ТЕСТВАНЕ НА УЯЗВИМОСТИ В СИГУРНОСТТА ПРИ БЕЗЖИЧНИ МРЕЖИ

TESTING OF VULNERABILITIES IN WIRELESS NETWORKS

Veneta Aleksieva
Technical University of Varna

Zhecho Dimitrov
Technical University of Varna

Abstract

This paper presents a tools for testing of vulnerabilities in wireless networks, based on the techniques "man-in-the-middle" and social engineering. It works under Kali Linux with multi-language interface. The tool gives the possibility to check the level of password protection for WiFi Networks with different encryption, such as WEP,WPA and WPA2. The development is modular and it allows to be extended easily. The results from experimental research are presented.

Keywords: IDS, WiFi network, network attacks.

ВЪВЕДЕНИЕ

В наши дни много организации изграждат безжични мрежи, за да осигурят удобство и мобилност на служителите си. Домашните потребители също масово използват безжични мрежи в домовете си, а Интернет доставчици с hot-spot решения осигуряват Интернет достъп на клиентите си на обществени места.

При много от безжичните мрежи обаче се пренебрегват проблемите със сигурността. Главният проблем при най-често изградените мрежи, базирани на стандарта 802.11 е, че радио - сигналът излъчва информация на по-голяма площ, отколкото администриращият я може да контролира. Сигналът лесно може да се прихване от лице, ползващо съвместимо мрежово устройство и това може да бъде първата стъпка към киберпрестъпление - да бъде откраднатa ценна информация без организацията да разбере; атакуващият да си осигури безплатен високоскоростен достъп до Интернет; да извърши електронни престъпления възползващи се от анонимното си неоторизирано свързване с чуждата безжична мрежа.

ИЗСЛЕДВАНЕ НА СИГУРНОСТТА ПРИ БЕЗЖИЧНИ МРЕЖИ. СЪЩЕСТВУВАЩИ РЕШЕНИЯ

Съществуват няколко метода за защита на Wi-Fi мрежи:

- Без защита - не се препоръчва
- Wired Equivalent Privacy (WEP) – въведен като стандарт през 1999г, при който открита практическа уязвимост през 2001г. в ползвания шифър (Rivest Cipher 4) RC4 за криптиране налага WiFi Aliance да обяви, че през 2003г. го замеля с WPA, а през 2004г. обявява, че WEP-40 и WEP-104 също са отхвърлени.
- Wi-Fi Protected Access (WPA) – въведен като предварителна версия на стандарт IEEE 802.11i през 2003г, при който открита практическа уязвимост през 2008г. в (Temporal Key Integrity Protocol) TKIP шифъра, който използва, налага отново WiFi Aliance [1] да търси по-добри решения.
- WPA2 – въведен през 2004г. като стандарт IEEE 802.11i, но също уязвим при използване на кратки пароли и в смесен режим с WPA.
- Wireless Protected Setup (WPS) – въведен през 2006г. като метод за свързване чрез 8 цифрен PIN, приложим за WPA/WPA2. Уязвим от 2011г. , т.к. отдалечен нападател може да възстанови PIN-а в рамките на няколко часа с атака на грубата сила и с WPS PIN и предварително споделения ключ WPA/WPA2 да влезе в мрежата.

Изследването на сигурността при безжични мрежи може да се направи по следните методи:

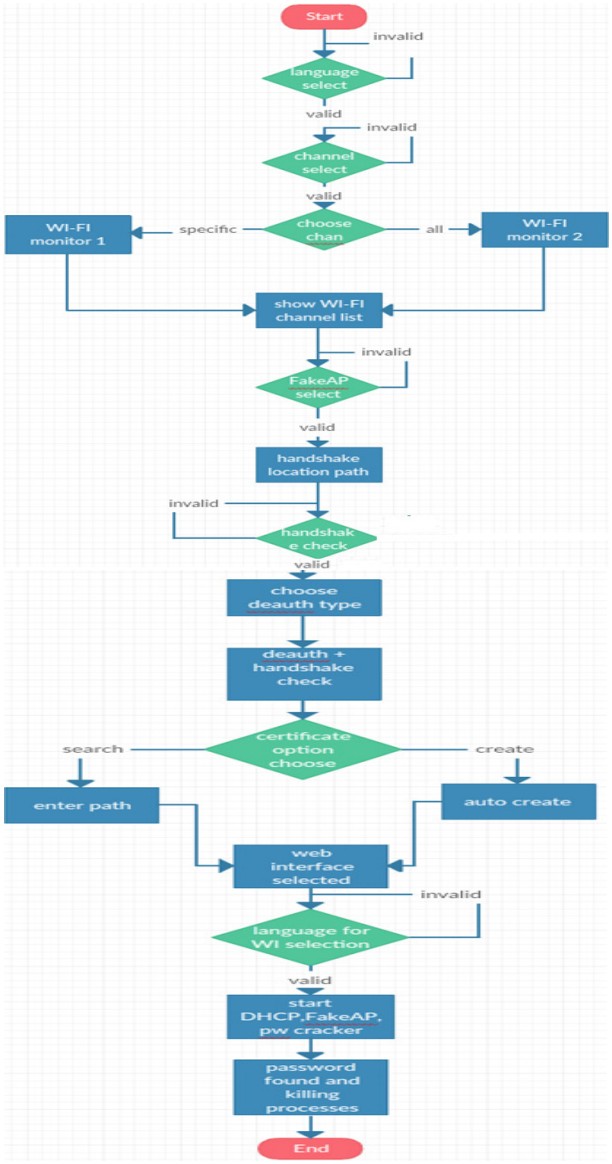
- Пасивно, познато под термина war driving. При този подход изводи за сигурността се правят само на база на публично достъпната информация, излъчвана от всяка точка на достъп от безжична мрежа (име, канал на работа, MAC адрес, методи на криптиране, MAC на клиентските устройства и др.) Подобни изследвания представляват интерес, за да проследят тенденциите в даден регион и да се направи сравнителен анализ. [2,3,4]
- Активно, познато под термина pentesting – свързване към WiFi мрежа чрез използване на познати пароли спрямо името на мрежата, деасоцииране на свързани клиентски устройства, опити за свързване чрез използване на познати слабости на марката/модела на устройството и др. Въпреки, че има предложени много средства за подобна дейност [5,6,7], ако тя не е с учебни цели или в лабораторни условия, излиза извън законовите норми.

СРЕДСТВО ЗА ТЕСТВАНЕ НА УЯЗВИМОСТИ В СИГУРНОСТТА

Настоящата разработка използва активния метод за изследване на сигурност на безжични мрежи и представя средство за изследване на уязвимости, разработено под Kali Linux. Проведените и представени тук тестове на безжични мрежи са за учебни цели и са направени в лабораторни условия.

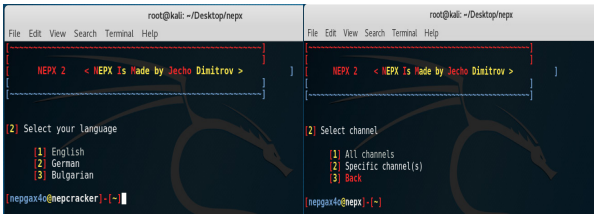
За реализация на генератора на атаки е избрана операционна система - Kali Linux 2.0 sana, т.к. тя е оптимизирана за извършване на penetration тестове и редица от рестрикциите наложени в други популярни Linux дистрибуции и в повечето версии на Windows (с изключение на Windows XP/2000/Server 2000/2008), по отношение на RAW сокетите, отсъстват. Kali Linux вече е официално достъпен и за смартфони като Nexus 5, Nexus 6, Nexus 7, Nexus 9, Nexus 10, OnePlus One, и някои модели на Samsung Galaxy, което прави възможно инсталиране на приложението на мобилно устройство.

На фиг. 1 е представена принципна схема на работа на приложението.



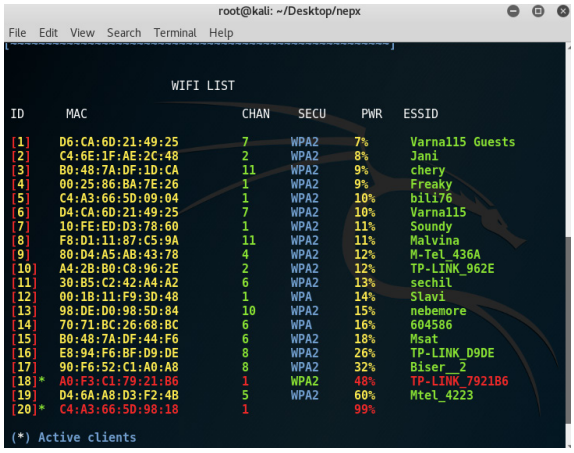
***Фиг. 1**. Диаграма на активностите на приложението за откриване на уязвимости в WiFi мрежи*

Необходимите модули за правилната работа на приложението са: Aircrack-ng, Aireplay-ng, Airmon-ng, Airodump-ng, Awk, Curl, Macchanger, Mdk3, Nmap, Pyrit и др. Ако някое от тях не е инсталирано, приложението дава нотификация за необходимата инсталация и спира работа. Приложението позволява многоезичност, като началният екран е представен на фиг.2, където може да види, че е реализирана възможност за избор на канал за прихващане на безжичните сигнали или следене на всички канали.



