Hacker Highschool

SECURITY AWARENESS FOR TEENS



УРОК 5
ІДЕНТИФІКАЦІЯ СИСТЕМИ

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

WWW.ISECOM.ORG - WWW.OSSTMM.ORG - WWW.HACKERHIGHSCHOOL.ORG - WWW.BADPEOPLEPROJECT.ORG - WWW.OSSTMMTRAINING.ORG

УВАГА

Проект Hacker Highschool є засобом навчання і, як в будь-якому навчальному засобі, існує небезпека. Деякі уроки, якщо ними зловживати, можуть призвести до фізичної травми. Також додаткові небезпеки можуть бути там, де ще недостатньо досліджень про можливі наслідки випромінювань від специфічної техніки. Студенти, які використовують ці уроки, повинні перебувати під контролем, і, в той же час, заохочуватися на вивчення, практику і заняття. ISECOM не несе відповідальності за застосування інформації, отриманої з даних матеріалів, і за подальші наслідки.

Наступні уроки та книги є відкритими і загальнодоступними на наступних умовах ISECOM:

Всі роботи проекту Hacker Highschool призначені для некомерційного використання з учнями початкової школи, слухачами юнацьких курсів Highschool, і студентами вищих навчальних закладів, приватних організацій або частково для домашнього навчання. Ці матеріали в будь-якій формі не можуть бути використані для продажу. Надання цих матеріалів будь-якому класу, навчальній організації або табору, в яких стягується плата, категорично заборонено без ліцензії, в тому числі на уроки в коледжі, університеті, професійно-технічних заняттях, літніх або комп'ютерних таборах тощо.

Для придбання ліцензії відвідайте розділ сайту призначений для Ліцензування: http://www.hackerhighschool.org/licensing.html.

Проект HHS є результатом праці відкритого співтовариства і, якщо Ви знаходите наші труди цінними і корисними, ми просимо Вас підтримати нас шляхом придбання ліцензії, пожертвувань, або спонсорства.

ЗМІСТ

СПІВРОБІТНИКИ ЖУРНАЛУ

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

Перекладачі

Vadim Chakryan, Kharkiv National University of Radio Electronics

Andrii Sezko, Kharkiv National University of Radio Electronics

ISECOM

ВСТУП

«Здається, в моєму ноутбуці з'явився вірус», — сказав мені один із моїх студентів. — «Можете його подивитися?»

Я взяв його ноутбук і не відкриваючи, пильно роздивився з усіх сторін. «По моєму, схоже на комп'ютер», — сказав я, передаючи його назад власнику.

«Але що з ним не так», — наполягав Ейден. «Я був у гостях у мого друга, зайшов в Інтернет, а потім щось потрапило в мій електронний лист і відправило якісь повідомлення всім моїм друзям».

«Гаразд. Як ти прочитав свій лист? Ти встановлював якусь програму?» — запитав я.

«Ні, я прочитав через веб, тобто через Інтернет».

«Ти маєш на увазі веб-браузер? У такому випадку, цей лист доступний тільки онлайн, а не на твоєму комп'ютері. Я почав би з твоєї поштової скриньки. Ти змінив пароль?»

«Так, звичайно. Мій акаунт було заблоковано, доки я не змінив пароль.» Він відводив погляд, наче не все мені розповів, але я не наполягав. Я був впевнений, що його і так достатньо лаяли через цей випадок.

Замість цього я запитав: «Твої друзі після цього отримували ще якісь повідомлення ?»

«Ні». Він пильно ховав погляд від мене.

«Ти обрав надійний пароль? Не 12345?»

Тепер він посміхається. «Він дійсно складний. Ніхто і ніколи не зможе його підібрати».

У мене були сумніви з цього приводу, але я погодився. «Добре, тоді схоже, що ти вже вирішив цю проблему».

«Ні», — наполягав він. — «Навіщо комусь таке робити?»

Нарешті він цим зацікавився. «Чому б тобі самому про це не дізнатися? У тебе збереглося хоч одне з повідомлень, які отримали твої друзі?»

«Так, всі. Друзі відправили їх мені назад. » Ось воно що. Я був упевнений, що список його контактів нараховував десятки, а може й сотні записів. Справа має бути цікавою.

«Гадаю, тобі потрібно з'ясувати, куди саме веде посилання у листі.»

Йому сподобалась ця ідея. «Ви хочете сказати, що ми можемо це зробити?»

«Ха», — засміявся я. — «Я хочу сказати, що ТИ можеш це зробити. Але я можу розповісти, що для цього потрібно.»

Ейден задумався. «Це як в тій історії про вівцю та вовка?»

«Саме так. Ти можеш бути як вівцею, так і вовком. Обирай», — сказав я йому.

Його дитяча наївність зникла вмить. «Хочу бути вовком», — вирішив він.

* * *

Ідентифікація системи, безперечно, може виявитися найбільш важливим кроком будь-якої комп'ютерної атаки або захисту. Подальший перебіг подій залежить від даних, які Ви зберете на цьому етапі. Яка операційна система встановлена на пристрої, який проводить атаку або на яке проводиться атака? Чи можете Ви, або хтось інший, переглянути які застосунки або служби запущені? Стосовно деталей облікового запису адміністратора: можливо ця

інформація лежить десь на видному місці? Це питання , які потрібно задати на даному етапі . Залежно від того, по який бік атаки Ви знаходитесь, Ви можете зрадіти або злякатися від того, яку інформацію Ви можете з легкістю отримати, якщо знаєте, де шукати.

