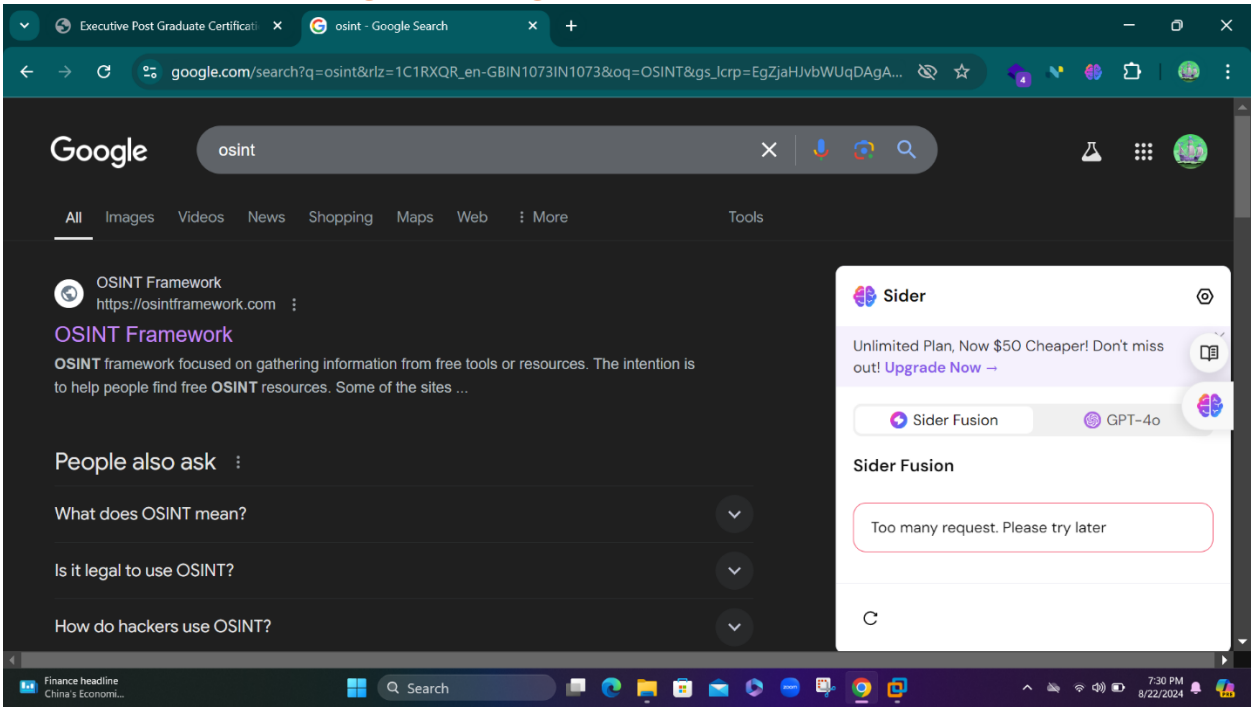
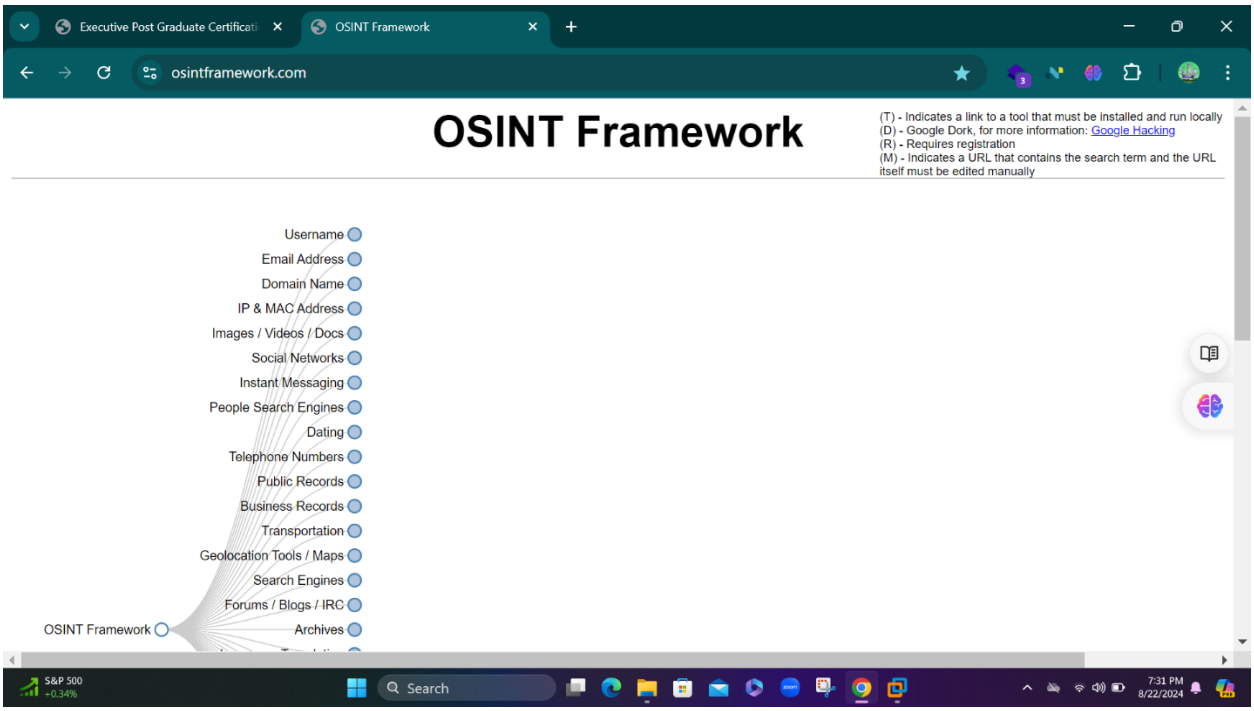
Executive Post Graduate Certification in Cyber Security and Ethical Hacking

