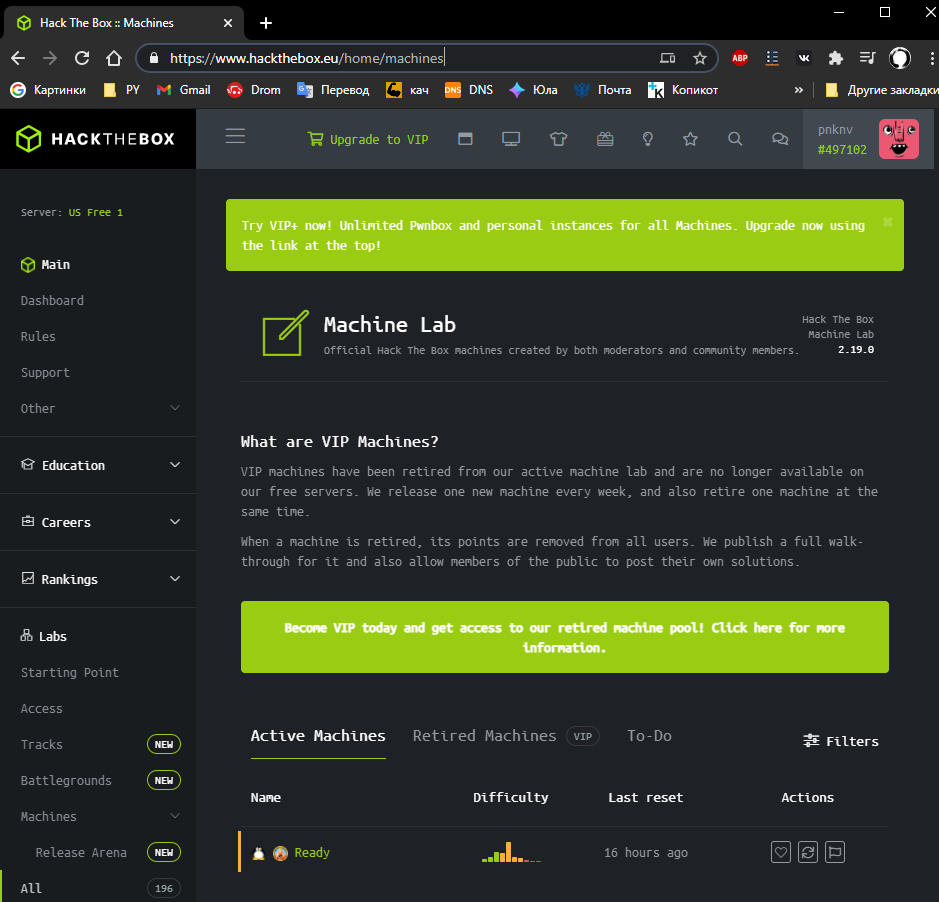
6lab Knyazev

**SCAN**

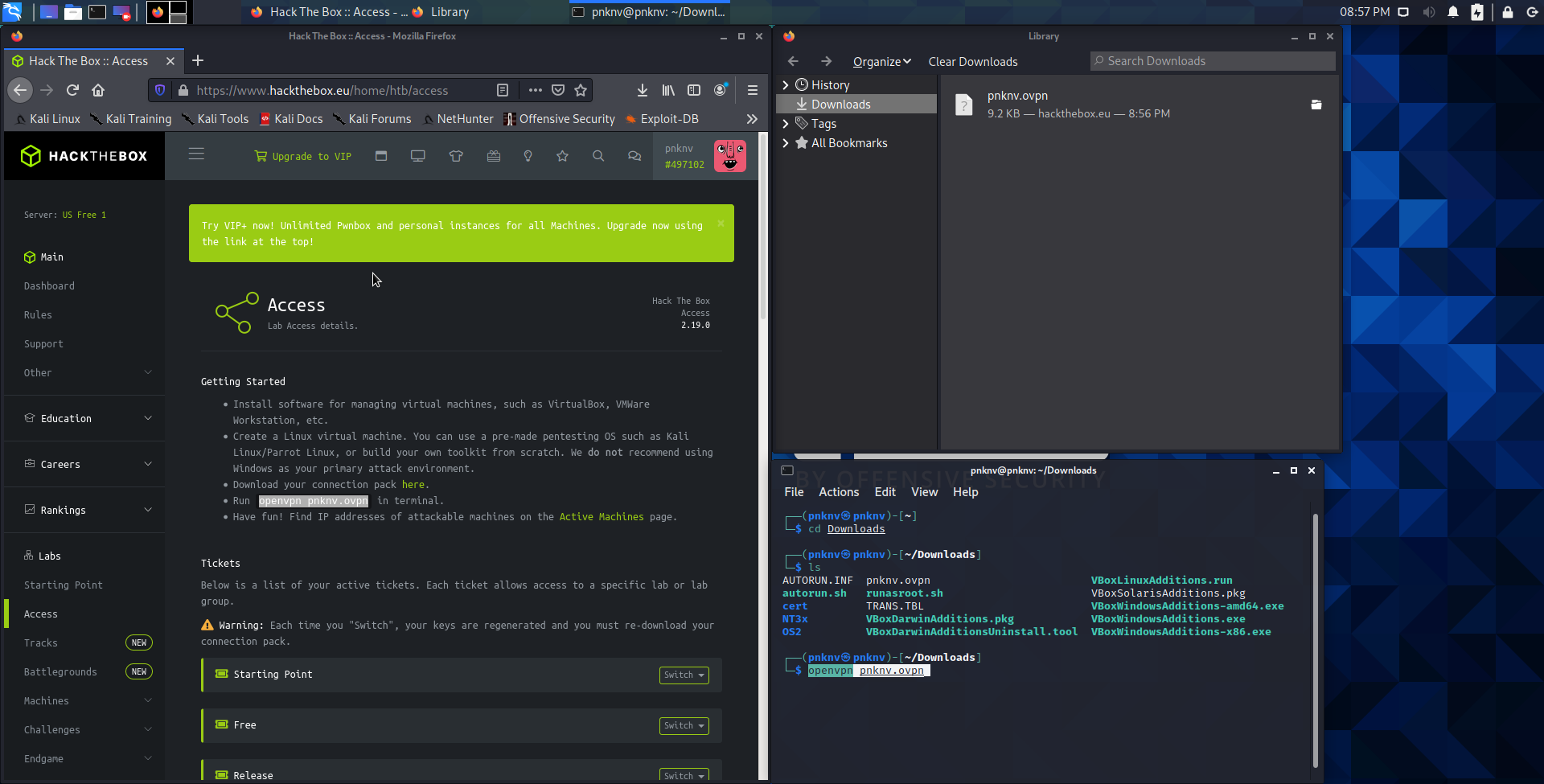


Регистрируемся в хтб - процесс сложный, лично у меня без гайда не получилось…

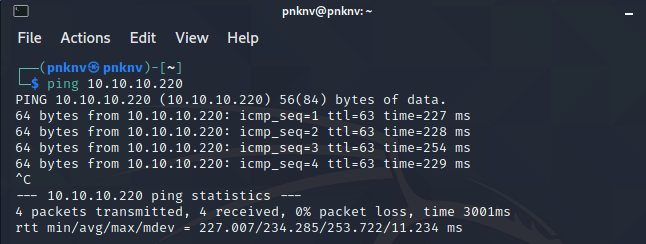
Находим среднюю машинку, доступную всем, я буду использовать Ready – 10.10.10.220

Ресетим ее (скрин 1 - ласт ресет - 16 часов назад)

