

Спешл фо кидс

Лекция в формате шоу



Мартенс Павел

Не совершай публичные выступления без презы



Кто я

Меня зовут Паша и я:

1. Имею опыт работы 2 года в практической ИБ
2. Веду кружок умелые ручки а.к.а. “СТФ в НГТУ”
3. За безопасность во всех её проявлениях



О чем поговорим?

1. Что такое СTF?
2. Какие практические направления в ИБ есть
3. Что бы я хотел знать будучи первокурсником
4. Вопросы

Quiz

1. Кто слышал о CTF?

CTF это дружба

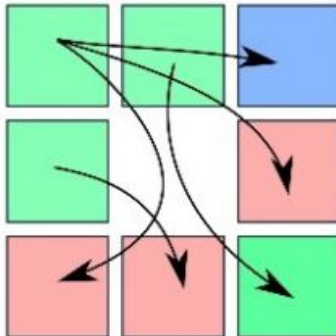
Capture the flag или CTF — это индивидуальная или командная игра, главной целью которой является захват "флага" у соперника. В рамках CTF участникам предлагается решить различные задания, основной целью которых является повышение квалификации и навыков информационной безопасности.



Какие CTF бывают?

Task-based или **jeopardy CTF** — это формат проведения, в рамках которого участниками предлагается решить набор заданий и сдать найденные ответы в жюриную систему.

Classic attack & defense



Task-based Jeopardy

Vulnerab	Binary	Web	Forensics
100	100	100	100
200	200	200	200
300	300	300	300
400	400	400	400
500	500	500	500

Attack-defence CTF - это формат проведения, который предполагает больше действий и экшена по сравнению с task-based. У каждой команды одинаковые сервера, которые надо защищать и атаковать чужие.

Quiz продолжение

1. Кто слышал о STF?
2. Кто участвовал в STF?



n57u_n00bz

Quiz

1. Кто слышал о СТФ?
2. Кто участвовал в СТФ?
3. А зачем он нужен?



Нужно для работы

Будет просто отлично, если вы:

- ◆ Имеете профильные сертификаты – OSCP/OSCE/OSEE/Crest/CISSP
- ◆ Проводили анализ вредоносного кода
- ◆ Принимали участие в **CTF** и BugBounty программах

сфере безопасности информации.

< Преимущество: />

- > Знание основных методов эксплуатации уязвимостей/вредоносного ПО.
- > Знание нормативной базы: ФЗ №149, №152, РД Гостехкомиссии, Профили защиты ФСТЭК России к СОВ и МЭ.
- > Понимание методики и классификации уязвимостей CVE, CVSS.
- > Опыт написания скриптов.
- > Опыт участия в командном **CTF**.

знание особенностей и различных векторов эксплуатации (mitM, MITM, DoS).

Будут плюсом:

- опыт участия в **CTF** и Bug Bounty;
- опыт поиска уязвимостей нулевого дня и написания эксплойтов;
- опыт работы с СУБД;
- английский на уровне чтения технической документации;
- наличие сертификатов в области информационной безопасности (OSCP, eWPTX, OSCE).

профильной литературы.

Будет плюсом, если вы:

- участвовали в **CTF**, bug bounty;
- понимаете процесс реверс-инжиниринга;
- писали технические статьи.

Кем можно работать с образованием ИБ?

Если твой HR ищет опытного пользователя РС.



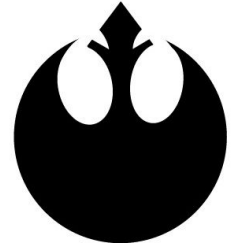
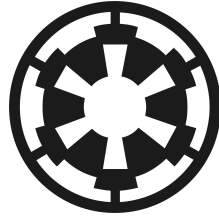
Кем можно работать с образованием ИБ?