Знати, як організувати атаку — це, звичайно, круто. Але набагато крутіше знати, як захиститися від такої атаки. Ми постараємося глибше розібратися в цій темі і вивчимо, як можна ідентифікувати систему і знайти її слабкі місця — будь це ваша система або когось іншого.

Ми будемо використовувати утиліти, які знаходяться у вільному доступі, а також покажемо, як ними користуватися. Практично безглуздо просто показати програму, не навчивши при цьому, як нею користуватися. Як і будь-які інші програми забезпечення безпеки, їх можна використовувати з добрими або злими намірами. В уроці будуть показані обидва підходи до їх використання, так що Ви зможете спробувати себе як у ролі організатора атаки, так і в ролі захисника від таких атак.

У цьому уроці Ви познайомитеся з двома персонажами: один з них буде вчити, інший - вчитися. Учитель не завжди знає відповідь, так що ви, як читач, теж не отримаєте всю інформацію на тарілочці. Вчіться зламувати і вчіться відновлювати те, що зламали.

Будьте особливо уважні до атрибутів, які використовуються в різних програмах. Невелика зміна (наприклад, введення літери в нижньому регістрі замість верхнього) може призвести до абсолютно інших результатів, тим більше в різних операційних системах.

У перших трьох уроках розглядаються основи роботи в мережі і основи того, як працює Інтернет. Кожен урок ґрунтується на знаннях, отриманих у попередніх параграфах і уроках, так що не поспішайте пропускати сторінки. Легко пропускати параграфи або сторінки, але при цьому можна проґавити розгляд дуже важливих питань.

ІДЕНТИФІКАЦІЯ СЕРВЕРА

«Добре, Ейден, що тобі вдалося дізнатися?» Я сподівався, що він не перейшов по тому посиланню в листі, який було відправлено з його зламаного аккаунту.

«Я не клацав по ньому», — відповів мені Ейден, усміхнувшись, наче прочитав мої думки. «Я скопіював її і вставив у текстовий файл.»

«Ти скопіював текст який відображувався? Чи фактичне посилання?»

Він нахмурився. «Я не дурень. Я натиснув праву кнопку мишки і обрав 'Скопіювати адресу посилання '. Після чого вставив у документ. Ось, дивіться, link.txt.»

«Вибач, я просто хотів упевнитись. Добре, куди веде це посилання? »

«Там якась маячня. Домен Chewmoogoo.com чи щось на нього схоже. І далі якийсь набір букв», — відповів він, відкриваючи свій ноутбук і показуючи посилання.

«Так, точно», — сказав я йому. — «Тепер ми їх точно спіймали. Давай подивимось, яку інформацію ми зможемо отримати. Для цього потрібні спеціальні утиліти. Спочатку поговоримо про доменні імена та IP-адреси».

ІДЕНТИФІКАЦІЯ ВЛАСНИКА ДОМЕНУ

Перший крок ідентифікації віддаленої системи — це аналіз імені хосту, а також імені і IP-адреси домену. За допомогою **whois-**пошуку за доменним ім'ям можна виявити багато корисної інформації:

- Особистість власника домену (зазвичай його повне ім'я);
- Контактна інформація: поштові адреси, номери телефонів та адреси електронної пошти;
- Сервери DNS, де зареєстрований домен, що також може вказати на Інтернет-провайдера, який обслуговує домен;
- IP-адреса сервера, ще один потенційний ключ до визначення Інтернет-провайдера;
- Інформація про доменне ім'я: дата створення, час оновлення інформації, дата закінчення терміну реєстрації;

Слід враховувати, що існує цілий ряд різних реєстраторів доменних імен, і не всі бази даних whois містять інформацію про всі домени. Можливо, Вам доведеться скористатися декількома базами даних whois для того, щоб знайти інформацію про досліджуваний домен.

Ейден миттєво засвоїв нову інформацію. «Добре, що мені робити тепер?»

«Ось твоє завдання», — сказав я йому.

ВПРАВИ

5.1 Використовуючи доменне ім'я, про яке Ви збираєте відомості (якщо Ви не Ейден, використовуйте isecom.org), виконайте наступну команду в Linux, Windows і OSX.

```
whois isecom.org
```

Хто є власником домену? Коли він був створений? Коли закінчується термін його реєстрації? (Чи дають ці відомості можливість для якихось дій?)

Коли він востаннє оновлювався?

Чиї контакти вказані?
Які у цього домену первинний і вторинний сервери доменних імен?

5.2 Тепер виконайте аналогічний пошук в браузері

(наприклад, http://www.whois.net -> "sample.com"). Важливим питанням є наступне: чи відповідають ці дані тим даним, які були отримані в результаті виконання команди whois?

5.3 Подивіться хоча б два веб-сайти whois (спробуйте http://whois.domaintools.com; зможете знайти інші сайти?).

ІДЕНТИФІКАЦІЯ **IP-**АДРЕСИ ДОМЕНУ

«Отже, що у тебе вийшло?» — Поцікавився я у Ейдена.

«Ось всі дані. Я додав їх у файл». — Він показав текстовий файл.

«Добре, зберігай будь-яку, навіть незначну інформацію. Яка IP-адреса у домену? »

«Схоже, що ось ця», — Ейден вказав на число з великою кількістю цифр.

«Так, ти правий. Ти можеш визначити IP-адресу домену за допомогою команди whois або переглянути DNS-записи за допомогою команди ping:

```
ping isecom.org
```

«У першому рядку результату виведеться IP-адреса домену».

> Якщо Ви зможете перехопити або просто отримати електронний лист від цілі, проаналізуйте заголовки листа (див. Урок 9, Безпека електронної пошти); там вказується IP-адреса пристрою відправника. Ви також можете використовувати пошукові системи (Урок 20, Соціальна інженерія) або утиліти (Maltego, FOCA). Пошукайте назву організації, контактну інформацію власника домену, номери телефонів та адреси. Будь-які подібні відомості можуть призвести до ще більш суттєвої інформації.