Далее – чтобы подключиться к машинке, надо организовать защищенное соединение. HTB в этом нам любезно помогает. Надо всего лишь скачать и установить пакеты (скриншот 2)



Проверяем соединение с машиной, пингуем айпишник (скрин 3):



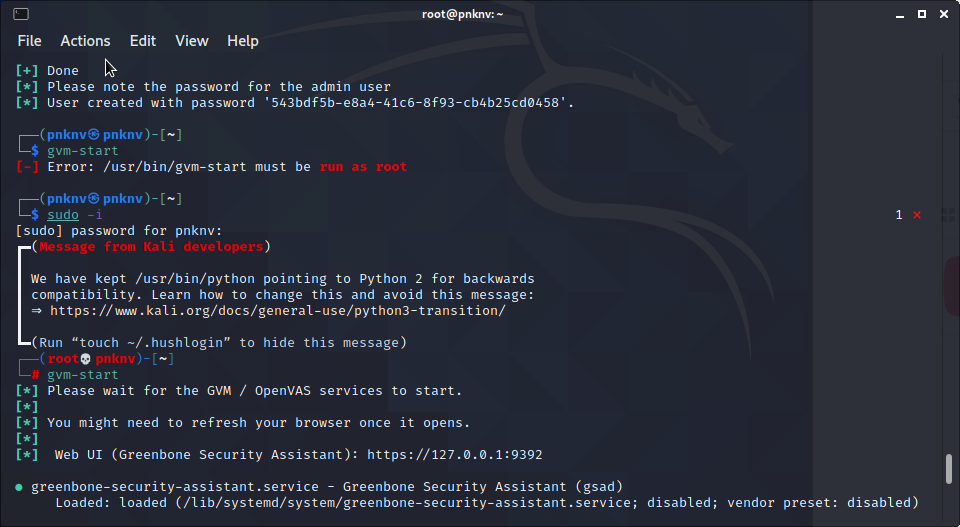
И можно начинать. Для начала попробуем openvas:

