Захист DHCP сервера в мережі підприємства

Сергій Сапанович[1], Віталій Мартовицький[2]

1. Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА, г. Харків, пр. Науки, 14, E-mail: serhii.sapanovych@nure.ua

2. Кафедра електронних обчислювальних машин, Харківський національний університет радіоелектроніки, УКРАЇНА, г. Харків, пр. Науки, 14, E-mail: vitalii.martovytskyi@nure.ua

This paper addresses the basic network security issues at the OSI link layer network. Different types of attacks on local computer networks are analyzed, as well as modern methods of their detection and prevention. The most promising areas for intrusion detection systems based on the use of Cisco Catalyst Switches are offered.

Ключові слова – інформаційні системи, мережа, Cisco Systems, DHCP, security, ARP.

I. Вступ

У сучасних локальних мережах обмін інформацією, як правило, передбачає передачу даних через комутатор. Тому сам комутатор і протоколи, які використовують комутатори можуть бути метою атак. Більш того, деякі настройки комутаторів (як правило, це налаштування за замовчуванням) дозволяють виконати ряд атак і отримати несанкціонований доступ до мережі або вивести з ладу мережеві пристрої. Однак, комутатор може бути і досить потужним засобом захисту. Так як через нього відбувається все взаємодії в мережі, то логічно контролювати це на ньому. Звичайно, використання комутатора як засобу захисту передбачає, що використовується не найпростіший комутатор 2-го рівня, а комутатор з відповідними функціями для забезпечення безпеки. В даній доповіді проведемо аналіз безпеки комутатора Cisco Catalyst 2960, використовуючи додаткові вбудовані функції, для забезпечення необхідних політик безпеки мережі.

II. Основний матеріал

Розглянемо докладніше функції комутаторів Cisco Catalyst для забезпечення безпеки мережі. Список їх наведено в табл. 1.

IP Source Guard (Dynamic IP Lockdown) – функція комутатора, яка обмежує IP-трафік на інтерфейсах 2-го рівня, фільтруючи трафік на підставі таблиці прив'язок DHCP snooping і статичних відповідностей. Функція використовується для боротьби з IP-spoofingом.

Port security – функція комутатора, що дозволяє вказати MAC-адреси хостів, яким дозволено передавати дані через порт. Після цього порт не передає пакети, якщо MAC-адресу відправника не вказано як дозволену. Крім того, можна вказувати не конкретні MAC-адреси, дозволені на порту комутатора, а обмежити кількість MAC-адрес, яким дозволено передавати трафік через порт. Використовується для запобігання [1]:

− несанкціонованої зміни MAC-адреси мережевого пристрою або підключення до мережі;

– атак спрямованих на переповнення таблиці комутації.

DHCP snooping – функція комутатора, призначена для захисту від атак з використанням протоколу DHCP. Наприклад, атаки з підміною DHCP- сервера в мережі або атаки DHCP starvation, яка змушує DHCP-сервер видати всі існуючі на сервері адреси зловмисникові. DHCP snooping регулює тільки повідомлення DHCP і не може вплинути безпосередньо на трафік користувачів або інші протоколи. Деякі функції комутаторів, що не мають безпосереднього відношення до DHCP, можуть виконувати перевірки на підставі таблиці прив'язок DHCP snooping (DHCP snooping binding database).

Для правильної роботи DHCP snooping, необхідно вказати які порти комутатора будуть довіреними (trusted), а які - ні (untrusted, в подальшому - ненадійними) [2]:

Ненадійні (Untrusted) – порти, до яких підключені клієнти. DHCP- відповіді, що приходять з цих портів відкидаються комутатором.

ТАБЛИЦЯ 1

Функції комутаторів для забезпечення безпеки роботи мережі на канальному рівні

Функція комутатора	Від яких атак захищає
Port security	Переповнення таблиці комутації, несанкціонована зміна MAC-адреси
DHCP Snooping	Підміна DHCP-сервера в мережі, DHCP starvation
Dynamic ARP Inspection	ARP-spoofing
IP Source Guard	IP-spoofing

Для ненадійних портів виконується ряд перевірок повідомлень DHCP і створюється база даних прив'язки DHCP (DHCP snooping binding database).

Довірені (Trusted) – порти комутатора, до яких підключений інший комутатор або DHCP-сервер. DHCP-пакети отримані з довірених портів, не відкидаються.

За замовчуванням комутатор відкидає DHCP-пакет, який прийшов на ненадійний порт, якщо:

– приходить одне з повідомлень, які відправляє DHCP-сервер (DHCPOFFER, DHCPACK, DHCPNAK або DHCPLEASEQUERY);

– приходить повідомлення DHCPRELEASE або DHCPDECLINE, в якому міститься MAC-адресу з бази даних прив'язки DHCP, але інформація про інтерфейс в таблиці не збігається з інтерфейсом, на якому був отриманий пакет;

– у DHCP-пакеті, що прийшов, не збігаються MAC-адреса, вказана в DHCP-запиті, і MAC-адреса відправника;

– приходить DHCP-пакет, в якому є опція 82.

Dynamic ARP Inspection – функція комутатора, призначена для захисту від атак з використанням протоколу ARP [3]. Наприклад, атаки ARP-spoofing, що дозволяє перехоплювати трафік між вузлами, які розташовані в межах одного широкомовного домену. Dynamic ARP Inspection регулює тільки повідомлення протоколу ARP і не може вплинути безпосередньо на трафік користувачів або інші протоколи.

Для правильної роботи Dynamic ARP Inspection, необхідно вказати які порти комутатора будуть довіреними (trusted), а які – ні (untrusted) [10]:

– ненадійні (Untrusted) – порти, до яких підключені клієнти. Для ненадійних портів виконується ряд перевірок повідомлень ARP.

– довірені (Trusted) – порти комутатора, до яких підключений інший комутатор. Повідомлення протоколу ARP отримані з довірених портів, не відкидаються.

Якщо порт ненадійний, комутатор перехоплює все ARP-запити і ARP- відповіді на ненадійних портах перш ніж перенаправляти їх. Комутатор перевіряє відповідність MAC-адреси IP-адресі на ненадійних портах. Перевірка відповідності MAC-адреси IP-адресі може виконуватися на підставі статичних записів або бази даних прив'язки DHCP.

Висновки

У роботі розглянуті основні проблеми, пов'язані з безпекою мереж на канальному рівні моделі OSI. Проаналізовано різні типи атак на локальні комп'ютерні мережі, а також сучасні методи їх виявлення і попередження. Запропоновано найбільш перспективні напрямки розвитку систем виявлення вторгнень, засновані на використанні вбудованих функцій безпеки комутаторів Cisco Catalyst.

Також показано, що без використання вбудованих функцій безпеки комутаторів всі атаки, при невеликих витратах часу, дозволили домогтися бажаного ефекту (відмова в обслуговуванні/перехоплення інформації). Після детальної настройки захисних функцій атаки виявилися абсолютно неефективними. Окремі сценарії мережевих атак, а також механізми їх виявлення були реалізовані програмно за допомогою засобів мережевого емулятора Cisco Packet Tracer 5.3.2.

Література

[5] Брюс Александер, Тони Аллен, Матт Карлинг и др. Руководство по технологиям объединенных сетей Cisco. Изд. 4-е. – М.: Издательский дом «Вильямс», 2005. – 1040 с.: ил.

[6] Официальный сайт Cisco Systems. Программа Cisco Packet Tracer [Електроний ресурс]. Режим доступу: http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html.

[7] Джеймс Бони. Руководство по Cisco IOS. – СПб.: Питер, М: Издательство «Русская редакция», 2008. – 784 с.: ил.