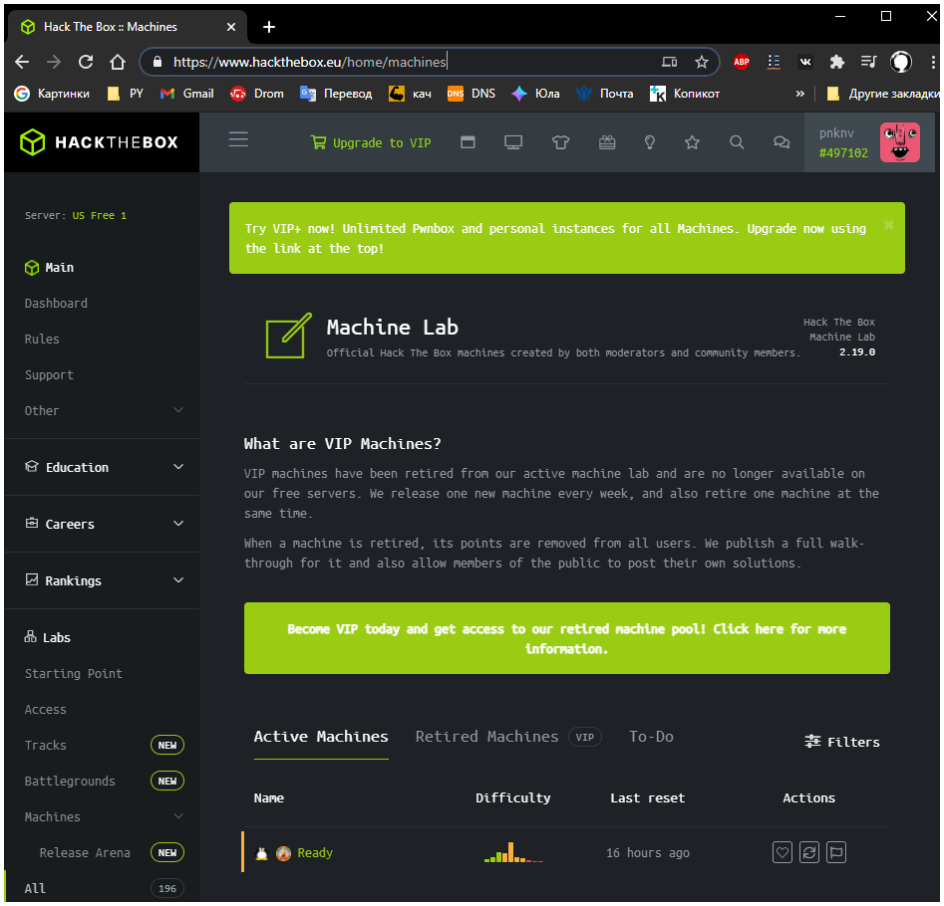
6lab Knyazev

SCAN

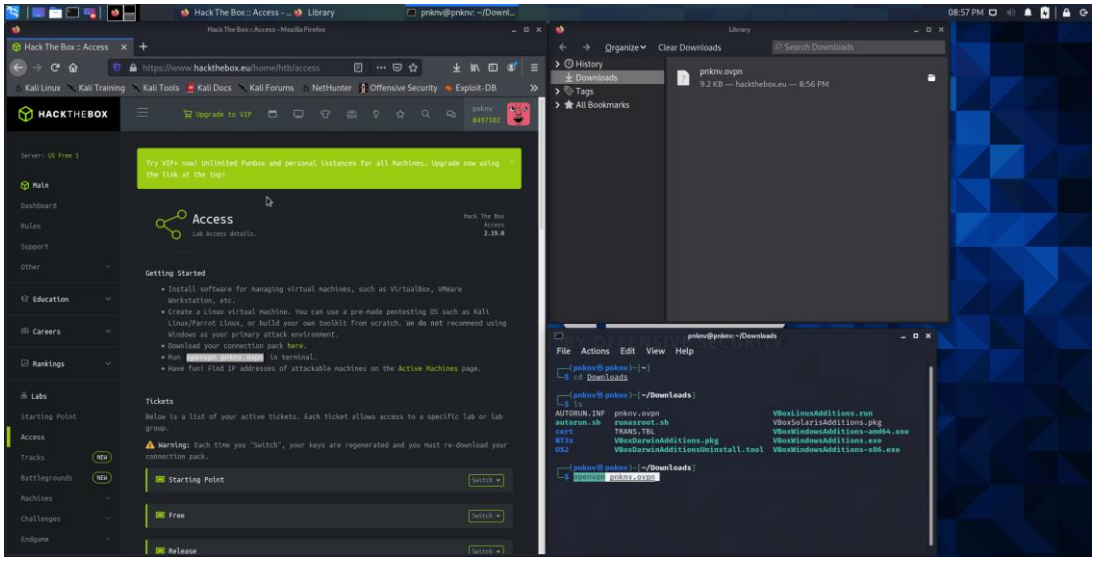


Регистрируемся в хтб - процесс сложный, лично у меня без гайда не получилось…