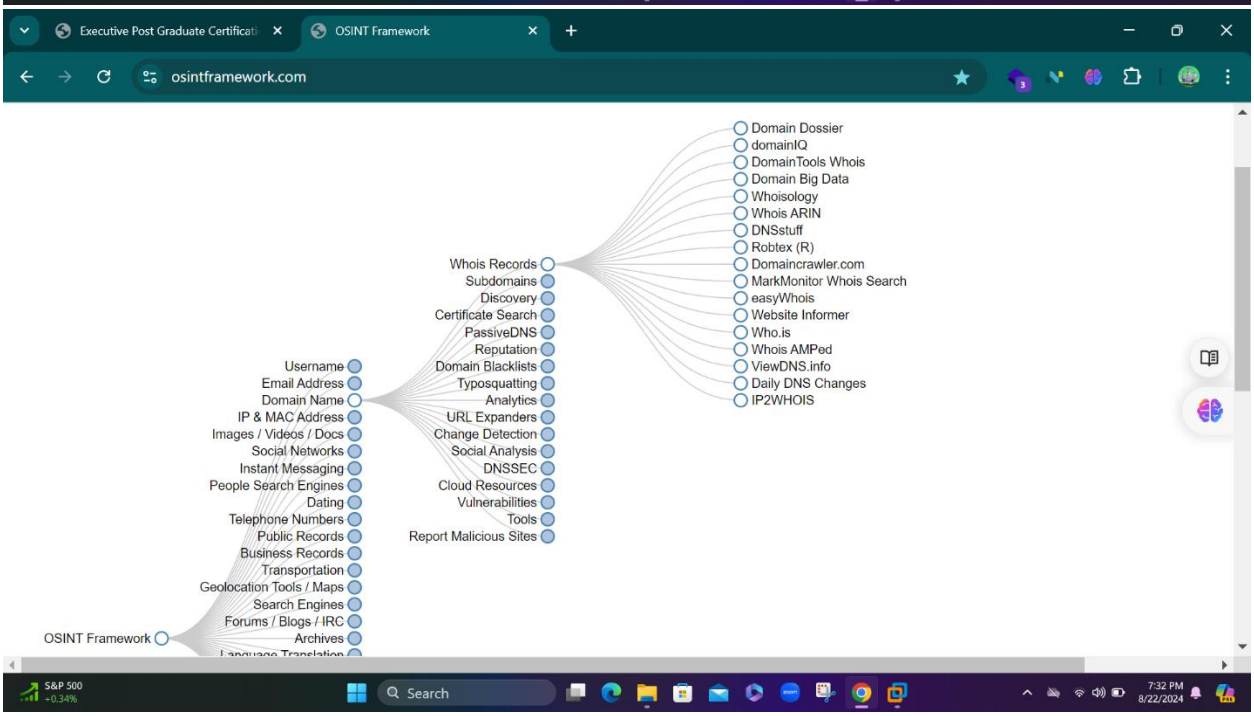
ASSIGNMENT-02

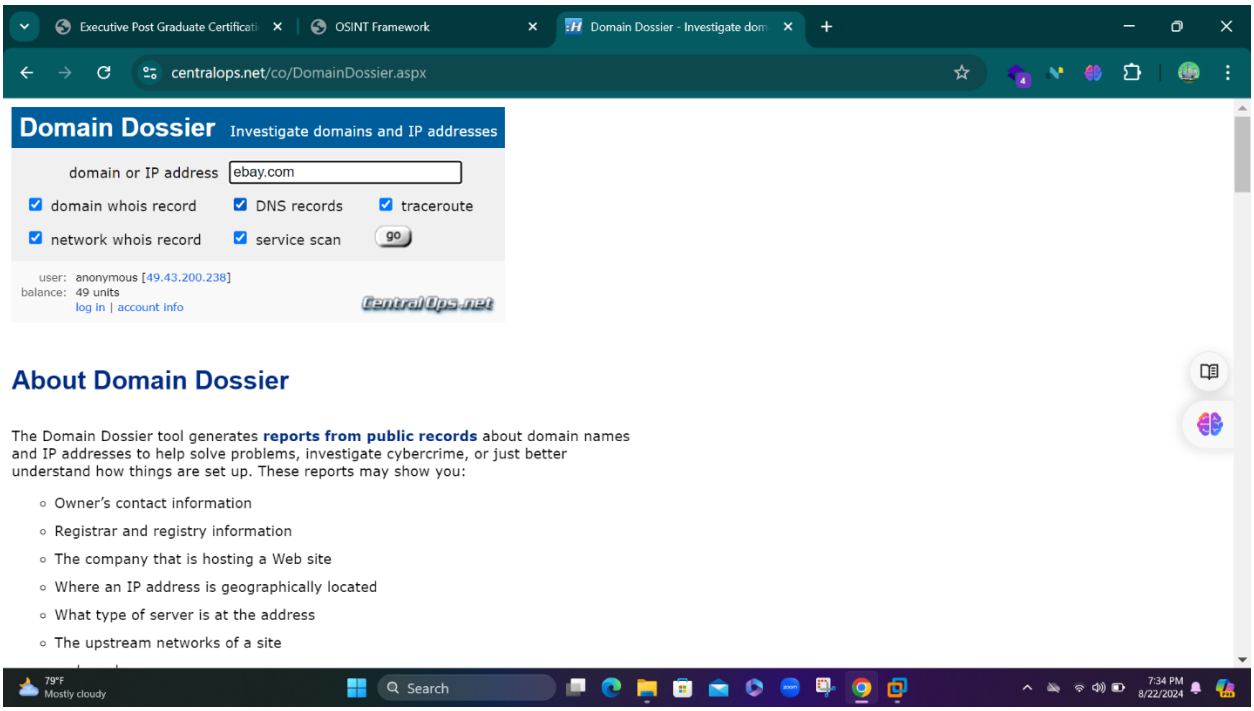
Objectives: 01

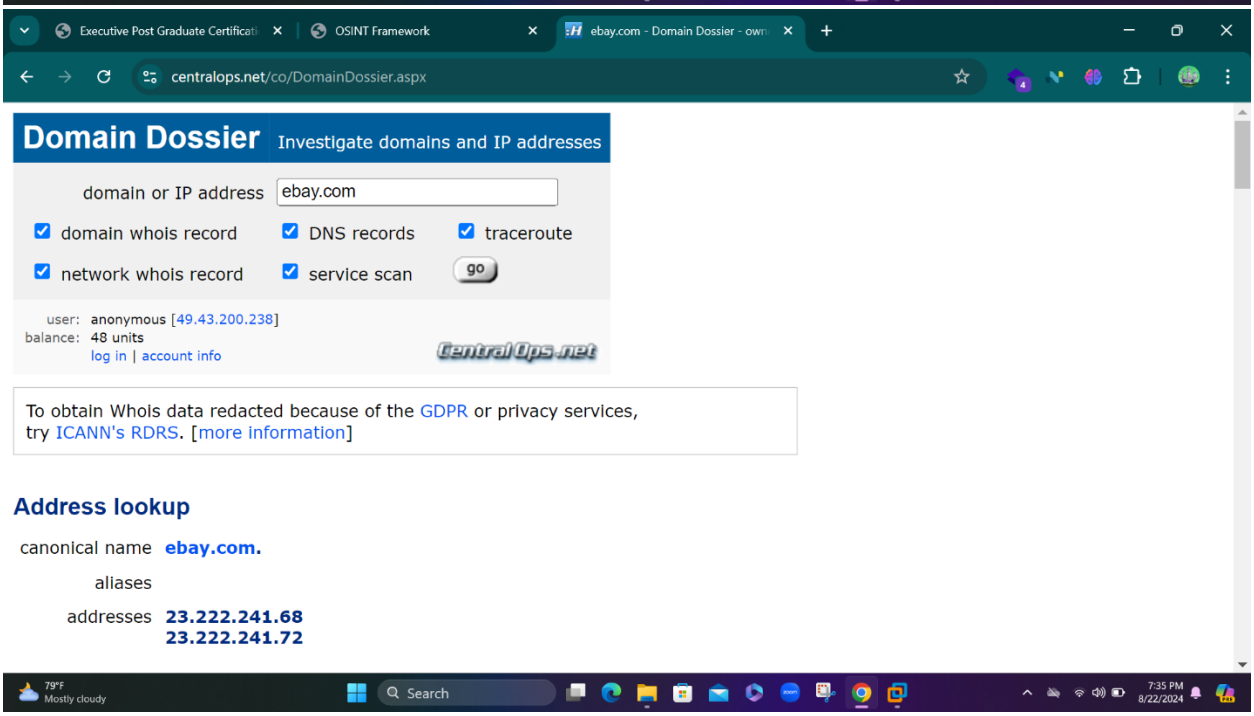
- Footprint a target using the OSINT Framework.

