

Описание SPARTA

SPARTA – это приложение с графическим интерфейсом (GUI) написанное на Python, которое упрощает тестирование на проникновение сетевой инфраструктуры, содействуя тестеру на проникновение на фазе сканирования и перебора. Она позволяет сэкономить время тестеру благодаря простому графическому интерфейсу и выводу полученной информации в удобочитаемом виде. Чем меньше времени тратится на ввод команд и настройку инструментов, тем больше времени может быть потрачено для фокусировки на анализе результатов.

Функции SPARTA:

- Запуск nmap из SPARTA или импорт вывода nmap XML.
- Незаметная работа nmap: быстрое получение результатов и архивирование в течение всего процесса.
- Настраиваемое контекстное меню для каждой службы. Вы можете настроить что запустить на обнаруженной службе. Любой инструмент может быть запущен в терминале, может быть запущен из SPARTA.
- Вы можете запустить любой скрипт или инструмент по отношению к службе в списке всех хостов кликом мыши.
- Определение автоматизированных задач для служб (например, запуск nikto в отношении каждой HTTP службы или sslscan для каждой ssl службы).
- Проверка дефолтных учётных данных для большинства популярных служб. Конечно, это также можно настроить для автоматического запуска.
- Повторное использование найденного пароля в тестируемой инфраструктуре. Если в Hydra были найдены имена пользователей/пароли, то они сохраняются во внутренних списках слов, которые затем будут использованы на целях в той же сети (срочные новости: сисадмины используют одни и те же пароли).
- Возможность помечать хосты, над которыми вы уже работали, чтобы вы не тратили впустую ваше время на их анализ.
- Скриншоты веб-сайтов, это позволит вам не тратить впустую время на не интересных веб-серверах.

Запуск

Sparta можно запустить через меню, в разделе Vulnerability Analysis

Или через консоль

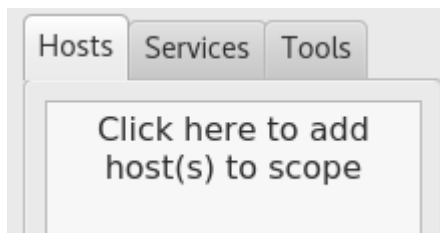
```
# sparta
```

Пример работы

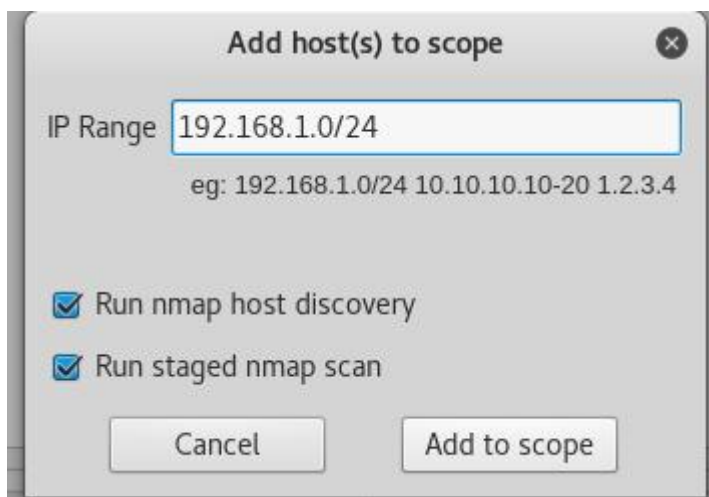
После запуска мы видим следующий интерфейс



И первое, что нам нужно сделать, обозначить наши цели.
Кликаем в этой области:



И задаем, к примеру, такую подсеть:



Сразу можно указать sparta провести обнаружение хостов при помощи Nmap. Вторая опция «Run staged nmap scan» запускает nmap особым образом, разделяя сканирование на этапы (stages). Они представлены в файле конфигурации Sparta.conf.
[StagedNmapSettings]

