УДК 004.075

Желєзняк В.В. (ХмНУ)
д.т.н., проф. **Мясіщев О.А.** (ХмНУ*)*
д.т.н., проф. **Лєнков С.В.** (ВІКНУ)
Сєлюков Д.О. (НУБіП)

АНАЛІЗ МЕТОДІВ ТА АЛГОРИТМІВ МОНІТОРИНГУ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ

У статті розглядаються існуючі методи та алгоритми ідентифікації операційних систем, засновані на аналізі значень RTO (Retransmission Timeouts), використовуваних стеком протоколів TCP/IP, які є основою для побудови і функціонування систем моніторингу обчислювальних мереж. Показані основні властивості, переваги та недоліки даних методів, які дозволяють спеціалісту повисити ефективність своєї роботи на етапі реалізації і експлуатації контрольованих інформаційних систем.

На теперішній час відсутні досконалі алгоритми моніторингу обчислювальних мереж, засновані на аналізі тимчасових закономірностей в роботі стека протоколів TCP / IP. У зв'язку з цим виникає проблема функціонування інформаційної мережі. Задачею є розробка ефективних засобів моніторингу та діагностики інформаційних систем. Широке розповсюдження систем мережевого моніторингу в корпоративних інформаційних системах призводить до необхідності приділяти активну увагу вирішенню притаманних їм проблем безперебійного функціонування. При цьому існуючі певні засоби для отримання якості роботи мережі.

Проведений аналіз методів моніторингу та алгоритмів спрямованих на визначення ідентифікатора операційної системи дає нам змогу більш швидше оцінювати рівень працездатності мережі та точність (достовірність) результуючого припущення про версії ОС цільового вузла.

Ключові слова: системи мережевого моніторингу, інформаційні системи, ідентифікатор операційної системи.

Вступ. В останні роки з ростом рівня автоматизації, проникнення інформаційних технологій в усі сфери діяльності людини і значним підвищенням вимог відмовостійкості та надійності до інформаційних систем важливе значення набувають питання розробки ефективних засобів моніторингу та діагностики інформаційних систем. У зв'язку з повсюдним використанням обчислювальних мереж (ОМ) і мереж передачі даних для організації взаємодії як між окремими робочими станціями для передачі інформації прикладного характеру (наприклад, при роботі в глобальній мережі Інтернет), так і взаємодії всередині замкнутих обчислювальних кластерів, інформаційно обчислювальних комплексів обробки даних, корпоративних мереж та інших розподілених систем, заснованих на використанні обчислювальних мереж, гостро постають питання моніторингу стану подібних систем.

Класичні системи моніторингу забезпечують безперервний моніторинг тільки поточного стану вузлів, що входять до складу ОМ, але в умовах сучасних все більш ускладнених розподілених систем і жорстких вимог до їх відмовостійкості та надійності, а також захищеності та інформаційної безпеки до сучасних систем моніторингу пред'являються також вимоги щодо забезпечення можливостей прогнозування і діагностики стану обслуговуваних інформаційних систем в короткостроковій і довгостроковій перспективах, а також реалізації комплексного моніторингу, що включає аналіз не діагностика потенційних проблем в захищеності системи або окремих її вузлів від різних типів зовнішнього втручання. Актуальність даних питань розглянута, зокрема, в роботах Р. Г. Шихаліева, а також В.В. Коренькова і А.В. Ужінского.

Крім того, актуальними проблемами розробки систем моніторингу мережі є збільшення точності аналізу стану входять до складу ОМ вузлів, тобто забезпечення максимальної відповідності показань системи моніторингу реального стану інформаційної системи, а також зменшення інтенсивності обміну службовим трафіком і мінімізація впливу підсистеми моніторингу на функціонування інших підсистем обчислювальної мережі або розподіленої

системи (наприклад, підсистем забезпечення мережевої інформаційної безпеки - систем виявлення вторгнень і т.д.) .

У зв'язку з викладеним завдання дослідження і розробки методів моніторингу та діагностики обчислювальних мереж і розподілених систем, а також систем моніторингу на їх основі в даний час є актуальними.

Постановка задачі. В умовах постійного розвитку, ускладнення і повсюдного впровадження в усі сфери життя людини розподілених інформаційних систем завдання постійного контролю за роботою обчислювальної мережі, що становить основу будь-якого сучасного цифрового обчислювального комплексу або інший розподіленої системи, набувають все більш важливе значення, оскільки необхідні для підтримки системи в працездатному стані і оперативного усунення збоїв і неполадок.