«Як тільки ти визначив один або кілька IP-адрес, тобі потрібно визначити їх місцезнаходження. Групи IP-адрес призначаються Інтернет-провайдерам по всьому світу. З'ясуй, до якої групи належать ті IP-адреси, які ти визначив (і хто має права на цю групу, якщо зможеш це з'ясувати). Це може допомогти тобі дізнатися, який сервер або Інтернет-провайдер використовує веб-сайт. Справжньою цінністю для тебе буде знайти, в якій країні розташований цей сервер», - сказав я Ейдену. «Можу посперечатися, що не в цій. Ось що тобі потрібно зробити далі. »

ВПРАВИ

5.4 Тепер ми безпосередньо розглянемо DNS-записи. Ще одним способом отримання інформації про домен і сервер (або сервери) є використання інформації в DNS. Почнемо з трьох основних команд.

5.5 Відкрийте вікно терміналу. Виконайте наступну команду:

```
dig isecom.org
```

5.6 Чи працює ця команда на вашій ОС? Спробуйте виконати її в Windows, Linux і OSX.

5.7 Тепер виконайте наступну команду:

```
host isecom.org
```

5.8 Чи працює ця команда на вашій ОС? Спробуйте виконати її в Windows, Linux і OSX.

5.9 Нарешті, виконайте наступну команду:

```
nslookup isecom.org
```

5.10 Чи працює ця команда на вашій ОС? Спробуйте виконати її в Windows, Linux і OSX.

5.11 Який DNS-сервер у досліджуваного об'єкта? Чи є у організації сервер електронної пошти? У цього сервера та ж IP-адреса, що і у веб-сервера? Які припущення можна зробити, ґрунтуючись на цих відомостях? Яку ще інформацію Ви можете отримати з отриманих результатів?

5.12 Якщо вам відома IP-адреса Ви можете звернутися до записів баз даних членів Організації ресурсів нумерації **(the Number Resource Organization)** (http://www.arin.net/, http://www.ripe.net/ або http:// www.apnic.net/), щоб дізнатися подробиці розподілу IP-адрес.

ГРА ПОЧАЛАСЬ: РУБАЙ ТА ПАЛИ

Це був матч-реванш, як була переконана Джейс. Битва століття — ось як вона її називала. І не важливо, скільки буде потрібно поту, крові, болю, фізичної чи інтелектуальної сили, — амбіційна дівчина була готова виграти цей бій. Вона повинна була перемогти, адже іншого плану не було. Її волосся кольору шоколаду погойдувалося над очима, ніби тореадор, що дратує бика червоною накидкою. Один останній глибокий вдих, щоб заспокоїтися, — і мережевий кіллер готовий до роботи.

Її пальці легко переміщалися по клавіатурі. Вона оцінила ситуацію і зробила переоблік доступних ресурсів. У Джейс була копія Nmap, вже завантажена в комп'ютерного монстра. Ping і Traceroute вже були запущені, так що войовничий хакер був готовий до початку нападу .

Перша черга команд була миттєво введена з клавітури. Кулемет не стріляє так швидко, як

Джейс вводить команди. Ping , пішов! Traceroute , пішов! Потік даних був настільки великий, що сервери не встигали відповідати на запити. « Кровопролиття » було жахливим: біти і байти безладно перемішувалися на моніторі. Здавалося, що командний рядок направляє блискавичну атаку на потужні маршрутизатори .

Джейс керувала основною атакою, щоб отримати точку опори і зміцнитися всередині мережі. Її віртуальні розвідники інтенсивно досліджували встановлені брандмауери, сервери і маршрутизатори. Вона порівняла ці дані зі словником вразливостей (Common Vulnerabilities and Exposures, CVE) і зіставила їх з інформацією по скануванню мережі Nmap. Кожне слабке місце, кожна вразливість і експлойт були проаналізовані задля отримання тактичної переваги та оцінки розмірів збитків. Перемир'я — не варіант для Джейс. Вона перемагала.

Але це ще не кінець, говорила вона собі. Насправді, все, що вона зробила до цього моменту, — це захоплення всього лише невеликої частини ворожих ресурсів, але все ж інформація була безцінною. Джейс зі свого боку зазнала невеликі втрати. Пальці злегка боліли. На лобі був невеликий синець, через удар головою об монітор у хвилину розпачу. TTL (time to live - час відгуку від сервера) вбивав її.

Незабаром вона подолала всі перешкоди і успішно завершила перший етап своєї операції. У Джейс тепер було достатньо інформації про ворога для того, щоб приступити до другого етапу мережевої атаки. Для наступного кроку були потрібні кілька електронних листів і допомога інсайдера (людина, що працює всередині компанії), який ні про що не підозрює .

Це завжди була найстрашніша частина будь-якої битви — видобуток потенційних шпигунів. Джейс потрібні були користувачі цієї мережі, які поспівчували б її мотивам. Настав час порушувати всі хороші звички, що стосуються безпеки систем. Соціальна інженерія була зброєю масової дезорганізації в її арсеналі. Їй потрібно було правильно сформувати електронні листи з прикріпленими троянцями, щоб проникнути за внутрішні стіни мережі .

Готуючи злочинницькі листи, Джейс розуміла, що вона була на правильній стороні цього протистояння. Не важливо, чого це буде коштувати і скільки часу займе — Джейс була сповнена рішучості довідатися, який наступний секретний смак морозива розробляв місцевий молочний магазин.

