Важливим етапом захисту комп'ютерної мережі є її захист по периметру, тобто мережа повинна ідентифікувати всі свої кінцеві пристрої, як дротові так і бездротові.

Існує два основних варіанти налаштування бездротової мережі:

– Ad-hoc - передача безпосередньо між пристроями;

– Hot-spot - передача здійснюється через точку доступу;

В Hot-spot мережах присутня точка доступу, за допомогою якої відбувається не тільки взаємодія всередині мережі, але і доступ до зовнішніх мереж. Hot-spot представляє найбільший інтерес з точки зору захисту інформації, бо зламавши точку доступу, зловмисник може отримати інформацію не тільки зі станцій, розміщених в даній бездротовій мережі.

Одним із методів обмеження доступу до мережі є фільтрація MAC-адреси: Фільтрацію можна здійснювати трьома способами:

– Точка доступу дозволяє отримати доступ станціям з будь-якою MAC-адресою;

– Точка доступу дозволяє отримати доступ тільки станціям, чиї MAC-адреси знаходяться в довірчому списку.

Найбільш надійним з точки зору безпеки є другий варіант, хоча він не розрахований на підміну MAC-адреси, що легко здійснити зловмисникові.

Список використаних джерел:

1. Воробієнко П. П. Телекомунікаційні та інформаційні мережі : Підручник / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, 2010. – 708 с.: іл.

д.т.н., с.н.с. Комарова Л.О. (ОНАЗ)
к.т.н. Кльоц Ю.П. (ХмНУ)
Брітов О.В. (ХмНУ)
Нагребецький О.В. (ХмНУ)
Шаховал Є.С. (ХмНУ)

Тестування обладнання корпоративної мережі

Корпоративні мережі є подальшим етапом розвитку локальних мереж, однак специфіка їх побудови та використання значно відрізняються як від локальних так і від глобальних чи регіональних мереж. Вони характеризуються обмеженим розміром, як локальні мережі та розподілом на підмережі, як глобальні чи регіональні мережі.

Оскільки до корпоративних мереж висуваються більш жорсткі вимоги до обсягів даних, що передаються мережею, захисту цих даних та надійності інфраструктури, важливим етапом підтримання функціонування корпоративної мережі є тестування обладнання, на базі якого збудована мережа.

Процес тестування мережевого обладнання в загальному використовує стек протоколів TCP/IP та складається з двох етапів. Перший – встановлення типів обладнання та зв'язків між ними (Neighbor Discovery Protocol). Другий – безпосередньо тестування мережевого обладнання. Для корпоративної мережі

характерно наявність проекту мережі та відсутність хаотично встановленого обладнання. Навпаки наявність активного мережевого обладнання, що не встановлено у відповідності до проекту є ознакою втручання в роботу мережі та повинно виявлятись на етапі тестування мережі.

При побудові тестів для перевірки справності та коректності налаштування обладнання корпоративної мережі необхідно вирішити наступні задачі:

1. Перевірка доступності активного вузла комутації.
2. Перевірка доступності вузла маршрутизації.
3. Перевірка доступності інших вузлів сегменту підмережі.
4. Перевірка доступності вузлів інших сегментів мережі.
5. Пошук стороннього обладнання в межах сегменту.
6. Перевірка доступності заборонених для доступу сегментів мережі.

Виконання цих задач необхідно проводити шляхом передачі пакетів TCP/IP вузлам мережі. Отримання чи не отримання переданих даних, а також використання протоколу NDP для пошуку сусідніх вузлів дозволить провести тестування обладнання, що в освою чергу дозволить зробити висновок про справність чи несправність обладнання та відповідність реальної топології мережі проектованій.

Список використаних джерел:

1. Jason Edelman Network Programmability and Automation: Skills for the Next-Generation Network Engineer / Jason Edelman, Scott Lowe, Matt Oswalt. – O'Reilly Media; 1st Edition (March, 2018). – 584p.

Корчак Ю.О.(ВІКНУ)
Гритчук М.Д. (УЗО та МТЗ СП КСП)
Ковба М.В.(НАСВ)

Інженерне забезпечення – один із видів оперативного (бойового) забезпечення АТО (ООС)

Досвід попередніх війн, динамічні зміни в способах ведення бойових дій у ході збройного конфлікту на сході країни, висувають нові, більш високі вимоги до виконання завдань інженерного забезпечення, розширюють їх зміст, вимагають удосконалення способів і прийомів їх виконання.

Успішне виконання бойових завдань частинами і підрозділами Збройних Сил не можливе без всебічного забезпечення, тим більше без такого важливого виду бойового забезпечення, як інженерне, що організовується з метою своєчасного та прихованого розгортання військ (сил), проведення ними маневру, створення необхідних умов для успішного виконання поставлених завдань, підвищення рівня захисту військ (сил) та об’єктів від засобів ураження противника, завдання противнику втрат та ускладнення його дій.

За період проведення АТО (ООС) основні зусилля з інженерного забезпечення були зосереджені на виконанні завдань інженерного забезпечення ізоляції кризового району на сході України, забезпеченні підготовки та ведення бойових дій, а саме: фортифікаційному обладнанні