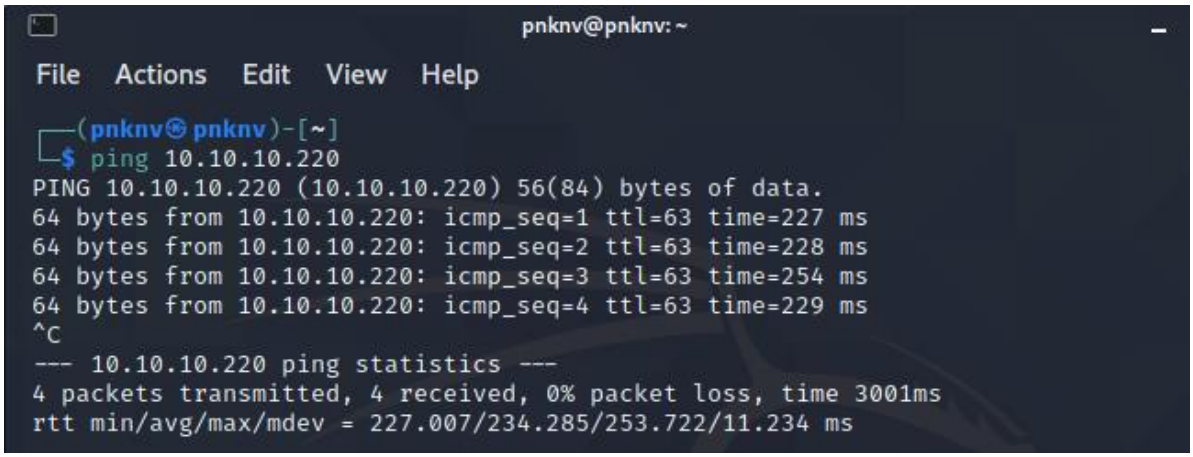
Находим среднюю машинку, доступную всем, я буду использовать Ready – 10.10.10.220

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):