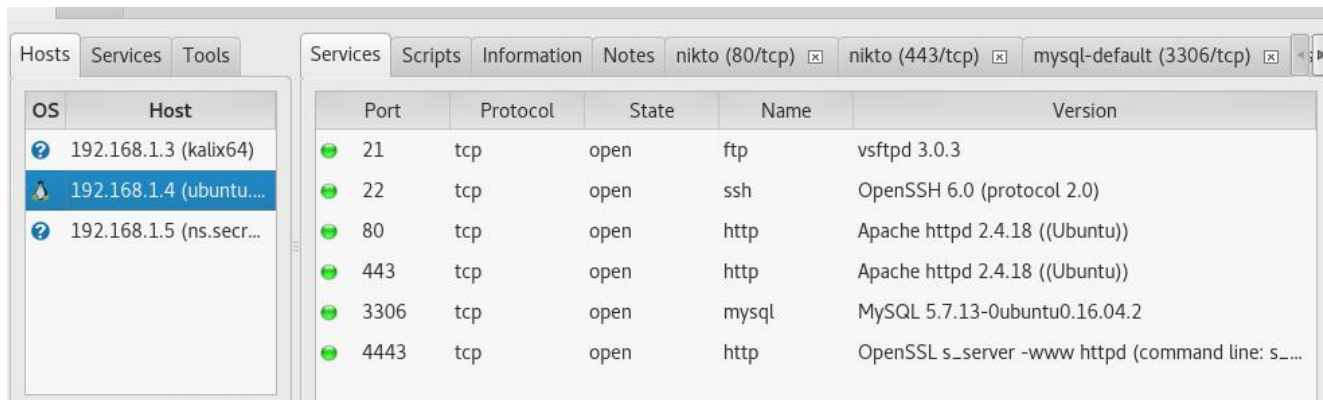
```
stage1-ports="T:80,443"
stage2-ports="T:25,135,137,139,445,1433,3306,5432,U:137,161,162,1434"
stage3-ports="T:23,21,22,110,111,2049,3389,8080,U:500,5060"
stage4-ports="T:0-20,24,26-79,81-109,112-134,136,138,140-442,444,446-1432,1434-2048,2050-3305,3307-3388,3390-5431,5433-8079,8081-29999"
stage5-ports=T:30000-65535
```

Этот режим позволяет быстрее получать информацию о найденных сервисах и оптимизирует работу по автоматическому запуску задач. После нажатия кнопки «Add to scope» в нижней части экрана можно увидеть информацию о работающих задачах. Видим, что множество инструментов работают параллельно.

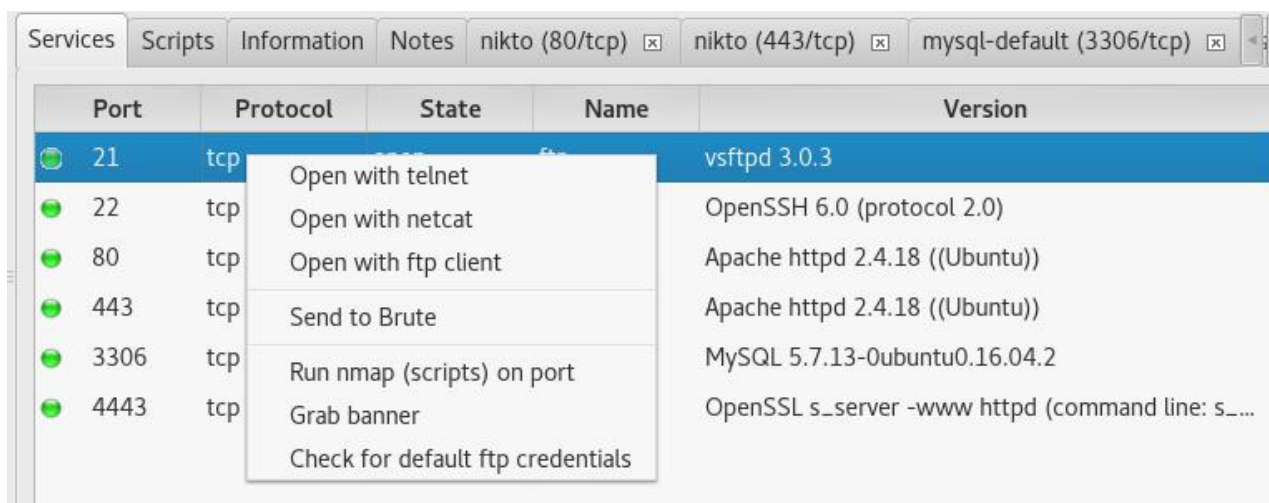
Log					
Progress	Tool	Host	Start time	End time	Status
	nikto (4443/tcp)	192.168.1.4	28 Feb 2017 09:30:56		Running
	nmap (stage 5)	192.168.1.0/24	28 Feb 2017 09:30:55		Running
	ftp-default (21/tcp)	192.168.1.4	28 Feb 2017 09:30:10	28 Feb 2017 09:30:21	Finished

