Quiz #1

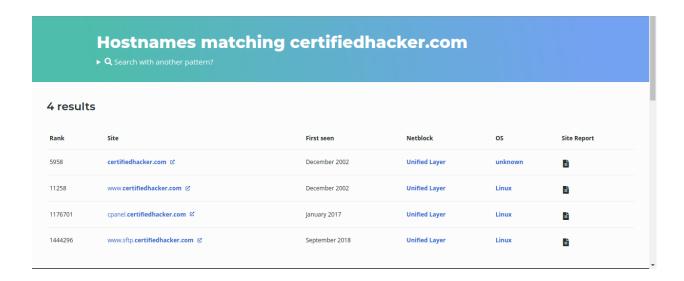
Given the website http://certifiedhacker.com. Using the following tools you learned in Footprinting module to find information about:

1- IP address "162.241.216.11"

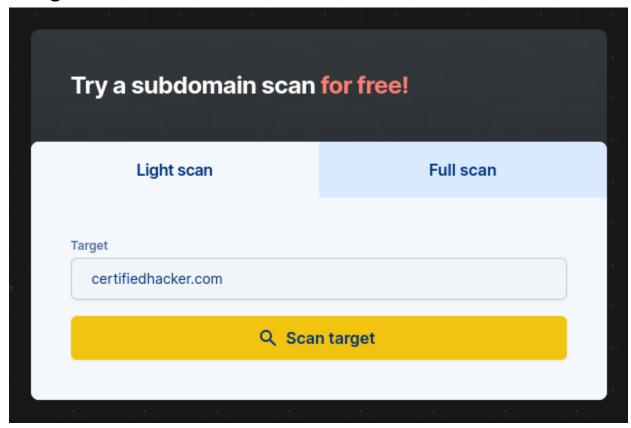
```
ping certifiedhacker.com
PING certifiedhacker.com (162.241.216.11) 56(84) bytes of data.
```

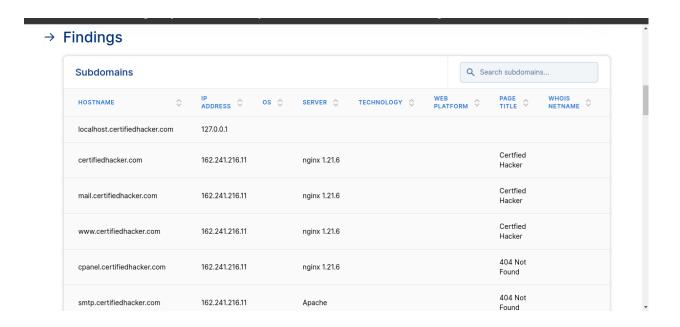
2- Subdomain



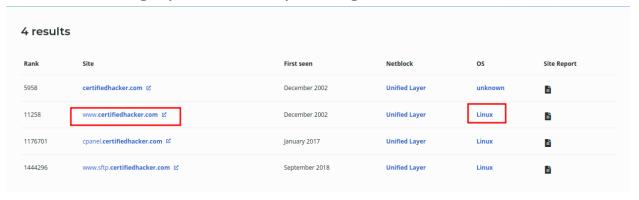


Using Pentest





3- OS through passive footprinting



4- Hosting websites

Site	http://certifiedhacker.com 먼 Unified Layer	
Netblock Owner		
Hosting company	Newfold Digita	
Hosting country	■■ US @	
IPv4 address	162.241.216.11 (VirusTotal @	



urglechket: nttps://rdap.arin.net/registry/entity/ENU/4-AKIN

DNS records

name	class	type	data	time to live	
certifiedhacker.com	IN	Α	162.241.216.11	4851s (01:20:51)	
certifiedhacker.com	IN	NS	ns2.bluehost.com	60212s (16:43:32)	
certifiedhacker.com	IN	NS	ns1.bluehost.com	60212s (16:43:32)	
11.216.241.162.in-addr.arpa	IN	HINFO	CPU: RFC8482 OS:	3789s (01:03:09)	
216.241.162.in-addr.arpa	IN	HINFO	CPU: RFC8482 OS:	3130s (00:52:10)	
216.241.162.in-addr.arpa	IN	NS	ns2.unifiedlayer.com	8349s (02:19:09)	
216.241.162.in-addr.arpa	IN	NS	ns1.unifiedlayer.com	8349s (02:19:09)	
end URL for this output return to CentralOps.net, a service of Hexillion					

5-DNS

```
# Coded By Ahmed Aboul-Ela - @aboul3la

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for certifiedhacker.com

[-] verbosity is enabled, will show the subdomains results in realtime

[-] Searching now in Bing..

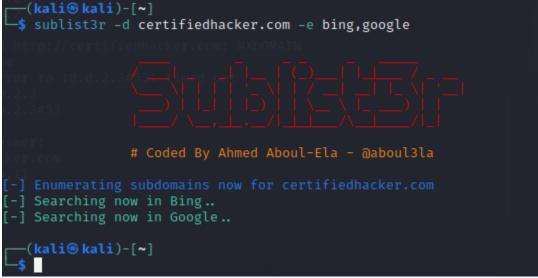
[-] Searching now in Google..

[-] Searching now in Netcraft..
```

6- DNS zone transfer

7- Fmails

```
email addresses for the target domain.
View the full module info with the info -d command.
msf6 auxiliary(gather/search_email_collector) > set DOMAIN certifiedh
DOMAIN => certifiedhacker.com
msf6 auxiliary(gather/search email collector) > ru
[-] Unknown command: ru
msf6 auxiliary(gather/search_email_collector) > run
[*] Harvesting emails .....
[*] Searching Google for email addresses from certifiedhacker.com
[*] Extracting emails from Google search results...
[*] Searching Bing email addresses from certifiedhacker.com
[*] Extracting emails from Bing search results...
[*] Searching Yahoo for email addresses from certifiedhacker.com
[*] Extracting emails from Yahoo search results...
[*] Located 0 email addresses for certifiedhacker.com
[*] Auxiliary module execution completed
  —(kali⊛kali)-[~]
 -$ sublist3r -d certifiedhacker.com -e bing,google
```



8- Files

```
(kali® kali)-[~]
$ metagoofil -d certifiedhacker.com -f -l 10 -o /home/kali/Desktop -t pdf -e 10
[*] Searching for 10 .pdf files and waiting 10.0 seconds between searches
[*] Results: 3 .pdf files found
https://certifiedhacker.com/docs/923332.pdf
http://certifiedhacker.com/docs/922990.pdf
https://certifiedhacker.com/docs/NIST.SP.800-63a.pdf
[+] Done!

(kali® kali)-[~]

(kali® kali)-[~]
```