apt-get install gvm\*

gvm-setup

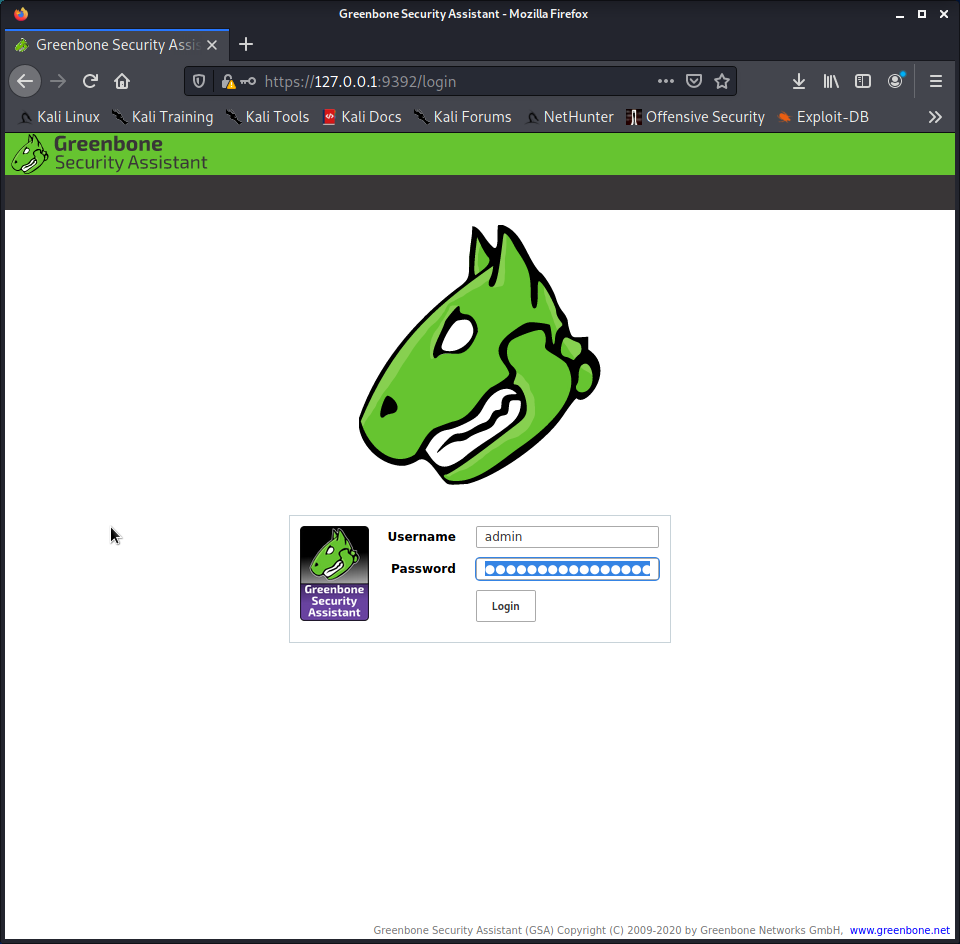
gvm-start

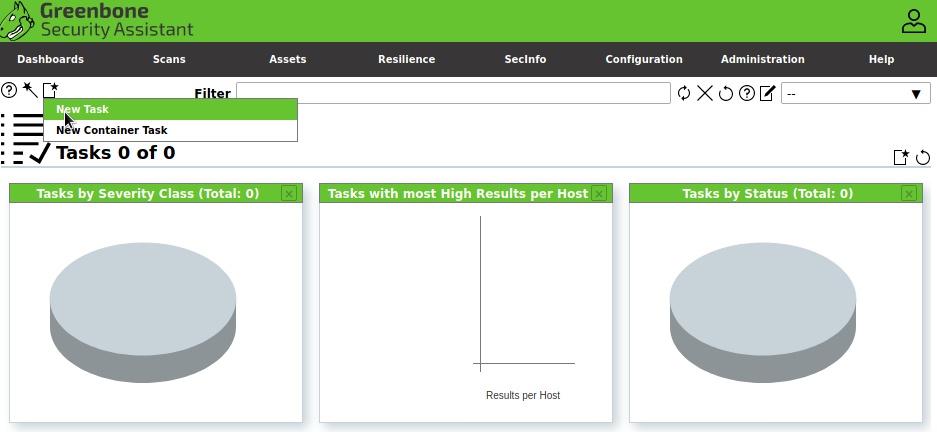
Ставился примерно полтора часа. Потом сгенерировал пароль для админа (скрины 4, 5):



