Єфіменко А.А., к.т.н.,
Власюк О.К., студ. 4-го курсу,
Житомирський державний технологічний університет

ПРОГРАМНИЙ ЕМУЛЯТОР АТАК НА ВІДМОВУ DHCP-СЕРВЕРА ЛОКАЛЬНОЇ МЕРЕЖІ ETHERNET

Якісне оволодіння фахівцем сучасними принципами та методами забезпечення безпеки інформації в комп'ютерних мережах неможливе без набуття відповідних практичних навичок. Отримати навички налагодження штатних засобів захисту інформації комунікаційного обладнання та операційних систем можна досить легко. У той же час досить складно виконати моніторинг і аналіз їх роботи під час проведення мережних атак. Це зумовлено тим, що засоби для проведення атак є важкодоступними або для певних систем взагалі не розроблені.

Одним із важливих сервісів, функціонування якого необхідно забезпечити у неперервному, а значить в захищеному режимі, є клієнт-серверний сервіс динамічного керування параметрами адресації кінцевих вузлів DHCP. Як правило, головною метою при проведенні атаки на DHCP-сервіс є виведення з ладу DHCP-сервера мережі. Архітектурні особливості реалізації DHCP-серверів дають змогу проводити на нього наступні мережні атаки:

– DHCP DoS (відмова в обслуговуванні DHCP);
– DHCP Starvation/Exhaustion (виснаження DHCP-набору адрес);
– DHCP Release (фальшиве інформування DHCP-сервера про звільнення IP-адреси вузлом);
– DHCP Server Spoofing/Rogue DHCP Server (фальшивий DHCP-сервер мережі).

Найвідомішими засобами для проведення мережних атак на DHCP-сервери є програмні продукти Gobbler та Yersinia. На жаль вони реалізовані лише для ОС Unix/Linux. Процедури їх інсталяціїта використання є досить складними. Дослідження функціональності Gobbler та Yersinia показало наступне: інтерфейси командного рядка вказаних програмних продуктів є досить складними; дані засоби дають змогу відносно легко проводити окремі прості атаки на DHCP-сервер; організація комплексної атаки або серії атак з використанням даних засобів є дуже складним процесом, вимагає значних часових затрат і не завжди призводить до кінцевого результату через внутрішні програмні помилки. На основі даного висновку було прийнято рішення розробити власний програмний емулятор, який би давав змогу легко проводити як прості, так і складні комплексні атаки.

На початковому етапі розробки головним завданням було виконати атаку на відмову у функціонуванні DHCP-сервера. Найпростішим варіантом такої атаки є атака DHCP DoS, яка реалізовується шляхом надсилання тільки DHCP-запитів до DHCP-сервера з метою отриманні параметрів адресної інформації. Реалізація цієї атаки показала наступне: DHCP-сервер резервує для призначення клієнтам IP-адреси з набору адрес і в певний момент часу цей набір вичерпується, але у складі DHCP-сервера наявні засоби, які контролюють процес видачі, і у випадку непідтвердження отримання адресної інформації з боку клієнта ознака резервування знімається та адреси знову можуть використовуватися для легальної видачі. Тобто, результат проведення атаки – повне виведення з ладу DHCP-сервера не є сталим, сервер може відновити своє нормальне функціонування.

Для досягнення мети було вирішено реалізувати комплексну атаку DHCP DoS, яка б надавала можливість отримати сталий результат. Для цього було обрано наступний підхід – поетапне виконання атаки. Етап I – виконання атаки DHCP Release з метою повного вивільнення набору IP-адрес за рахунок надсилання некоректної інформації DHCP-серверу. Етап II – виконання модифікованої атаки DHCP DoS – атаки DHCP Starvation, яка за рахунок надсилання відповідних підтверджень забезпечує постійній видачі параметрів IP-адресації на боці сервера. Тестування такої комплексної атаки показало досягнення поставленої мети – DHCP-сервер повністю відмовлявся обслуговувати DHCP-клієнтів.

Як засіб для програмної реалізації емулятора було обрано середовище Visual Studio, мову C# та бібліотеки SharpPcap. Тестування виконання окремих атак, як складових комплексної атаки, та комплексної атаки в цілому здійснювалося у середовищах моделювання GNS3, eNSP, H3C Cloud Lab при умовах використання як DHCP-серверів маршрутизаторів різних виробників. Також тестування було проведено в умовах реальної мережі, побудованої на базі обладнання Cisco. Результати тестування показали 100% ефективність реалізованої атаки на відмову.

У подальшому планується удосконалення програмного емулятора за рахунок реалізації адаптивного сценарного підходу до виконання атак та реалізації компонентів емулятора, які будуть орієнтовані на обхід штатних засобів захисту від атак на DHCP-сервер, додавання можливості реалізації атак у Wi-Fi мережах, створення кросплатформенної версії програмного продукту.