

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”

```
(kali㉿kali)-[~]  
$ host certifiedhacker.com  
certifiedhacker.com has address 162.241.216.11  
  
(kali㉿kali)-[~]  
$
```

```
ping: http://certifiedhacker.com: Name or service not known  
ping certifiedhacker.com  
PING certifiedhacker.com (162.241.216.11) 56(84) bytes of data.  
■
```

2- Subdomain

Hostnames matching aliexpress.com

▼ 🔍 Search with another pattern?





Subdomain matches ▼

<http://certifiedhacker.com>

Example: site contains [.netcraft.com](#)

[Search](#)

[Search tips](#)

Hostnames matching certifiedhacker.com					
🔍 Search with another pattern?					
4 results					
Rank	Site	First seen	Netblock	OS	Site Report
5958	certifiedhacker.com 🔗	December 2002	Unified Layer	unknown	
11258	www.certifiedhacker.com 🔗	December 2002	Unified Layer	Linux	
1176701	cpanel.certifiedhacker.com 🔗	January 2017	Unified Layer	Linux	
1444296	www.sftp.certifiedhacker.com 🔗	September 2018	Unified Layer	Linux	

Using Pentest

Try a subdomain scan **for free!**

Light scan

Full scan

Target

certifiedhacker.com

🔍 Scan target

→ Findings

Subdomains							Search subdomains...	
HOSTNAME	IP ADDRESS	OS	SERVER	TECHNOLOGY	WEB PLATFORM	PAGE TITLE	WHOIS NETNAME	
localhost.certifiedhacker.com	127.0.0.1							
certifiedhacker.com	162.241.216.11		nginx 1.21.6			Certified Hacker		
mail.certifiedhacker.com	162.241.216.11		nginx 1.21.6			Certified Hacker		
www.certifiedhacker.com	162.241.216.11		nginx 1.21.6			Certified Hacker		
cpanel.certifiedhacker.com	162.241.216.11		nginx 1.21.6			404 Not Found		
smtp.certifiedhacker.com	162.241.216.11		Apache			404 Not Found		

3- OS through passive footprinting

4 results

Rank	Site	First seen	Netblock	OS	Site Report
5958	certifiedhacker.com	December 2002	Unified Layer	unknown	
11258	www.certifiedhacker.com	December 2002	Unified Layer	Linux	
1176701	cpanel.certifiedhacker.com	January 2017	Unified Layer	Linux	
1444296	www.sftp.certifiedhacker.com	September 2018	Unified Layer	Linux	

4- Hosting websites

Site	http://certifiedhacker.com 
Netblock Owner	Unified Layer
Hosting company	Newfold Digital
Hosting country	 US 
IPv4 address	162.241.216.11 (VirusTotal 
IPv4 autonomous systems	AS46606 

```
(kali㉿kali)-[~]
└─$ theHarvester -d certifiedhacker.com
*****
*                                     *
* [ _ ] certifi                     *
* [ _ ] [ _ ] ^ ^                   *
* [ _ ] [ _ ] [ _ ] \ /              *
* [ _ ] [ _ ] [ _ ] \ /              *
* [ _ ] [ _ ] [ _ ] \ /              *
* [ _ ] [ _ ] [ _ ] \ /              *
* [ _ ] [ _ ] [ _ ] \ /              *
* theHarvester 4.2.0                 *
* Coded by Christian Martorella      *
* Edge-Security Research             *
* cmartorella@edge-security.com     *
*                                    *
*****
[*] No IPs found.
[*] No emails found.
[*] No hosts found.
```

org:techner: https://rdap.arin.net/registry/entity/ENU/4-AK1N

DNS records

name	class	type	data	time to live
certifiedhacker.com	IN	A	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

```
(kali㉿kali)-[~]
└─$ sublist3r -d certifiedhacker.com -v -e bing,google,netcraft
0.2.3#53
nd http://certifi
com
error to 10.0.2.3#53
0.2.3
0.2.3#53
# 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..

(kali㉿kali)-[~]
└─$
```

6- DNS zone transfer

```
dig: couldn't get address for 'ns1.certifiedhacker.com': not found

(kali㉿kali)-[~]
└─$ dig AXFR certifiedhacker @ns2.certifiedhacker.com
dig: couldn't get address for 'ns2.certifiedhacker.com': not found

(kali㉿kali)-[~]
└─$
```

7- Emails

email addresses for the target domain.

View the full module info with the `info -d` command.

```
msf6 auxiliary(gather/search_email_collector) > set DOMAIN certifiedhacker.com
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
http://certifiedhacker.com: NXDOMAIN
n
ror to 10.0.2.3#53
2.3
2.3#53
ower:
ker.com
11)
[-] Enumerating subdomains now for certifiedhacker.com
[-] Searching now in Bing..
[-] Searching now in Google..

(kali㉿kali)-[~]
$
```

