Hacker Highschool

SECURITY AWARENESS FOR TEENS



УРОК 5
ИДЕНТИФИКАЦИЯ СИСТЕМЫ

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

ПРЕДУПРЕЖДЕНИЕ

Проект Hacker Highschool является средством обучения и, как в любом обучающем средстве, существует опасность. Некоторые уроки, если ими злоупотреблять, могут привести к физической травме. Также дополнительные опасности могут быть там, где еще недостаточно исследований о возможных последствиях излучений от специфической техники. Студенты, использующие эти уроки находится под контролем преподавателя, и, в тоже время, должны быть мотивированы на изучение материалов и непрерывную практику. ISECOM не несет ответственности за применение информации, полученной из данных материалов и за дальнейшие последствия.

Все представленные здесь материалы являются открытыми и общедоступными в соответствии с положениями и условиями организации ISECOM:

Все материалы проекта Hacker Highschool предназначены для некоммерческого использования в работе с учениками средних государственных или частных школ, техникумов, студентами высших учебных заведений, слушателями младших курсов Hacker Highschool и учащимися на дому. Эти материалы в любой форме не могут быть использованы для продажи. Обучение по этим материалом в обучающей организации, техникумах, университетах, профессионально-технических заведениях, летних или компьютерных лагерях и других организациях, в которых взимается плата за обучение, категорически запрещено без приобретения лицензии. Для более подробного ознакомления с условиями использования либо приобретения лицензии для коммерческого использования материалов, посетите раздел сайта предназначенный для Лицензирования http://www.hackerhighschool.org/licensing.html.

Проект HHS является результатом труда открытого сообщества и, если Вы находите наши труды ценными и полезными, мы просим Вас поддержать нас путем приобретения лицензии, пожертвований, либо спонсорства.

СОДЕРЖАНИЕ

СОТРУДНИКИ ЖУРНАЛА

Pete Herzog, ISECOM
Glenn Norman, ISECOM
Marta Barceló, ISECOM
Chuck Truett, ISECOM
Kim Truett, ISECOM
Marco Ivaldi, ISECOM
Greg Playle, ISECOM
Bob Monroe, ISECOM
Simone Onofri, ISECOM
Ryan Oberto, Johannesburg South Africa
Dennis King
Mario Platt
Grigoris Chrysanthou, Cypress

Переводчики

Vadim Chakryan, Kharkiv National University of Radio Electronics
Olena Boiko, Kharkiv National University of Radio Electronics
Dmitriy Pichuev, Ukrainian Engineering Pedagogical Academy

ISECOM

ВВЕДЕНИЕ

«Мне кажется, на моём ноутбуке появился вирус», — сказал мне один из моих студентов. — «Можете взглянуть?»

Я взял его ноутбук, и, не открывая его, покрутил его во всех направлениях, внимательно осматривая. «По-моему, похоже на компьютер», — сказал я, передавая его обратно владельцу.

«Но что-то с ним не так», — настаивал Эйден. «Я заглянул в гости к своему другу, зашёл в Интернет, а потом что-то попало в моё электронное письмо и отправило какие-то сообщения всем моим друзьям».

«Хорошо. Как ты прочитал своё письмо? Ты установил какое-то приложение?» — спросил я.

«Нет, я прочитал через веб. То есть Интернет».

«Ты имеешь в виду веб-браузер?» Он кивнул. «В таком случае, это письмо находится онлайн, а не на твоём компьютере. Я бы начал с твоего почтового ящика. Ты поменял пароль?»

«Да, конечно. Мой аккаунт был заблокирован, пока я не поменял пароль.» Он смотрел в пол, как будто не досказал всю историю, но я и не настаивал. Я был уверен, что на него и так много кричали из-за этой ситуации.

Вместо этого я спросил: «Твои друзья после этого получали ещё такие сообщения?»

«Нет». Он пристально смотрел в пол на свои ботинки.

«Ты выбрал надёжный пароль? Не 12345?»

Теперь он улыбнулся. «Он действительно сложный. Никто и никогда не сможет его подобрать».

У меня были сомнения по этому поводу, но я кивнул. «Хорошо, тогда похоже, что ты уже решил проблему».

«Нет», — настаивал он. — «Зачем кому-то такое делать?»

Наконец-то рыбка попалась на крючок. «Почему бы тебе не узнать это? У тебя сохранилось какое-нибудь сообщение из тех, которые получили твои друзья?»

«Да, целая пачка. Друзья отправляли их обратно мне.» Ах, вот оно что. Я мог поспорить, что список его контактов насчитывал десятки, а то и сотни записей. Дело обещает быть весёлым.

«Похоже, что тебе нужно выяснить, куда конкретно ведёт та ссылка в письме.»

Он загорелся этой идеей. «Вы хотите сказать, что мы можем это сделать?»

«Ха», — засмеялся я. — «Я хочу сказать, что ТЫ можешь это сделать. Но я могу рассказать, что для этого нужно.»

Эйден задумался. «Это как в той истории про овцу и волка?»

«Да, именно. Ты можешь быть как овцой, так и волком. Выбирай», — сказал я ему.

Внезапно куда-то исчезла его детская наивность. «Хочу быть волком», — решил он.

* * *

Идентификация системы несомненно может оказаться наиболее важным шагом любой компьютерной атаки или защиты. Дальнейшие ваши действия зависят от данных, которые Вы соберёте на этом этапе. Какая операционная система установлена на устройстве, которое

проводит атаку или на которое проводится атака? Можете ли Вы или кто-то другой посмотреть запущенные приложения или службы? Что насчёт деталей учётной записи администратора: возможно это информация лежит где-то на виду? Это те вопросы, которые нужно задать на данном этапе. В зависимости от того, по какую сторону атаки Вы находитесь, Вы можете обрадоваться или ужаснуться тому, какую информацию Вы можете с лёгкостью получить, если знаете, где искать.

Знать, как организовать атаку, — это, конечно, круто. Но гораздо круче знать, как защититься от такой атаки. Мы постараемся глубже разобраться в этой теме и изучим, как можно идентифицировать систему и найти её слабые места — будь это ваша система или кого-то другого.

Мы будем использовать утилиты, которые находятся в свободном доступе, а также покажем, как ими пользоваться. Практически бессмысленно просто показать программу, не научив при этом, как ею пользоваться. Как и любые другие программы обеспечения безопасности, их можно использовать для хороших или плохих целей. В уроке будут показаны оба подхода к их использованию, так что Вы сможете попробовать себя как в роли организатора атаки, так и в роли защитника от таких атак.

В этом уроке Вы познакомитесь с двумя персонажами: один из них будет учить, другой — учиться. Учитель не всегда знает ответ, так что вы, как читатель, тоже не получите всю информацию на тарелочке. Учитесь взламывать и учитесь восстанавливать то, что взломали.

Будьте особенно внимательны к атрибутам, которые используются в различных программах. Небольшое изменение (к примеру, ввод буквы в нижнем регистре вместо верхнего) может привести к абсолютно другим результатам, тем более в разных операционных системах. В первых трёх уроках рассматриваются основы работы в сети и основы того, как работает Интернет. Каждый урок основывается на знаниях, полученных в предыдущих параграфах и уроках, так что не торопитесь проскакивать страницы. Легко пропускать параграфы или страницы, но при этом можно упустить рассмотрение очень важных вопросов.

ИДЕНТИФИКАЦИЯ СЕРВЕРА

«Хорошо, Эйден, что тебе удалось узнать?» Я пытался не стиснуть зубы от опасения, что он перешёл по той дурацкой ссылке в письме, которое было отправлено с его взломанного аккаунта.

«Я не щёлкал по ней», — ответил мне Эйден, улыбнувшись, как будто он прочитал мои мысли. «Я скопировал её и вставил в текстовый файл.»