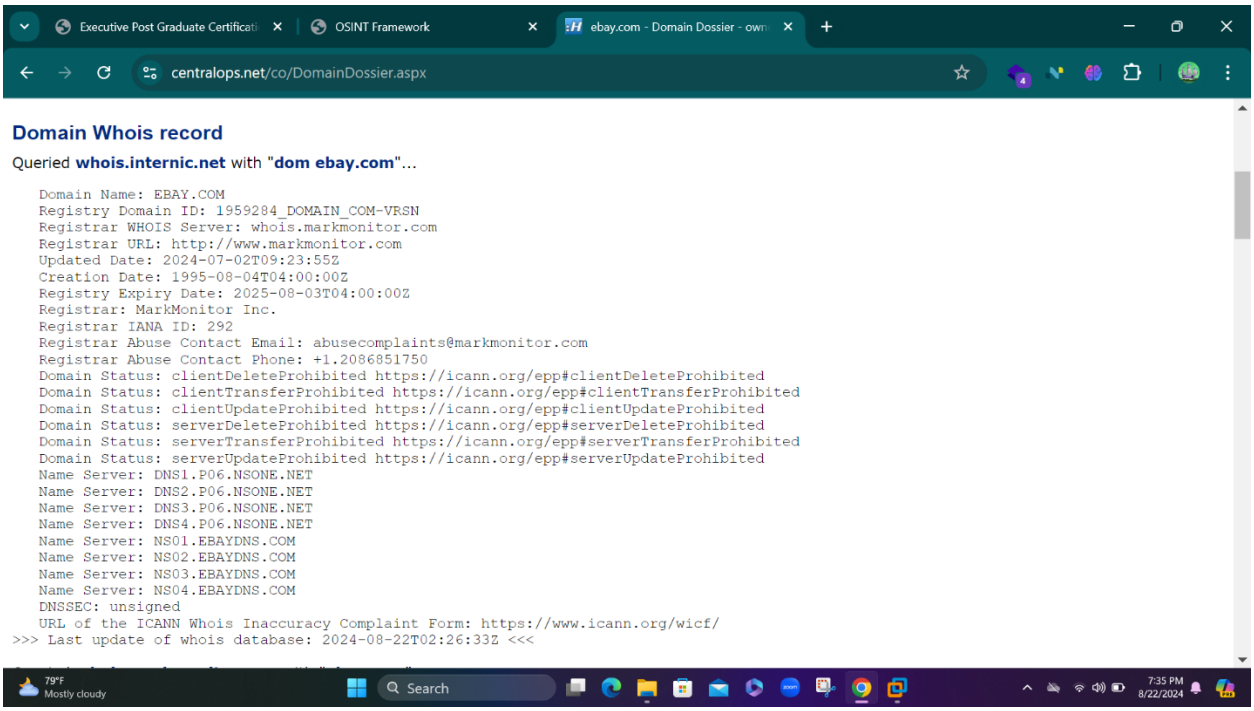


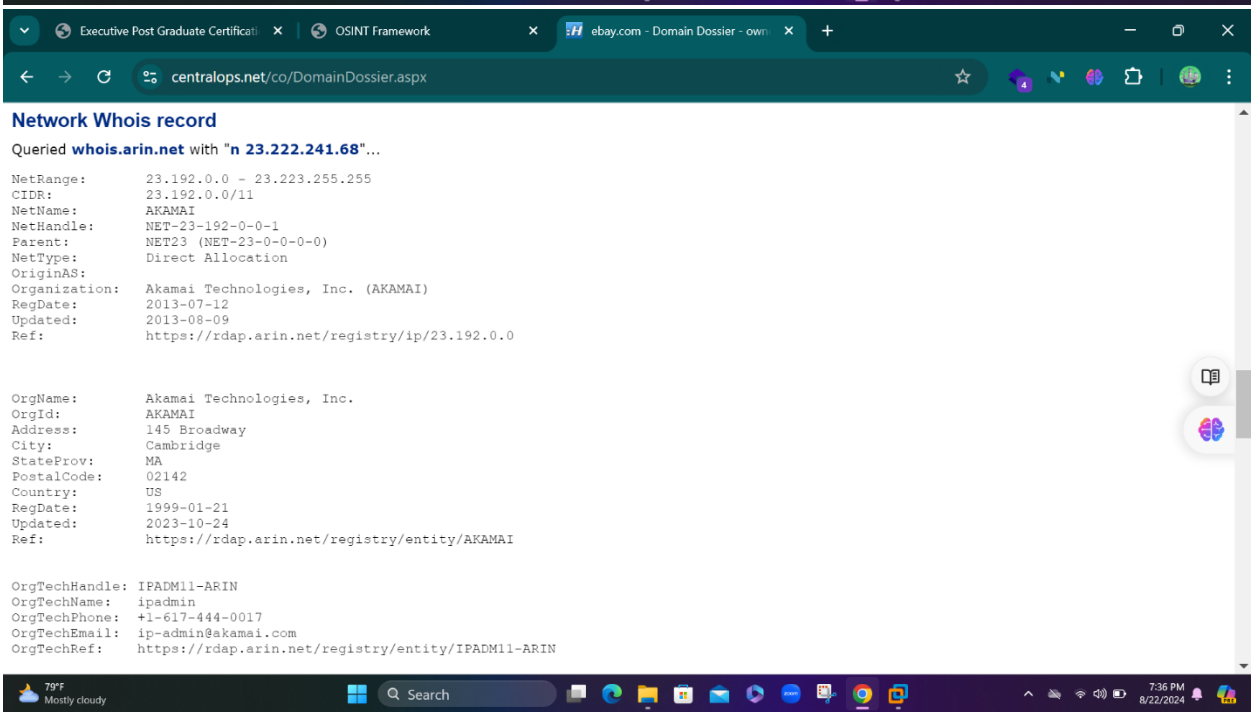

Executive Post Graduate Certificati
OSINT Framework
osintframework.com
OSINT Framework
(T) - Indicates a link to a tool that must be installed and run locally
(D) - Google Dork, for more information: Google Hacking
(R) - Requires registration
(M) - Indicates a URL that contains the search term and the URL itself must be edited manually
Username
Email Address
Domain Name
IP & MAC Address
Images / Videos / Docs
Social Networks
Instant Messaging
People Search Engines
Dating
Telephone Numbers
Public Records
Business Records
Transportation
Geolocation Tools / Maps
Search Engines
Forums / Blogs / IRC
Archives
OSINT Framework
S&P 500
-0.34%
Search
7:31 PM
8/22/2024

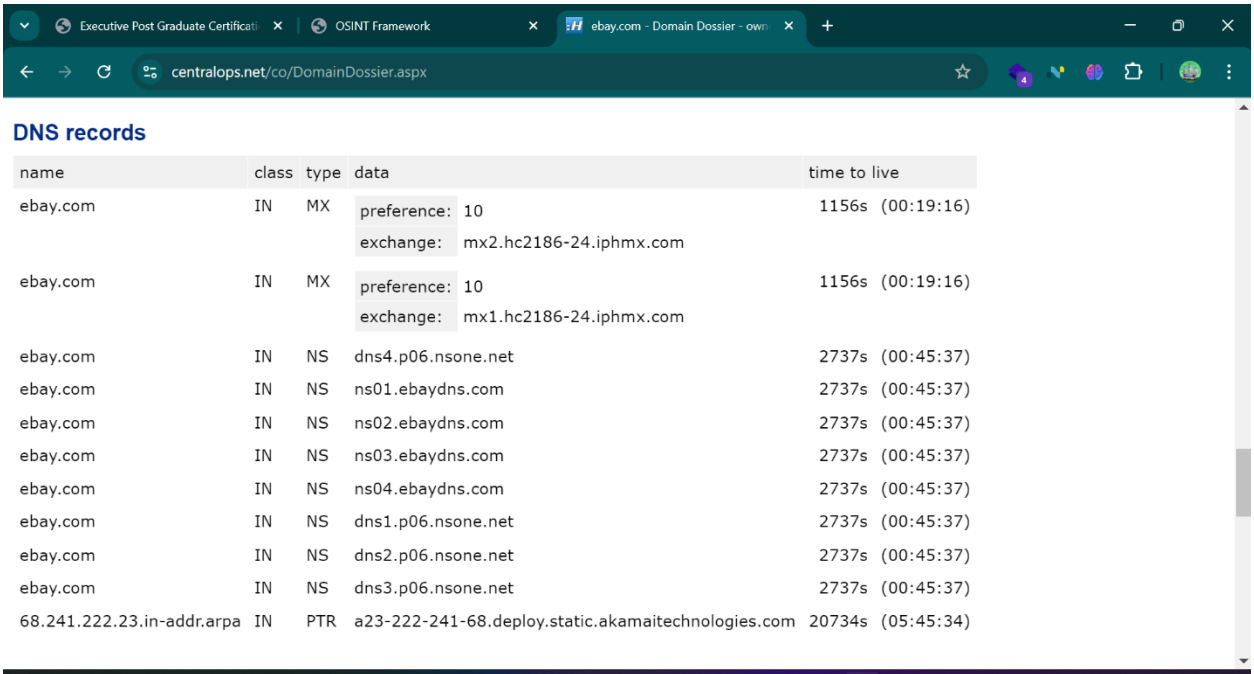

Executive Post Graduate Certificati
OSINT Framework
osintframework.com
Domain Dossier
domainIQ
DomainTools Whois
Domain Big Data
Whoisology
Whois ARIN
DNSstuff
Robtex (R)
Domaincrawler.com
MarkMonitor Whois Search
easyWhois
Website Informer
Who.is
Whois AMPed
ViewDNS.info
Daily DNS Changes
IP2WHOIS
Whois Records
Subdomains
Discovery
Certificate Search
PassiveDNS
Reputation
Domain Blacklists
Typosquatting
Analytics
URL Expanders
Change Detection
Social Analysis
DNSSEC
Cloud Resources
Vulnerabilities
Tools
Report Malicious Sites
Username
Email Address
Domain Name
IP & MAC Address
Images / Videos / Docs
Social Networks
Instant Messaging
People Search Engines
Dating
Telephone Numbers
Public Records
Business Records
Transportation
Geolocation Tools / Maps
Search Engines
Forums / Blogs / IRC
Archives
OSINT Framework
S&P 500
-0.34%
Search
7:32 PM
8/22/2024


Executive Post Graduate Certificati
OSINT Framework
Domain Dossier - Investigate dom
centralops.net/co/DomainDossier.aspx
Domain Dossier
Investigate domains and IP addresses
domain or IP address
ebay.com
domain whois record
DNS records
traceroute
network whois record
service scan
go
user: anonymous [49.43.200.238]
balance: 49 units
log in | account info
CentralOps.net
About Domain Dossier
The Domain Dossier tool generates reports from public records about domain names and IP addresses to help solve problems, investigate cybercrime, or just better understand how things are set up. These reports may show you:
Owner's contact information
Registrar and registry information
The company that is hosting a Web site
Where an IP address is geographically located
What type of server is at the address
The upstream networks of a site
79°F
Mostly cloudy
Search
7:34 PM
8/22/2024


