Специфікація відбитків пальців (fingerprinting) TCP/IP

Лісовський О.С.
Науковий керівник – к.т.н.,доц. Муляр І. В.
Хмельницький національний університет

Важливим процесом в рамках реалізації функцій мережного моніторингу є збір відомостей про стан вузлів мережі. Для забезпечення ефективного вирішення завдань аналізу необхідно отримати характеристики широкого спектру показників, що описують роботу як всієї комп'ютерної мережі, так і окремих її компонентів.

Зняття відбитків пальців стека TCP/IP (TCP/IP stack fingerprinting) - пасивна колекція ознак конфігурації від віддаленого пристрою під час стандартного шару 4 мережевих комунікації [1]. Комбінація параметрів може тоді використовуватися, щоб вивести операційну систему віддаленої машини (інакше, зняття відбитків пальців OS), або включатися у відбиток пальця пристрою.

OS fingerprinting (OSF) - метод отримання інформації про ОС. OSF актуальне на початковому етапі реалізації атаки на хост. Так як маючи інформацію про тип ОС атакуючий може планувати на які відомі уразливості він буде впливати. При цьому, чим точніше атакуючий визначить тип і версію ОС віддаленого хоста, тим ефективніше буде виконано його "злом". Адміністратори йдуть на всілякі хитрощі, щоб виключити точне визначення своєї ОС. І для того, щоб точно визначити ОС доводиться використовувати комплексний підхід, що власне і описано в цьому документі. Сам процес визначення ОС не можна уявити не описавши методи сканування. Після застосування яких складається відбиток системи (fingerprint) по якому вже з бази заздалегідь відомих відбитків вибирається відповідність. OS fingerprinting буває двох видів - активний і пасивний. Активний OSF - це визначення типу ОС шляхом відсилання пакетів на досліджуваний хост.

Певні параметри в межах визначення протоколу TCP залишаються до реалізації. Різні операційні системи та різні версії однієї операційної системи встановлюють різні значення за замовчуванням для цих значень. Збираючи та вивчаючи ці значення, можна диференціюватися між різними операційними системами та реалізаціями TCP/IP. Поля TCP/IP, які можуть відрізнятися, включають:

- Початковий розмір пакета (16 біт)
- Початковий TTL (8 біт)
- Розмір вікна (16 біт)
- Максимальний розмір сегмента (16 біт)
- Значення масштабування вікон (8 біт)
- Прапор "не фрагментувати" (1 біт)
- Прапор "sackOK" (1 біт)
- прапор "nop" (1 біт)

Ці значення можуть бути об'єднані для формування 67-розрядного підпису або відбитка пальця для цільової машини. [1] Досить просто перевірити початкові поля TTL та розмір вікон, щоб успішно визначити операційну систему, що полегшує завдання виконання відбитків пальців вручну на ОС [2].

Інструменти для відбитків пальців мережі:

– Ettercap - пасивний відбиток стека TCP/IP.

– NetworkMiner - пасивний відбиток пальців стека DHCP та TCP/IP (поєднує бази даних p0f, Ettercap та Satori)

– Nmap - всебічний відбиток пальців активного стека.

– p0f - всебічний пасивний відбиток пальців TCP/IP.

– NetSleuth - безкоштовний пасивний інструмент для відбитків пальців та аналізу

– PacketFence [38] - відкритий код NAC з пасивним відбитком пальців DHCP.

– PRADS - Пасивний комплексний відбиток пальців TCP/IP та виявлення послуги

– Satori - пасивні CDP, DHCP, ICMP, HPSP, HTTP, TCP/IP та інші відбитки стека.

– SinFP - однопортовий активний / пасивний відбиток пальців.

– XProbe2 - активний відбиток стека TCP/IP.

– Веб-сайт пристрою для відбитків пальців[3] - відображає пасивний відбиток TCP SYN комп'ютера вашого браузера (або проміжного проксі)

– Queso - відомий інструмент з кінця 1990-х, який більше не оновлюється для сучасних операційних систем

Витяг значень RTO реалізується в такий спосіб. Клієнт відправляє запит SYN на встановлення з'єднання, після чого фіксує моменти часу, що відповідають отриманню пакетів SYN-ACK. Пакет з установленим прапором ACK при цьому не відправляється, тим самим клієнт імітує ситуацію втрати пакетів, що запускає механізм повторних передач на віддаленому вузлі. Послідовність значень часових інтервалів між посилками повторних пакетів SYN-ACK, а також кількість повторних передач є характеристиками, відмінними для різних реалізацій стека протоколів TCP/IP. Таким чином, аналіз даних значень дозволяє ідентифікувати версію ОС віддаленого вузла.

