

## DeepBlue Challenges

Challenge

214 Solves



### DeepBlue Web Server 10

OSINT

A new security training company Secure in the Deep Blue has been started to compete with Security Blue Team. Can you determine the web server of their website?

- ☐ Apache
- ☐ Nginx
- ☐ IIS
- ☐ GWS

You only have two attempts to select the right answer. (This is Part 1 of 4)

Unlock Hint for 5 points

Submit

**Answer:** This is part 1 of a 4-part Challenge. Google secureinthedeepblue and we find a domain registered page that point the website. When you visit the web page you are presented with the default webserver page. Nginx

cubdomain.com/domains-registered-by-date/2020-02-12/23		
cretshappiness.com	secretslagos.com	secretsofinnerspace
cretsoftstore.com	secretstashies.com	secretstothelawofat
cretsviptravel.com	secretwhiteboard.com	secretyoubeauty.coi
rtetbenefits.com	sectionaldensity.com	sectionweekwater.c
tor43.com	sector43.net	sectorlevel.com
ctorys.com	secular-franciscan.com	securakerala.com
ure-aes-financial.com	secure-flo.com	secure-login-server.ç
ure-moneyme.com	secure-tweet.com	secure-update.fr
ure219.com	secureatlantanorthdermatology.com	securecmp.com
urecorreos.com	securefilesajc.com	securefutureunlimit
urehostserverweb.com	secureinthedeepblue.com	securelayers7.com

## Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](https://nginx.org).  
Commercial support is available at [nginx.com](https://nginx.com).

*Thank you for using nginx.*

Challenge

145 Solves



## DeepBlue on the Port

5

General Knowledge

You are looking to exploit Secure in the Deep Blue, for leaking classified information about their competitors new exam. How many ports are open on their website? (Use nmap -sT)

- ☐ 2
- ☐ 3
- ☐ 5
- ☐ 6

You only have two attempts to select the right answer. (This is Part 2 of 4)

Submit

**Answer:** This is part 2 of a 4-part Challenge. Using Nmap to scan `secureinthedeepblue.com`. The results show 3 open ports. Only 2 are used for the website, port 22 is used for SSH. Answer is 2

```
kali@kali:~/Pictures$ nmap -sT www.secureinthedeepblue.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-16 08:31 EDT
Nmap scan report for www.secureinthedeepblue.com (52.205.129.193)
Host is up (0.039s latency).
rDNS record for 52.205.129.193: ec2-52-205-129-193.compute-1.amazonaws.com
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 5.93 seconds
```

## DeepBlue Port Exploitation

5

General Knowledge

You noticed that Port 22 is open on Secure the Deep Blue's website. Of the following tools, what would you use to try to brute force the SSH information.

- ☐ John the Ripper
- ☐ Hydra
- ☐ HackerApp001011
- ☐ Maltego

You only have 2 attempts to choose the right answer. (This is Part 3 of 4)

Submit

**Answer:** This is part 3 of a 4-part Challenge. This one is just a knowledge question to which the answer is Hydra.

## DeepBlue Admin

10

After finding possible exploits in Secure in the Deep Blues website, you decide to report them to authorities for intellectual theft. However, you want to have a word with the owner of Secure in the Deep Blue and discover their intentions. Find out the administrators email address and pay close attention to their response.

Flag will be in SBTVIP{---} format.

You only have two attempts to submit the right answer. (This is Part 4 of 4)

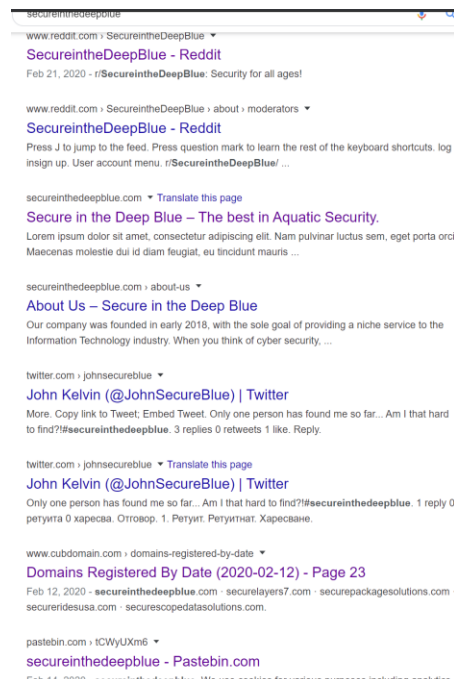
Unlock Hint for 5 points

Flag

Submit

**Answer:** This is part 4 of a 4-part Challenge. This challenge is a bit a challenge. To start let's do a DNS Dig on secureinthedeepblue.com. Do so we can see that the MX server secureinthedeepblue-com.mail.protection.outlook.com

Earlier when we googled secureinthedeepblue we had a few hits.



There is a lot of information in these that are used in another challenge but the one that we are interested in is the twitter link.



Looks like we found someone the works for secureinthedeepblue.com. Going though the feed there is one tweet of interest.



Looks like John is the owner of the site. Now before I go further let me say that I spent about 6 hours using every tool and resource I have to try and find his e-mail address online with no luck.

In the end all we had to do was assume that his e-mail would be john@ secureinthedeepblue.com. Sending him an e-mail would get you the following reply.

**From:** webadmin <john@secureinthedeepblue.com>  
**Date:** February 28, 2020 at 1:41:33 PM EST  
**To:** [REDACTED]  
**Subject:** Automatic reply: Test

Hello fellow hacker! I am currently out of the office due to an external conflict in my programming. Please take this token of appreciation:

SBTVIP{secur3de3pC}

And thus we finally have our flag.

FLAG: SBTVIP{secur3de3pC}