УДК 004.7

АТАКИ ТИПУ «VLAN HOPPING»

VLAN HOPPING ATTACKS

Оксана Жигаревич, Богдан Корольов

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

Abstract. *VLAN hopping is an attack method allowing a host in one VLAN to access traffic in other VLANs. The two main techniques are switch spoofing and double tagging. Switch spoofing involves emulating a trunking switch to access multiple VLANs. Double tagging involves adding two VLAN tags to a frame to bypass VLAN isolation. Proper switch port configuration can mitigate these attacks.*

VLAN hopping – це метод атаки на мережеві ресурси у віртуальній локальній мережі (VLAN). Основна концепція всіх VLAN hopping атак полягає в тому, щоб атакуючий хост, находячись у одному VLAN-і отримав доступ до трафіку в інших VLAN-ах, який зазвичай був би недоступний. Існує два основні методи VLAN hopping атак: спуфінг комутатора (switch spoofing) та подвійне тегування (double tagging). Обидва методи атак можна усунути за допомогою належної конфігурації портів комутатора.

Під час атаки switch spoofing атакуючий хост імітує транкінговий комутатор, озвучуючи протоколи тегування та транкінгу (напр. Multiple VLAN Registration Protocol, IEEE 802.1Q, Dynamic Trunking Protocol), які використовуються для підтримки VLAN. Трафік для кількох VLAN-ів таким чином стає доступним для атакуючого хоста. Спуфінгом комутатора можна скористатися лише тоді, коли інтерфейси налаштовані на узгодження транка. Щоб запобігти цій атаці, необхідно скористатися одним із наступних методів. Переконайтеся, що порти не налаштовані на автоматичне узгодження транків, вимкнувши прокол DTP (Dynamic Trunking Protocol). Переконайтеся, що порти, які не призначені бути транками, явно налаштовані як порти доступу (access ports).

Під час атаки подвійного тегування зловмисник, підключений до порту з підтримкою 802.1Q, додає два теги VLAN до кадру, який він передає. Кадр (зовнішньо позначений ідентифікатором VLAN, членом якого дійсно є порт зловмисника) пересилається без першого тегу, оскільки це native VLAN транкового інтерфейсу. Другий тег стає видимим для другого комутатора, який зустрічає кадр. Цей другий тег VLAN вказує, що кадр призначено для цільового хоста на другому комутаторі. Потім кадр надсилається на цільовий хост так, ніби він і знаходиться у цільовому VLAN, фактично обходячи мережеві механізми, які логічно ізолюють VLAN-и один від одного. Однак можливі відповіді цільового хоста не можуть бути надіслані назад на атакуючий хост. Подвійне тегування можна використовувати лише на портах комутатора, налаштованих на використання native VLAN. Транкові порти, налаштовані на native VLAN, не застосовують тег VLAN під час надсилання кадрів. Це дозволяє наступному комутатору прочитати підроблений тег VLAN зловмисника. Щоб запобігти подвійному тегуванню можна скористатися будь-яким з наступних методів. Не розміщуйте жодних хостів у VLAN 1 (VLAN за замовчуванням), тобто призначте VLAN доступу, відмінний від VLAN 1, кожному порту доступу. Змініть native VLAN на всіх транкових портах на невикористовуваний VLAN ID. Застосовуйте явне тегування native VLAN на всіх транкових портах.

Бібліографія

1. VLAN Hopping - N10-008 CompTIA Network+ : 4.2 - Professor Messer IT Certification Training Courses. *Professor Messer IT Certification Training Courses*. URL: http://www.professormesser.com/network-plus/n10-008/n10-008-video/vlan-hopping-n10-008/ (дата звернення: 01.06.2024).
2. TechKnowSurge. CCNA Practical 10-4: VLAN Hopping, 2022. *YouTube*. URL: https://www.youtube.com/watch?v=a6yVV6dD6F0 (дата звернення: 01.06.2024).