УДК 004.77+0004.56

А. В. Борусевич
Л. М. Куперштейн

АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ТИПУ ОПЕРАЦІЙНОЇ СИСТЕМИ ВІДДАЛЕНОГО ХОСТА

Вінницький національний технічний університет

Анотація

У даній роботі розглянуто методи та засоби виявлення типу операційної системи пристрою. Обґрунтовано доцільність використання нейромереж для визначення типу операційної системи.

Ключові слова: операційна система, виявлення, безпека, мережа.

Abstract

In this work methods and means of operating system detection are analized. Use of neural networks for operating system detection is reasoned.

Keywords: operating system, detection, security, network.

Вступ

Щодня кількість пристроїв у мережах зростає. Проте не всі пристрої, якими користуються, мають останню версію операційної системи та\або оновлення. Причинами можуть бути як обмеження апаратного забезпечення, так і небажання користувачів. Старі версії операційних систем можуть містити велику кількість вразливостей. Адміністраторам великих мереж потрібно мати інструмент для моніторингу мереж для виявлення неавторизованих пристроїв. Пентестерам важливо мати спосіб проаналізувати склад мережі для виявлення потенційних загроз та вразливостей. Саме тому питання визначення типу операційної системи є актуальним.

Метою роботи є підвищення ефективності методів та засобів виявлення типу операційної системи за рахунок використання нейромереж.

Необхідність виявлення типу операційної системи

При проведенні аудиту або під час адміністрування мережі доволі часто необхідно дізнатися не лише IP-адреси пристроїв, а й додаткову інформацію, таку як тип операційної системи, її версію, тип пристрою (персональний комп'ютер, роутер, принтер) тощо. Пункти політики безпеки можуть залежати від кількості пристроїв та версії операційної системи, які встановлені на цих пристроях.

Причинами для виявлення типу операційної системи можуть бути [1]:

1. Адаптація атак при використанні вразливостей. В разі, якщо зловмисник або пентестер отримає детальну інформацію про тип та версію операційної системи, він зможе коригувати шкідливий код для конкретного пристрою. Без цього служба може зупинитись й іншої спроби не буде.

2. Необхідність віддалено виявити перелік доступних вразливостей цільового пристрою. Так, наприклад, при виконанні аудиту безпеки на замовлення компанії рідко коли є можливість переглянути інформацію про тип та версію операційної системи пристрою. Деякі вразливості наявні лише на певних версіях операційної системи.

3. Аналіз мережі для знаходження неавторизованих пристроїв. Трапляються випадки, коли користувачі підключаються до корпоративної мережі з інфікованих пристроїв. Регулярне сканування дозволяє вести постійний контроль у мережі і виявляти нові пристрої.

4. Використання інформації при здійсненні інших атак. Так, якщо зловмисник або пентестер зможе отримати детальну інформацію про пристрій, він зможе збільшити власні шанси на реалізацію атаки типу соціальна інженерія, представляючись, наприклад, під виглядом інженера виробника.

5. Інвентаризація пристроїв. У великих компаніях з великою кількістю пристроїв часом потрібно перевірити, чи досі хтось користується певним пристроєм або групою пристроїв. Це дозволяє ефективно планувати бюджет та в певних випадках економити кошти і зменшувати ризики завдяки тому, що певні пристрої не будуть підключені до мережі і не надаватимуть зловмисникам додаткові вразливості для використання.

Методи виявлення ОС

Є два основні методи виявлення типу ОС: активний та пасивний

1. Активний. Метод базується на відправці службових пакетів та аналізі отриманих відповідей. Після чого формуються відповідні висновки щодо встановленої на пристрої операційної системи та її версії [2].

Одним із прикладів такої програми є Nmap. Програма формує «відбиток», надсилаючи до 16 TCP, UDP та ICMP пакетів на відомі відкриті та закриті порти. Потім програма очікує та аналізує відповіді на ці пакети. В результаті формується висновок, де зазначається тип операційної системи пристрою і точність цього висновку.

Іншою програмою є NetScanTools Pro. Програма використовує відповіді на ICMP пакети для встановлення типу операційної системи. Проте програма має схожий із Nmap недолік: висновок надається з певною точністю, яку проте не можна побачити у результаті.

2. Пасивний. Метод базується на використанні пасивного прослуховування та аналізу трафіку в мережі [3]. Метод є більш трудомістким, оскільки не можна керувати пакетами, надсилати з користувацькими параметрами. Проте цей метод є непомітним для цілі, оскільки прямий вплив на мережу не відбувається. Проте цей метод має аналогічний недолік, а саме – ймовірнісний висновок щодо встановленої операційної системи, оскільки йде порівняння отриманих параметрів (наприклад, TTL, TOS, Window Size) із базою сигнатур. В разі, якщо база сигнатур застаріла або містить помилкові записи, обидва методи матимуть меншу ймовірність надати правильну відповідь.

