

Contents

WriteUp_Lab_1 Поиск сотрудника на сайте в открытой сети

1

WriteUp_Lab_1 Поиск сотрудника на сайте в открытой сети

1. Разведка по сайту codovix.ru -> Найдена "интересная" информация по пользователям

История Одного Найма: Взгляд Технического Директора

В компании "Кодовикс" каждый найм — это событие, и технический директор, Аверьян Владиславович Жуков, расскажет вам об одном из интересных моментов в этом процессе.

Не так давно мы приветствовали нового сотрудника, который был поручен настройкой WI-FI сети в нашем офисе. Интересно, что в ходе беседы наш технический гуру смог узнать много интересных вещей о новом коллеге.

Оказалось, что он любит свою собаку по имени "Бобик", увлекается франшизой "Форсаж", лепит вкусные "Пельмени", проводит время за игрой в "Компьютер", придумывает оригинальные "Пароли", занимается настройкой "Сетей", наслаждается "Музыкой", посещает "Кинотеатры", гуляет с "Друзьями" и увлекается "Запутыванием" хакеров.

Аверьян Владиславович в своих размышлениях подчеркнет важность уникальности каждого сотрудника и того, как разнообразные интересы могут сказаться на творческом подходе к работе. Может быть, именно из этих слов был придуман новый пароль от WI-FI.

Дата публикации: 10 июля 2023

Автор: Аверьян Владиславович

2. Составление 2 словарей паролей. На словарик имеется 10 слов, необходимо составить список паролей в которых используется 5 слов в разном порядке

Можно использовать утилиты crunch, combinator.bin, написать свой скрипт, взять чужой [1](#), [2](#) или собрать словарь руками :)

Пример `crunch 1 1 -p Alex Company Position`

```

(kali㉿kali)-[~] dns.org codovix.ru.conf
$ crunch 1 1 -p Alex Company Position
Crunch will now generate approximately the following amount of data: 120 bytes
0 MB 0 PB codovix.duckdns.org
0 GB
0 TB
(kali㉿kali)-[~/Desktop/page/bind-alpine/zone]
0 PB 0 PB codovix.ru.conf
Crunch will now generate the following number of lines: 6
AlexCompanyPosition desktop/page/bind-alpine/zone
AlexPositionCompany .ru 127.0.0.1
CompanyAlexPosition rror to 127.0.0.1#53: connection refused
CompanyPositionAlex rror to 127.0.0.1#53: connection refused
PositionAlexCompany rror to 127.0.0.1#53: connection refused
PositionCompanyAlex be reached

```

3. Отчет должен содержать название уязвимости, cvss вектор, описание уязвимости, пример её эксплуатации, рекомендации к устранению