УДК 681.3.067

Єфіменко А.А., к.т.н., доц.,
Зозуля Я.В., студ.,
Житомирський військовий інститут
Державного університету телекомунікацій

МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ АТАК НА ПРИСТРОЇ КАНАЛЬНОГО РІВНЯ КОМУТОВАНИХ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Безпеку канального рівня можна вважати синонімом безпеки локальної комп'ютерної мережі. Як правило, при атаках на канальному рівні вважається, що зловмисник або вже знаходиться у мережі, або наявний деякий посередник, що навмисно або ненавмисно сприяє виконанню атаки. Завданням зловмисника є отримання доступу до певних ресурсів або, як мінімум, порушення нормальної роботи мережі. Проблема безпеки канального рівня полягає у тому, що успішна атака на канальному рівні створює передумови подолання засобів захисту більш високих рівнів. Залежно від результату, який буде отриманий, атаки можна поділити на такі типи: людина посередині; відмова в обслуговуванні; несанкціонований доступ до ресурсів мережі або її частини; порушення нормального функціонування мережі або її частини.

До основних атак канального рівня локальних мереж можна віднести наступні види атак: 1) атаки на функції комутатора; 2) атаки на протокол STP; 3) атаки на протокол DHCP; 4) атаки на протокол ARP. Всі ці атаки використовують особливості функціонування пристроїв та мережевих протоколів.

Серед атак першого виду слід виділити атаки «MAC Flooding», «MAC Spoofing», «Flow Control». Сенс «MAC Flooding» полягає у постійному заповненні всієї таблиці комутації випадковими MAC-адресами, що перетворює комутатор у концентратор, і в результаті мережа заповнюється надлишковим трафіком. Сенс MAC Spoofing полягає у підміні адреси існуючого вузла адресою зловмисником. Зміна MAC-адресу на мережевій карті зловмисника на MAC-адрес жертви примусить комутатор відправляти на порт, до якого приєднаний зловмисник, пакети, які до цього зловмисник бачити не міг, тобто відбуватиметься комутація кадрів на некоректний порт. Сенс Flow Controlполягаєу використанні можливості комутатора керувати потоком даних; можна здійснити атаку, шляхом затоплення мережі кадрами, що генерує функція Flow Control (Pause Frame), які сповіщають обладнання мережі про те, що потрібно заборонити прийом та передачу кадрів, як результат – взаємодія пристроїв припиняється.

До атак на протокол STP належать «Передача Hello BPDU», «Передача TCN BPDU», «Отримання ролі кореневого комутатора». Сенс атаки «Передача Hello BPDU» полягає уотриманніBPDU з меншим ідентифікатором, що примушує комутатори здійснювати перерахунок дерева топології. Відповідно, якщо через певний проміжок часу посилати фальшиві Hello BPDU пакет, то мережа буде недоступною. Сенс атаки «Передача TCN BPDU» полягає у наступному:пакети TCN BPDU використовують для анонсування змін в топології мережі. Після кожної зміни відбувається перерахунок топології і мережа є недоступною. Дана атака схожа на попередню, лише змінюється тип пакету. Сенс атаки «Отримання ролі кореневого комутатора» полягає в наступному:оскільки протокол STP не забезпечує механізм аутентифікації, можна відправляти BPDU з меншим пріоритетом, що забезпечить перемогу вузла у процесі виборів кореневого комутатора. Як результат – можливе перехоплення значної частини трафіку мережі, який проходить через кореневий комутатор.

До атак на протокол DHCP належать: «Виснаження DHCP», «DHCP DoS», «Фальшивий сервер DHCP». Сенс атаки «Виснаження DHCP» полягає в наступному: шляхом генерації випадкових DHCP DISCOVER пакетів, можна примусити DHCP сервер видати всі IP адреси з пулу адрес. Відповідно клієнти мережі не матимуть змогу отримати IP адрес і будуть недоступні в мережі. Сенс атаки «DHCP DoS»: при реалізації атаки «Виснаження DHCP» на DHCP сервер посилається велика кількість пакетів. Після цього сервер буде завантажений фальшивими запитами і тому справжні запити не будуть опрацьовані. Відповідно для клієнтів сервер буде недоступним. Сенс атаки «Фальшивий сервер DHCP»: при встановленні фальшивого сервера, клієнти не лише отримують адреси з фальшивого пулу, але й отримують адресу фальшивого шлюзу за замовчуванням, що призведе до передачі всього трафіку через зловмисника.

До атак на протокол ARP належать ARP Flooding, ARP Spoofing. Сенс ARP Flooding: зловмисник посилає велику кількість фальшивих ARP пакетів з різним IP адресом відправника. У цьому випадку, ARP таблиця заповнюється і пристрій не здатний утворювати нові ARP записи для ARP пакетів від авторизованих користувачів. Зв'язок між користувачами обривається. Сенс ARP Spoofing: передача фальшивих ARP-відповідей, у результаті чого зловмисник підміняє клієнта і весь трафік між клієнтами ретранслюється через зловмисника.

З метою моделювання та дослідження вищезазначених атак, а також моделювання захисту пристроїв канального рівня комутованих локальних комп'ютерних мереж розроблено віртуальну лабораторію, яка використовує відкриті програмні платформи по моделюванню мереж (eNSP, VirtualBox) та відкриті програмні засоби атакування (Macof; Yersinia; Ettercap; PackETH; WireShark).