Гра продовжується...

ІДЕНТИФІКАЦІЯ СЛУЖБ

«Так, ти зберіг всі зібрані дані?» Я спробував приховати усмішку, так як я знав відповідь, але мій обов'язок викладача змусив запитати про це.

Ейден тільки скоса глянув на мене: ось зануда подумав він, але вголос сказав: «Можете подивитися», - і дав мені свій ноутбук.

«Тепер їх дуже багато, чи не так?» - Я прокрутив кілька сторінок.

«Однак, мені потрібно якось трохи краще і зручніше зберігати і відстежувати інформацію», - сказав Ейден, забираючи назад комп'ютер.

«Дійсно, яка IP-адреса твоєї цілі?». На цей раз посмішку я не стримував.

«Емм... їх приблизно п'ять. Може, навіть більше. Я намагаюся з'ясувати, чому так, адже на деякі IP я можу запустити ping, а на інші - ні. »

«Молодець» - подумав я. При відомих IP-адресах для домену ти можеш починати досліджувати служби, які на них працюють. Ось де починаються веселощі.

PING І TRACEROUTE

«Ти все правильно починаєш робити. Ти повинен переконатися в тому , що за цими адресами є працюючі машини. І так, ти правий: ping - твій друг. Ти ж не забув запустити ping на доменне ім'я, IP- адреси і різні імена хосту, чи не так? »

« Які з них — імена хосту ", - запитав Ейден .

«Ті , в яких є букви і точка перед доменним ім'ям, як, наприклад, www.isecom.org » , — відповів я.

«Щось я таких не бачу. »

«Перевір результати, які тобі показала утиліта dig. Ти пробував запустити ping на www.isecom.org, ftp.isecom.org і mail.isecom.org?»

«Ні...»

«Якщо ти отримаєш відповідь, то за цією адресою є робочий хост. Ти проходиш через брандмауер. І вони пропускають ICMP. » — Я відкрив вікно консолі і ввів 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
```

«Ти можеш припустити, наскільки далеко від тебе розташований сервер, як в мережевому відношенні, так і фізично, за часом отримання відповіді. Розділи число "time" на два і ти зможеш оцінити відстань до сервера. Спробуй ще одну утиліту — traceroute. У Windows використовується команда tracert, а в Linux — traceroute. З її допомогою можна переглянути шлях пакета від твого комп'ютера до цілі крок за кроком. Наприклад, ось так», — пояснив я йому і ввів команду:

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

«Я хочу, щоб ти виконав завдання.»

ВПРАВИ

5.13 Використовуйте traceroute / tracert, щоб скомпонувати всю інформацію, яку Ви можете знайти про комп'ютери та маршрутизатори між вашим комп'ютером і ціллю.

5.14 Комп'ютери зі схожими IP-адресами зазвичай знаходяться в одній і тій же мережі. Запустіть ping на веб-сайт або IP- адресу (наприклад , виконайте команду ping www.isecom.org або ping 216.92.116.13). Якщо Ви отримаєте успішний відгук, то запустіть ping на наступну IP-адресу. Ви отримали відповідь? Повторіть ту ж команду для довколишніх адрес.

5.15 Використовуйте пошукову систему, щоб визначити, як оцінити відстань до сервера.

5.16 Пошукайте утиліту, яка допоможе визначити фізичне розташування сервера.

5.17 Спробуйте використовувати онлайн-утиліту Visual Trace Route. Існує досить багато сайтів з схожими утилітами. Вони візуалізують шлях трафіку.

Nmap

«Все вдалося? Тепер дозволь познайомити тебе з моїм маленьким другом» , — сказав я, намагаючись говорити страхітливим голосом. Ейден подивився на мене як на божевільного. Я прокашлявся і завершив речення: «Це nmap. »

«З цією утилітою можна проводити як прості запити, так і хитрі і розширені. Виконай команду nmap, а в якості її аргументів використовуй ім'я хосту або IP-адресу, і він просканує цей хост. Або використовуй кілька маршрутизаторів, щоб зробити хитрий запит. Якщо ти правильно введеш параметри та опції, то в результаті дізнаєшся операційну систему, яка встановлена на досліджуваній цілі. Ми будемо використовувати опцію ' сканувати TCP ' , тобто - 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
```

Пам'ятайте, що nmap — не єдина утиліта для проведення такого сканування. І це добре. Різні утиліти можуть дати різні результати, і, насправді, будь-яка з них може повести Вас по хибному шляху.

Ви можете задати nmap, наприклад, визначення операційної системи — але Вам не слід довіряти такій гіпотезі! Перевіряйте цей варіант за допомогою інших утиліт.

АНАЛІЗ БАНЕРІВ

Ейден був щасливий — "Погляньте, що у мене є!" У нього були текстові документи й електронні таблиці на ноутбуці, а також малюнки і кольорові роздруківки, які комусь обійшлися в копієчку.

"Чудово, тепер ти отримав кілька працюючих хостів, знаєш чиї вони і де розташовуються. Тепер ти, напевно, хочеш дізнатися більше про ці пристрої: яка операційна система на них працює? Які сервіси на них запущені? Чи не так?" — Запитав я його.

Це зробило його менш радісним — "Ну , що я можу сказати?"

"Тобі не потрібно нічого говорити. Змусь машину розповісти тобі про все: яка версія операційної системи на ній встановлена, які сервіси працюють і які патчі були застосовані. Якщо ти виступаєш в якості нападника — ця інформація значно полегшить тобі життя; все, що тобі потрібно буде зробити — це знайти відповідні експлойти під програми і служби цих машин. Якщо ти захищаєш систему, тобі варто обмежити подібного роду інформацію для нападників. Або, принаймні, видати неправдиву інформацію." — Ця розмова змусила його замислитися.

"Отже, те, чим ти будеш займатися далі називається — аналіз банерів. Це техніка інвентаризації дозволяє отримати всю інформацію про активні служби і порти на досліджуваних пристроях. Я покажу тобі кілька команд. Ти можеш використовувати telnet, ftp або netcat щоб проаналізувати банери. Банер — це текстове повідомлення, яке ти бачиш в консолі, коли підключаєшся до віддаленого пристрою. Банер показує тобі яка програма запущена на сервері на певному порті. «Коли я підключаюся до анонімного FTP серверу, я отримую банер. Перевір сам." — Я набрав команду в консолі:

```
ftp isecom.org

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

"Число 220 — це код, який оповіщає про те, що сервер готовий до використання. Як видно, на цій машині запущений ProFTPD сервер. Тепер ми дивимося в Інтернеті, на яку операційну систему можна встановити ProFTPD і який у сервера функціонал..." — я відсунувся від клавіатури. "Отже, твоє наступне завдання - використання ftp команд".

ВПРАВИ

5.18 Ви можете використовувати команду FTP, вказавши ім'я хосту або його IP-адресу, ось так:

```
ftp isecom.org
```

або

```
ftp 216.92.116.13
```

Спробуйте обидва варіанти, щоб подивитися які банери Ви отримаєте. Результати будуть виглядати приблизно так:

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

5.19 Ви можете використовувати утиліту Telnet із зазначенням імені хосту або його IP-адресою. Так само Ви можете вказати порт, до якого хочете підключитися, наприклад введіть порт 21, щоб підключитися до FTP:

```
telnet isecom.org 21
```

або

```
telnet 216.92.116.13 21
```

Знов таки, подивіться на те, що за банер Вам повертає сервер, якщо він звичайно взагалі щось повертає. Результат, також, може виглядати наступним чином, наприклад:

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

5.20 Використовуйте утиліту netcat із вказанням імені хосту або його IP адресою. Точно так, як і у випадку з використанням Telnet, Ви можете вказати порт, до якого хочете зробити підключення, наприклад введіть порт 21 щоб підключитися до FTP:

```
nc isecom.org 21
```

або

```
nc 216.92.116.13 21
```

Знову, зверніть увагу на те, який банер Вам повернув сервер.

Банери, які вводять в оману

"Ось фокус." — Сказав я Ейдену. — "Ти можеш змінити банер. Це один з методів маскування — брехати про те, хто ти є насправді. Отже, я можу змінити свій банер, наприклад, на наступні "НеТвояСправаЩоЦеЗаСервер Сервер». Звичайно, банер класний, все ж не найкращий. Наприклад, якщо я використовую Unix систему, а в банері до ftp напишу "WS_FTP Server", який працює лише під Windows системами, — це зіб'є нападника з пантелику."

"Хвилинку, як Ви змінили банер?" — Запитав він.

"Дуже радий, що ти запитав," — відповів я.

ВПРАВА

5.21 Знайди в Інтернеті інформацію про те, як змінювати банер на SMTP, FTP, SSH, HTTP і HTTPS. Хіба це складно? Іншими словами, чи варто довіряти тому, що зазначено в банері?

АВТОМАТИЗОВАНИЙ АНАЛІЗ БАННЕРІВ

"А тепер спробуй ось що. Давай повернемося до nmap і автоматизуємо процес аналізу банерів; нам потрібно буде використовувати опції (параметри) **-sTV** для збору банерів." — я набрав команду і отримав звіт:

```
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 знайшов NcFTPd, OpenSSH 5.9 (protocol 2.0) і Apache httpd 2.2.22. Ура: операційна система - Unix. Іноді аналіз банерів дає тобі можливість дізнатися версію операційної системи,

однак нам потрібно трохи більше інформації", — продовжив я. "Ось, що я пропоную тобі зробити."

ВПРАВИ

5.22 Використовуючи nmap зроби сканування обраного хосту (hackerhighschool.org, якщо Ви не Ейден).

5.23 Спробуйте зробити сканування хосту знову, використовуючи опцію **--version-intensity number** вибравши номер від 0 до 9 для отримання точних результатів. Яку різницю Ви помітили між отриманими звітами?

ІДЕНТИФІКАЦІЯ СЛУЖБИ ПОРТІВ І ПРОТОКОЛІВ

"Nmap зробив останнє сканування, використовуючи пошук по стандартним службам. Однак можна піти й іншим шляхом: спершу отримати список відкритих портів, а потім перевірити які служби на них працюють. " — Сказав я .

"Почекай хвилинку" — наполіг Ейден. " Хіба порти для служб не завжди одні й ті ж самі?"

"Так, в теорії це так. Проте в реальності, номери портів це щось на кшталт джентльменської угоди. Я можу змусити службу працювати і на іншому порті, якщо захочу. "

"Добре, і як це зробити? "

"Почни з перегляду свого домашнього комп'ютера. Зайди в командний рядок і запусти команду **netstat** використовуючи параметр **-a** , щоб отримати список всіх портів. Ось так." — показав йому я .

```
netstat -a
```

Юний хакер послідував моєму прикладу і запустив утиліту — "Ого! І всі вони відкриті? "

Я подивився на монітор — "ім'я твого комп'ютера 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        *:*
```

"Так, Quasimodo." — посміхнувся Ейдан. "Hunchback (Горбань)."

"Добре, Ейдан, ось що я хочу, щоб ти зробив."

ВПРАВИ

5.24 Запустіть утиліту netstat на локальному комп'ютері, використовуючи параметр **-a**.

```
netstat -a
```

5.25 Які порти відкриті?

5.26 Запустіть утиліту netstat на локальному комп'ютері, використовуючи параметр **-o**.

```
netstat -o
```

5.27 Які служби слухають відкриті порти?

5.28 Запустіть утиліту netstat на локальному комп'ютері, використовуючи комбінацію параметрів **-aon**.

```
netstat -aon
```

5.29 Що виводиться за допомогою даної комбінації?

5.30 Використовуючи пошук, знайдіть які служби працюють на даних портах. Деякі з них Вам потрібні, щоб працювати в мережі. Однак хіба Ви хочете, щоб всі служби, які Ви бачите, дійсно були запущені?

5.31 Запустіть nmap, використовуючи параметр -sS (щоб виконати SYN або тихе сканування) і параметр -O (щоб спробувати розпізнати тип операційної системи) і вкажіть IP-адресу 127.0.0.1 в якості мети сканування. IP-адреса 127.0.0.1 називається loopback адресою. Вона завжди веде на локальну машину.

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

5.32 Які відриті порти знайшов nmap? Які служби та програми використовують знайдені порти?

5.33 Тепер спробуйте запустити nmap, поки у Вас працює веб-браузер або telnet. Як це змінило результати?

«Тихе» сканування використовує тільки першу частину процедури потрійного рукостискання TCP - пакет SYN - щоб перевірити порт, не встановлюючи з'єднання повністю. Хоча це дозволяє Вам не бути зафіксованими в системних логах (що не записують у лог-файл вашу спробу сканування, якщо з'єднання не буде дійсно встановлено), цей метод НЕ є абсолютно безпечним. Будь-яка система виявлення несанкціонованого проникнення (IDS/IPS) виявить Ваші жирні відбитки, залишені по всій мережі, так що не тіште себе ілюзіями того, що ваше сканування буде дійсно тихим.

5.34 Nmap має також додаткові параметри. Що означають такі параметри як:

-sV,-sU,-sP,-A і що вони роблять? Які ще можливі параметри? Якби Ви були нападником і хотіли б залишитися непоміченими, які параметри Ви б використовували, а які ні?

5.35 Зайдіть на www.foundstone.com. Потім знайдіть, завантажте та встановіть програму **fport** на свою Windows машину. Вона схожа на утиліту netstat і показує, які програми в даний момент використовують відкриті порти і протоколи. Запустіть її. Порівняйте її з утилітою netstat.

АНАЛІЗ ВІДБИТКІВ СИСТЕМИ

"Ти не помилився і не підняв тривогу, чи не так ?" - Запитав я .

Ейден відповідав довго, серйозно замисливши над питанням - "Я думаю ні. Хіба це має значення? Я маю на увазі, що їх сервери..."

Я перебив його - "Я не знаю де їх сервери, мені всеодно. Ти будеш працювати етично, до тих пір, поки працюєш зі мною. "

"Добре" - соромливо відповів Ейден.

"Є одне хороше правило - не залишати слідів. Це практично неможливо, проте до цього завжди варто прагнути. Сліди це те, з чим ти будеш працювати далі. Їх ще називають — відбитки..."

"Гей! Це не одне і теж!"

"Так, зловив мене. Не дивлячись на це наступним нашим завданням буде зліпити це все в одну купу: проаналізувати відбитки системи, виявити версію і тип операційної системи (ОС) і всі служби, які в ній запущені."

СКАНУВАННЯ ВІДДАЛЕНИХ КОМП'ЮТЕРІВ

"Яку інформацію ти отримав за допомогою тихого сканування?" — запитав я. Эйден показав мені звіт, який він скопіював у текстовий 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
```

"Бачиш всі ці значення, помічені як **filtered**? Це означає, що вони захищені брандмауером. Вони добре відомі і уразливі, тому завжди повинні бути заблоковані. Однак подивися: порти 21, 22 і 80 - це FTP, SSH (Secure Shell) та HTTP - порти цих сервісів відкриті." — Я подивився на Ейдена.

"Улов", — запитав він з надією.

"Чесний видобуток, принаймні. В останню чергу nmap намагається визначити тип операційної системи на заданому хості. В основному, він лише 'грубо вгадує' тип ОС, хоча, дуже часто, показує точні результати. Так як сканування показало, що порти для служб FTP і SSH відкриті, отримані банери будуть ще одним підтвердженням правильності результатів сканування.

Перевір в Інтернет, там написано, що NcFTPd встановлюється на Unix системи, що підтверджує правильність ідентифікації типу операційної системи - FreeBSD - на сканованому комп'ютері. SSH часто за замовчуванням встановлений в Unix системах. Банери, звичайно, можна підробити, проте у нас на руках занадто багато збігів.

Тепер, залежно від розташування цілі сканування, можливо варто визначити ISP (постачальника послуг Інтернет), послугами якого користується пристрій який ми скануємо. У ISP також можуть бути зареєстровані і спамери і шкідливі сайти - однак ти можеш поскаржитися їм і пристрії нападників відключать. У твоєму випадку, я не думаю, що тобі доведеться мати справу з ISP..."

"Тому що сканований комп'ютер знаходиться в..." — випалив Ейден, однак я підняв вказівний палець вгору.

"Стоп. Твоя інформація це твоя інформація. Мені вона ні до чого. Ти ж етичний і безпечний хакер."

Ейден кивнув.

"Отже, що ти збираєшся робити?" — запитав я його.

"Гаразд, у них запущений веб-сервер, вірно?" — почав Еайдан, а мені нічого не залишилося, окрім як посміхнутися.