1. мастер по бровкам и ноготочкам
2. тренер в спортзале
3. кассир/официант/консультант
4. детские аниматоры
5. продавники (иногда ИБ)
6. сетевой маркетинг
7. тиктокер
8. косметолог
9. амбассадор Vizit

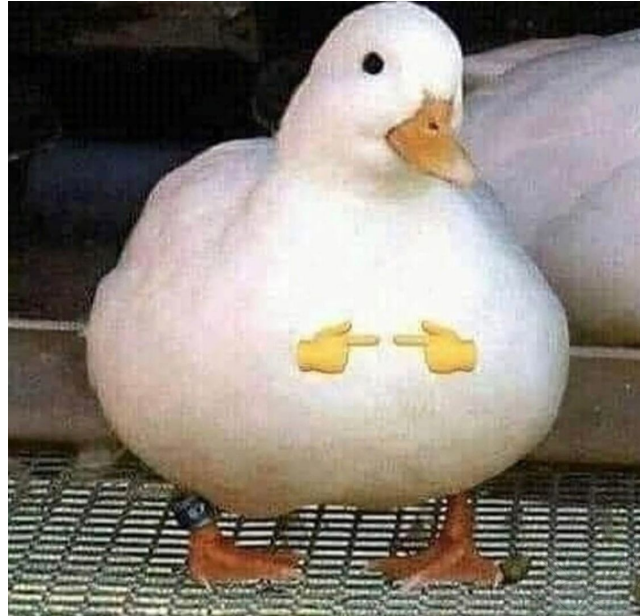


Кем можно работать с образованием ИБ?

1. Pentester
2. AppSec
3. Аналитик
4. SOC
5. Комплаенс
6. Форензика
7. Интегратор
8. Реверсер
9. Хардварщик
10. Силловые структуры

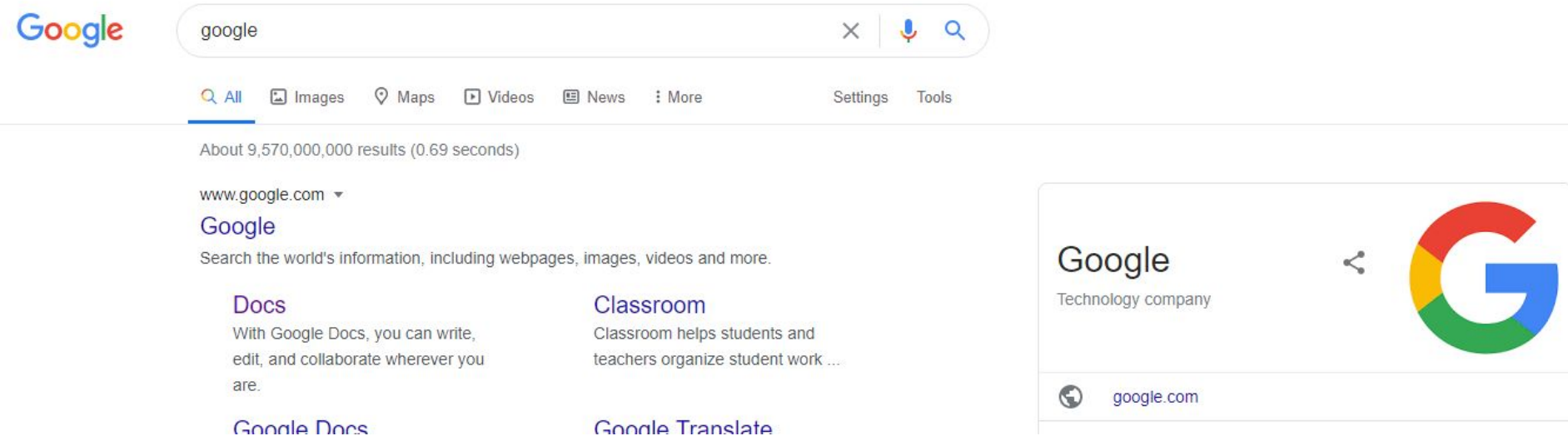


Что бы я хотел знать будучи
первокурсником ИБ?



Что бы я хотел знать будучи первокурсником ИБ?