«Ты скопировал текст, который отображается? Или фактическую ссылку?»

Он нахмурил брови. «Я не дурак. Я нажал правую кнопку мыши и выбрал 'Копировать адрес ссылки'. Затем вставил в документ. Вот, смотрите, link.txt.»

«Извини. Я просто хотел удостовериться. Хорошо. Куда ведёт эта ссылка?»

«Это какая-то абракадабра. Домен Chewmoogoo.com или что-то вроде того. И дальше какой-то набор букв», — ответил он, открывая свой ноутбук и показывая ссылку.

«Да, точно», — сказал я ему. — «Теперь-то они попались. Давай посмотрим, какую информацию мы можем собрать. Для этого нужно подобрать специальные утилиты. Сначала поговорим о доменных именах и IP-адресах».

ИДЕНТИФИКАЦИЯ ВЛАДЕЛЬЦА ДОМЕНА

Первый шаг идентификации удалённой системы — это анализ имени хоста, а также имени и IP-адреса домена. С помощью **whois-**поиска по доменному имени можно обнаружить много полезной информации:

- Личность владельца домена (обычно его полное имя);
- Контактная информация: почтовые адреса, номера телефонов и адреса электронной почты;
- Серверы DNS, где зарегистрирован домен, что также может указать на Интернет-провайдер, который обслуживает домен;
- IP-адрес сервера, еще один потенциальный ключ к определению Интернет-провайдера;
- Информация о доменном имени: дата создания, время обновления информации, дата истечения срока регистрации

Следует учитывать, что существует целый ряд различных регистраторов доменных имён, и не все базы данных whois содержат информацию по всем доменам. Возможно, Вам придется воспользоваться несколькими базами данных whois для того, чтобы найти информацию об исследуемом домене.

Эйден мгновенно усвоил все эти сведения. «Хорошо. Что мне теперь делать?»

«Вот твоё задание», — сказал я ему.

УПРАЖНЕНИЯ

5.1 Используя доменное имя, о котором Вы собираете сведения (если Вы не Эйден, используйте isecom.org), выполните следующую команду в Linux, Windows и OSX.

```
whois isecom.org
```

Кто владеет доменом?
Когда он был создан? Когда истекает срок его регистрации? (Дают ли эти сведения возможность для каких-то действий?)
Когда он в последний раз обновлялся?
Чьи контакты указаны?
Какие у этого домена первичный и вторичные серверы доменных имён?

5.2 Теперь выполните аналогичный поиск в браузере (например, http://www.whois.net -> "sample.com"). Важным вопросом является следующий: соответствуют ли эти данные тем данным, которые были получены в результате выполнения команды whois?
Посмотрите хотя бы два веб-сайта whois (попробуйте http://whois.domaintools.com; сможете найти другие сайты?).

ИДЕНТИФИКАЦИЯ **IP-**АДРЕСА ДОМЕНА

«Итак, что же у тебя получилось?» — поинтересовался я у Эйдена.

«Вот все эти данные. Я добавил их в файл.» Он показал текстовый файл.

«Хорошо. Сохраняй любую, даже незначительную информацию. Какой IP-адрес у домена?»

«Похоже, что вот этот», — Эйден указал на число с большим количеством цифр.

«Да, ты прав. Ты можешь определить IP-адрес домена с помощью команды whois или просмотреть DNS-записи с помощью команды **ping**:

```
ping isecom.org
```

«В первой строке результата выведется IP-адрес домена.»

> Если Вы сможете перехватить или просто получить электронное письмо от цели, проанализируйте заголовки письма (см. Урок 9, Безопасность электронной почты); там указывается IP-адрес устройства отправителя. Вы также можете использовать поисковые системы (Урок 20, Социальная инженерия) или утилиты (**Maltego**, **FOCA**). Поищите название организации, контактную информацию владельца домена, номера телефонов и адреса. Любые подобные сведения могут привести к ещё более существенной информации.

«Как только ты определил один или несколько IP-адресов, тебе нужно определить их местонахождение. Группы IP-адресов назначаются Интернет-провайдерам по всему миру. Выясни, к какой группе принадлежат те IP-адреса, которые ты определил (и кто имеет права на эту группу, если сможешь это выяснить). Это может помочь тебе узнать, какой сервер или Интернет-провайдер использует веб-сайт. Настоящей ценностью для тебя будет найти, в какой стране расположен этот сервер», — сказал я Эйдену. «Могу поспорить, что не в этой. Вот что тебе нужно сделать дальше.»

УПРАЖНЕНИЯ

Теперь мы непосредственно рассмотрим DNS-записи. Ещё одним способом получения информации о домене и сервере (или серверах) является использование информации в DNS. Начнём с трёх основных команд.

5.3 Откройте окно терминала. Выполните следующую команду:

```
dig isecom.org
```

Работает ли эта команда на вашей ОС? Попробуйте выполнить её в Windows, Linux и OSX.

5.4 Теперь выполните следующую команду:

```
host isecom.org
```

Работает ли эта команда на вашей ОС? Попробуйте выполнить её в Windows, Linux и OSX.

5.5 Наконец, выполните следующую команду:

```
nslookup isecom.org
```

Работает ли эта команда на вашей ОС? Попробуйте выполнить её в Windows, Linux и OSX.

Какой DNS-сервер у исследуемого объекта? Есть ли у организации сервер электронной почты? У этого сервера тот же IP-адрес, что и у веб-сервера? Какие предположения можно сделать, основываясь на этих сведениях? Какую ещё информацию Вы можете извлечь из полученных результатов?

5.6 При известном IP-адресе Вы можете обратиться к записям баз данных членов Организации ресурсов нумерации **(the Number Resource Organization)** (http://www.arin.net/, http://www.ripe.net/ или http://www.apnic.net/), чтобы узнать подробности распределения IP-адресов.

ИГРА НАЧАЛАСЬ: РУБИ И ЖГИ

Это был матч-реванш, как была убеждена Джейс. Битва столетия — вот как она её называла. И не важно, сколько потребуется пота, крови, боли, физической или интеллектуальной силы, — амбициозная девушка была готова выиграть этот бой. Она должна была победить, ведь другого плана не было. Её волосы цвета шоколада покачивались над глазами, будто тореадор, дразнящий быка красным плащом. Один последний глубокий вдох, чтобы успокоиться, — и сетевой киллер готов к работе.

Её пальцы легко скользили по клавиатуре. Она оценила ситуацию и сделала переучёт доступных ресурсов. У Джейс была копия Nmap, уже загруженная в компьютерное чудовище. Ping и Traceroute уже были запущены, так что воинственный хакер был готов к началу нападения.

В атаку пошёл первый черёд команд, мгновенно вводимых с клавиатуры. Пулемёт не стреляет так быстро, как Джейс вводит команды. Ping, пошёл! Traceroute, пошёл! Поток данных был настолько велик, что сервера не успевали отвечать на запросы.

«Кровопролитие» было ужасным: биты и байты беспорядочно перемешивались на мониторе. Казалось, что командная строка направляет молниеносную атаку на мощные маршрутизаторы.

Джейс управляла основной атакой, чтобы получить точку опоры и укрепиться внутри сети. Её виртуальные разведчики интенсивно исследовали установленные брандмауэры, серверы и маршрутизаторы. Она сравнила эти данные со словарём уязвимостей (Common Vulnerabilities and Exposures, CVE) и сопоставляла их с информацией по сканированию сети Nmap. Каждое слабое место, каждая уязвимость и эксплойт были проанализированы ради получения тактического преимущества и оценки размеров ущерба. Перемирие — не вариант для Джейс. Она побеждала.