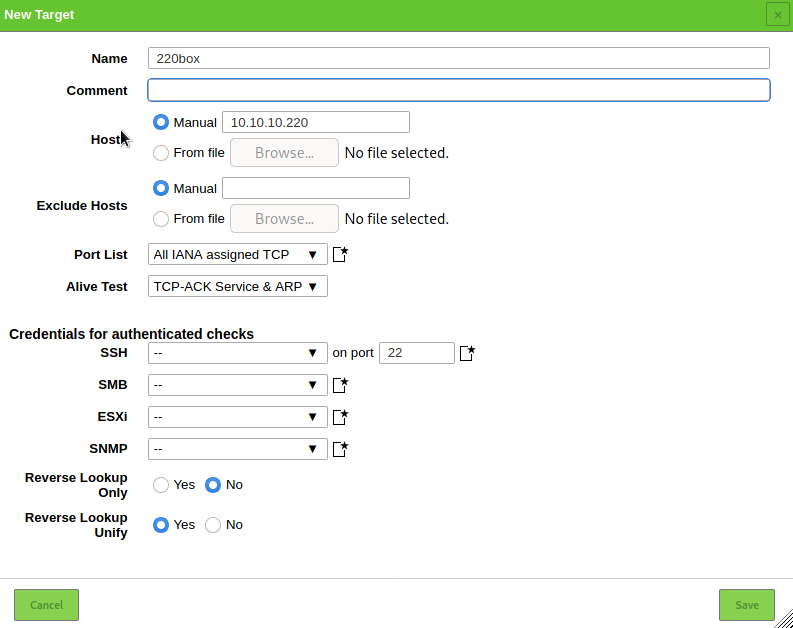
У программы достаточно удобный графический интерфейс.

Он запускается из браузера по 127.0.0.1 и порту. Окно входа и интерфейс программы на скринах 6-7. Можно переходить к настройке.