У зв'язку з цим виникає небхідність розробки методів і алгоритмів моніторингу ОМ, заснованих на аналізі тимчасових закономірностей в роботі стека протоколів TCP / IP, і побудова системи моніторингу мережі на їх основі.

Основна частина. Алгоритм Франка Вейсета (RING)

Першою реалізацією методу ідентифікації операційної системи(ІОС), заснованого на аналізі значень RTO стека протоколів TCP / IP, став алгоритм, заснований на аналізі значень RTO для ситуації втрати пакетів при встановленні TCP-з'єднання, запропонований Франком Вейсетом (Franck Veysset) в 2002 р. і покладений в основу відповідної утиліти, що отримала назву RING [1].

Алгоритм RING заснований на імітації клієнтом ситуації втрати пакетів в процесі «тристороннього рукостискання», використовуваного для встановлення TCP-з'єднання.

У відповідності зі специфікою TCP по надійній доставці повідомлень кожен пакет, в тому числі запити SYN на встановлення з'єднання, обов'язково підтверджується одержувачем з використанням відповідей-підтверджень - пакетів з встановленим прапором ACK. У разі неотримання підтвердження відправник повторно відправляє непідтверджений пакет, втрата якого могла статися, наприклад, внаслідок виходу з ладу деяких сегментів мережі між учасниками інформаційного обміну, перевантаженням мережі або іншими причинами. Процедура надійної передачі даних діє і в процесі встановлення TCP-з'єднання. Таким чином, можливий наступний сценарій розвитку подій: клієнт з яких-небудь причин не відправляє останній, третій, пакет ACK, в результаті чого сервер класифікує останній відправлений ним пакет SYN-ACK як втрачений і запускає цикл його повторних передач, чекаючи від клієнта підтвердження про успішне встановлення з'єднання (рис. 1).

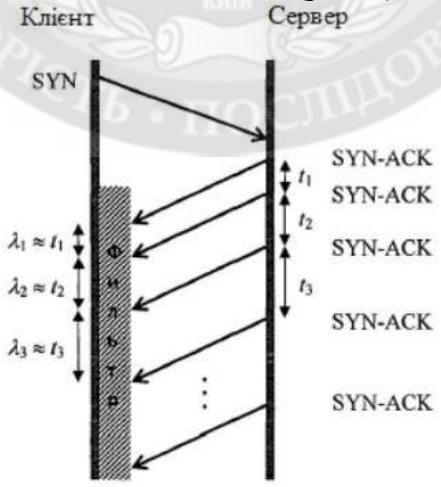

Рис. 1. Імітація втрати клієнтом

Імітація клієнтом перевантаженості мережі, яка потягнула за собою втрату пакетів між сервером і клієнтом, примусово вводить сервер в ситуацію, при якій він відпрацьовує затримку читання підтвердження у відповідь на відправлений пакет і запускає серію повторних передач SYN-ACK «втраченого» пакета. Реєстрація клієнтом інтервалів часу між отриманням

повторних запитів SYN-пакетів при встановленні TCP-з'єднання ACK від сервера, аналіз послідовності значень часових інтервалів $\lambda_1, \lambda_2, \ldots, \lambda_n$ та її зіставлення з сигнатурами (наборами аналогічних тимчасових характеристик) відомих ОС дозволяє зробити припущення про версії ОС, яка працює на сервері [1].

Ступінь відповідності версії ОС аналізованого вузла деякої ОС з відомою сигнатурою може бути оцінена наступним чином:

$$D = \sum |\lambda_i - \delta_i| \ , \tag{1}$$

де δ_i, - інтервал часу між відправленням i-го та $i+1$-го пакетів для даної ОС з існуючої бази сигнатур.

За результатами аналізу найбільш вірогідною версією ОС віддаленого вузла буде ОС з використовуваної бази сигнатур, що відповідає мінімальному значенню D з безлічі значень $\{D_j\}$, отриманих за результатами порівняння отриманої сигнатури з відомими сигнатурами різних ОС, тобто така ОС з бази сигнатур, для якої справедливо умова

$$D = mm\{D_j\}, 1 < j < n, \tag{2}$$

де n - кількість ОС в базі сигнатур, D_j обчислюється за формулою (1).