Но ещё не всё, говорила она себе. На самом деле, всё, что она сделала к этому моменту, — так это захват всего лишь небольшой части вражеских ресурсов, но всё же информация была бесценной. Джейс со своей стороны понесла небольшие потери. Пальцы слегка болели. На лбу был небольшой ушиб, из-за удара головой о монитор в минуту отчаяния. TTL (time to live – время отклика от сервера) убивали её.

В скором времени она преодолела все преграды и успешно завершила первый этап своей операции. У Джейс теперь было достаточно информации о неприятеле для того, чтобы приступить ко второму этапу сетевой атаки. Для следующего шага были нужны несколько электронных писем и помощь ни о чём не подозревающего инсайдера (человек, работающий внутри компании).

Это всегда была самая страшная часть любой битвы — добыча потенциальных шпионов. Джейс нужны были пользователи этой сети, которые посочувствовали бы её мотивам. Настало время нарушать все хорошие привычки, касающиеся безопасности систем. Социальная инженерия была оружием массовой дезорганизации в её арсенале. Ей нужно было правильно сформировать электронные письма с прикреплёнными троянцами, чтобы проникнуть за внутренние стены сети.

Подготавливая злодейские письма, Джейс поняла, что она была на правильной стороне этого противостояния. Не важно, чего это будет стоить и сколько времени займёт — Джейс была полна решимости узнать, какой следующий секретный вкус мороженого разрабатывал местный молочный магазин.

Игра продолжается...

ИДЕНТИФИКАЦИЯ СЛУЖБ

«Так, ты сохранил все собранные данные, да?» Я попытался скрыть ухмылку, так как я знал ответ, но мой преподавательский долг заставил спросить об этом.

Эйден только искоса взглянул на меня: вот зануда подумал он, но вслух сказал: «Можете посмотреть», — и дал мне свой ноутбук.

«Теперь их очень много, не правда ли?» — я прокрутил несколько страниц.

«Да уж. Мне нужно как-то получше и поудобнее сохранять и отслеживать информацию», — сказал Эйден, забирая обратно компьютер.

«Действительно. Какой IP-адрес твоей цели?». На этот раз улыбку я не сдерживал.

«Эмм... их около пяти. Может, даже больше. Я пытаюсь выяснить, почему так, ведь на некоторые IP я могу запустить ping, а на другие — нет.»

«Молодец» - подумал я. При известных IP-адресах для домена ты можешь начинать исследовать службы, которые на них работают. Вот где начинается веселье.

PING И TRACEROUTE

«Ты всё правильно начинаешь делать. Ты должен убедиться в том, что по этим адресам есть работающие машины. И да, ты прав: ping — твой друг. Ты ведь не забыл запустить ping на доменное имя, IP-адреса и различные имена хоста, не так ли?»

«Какие из них — имена хоста?» — спросил Эйден.

«Те, в которых есть буквы и точка перед доменным именем, как, например, www.isecom.org», — ответил я.

«Что-то я таких не вижу.»

«Проверь результаты, которые тебе показала утилита dig. Ты пробовал запустить ping на www.isecom.org, ftp.isecom.org и mail.isecom.org?»

«Нет...»

«Если ты получишь ответ, то по этому адресу есть рабочий хост. Ты проходишь через брандмауэр. И они пропускают ICMP.» Я открыл окно консоли и ввёл команду:

```
C:\>ping isecom.org

Pinging isecom.org [216.92.116.13] with 32 bytes of data:
Reply from 216.92.116.13: bytes=32 time=186ms TTL=56
Reply from 216.92.116.13: bytes=32 time=186ms TTL=56
Reply from 216.92.116.13: bytes=32 time=186ms TTL=56
Reply from 216.92.116.13: bytes=32 time=186ms TTL=56

Ping statistics for 216.92.116.13:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 186ms, Maximum = 186ms, Average = 186ms
```

«Ты можешь предположить, насколько далеко от тебя расположен сервер, как в сетевом отношении, так и физически, по времени получения ответа. Раздели это число на два и ты сможешь оценить расстояние до сервера. Попробуй ещё одну утилиту — traceroute. В Windows используется команда **tracert**, а в Linux — **traceroute**. С её помощью можно пошагово просмотреть путь пакета от твоего компьютера до цели. К примеру, вот так», — объяснил я ему и ввёл команду.

```
C:\>tracert isecom.org
```

«Я хочу, чтобы ты выполнил задание.»

УПРАЖНЕНИЯ

5.7 Используйте traceroute/tracert, чтобы скомпоновать всю информацию, которую Вы можете найти о компьютерах и маршрутизаторах между вашим компьютером и целью.

5.8 Компьютеры с похожими IP-адресами обычно находятся в одной и той же сети. Запустите ping на веб-сайт или IP-адрес (например, выполните команду ping www.isecom.org или ping 216.92.116.13). Если Вы получите успешный отклик, то запустите ping на следующий IP-адрес. Вы получили ответ? Повторите ту же команду для близлежащих адресов.

5.9 Используйте поисковую систему, чтобы определить, как оценить расстояние до сервера.

5.10 Поищите утилиту, которая поможет определить физическое расположение сервера.

5.11 Попробуйте использовать онлайн-утилиту Visual Trace Route. Существует довольно много сайтов с похожими утилитами. Они визуализируют путь трафика.

Nmap

«Всё получилось? Теперь позволь познакомить тебя с моим маленьким другом», — сказал я, пытаясь говорить пугающим голосом. Эйден посмотрел на меня как на выжившего из ума. Я прокашлялся и, хм, завершил предложение: «Это nmap.»

«С этой утилитой можно проводить как простые запросы, так и хитрые и продвинутые. Выполни команду nmap, а в качестве её аргументов используй имя хоста или IP-адрес, и он просканирует этот хост. Или используй несколько маршрутизаторов, чтобы сделать хитрый запрос. Если ты правильно введёшь параметры и опции, то в результате узнаешь операционную систему, которая установлена на исследуемой цели. Мы будем использовать опцию 'сканировать TCP', то есть -sT.»

```
nmap -sT 216.92.116.13

Starting Nmap 5.51 ( http://nmap.org ) at 2012-05-28 10:58 GTB Daylight Time
Nmap scan report for 216.92.116.13
Host is up (1.1s latency).
Not shown: 969 closed ports
PORT   STATE SERVICE
25/tcp  open smtp
80/tcp  open http
110/tcp  open pop3
119/tcp  open nntp
135/tcp  open msrpc
139/tcp  open netbios-ssn
143/tcp  open imap
445/tcp  open microsoft-ds
465/tcp  open smtps
554/tcp  open rtsp

Nmap done: 1 IP address (1 host up) scanned in 215.42 seconds
```

Помните, что nmap — не единственная утилита для проведения такого сканирования. И это хорошо. Разные утилиты могут дать разные результаты, и, на самом деле, любая из них может повести Вас по ложному пути.

Вы можете задать nmap, к примеру, определение операционной системы – но Вам не следует доверять такой догадке! Проверяйте этот вариант с помощью других утилит.

АНАЛИЗ БАННЕРОВ

Эйдан был счастлив - "Посмотри ка, что у меня есть!". У него были текстовые документы и электронные таблицы на ноутбуке, а также рисунки и цветные распечатки, которые кому-то обошлись в копеечку.

"Отлично, теперь ты получил несколько работающих хостов, знаешь чьи они и где располагаются. Теперь ты, наверняка, хочешь узнать побольше об этих устройствах: какая операционная система на них работает? Какие сервисы на них запущены? Не так ли?" - спросил я его.

Это сделало его менее радостным - "Ну, что я могу сказать?"

