СЕКЦІЯ 6
ПРАВОВІ Й ТАКТИЧНІ ОСНОВИ ОРД. СПЕЦТЕХНІКА. ТАКТИКО-СПЕЦІАЛЬНА ПІДГОТОВКА. ВОГНЕВА ТА СПЕЦІАЛЬНА ФІЗИЧНА ПІДГОТОВКА. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ ПОЛІЦІЇ. СТВОРЕННЯ ЗАСОБІВ ТА КОМПЛЕКСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

НАУКОВИЙ ГУРТОК КАФЕДРИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ФАКУЛЬТЕТУ № 4

УДК 342.922

Анна Олександрівна ОСТРОВЕРХОВА,
курсант групи Ф4-302 ХНУВС
Науковий керівник: кандидат технічних наук, доцент Клімушин П. С.

ШПИГУНСЬКІ ПРИСТРОЇ БЕЗДРОТОВИХ МЕРЕЖ ЯК НЕБЕЗПЕКА ВТРАТИ ІНФОРМАЦІЇ

Незвичайні види пристроїв і гаджетів є не тільки у співробітників спецслужб, але і у осіб, які мають на меті заволодіти конфіденційною інформацією. Чимало девайсів та гаджетів було спеціально розроблено для потреб хакерів і дослідників безпеки. Проведемо дослідження таких пристроїв.

1. Інструмент WiFiPineappleMark може діяти під виглядом відкритого хот-спота (гаряча пляма) спеціально налаштованого роутера, який перехоплює весь відкритий трафік і використовує різні види MITM-атак, щоб перехопити ті дані, які передаються по захищеному з'єднанню. Для більшого успіху зловмисник може використовувати звучне ім'я мережі на кшталт «WiFiGuest» або взагалі маскуватися під популярних провайдерів.

2. Інструмент Ubertooth One розроблений для можливого перехоплювання даних з Bluetooth-ефіру, що передаються іншими девайсами. Він може використовуватися в якості аналізатора спектра Bluetooth в режимі реального часу, а також в якості аналізатора пакетів Bluetooth. Це дозволяє отримати доступ до мікрофонів в гарнітурі або зламати клавіатуру або мишу, що забезпечує віддалений доступ до систем.

3. ReaverPro призначений для добірки піна WPS (WifiProtectedSetup) методом перебору. Кінцевою метою є розшифровка пароля WPA/WPA2. Reaver створений для надійної і практичної атаки на WPS, він пройшов тестування на великій кількості точок доступу з різними реалізаціями WPS.

4. Наступний девайс ThrowingStarLANTap який передбачає, що у атакуючого є доступ не до конкретного комп'ютера, а до кабелів локальної мережі.

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