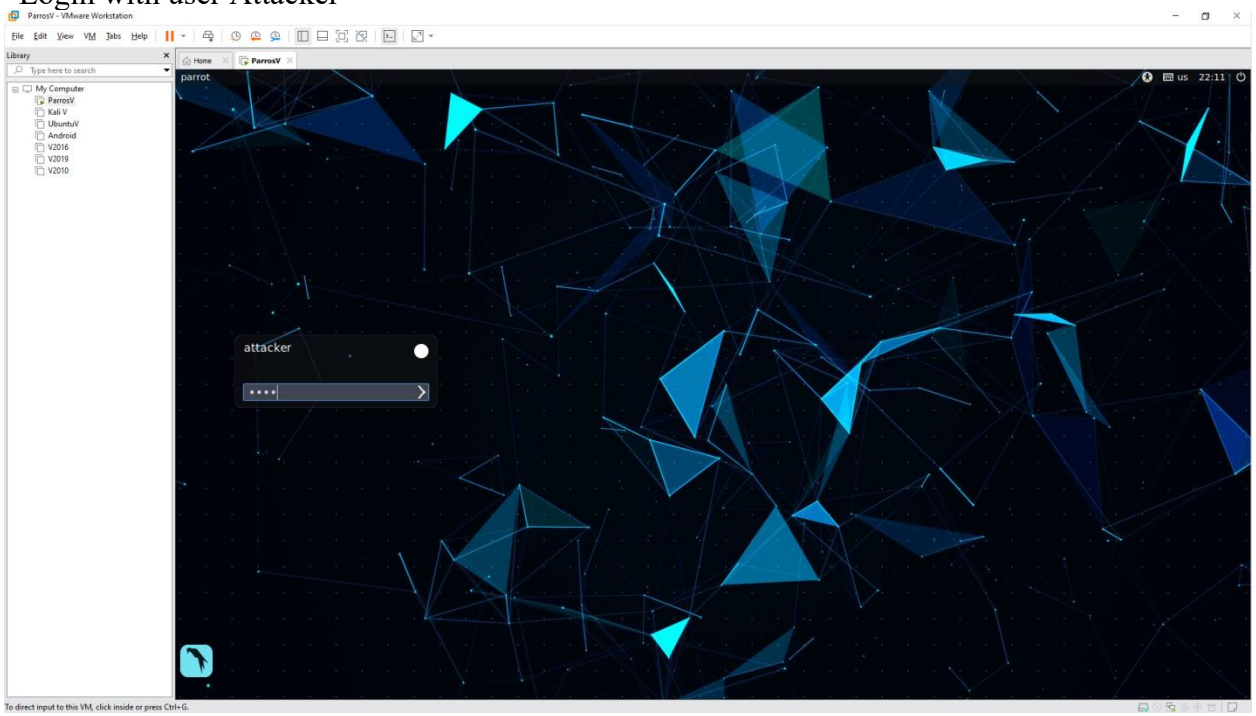
V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
ARIN Whois/RDAP - American Re
search.arin.net/rdap/?query=162.241.216.11
Your IPv4 address is 42.119.149.96
Log in
Related Entities 2 Entities
Source 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://rdap.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 ENO74-ARIN
Email eig-net-team@endurance.com
Email eig-noc@endurance.com
Type here to search
30°C Nhiều mây
2:29 PM
9/13/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