"Тебе не нужно ничего говорить. Заставь машину рассказать тебе обо всем: какая версия операционной системы на ней установлена, какие сервисы работают и какие патчи были применены. Если ты выступаешь в качестве атакующего — эта информация значительно облегчит тебе жизнь; все, что тебе нужно будет сделать, так это найти подходящие эксплойты под программы и сервисы этих машин. Если ты защищаешь систему, тебе стоит ограничить подобного рода информацию для атакующего. Или, по крайней мере, выдать ложную информацию." - этот разговор заставил его задуматься..

"Итак, то, чем ты будешь заниматься далее называется — анализ баннеров. Это техника инвентаризации позволяет получить всю информацию об активных службах и портах на исследуемых устройствах. Я покажу тебе несколько команд. Ты можешь использовать telnet, ftp или netcat чтобы проанализировать баннеры. Баннер — это текстовое сообщение, которое ты видишь в консоли, когда подключаешься к удаленному устройству. Баннер показывает тебе какая программа запущена на сервере на определенном порту. «Когда я подключаюсь к анонимному FTP серверу, я получаю баннер. Проверь сам." - Я набрал команду в консоли:

```
ftp isecom.org

Connected to anon.server.
220 ProFTPD Server (Welcome . . . )
User (anon.server:(none)):
```

"Число 220 — это код, который оповещает о том, что сервер готов к использованию. Как видно, на этой машине запущен ProFTPD сервер. Теперь мы смотрим в Интернете, на какую операционную систему можно установить ProFTPD и какой у сервера функционал..." - я отодвинулся от клавиатуры. "Итак, твое следующее задание — использование ftp команд".

УПРАЖНЕНИЯ

5.12 Вы можете использовать команду FTP, указав имя хоста или его IP-адрес, вот так:

```
ftp isecom.org
```

или

```
ftp 216.92.116.13
```

Попробуйте оба варианта, чтобы посмотреть какие баннеры Вы получите. Результаты будут выглядеть примерно следующим образом:

```
Connected to isecom.org.
220 ftp316.pair.com NcFTPd Server (licensed copy) ready.
User (isecom.org:(none)):
```

5.13 Вы можете использовать утилиту Telnet с указанием имени хоста или его IP-адресом. Так же Вы можете указать порт, к которому хотите подключиться, к примеру введите порт 21, чтобы подключиться к FTP:

```
telnet isecom.org 21
```

или

```
telnet 216.92.116.13 21
```

Снова же, посмотрите на то, что за баннер Вам возвращает сервер, если он конечно вообще что-то возвращает. Результат, также, может выглядеть следующим образом:

```
220 ftp316.pair.com NcFTPd Server (licensed copy) ready.
```

5.14 Используйте утилиту netcat с указанием имени хоста или его IP адресом. Точно также как в случае с использованием Telnet, Вы можете указать порт, к которому хотите произвести подключение, к примеру введите порт 21 чтобы подключиться к FTP:

```
nc isecom.org 21
```

или

```
nc 216.92.116.13 21
```

Снова, обратите внимание, на то какой баннер Вам вернул сервер.

Баннеры, вводящие в заблуждение

"Вот фокус." - сказал я Эйдану. - "Ты можешь изменить баннер. Это один из методов маскировки – лгать о том, кто ты есть на самом деле. Итак, я могу изменить свой баннер, к примеру, на следующие "НеТвоеДелоЧтоЭтоЗаСервер Сервер». Конечно, баннер классный, все же не самый лучший. К примеру, если я использую Unix систему, а в баннере к ftp напишу "*WS_FTP Server*", который работает лишь под Windows системами, — это будет вводить атакующего в замешательство."

"Минутку, как Вы изменили баннер?" - спросил он.

"Очень рад, что ты спросил," - ответил я.

УПРАЖНЕНИЕ

5.15 Найди в Интернет информацию о том, как менять баннер на SMTP, FTP, SSH, HTTP и HTTPS. Разве это сложно? Другими словами, стОит ли доверять тому, что указано в баннере?

АВТОМАТИЗИРОВАННЫЙ АНАЛИЗ БАННЕРОВ

"А теперь попробуй вот что. Давай вернемся к nmap и автоматизируем процесс анализа баннеров; нам нужно будет использовать опции (параметры) -sTV для сбора баннеров." - я набрал команду и получил отчет:

```
nmap -sTV -Pn -n --top-ports 10 --reason -oA hhs_5_06 hackerhighschool.org

Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 05:10 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.30s latency).
PORT    STATE  SERVICE     REASON     VERSION
21/tcp  open   ftp         syn-ack    NcFTPd
22/tcp  open   ssh         syn-ack    OpenSSH 5.9 (protocol 2.0)
23/tcp  closed telnet      conn-refused
25/tcp  filtered smtp      no-response
80/tcp  open   http        syn-ack    Apache httpd 2.2.22
110/tcp open   pop3        syn-ack    Dovecot pop3d
139/tcp closed  netbios-ssn  conn-refused
443/tcp open   ssl/http    syn-ack    Apache httpd 2.2.22
445/tcp closed  microsoft-ds conn-refused
3389/tcp closed  ms-wbt-server conn-refused
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.32 seconds
```

"Nmap нашел NcFTPd, OpenSSH 5.9 (protocol 2.0) и Apache httpd 2.2.22. Ура: операционная система - Unix. Иногда анализ баннеров дает тебе возможность узнать версию операционной системы, однако нам потребуется чуть больше информации," - продолжил я. "Вот, что я предлагаю тебе сделать."

УПРАЖНЕНИЯ

5.16 Используя nmap просканируйте выбранный хост (hackerhighschool.org, если Вы не Эйдан).

5.17 Попробуйте просканировать хост снова, используя опцию --version-intensity number выбрав номер от 0 до 9 для получения точных результатов. Какую разницу Вы заметили между полученными отчетами?

ИДЕНТИФИЦИРУЕМ СЛУЖБЫ ПОРТОВ И ПРОТОКОЛОВ

"Nmap произвел последнее сканирование, используя поиск по стандартным службам. Однако можно пойти и другим путем: сперва получить список открытых портов, а затем проверить какие службы на них работают." - сказал я.

"Погоди минутку" - настоял Эйдан. "Разве порты для служб не всегда одни и те же?"

"Да, в теории это так. Однако в реальности, номера портов это что-то на подобии джентльменского соглашения. Я могу заставить службу работать и на другом порту, если захочу."

"Хорошо, и как это сделать?"

"Начни с просмотра своего домашнего компьютера. Зайди в командную строку и запусти команду **netstat** используя параметр **-a**, чтобы получить список всех портов. Вот так." - показал ему я.

```
netstat -a
```

Юный хакер последовал моему примеру и запустил утилиту - "Ого! И все они открыты?"

Я посмотрел на монитор - "Имя твоего компьютера Quasimodo?"

```
Active Connections
Proto  Local Address                  Foreign Address        State
TCP    Quasimodo:microsoft-ds         Quasimodo:0            LISTENING
TCP    Quasimodo:1025                 Quasimodo:0            LISTENING
TCP    Quasimodo:1030                 Quasimodo:0            LISTENING
TCP    Quasimodo:5000                 Quasimodo:0            LISTENING
TCP    Quasimodo:netbios-ssn          Quasimodo:0            LISTENING
TCP    Quasimodo:1110                 216.239.57.147:http    TIME_WAIT
UDP    Quasimodo:microsoft-ds         *:*
UDP    Quasimodo:isakmp               *:*
UDP    Quasimodo:1027                 *:*
UDP    Quasimodo:1034                 *:*
UDP    Quasimodo:1036                 *:*
UDP    Quasimodo:ntp                  *:*
```

```
UDP    Quasimodo:netbios-ns          *:*
UDP    Quasimodo:netbios-dgm         *:*
```

"Да, Quasimodo." - усмехнулся Эйдан. "Hunchback (Горбун)."