Аналіз значень RTO для ситуації розриву TCP-з'єднання. Процес завершення TCP-з'єднання передбачає процедуру обміну чотирма пакетами між учасниками з'єднання. Для реалізації функцій IOC виконується аналіз послідовності значень часових інтервалів між повторними передачами пакету FIN, що відправляється віддаленим вузлом. З метою вилучення значень RTO клієнт імітує ситуацію втрати пакетів, які не відправляючи заключний пакет ACK [4].

Сканування з встановленням наполовину відкритого з'єднання (SYN)/ Ідея сканування з встановленням наполовину відкритого з'єднання (також відомого як SYN-сканування) дуже проста. Без завершення трьохетапного

встановлення TCP з'єднання, надсилається пакет SYN і очікується відповідь. Якщо відповідь одержано SYN ACK, це означає, що віддалений порт відкритий, в іншому випадку, якщо отриманий пакет з прапором RST, порт закритий [5].

Однак, в деяких випадках, міжмережевий екран може просто заблокувати доступ до деяких відкритим портів. У цих випадках кажуть, що порт фільтровано. У таких ситуаціях ми не отримаємо відповідь на наш пакет SYN. Також багато ME блокують RST пакети, які є відповіддю на закритий порт. У таких ситуаціях складно зрозуміти, які порти закриті, а які фільтруватися. Нижче наводяться результати сканування з допомогою nmap хоста без ME.

root@life# nmap -P0 -p 1,2,21,80 202.83.174.99

Interesting ports on (202.83.174.99):
PORT STATE SERVICE
1/tcp closed tcpmux
2/tcp closed compressnet
21/tcp open ftp
80/tcp open http
Nmap finished: 1 IP address (1 host up) scanned in 1.140 seconds

Як можна помітити, даний хост не схожий на що знаходиться за ME. Ми просканували порти 1, 2, 21, 80, і встановили, що порти 1 і 2 закриті, а що залишилися два відкриті.

При активному зняття відбитка виробляється відправка довільних пакетів на цільової хост і робиться спроба визначення ОС на підставі таких значень полів заголовка відповідних TCP/IP пакетів, як тимчасові характеристики або IPID, TOS, TCP ISN, прапор фрагментації і т.д. інший старий метод визначення віддаленої ОС полягає в аналізі значення TTL ICMP echo-пакета. Це простий спосіб, однак він не може виявити відмінності різних варіантів однієї і тієї ж ОС, наприклад win98, XP і win2k. Зазвичай в кожній ОС встановлено фіксований, заздалегідь певне, значення TTL. В операційних системах Microsoft це значення за замовчуванням дорівнює 128, тоді як в Linux - 256. Нижче показаний приклад визначення віддаленої ОС за значенням TTL відповідного ICMP echo-пакета. Я просто пінгую цільову машину і перевіряю значення TTL отриманого у відповідь пакету. В даному випадку воно дорівнює 113, що дозволяє припустити, що віддалена ОС належить до сімейства Windows, так як стартове значення TTL цих систем дорівнює 128, а маршрут від моєї машини до цільової становить приблизно 15 проміжних хостів (113 + 15 = 128), що може бути перевірено за допомогою traceroute.

E:\>ping 209.41.165.180

Pinging 209.41.165.180 with 32 bytes of data:
Reply from 209.41.165.180: bytes=32 time 38ms TTL=113

Reply from 209.41.165.180: bytes=32 time 51ms TTL=113
Ping statistics for 209.41.165.180:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
Minimum = 38ms, Maximum = 51ms, Average = 44ms

Тепер спробуємо застосувати описану вище SYN ACK методику. Для початку ми повинні налаштувати локальний MCE на тихе блокування всіх SYN ACK пакетів, що приходять з віддаленого хоста.

life1# iptables -A INPUT -p tcp -j DROP -s 202.83.162.27

Тепер відправимо SYN пакет на відкритий 80 порт і почнемо стеження за виводом tcpdump

root@life# hping -S -p 80 -c 1 202.83.162.27

17:22:51.079596 202.134.134.230.1816 > 202.83.162.27.http: S win 512
17:22:51.208938 202.83.162.27.http > 202.134.134.230.1816: S ack win 5840
17:22:53.218939 202.83.162.27.http > 202.134.134.230.1816: S ack win 5840
17:23:57.218939 202.83.162.27.http > 202.134.134.230.1816: S ack win 5840
17:23:03.218939 202.83.162.27.http > 202.134.134.230.1816: S ack win 5840
17:23:11.468939 202.83.162.27.http > 202.134.134.230.1816: S ack win 5840
17:24:21.618938 202.83.162.27.http > 202.134.134.230.1816: S ack win 5840

Різниця в часі, між отриманням SYN ACK пакетів становить приблизно 2, 4, 5, 7 і 10 секунд.

