УДК 004

Дзядек М.І. студент гр. 125-20-2
Науковий керівник: Олішевський І.Г., асистент кафедри БІТ
(Національний технічний університет "Дніпровська політехніка", м. Дніпро, Україна)

РОЗГОРТАННЯ МЕРЕЖІ MESH ТА ТЕСТУВАННЯ СИСТЕМИ НА ПРОНИКНЕННЯ

Mesh-система - це безшовна передача трафіку. За цією технологією будують бездротові мережі, у яких немає чіткої централізації, кожен вузол працює незалежно від інших. В результаті зберігається висока швидкість інтернет-зв'язку, і для користувача зникає необхідність постійно перемикатися на іншу точку доступу Wi-Fi, коли сигнал основної мережі стає слабкий.

Було взято участь в дослідженні в навчальному корпусі кафедри військової підготовки. Мета дослідження – розгортання безшовної мережі для всього корпусу, та тестування системи на проникнення. Для розгортання мережі Mesh у корпусі, який складається з двох поверхів, було використано обладнання Keenetic Viva як транслятор сигналу, та два маршрутизатори Keenetic Speedster як сателіти. До транслятора під’єднано кабелі електроживлення та Ethernet. Для базових налаштувань маршрутизатора, а саме для задання SSID, паролю та введення налаштувань провайдера і задання налаштувань безпеки було виконано вхід на сторінку керування пристроєм за адресою my.keenetic.net та задано необхідні параметри. Після налаштувань Host-маршрутизатора, було під’єднано до електромережі маршрутизатор, який буде виконувати роль ретранслятора сигналу, під’єднано кабелем Ethernet до інтернету. Для введення маршрутизатора у режим ретрансляції, на сторінці налаштувань було обрано необхідний режим роботи. Таким самим чином зроблено підключення та налаштування другого сателіту. На сторінці налаштувань Host-маршрутизатора з'явилися для "захоплення" та додання їх до модульної (Mesh) системи два роутери Keenetic Speedster, які ми використали в ролі ретрансляторів сигналу. Після захоплення обох сателітів до однієї мережі, в налаштуваннях було видано назви роутерам-ретрансляторам згідно з аудиторіями, в яких розташоване обладнання.

Після перезавантаження Host-маршрутизатора для збереження та застосування нових налаштувань, було проведено базове тестування працездатності створеної модульної системи. Для цього було проведено тестування сигналу в різних точках корпусу, обриву не сталося. Виміряно швидкість з'єднання, показники стабільні під час вимірювання на різних локаціях. Проведено аналіз журналу логів Mesh, який показує час та MAC-адресу пристрою, який під’єднався до будь-якого маршрутизатору чи від'єднався від нього, під’єднавшись до іншого сателіту всередині Mesh-системи. Збережені дані точно показують підключення пристрою до трьох різних маршрутизаторів (Host-роутеру та двох сателітів) під час вимірювання швидкості з'єднання в різних локаціях корпусу, що являє собою стабільність та повну працездатність розгорнутої мережі.

Для тестування мережі на проникнення використано систему Kali Linux та необхідні для цього інструменти. Перша атака на проникнення методом грубої сили була неуспішна, програма завершила перебір словника з паролями та не підібрала той, який потрібен для доступу до мережі. Слід зазначити, що налаштування обладнання Keenetic дозволяють встановити ряд обмежень для пристроїв, які не були вручну підтверджені адміністратором, і тому навіть після успішного підбору паролю, нанести шкоду мережі або перехопити дані можливості не буде. Після проведеної атаки методом грубої сили, було проведено ще ряд атак, такі як автоматизована атака на WPS

(неуспішна через вимкнення технології WPS при базовому налаштуванні), атака на Handshake-файли (неуспішна через використання механізму WPA3-Enterprise для захисту розгорнутої мережі, який використовує 192-бітне шифрування даних), атака на DNS (неуспішна через підключення протоколів, які шифрують DNS-запити).

Для усіх тестів було використано такі утиліти як Aircrack-ng, Reaver, Wifite, Crunch, які реалізовані безпосередньо в Kali Linux. Результат тестування на проникнення успішний, розгорнута система є безпечною, всі атаки були невдалими через те, що обладнання Keenetic дозволяє використовувати останні технології для захисту бездротової мережі. Окрім використання технологій захисту системи, при налаштуванні Host-маршрутизатора обрані необхідні параметри безпеки та конфіденційності, такі як вимкнення технології WPS, приховування SSID, встановлення стійкого до підбору паролю, налаштування дозволів незареєстрованим пристроям.

Висновок. Mesh-мережа має багато переваг у порівнянні з іншими способами розгортання мережі для великих приміщень (репітери сигналу, додаткові точки доступу тощо):

- Стабільність. При переміщенні пристрою по будівлі не втрачається сигнал інтернету при зміні його джерела.
- Швидкодія. Завдяки багатоканальній системі досягається виняткова швидкість передачі даних.
- Децентралізація. Бездротова мережа не припине функціонування у разі збою одного з модулів.
- Швидкість налаштування. Для завдання параметрів усієї мережі достатньо налаштувати Host-маршрутизатор, на відміну від використання додаткових точок доступу, де потрібно налаштовувати кожен маршрутизатор окремо.

Високі показники безпеки досягаються завдяки правильності налаштування та великому переліку технологій, які доступні на обладнанні Keenetic для забезпечення безпеки розгорнутої мережі.

Перелік посилань

1. Keenetic. Руководство пользователя. Mesh Wi-Fi [Електронний ресурс].- Режим доступу: https://help.keenetic.com/hc/ru/articles/360007279039?utm_source=webhelp&utm_campaign=3.08.C.5.0-1&utm_medium=ui_notes&utm_content=controlpanel/wifisystem

2. Keenetic. Руководство пользователя. Организация Wi-Fi системы [Електронний ресурс].- Режим доступу: https://help.keenetic.com/hc/ru/articles/360002155079

3. Актуальные техники взлома Wi-Fi [Електронний ресурс].- Режим доступу: https://spy-soft.net/wifi-hacking/