"Хорошо, Виктор, вот что я хочу, чтобы ты сделал."

УПРАЖНЕНИЯ

5.18 Запустите утилиту netstat на локальном компьютере, используя параметр -a.

```
netstat -a
```

Какие порты открыты?

5.19 Запустите утилиту netstat на локальном компьютере, используя параметр -o.

```
netstat -o
```

Какие службы слушают открытые порты?

5.20 Запустите утилиту netstat на локальном компьютере, используя комбинацию параметров -aon.

```
netstat -aon
```

Что выводится с помощью данной комбинации?

5.21 Используя поисковик, найдите какие службы работают на данных портах. Некоторые из них Вам нужны, чтобы работать в сети. Однако разве Вы хотите, чтобы все службы, которые Вы видите, действительно были запущены?

5.22 Запустите nmap, используя параметр -sS (чтобы произвести SYN или тихое сканирование) и параметр -O (чтобы попробовать распознать тип операционной системы) и укажите IP-адрес 127.0.0.1 в качестве цели сканирования. IP-адрес 127.0.0.1 называется loopback адресом. Он всегда ведет на локальную машину.

```
nmap -sS -O 127.0.0.1
```

Какие отрытые порты нашел nmap? Какие службы и программы используют найденные порты?

Теперь попробуйте запустить nmap, пока у Вас работает веб-браузер или telnet. Как это изменило результаты?

«Тихое» сканирование использует только первую часть процедуры тройного рукопожатия TCP – пакет SYN – чтобы опробовать порт, не устанавливая соединение полностью. Хотя это позволяет Вам не быть зафиксированными в системных логах (которые не записывают в лог-файл вашу попытку сканирования, если соединение не будет действительно установлено), этот метод НЕ является абсолютно безопасным. Любая система обнаружения несанкционированного проникновения (IDS/IPS) обнаружит Ваши жирные отпечатки, оставленные по всей сети, так что не тешьте себя иллюзиями того, что ваше сканирование будет действительно тихим.

5.23 Nmap имеет также дополнительные параметры. Что значат такие параметры как: -sV, -sU, -sP, -A и что они делают? Какие еще возможны параметры? Если бы Вы были атакующим и хотели бы остаться незамеченными, какие параметры Вы бы использовали, а какие нет?

5.24 Зайдите на www.foundstone.com. Затем найдите, скачайте и установите программу fport на свою Windows машину. Она похожа на утилиту netstat и показывает, какие программы в данный момент используют открытые порты и протоколы. Запустите её. Сравните её с утилитой netstat.

АНАЛИЗ ОТПЕЧАТКОВ СИСТЕМЫ

"Ты не ошибся и не поднял тревогу, не так ли?" - спросил я.

Эйдан отвечал долго, серьезно задумавшись над вопросом - "Я думаю нет. Разве это имеет значение? Я имею ввиду, что их сервера…."

Я перебил его - "Я не знаю где их сервера, мне все равно. Ты будешь работать этично, до тех пор, пока работаешь со мной."

"Хорошо" - застенчиво ответил Эйдан.

"Есть одно хорошее правило — не оставлять следов. Это практически невозможно, однако к этому всегда стоит стремиться. Следы это то, с чем ты будешь работать дальше. Их еще называют - отпечатки…."

"Эй! Это не одно и тоже!"

"Да, поймал меня. Не смотря на это следующим нашим заданием будет слепить это все в одну кучу: проанализировать отпечатки системы, обнаружить версию и тип операционной системы (ОС) и все службы, которые в ней запущены."

СКАНИРОВАНИЕ УДАЛЕННЫХ КОМПЬЮТЕРОВ

"Какую информацию ты получил при тихом сканировании?" - спросил я. Эйдан показал мне отчет, который он скопировал в текстовый документ.

```
nmap -sS -O 216.92.116.13

Starting Nmap 5.51 ( http://nmap.org ) at 2012-05-28 16:54 GTB Daylight Time
```

```
Nmap scan report for isecom.org (216.92.116.13)
Host is up (0.19s latency).
Not shown: 965 closed ports

PORT    STATE  SERVICE
21/tcp  open   ftp
22/tcp  open   ssh
25/tcp  filtered smtp
26/tcp  open   rsftp
80/tcp  open   http
110/tcp  open   pop3
111/tcp  filtered rpcbind
113/tcp  filtered auth
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  open   imap
161/tcp  filtered snmp
179/tcp  filtered bgp
306/tcp  open   unknown
443/tcp  open   https
445/tcp  filtered microsoft-ds
465/tcp  open   smtps
514/tcp  filtered shell
543/tcp  open   klogin
544/tcp  open   kshell
587/tcp  open   submission
646/tcp  filtered ldp
800/tcp  filtered mdbs_daemon
993/tcp  open   imaps
995/tcp  open   pop3s
1720/tcp filtered H.323/Q.931
2105/tcp open   eklogin
6667/tcp filtered irc
7000/tcp filtered afs3-fileserver
7001/tcp filtered afs3-callback
7007/tcp filtered afs3-bos
7777/tcp filtered cbt
9000/tcp filtered cslistener
12345/tcp filtered netbus
31337/tcp filtered Elite

Device type: general purpose|storage-misc

Running (JUST GUESSING): FreeBSD 7.X|6.X (88%)

Aggressive OS guesses: FreeBSD 7.0-BETA4 - 7.0 (88%), FreeBSD 7.0-RC1 (88%),
FreeBSD 7.0-RELEASE - 8.0-STABLE (88%), FreeBSD 7.0-STABLE (88%), FreeBSD

 7.1-RELEASE (88%), FreeBSD 6.3-RELEASE (86%), FreeNAS 0.7 (FreeBSD 7.2-RELEASE)
(85%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 8 hops
```

```
OS detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 24.09 seconds
```

"Видишь все эти значения, помеченные как **filtered**? Это означает, что они защищены брандмауэром. Они хорошо известны и уязвимы, поэтому всегда должны быть заблокированы. Однако посмотри: порты 21, 22 и 80 – это FTP, SSH (Secure Shell) и HTTP – порты этих сервисов открыты." - я посмотрел на Эйдана.

"Улов?" - спросил он с надеждой.

"Честная добыча, по крайней мере. В последнюю очередь nmap пытается определить тип операционной системы на заданном хосте. В основном, он лишь 'грубо угадывает' тип ОС, хотя, очень часто, показывает точные результаты. Так как сканирование показало, что порты для служб FTP и SSH открыты, полученные баннеры будут еще одним подтверждением правильности результатов сканирования.

Проверь в Интернет, там написано, что NcFTPd устанавливается на Unix системы, что подтверждает правильность идентификации типа операционной системы — FreeBSD – на сканируемом компьютере. SSH часто по умолчанию установлен в Unix системах. Баннеры, конечно, можно подделать, однако у нас на руках слишком много совпадений.

Теперь, в зависимости от расположения цели сканирования, возможно стоит определить ISP (Интернет сервис провайдера), услугами которого пользуется сканируемое устройство. В ISP также могут быть зарегистрированы и спаммеры и вредоносные сайты – однако ты можешь пожаловаться им и атакующее устройство отключат. В твоем случае, я не думаю, что тебе придется иметь дело с ISP...."

"Потому что сканируемый компьютер находится в.." - выпалил Эйдан, однако я поднял указательный палец вверх.

"Стоп. Твоя информация это твоя информация. Мне она ни к чему. Ты ведь этичный и безопасный хакер."

Эйдан кивнул.

"Итак, что ты собираешься делать?" - спросил я его.

"Ладно, у них запущен веб-сервер, верно?" - начал Эайдан, а мне ничего не осталось, кроме как улыбнуться.