ПОЖИВА ДЛЯ РОЗУМУ: ДЕТАЛЬНІШЕ ПРО NMAP

Припустимо, що Ви ідентифікували ім'я хосту, власника мережі і переконалися, що хост підключений до мережі. Тепер необхідно знайти відкриті порти. Не забувайте, що, навіть якщо хост активний, порти на ньому можуть бути закриті (або перебувати в стані відфільтрованих).

Ви можете використовувати відомий мережевий сканер **nmap** від Fyodor для виконання цього завдання. Nmap дозволяє віддалено тестувати комп'ютери на наявність відкритих портів і пов'язаних з ними мережевих служб. По завершенню сканування nmap, залежно від типу командного рядка, яку Ви використовуєте, надасть Вам список відкритих портів і служб або протоколів, які працюють на знайдених портах. Nmap може також визначити операційну систему Вашого комп'ютера.

Nmap має безліч опцій і типів сканування. Ми будемо використовувати кілька опцій nmap. Також Ви завжди можете скористатися командою

```
nmap --help
```

для отримання детальної довідки.

Спершу сканування. Ви вже прочитали урок № 3? Ні? Поверніться і перечитайте! Можете пояснити різницю між TCP і UDP, описати процес потрійного рукостискання? Ці знання потрібні, щоб розуміти як працює nmap.

Синтаксис Nmap :

`nmap` техніка_сканування визначення_хосту опції ціль

- техніка_сканування вказує, які частини пакетів будуть використані і як повинні інтерпретуватися відповіді від цілі. Ми також проаналізуємо два базових типу сканування:
  - **-sS** SYN сканування (тільки перша частина потрійного рукостискання)
  - **-sT** TCP з повним встановленням з'єднання (повне потрійне рукостискання)
  - **-sA** ACK сканування (відправка ACK пакетів)
  - **-sU** UDP сканування
  - **-O** визначення ОС
  - **-A** Виконує всі функції: визначення ОС, плагіни, traceroute
- визначення_хосту вказує метод визначення присутності цілі в мережі. Якщо хост підключений до мережі, він буде скануватися, в іншому випадку ні.
  - **-PE** перевіряє, чи відповідає хост на ping
  - **-PS** перевіряє, чи відповідає хост на SYN
  - **-PA** перевіряє, чи відповідає хост на ACK
  - **-PU** перевіряє, чи відповідає хост на UDP дейтаграми
  - **-Pn** не перевіряє, звертається до всіх хостів як до активних (ми будемо використовувати цей параметр, оскільки знаємо, що наша ціль сканування знаходиться в мережі).

- Опції вказує деякі деталі для обраного типу сканування, наприклад:
  - **-p0-65535** діапазон портів, які потрібно сканувати (в даному прикладі від 0 до 65535).
  - **--top-ports number** nmap сканує лише загальновідомі порти, які часто використовуються (до 1024)
  - **-T0, -T1, -T2, -T3, -T4** для визначення швидкості сканування, 0 - повільне і 4 - швидке сканування (маленька швидкість сканування підвищує таємність і зменшує перевантаження мережі)
  - **-oA** ім`я_файлу для створення звіту в трьох форматах, які підтримує nmap (ми завжди будемо використовувати звіти для відстежування нашої активності після сканування)
  - **--reason** nmap описує причини вказаних результатів (будемо завжди використовувати)
  - **--packet-trace** те саме, що і **--reason**, плюс Ви побачите tracert для трафіка (завжди використовуйте, щоб дізнатися більше про метод сканування і для коригування отриманих результатів)
  - **-n** не дозволяє розпізнання імені хосту через DNS (цю опцію ми не будемо використовувати тому, що ми вже дізналися DNS-ім'я)

TCP Сканування

Наше перше сканування буде виглядати 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
```

Ми знайшли деякі відкриті порти, кілька закритих портів і один фільтрований. Що це означає? Значення залежить від типу сканування (в даному випадку ми використовували

-sT). Ми можемо використовувати стовпець Reason, щоб побачити, чому nmap виявляє частковий стан.

```
# 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
```

Тепер ми знаємо причини ідентифікації певного стану порту і ми знаємо, як nmap "зіставляв" одержувані відповіді з станами **TCP** Сканування:

- **open**: ціль відповіла SYN ACK пакетом
- **closed**: TCP з'єднання припинене
- **ltered**: немає відповіді від цілі

Для інших методів сканування і, зокрема, якщо Ви знайшли порти зі станом open | filtered, Вам слід копнути глибше, щоб дізнатися точну причину.

SYN Сканування

Інший відомий метод сканування - **SYN** сканування. Це тип сканування під час якого nmap відправляє тільки SYN пакети без завершення потрійного рукостискання. Також його називають "напіввідкрите" або "приховане" сканування, оскільки відсутня повне TCP з'єднання. Для даного типу сканування використовується опція **-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
```

Ми знову отримали звіт про причини та методи "зіставлення" одержуваних відповідей зі станом для **SYN** сканування:

- **open**: ціль відповіла SYN ACK пакетом
- **closed**: ціль відповіла пакетом, який містить RST прапор
- **filtered**: ціль не відповіла

Результати схожі на результати при TCP скануванні, однак будьте уважні і враховуйте відмінності між "повним" TCP скануванням і "напіввідкритим" SYN скануванням. Відмінності виникають у випадку захисту цілі сканування брандмауером з простою фільтрацією або фільтрацією з урахуванням стану потоку. Щоб знайти відмінності, порівняйте результати [з використанням опцій --reason та --packet-trace] використовуючи ту ж ціль сканування і різні методи сканування [-sT,-sS,-sA].