Правым кликом можно завершить любое из заданий. Так же, вы можете заметить, что таблица с хостами заполняется, и при

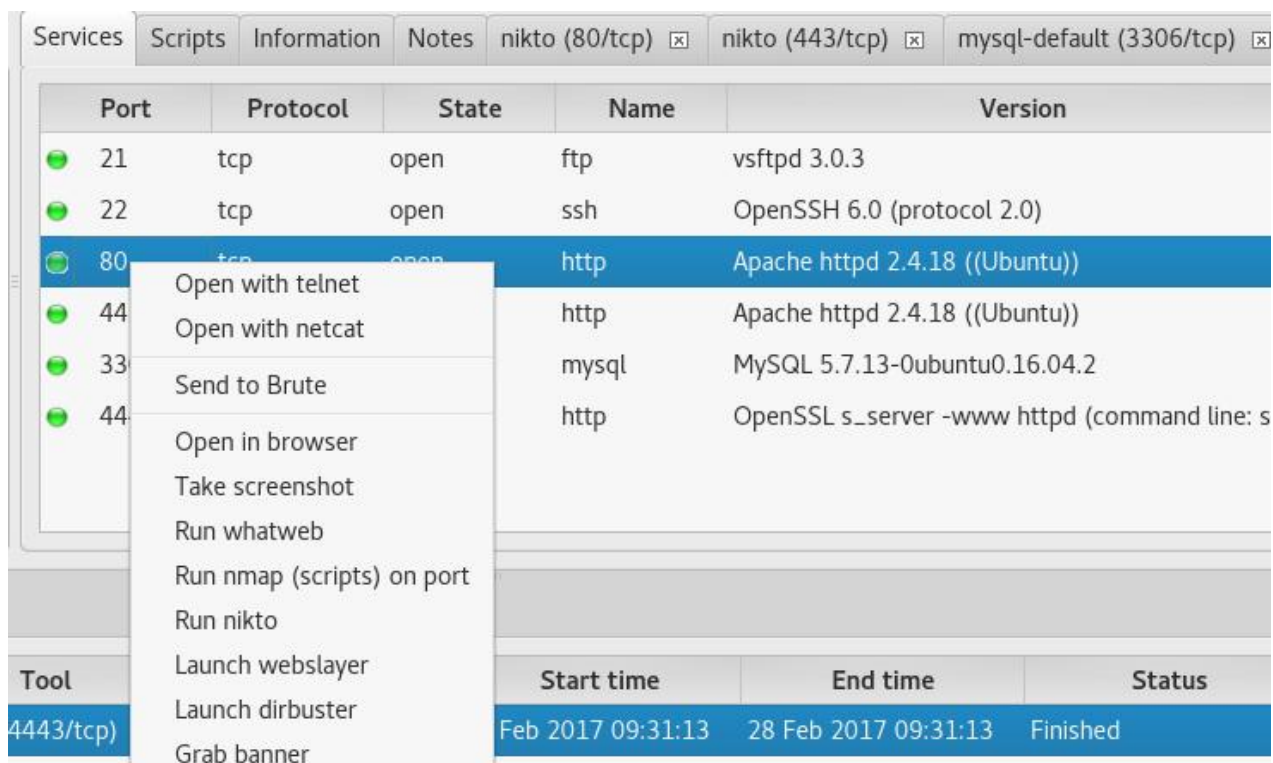
выборе одного из хостов, в правой части интерфейса доступны вкладки с результатом работы скриптов.