У порівнянні з використовуваними в сучасних програмних засобах мережевого моніторингу методів IOC, заснованих на обміні нестандартними TCP-пакетами та аналізі функціональних характеристик стека протоколів TCP / IP, алгоритм Франка Вейсета володіє наступними основними перевагами:

1. Для успішного аналізу на цільовій системі необхідна наявність тільки одного відкритого TCP-порту. У зв'язку з тим, що в сучасних обчислювальних мережах(ОМ) на мережевих вузлах з міркувань безпеки в більшості випадків блокуються всі невикористовувані безпосередньо порти TCP і UDP, алгоритм Франка Вейсета в багатьох випадках може бути значно більш ефективним в порівнянні з іншими методами IOC [2].

2. Для ідентифікації ОС використовуються стандартні TCP-запити, що значно знижує ймовірність класифікації переданого трафіку як аномального і / або є ознакою зовнішнього вторгнення або сканування. Таким чином, розглянутий алгоритм характеризується більшою прозорістю для систем виявлення вторгнень і міжмережевих екранів.

3. Низький рівень споживання трафіку (менше 1Кб для сканування одного мережевого вузла).

4. При наявності якісної бази сигнатур RING забезпечує більш високу достовірність результатів у порівнянні з іншими методами IOC . Найбільшою мірою це справедливо для ситуацій, коли аналізовані вузли не задовольняють вимогам існуючих методів IOC за критеріями доступності портів TCP / UDP і можливості використання для аналізу протоколу ICMP [12].

Одним з переваг RING є використання коректних пакетів TCP, що забезпечує високу прозорість для систем виявлення вторгнень і фільтрації трафіку. Крім того, можливість штучного навмисного спотворення значень RTO на стороні аналізованого вузла зведена до мінімуму, оскільки значення тимчасових характеристик TCP визначаються внутрішніми системними налаштуваннями ядра ОС і в більшості випадків не можуть бути змінені користувачем або спеціальним програмним забезпеченням, а також в загальному випадку не залежать від встановленого на цільовому вузлі ПО, включаючи міжмережеві екрани, системи фільтрації трафіку і інші засоби забезпечення мережевої інформаційної безпеки. Перераховані властивості забезпечують методам IOC, заснованим на аналізі тимчасових характеристик TCP, і, в тому числі, алгоритму Франка Вейсета, універсальну застосовність щодо будь-яких мережевих вузлів, що використовують стек протоколів TCP / IP. При цьому будь-яка спеціальна підготовка або налаштування цільового вузла не потрібна.

Основним функціональним недоліком алгоритму Франка Вейсета є відносно високі витрати часу на збір даних, що аналізуються, що досягають декількох хвилин, що значно вище

аналогічних показників для інших методів IOC, реалізованих в сучасних мережевих сканерах (NMap, Xprobe і ін.).

Як недолік алгоритму також можна розглядати необхідність спеціальної настройки вузла моніторингу, необхідну для імітації втрати пакетів. Для цього необхідно блокувати або вихідні TCP-пакети з встановленим прапором ACK в разі, якщо відправка пакетів здійснюється засобами стандартних сокетів TCP / IP ОС вузла моніторингу, або вихідні пакети з встановленим прапором RST в разі використання «сирих» сокетів. Подібне налаштування може бути здійснена засобами міжмережевих екранів [3].

Проте, в ряді випадків застосовність алгоритму Франка Вейсета може бути обмежена. Одним з найбільш серйозних обмежень для функціонування розглянутого алгоритму є використання в мережі міжмережевих екранів сеансового рівня {stateful firewall) . До числа подібних систем відносяться зокрема міжмережеві екрани, що реалізують функціональність SYN-шлюзів (SYN Relay або SYN Gateway) [10].

Застосування алгоритму Франка Вейсета, тим не менш, може викликати спрацьовування систем виявлення вторгнень у разі класифікації SYN-запитів, які не завершуються коректним чином з боку клієнта, як аномального трафіку. В цьому випадку для використання розглянутого алгоритму в складі систем моніторингу мережі необхідна відповідне налаштування засобів IDS, що збільшує трудомісткість розгортання СММ. Проте, основною перешкодою для використання алгоритму Франка Вейсета при реалізації функцій мережевого моніторингу є неможливість його застосування в випадку наявності в мережі SYN-шлюзів. Як правило, в сучасних ОМ сервери-шлюзи перед основними серверами в тому чи іншому вигляді існують [4].