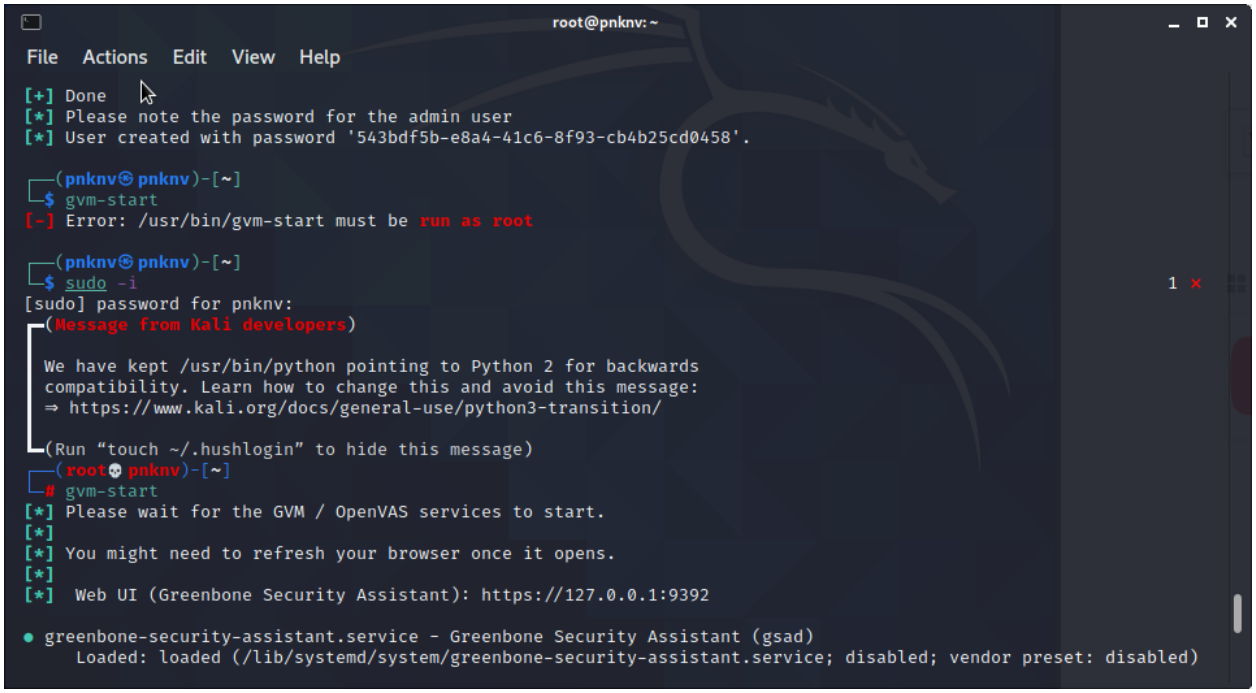
И можно начинать. Для начала попробуем openvas:

apt-get install gvm*

gvm-setup

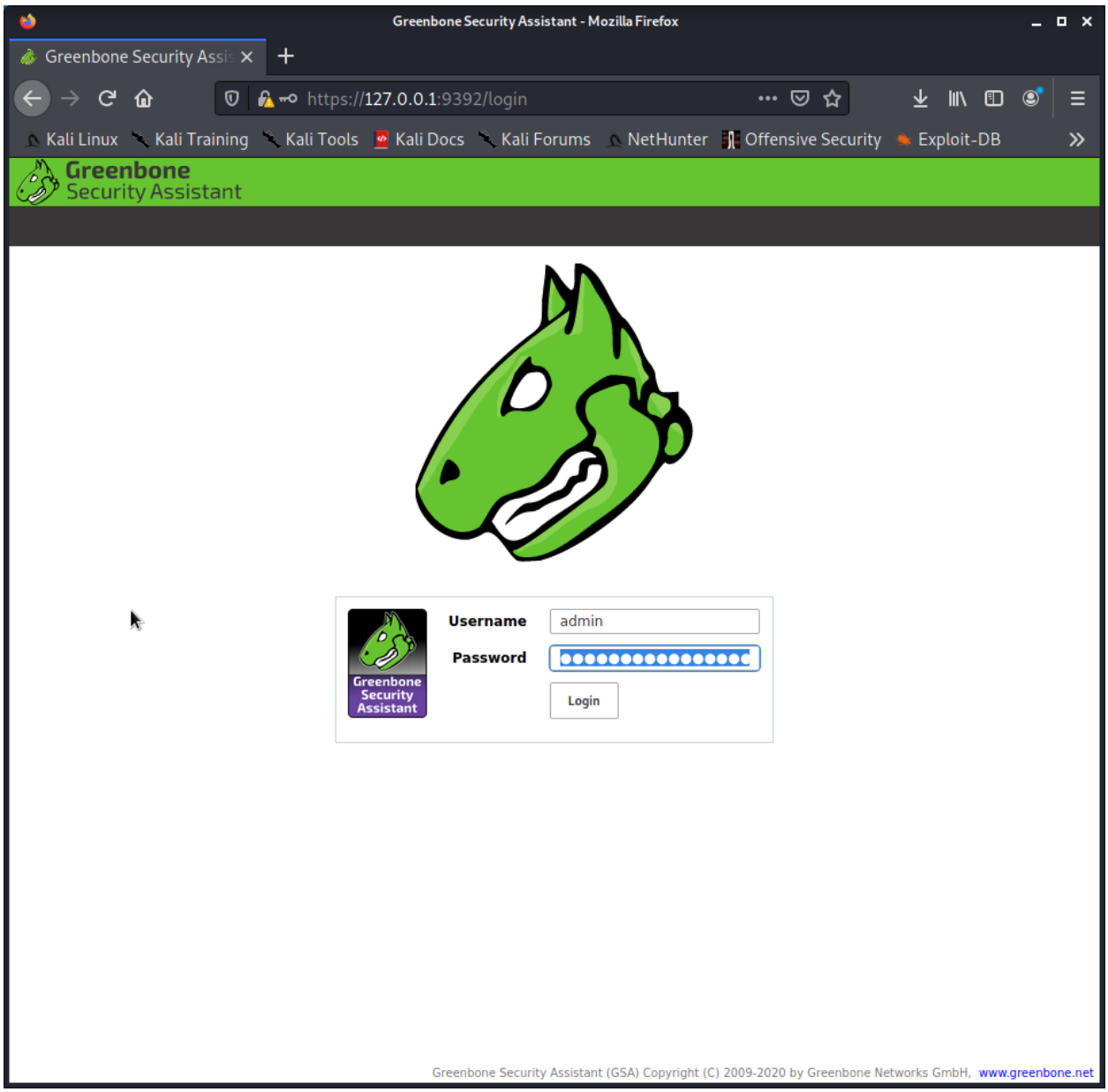
gvm-start

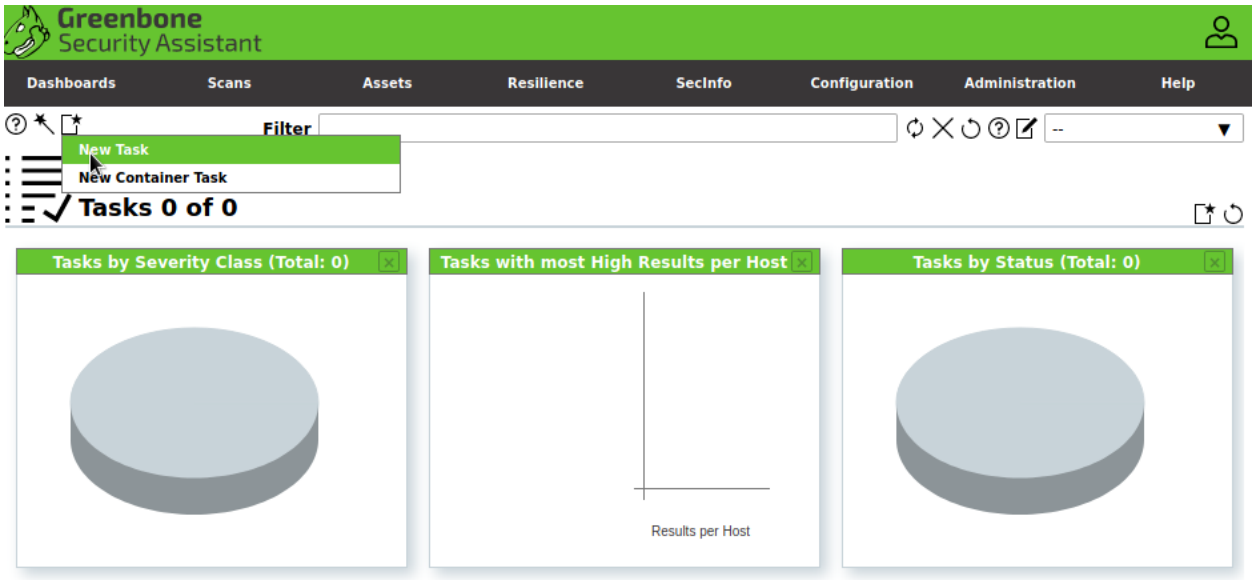
Ставился примерно полтора часа. Потом сгенерировал пароль для админа (скрины 4, 5):



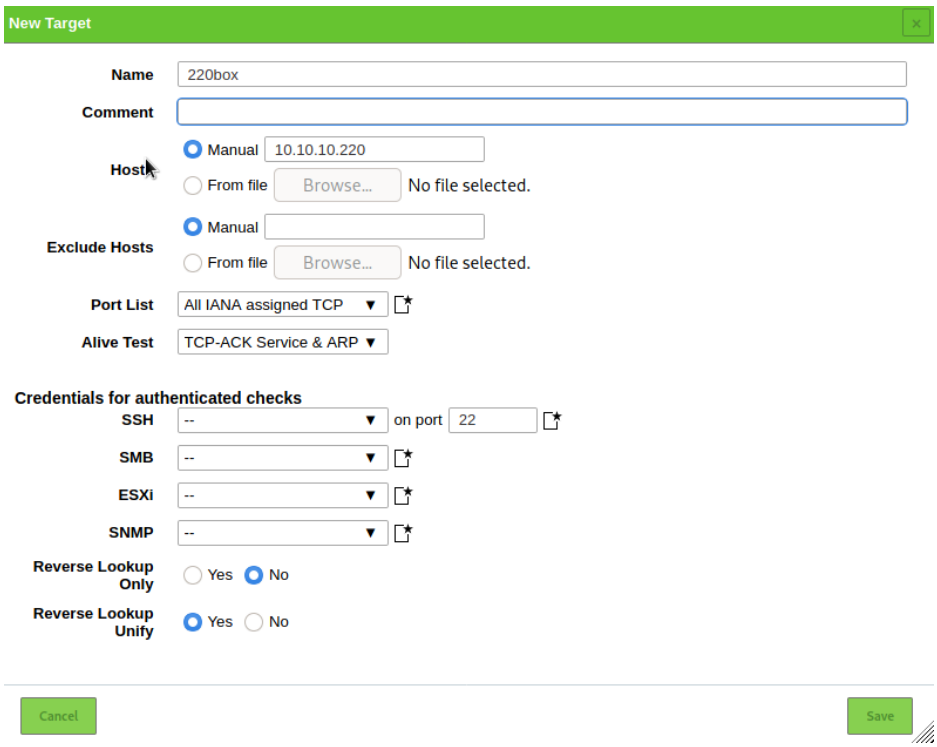
У программы достаточно удобный графический интерфейс.

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

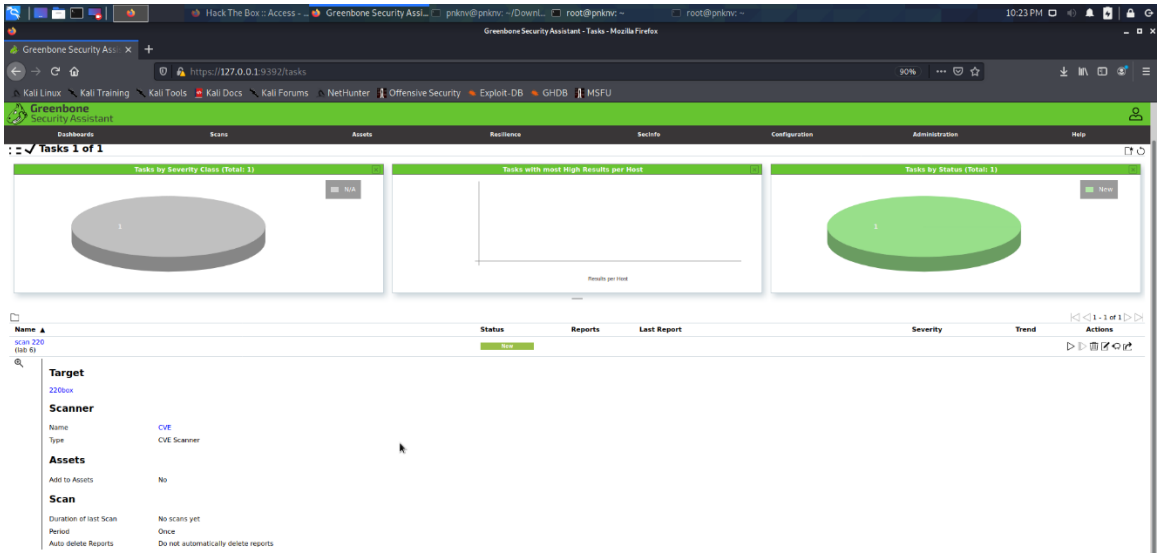

Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assis
https://127.0.0.1:9392/login
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
Greenbone
Security Assistant
Username
admin
Password
Login
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net


Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
New Task
New Container Task
Tasks 0 of 0
Tasks by Severity Class (Total: 0)
Tasks with most High Results per Host
Results per Host
Tasks by Status (Total: 0)

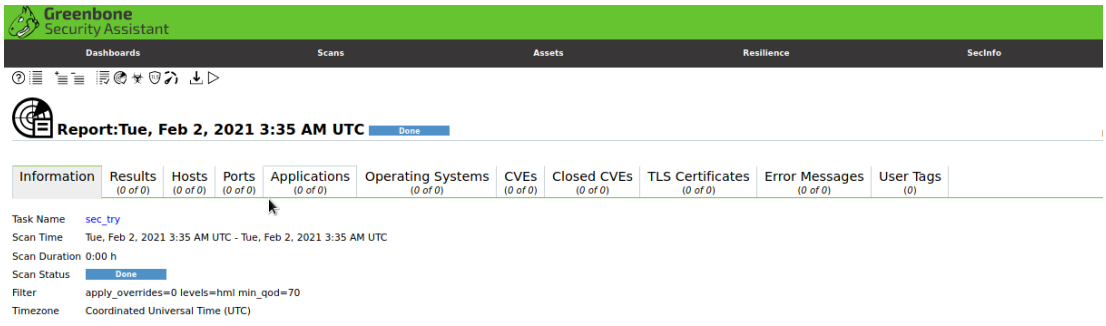
Настройка: выбираем таргеты, выбираем расписание проверок или задаем галочку единожды. Сохраняем результаты, позволяем проге перезаписывать, запрещаем автоудаление отчетов (скриншот 8)



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

```
┌──(root💀pknkv)-[~]
└─# nmap -sC -sV -oA ready 10.10.10.220
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-01 22:42 EST
Nmap scan report for 10.10.10.220 (10.10.10.220)
Host is up (0.23s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
5080/tcp open  http    nginx
| http-robots.txt: 53 disallowed entries (15 shown)
| / /autocomplete/users /search /api /admin /profile
| /dashboard /projects/new /groups/new /groups/*/edit /users /help
|_/s/ /snippets/new /snippets/*/edit
| http-title: Sign in \xC2\xB7 GitLab
|_Requested resource was http://10.10.10.220:5080/users/sign_in
|_http-trane-info: Problem with XML parsing of /evox/about
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.88 seconds
```