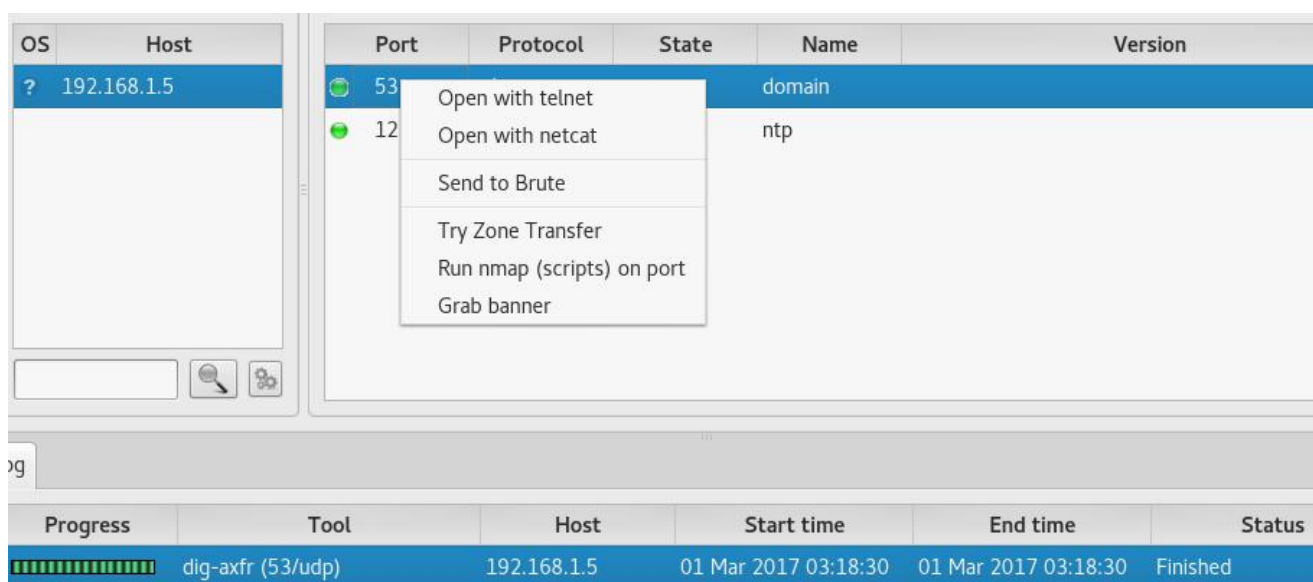
Кликнув правой кнопкой на обнаруженном открытом порте, мы можем выполнить всевозможные задачи, например, подключиться к сервису при помощи telnet или nc, провести брутфорс и т.д. Стоит заметить, что вид меню зависит от сервиса. Ниже скриншот для FTP сервиса



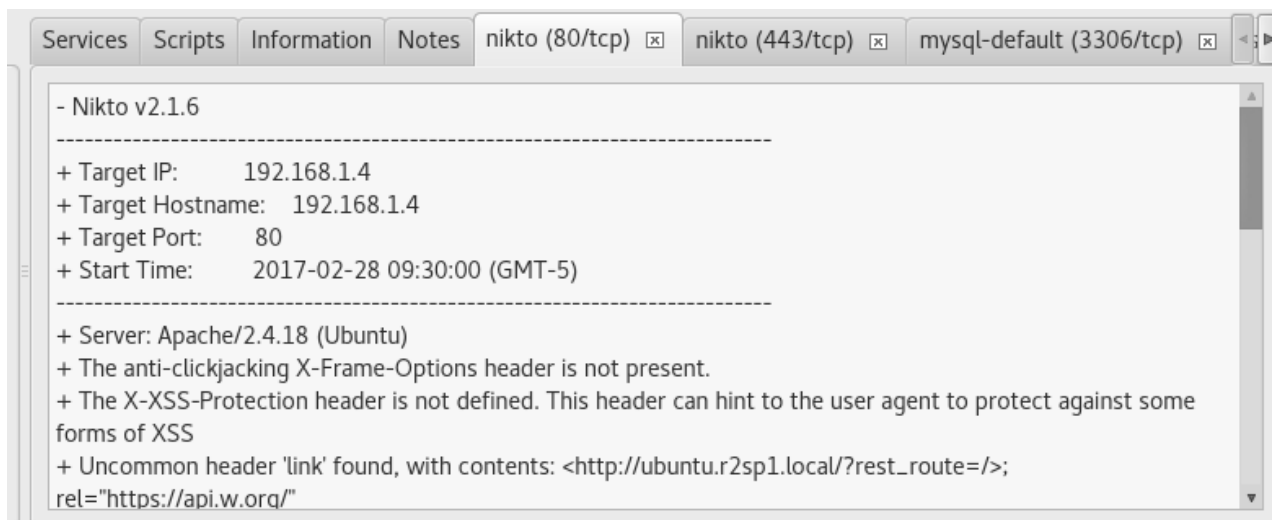
Дополнительно мы можем запустить whatweb, dirbuster, сделать скриншот выбранного веб-приложения.