Метод Грега Талек (ГТ). Суть методу Грега Талек 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 [5].

Приклад реалізації процесу збору даних, що аналізуються для випадку взаємодії по протоколу HTTP представлений на рис. 2.

У прикладі на рис. 2 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 «ACK» відповідають відносним номерами підтвердження, які встановлюються в переданих пакетах [5].

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 ACK-пакета клієнт підтверджує успішне отримання кількох перших пакетів даних від сервера, після чого припиняє відправляти ACK-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 [12].

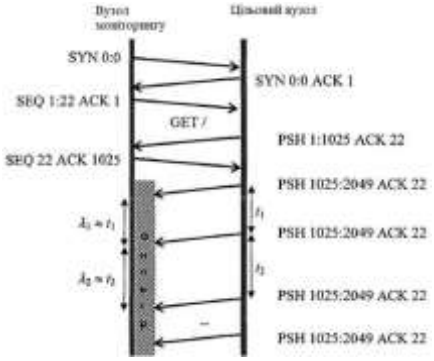

Рис. 2. Метод IOC на основі значень аналізу RTO для ситуації втрати пакетів при передачі даних

Аналіз значень часових інтервалів $\lambda_1, \lambda_2, \ldots, \lambda_n$ "між повторними передачами і їх порівняння з існуючою базою сигнатур, що виконуються аналогічно алгоритму Франка Вейсета, дозволяють зробити припущення про версії ОС, що виконується на сервері [7].

Слід зазначити, що в рамках методу Грега Талек можливе використання не тільки протоколу HTTP, а й будь-якого протоколу прикладного рівня, заснованого на TCP / IP. Оскільки будь-який сучасний сервер надає один або кілька мережних сервісів, що реалізуються протоколами прикладного рівня (наприклад, DNS, POP3, IMAP, SSH, FTP та ін.), можна зробити висновок про універсальну застосовність методу Грега Талек для мереж TCP / IP [8].

Основною перевагою методу Грега Талек в порівнянні з алгоритмом Франка Вейсета є відсутність обмежень, що накладаються використанням в мережі SYN-шлюзів. Крім того, метод Грега Талек характеризується значно більш низьким ступенем виявлення системами IDS, оскільки ймовірність виникнення ситуації втрати пакетів при передачі даних по TCP-з'єднання вища, ніж вірогідність втрати пакетів в процесі встановлення з'єднання, і в загальному випадку подібні факти не є свідченням здійснення спроб мережевого вторгнення або несанкціонованого сканування мережі [9].

Результати вимірювань свідчить про наявність відмінностей між сигнатурами ГТ для різних ОС, в тому числі для ОС одного і того ж сімейства. Важливою відмінністю сигнатур ГТ від сигнатур RING є більший обсяг доступних для аналізу даних, що дозволяє визначати версію ОС цільового вузла з більш високою вірогідністю.

Недоліком методу ГТ є сигнатури деяких ОС, в тому числі що належать до різних сімейств, ідентичні, що в ряді випадків призведе до неоднозначності результатів аналізу і зниження вірогідності припущення про версії ОС цільового вузла. Крім того, в порівнянні з алгоритмом Франка Вейсета метод Грега Талек вимагає більше часу для збору значень аналізованих характеристик [11].

Висновки. Найважливішою характеристикою процесу ІОС є точність (достовірність) результуючого припущення про версії ОС цільового вузла. Разом з тим, важливе значення мають характеристики рівня споживання мережевого трафіку, прозорості для систем IDS і впливу на працездатність аналізованого вузла [6].

Для реалізації функцій ІОС можливе використання в якості аналізованих даних значень тимчасових характеристик функціонування TCP / IP, до числа яких відносяться таймаут повторних передач втрачених пакетів. Перевагами такого підходу є низький обсяг споживаного мережевого трафіку, висока прозорість для систем IDS і фільтрації трафіку і відсутність деструктивного впливу на працездатність цільового вузла.