ПИЩА ДЛЯ УМА: УГЛУБЛЯЕМСЯ В NMAP

Предположим, что Вы идентифицировали имя хоста, владельца, сеть и убедились, что хост подключен к сети. Теперь необходимо найти открытые порты. Не забывает, что, даже если хост активен, порты на нем могут быть закрыты (либо находится в состоянии отфильтрованных).

Вы можете использовать известный сетевой сканер **nmap** от Fyodor для выполнения этой задачи. Nmap позволяет удаленно тестировать компьютеры на наличие открытых портов и связанных с ними сетевых служб. По завершению сканирования nmap, в зависимости от типа командной строки, которую Вы используете, предоставит Вам список открытых портов и служб или протоколов, которые работают на найденных портах. Nmap может также определить операционную систему Вашего компьютера.

Nmap имеет множество опций и типов сканирования. Мы будем использовать несколько опций nmap. Также Вы всегда можете воспользоваться командой

```
nmap --help
```

для получения детальной справки.

Сперва сканирование. Вы уже прочли урок №3? Нет? Вернитесь и перечитайте! Можете объяснить разницу между TCP и UDP, описать процесс тройного рукопожатия? Эти знания нужны, чтобы понимать как работает nmap.

Синтаксис Nmap :

`nmap` техника_сканирования обанаружение_хоста опции цель

- техника_сканирования указывает, какие части пакетов будут использованы и как ответы от цели должны быть интерпритированы. Мы также проанализируем два базовых типа сканирования:
  - **-sS** SYN скансирование (да, только первая часть тройного рукопожатия)
  - **-sT** TCP с полным установлением соединения (полное тройное рукопожатие)
  - **-sA** ACK сканирование (отправка только ACK пакетов)
  - **-sU** UDP сканирование
  - **-O** обанаружение ОС
  - **-A** Выполняет все функции: обнаружение ОС, плагины, traceroute
- обанаружение_хоста указывает метод определения присутствия цели сканирования в сети. Если хост подключен к сети, он будет просканирован, в противном случае нет.
  - **-PE** проверяет, отвечает ли хост на ping
  - **-PS** проверяет, отвечает ли хост на SYN
  - **-PA** проверяет, отвечает ли хост на ACK
  - **-PU** проверяет, отвечает ли хост на UDP дейтаграммы
  - **-Pn** не проверяет, обращается ко всем хостам как к активным (мы будем использовать этот параметр, поскольку мы знаем, что наша цель сканирования находится в сети).

- Опции указывает некоторые детали для выбранного типа сканирования, в частности
  - **-p0-65535** диапазон портов, которые следует сканировать (в этом примере от 0 до 65535).
  - **--top-ports number** nmap сканирует лишь часто используемые общеизвестные порты (до 1024)
  - **-T0, -T1, -T2, -T3, -T4** для определения скорости сканирования, 0 - медленное и 4 - быстрое сканирование (маленькая скорость сканирования повышает скрытность и уменьшает перегрузки в сети)
  - **-oA** имя_файла для создания отчета во всех трех формата, поддерживаемых nmap (мы всегда будем использовать отчеты для отслеживания нашей активности после сканирования)
  - **--reason** nmap описывает интерпретацию результатов (всегда будем использовать)
  - **--packet-trace** тоже, что и --reason, плюс Вы увидите tracert для трафика (всегда используйте, чтобы узнать больше про метод сканирования и для корректировки полученных результатов)
  - **-n** не разрешает распознание имени хоста через dns (эту опцию мы не будем использовать, потому что мы уже вручную узнали dns-имя)

TCP Сканирование

Наше первое сканирование будет выглядеть так

```
# nmap -sT -Pn -n --top-ports 10 -oA hhs_5_tcp hackerhighschool.org

Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 04:10 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up (0.23s latency).
PORT    STATE  SERVICE
21/tcp  open   ftp
22/tcp  open   ssh
23/tcp  closed telnet
25/tcp  filtered smtp
80/tcp  open   http
110/tcp open   pop3
139/tcp closed  netbios-ssn
443/tcp open   https
445/tcp closed  microsoft-ds
3389/tcp closed  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.04 seconds
```

Мы нашли некоторые открытые порты, несколько закрытых портов и один фильтрованный. Что это значит? Значение зависит от типа сканирования (в данном случае мы использовали -sT). Мы можем использовать столбец Reason, чтобы увидеть, почему nmap обнаруживает частичное Состояние.

```
# nmap -sT -Pn -n --top-ports 10 --reason -oA hhs_5_tcp_02
hackerhighschool.org

Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 04:17 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.22s latency).
PORT    STATE  SERVICE     REASON
21/tcp  open   ftp         syn-ack
22/tcp  open   ssh         syn-ack
23/tcp  closed telnet      conn-refused
25/tcp  filtered smtp      no-response
80/tcp  open   http        syn-ack
110/tcp open   pop3        syn-ack
139/tcp closed netbios-ssn conn-refused
443/tcp open   https       syn-ack
445/tcp closed microsoft-ds conn-refused
3389/tcp closed ms-wbt-server conn-refused

Nmap done: 1 IP address (1 host up) scanned in 2.26 seconds
```

Теперь мы знаем причины идентификации определенного состояния порта и мы знаем, как nmap "сопоставлял" получаемые ответы с состояниями **TCP** Сканирования:

- **open**: цель ответила SYN ACK пакетом
- **closed**: TCP соединение прервано
- **filtered**: нет ответа от цели

Для других методов сканирования и, в частности, если Вы нашли порты с состоянием *open | filtered,* Вам следует копнуть глубже, чтобы узнать точную причину.

SYN Сканирование

Другой известный метод сканирования - **SYN** сканирование. Это тип сканирования nmap отправляет только SYN пакеты без завершения тройного рукопожатия. Также его называют "полуоткрытое" или "скрытое" сканирование, поскольку отсутствует полное TCP соединение. Для данного типа сканирования используется опция **-sS**.

```
# nmap -sS -Pn -n --top-ports 10 --reason -oA hhs_5_syn hackerhighschool.org

Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-24 12:58 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.15s latency).
PORT    STATE  SERVICE     REASON
21/tcp  open   ftp         syn-ack
22/tcp  open   ssh         syn-ack
23/tcp  closed telnet      reset
25/tcp  filtered smtp      no-response
```

```
80/tcp  open   http     syn-ack
110/tcp open   pop3     syn-ack
139/tcp filtered netbios-ssn  no-response
443/tcp open   https     syn-ack
445/tcp filtered microsoft-ds no-response
3389/tcp closed  ms-wbt-server reset

Nmap done: 1 IP address (1 host up) scanned in 1.81 seconds
```

Мы снова получили отчет о причинах и методах "сопоставления" получаемых ответов с состоянием для **SYN** сканирования:

- **open**: цель ответила SYN ACK пакетом)
- **closed**: цель ответила пакетом, содержащим RST флаг
- **filtered**: цель не ответила

Результаты похожи на результаты при TCP сканировании, однако будьте внимательны и учитывайте различия между "полным" TCP сканированием и "полуоткрытым" SYN сканированием. Отличия возникают в случае защиты цели сканирования брандмауэром с простой фильтрацией или фильтрацией с учётом состояния потока. Чтобы найти отличия, сравните результаты [с использованием опций --reason и --packet-trace] используя ту же цель сканирования и разные методы сканирования [-sT, -sS, -sA].

