МОНІТОРИНГ МЕРЕЖЕВОГО ТРАФІКУ ПРОМИСЛОВОЇ МЕРЕЖІ ETHERCAT

Коломійчук Д. С., Крапівний Ю. М.
Одеський національний університет І.І. Мечникова

Робота присвячена розробці сніфера на основі бібліотек WinPcap та packet.dll для моніторингу пакетів EtherCAT в EtherNet-мережі. EtherCAT представлена компанією Beckhoff в 2003 як промислова шина, заснована на мережі Ethernet. Дана технологія поєднує високу продуктивність, гнучкість конфігурації і надійність з низькою вартістю апаратних засобів, що дозволяє створювати високоефективні розподілені системи контролю і управління [1,2].

Аналіз трафіку дуже важливий процес для програмістів та мережевих адміністраторів, особливо при розробці розподілених систем. Для моніторингу трафіку використовують сніфер. Це програма призначена для перехоплення та подальшого аналізу. Отриманий аналіз дозволяє:

- відслідковувати протокол обміну між MASTER і SLAVE пристроями;
- виявити шкідливе програмного забезпечення, такі як троянські програми, мережеві сканери, флудери;
- виявити вірусний, паразитний та закільцьований трафік через який навантажується мережа;
- локалізувати помилку конфігурації мережних агентів;
- перехопити незашифрований трафік призначений для користувача з метою отримання інформації та паролів.

WinPcap - низькорівнева бібліотека 32-бітних Windows систем, для взаємодії с мережевими драйверами інтерфейсів. Завдяки їй можна захоплювати та передавати мережеві пакети в обхід стека протокола.

Бібліотека packet.dll - це динамічно завантажуюча бібліотека, за допомогою якої додаток користувача взаємодіє з драйвером захоплення пакетів. Функції бібліотеки призначені для спрощення процесу взаємодії з драйвером і забезпечують виконання таких операцій, як одержання дескрипторів мережевих адаптерів, прийом і передачу пакетів по мережі, установку буферів і фільтрів драйвера і т.д. [3]

Відомими аналогами систем моніторингу мережевого трафіку є:

- Wireshark - програма з розвиненим графічним інтерфейсом для захоплення і аналізу мережевих даних.
- The Bro IDS - моніторинг мережі.
- tcpdump – моніторинг мережі.

Практично все, що пов'язано з отриманням і передачею даних в мережі, може бути швидко ідентифіковано і виправлено завдяки даним, отриманим за допомогою розробленого сніфера.

Література

1. EtherCAT – технология будущего. / Control Engeneering Россия - Сентябрь 2007.-2007.-С.28-29.
2. Beckhoff EtherCAT Slave Controller. Section I – Technology. [Електронний ресурс] - Режим доступу: https://download.beckhoff.com/download/Document/io/ethercat-development-products/ethercat_esc_datasheet_sec1_technology_2i3.pdf
3. А.Волков, В.Семенов. Архитектура захвата пакетов для Windows WinPCAP: бальзам на душу хакера или панацея для программиста? [Електронний ресурс] - Режим доступу: http://cherepovets-city.ru/insecure/reading/papers/packet_dll.htm