УДК 004.732

Неустроев Н.С.

студент магистратуры

Северо-Восточный федеральный университет им. М.К. Аммосова

Российская Федерация, г. Якутск

Научный руководитель: Леонтьев Н.А., к.т.н.

доцент

ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ WI-FI СЕТИ ПО МЕТОДУ АТАКИ НА ТОЧКИ ДОСТУПА ИЗ ГЛОБАЛЬНОЙ И ЛОКАЛЬНОЙ СЕТЕЙ

Аннотация: *В статье изложено исследование уязвимости Wi-Fi сетей через атаку из глобальной и локальной сетей. Исследуется уязвимости Wi-Fi сетей с помощью программы Router Scan.*

Ключевые слова: *Wi-Fi, беспроводные сети, безопасность Wi-Fi, Router Scan.*

Neustroev Nikita Sergeevich

M. K. Ammosov North-Eastern Federal University

Yakutsk, Russia

RESEARCH OF THE SECURITY OF WI-FI NETWORKS ON ATTACK ON WI-FI ACCESS POINTS FROM WAN AND LAN

Abstract: *In this article is set out the research vulnerability of wireless networks through attack from global and local networks. Vulnerability of Wi-Fi networks is investigated using Router Scan.*

Keywords: *Wi-Fi, wireless networks, Protection of WiFi, Router Scan.*

В этой статье изложен обзор атаки на точки доступа из глобальной и локальной сетей. Это достаточно недооценённая проблема. Огромное

количество людей имеют беспроводной роутер или модем дома. Как правило, дальше настройки Интернета и Wi-Fi мало кто доходит. Мало кто заботится о том, чтобы сменить пароль администратора, и уже совсем единицы вовремя обновляют прошивку устройств.

Уже есть реализации массовой атаки на дефолтные учётные данные и на известные уязвимости роутеров: Router Scan by Stas'M.

Router Scan умеет находить и определять различные устройства из большого числа известных роутеров/маршрутизаторов и, что самое главное, - вытаскивать из них полезную информацию, в частности характеристики беспроводной сети: способ защиты точки доступа (шифрование), имя точки доступа (SSID) и ключ точки доступа (парольная фраза).

Также получает информацию о WAN соединении (удобно при сканировании локальной сети) и выводит марку и модель роутера.

Получение информации происходит по двум возможным путям:

1. Программа попытается подобрать пару логин/пароль к маршрутизатору из списка стандартных паролей, в результате чего получит доступ.
2. Либо будут использованы неразрушающие уязвимости (или баги) для конкретной модели маршрутизатора, позволяющие получить необходимую информацию и/или обойти процесс авторизации [3].

Для взлома достаточно знать внешний IP-адресс. Злоумышленник может узнать внешний IP-адресс города, страны, области или интернет-провайдера через сайты, такие как Hurricane Electric BGP Toolkit, Тест IP v 1.7, 2ip.ua и другие.

Также реализованы возможности беспроводного аудита - перебор ключа WPA/WPA2 сети, получение пароля по WPS PIN, а также атака Pixie Dust.

Результаты сканирования IP адресов в г. Якутске (см. Рис. 1) обнаружила 86 уязвимых устройств из 1917 просканированных (больше 4 %). Можно использовать другие значения Use credentials (указывает пару логин/пароль, которая будет проверена на устройстве в первую очередь), чтобы найти больше уязвимых устройств.