UDP сканирование

Еще один метод сканирования это UDP сканирование (-sU): знание причины - основа получения хорошего результата.

```
# nmap -sU -Pn -n --top-ports 10 --reason -oA hhs_5_udp hackerhighschool.org

Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 04:28 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.23s latency).
PORT    STATE         SERVICE    REASON
53/udp  closed        domain     port-unreach
67/udp  open|filtered dhcps      no-response
123/udp closed        ntp        port-unreach
135/udp closed        msrpc      port-unreach
137/udp closed        netbios-ns  port-unreach
138/udp closed        netbios-dgm port-unreach
161/udp closed        snmp       port-unreach
445/udp closed        microsoft-ds port-unreach
631/udp closed        ipp        port-unreach
1434/udp closed       ms-sql-m   port-unreach

Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
```

Это может немного сбивать с толку. Что же произошло? Мы видим некоторые нестандатные причины, такие как: port-unreach (closed) и no-response (open | filtered). Почему? Нам нужно больше деталей. Мы можем использовать опцию --packet-trace и

ограничить сканирование лишь двумя портами, в нашем случае на интересуют UDP -порты 53 и 67:

```
# nmap -sU -Pn -n -p53,67 --reason --packet-trace -oA hhs_5_udp_02
hackerhighschool.org

Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 04:32 CEST
SENT (0.0508s) UDP 192.168.100.53:54940 > 216.92.116.13:67 ttl=46 id=54177
iplen=28
SENT (0.0509s) UDP 192.168.100.53:54940 > 216.92.116.13:53 ttl=37 id=17751
iplen=40
RCVD (0.3583s) ICMP 216.92.116.13 > 192.168.100.53 Port unreachable
(type=3/code=3) ttl=54 id=1724 iplen=56
SENT (2.5989s) UDP 192.168.100.53:54941 > 216.92.116.13:67 ttl=49 id=33695
iplen=28
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.31s latency).
PORT STATE SERVICE REASON
53/udp closed domain port-unreach
67/udp open|filtered dhcps no-response

Nmap done: 1 IP address (1 host up) scanned in 4.15 seconds
```

Мы видим IP-адрес 192.168.100.53, с которого проводится сканирование UDP-портов 53 и 67 на сайте hackerhighschool.org. Порт 67 не отвечает, а для порта 53 мы получили причину The Port Unreachable (T03C03).

Port Unreachable значит, что порт закрыт и не отвечает – даже если это обычный ответ для UDP – мы не знаем, активна ли служба на этом порту или нет, поскольку UDP протокол может отвечать только если получает необходимые для него пакеты. Можно ли узнать больше? Да, используя метод сканирования -sV (Служебное Сканирование, англ. «Service Scan»), при котором nmap пытается отправить стандартные общеизвестные пакеты для UDP служб.

Служебное Сканирование **(Service Scan) (UDP)**

```
# nmap -sUV -Pn -n -p53,67 --reason --packet-trace -oA hhs_5_udp_03
hackerhighschool.org

Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 04:44 CEST
SENT (0.1730s) UDP 192.168.100.53:62664 > 216.92.116.13:53 ttl=48 id=23048
iplen=40
SENT (0.1731s) UDP 192.168.100.53:62664 > 216.92.116.13:67 ttl=48 id=53183
iplen=28
RCVD (0.4227s) ICMP 216.92.116.13 > 192.168.100.53 Port unreachable
(type=3/code=3) ttl=54 id=20172 iplen=56
SENT (2.4252s) UDP 192.168.100.53:62665 > 216.92.116.13:67 ttl=50 id=39909
iplen=28
NSOCK (3.8460s) UDP connection requested to 216.92.116.13:67 (IOD #1) EID 8
NSOCK (3.8460s) Callback: CONNECT SUCCESS for EID 8 [216.92.116.13:67]
Service scan sending probe RPCCheck to 216.92.116.13:67 (udp)
```

```
...and more 80 packets...
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.25s latency).
PORT  STATE     SERVICE REASON    VERSION
53/udp closed    domain port-unreach
67/udp open|filtered dhcps  no-response
```

В этот раз нам не повезло, мы получили те же результаты. Однако nmap,в процессе последнего сканирования отправил множество пакетов. Хороший хакер может также попробовать использовать сканирование при помощи специфических UDP пакетов вручную. Хорошенько изучите общеизвестные службы на вашем компьютере и сделайте несколько упражнений, а затем продолжайте анализировать баннеры.

УПРАЖНЕНИЯ

5.25 Перейдите на http://insecure.org/, скачайте и установите последнюю версию nmap для Вашей ОС.
5.26 Повторите все сканирования в этой секции урока, используя больше портов. Имейте ввиду, что в некоторых случаях необходимо использование команды sudo (Linux) для запуска nmap от имени администратора (root).
5.27 Создайте таблицу с описание всех методов сканирования, отображающих состояние, причинами и реальными ответами от цели сканирования (packet-trace).

