І потрібен він для пасивного і максимально непомітного моніторингу сегмента мережі. Його неможливо виявити програмними засобами. Throwing Star LANTap виглядає як невелика мікросхема хрестоподібної форми, на кінцях якої розташовані чотири Ethernet-порту. ThrowingStarLANTap спроектована для моніторингу мереж 10BaseT і 100BaseTX і для своєї роботи не вимагає підключення джерел живлення. Завдяки тому що пристрій не використовує ніякого електроживлення, він не може моніторити мережі 1000 Base T. У такому випадку йому доводиться знижувати якість зв'язку, змушуючи машини спілкуватися на більш низькій швидкості яку вже можна пасивно моніторити.

5. Всі бездротові пристрої володіють серйозним недоліком – обмеженим радіусом дії. Надійний прийом часто є ключовим параметром для успішної реалізації атаки. Існують все спрямовані, а також цілеспрямовані антени. Для прикладу представником другого типу є антена 16dBi YagiAntenna. Ця антена дозволяє перебувати на достатній відстані від бездротової мережі і зберігати необхідний рівень сигналу. Завдяки конвектор RP-SMA її можна підключити до розглянутих інструментів WiFiPineapple та UbertoothOne, а також до багатьох інших WiFi-пристроїв. Важливо розуміти, що це лише одна з тисяч найрізноманітніших антен. У Мережі не тільки продається величезна кількість самих різних антен з різноманітними характеристиками, але і лежить чимало інструкцій про те, як швидко створити антену з підручних матеріалів.

Перед фахівцем в області інформаційної безпеки стоять завдання ефективного вирішення головоломок з пошуку вразливостей досліджуваних систем. Важливим елементом будь-якої роботи з тестування захищеності інфраструктури замовника є перевірка бездротових мереж. Значно підвищити ефективність такої перевірки допоможуть розглянути спеціалізовані інструменти.

Одержано 11.04.2019

УДК 332.012

Владислав Романович ПЛЕХАНОВ,
курсант групи Ф4-202 ХНУВС
Науковий керівник: Рог В. Є.

ВАЖЛИВІСТЬ НАДІЙНОГО ПАРОЛЯ ПІД ЧАС ВИКОРИСТАННЯ ІНТЕРНЕТ-РЕСУРСІВ

«Обов'язково використовуйте надійний пароль» – це порада, яку ми всі постійно бачимо в Інтернеті, хтось ставиться до неї з великою відповідальністю, а хтось не приділяє власним паролям жодного значення, про що потім шкодує.

Як створити надійний пароль і, що більш важливо, як його запам'ятати.

Важливість надійного пароля зростає з кожним днем, адже завдяки науково-технічному прогресу зростають обчислювальні можливості комп'ютерів. Від обчислювальної потужності комп'ютера залежить швидкість перебору паролів, підчас атаки «Brute-force» (Атака грубої сили) Brute-force – це атака

коли зловмисник використовує набір попередньо визначених значень, щоб атакувати ціль. Успіх залежить від набору визначених значень. Якщо він більший, це займе більше часу, але є більша ймовірність успіху. Найбільш поширеним і простим для розуміння прикладом атаки з грубою силою є атака за словником. У цьому випадку, зловмисник використовує словник паролів, який містить мільйони слів, які можна використовувати як пароль. Тоді зловмисник спробує ці паролі один за одним. Якщо цей словник містить правильний пароль, зловмисник матиме успіх.

Атака з використанням грубої сили як і раніше є однією з найпопулярніших методів злому паролів, адже використовуючи звичайний сучасний комп'ютер є можливість спробувати близько 150 мільйонів паролів лише за годину.

Надійний пароль достатнього рівня, складається з 12 символів. Немає мінімальної довжини пароля, з якою завжди варто погоджуватись, але, як правило, ви повинні використовувати паролі довжиною від 12 до 14 символів. Пароль який містить ще більше символів буде надійним та кращим.

Можна подумати що довгий пароль вже є надійним, але це не зовсім так. Дійсно надійний пароль включає цифри, символи, великі літери та літери нижнього регістру: використовуйте суміш різних типів символів, щоб зробити його більш міцним, такий пароль важче зламати.

Не використовуйте слово зі словника чи комбінацій слів. Будь-яке слово погано відображується на вашому паролі. Будь-яка комбінація декількох слів, особливо якщо вони очевидні, також погана. Наприклад, «House 123456» – це жахливий пароль. «Red_house 54321» теж дуже поганий.

