

DeepBlue Challenges

Challenge 214 Solves X

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		
cryptshappiness.com	secretslagos.com	secretsofimberspace
cryptsoftstore.com	secretstashies.com	secretstothelawofat
cryptviptravel.com	secretwhiteboard.com	secretyoubeauty.co
cryptthebenefits.com	sectionaldensity.com	sectionweekwater.c
ctor43.com	sector43.net	sectorlevel.com
ctorys.com	secular-franciscan.com	securakerala.com
cure-aes-financial.com	secure-flo.com	secure-login-server.r
cure-moneyme.com	secure-tweet.com	secure-update.fr
cure219.com	secureatlantanorthdermatology.com	securecmp.com
curecorreos.com	securefilesajc.com	securefutureunlimite
curehostserverweb.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. Commercial support is available at nginx.com.

Thank you for using nginx.

Challenge

145 Solves

X

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 Namp to scan www.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
```

Challenge

136 Solves

X

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.

Challenge

20 Solves

X

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.

The screenshot shows a search results page with several links:

- [www.reddit.com › SecureintheDeepBlue › about › moderators](#)
SecureintheDeepBlue - Reddit
Press J to jump to the feed. Press question mark to learn the rest of the keyboard shortcuts. log in sign up. User account menu. rSecureintheDeepBlue/ ...
- [secureinthedeepblue.com › Translate this page](#)
Secure in the Deep Blue – The best in Aquatic Security.
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nam pulvinar luctus sem, eget porta orci. Maecenas molestie dui id diam feugiat, eu tincidunt mauris ...
- [secureinthedeepblue.com › about-us](#)
About Us – Secure in the Deep Blue
Our company was founded in early 2018, with the sole goal of providing a niche service to the Information Technology industry. When you think of cyber security, ...
- [twitter.com › johnsecureblue](#)
John Kelvin (@JohnSecureBlue) | Twitter
More. Copy link to Tweet. Embed Tweet. Only one person has found me so far... Am I that hard to find?!#secureinthedeepblue. 3 replies 0 retweets 1 like. Reply.
- [twitter.com › johnsecureblue](#)
John Kelvin (@JohnSecureBlue) | Twitter
Only one person has found me so far... Am I that hard to find?!#secureinthedeepblue. 1 reply 0 retweets 0 likes. Reply.
- [www.cubdomain.com › domains-registered-by-date](#)
Domains Registered By Date (2020-02-12) - Page 23
Feb 12, 2020 · secureinthedeepblue.com · securelayers7.com · securepackagesolutions.com · secureridesusa.com · securescopedsatasolutions.com
- [pastebin.com › tCWYUxm6](#)
secureinthedeepblue - Pastebin.com
Feb 14, 2020 · secureinthedeepblue. No use outside for personal purposes, no including applications.

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.

The screenshot shows a Twitter profile for **John Kelvin** (@JohnSecureBlue). The profile picture is a person wearing a black hoodie and a balaclava, holding a laptop. The bio reads: "My Name is John and I work for Secure in the Deep Blue." The account was joined in February 2020, has 9 following, and 15 followers. It is noted that the account is not followed by anyone. The timeline shows two tweets:

- John Kelvin** @JohnSecureBlue · Feb 17
Clock is ticking 🕒
2 replies 0 retweets 0 likes
- John Kelvin** @JohnSecureBlue · Feb 17
Only one person has found me so far... Am I that hard to find?!#secureinthedeepblue

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



John Kelvin @JohnSecureBlue · Feb 14
Hello! My name is John and I have found a leak regarding BTL1. Please go to my website for the full leak. Thank you.

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: SBTVP{secur3de3pC}