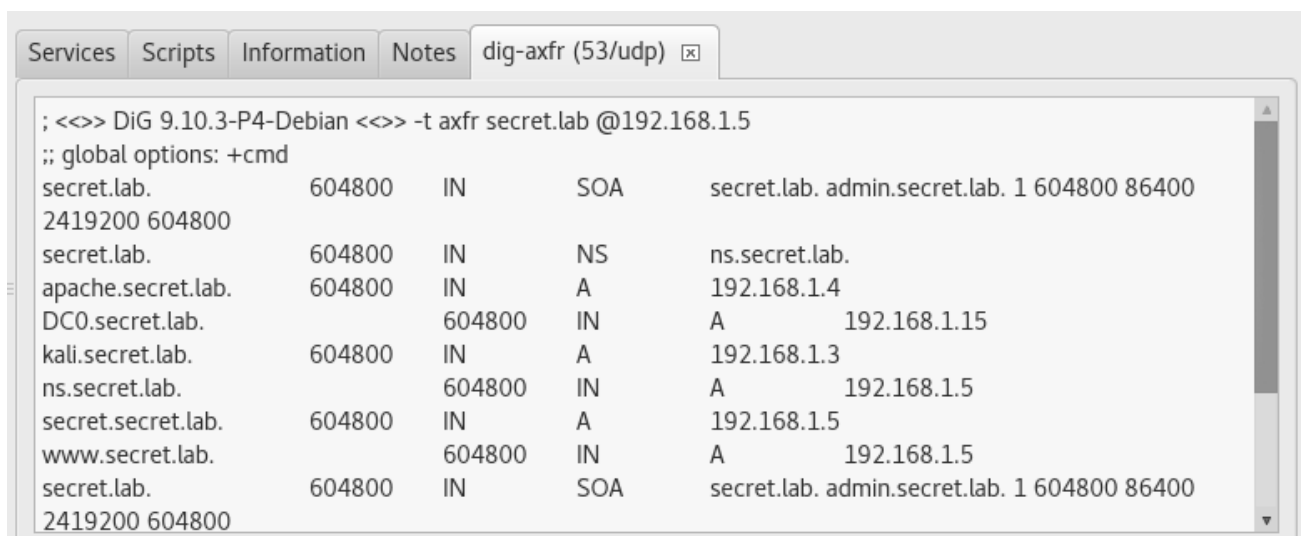
Для MySQL, соответственно, будет доступна опция mysql client и так далее. Для DNS доступен трансфер зоны, который мы добавили в начале статьи.



Так же в логе видно, что автоматически было выполнено задание dig-axfr. Если вы хотите увидеть весь список инструментов, удерживайте SHIFT во время правого клика. Вкладки с выводом от запущенных инструментов содержат полный вывод результатов работы инструмента



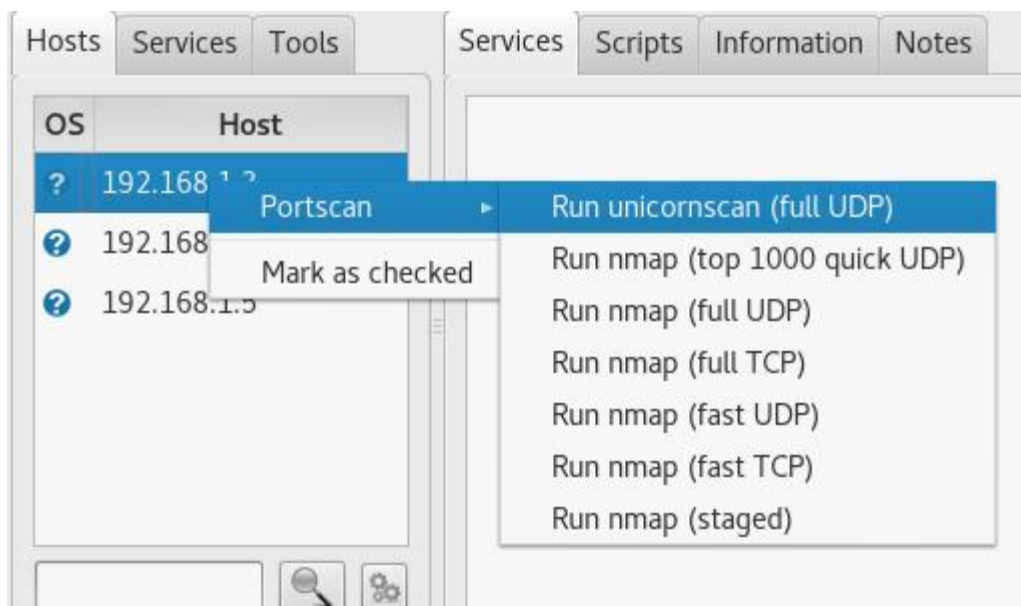
Вывод добавленного нами инструмента отображается корректно:



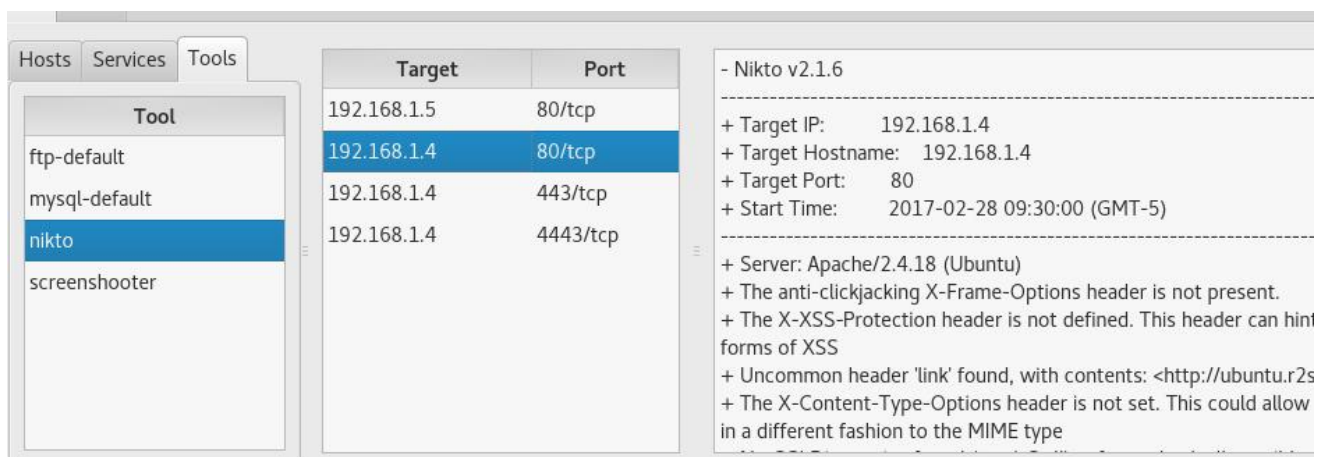
Помимо вкладок, привязанных к инструментам, запускаемым Sparta, нам доступны следующие:

- **Services** – содержит список обнаруженных сервисов
- **Scripts** – содержит результат работы скриптов nmap NSE (заполняется при запуске nmap с -sC или при правом клике на сервисе и выборе соответствующей опции)
- **Information** – содержит базовую информацию о хосте, такую как IP, MAC адреса, тип и версию ОС, статические показатели
- **Notes** – позволяет добавить собственный комментарий к хосту

- Есть возможность провести дополнительное сканирование выбранных хостов при помощи правого клика на выбранном хосте в списке.



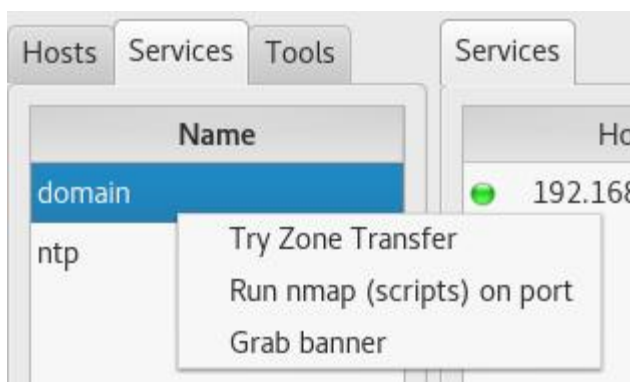
Так же, есть возможность просмотреть найденную информацию не только в разрезе хостов, но и в разрезе сервисов или отработавших инструментов. Например, посмотреть результат работы nikto по всем хостам:



Или увидеть, на каких машинах есть веб-приложения:

Name	Host	Port	Protocol	State	Details
domain	192.168.1.4	80	tcp	open	Apache httpd 2.4.18 ((Ubuntu))
ftp	192.168.1.4	443	tcp	open	Apache httpd 2.4.18 ((Ubuntu))
http	192.168.1.4	4443	tcp	open	OpenSSL s_server -www httpd (cc
mysql	192.168.1.5	80	tcp	open	nginx 1.10.0 (Ubuntu)
ssh					

Здесь есть важная особенность, что Sparta не будет запускать один и тот же инструмент в отношении хоста, против которого уже проводилось сканирование этим инструментом, если вы запустите инструмент через вкладку Services. Чтобы запустить инструмент против всех хостов, удерживайте SHIFT во время правого клика.



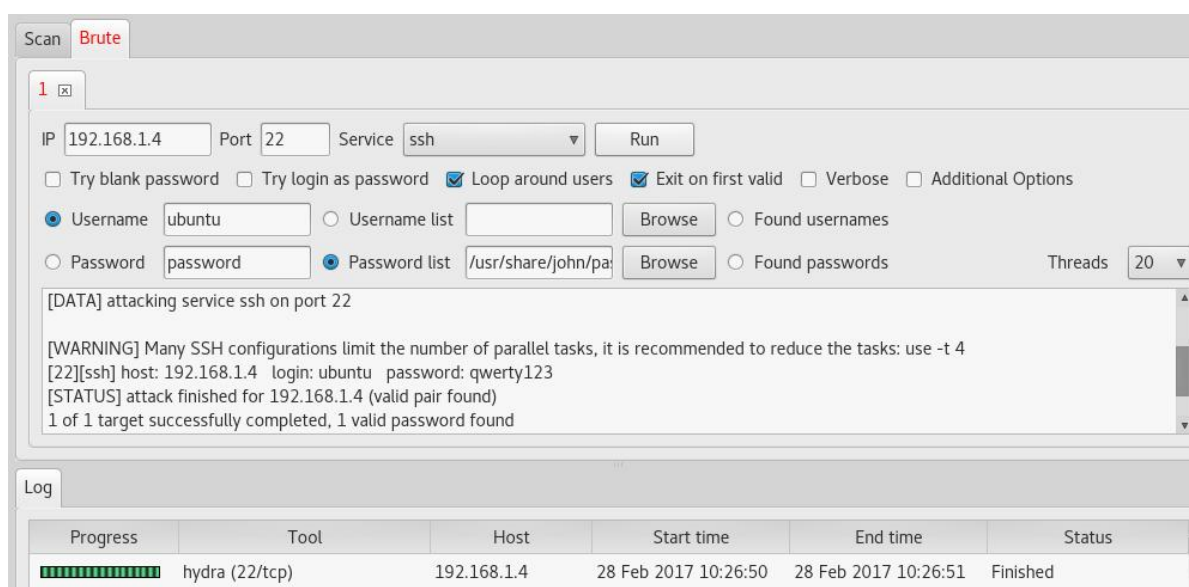
После того как вы решили, что исследовали хост, можно правым кликом и опцией «Mark as checked» пометить его в списке:

OS	Host
?	192.168.1.3 (kalix64)
?	192.168.1.4
?	192.168.1.5

После этого против данного хоста инструменты больше запускаться не будут.

Вкладка Bruteforce позволяет настроить и запустить брутфорс при помощи hydra.

Основные опции вынесены в графический интерфейс, такие как выбор файлов с пользователями и паролями, опция Loop around users, которая позволяет проверять все словарные пароли для каждого пользователя по порядку, а не каждый пароль по всем пользователям и другие. При помощи опции Additional options вы можете дописать свои ключи.



Так же полезными будут опции Found usernames и Found passwords для брутфорса по уже найденным логинам и паролям. Сохранить результат своих исследований можно через меню File – Save в специальном формате:



Задание

Необходимо запустить виртуальную машину Kali Linux. Пароль и логин для авторизации в системе root:toor

Вариант брать согласно журналу из файла Variants.txt

По варианту, согласно номеру журнала, произвести сканирование сайта. Описать этапы, найденные уязвимости, варианты их закрытия. Составить отчет, в котором указать:

- Цель сканирования
- Найденные уязвимости
- Возможные вектора атак
- Варианты патча (закрытия уязвимости)