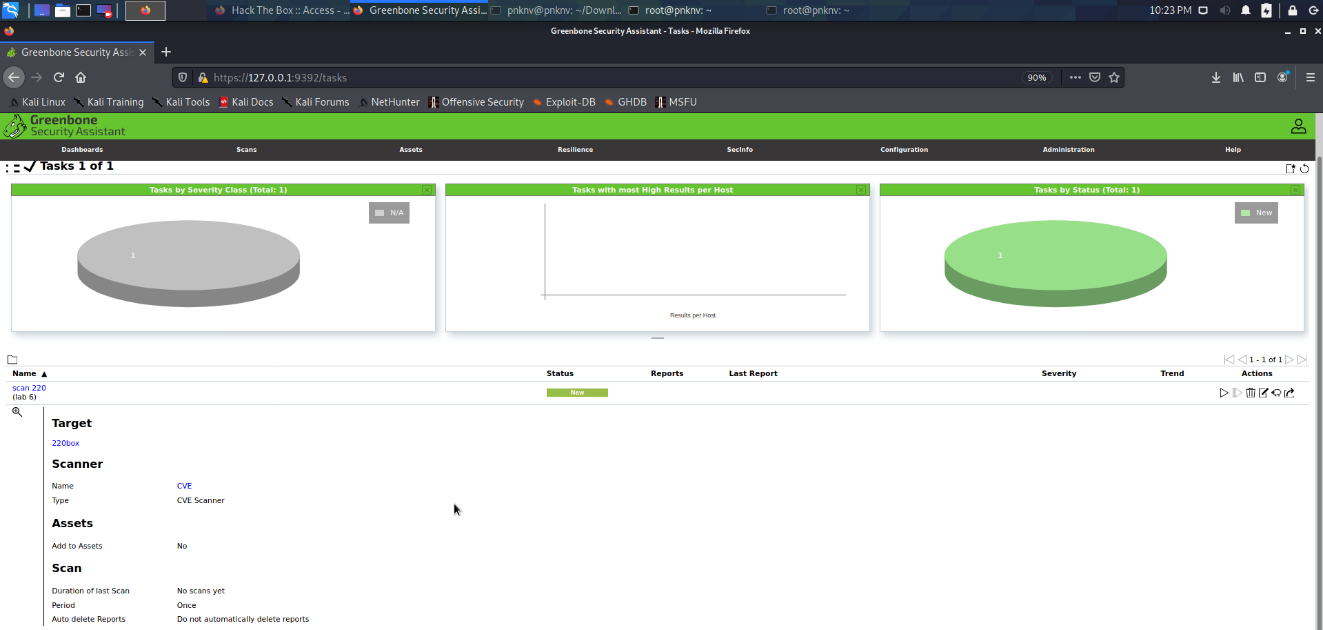




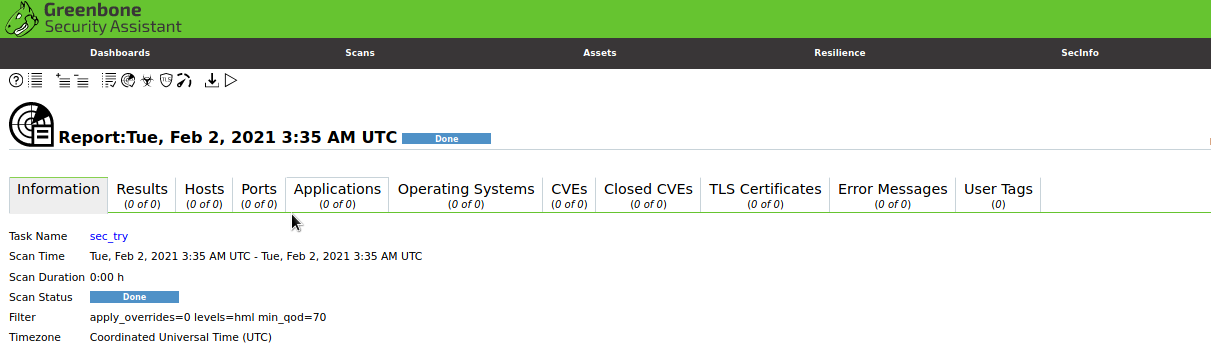
Настройка: выбираем таргеты, выбираем расписание проверок или задаем галочку единожды. Сохраняем результаты, позволяем проге перезаписывать, запрещаем автоудаление отчетов (скриншот 8)



Результат настройки хорошо видно в гуи (скриншот 9):



Графика, кстати, очень удобная. чтобы начать скан жмем на плей (скриншот 10):



Жаль, что не полуилось выбрать openvas деволт сканер. Пришлось использовать cve по отзывам пользователей в интернете, он работает через раз. У меня запустить его не получилось после продолжительных попыток.

Перейдем к нмап

nmap — свободная утилита, предназначенная для разнообразного настраиваемого сканирования IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети. Изначально программа была реализована для систем UNIX, но сейчас доступны версии для множества операционных систем.

Эта утилитка используется всеми и везде (кибербезопасниками в кибербезопасности, естественно)

она предустановлена в кали и имеет множество опций. Список и правда поражает

Можно использовать сетевые имена, IP адреса, сети и т.д.

Пример: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254

-iL <имя\_входного\_файла>: Использовать список хостов/сетей из файла

-iR <количество\_хостов>: Выбрать произвольные цели

--exclude <хост1[,хост2][,хост3],...>: Исключить хосты/сети

--excludefile <имя\_файла>: Исключить из сканирования список хостов/сетей, находящийся в файле

ОБНАРУЖЕНИЕ ХОСТОВ:

-sL: Сканирование с целью составления списка - просто составить список целей для сканирования

-sP: Пинг сканирование - просто определить, работает ли хост

-PN: Расценивать все хосты как работающие - пропустить обнаружение хостов

-PS/PA/PU [список\_портов]: TCP SYN/ACK или UDP пингование заданных хостов

-PE/PP/PM: Пингование с использованием ICMP-эхо запросов, запросов временной метки и сетевой маски

-PO [список\_протоколов]: Пингование с использованием IP протокола

-n/-R: Никогда не производить DNS разрешение/Всегда производить разрешение [по умолчанию: иногда]