UDP сканування

Ще один метод сканування це UDP сканування (-sU): знання причини - основа отримання гарного результату.

```
# 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
```

Це може трохи збивати з пантелику. Що ж сталося? Ми бачимо деякі нестандартні причини, такі як: port-unreach (closed) та no-response (open | filtered). Чому? Нам

потрібно більше деталей. Ми можемо використовувати опцію --packet-trace і обмежити сканування лише двома портами, в нашому випадку нас цікавлять UDP-порти 53 і 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
```

Ми бачимо IP -адресу 192.168.100.53, з якої проводиться сканування UDP-портів 53 і 67 на сайті hackerhighschool.org . Порт 67 не відповідає, а для порту 53 ми отримали причину The Port Unreachable (T03C03).

Port Unreachable значить, що порт закритий і не відповідає - навіть якщо це звичайна відповідь для UDP - ми не знаємо, активна чи служба на цьому порту чи ні, оскільки UDP протокол може відповідати тільки якщо отримує необхідні для нього пакети. Чи можна дізнатися більше? Так, використовуючи метод сканування **- sV** (Службове Сканування, англ. «Service Scan»), при якому nmap намагається відправити стандартні загальновідомі пакети для UDP служб.

Службове сканування **(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
```

Цього разу нам не пощастило, ми отримали ті ж результати. Однак nmap, в процесі останнього сканування відправив безліч пакетів. Хороший хакер може також спробувати використовувати сканування за допомогою специфічних UDP пакетів вручну. Гарненько вивчіть загальновідомі служби на вашому комп'ютері і зробіть кілька вправ, а потім продовжуйте аналізувати банери.

ВПРАВИ

5.25 Перейдіть на http://insecure.org/, завантажте і встановіть останню версію nmap для Вашої ОС.
5.26 Повторіть всі сканування в цій секції уроку, використовуючи більше портів.
5.27 Майте на увазі, що в деяких випадках необхідне використання команди sudo (Linux) для запуску nmap від імені адміністратора (root).
5.28 Створіть таблицю з описанням всіх методів сканування, що відображають стан, причинами і реальними відповідями від цілі сканування (packet-trace).

Виявлення ОС

Визначення відомих служб - дуже важливий крок для отримання даних про ціль сканування. Nmap знову може прийти на допомогу. Ви можете отримати значно більше інформації використовуючи такі опції як **-A** для повнофункціонального сканування та **-O** лише для виявлення ОС, використовуючи порти по-замовчуванню:

```
# 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 використанні параметра **-A** спеціалізовані плагіни допомагають отримати більше інформації про мету сканування, " вгадують" ОС і проводять трасування маршруту, використовуючи методики, відмінні від tracert і traceroute. Чим більше знайдено відкритих портів, тим більше вірогідність вірно визначити ОС.

ВПРАВИ

5.29 Зробіть сканування свого комп'ютеру. Наскільки вірно nmap вгадав ОС?

5.30 Використовуйте опцію traceroute в nmap з різними портами:

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

5.31 Чи є якісь відмінності в результатах, отриманих при використанні traceroute в nmap з різними портами і результатами утиліт tracert / traceroute на Вашій операційній системі?

Використання скриптів

Nmap також має безліч корисних скриптів для сканування. Щоб використовувати скрипт при скануванні введіть параметр:

--script script-name

Один з них - скрипт **ipidseq**. Також відомий як Incremental IP fingerpriting. Цей скрипт може бути використаний для знаходження хостів, які можуть бути використані для методу холостого сканування (Idle Scan) (**-sI**). Цей тип сканування використовує проблемну реалізацію IP протоколу для того, щоб зомбувати жертву і сканувати інші хости з її IP-адреси.

```
# 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
```

ВПРАВИ

5.32 Дослідіть техніку холостого сканування. Що це за техніка і як Ви можете її використовувати?

ВИСНОВКИ

Знання де і що шукати, всього лише частина битви за безпеку. Комп'ютерні мережі постійно досліджують, аналізують, перевіряють на міцність. Якщо за мережею, яку Ви захищаєте, не стежать, значить Ви використовуєте неправильні утиліти, щоб визначити поведінку. Як фахівець у галузі комп'ютерної безпеки, Ви повинні знати кожен дюйм системи, яку Ви захищаєте. Ви також повинні знати, слабкі і сильні сторони мережі.

У наші дні вже не досить просто збирати дані про сервери, такі як операційна система і відкриті порти. Постійно виникаючі нові загрози намагаються дізнатися більше про Вашу мережу настільки, наскільки це можливо. Ця інформація може включати в себе:

- Марку брандмауера, модель, версію прошивки і встановлені патчі;
- Дистанційні з'єднання аутентифікації і права доступу;
- Інші сервери, які підключені до мережі. Наприклад: сервери електронної пошти, HTML, резервне копіювання, системи резервування, взяті напрокат або сервера аутсорсингових компаній, і навіть підрядників, які, можливо, використовували мережу або використовують її зараз ;
- Принтери, факси, сканери, беспроводові маршрутизатори та мережеві з'єднання у Вашій компанії ;
- Переносні пристрої, такі як: планшети, смартфони, цифрові камери і все те , що підключено до мережі.

Хоча ми розглянули багато тем в цьому уроці, системи ідентифікації охоплюють набагато більшу область. Існує досить багато інформації, яка проходить через мережі, які ідентифікують частині кожного пристрою. Кожен пристрій в мережі може бути використано в якості відправної точки для атаки. Підхід до вирішення цієї складної проблеми вимагає більшого, ніж просто використання програмного забезпечення. Досліджуйте власне устаткування і вивчіть так багато, наскільки це можливо. Ці знання Вам знадобляться.

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