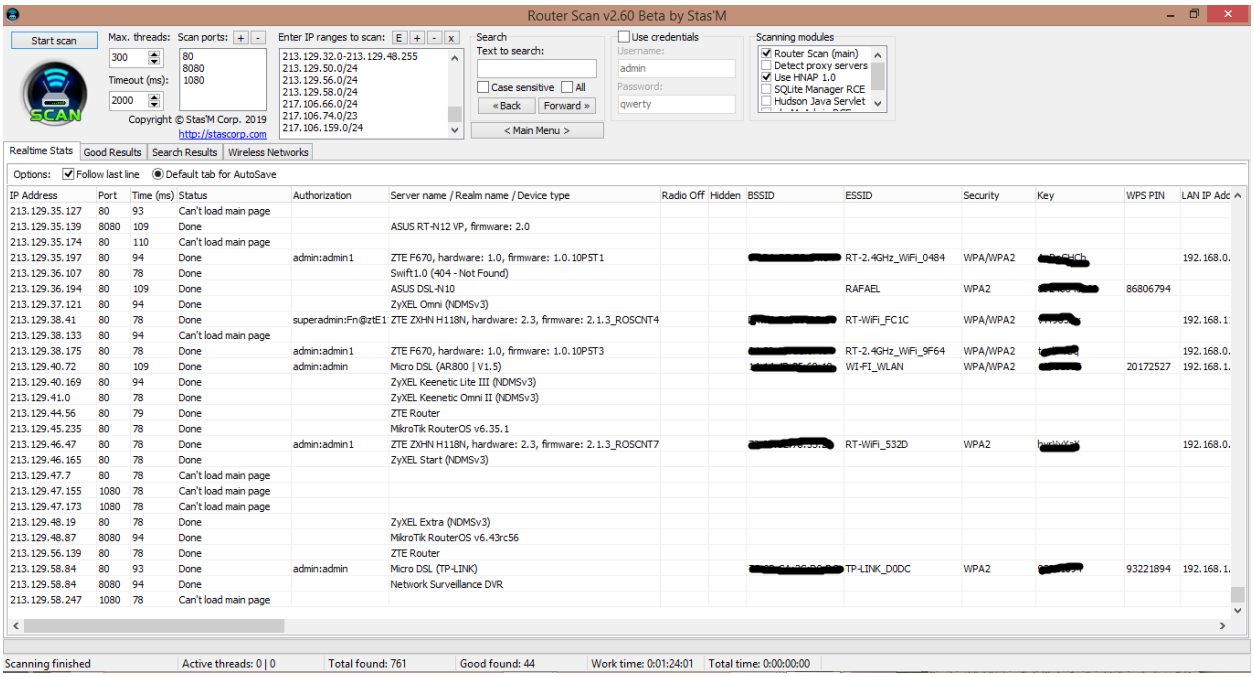

Рис. 1. Результаты сканирования глобальной сети

Результат сканирования IP адресов в г. Якутске обнаружила 26 уязвимых устройств без дополнительной настройки (см Рис.1.). В Router Scan можно видеть имя устройства, MAC-адресс, пароль, пин-код WPS и другие исчерпывающие данные. Можно сколько угодно добавлять внешние IP-адреса и порты.

Результаты сканирования локальной сети выложены в Рис. 2. Здесь доступна расширенная информация о точках доступа. В том числе, можно увидеть точную модель (поля WSC Name и Model) для ТД с WPS. Отсюда можно провести атаки по WPS и перебор ключа.

Active	Stored	Chn	Hidden	BSSID	ESSID	Security	Key	WPS PIN	Level	WPS	Configured	Locked	WSC Name	Model	Serial Number	IP Address
		1		B4:E9:B0:9F:35:83	GUEST	None	<empty>		-67 dBm							
		1		B4:E9:B0:9F:35:80	PREP	WPA2 Enterprise			-68 dBm							
		1		B4:E9:B0:9F:35:84	KIOSK	WPA2			-67 dBm							
		1		B4:E9:B0:9F:35:82	ADM	WPA2 Enterprise			-67 dBm							
		1		B4:E9:B0:9F:35:86	EMPLOYEE	WPA2 Enterprise			-65 dBm							
		1		B4:E9:B0:9F:35:85	STUDENT	WPA2 Enterprise			-58 dBm							10.15.218.7
		4		EC:43:F6:09:5A:E0	Keenetic-5900	WPA2			-65 dBm							
		11		D4:D7:48:23:BD:50	PREP	WPA2 Enterprise			-80 dBm							
		11		D4:D7:48:23:BD:58	KIOSK	WPA2			-82 dBm							
		11		D4:D7:48:23:BD:54	EMPLOYEE	WPA2 Enterprise			-81 dBm							
		11		D4:D7:48:23:BD:52	ADM	WPA2 Enterprise			-82 dBm							
		11		D4:D7:48:23:BD:53	GUEST	None	<empty>		-83 dBm							
		11		D4:D7:48:23:BD:55	STUDENT	WPA2 Enterprise			-80 dBm							
		1		B4:E9:B0:9F:4A:84	KIOSK	WPA2			-96 dBm							
		1		B4:E9:B0:9F:4A:83	GUEST	None	<empty>		-97 dBm							
	[X]	9		58:D5:6E:D5:6E:ED	714/1	WPA2										
		11		D4:D7:48:23:BA:D5	STUDENT	WPA2 Enterprise			-82 dBm							
		3		F8:F0:82:56:45:E2	703/2	WPA2			-59 dBm							
		6	[X]	70:62:B8:8D:76:FB	<length: 10>	WPA/WPA2			-55 dBm							
		4		B0:BE:76:3E:80:10	516/1	WPA2			-73 dBm	2.0	Yes		Wireless N Router TL-WR841N	TP-Link TL-WR841N 14.0	1.0	
		9		58:D5:6E:D5:72:21	FRUTY	WPA2			-66 dBm							
		157		B4:E9:B0:9F:4A:8D	ADM	WPA2 Enterprise										
		157		B4:E9:B0:9F:4A:89	EMPLOYEE	WPA2 Enterprise										
		157		B4:E9:B0:9F:4A:8C	GUEST	None	<empty>									
	[X]	157		B4:E9:B0:9F:4A:8A	STUDENT	WPA2 Enterprise										
		1		B4:E9:B0:9F:4A:86	EMPLOYEE	WPA2 Enterprise			-88 dBm							
		1		78:32:1B:6A:57:C7	503/3	WPA2			-86 dBm							

Рис. 2. Результат сканирования локальной сети.

WPS PIN Companion (см. Рис. 3) вычисляет WPS ПИН беспроводной сети. ПИН рассчитывается по определённым алгоритмам, за основу берётся MAC-адрес и серийный номер роутера (только для некоторых алгоритмов генерации). В новой версии WPS PIN Companion получил новые алгоритмы и другие улучшения, но главным является его комбинация с другим инструментом

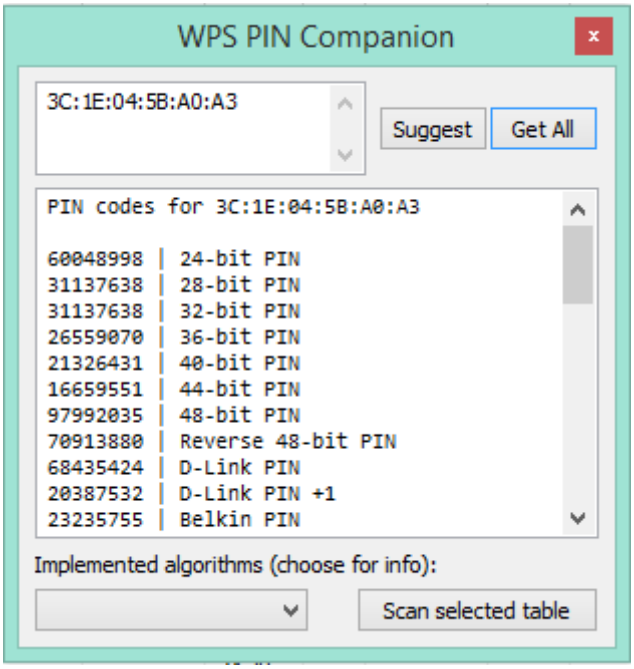

Рис. 3. WPS PIN Companion рассчитывает ПИН по алгоритмам для конкретной точки доступа

Получение WPA пароля на основе предсказанного WPS ПИНа. Можно получить пароль WiFi по атаке Pixie Dust или на основе полученных ПИНов от WPS PIN Companion (см. Рис. 4).

