Прокачай свой профиль! Используем популярный сканер для облака фишинков, доработанный, DoS-атаки и много другого

Andrey Ustinov aka Cryptanalyst, 27 лет, Специалист по ИБ, Москва

Привет. Сегодня хочу рассказать вам пару статей о том, как прокачивать пользовательский профиль. Что касается, как мы знаем, что это доказывает наличие знаний или особенности в определенной области. Сегодня я расскажу вам о том, как прокачивать свой профиль, используя популярный сканер, доработанный, пишем DoS-атаки, а также рассмотрим несколько способов, как можно с помощью VPS прокачивать свой профиль и какие сервисы, какие VPS подходят.

Содержание статьи

1. Базовая эксплуатация
2. Определение наличия и версии сервиса на порте
3. Определение версии и скрытого сервиса
4. Повышение скорости сканирования
5. Скрытое сканирование
6. Обходим IDS и Брандмауэры
7. Выполняем Брут-форс, доработанный (перебор директорий), DoS и другие атаки
8. Используем Metasploit для обнаружения жертв и сбора информации
9. Подготовка VPS для обнаружения жертв и сбора информации
10. Подготовка VPS для обнаружения жертв и сбора информации. Часть 2
11. Сбор информации с помощью Metasploit
12. Сбор информации с помощью Metasploit. Часть 2
13. Итоги

WARNING

Все изложенные материалы в данной статье приведены исключительно в ознакомительных целях. Не допускаю, не несу ни какой ответственности за любой возможный вред, причиненный материалами данной статьи.

Базовая эксплуатация

Сначала мы с вами рассмотрим несколько примеров использования Nmap, уже данных знаний достаточно для использования Nmap на Windows, уже. Я полагаю, что вы знаете, что такое Nmap, для чего он используется, но все же, для тех, кто не знает, я все-таки расскажу. Nmap — это сканер сетевых портов. Он позволяет определять открытые порты на сервере и определять версию сервиса на определенном порту.

```
C:\nmap -sV
C:\nmap -sV -p 21,22,80,443
```

Это действительно так, это может сказать для особенности администратора. Порядок определения версии сервиса на определенном порту. Также, вы можете определять версии сервиса на нескольких портах. Для этого вам необходимо перечислить через запятую. Также, вы можете сканировать диапазон портов. Для этого вам необходимо перечислить через дефис. Также, вы можете сканировать все порты