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:

```
Nmap scan report for 10.10.10.220 (10.10.10.220)
Host is up, received echo-reply ttl 63 (0.23s latency).
Scanned at 2021-02-01 23:04:34 EST for 28s
Not shown: 998 closed ports
Reason: 998 resets
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC82vTuN1hMqiqUfN+Lwih4g8rSJjaMjDQdhfdT8vEQ67urtQIyPszlNtkCDn6MNcBfibD/7Zz4
r8lr1iNe/Afk6LJqTt3OWewzS2a1TpCrEbvoileYAl/Feya5PfbZ8mv77+MWEA+kT0pAw1xW9bpkhYCGkJQm9OYdcsEEg1i+kQ/ng3+GaFrGJjxqYa
W1LXyXN1f7j9xG2f27rKEZoRO/9HOH9Y+5ru184QQXjW/ir+lEJ7xTwQA5U1GOW1m/AgpHIfI5j9aDfT/r4QMe+au+2yPotnOGBBJBz3ef+fQzj/Cq
7OGRR96ZBfJ3i00B/Waw/RI19qd7+ybNXF/gBzptEYXujySQZSu92Dwi23itxJBolE6hpQ2uYVA8VBlF0KXESt3ZJVWSAsU3oguNCXtY7krjqPe6BZ
Ry+lrbeska1bIGPZrqLEgptpKhz14UaOcH9/vpMYFdSKr24aMXvZBDK1GJg50yihZx8I9I367z0my8E89+TnjGFY2QTzxmbmU=
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH2y17GUe6keBxOcBGNkWsliFwTRwUtQB3NXEhTA
FLziGDfCgBV7B9Hp6GQMPGQXqMk7nnveA8vUz0D7ug5n04A=
|   256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKfXa+OM5/utlol5mJajysEsV4zb/L0BJ1lKxMPadPvR
5080/tcp open  http    syn-ack ttl 62 nginx
|_http-favicon: Unknown favicon MD5: F7E3D97F404E71D302B3239EEF48D5F2
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 53 disallowed entries (40 shown)
| / /autocomplete/users /search /api /admin /profile
| /dashboard /projects/new /groups/new /groups/*/edit /users /help
| /s/ /snippets/new /snippets/*/edit /snippets/*/raw
| /*/*.git /*/*/fork/new /*/*/repository/archive* /*/*/activity
| /*/*/new /*/*/edit /*/*/raw /*/*/blame /*/*/commits/*/*
| /*/*/commit/*.patch /*/*/commit/*.diff /*/*/compare /*/*/branches/new
| /*/*/tags/new /*/*/network /*/*/graphs /*/*/milestones/new
| /*/*/milestones/*/edit /*/*/issues/new /*/*/issues/*/edit
| /*/*/merge_requests/new /*/*/merge_requests/*.patch
|_/*/*/merge_requests/*.diff /*/*/merge_requests/*/edit
| http-title: Sign in \xC2\xB7 GitLab
|_Requested resource was http://10.10.10.220:5080/users/sign_in
|_http-trane-info: Problem with XML parsing of /evox/about
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:05
Completed NSE at 23:05, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:05
Completed NSE at 23:05, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:05
Completed NSE at 23:05, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.92 seconds
           Raw packets sent: 1005 (44.196KB) | Rcvd: 1002 (40.076KB)
```

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.