Прикладом програми, яка використовує пасивний метод виявлення типу операційної системи, є NetworkMiner. Усе, що необхідно зробити пентестеру – запустити сканування на обраному інтерфейсі. Програма, так само, як і Nmap, надає відповідь із певною точністю, використовуючи при цьому кілька баз сигнатур.

Для пасивного виявлення можна також використовувати WireShark. Для цього потрібно власноруч аналізувати певні поля: TTL, User-Agent тощо. Так, наприклад, якщо значення TTL становить 128, а параметр User-Agent міститься значення «Windows NT 10.0», то можна зробити висновок, що на пристрої встановлено операційну систему Windows 10 [4,5]. Проте в такому разі необхідно мати таблиці, де у відповідності до значень записані типи операційних систем[6].

Головним недоліком зазначених методів визначення є точність. А саме – невелике її значення (менше 80%). Цей недолік є доволі суттєвим, оскільки в разі якщо тип визначено неправильно, пентестер або фахівець з інформаційної безпеки може зробити хибний висновок щодо наявності або відсутності у системі певних вразливостей. Це може призвести як до збільшення витрат на організацію безпеки мережі, так і до збільшення часу виявлення загрози або атаки.

Для підвищення точності виявлення можна використовувати методи машинного навчання, зокрема нейромережі. Перевагою такого методу є те, що нейромережі є універсальними апроксиматорами, які зарекомендували себе при вирішення широкого кола задач [7]. Використання нейромереж та машинного навчання дозволяє отримувати результати визначення типу операційної системи з доволі високою точністю (більше 80%) [8].

Також варто звернути увагу на те, що на якість визначення типу операційної системи має великий вплив репрезентативність навчальної вибірки. Тому першочерговим завданням є обґрунтоване визначення ознак для визначення типу ОС та формування відповідного набору даних для навчання .

Висновки

З’ясовано, що існує два головних підходи до виявлення операційної системи пристрою, кожен з яких має власні переваги та недоліки. Активний метод є доволі швидким, проте не є непомітним. Пасивний має відповідно протилежні якості – відсутність пакетів, які б можна було відслідкувати, проте на збирання пакетів може витрачатись велика кількість часу в разі відсутності трафіку. Проте обидва методи не дають гарантовану відповідь, оскільки аналіз базується на сигнатурах. Пропонується використовувати нейромережі для аналізу трафіку в пасивному режимі (якщо необхідно виконувати виявлення операційної системи непомітно) із можливістю виконання активного аналізу, надсилаючи пакети із певними параметрами, як це впроваджено, наприклад, у Nmap. Це дозволить більш гнучко використовувати програмний засіб, а також швидше та із більшою точністю отримувати результати сканування та виявлення типу операційної системи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Chapter 8. Remote OS Detection. Reasons for OS Detection: веб-сайт. URL: https://nmap.org/book/osdetect.html#osdetect-reasons (дата звернення: 03.03.2021).

2. TCP/IP Fingerprinting Methods Supported by Nmap : веб-сайт. URL: https://nmap.org/book/osdetect-methods.html (дата звернення: 03.03.2021).

3. Огляд статистики зарплатні професії "Разработчик C# в Україні" : веб-сайт. URL: http://cybervlad.net/lspitz/finger/index.html (дата звернення: 03.03.2021).

4. Passive OS Fingerprinting : веб-сайт. URL: https://www.netresec.com/?page=Blog&month=2011-11&post=Passive-OS-Fingerprinting (дата звернення: 03.03.2021).

5. Wireshark Tutorial: Identifying Hosts and Users : веб-сайт. URL: https://unit42.paloaltonetworks.com/using-wireshark-identifying-hosts-and-users/ (дата звернення: 03.03.2021).

6. OS Detection Techniques : веб-сайт. URL: https://jonathansblog.co.uk/os-detection-techniques (дата звернення: 04.03.2021).

7. Васюра А.С., Мартинюк Т.Б., Куперштейн Л.М. Методи та засоби нейроподібної обробки даних для систем керування. Монографія. Вінниця: УНІВЕРСУМ−Вінниця, 2008. 175 с.

8. A. Aksoy, S. Louis and M. H. Gunes, "Operating system fingerprinting via automated network traffic analysis," 2017 IEEE Congress on Evolutionary Computation (CEC), Donostia, Spain, 2017, pp. 2502-2509, doi: 10.1109/CEC.2017.7969609.

Борусевич Артур Вячеславович — студент групи 1БС-17б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, e-mail: borusevych.av@gmail.com

Куперштейн Леонід Михайлович — кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Borusevych Artur V. — Student of Information Technologies and Computer Engineering Department, Vinnytsia National Technical University, email : borusevych.av@gmail.com

Kupershtein Leonid M. — PhD, Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, email: kupershtein.lm@gmail.com