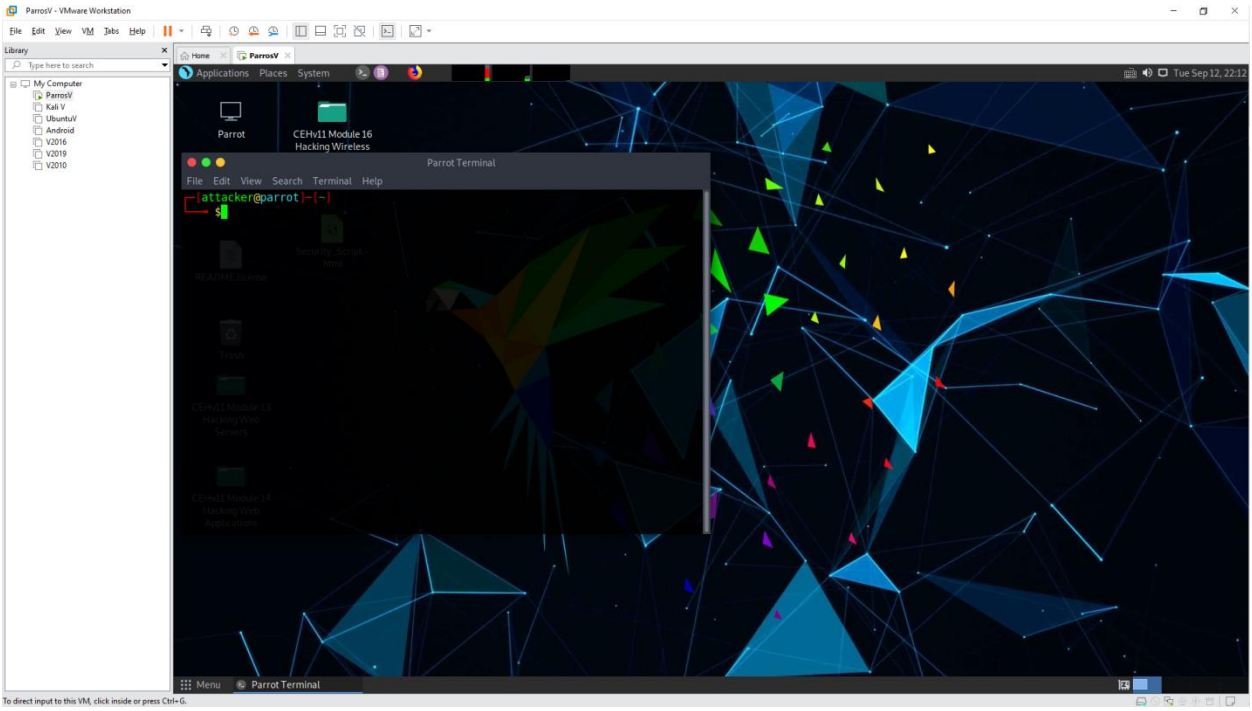
9. Perform Footprinting using Various Footprinting Tools

- Footprinting a Target using Recon-ng

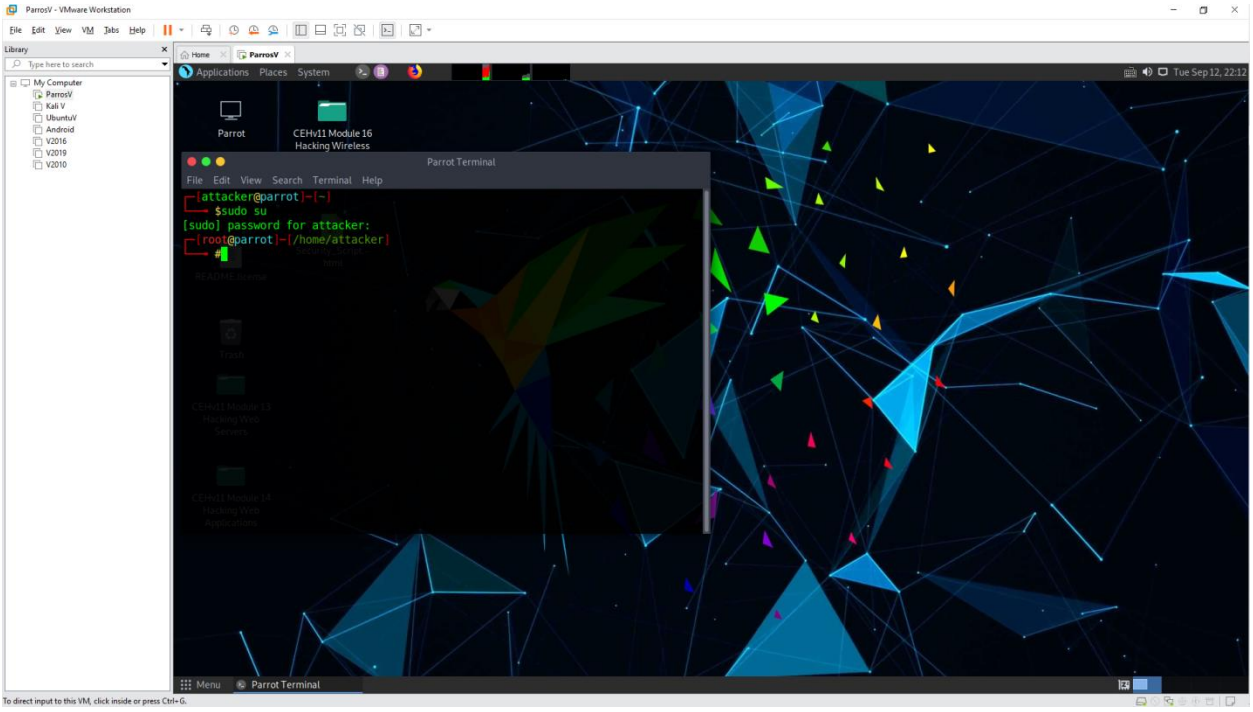
- Using Parrot
- Login with user Attacker