Експерименти з іншими хостами показали, що затримки повторної передачі SYN ACK пакетів системи FreeBSD складають приблизно 3, 6, 12, 24 секунди, а Windows-хостів відповідно 2, 4, 6, 8, 10 секунд. Це інформація може бути корисною для правильного впізнання операційної системи в тих випадках, коли інші методи зазнають невдачі і дають невірні результати. Зверніть увагу, представлені вище значення не дуже точні і були отримані в результаті дослідів з двома хостами, на одному з яких встановлена indows 2010, а на іншому FreeBSD 4.6.

Автоматизовані способи зняття відбитків віддаленої системи можуть давати непогані результати, проте в деяких середовищах вони не завжди ефективні. У цих випадках для отримання найбільш точних результатів потрібно комбінувати кілька різних методик.

Більш досконалий метод IOC, заснований на аналізі значень RTO стека протоколів TCP/IP для ситуації втрати пакетів при передачі даних, є продовженням ідей Франка Вейсета і вперше був згаданий в роботі Грега Талек (Greg Taleck) [28] в 2004 р. Це метод Synscan.

Суть методу Synscan полягає в вимірі і аналізі значень RTO, характерних для відпрацювання механізму повторних передач втрачених пакетів з даними, переданими по TCP-з'єднання, наприклад, в процесі взаємодії по протоколу HTTP.

У прикладі на рисунку 2.1 числа, розділені двокрапкою, вказують на початок і кінець переданої в даному пакеті послідовності байт даних (тобто відповідають відносному номеру послідовності і довжині поля даних). Числа після «АСК» відповідають відносним номерами підтвердження, які встановлюються в переданих пакетах.

Обмін даними в представленому прикладі відбувається наступним чином:

1. Виконується успішне встановлення TCP-з'єднання з веб-сервером, і клієнт по протоколу HTTP запитує з сервера індексний файл.

2. Сервер починає відправку пакетів даних.

3. Відправкою АСК-пакета клієнт підтверджує успішне отримання кількох перших пакетів даних від сервера, після чого припиняє відправляти АСК-пакети.

4. Після закінчення часу очікування повторної передачі першого недоставленого пакета (в розглянутому прикладі пакет даних з номером послідовності 1025) сервер починає цикл його повторних передач.

Результати дослідження свідчить про наявність відмінностей між сигнатурами Synscan для різних ОС, в тому числі для ОС одного і того ж сімейства. Важливою відмінністю сигнатур Synscan від сигнатур RING є більший обсяг доступних для аналізу даних, що дозволяє визначати версію ОС цільового вузла з більш високою вірогідністю. Проте, сигнатури Synscan деяких ОС, в тому числі що належать різних сімейств, ідентичні, що в ряді випадків призведе до неоднозначності результатів аналізу і зниження вірогідності припущення про версії ОС цільового вузла.

Перелік посилань

1. Murphy, S. An Application of Deception in Cyberspace: Operation System Ob-fuscation / S. Murphy, T. McDonald, R. Mills // Proceedings of the 5th International Conference on Information Warfare and Security. - Ohio, 2010. - pp. 241-250.

2. Лавров, А. А. Алгоритмы классификации в задаче идентификации версии ОС удаленного сетевого узла / А. А. Лавров // Сб. тр. 65-й науч.-техн. конф. проф.-преп. состава СПбГЭТУ «ЛЭТИ». - СПб., 2012. - 102-106 с.

3. Chang, C.-C. LIBSVM: A library for support vector machines / C.-C. Chang, C-J. Lin // ACM Transactions on Intelligent Systems and Technology. - 2011. -Vol. 2, Issue 3. - Article No. 27.

4. Кореньков В. В. Архитектура и пути реализации системы локального мониторинга ресурсного центра / В. В. Кореньков, П. В. Дмитриенко // Системный анализ в науке и образовании. - Дубна, 2011. – 201-204 с.

5. Максимов, Н. В. Компьютерные сети / Н. В. Максимов, И. И. Попов. - М.: Форум, 2010. - 464 с.