

## Задание выполнил студент группы 2345 Романенко К.Д.

1. Выбрать подсеть с маской 24 и просканировать ее по tcp по всем портам (65535) с детектированием версий сервисов и ОС. Желательно использовать скрипты NSE. Можно взять четыре любых октета в глобальной сети.

Результаты могут быть и не впечатляющими. Не надо искать самую «интересную» сеть. Задача — попрактиковаться и сдать репорт.

В директории /usr/share/nmap/scripts находятся скрипты для всестороннего сканирования сетевых ресурсов утилитой nmap. Ресурс [vulners.com](https://vulners.com) – сайт со всеми CVE. Разработали скрипт `vulners.nse`, который nmap включили в свой арсенал. Воспользуюсь этим скриптом для сканирования VM Metasploitable3

```
nmap -sV --script vulners.nse 192.168.56.102
```

, где 192.168.56.102 -ip адрес VM

```
3000/tcp closed ppp
3306/tcp open  mysql      MySQL (unauthorized)
8181/tcp open  http       WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28))
_http-server-header: WEBrick/1.3.1 (Ruby/2.3.7/2018-03-28)
vulners:
  cpe:/a:ruby-lang:ruby:2.3.7:
    EDB-ID:43381  9.3  https://vulners.com/exploitdb/EDB-ID:43381  *EXPLOIT*
    SMNTC-105952  7.5  https://vulners.com/symantec/SMNTC-105952
    CVE-2018-8780  7.5  https://vulners.com/cve/CVE-2018-8780
    CVE-2018-16395 7.5  https://vulners.com/cve/CVE-2018-16395
    CVE-2018-16396 6.8  https://vulners.com/cve/CVE-2018-16396
    CVE-2018-8779  5.0  https://vulners.com/cve/CVE-2018-8779
    CVE-2018-8778  5.0  https://vulners.com/cve/CVE-2018-8778
    CVE-2018-8777  5.0  https://vulners.com/cve/CVE-2018-8777
    CVE-2018-6914  5.0  https://vulners.com/cve/CVE-2018-6914
    CVE-2017-17742 5.0  https://vulners.com/cve/CVE-2017-17742
    SMNTC-110992  0.0  https://vulners.com/symantec/SMNTC-110992
    RUBY:RUBY-2018-8780 0.0 https://vulners.com/rubygems/RUBY:RUBY-2018-8780
    RUBY:RUBY-2018-8779 0.0 https://vulners.com/rubygems/RUBY:RUBY-2018-8779
    RUBY:RUBY-2018-8778 0.0 https://vulners.com/rubygems/RUBY:RUBY-2018-8778
    RUBY:RUBY-2018-8777 0.0 https://vulners.com/rubygems/RUBY:RUBY-2018-8777
    RUBY:RUBY-2018-6914 0.0 https://vulners.com/rubygems/RUBY:RUBY-2018-6914
    RUBY:RUBY-2018-16396 0.0 https://vulners.com/rubygems/RUBY:RUBY-2018-16396
```

Скрипт выдал всю информацию по открытым портам, наличию CVE и ссылкам на них

Ссылки урока:

<https://www.first.org/cvss/>

<https://vulners.com/>

<https://bdu.fstec.ru/calc31>

<https://bdu.fstec.ru/site/scanoval>

<https://www.greenbone.net/>

<https://cve.mitre.org>

<https://cwe.mitre.org/>

<https://attack.mitre.org>

<https://mitre.ptsecurity.com/ru-RU/techniques/product/mp-siem>

<https://attack.mitre.org/matrices/enterprise/cloud/>

<https://nmap.org>