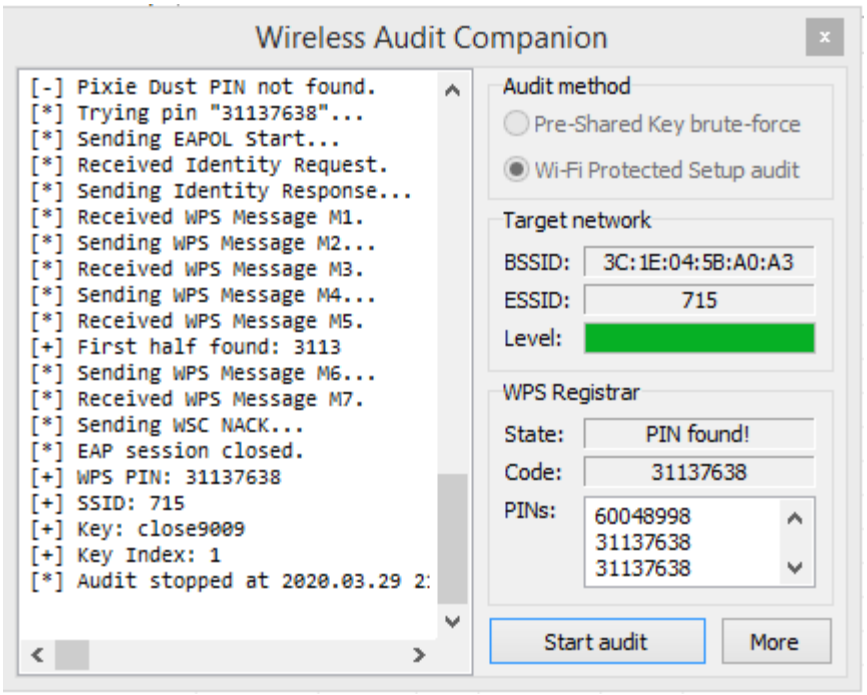

Рис. 4. Получение WPA пароля на основе предсказанного WPS ПИНа

Для всех остальных точек доступа доступен более универсальный, но медленный метод. Суть его заключается в том, что Router Scan пытается подключиться к Wi-Fi сети с паролем, который берёт из словаря (см. Рис. 5). Если подключение прошло удачно – значит пароль угадан, если подключение не получилось, значит программа переходит к следующему паролю и пробует его и т.д. далее, пока не будет подобран пароль или не закончится словарь. На каждую попытку требуется несколько секунд – это медленно.

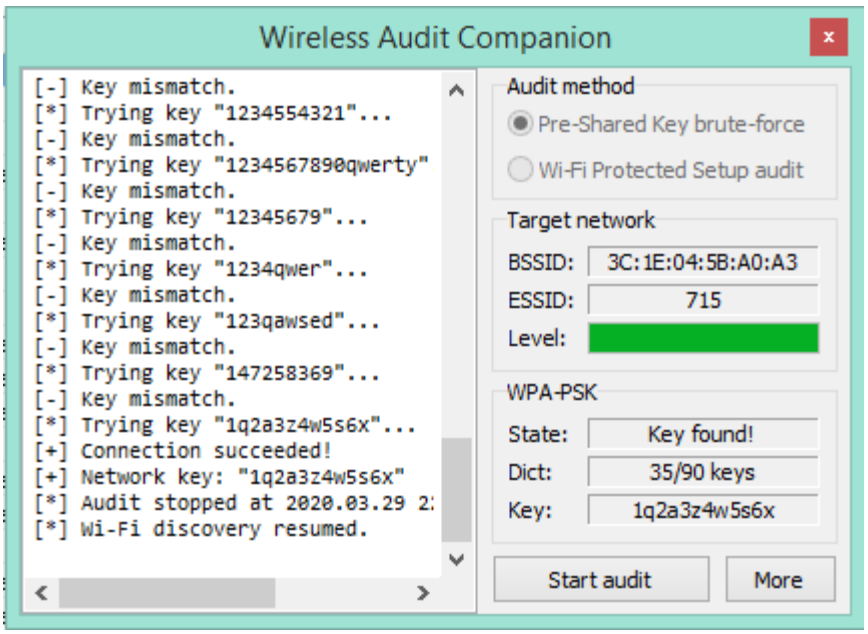

Рис. 5. Подбор пароля Wi-Fi сети

Заключение

В этой статье мы рассмотрели атаки на точки доступа из глобальной и локальной сетей в г. Якутск, а также сделали обзор программы Router Scan. При большом количестве IP-адресов, удалось взломать 86 устройств из 1917 просканированных (больше 4 %). Если бы использовались другие пары логин/пароль, то взломов было бы намного больше.

Принцип работы Router Scan основывается на проверке заводских паролей роутеров, на использование уязвимостей в их прошивках и на атаке по уязвимости WPS. Поэтому защита очевидна:

1) смена заводских паролей для входа в панель администратора

2) регулярное обновление прошивки устройства

3) смена паролей для FTP, Telnet, SSH или отключение этих служб, если они не используются

4) отключить функцию WPS.

Список использованных источников

1. Губсков Ю. А. Анализ атак на протокол регистрации стандарта WPS и способы защиты от них / Ю. А. Губсков, А. В. [и др.] // Информатика: проблемы, методология, технологии. – Воронеж: Издательство: Общество с ограниченной ответственностью "Вэлборн", 2017. – С. 54-59

2. Прокопайло А. А. Методы взлома и защита Wi-Fi сетей / А. А. Прокопайло, Н. В. Дьяченко // Реформирование и развитие естественных и технических наук. – Москва: Изд-во: Научно-издательский центр "Империя", 2019. – С. 100-103.

3. Router Scan v2.60 Beta by Stas'M [Электронный ресурс] URL: http://stascorp.com/load/1-1-0-56 (дата обращения 25.02.2020).