Не використовуйте звичайні, або передбачувані заміни – наприклад: «H0use 769842» не є сильним, бо ви замінили о на 0. Це просто та дуже передбачувано, створюючи базу паролів для перебору завжди враховують цей метод.

Намагайтеся змішувати всі поради, а не використовувати кожну окремо, наприклад:«AlfaHouse@123» відповідає багатьом вимогам. Він містить аж 14 символів і включає літери верхнього регістру, малі літери, спеціальні символи і деякі цифри. Але це досить передбачувано, кожне слово правильно вживається з великої літери. Є тільки один символ, всі цифри знаходяться в кінці, і їх легко вгадати.

З наведеними вище порадами досить легко створити дійсно надійний пароль. Наприклад: «M1_kP6G5Vh@hoL$b» – це міцний пароль на 16 символів, він поєднує безліч різних типів символів і важко здогадатися, яких саме, тому що це просто серія випадкових символів. Але як запам'ятати такий важкий пароль для кожного веб-сайту: його важко асоціювати з чимось та аналізувати. Впоратися з цією задачею вам допоможе менеджер паролів. Менеджер паролів – програмне забезпечення з не типовим шифруванням високого рівня, яке зберігає усі ваші паролі, надає можливість отримувати до них доступ знаючи лише один (головний) пароль, який потрібно вивчити.

Варто пам'ятати про надійність пароля. Але, наприклад, якщо ви повторно використовуєте пароль у кількох місцях, він може бути зламаний, і зловмисники можуть використовувати цей пароль для доступу до інших ваших

облікових записів. Також важливим є уникнення підозрілих сайтів і збереження вашого комп'ютера від шкідливого програмного забезпечення. Використання більш потужних паролів не допоможе вам захиститися від усіх загроз, але це перший й дуже важливий крок.

Одержано 12.04.2019

УДК 332.012

Владислав Романович ПЛЕХАНОВ,
курсант групи Ф4-202 ХНУВС
Науковий керівник: кандидат технічних наук, доцент Клімушин П. С.

ВИКОРИСТАННЯ ЗМАГАНЬ МІЖ ФАХІВЦЯМИ З БЕЗПЕКИ ДЛЯ ПІДГОТОВКИ КІБЕРПОЛІЦЕЙСЬКИХ

Кібербезпека є високим пріоритетом для держави та компаній, малих і великих, тому що останнім часом в країні спостерігається зростання числа кібератак. У відповідь на це майбутні фахівці повинні пройти ретельну підготовку та зрозуміти як саме працюють хакери та як від них захищатись. Один із новітніх способів навчання в галузі кібербезпеки– це змагання між фахівцями з безпеки під назвою захоплення флага (capturetheflag – CTF). Цей конкурс використовується як навчальний посібник для всіх, хто цікавиться кібербезпекою, і може допомогти покращити навички та інструменти, які вони використовували під час навчання.

CTF для кібербезпеки була вперше розроблена та розміщена ще в 1996 році в Лас-Вегасі, штат Невада, але лише зараз вона має можливість проявити себе, коли обчислювальна техніка на достатньому рівні підтримує функції віртуалізації операційної системи. Турніри CTF глобальні, оскільки вони не мають кордонів і можуть бути зроблені через Інтернет. Міжнародні команди змагаються за різні призи, чемпіонами CTF з України є команда DCUA. Існує два формати CTF для кібербезпеки «атака-захист» та гра Jeopardy з різними категоріями та точковими значеннями.

CTF «атака-захист» –є атакуюча команда, а також та яка захищає свою власну систему. Зазвичай існує два раунди гри, в якій однією командою є атакуюча команда, а інша команда є захисною командою в першому раунді, а потім переходять на другий тур. У оборонних машинах є прапори (текстові файли, папки, зображення тощо), які команда атакуючих намагається знайти, оскільки вони компрометують машини. Команда, що належить, може використовувати різні інструменти зловмисника для того, щоб поставити під загрозу захисні машини, але існують правила, які гарантують, що команди не мають переваг перед іншим. Команда-захисник може зробити що-небудь в рамках правил, щоб захистити свої машини від атакуючої команди. Їм заборонено вимикати будь-які мережні з'єднання або вимикати пристрої. Якщо є якесь порушення правил, команда понесе штраф або дискваліфікується.