Executive Post Graduate Certificati
OSINT Framework
ebay.com - Domain Dossier - own
centralops.net/co/DomainDossier.aspx
Domain Dossier
Investigate domains and IP addresses
domain or IP address
ebay.com
domain whois record
DNS records
traceroute
network whois record
service scan
go
user: anonymous [49.43.200.238]
balance: 48 units
log in | account info
CentralOps.net
To obtain Whois data redacted because of the GDPR or privacy services, try ICANN's RDRS. [more information]
Address lookup
canonical name ebay.com.
aliases
addresses 23.222.241.68
23.222.241.72
79°F
Mostly cloudy
Search
7:35 PM
8/22/2024

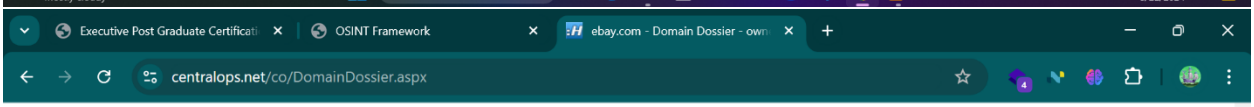

Executive Post Graduate Certificati
OSINT Framework
ebay.com - Domain Dossier - own
centralops.net/co/DomainDossier.aspx
Domain Whois record
Queried whois.internic.net with "dom ebay.com"...
Domain Name: EBAY.COM
Registry Domain ID: 1959284_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2024-07-02T09:23:55Z
Creation Date: 1995-08-04T04:00:00Z
Registry Expiry Date: 2025-08-03T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: DNS1.P06.NSONE.NET
Name Server: DNS2.P06.NSONE.NET
Name Server: DNS3.P06.NSONE.NET
Name Server: DNS4.P06.NSONE.NET
Name Server: NS01.EBAYDNS.COM
Name Server: NS02.EBAYDNS.COM
Name Server: NS03.EBAYDNS.COM
Name Server: NS04.EBAYDNS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-08-22T02:26:33Z <<<
79°F
Mostly cloudy
Search
7:35 PM
8/22/2024


Executive Post Graduate Certificati
OSINT Framework
ebay.com - Domain Dossier - own
centralops.net/co/DomainDossier.aspx
Network Whois record
Queried whois.arin.net with "n 23.222.241.68"...
NetRange: 23.192.0.0 - 23.223.255.255
CIDR: 23.192.0.0/11
NetName: AKAMAI
NetHandle: NET-23-192-0-0-1
Parent: NET23 (NET-23-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Akamai Technologies, Inc. (AKAMAI)
RegDate: 2013-07-12
Updated: 2013-08-09
Ref: https://rdap.arin.net/registry/ip/23.192.0.0
OrgName: Akamai Technologies, Inc.
OrgId: AKAMAI
Address: 145 Broadway
City: Cambridge
StateProv: MA
PostalCode: 02142
Country: US
RegDate: 1999-01-21
Updated: 2023-10-24
Ref: https://rdap.arin.net/registry/entity/AKAMAI
OrgTechHandle: IPADM11-ARIN
OrgTechName: ipadmin
OrgTechPhone: +1-617-444-0017
OrgTechEmail: ip-admin@akamai.com
OrgTechRef: https://rdap.arin.net/registry/entity/IPADM11-ARIN
79°F
Mostly cloudy
Search
7:36 PM
8/22/2024



DNS records

name	class	type	data	time to live
ebay.com	IN	MX	preference: 10 exchange: mx2.hc2186-24.iphmx.com	1156s (00:19:16)
ebay.com	IN	MX	preference: 10 exchange: mx1.hc2186-24.iphmx.com	1156s (00:19:16)
ebay.com	IN	NS	dns4.p06.nsone.net	2737s (00:45:37)
ebay.com	IN	NS	ns01.ebaydns.com	2737s (00:45:37)
ebay.com	IN	NS	ns02.ebaydns.com	2737s (00:45:37)
ebay.com	IN	NS	ns03.ebaydns.com	2737s (00:45:37)
ebay.com	IN	NS	ns04.ebaydns.com	2737s (00:45:37)
ebay.com	IN	NS	dns1.p06.nsone.net	2737s (00:45:37)
ebay.com	IN	NS	dns2.p06.nsone.net	2737s (00:45:37)
ebay.com	IN	NS	dns3.p06.nsone.net	2737s (00:45:37)
68.241.222.23.in-addr.arpa	IN	PTR	a23-222-241-68.deploy.static.akamaitechnologies.com	20734s (05:45:34)

