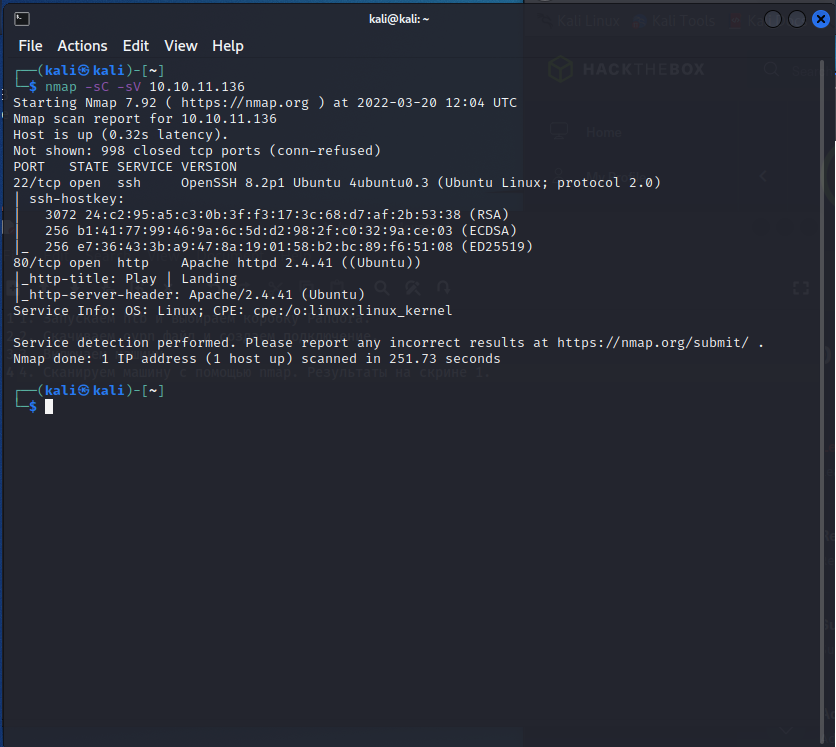
Решение Pandora

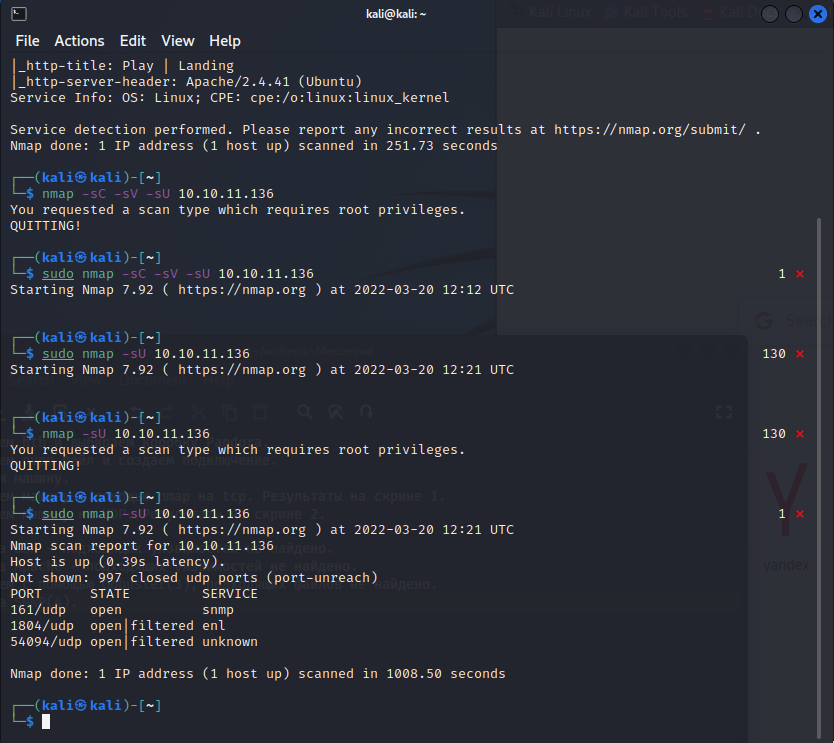
Ленц Олег, М-09.04.01кб

В качестве машины для решения была выбрана *Pandora*. Для решения машины создаем создаем *VPN* соединение, скачиваем *ovpn* файл и открываем с помощью *openvpn*. Включаем машину.