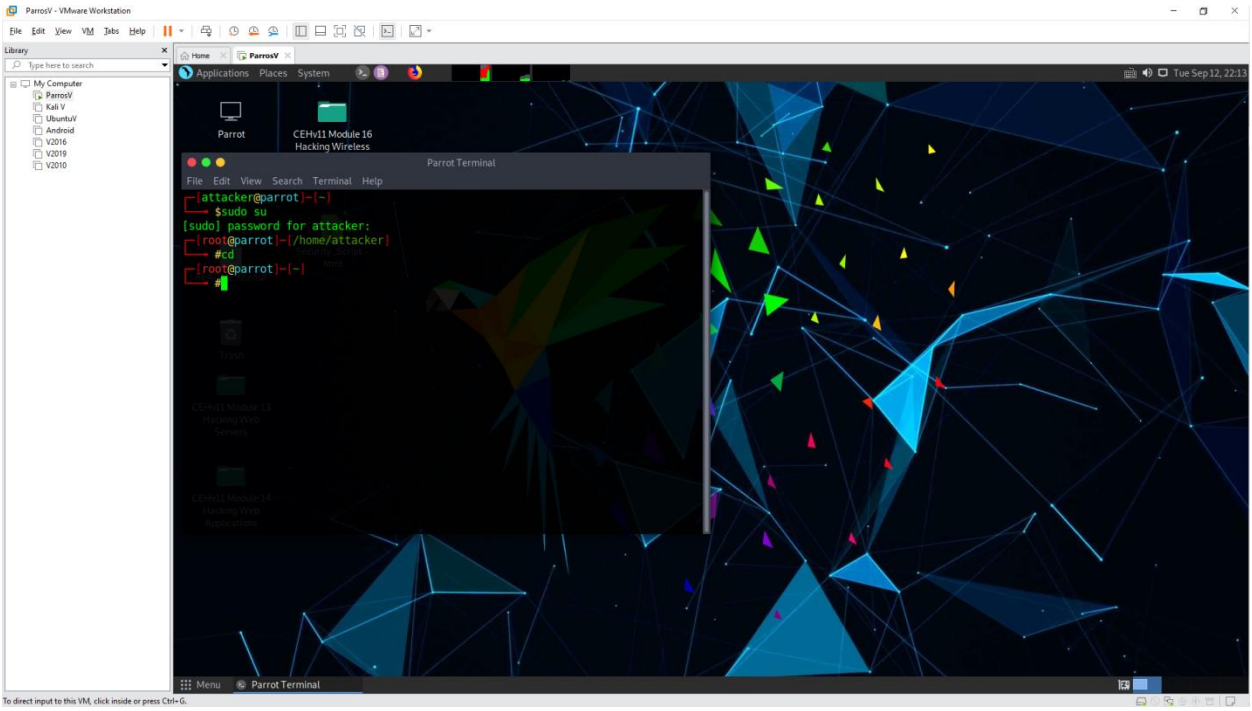
- Open terminal


ParrosV - VMware Workstation
Applications Places System
Tue Sep 12, 22:12
Parrot
CEHv11 Module 16
Hacking Wireless
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$
Menu
Parrot Terminal