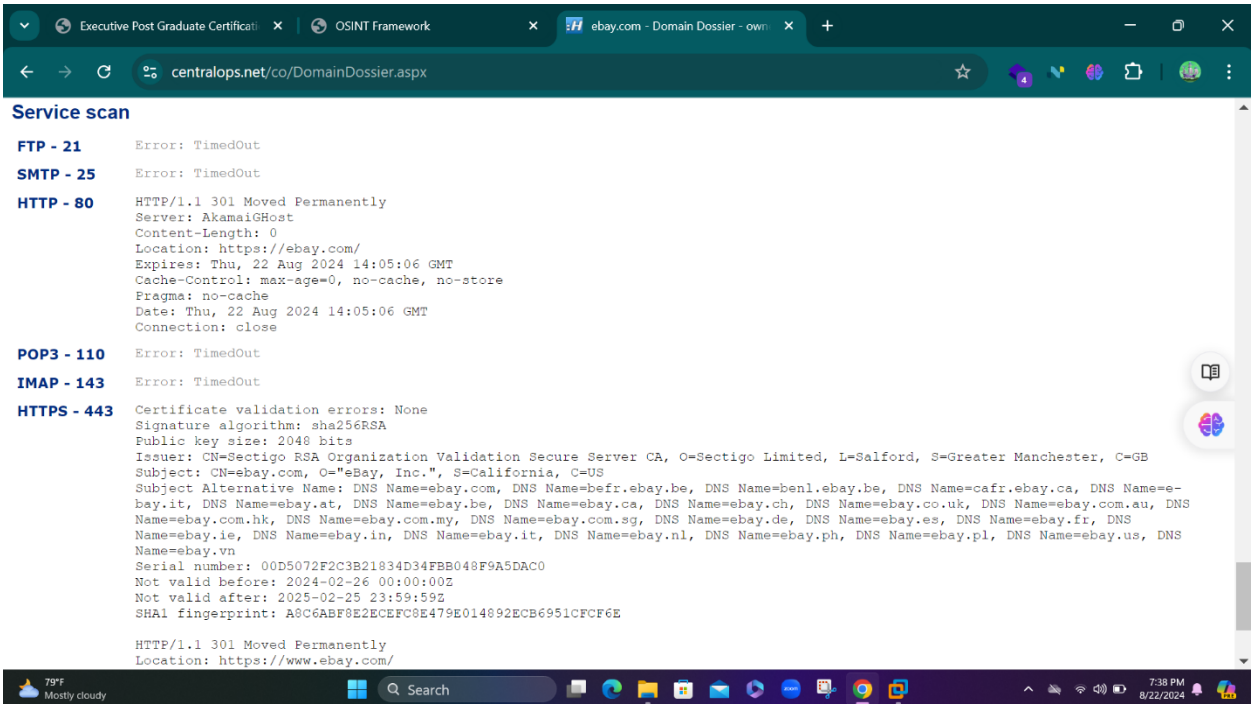


Traceroute

Tracing route to **ebay.com [23.222.241.68]**...

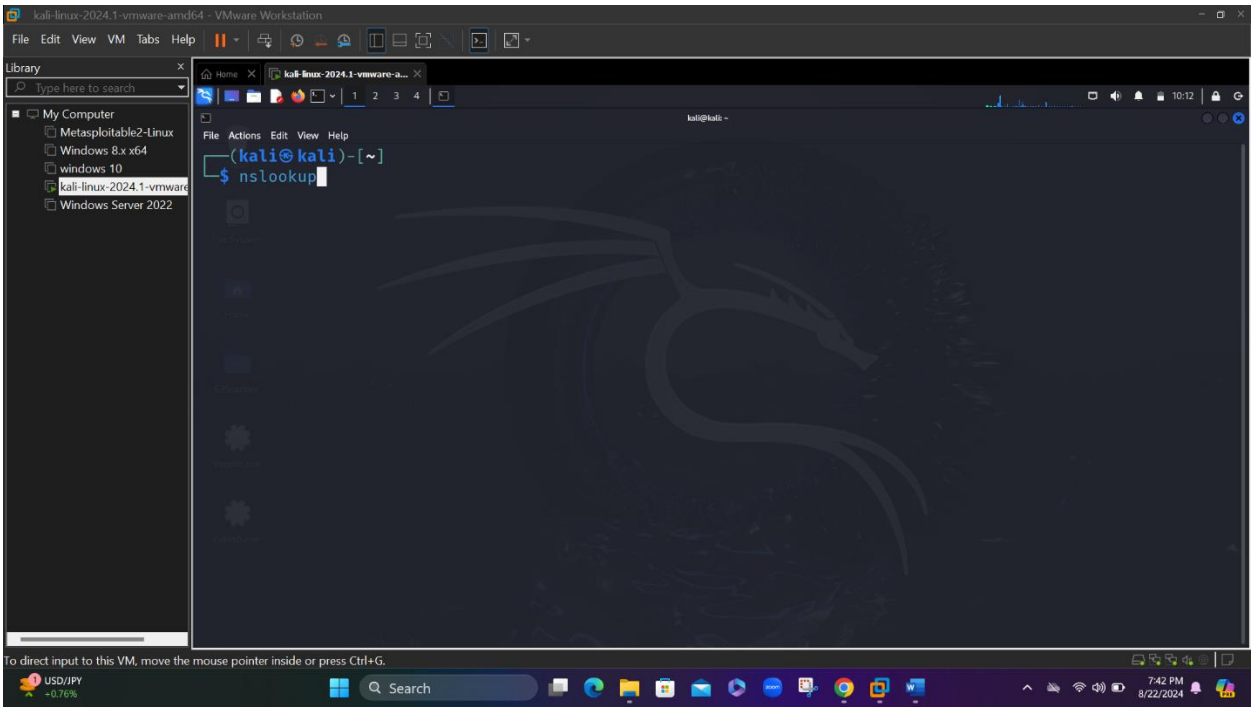
hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	1	1	0	169.254.158.58	
2	8	1	1	169.48.118.158	ae103.ppr02.dal13.networklayer.com
3	1	0	0	169.48.118.130	82.76.30a9.ip4.static.sl-reverse.com
4	2	3	3	169.45.18.86	ae16.cbs01.eq01.dal03.networklayer.com
5	2	1	2	50.97.17.55	ae33.bbr02.eq01.dal03.networklayer.com
6	2	2	2	206.53.202.27	de-cix-dfw1.netarch.akamai.com
7	*	*	*		
8	*	*	*		
9	*	*	*		
10	2	2	2	23.222.241.68	a23-222-241-68.deploy.static.akamaitechnologies.com