1. Подружиться с гуглом



The image shows a screenshot of a Google search page. At the top left is the Google logo. The search bar contains the word "google". To the right of the search bar are icons for clearing the search, voice search, and search. Below the search bar are navigation links: "All", "Images", "Maps", "Videos", "News", "More", "Settings", and "Tools". The search results show "About 9,570,000,000 results (0.69 seconds)". The first result is for "www.google.com", with the title "Google" and the description "Search the world's information, including webpages, images, videos and more." Below this are four suggested links: "Docs" (With Google Docs, you can write, edit, and collaborate wherever you are.), "Classroom" (Classroom helps students and teachers organize student work ...), "Google Docs", and "Google Translate". On the right side of the page, there is a large card for "Google" with the text "Technology company" and a large, colorful "G" logo. Below the card is a globe icon and the text "google.com".

Google

google

All Images Maps Videos News More Settings Tools

About 9,570,000,000 results (0.69 seconds)

www.google.com

Google

Search the world's information, including webpages, images, videos and more.

Docs
With Google Docs, you can write, edit, and collaborate wherever you are.

Classroom
Classroom helps students and teachers organize student work ...

Google Docs

Google Translate

Google
Technology company

google.com



Интерактив

Хочу узнать расписание на завтра?

расписание нгту



All

Images

Maps

News

Shopping

More

Tools

About 77,700 results (0.56 seconds)

<https://www.nstu.ru> > [schedule_classes](#) ▾ [Translate this page](#)

Расписание занятий - НГТУ

<https://www.nstu.ru/>

<https://www.nstu.ru> > [schedule](#) ▾ [Translate this page](#)

Расписание - НГТУ

<https://www.nstu.ru/>

Интерактив

Найти книгу/лабу/РГЗ

Интерактив

Найти книгу/лабу/РГЗ

Моя страница

Новости

Мессенджер

Друзья

Сообщества

Фотографии

Музыка

Видео

Клипы

Игры

Объявления

Мини-приложения

VK Pay

Работа

Закладки

Файлы

Файлы

Загрузить файл

Олифер

По запросу **Олифер** не найдено ни одного файла.

Результаты поиска 114



Олифер и 2кари.jpg
404 КБ, 4 августа в 20:49



Олифер В.Г., Олифер Н.А. - Компьютерные сети. Принципы, технологии, ...
91.2 МБ, 21 февраля 2021 в 6:45



Олифер_В_Г_Олифер_Н_А_Комрьютерные_сети_Принципы_технологи...
55.3 МБ, 22 октября 2020 в 22:29



Олиферов. ГИДРОЭНЕРГЕТИЧЕСКАЯ МОЩНОСТЬ РЕК КРЫМА.pdf
253 КБ, 27 мая 2020 в 4:33

Файлы

Загрузить файл

матан нгту

По запросу **матан нгту** не найдено ни одного файла.

Результаты поиска 65



практика матан 1 сем.rar
1.8 МБ, 28 октября 2020 в 17:49
[НГТУ \(НЭТИ\)](#)



матан теория 1 сем.rar
5.6 МБ, 28 октября 2020 в 17:49
[НГТУ \(НЭТИ\)](#)

Что бы я хотел знать будучи
первокурсником ИБ?

1. Подружиться с гуглом

Что бы я хотел знать будучи первокурсником ИБ?

1. Подружиться с гуглом
2. Найдите единомышленников и комьюнити

С чего начать в ИБ

Спросить в чате

Найти метора

Читать книги

какие книги спросить в чате



Что бы я хотел знать будучи первокурсником ИБ?

1. Подружиться с гуглом
2. Найдите единомышленников и комьюнити
3. Участвуйте в любой движухе - ищите “слабые связи”

Слабые связи — это люди, с которыми мы встречаемся или поддерживаем контакт, но не знакомы достаточно близко. (с) Важные годы (Мэг Джей)

Что бы я хотел знать будучи первокурсником ИБ?

1. Подружиться с гуглом
2. Найдите единомышленников и комьюнити
3. Участвуйте в любой движухе - ищите “слабые связи”
4. Незнание закона не освобождает от ответственности

Не пуляй свою паутину куда попало



- 272. Неправомерный доступ к компьютерной информации. Несанкционированный доступ (взлом и получение информации) - до 7 лет
- 273. готовься получить до 7 лет.
- 274. готовься получить до 5 лет
- 274.1. В зависимости от ситуации, сроки растут не по дням, а по годам.



Вопросы?

Tg: @RegularITCat



n57u_n00bz