--dns-servers <сервер1[,сервер2],...>: Задать собственные DNS сервера для разрешения доменных имён

--system-dns: Использовать системный DNS-преобразователь

РАЗЛИЧНЫЕ ПРИЕМЫ СКАНИРОВАНИЯ:

-sS/sT/sA/sW/sM: TCP SYN/с использованием системного вызова Connect()/ACK/Window/Maimon сканирования

-sU: UDP сканирование

-sN/sF/sX: TCP Null, FIN и Xmas сканирования

--scanflags <флаги>: Задать собственные TCP флаги

-sI <зомби\_хост[:порт]>: "Ленивое" (Idle) сканирование

-sO: Сканирование IP протокола

-b <FTP\_хост>: FTP bounce сканирование

--traceroute: Трассировка пути к хосту

--reason: Выводить причину, почему Nmap установил порт в определенном состоянии

ОПРЕДЕЛЕНИЕ ПОРТОВ И ПОРЯДКА СКАНИРОВАНИЯ:

-p <диапазон\_портов>: Сканирование только определенных портов

Пример: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080

-F: Быстрое сканирование - Сканирование ограниченного количества портов

-r: Сканировать порты последовательно - не использовать случайный порядок портов

--top-ports <количество\_портов>: Сканировать <количество\_портов> наиболее распространенных портов

--port-ratio <рейтинг>: Сканировать порты с рейтингом большим, чем <рейтинг>

ОПРЕДЕЛЕНИЕ СЛУЖБ И ИХ ВЕРСИЙ:

-sV: Исследовать открытые порты для определения информации о службе/версии

--version-intensity <уровень>: Устанавливать от 0 (легкое) до 9 (пробовать все запросы)

--version-light: Ограничиться наиболее легкими запросами (интенсивность 2)

--version-all: Использовать каждый единичный запрос (интенсивность 9)

--version-trace: Выводить подробную информацию о процессе сканирования (для отладки)

СКАНИРОВАНИЕ С ИПОЛЬЗОВАНИЕМ СКРИПТОВ:

-sC: эквивалентно опции --script=default

--script=<Lua скрипты>: <Lua скрипты> - это разделенный запятыми список директорий, файлов скриптов или

категорий скриптов

--script-args=<имя1=значение1,[имя2=значение2,...]>: Передача аргументов скриптам

--script-trace: Выводить все полученные и отправленные данные

--script-updatedb: Обновить базу данных скриптов

ОПРЕДЕЛЕНИЕ ОС:

-O: Активировать функцию определения ОС

--osscan-limit: Использовать функцию определения ОС только для "перспективных" хостов

--osscan-guess: Угадать результаты определения ОС

ОПЦИИ УПРАВЛЕНИЯ ВРЕМЕНЕМ И ПРОИЗВОДИТЕЛЬНОСТЬЮ:

Опции, принимающие аргумент <время>, задаются в миллисекундах, пока вы не добавите 's' (секунды), 'm' (минуты),

или 'h' (часы) к значению (напр. 30m).

-T[0-5]: Установить шаблон настроек управления временем (больше - быстрее)

--min-hostgroup/max-hostgroup <кол\_хостов>: Установить размер групп для параллельного сканирования

--min-parallelism/max-parallelism <количество\_запросов>: Регулирует распараллеливание запросов

--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <время>: Регулирует время ожидания ответа на запрос

--max-retries <количество\_попыток>: Задает максимальное количество повторных передач запроса

--host-timeout <время>: Прекращает сканирование медленных целей

--scan-delay/--max-scan-delay <время>: Регулирует задержку между запросами

--min-rate <число>: Посылать запросы с интенсивностью не меньше чем <число> в секунду

--max-rate <число>: Посылать запросы с интенсивностью не больше чем <число> в секунду

ОБХОД БРАНДМАУЭРОВ/IDS:

-f; --mtu <значение>: Фрагментировать пакеты (опционально с заданным значениме MTU)

-D <фикт\_хост1,фикт\_хост2[,ME],...>: Маскировка сканирования с помощью фиктивных хостов

-S <IP\_адрес>: Изменить исходный адрес

-e <интерфейс>: Использовать конкретный интерфейс

-g/--source-port <номер\_порта>: Использовать заданный номер порта

--data-length <число>: Добавить произвольные данные к посылаемым пакетам

--ip-options <опции>: Посылать пакет с заданным ip опциями

--ttl <значение>: Установить IP поле time-to-live (время жизни)

