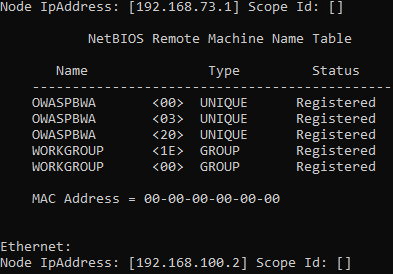
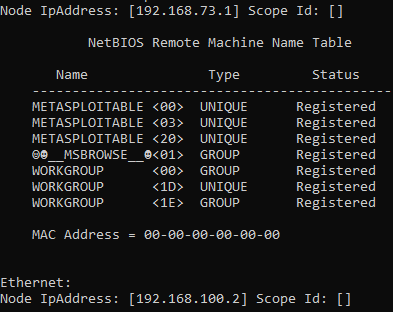
**Практика.** Оценка информации о системе и идентификация уязвимостей

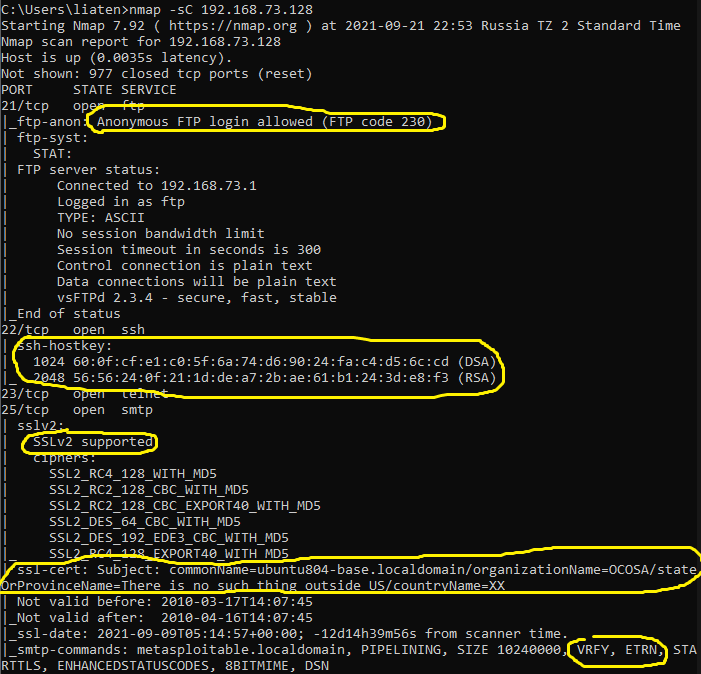
У нас есть **nmap**, но кроме него есть и встроенный в систему Windows инструмент, который мы можем использовать для сбора информации о цели, на которой работает [NetBIOS](https://ru.wikipedia.org/wiki/NetBIOS) или протокол [Server Message Block](https://ru.wikipedia.org/wiki/Server_Message_Block). Мы поняли, что можем использовать этот инструмент, т.к. на шаге анализа сервисов мы обнаружили что в системе присутствует пакет программ [Samba](https://ru.wikipedia.org/wiki/Samba).

1. Введем в командной строке **nbtstat -A 192.168.86.176**, мы обратились к службе NetBIOS и запросили таблицы имён удаленной машины. Мы выяснили что эта машина называется **OWASPBWA** и она является членом рабочей группы **WORKGROUP**. Теперь давайте сделаем тоже самое для второй машины **192.168.86.177.** Машина называется **METASPLOITABLE** и она является членом рабочей группы **WORKGROUP**.