У зв'язку з наявністю зазначених раніше недоліків алгоритму Франка Вейсета і методу Грега Талек, пропонується метод ІОС, заснований на спільному аналізі тимчасових і функціональних характеристик стека протоколів TCP / IP цільового вузла і зберігає переваги алгоритму Франка Вейсета і методу Грега Талек - необхідність наявності тільки одного відкритого TCP-порту на цільовому вузлі , низький рівень споживання трафіку і низький ступінь виявлення системами IDS [2].

ЛІТЕРАТУРА:

1. Veysset, F. New Tool And Technique For Remote Operating System Fingerprinting / F. Veysset, O. Courtay, O. Heen. - Intranode Software Technologies, 2002.- 13 с;

2. Лавров, А. А. Метод идентификации ОС удаленного хоста на основе анализа временных характеристик стека TCPЛР в задачах сетевого мониторинга / А. А. Лавров, А. К. Большее // Сб. тр. 64-й науч.-техн. конф. проф.-преп. состава СПбГЭТУ «ЛЭТИ» - СПб, 2011. - С. 104-110;

3. Oracle Database Reference 11g Release2 (11.2) E40402-18 [Текст] // Bert Rich – Oracle, 2015. – 1306 с.;

4. Лавров, А. А. Идентификация операционной системы удаленного хоста методами анализа временных характеристик / А. А. Лавров, В. В. Яновский // Известия СПбГЭТУ «ЛЭТИ». - 2011. - №3.

- С. 34-39;

5. Beardsley, T. A. Intrusion Detection and Analysis: Theory, Techniques, and Tools / T. A. Beardsley. - SANS Lone Star, 2002. - 70 с.;

6. Oracle Database Reference 11g Release2 (11.2) E40402-18 [Текст] // Bert Rich – Oracle, 2015. – 1306 с.;

7. Кореньков, В. В. История развития технологий мониторинга информационных систем / В. В. Кореньков, А. В. Ужинский // Системный анализ в науке и образовании. - 2007. - №1. - С. 36-49;

8. Олифер, Н. А. Средства анализа и оптимизации локальных сетей [Электронный ресурс] / Н. А. Олифер, Н. Г. Олифер. - М.: Центр Информационных Технологий, 1998;

9. Лавров, А. А. Мониторинг и администрирование в корпоративных вычислительных сетях: монография / С. А. Ивановский, А. А. Лавров, В. В. Яновский. - СПб.: Изд-во «СПбГЭТУ «ЛЭТИ», 2013 - 160 с;

10. Шыхалиев, Р. Г. О применении интеллектуальных технологий в мониторинге компьютерных сетей / Р. Г. Шыхалиев // Informasiya Texnologiyalan Problembri. - 2011. - №2. - С. 82-90;

11. 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. - С. 102-106;

12. Ермаков, А. В. Использование сетевого сканера для повышения защищенности корпоративной информационно-вычислительной сети / А. В. Ермаков. - М., 2001. - 16 с. (Препринт / Институт прикладной математики им. М. В. Келдыша РАН; №61).

REFERENCES:

1. Veysset, F. New Tool And Technique For Remote Operating System Fingerprinting / F. Veysset, O. Courtay, O. Heen. - Intranode Software Technologies, 2002.- 13 s;

2. Lavrov, A. A. Metod identifikacii OS udalennogo hosta na osnove analiza vremennyh harakteristik steka TSRLR v zadachah setevogo monitoringa / A. A. Lavrov, A. K. Bol'shee // Sb. tr. 64-j nauch.-tehn. konf. prof.-prep. sostava SPbGJeTU «LJeTI» - SPb, 2011. - S. 104-110;

3. Oracle Database Reference 11g Release2 (11.2) E40402-18 [Tekst] // Bert Rich – Oracle, 2015. – 1306 c.;

4. Lavrov, A.A. Identifikacija operacionnoj sistemy udalennogo hosta metodami analiza vremennyh harakteristik / A.A. Lavrov, V.V. Janovskij // Izvestija SPbGJeTU «LJeTI». - 2011. - №3. - S. 34-39;

5. Beardsley, T.A. Intrusion Detection and Analysis: Theory, Techniques, and Tools / T. A. Beardsley. - SANS Lone Star, 2002. - 70 s.;

6. Oracle Database Reference 11g Release2 (11.2) E40402-18 [Tekst] // Bert Rich – Oracle, 2015. – 1306 c.;

7. Koren'kov, V.V. Istorija razvitija tehnologij monitoringa informacionnyh sistem / V.V. Koren'kov, A. V. Uzhinskij // Sistemnyj analiz v nauke i obrazovanii. - 2007. - №1. - S. 36-49;