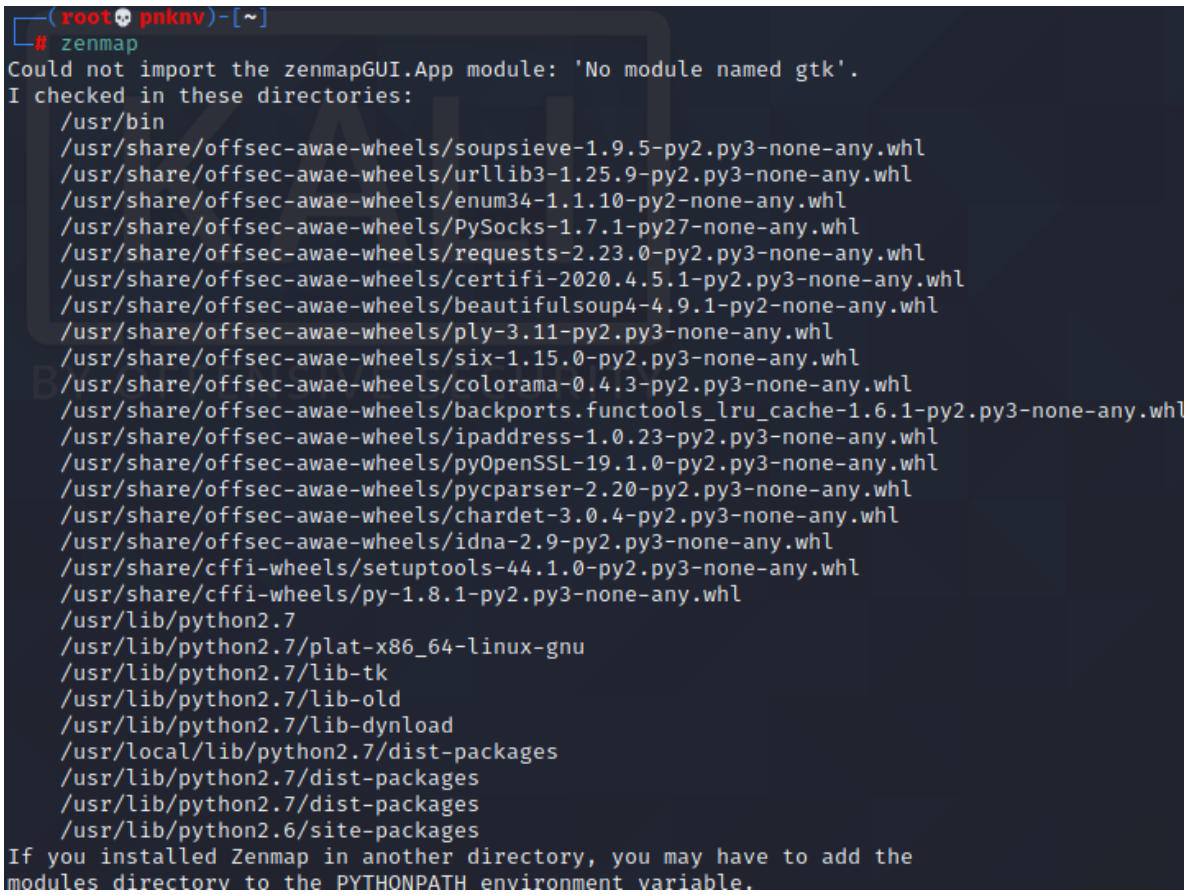
Так что же было на машине?

```
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
5080/tcp open  http    nginx
| http-robots.txt: 53 disallowed entries (15 shown)
| / /autocomplete/users /search /api /admin /profile
| /dashboard /projects/new /groups/new /groups/*/edit /users /help
|_/s/ /snippets/new /snippets/*/edit
| http-title: Sign in \xC2\xB7 GitLab
|_Requested resource was http://10.10.10.220:5080/users/sign_in
|_http-trane-info: Problem with XML parsing of /evox/about
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

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…


┌──(root💀 pnknv)-[~]
└─# zenmap
Could not import the zenmapGUI.App module: 'No module named gtk'.
I checked in these directories:
/usr/bin
/usr/share/offsec-awae-wheels/soupsieve-1.9.5-py2.py3-none-any.whl
/usr/share/offsec-awae-wheels/urllib3-1.25.9-py2.py3-none-any.whl
/usr/share/offsec-awae-wheels/enum34-1.1.10-py2-none-any.whl
/usr/share/offsec-awae-wheels/PySocks-1.7.1-py27-none-any.whl
/usr/share/offsec-awae-wheels/requests-2.23.0-py2.py3-none-any.whl
/usr/share/offsec-awae-wheels/certifi-2020.4.5.1-py2.py3-none-any.whl
/usr/share/offsec-awae-wheels/beautifulsoup4-4.9.1-py2-none-any.whl
/usr/share/offsec-awae-wheels/ply-3.11-py2.py3-none-any.whl
/usr/share/offsec-awae-wheels/six-1.15.0-py2.py3-none-any.whl
/usr/share/offsec-awae-wheels/colorama-0.4.3-py2.py3-none-any.whl
/usr/share/offsec-awae-wheels/backports.functools_lru_cache-1.6.1-py2.py3-none-any.whl
/usr/share/offsec-awae-wheels/ipaddress-1.0.23-py2.py3-none-any.whl
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl
/usr/share/offsec-awae-wheels/pycparser-2.20-py2.py3-none-any.whl
/usr/share/offsec-awae-wheels/chardet-3.0.4-py2.py3-none-any.whl
/usr/share/offsec-awae-wheels/idna-2.9-py2.py3-none-any.whl
/usr/share/cffi-wheels/setuptools-44.1.0-py2.py3-none-any.whl
/usr/share/cffi-wheels/py-1.8.1-py2.py3-none-any.whl
/usr/lib/python2.7
/usr/lib/python2.7/plat-x86_64-linux-gnu
/usr/lib/python2.7/lib-tk
/usr/lib/python2.7/lib-old
/usr/lib/python2.7/lib-dynload
/usr/local/lib/python2.7/dist-packages
/usr/lib/python2.7/dist-packages
/usr/lib/python2.7/dist-packages
/usr/lib/python2.6/site-packages
If you installed Zenmap in another directory, you may have to add the
modules directory to the PYTHONPATH environment variable.