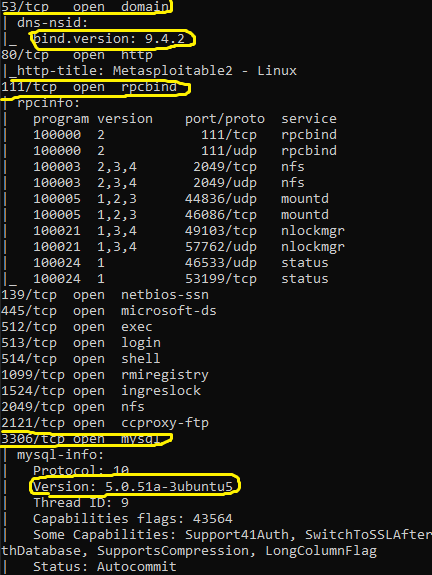




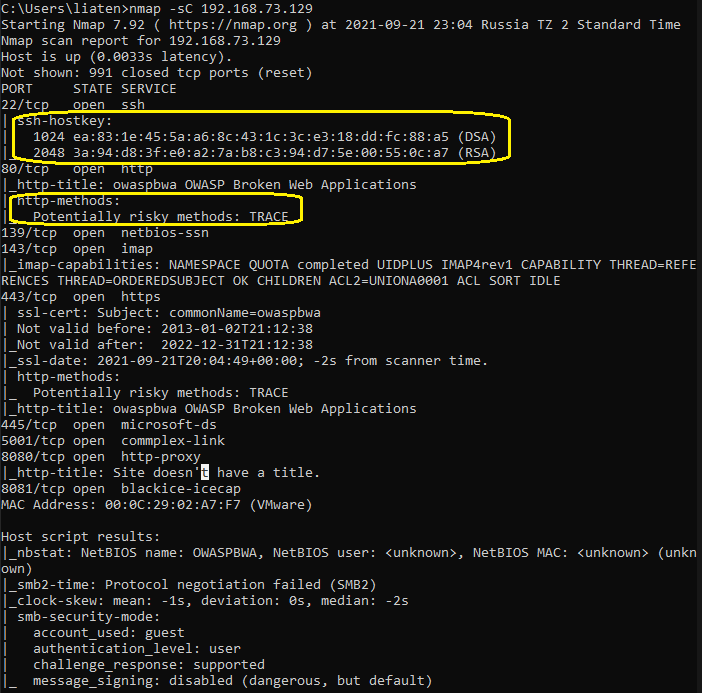
1. Теперь давайте воспользуемся [скриптовым движком nmap](https://nmap.org/man/ru/man-nse.html). Введем команду **nmap -sC 192.168.73.128** (metasploitable).



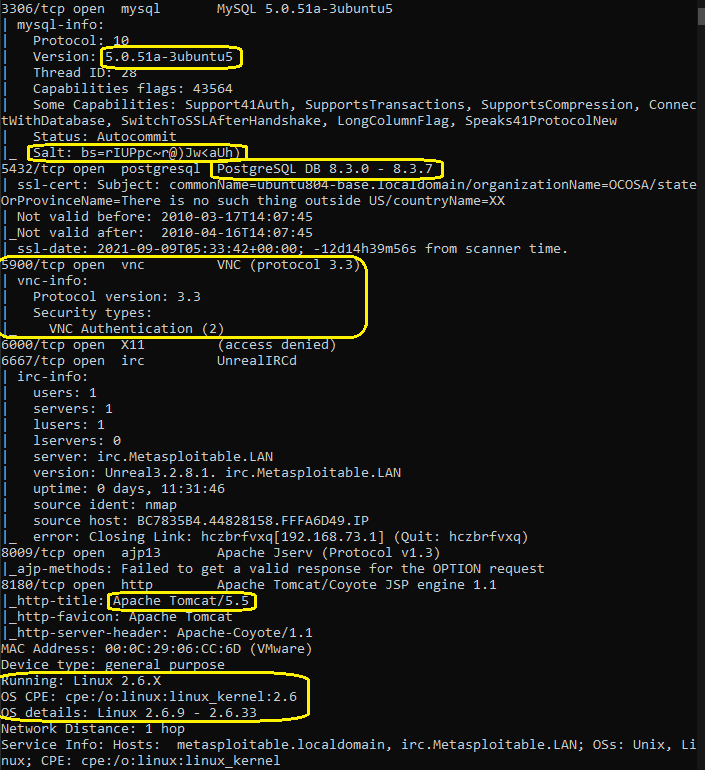
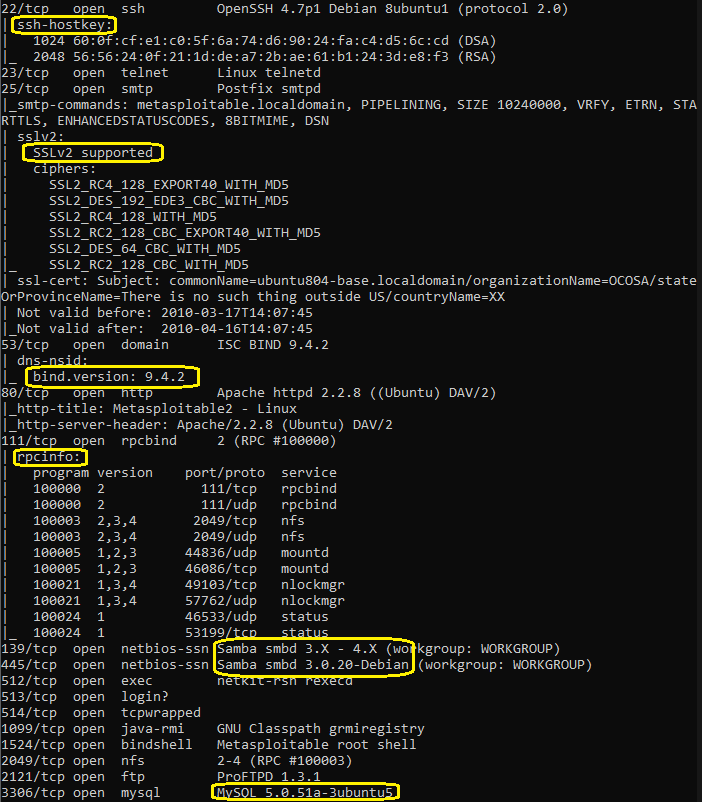
1. Мы получаем довольно большой ответ, мы видим, что
   1. Разрешен анонимный доступ к ftp,
   2. Есть в наличии отпечаток ssh ключа
   3. Есть SMTP команды доступные на машине (VRFY и ETRN)
   4. Есть сертификат SSL и информация о том, что поддерживается SSLv2, он является уязвимым на сегодняшний день и не должен поддерживаться.
2. Смотрим дальше:



1. Мы видим, что
   1. на 53 порту работает служба доменных имен, мы знаем версию софта, на которой она работает, 9.4.2. Возможно в этой версии есть уязвимости.
   2. у нас есть порт 111 (удаленный вызов процедур), видим информацию о [rpc](https://ru.wikipedia.org/wiki/%D0%A3%D0%B4%D0%B0%D0%BB%D1%91%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B2%D1%8B%D0%B7%D0%BE%D0%B2_%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D0%B4%D1%83%D1%80).
   3. на порте 3306 ведётся mysql и мы даже знаем её версию, 5.0.51a
   4. есть информация о Samba которую мы уже получали ранее, и много-много всего другого.
2. Давайте посмотрим на вторую целевую машину, **nmap -sC 192.168.73.129** (OWASP)**.**



1. Мы видим опять отпечаток ssh ключа, на 80 порту доступен потенциально опасный http метод TRACE, есть данные об imap и многие другие детали, которые мы можем использовать для создания векторов атак.
2. Давайте введём команду **nmap -A 192.168.73.128 -T 4** (meta) используем тайминг 4, для ускорения процесса. Данная команда определяет всё что доступно, её нужно запускать в последнюю очередь, т.к. это занимает много времени. Можно было бы сразу запустить данную команду, но бывают случаи что она может что-то упустить. Методология советует проводить сканирование шаг за шагом, как это делали мы в данной работе. Команда -A вызывает довольно мощное сканирование, в принципе она может вызвать отказ в обслуживании, т.е. вывод из строя машину, которую вы сканируйте. Ну что, смотрим на результаты:



1. Мы получили много информации для изучения. Мы узнали, что на машине работает [протокол VNC](https://ru.wikipedia.org/wiki/Virtual_Network_Computing), получили информацию по соли и другие данные, видим те же данные по rpc и SSLv2 и т.д. Мы видим версию базы данных PastgreSQL версии 8.3.0-8.3.7, версию Samba 3.0.20, версию и ядро операционной системы и много другой интересной информации.

Теперь вы понимаете, как провести оценку информации о системе.