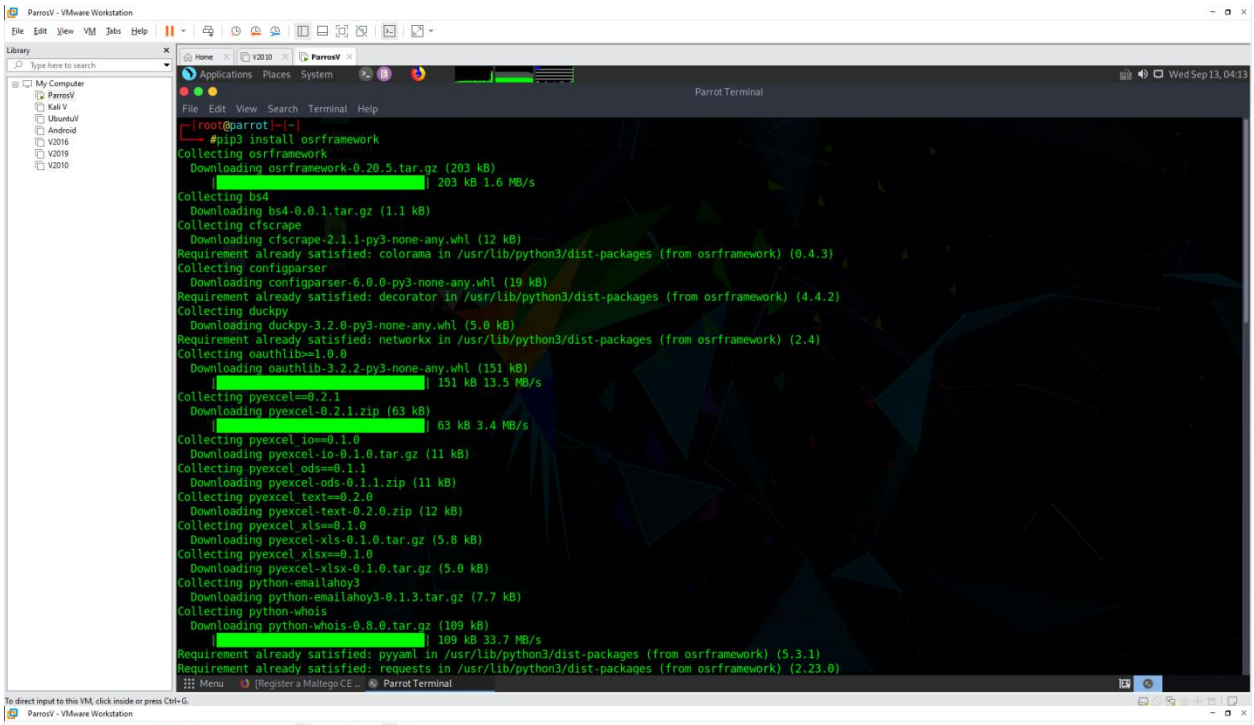
- sudo su

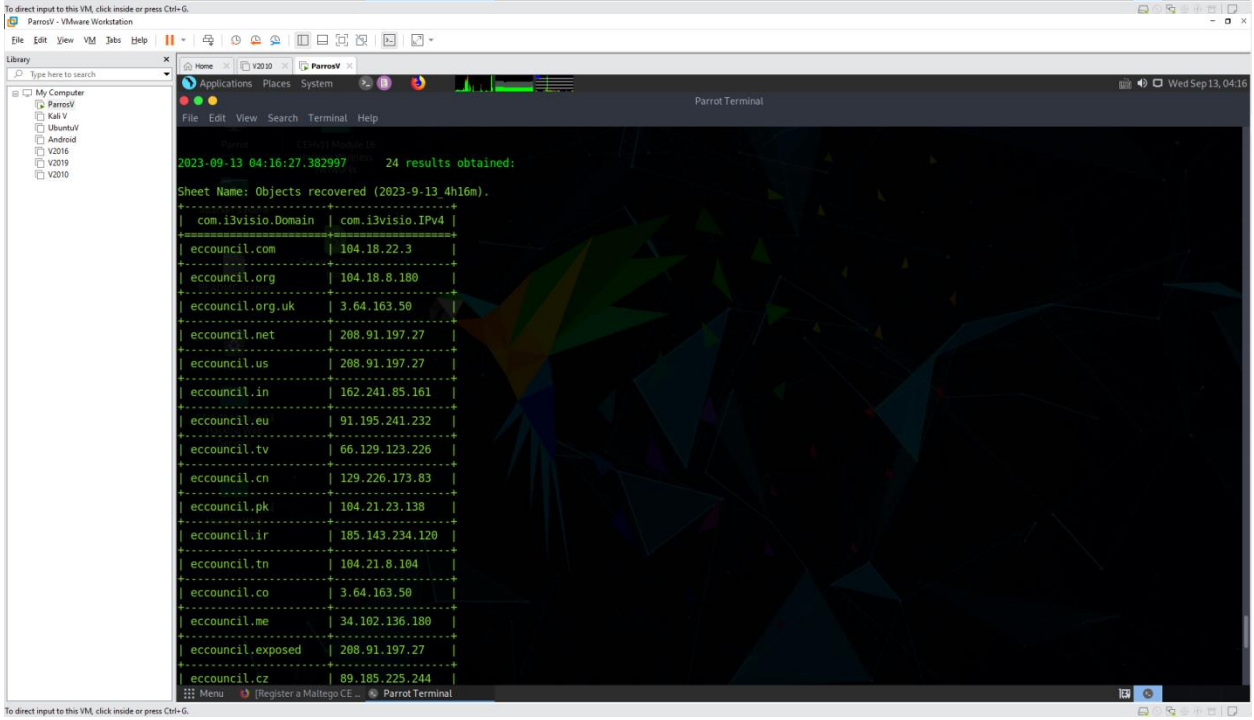

ParrosV - VMware Workstation
Applications Places System
Tue Sep 12, 22:12
Parrot
CEHv11 Module 16
Hacking Wireless
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#
Menu
Parrot Terminal

- cd



- install osrframework


ParrosV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
ParrosV
Applications Places System
Wed Sep 13, 04:13
Parrot Terminal
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-6.0.0-py3-none-any.whl (19 kB)
Requirement already satisfied: decorator in /usr/lib/python3/dist-packages (from osrframework) (4.4.2)
Collecting duckpy
Downloading duckpy-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>=1.0.0
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_io==0.1.0
Downloading pyexcel-io-0.1.0.tar.gz (11 kB)
Collecting pyexcel_ods==0.1.1
Downloading pyexcel-ods-0.1.1.zip (11 kB)
Collecting pyexcel_text==0.2.0
Downloading pyexcel-text-0.2.0.zip (12 kB)
Collecting pyexcel_xls==0.1.0
Downloading pyexcel-xls-0.1.0.tar.gz (5.8 kB)
Collecting pyexcel_xlsx==0.1.0
Downloading pyexcel-xlsx-0.1.0.tar.gz (5.0 kB)
Collecting python-emailahoy3
Downloading python-emailahoy3-0.1.3.tar.gz (7.7 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)
Menu
[Register a Maltego CE ...
Parrot Terminal
To direct input to this VM, click inside or press Ctrl+G.


ParrosV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
ParrosV
Applications Places System
Wed Sep 13, 04:16
Parrot Terminal
File Edit View Search Terminal Help
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
Menu
[Register a Maltego CE ...
Parrot Terminal
To direct input to this VM, click inside or press Ctrl+G.