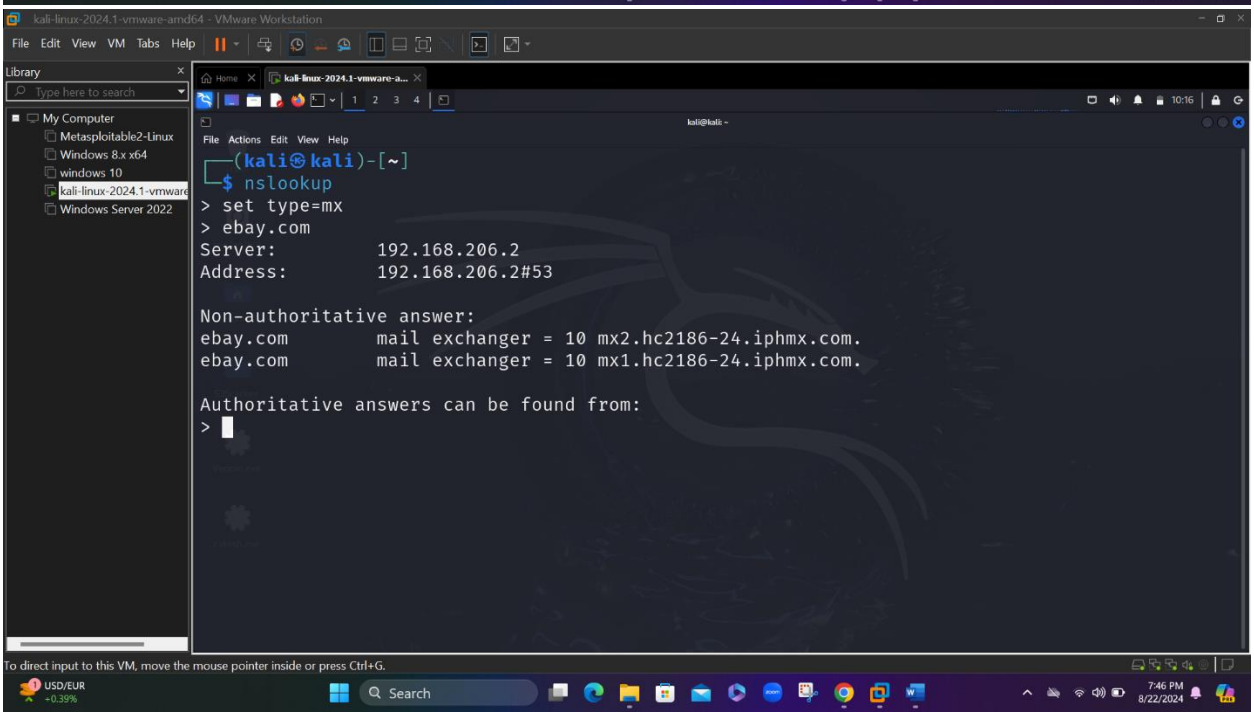
Trace complete

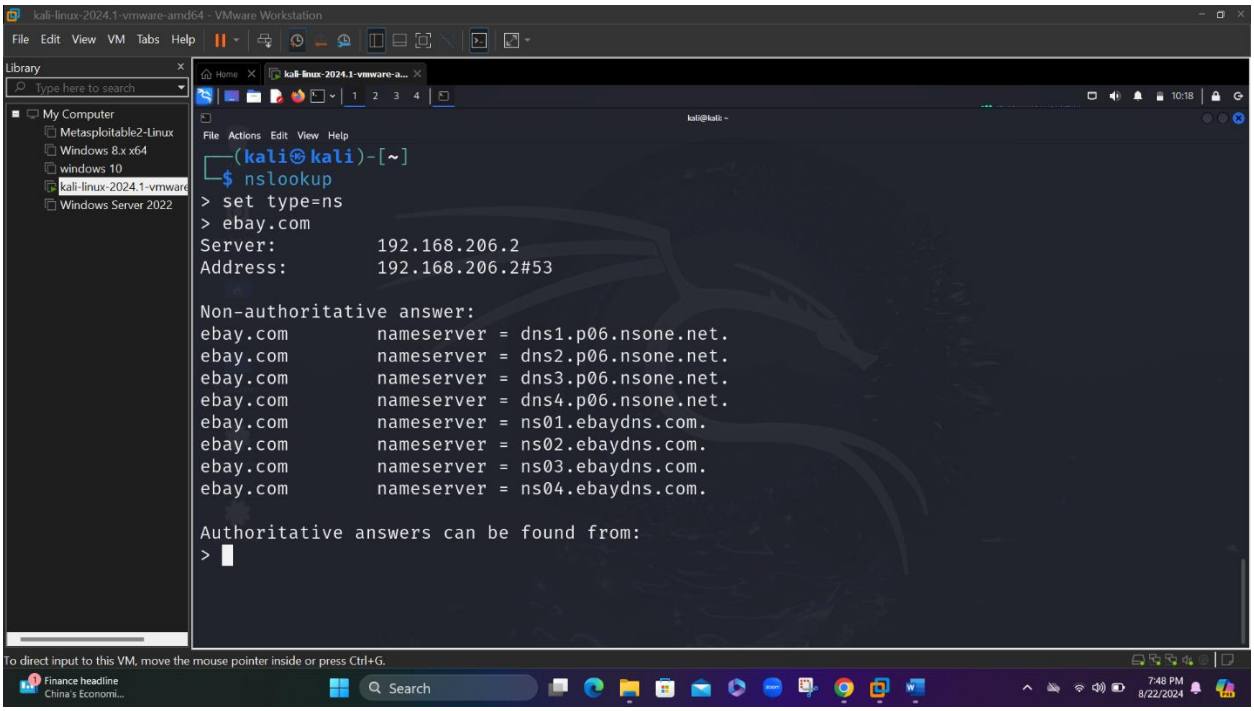


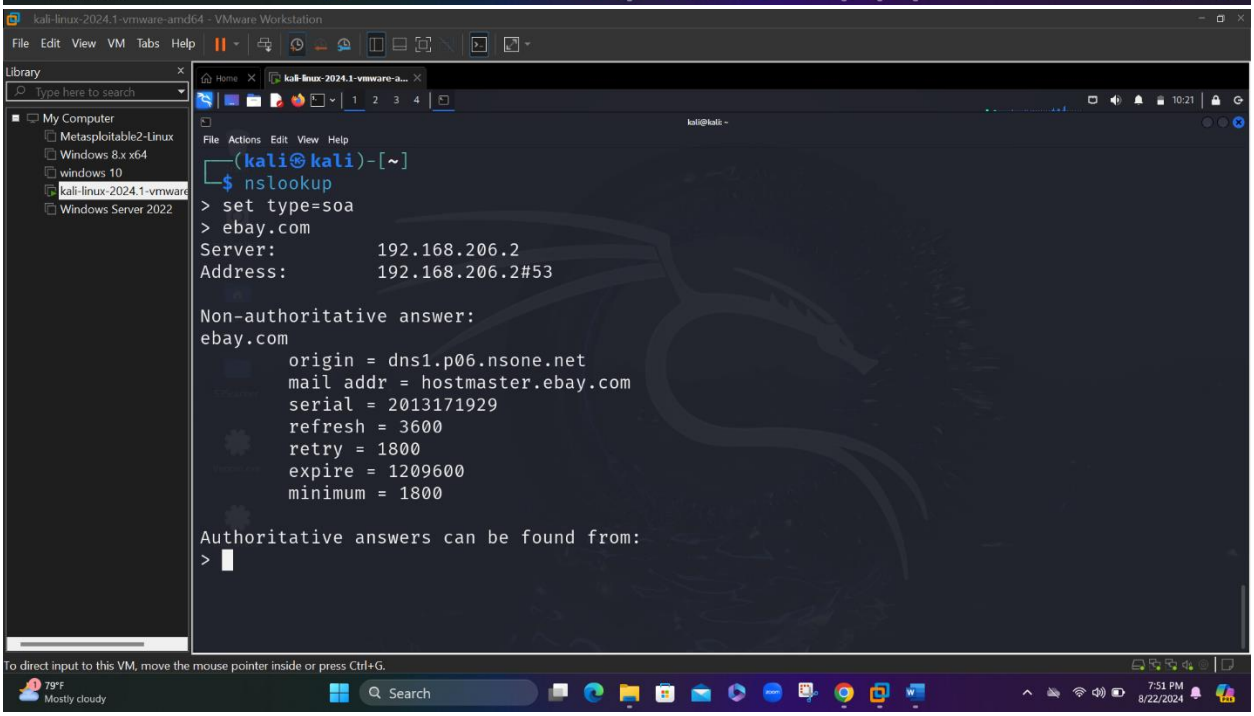
Objectives: 02

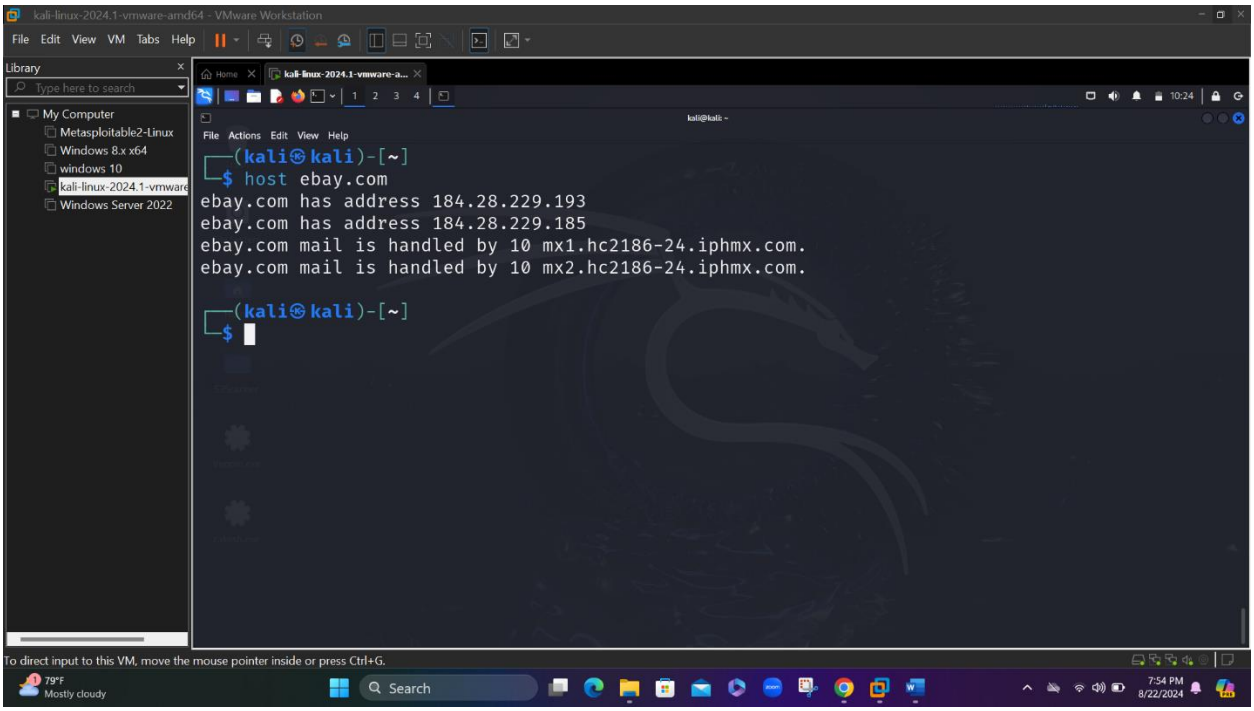
- Gather DNS information using nslookup command line utility and online tools


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Metasploitable2-Linux
Windows 8.x x64
windows 10
kali-linux-2024.1-vmware
Windows Server 2022
Home
kali-linux-2024.1-vmware-a...
File Actions Edit View Help
(kali㉿kali)-[~]
$ nslookup
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
USD/JPY
+0.76%
Search
7:42 PM
8/22/2024


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Metasploitable2-Linux
Windows 8.x x64
windows 10
kali-linux-2024.1-vmware
Windows Server 2022
Home
kali-linux-2024.1-vmware-a...
File Actions Edit View Help
(kali㉿kali)-[~]
$ nslookup
> set type=mx
> ebay.com
Server: 192.168.206.2
Address: 192.168.206.2#53
Non-authoritative answer:
ebay.com mail exchanger = 10 mx2.hc2186-24.iphmx.com.
ebay.com mail exchanger = 10 mx1.hc2186-24.iphmx.com.
Authoritative answers can be found from:
>
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
USD/EUR
+0.39%
Search
7:46 PM
8/22/2024


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Metasploitable2-Linux
Windows 8.x x64
windows 10
kali-linux-2024.1-vmware
Windows Server 2022
Home