--spoof-mac <MAC\_адрес/префикс/название производителя>: Задать собственный MAC адрес

--badsum: Посылать пакеты с фиктивными TCP/UDP контрольными суммами

ВЫВОД РЕЗУЛЬТАТОВ:

-oN/-oX/-oS/-oG <файл>: Выводить результаты нормального, XML, s|<rIpt kIddi3,

и Grepable формата вывода, соответственно, в заданный файл

-oA <базовове\_имя\_файла>: Использовать сразу три основных формата вывода

-v: Увеличить уровень вербальности (задать дважды или более для увеличения эффекта)

-d[уровень]: Увеличить или установить уровень отладки (до 9)

--open: Показывать только открытые (или возможно открытые) порты

--packet-trace: Отслеживание принятых и переданных пакетов

--iflist: Вывести список интерфейсов и роутеров (для отладки)

--log-errors: Записывать ошибки/предупреждения в выходной файл нормального режима

--append-output: Добавлять выходные данные в конец, а не перезаписывать выходные файлы

--resume <имя\_файла>: Продолжить прерванное сканирование

--stylesheet <путь/URL>: Устанавливает XSL таблицу стилей для преобразования XML вывода в HTML

--webxml: Загружает таблицу стилей с Nmap.Org

--no-stylesheet: Убрать объявление XSL таблицы стилей из XML

РАЗЛИЧНЫЕ ОПЦИИ:

-6: Включить IPv6 сканирование

-A: Активировать функции определения ОС и версии, сканирование с использованием скриптов и трассировку

--datadir <имя\_директории>: Определяет место расположения файлов Nmap

--send-eth/--send-ip: Использовать сырой уровень Ethernet/IP

--privileged: Подразумевать, что у пользователя есть все привилегии

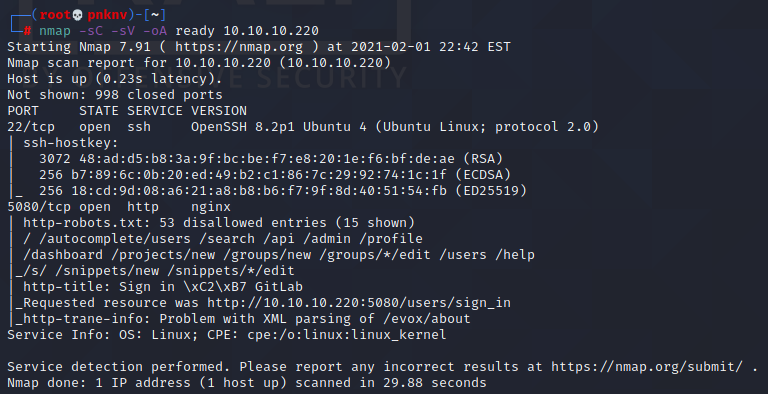
--unprivileged: Подразумевать, что у пользователя нет привилегий для использования сырых сокетов

-V: Вывести номер версии

-h: Вывести эту страницу помощи

попробуем просканировать тачку с хакзебокса (скриншот 11):

nmap -sC -sV -oA ready 10.10.10.220



параметры, которые использовал я:

-sc - сканирование с использованием скриптов

-sv - исследовует открытые порты для определения информации о службе/версии

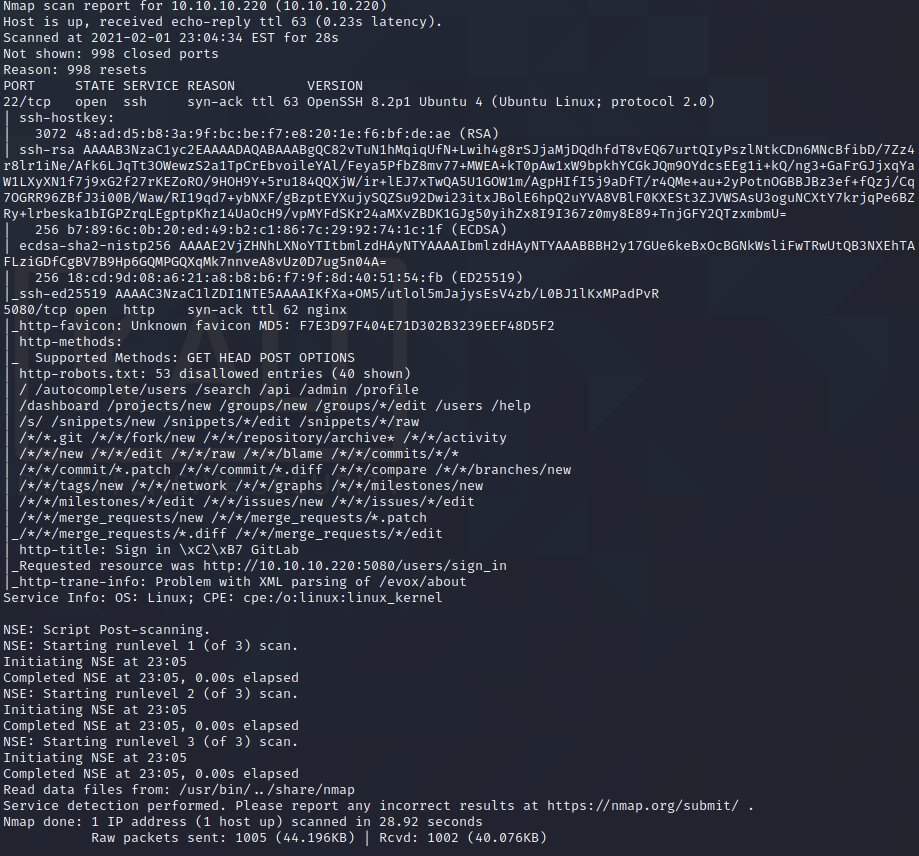
-oa - позволяет использовать сразу все форматы вывода

так же нмапу можно указывать конкретные порты для перебора -p

выбрать случайные порты

логировать результаты в xml и многое, многое другое

Например, на скриншоте 12 реализован лайв вывод результатов сканирования в консоль:

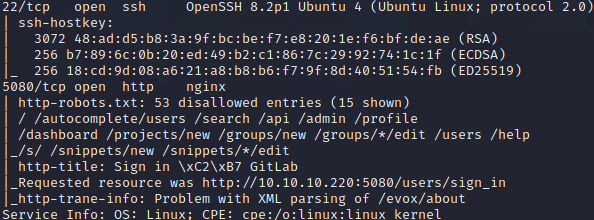


еще один полезный операнд -v (-vv) (increase verbosity level - ) именно с его помощью было получено так много информации

Он повышает уровень детализации, заставляя Nmap печатать больше информации о сканирование в процессе. Открытые порты отображаются по мере их нахождения и завершения оценки времени предоставляются, когда Nmap считает, что сканирование займет больше, чем несколько минут. Используйте его дважды или более для большей детализации: -vv или укажите уровень детализации напрямую.

Для удобства можно задать опцию -oA <базовове\_имя\_файла>, чтобы сохранить результаты сканирования в обычном, XML и grepable форматах сразу. Они будут содержаться в файлах <базовове\_имя\_файла>.nmap, <базовове\_имя\_файла>.xml и <базовове\_имя\_файла>.gnmap соответственно. Как и с большинством программ вы можете предварять имя файла путем к директории, например, ~/nmaplogs/foocorp/ для Unix или c:\hacking\sco для Windows.

Так что же было на машине?



Файл robots.txt или индексный файл — обычный текстовый документ в кодировке UTF-8, действует для протоколов http, https, а также FTP. Файл дает поисковым роботам рекомендации: какие страницы/файлы стоит сканировать. Если файл будет содержать символы не в UTF-8, а в другой кодировке, поисковые роботы могут неправильно их обработать. Правила, перечисленные в файле robots.txt, действительны только в отношении того хоста, протокола и номера порта, где размещен файл

Клиент scp в OpenSSH 8.2 неправильно отправляет дублирующиеся ответы на сервер при сбое системного вызова utimes, что позволяет злонамеренному непривилегированному пользователю на удаленном сервере перезаписывать произвольные файлы в каталоге загрузки клиента, создавая созданный подкаталог в любом месте удаленного сервера. Жертва должна использовать команду scp -rp для загрузки иерархии файлов, содержащей в любом месте этот созданный подкаталог. ПРИМЕЧАНИЕ: поставщик указывает, что «эта атака может достичь не большего, чем враждебный одноранговый узел уже может достичь в рамках протокола scp» и «utimes не дает сбоев при нормальных обстоятельствах».

Так же я попробовал поставить zenmap, он находится под нмапомв репозитории, но сломал тачку, скриншот 14. Починить не удалось…