8. Olifer, H.A. Sredstva analiza i optimizacii lokal'nyh setej [Jelektronnyj resurs] / N.A. Olifer, N.G. Olifer. - M.: Centr Informacionnyh Tehnologij, 1998;

9. Lavrov, A.A. Monitoring i administrirovanie v korporativnyh vychislitel'nyh setjah: monografija / S.A. Ivanovskij, A.A. Lavrov, V.V. Janovskij. - SPb.: Izd-vo «SPbGJeTU «LJeTI», 2013 - 160 s.;

10. Shyhaliev, R. G. O primenenii intellektual'nyh tehnologij v monitoringe komp'juternyh setej / R. G. Shyhaliev // Informasiya Texnologiyalan Problembri. - 2011. - №2. - S. 82-90;

11. Lavrov, A.A. Algoritmy klassifikacii v zadache identifikacii versii OS udalennogo setevogo uzla / A.A. Lavrov // Sb. tr. 65-j nauch.-tehn. konf. prof.-prep. sostava SPbGJeTU «LJeTI». - SPb., 2012. - S. 102-106;

12. Ermakov, A.V. Ispol'zovanie setevogo skanera dlja povyshenija zashhishhennosti korporativnoj informacionno-vychislitel'noj seti / A. V. Ermakov. - M., 2001. - 16 s. (Preprint / Institut prikladnoj matematiki im. M. V. Keldysha RAN; №61).

Без рецензії.

Железняк В.В., д.т.н., проф. Мясищев А.А., д.т.н., проф. Ленков С.В., Селюков Д.А.

АНАЛИЗ МЕТОДОВ И АЛГОРИТМОВ МОНИТОРИНГА ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

В статье рассматриваются существующие методы и алгоритмы идентификации операционных систем, основанные на анализе значений RTO (Retransmission Timeouts),, используемых стеком протоколов TCP / IP, которые являются основой для построения и функционирования систем мониторинга вычислительных сетей. Показаны основные свойства, преимущества и недостатки данных методов, которые позволяют специалисту повисит эффективность своей работы на этапе реализации и эксплуатации контролируемых информационных систем.

В настоящее время отсутствуют совершенные алгоритмы мониторинга вычислительных сетей, основанные на анализе временных закономерностей в работе стека протоколов TCP / IP. В связи с этим возникает проблема функционирования информационной сети. Задачей является разработка эффективных средств мониторинга и диагностики информационных систем. Широкое распространение систем сетевого мониторинга в корпоративных информационных системах приводит к необходимости уделять активное внимание решению присущих им проблем бесперебойного функционирования. При этом существующие определенные средства для получения качества работы сети.

Проведенный анализ методов мониторинга и алгоритмов, направленных на определение идентификатора операционной системы дает нам возможность более быстро оценивать уровень работоспособности сети и точность (достоверность) результирующего предположение о версии ОС целевого узла.

Ключевые слова: системы сетевого мониторинга, информационные системы, идентификатор операционной системы

Zheliezniak V.V., prof. Myasischev O.A., prof. Lenkov S.V., Selyukov D.O.

ANALYSIS OF METHODS AND ALGORITHMS OF MONITORING OF COMPUTER NETWORKS

The article considers existing methods and algorithms of identifying operating systems based on the analysis of RTO (Retransmission Timeouts), values which used for the TCP / IP protocol stack, which are the basis for the construction and operation of computer monitoring systems. There are shown the basic properties, advantages and disadvantages of these methods which allow the expert to increase the efficiency of his work at the stage of implementation and operation of controlled information systems.

At the moment, there are no perfect algorithms for monitoring the networks which based on the analysis of time patterns in TCP / IP protocol stack operation. In connection with this appeared the problem of functioning of the information network. The task is to develop effective means of monitoring and diagnosing information systems. The widespread distribution of network monitoring systems in corporate information systems leads to the need to pay close attention to solving their inherent problems of uninterrupted functioning. At the same time, there are certain means available to obtain the quality of the network.

The monitoring of analysis methods and algorithms aimed at identifying an operating system identifier allows us to more quickly evaluate the network performance and the accuracy (reliability) of the resulting assumption about the version of the operating system of the target node.

Keywords: network-monitoring systems, information systems, operating system identifier.