Задание выполнил студент группы 2345 Романенко К.Д.

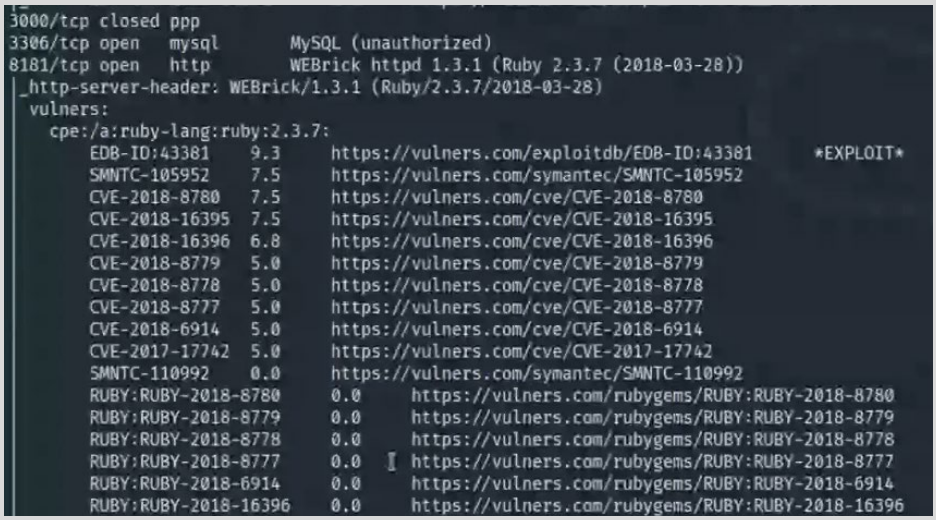
1. Выбрать подсеть с маской 24 и просканировать ее по tcp по всем портам (65535) с детектированием версий сервисов и ОС. Желательно использовать скрипты NSE. Можно взять четыре любых октета в глобальной сети.

   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 – сайт со всеми cve. Разработали скрипт vulners.nse, который nmap включили в свой арсенал. Воспользуюсь этим скриптом для сканирования ВМ Metasploitable3

   nmap -sV --script vulners.nse 192.168.56.102

   , где 192.168.56.102 -ip адрес ВМ



   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