kali-linux-2024.1-vmware-a...
File Actions Edit View Help
(kali㉿kali)-[~]
$ nslookup
> set type=ns
> ebay.com
Server: 192.168.206.2
Address: 192.168.206.2#53
Non-authoritative answer:
ebay.com nameserver = dns1.p06.nsone.net.
ebay.com nameserver = dns2.p06.nsone.net.
ebay.com nameserver = dns3.p06.nsone.net.
ebay.com nameserver = dns4.p06.nsone.net.
ebay.com nameserver = ns01.ebaydns.com.
ebay.com nameserver = ns02.ebaydns.com.
ebay.com nameserver = ns03.ebaydns.com.
ebay.com nameserver = ns04.ebaydns.com.
Authoritative answers can be found from:
>
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Finance headline
China's Economi...
Search
7:48 PM
8/22/2024


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Metasploitable2-Linux
Windows 8.x x64
windows 10
kali-linux-2024.1-vmware
Windows Server 2022
Home
kali-linux-2024.1-vmware-a...
File Actions Edit View Help
(kali㉿kali)-[~]
$ nslookup
> set type=soa
> ebay.com
Server: 192.168.206.2
Address: 192.168.206.2#53
Non-authoritative answer:
ebay.com
origin = dns1.p06.nsone.net
mail addr = hostmaster.ebay.com
serial = 2013171929
refresh = 3600
retry = 1800
expire = 1209600
minimum = 1800
Authoritative answers can be found from:
>
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
79°F
Mostly cloudy
Search
7:51 PM
8/22/2024



Submitted By

SairajMothukuri

[sairajmothukuri28@gmail.com]