Обнаружение ОС

Определение известных служб — очень важный шаг для получения данных о цели сканирования. Nmap снова может прийти на помощь. Вы можете получить значительно больше информации используя такие опции как *-A* для полнофункционального сканирования и *-O* лишь для обнаружения ОС, используя порты по-умолчанию:

```
# sudo nmap -A -Pn -n --reason -oA hhs_5_all hackerhighschool.org

Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 05:38 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.21s latency).
Not shown: 971 closed ports
Reason: 971 resets
PORT    STATE  SERVICE     REASON   VERSION
21/tcp  open   ftp         syn-ack  NcFTPd
22/tcp  open   ssh         syn-ack  OpenSSH 5.9 (protocol 2.0)
| ssh-hostkey: 1024 cd:27:c2:bf:ad:35:e5:67:e0:1b:cf:ef:ac:2b:18:9a (DSA)
|_1024 17:83:c5:8a:7a:ac:6c:90:48:04:0b:e5:9c:e5:4d:ab (RSA)
25/tcp  filtered smtp      no-response
26/tcp  open   tcpwrapped  syn-ack
80/tcp  open   http        syn-ack  Apache httpd 2.2.22
|_http-title: Hacker High School - Security Awareness for Teens
110/tcp  open   pop3       syn-ack  Dovecot pop3d
|_pop3-capabilities: USER CAPA UIDL TOP OK(K) RESP-CODES PIPELINING STLS
SASL(PLAIN LOGIN)
```

```
111/tcp  filtered rpcbind     no-response
113/tcp  open    tcpwrapped   syn-ack
143/tcp  open    imap         syn-ack    Dovecot imapd
|_imap-capabilities: LOGIN-REFERRALS QUOTA AUTH=PLAIN LIST-STATUS CHILDREN
CONTEXT=SEARCH THREAD=REFERENCES UIDPLUS SORT IDLE MULTIAPPEND CONDSTORE
ESEARCH Capability UNSELECT AUTH=LOGINA0001 IMAP4rev1 ID WITHIN QRESYNC LIST-
EXTENDED SORT=DISPLAY THREAD=REFS STARTTLS OK completed SEARCHRES ENABLE
I18NLEVEL=1 LITERAL+ ESORT SASL-IR NAMESPACE
161/tcp  filtered snmp       no-response
179/tcp  filtered bgp        no-response
306/tcp  open    tcpwrapped   syn-ack
443/tcp  open    ssl/http     syn-ack    Apache httpd 2.2.22
| ssl-cert: Subject: commonName=www.isecom.org/organizationName=ISECOM - The
Institute for Security and Open Methodologies/stateOrProvinceName=New
York/countryName=US
| Not valid before: 2010-12-11 00:00:00
|_Not valid after: 2013-12-10 23:59:59
|_http-title: Site doesn't have a title (text/html).
|_sslv2: server supports SSLv2 protocol, but no SSLv2 cyphers
465/tcp  open    ssl/smtp     syn-ack    Postfix smtpd
|_smtp-commands: kunatri.pair.com, PIPELINING, SIZE 41943040, ETRN, AUTH
PLAIN LOGIN, AUTH=PLAIN LOGIN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=*.pair.com/organizationName=pair Networks,
Inc./stateOrProvinceName=Pennsylvania/countryName=US
| Not valid before: 2012-01-10 00:00:00
|_Not valid after: 2015-01-09 23:59:59
543/tcp  open    tcpwrapped   syn-ack
544/tcp  open    tcpwrapped   syn-ack
587/tcp  open    smtp         syn-ack    Postfix smtpd
|_smtp-commands: kunatri.pair.com, PIPELINING, SIZE 41943040, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=*.pair.com/organizationName=pair Networks,
Inc./stateOrProvinceName=Pennsylvania/countryName=US
| Not valid before: 2012-01-10 00:00:00
|_Not valid after: 2015-01-09 23:59:59
646/tcp  filtered ldp        no-response
800/tcp  filtered mdbs_daemon   no-response
993/tcp  open    ssl/imap     syn-ack    Dovecot imapd
| ssl-cert: Subject: commonName=*.pair.com/organizationName=pair Networks,
Inc./stateOrProvinceName=Pennsylvania/countryName=US
| Not valid before: 2012-01-10 00:00:00
|_Not valid after: 2015-01-09 23:59:59
|_sslv2: server supports SSLv2 protocol, but no SSLv2 cyphers
|_imap-capabilities: LOGIN-REFERRALS completed OK SORT=DISPLAY Capability
UNSELECT AUTH=PLAIN AUTH=LOGINA0001 IMAP4rev1 QUOTA CONDSTORE LIST-STATUS ID
SEARCHRES WITHIN CHILDREN LIST-EXTENDED ESORT ESEARCH QRESYNC CONTEXT=SEARCH
THREAD=REFS THREAD=REFERENCES I18NLEVEL=1 UIDPLUS NAMESPACE ENABLE SORT
LITERAL+ IDLE SASL-IR MULTIAPPEND
995/tcp  open    ssl/pop3     syn-ack    Dovecot pop3d
|_sslv2: server supports SSLv2 protocol, but no SSLv2 cyphers
|_pop3-capabilities: OK(K) CAPA RESP-CODES UIDL PIPELINING USER TOP
```

```
SASL(PLAIN LOGIN)
| ssl-cert: Subject: commonName=*.pair.com/organizationName=pair Networks,
Inc./stateOrProvinceName=Pennsylvania/countryName=US
| Not valid before: 2012-01-10 00:00:00
|_Not valid after: 2015-01-09 23:59:59
2105/tcp open   tcpwrapped   syn-ack
6667/tcp filtered irc       no-response
7000/tcp filtered afs3-fileserver no-response
7001/tcp filtered afs3-callback  no-response
7007/tcp filtered afs3-bos    no-response
7777/tcp filtered cbt       no-response
9000/tcp filtered cslistener   no-response
31337/tcp filtered Elite      no-response
Device type: general purpose|firewall|specialized|router
Running (JUST GUESSING): FreeBSD 6.X|7.X|8.X (98%), m0n0wall FreeBSD 6.X
(91%), OpenBSD 4.X (91%), VMware ESX Server 4.X (90%), AVtech embedded (89%),
Juniper JUNOS 9.X (89%)
OS       CPE:       cpe:/o:freebsd:freebsd:6.3       cpe:/o:freebsd:freebsd:7.0
cpe:/o:freebsd:freebsd:8.1 cpe:/o:m0n0wall:freebsd cpe:/o:openbsd:openbsd:4.0
cpe:/o:vmware:esxi:4.1 cpe:/o:m0n0wall:freebsd:6 cpe:/o:juniper:junos:9
Aggressive OS guesses: FreeBSD 6.3-RELEASE (98%), FreeBSD 7.0-RELEASE (95%),
FreeBSD 8.1-RELEASE (94%), FreeBSD 7.1-PRERELEASE 7.2-STABLE (94%), FreeBSD
7.0-RELEASE - 8.0-STABLE (92%), FreeBSD 7.1-RELEASE (92%), FreeBSD 7.2-
RELEASE - 8.0-RELEASE (91%), FreeBSD 7.0-RC1 (91%), FreeBSD 7.0-STABLE (91%),
m0n0wall 1.3b11 - 1.3b15 FreeBSD-based firewall (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 12 hops
Service Info: Host: kunatri.pair.com; OS: Unix

TRACEROUTE (using port 1723/tcp)
HOP RTT    ADDRESS
[...]
8  94.98 ms 89.221.34.153
9  93.70 ms 89.221.34.110
10 211.60 ms 64.210.21.150
11 ...
12 209.28 ms 216.92.116.13

OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 57.94 seconds
```

При использовании параметра -A специализированные плагины помогают получить больше информации о цели сканирования, "угадывают" ОС и проводят трассировку маршрута, используя методики, отличные от tracert и traceroute. Чем больше найдено открытых портов, тем больше вероятность верно определить ОС.

УПРАЖНЕНИЯ

5.28 Просканируйте свой компьютер. Насколько верно nmap угадал ОС?

5.29 Используйте опцию traceroute в nmap с различными портами.

nmap -n -Pn --traceroute –-version-trace -p80 hackerhighschool.org

5.30 Есть ли какие-то отличия в результатах, полученных при использовании traceroute в nmap с различными портами и результатами утилит tracert/traceroute на Вашей операционной системе?

Использование скриптов

Nmap также имеет множество полезных скриптов для сканирования. Чтобы использовать скрипт при сканировании введите параметр:

--script script-name

Один из них - скрипт `ipidseq`. Также известный как Incremental IP fingerpriting. Этот скрипт может быть использован для нахождения хостов, которые могут быть использованы для метода холостого сканирования (Idle Scan) (-sI). Этот тип сканирования использует проблемную реализацию IP протокола для того, чтобы зомбировать жертву и сканировать другие хосты с ее IP-адреса.

```
# nmap --script ipidseq -oA hhs_5_ipidseq hackerhighschool.org

Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 05:47 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up (0.23s latency).
rDNS record for 216.92.116.13: isecom.org
Not shown: 971 closed ports
```

УПРАЖНЕНИЯ

5.32 Исследуйте технику холостого сканирования. Что это за техника и как Вы можете ее использовать?

ЗАКЛЮЧЕНИЕ

Знание того, где и что искать, всего лишь часть битвы за безопасность. Компьютерные сети постоянно исследуют, анализируют, проверяют на прочность. Если за сетью, которую Вы защищаете, не следят, значит Вы используете неправильные утилиты, чтобы определить поведение. Как специалист в области компьютерной безопасности, Вы должны знать каждый дюйм системы, которую Вы защищаете. Вы также должны знать, слабые и сильные стороны сети.

В наши дни уже не достаточно просто собирать данные о серверах, такие как операционная система и открытые порты. Постоянно возникающие новые угрозы стараются узнать больше о Вашей сети настолько, насколько это возможно. Эта информация может включать в себя:

- Марку брандмауэра, модель, версию прошивки и установленные патчи;
- Удаленные соединения аутентификации и права доступа;
- Другие серверы, которые подключены к сети. К примеру, серверы: электронной почты, HTML, резервное копирование, системы резервирования, взятые напрокат или сервера аутсорсинговых услуг, и даже подрядчиков, которые, возможно, использовали сеть или используют ее сейчас;
- Принтеры, факсы, сканеры, беспроводные маршрутизаторы и сетевые соединения в Вашей компании;
- Переносные устройства, такие как: планшеты, смартфоны, цифровые камеры и все то, что подключено к сети.

Хотя мы рассмотрели много тем в этом уроке, системы идентификации охватывают намного большую область. Существует довольно много информации, которая проходит через сети, которые идентифицируют части каждого устройства. Каждое устройство в сети может быть использовано в качестве отправной точки для атаки. Подход к решению этой сложной проблемы требует большего, чем просто использование программного обеспечения. Исследуйте собственное оборудования и изучите так много, насколько это возможно. Эти знания окупятся.

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM