векторів атаки або циклічні вектори атаки, потенційно засновані на контрзаходи, зроблених метою.

Атаки прикладного рівня. Мета цих атак полягає в тому, щоб вичерпати ресурси цілі. Таки атаки важко захистити, так як трафік може бути важко помітити як шкідливий.

Протокольні атаки викликають збої в роботі служби, оскільки використовують всю доступну ємність таблиці станів серверів веб-додатків або проміжних ресурсів, таких як брандмауери і балансувальник навантаження. Протокольні атаки використовують слабкості на рівні 3 і рівні 4 стека протоколів, щоб зробити ціль недоступною. SYN Flood атака використовує рукостискання TCP, відправляючи цільового об'єкту велика кількість пакетів SYN «Початковий запит з'єднання» TCP з підробленими IP-адресами джерела. Цільова машина відповідає на кожен запит на підключення, а потім чекає останнього кроку рукостискання, який ніколи не відбувається, виснажуючи ресурси мети в процесі.

Об'ємні атаки. Ця категорія атак намагається створити перевантаження, споживаючи всю доступну пропускну здатність між ціллю та Інтернетом. Великі обсяги даних відправляються на ціль з використанням форми посилення або іншого засобу створення великого трафіку, такого як запити з ботнету.

Посилення DNS. Відправляючи запит на відкритий DNS- сервер з підробленим IP-адресом (реальний IP-адресу цілі), цільової IP-адреса потім отримує відповідь від сервера. Зловмисник структурує запит так, щоб DNS-сервер відповідав на ціль великою кількістю даних. В результаті ціль отримує посилення початкового запиту атакуючого.

У висновку необхідно відзначити, що атаки DDOS відбуваються щодня. Тому, якщо у вас є ресурси в мережі, то необхідно звернутися до фахівців з безпеки в Інтернеті. Але послуги фахівців можуть бути дорогими, і програмне забезпечення, яке вам потрібно, може бути ще дорожче, але ви ніколи не знаєте, коли вам може знадобитися захист.

Одержано 11.04.2019

УДК 681.3.06

Олексій В'ячеславович ПЕРЕЦЬ,
курсант групи Ф4-102 ХНУВС
Науковий керівник: кандидат технічних наук, доцент Світличний В. А.

ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ЧЕРЕЗ СМАРТФОН

Мобільний телефон просто незамінним для кожної сучасної людини. Але, хоча такий зв'язок і має безліч позитивних якостей, її безпека все ж викликає чималі сумніви. Річ у тому, що сигнали, передаванні смартфонами, цілком можна перехопити та розшифрувати. Смартфон також схильний до вірусних атак. В цьому випадку, навіть якщо смартфон просто лежить на столі,

то це не означає, що він пасивний – цілком можливо, що саме у цей момент він передає отримані відомості, або приймає деякі команди керування. Що ж робити, якщо ваша інформація коштовна і значима, і може вплинути на долю компанії або долю конкретної людини? Відповідь є – для цього існує захист від прослуховування. Наприклад, захист переговорів сповна може бути забезпечений за допомогою такого пристрою, як глушник мобільних телефонів, який спотворює сигнали – завади і робить неможливим роботу телефонів. При цьому мобільний глушник телефонів спотворює не лише сигнал, що йде з телефону, але і запис, вироблений на цифрові носії. Виходячи з цього, можна зрозуміти, що глушник стільникового зв'язку просто необхідний аналітикам, професіоналам, що заробляють на наданні секретної інформації конкурентам чи злочинцям. Такі пристрої, що блокують стільниковий зв'язок, просто незамінні в офісах керівництва, на переговорах, де необхідне дотримання повної тиші, або циркулює конфіденційна інформація.

У таких випадках, коли Ви не бажаєте, щоб озвучена інформація не виходила за межі її обговорення, бажаний також глушник диктофонів. Хто знає – раптом саме зараз вся секретна розмова записується, і щоб цього не сталося, придушення диктофонів вельми бажано. Схема глушника GSM така – глушник стільникових телефонів уловлює і реєструє потік, гасячи його. GSM глушник має в своїй основі генератор шуму, схема якого схожа в різних пристроях. Захист від прослуховування може працювати на різних відстанях від об'єкту за рахунок варіювання потужності силового сигналу.

Існує декілька принципів роботи пристроїв, що блокують телефоні. Найпростіший – це глушник мобільних телефонів, схема яких не вимагає особливих витрат. При цьому на стіни встановлюються спеціальні панелі, пасивно блокуючи сигнали. Існує і інший прилад – глушник мобільних телефонів, схема якого визначає наявність працюючого телефону в певному радіусі. Виявивши спробу дзвінка, глушник блокує сигнал управління. Глушник мобільних працює з радіосигналом, і якщо шукачі просто реєструють сигнал, то пригнічувачі його глушать. По цих причинах глушник мобільних апаратів є найкращим захистом від шпигунських штучок, на сьогоднішній день захист від прослухування і від посягання на ділове і приватне життя.

Незамінний глушник стільникових апаратів, схема яких дозволяє протидіяти радіокерованим бомбам. Такі апарати корисно використовувати в місцях масового скупчення людей, які часто стають об'єктами терактів.

Також корисно використовувати глушники працівникам Національної поліції та Національної Гвардії наприклад, для перешкоджання втрати секретної інформації.

Одержано 14.04.2019