1. Сначала проводим сканирование машины с помощью *nmap* по *TCP* портам:

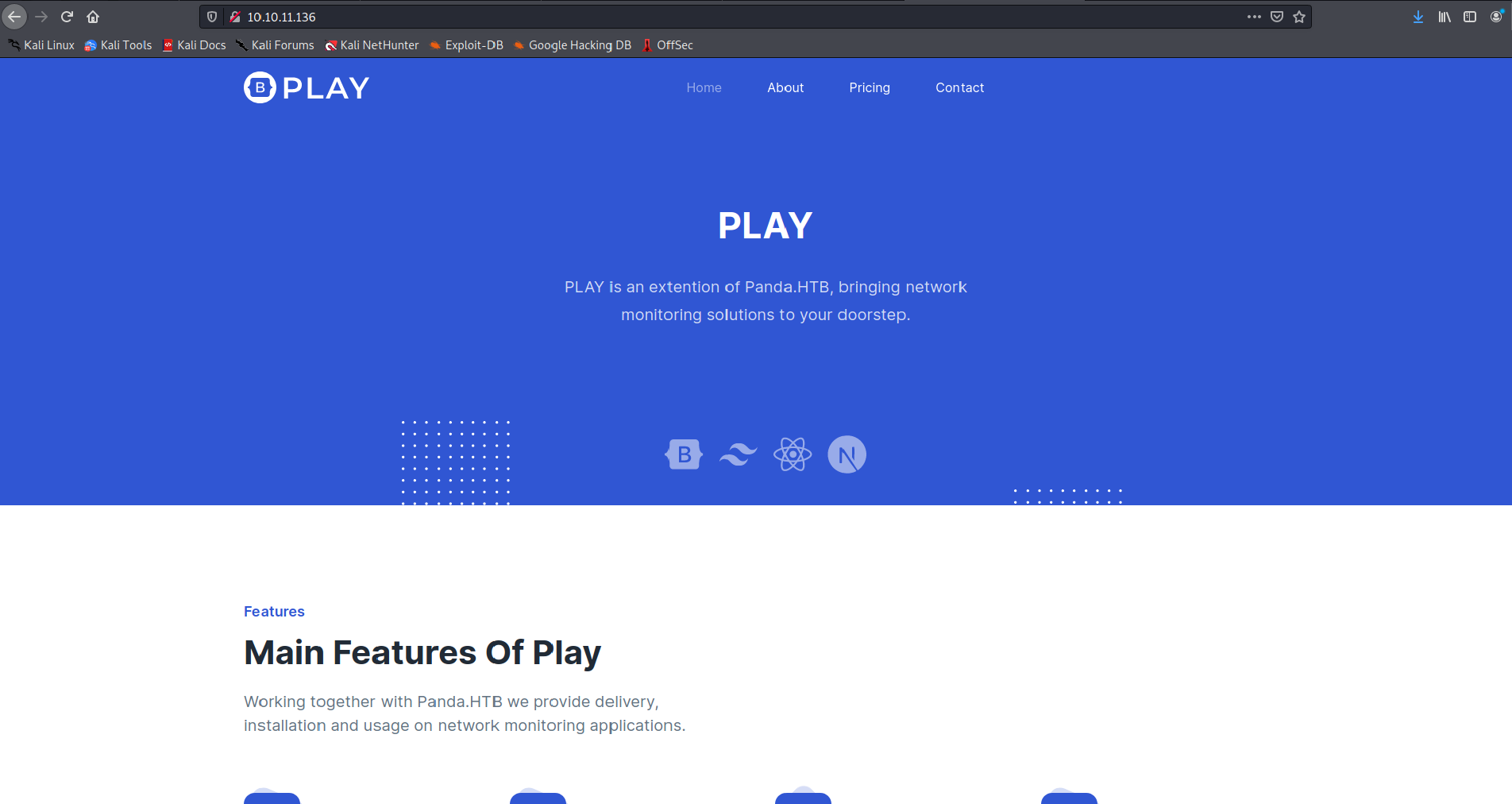


и по *UDP* портам:

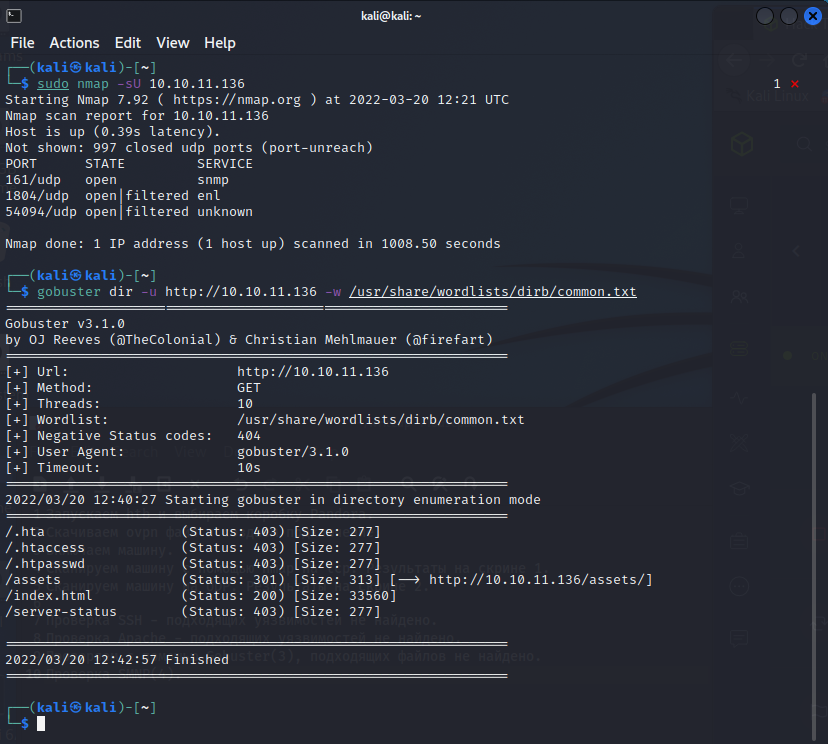


В результате находим три службы: *SSH*, *Apache* и *SNMP*. Для *SSH* подходящих уязвимостей не найдено. Сервер *Apache* тоже не предоставляет интересных возможностей.

Смотрим сайт на сервере:



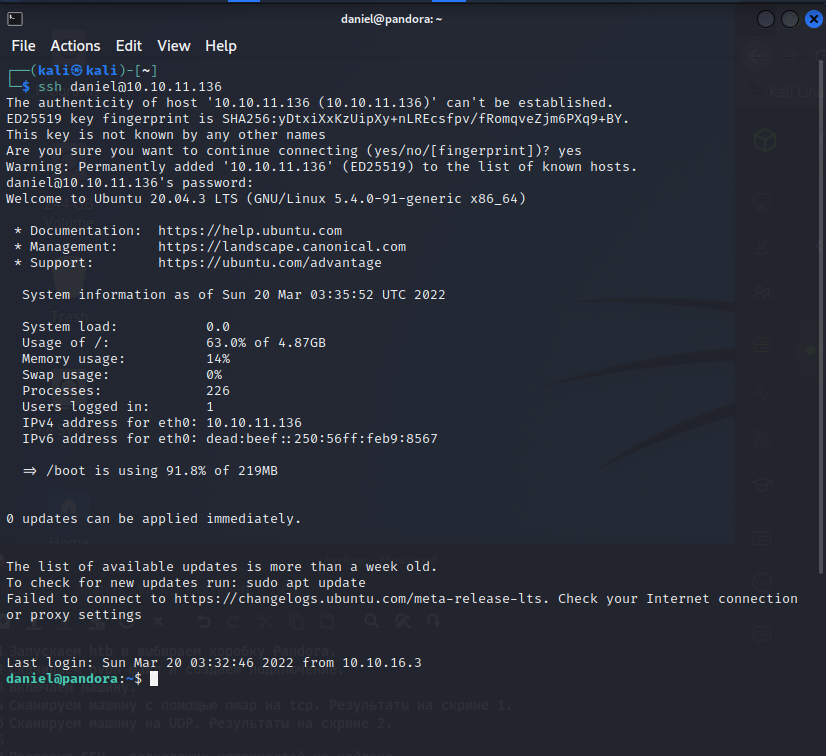
Ничего полезного на сайте нет. Пробуем использовать *gobuster* для перечисления сайта:



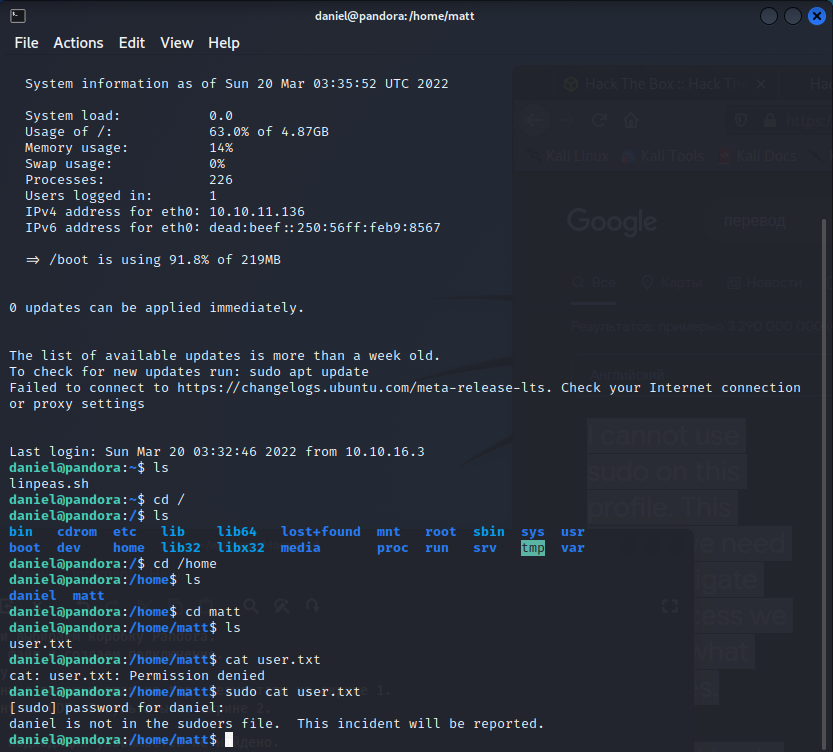
Также ничего полезного. Остается *SNMP*, для анализа используем следующую команду: *snmpwalk -c public -v2c -On 10.10.11.136*. Вывод значителен, поэтому переводим его в файл. Там мы находим учетные данные пользователя daniel:

*.1.3.6.1.2.1.25.4.2.1.5.1117 = STRING: "-u daniel -p HotelBabylon23"*

Пробуем подключиться к *SSH* по этим данным:



Подключение установлено, файл *user.txt* найден, но доступа к нему нет. Надо повышать привилегии.



Для этого эффективным решением будет использование скрипта *linpeas.sh.* Скачиваем его на свою машину, с помощью *scp* переносим на уязвимую машину и выдаем права на исполнение. В результате работы скрипт выдает интересную информацию:



В системе найдена уязвимость CVE 2021-4034, связанная с pkexec. При эксплуатации уязвимости пользователь получает возможность выполнять команды под правами root. В интернете находим существующие эксплоиты, выбираем тот, что написан на Python (*https://github.com/joeammond/CVE-2021-4034*), так как скомпилировать эксплоит на *c* нельзя. Передаем эксплоит на уязвимую машину и запускаем. Эксплоит позволяет нам ввести команду *cat* *home/matt/user.txt* под правами root, так мы получаем ключ.