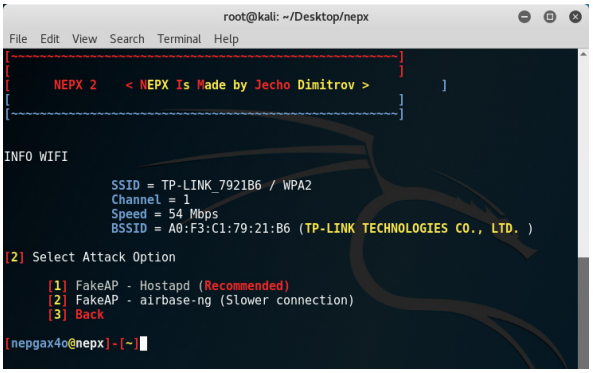
***Фиг. 2**. Начален екран. Избор на канал*

Визуализират се резултатите от сканирането и се прави избор на ESSID.



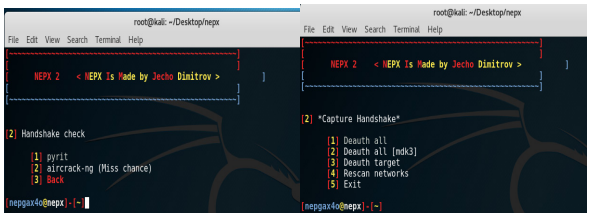
***Фиг. 3**. Списък на сканираните мрежи*

От тях чрез клавиатура може да се посочи избраната мрежа (фиг.3), след което се избират опции за атака (фиг.4) - стандартна или при по-бавна връзка, когато устройствата се намират по-далеч и сигналът е по-слаб.



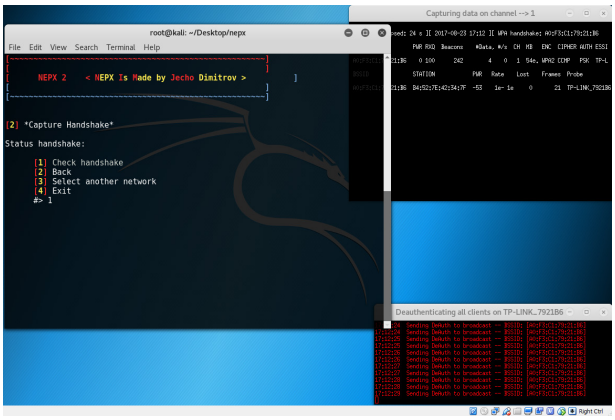
***Фиг. 4**. Избор на опции за атака*

Приложението предлага избор на средство за прихващане на ръкостискането и избор за деоторизация (фиг. 5)



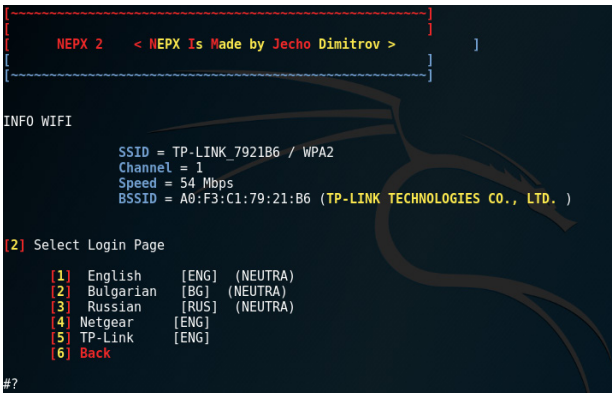
***Фиг. 5.** Опции за прихващане на ръкостискане и деоторизация*

Примерен резултат е представен на фиг.6.



***Фиг. 6.** Проверка за ръкостискане*

Аналогично се прави избор за проверка и направа на SSL сертификат, който ще осъществи декриптирането на паролата. В следващата стъпка се предлага създаване на web интерфейс, имитиращ оригиналния за даден рутер, като се предлага меню за избор на език на страницата. (фиг. 7)



***Фиг. 7.** Език за имитиращата страница*

След създаване/намиране на сертификат се избира метод за получаването на дадена парола, ако то не е bruteforce или не се ползва в списък с ключови пароли. Стартира се FakeAP, DHCP сървър-а, деоторизатора към истинската точка за достъп и се извършва проверката за пароли. Използват се iptables за HTTP/HTTPS портовете за пренасочване на трафика. Времето за тестване и резултатът (дали е открита или не паролата) зависи от активността и броя на свързаните потребители. След успешно намиране на паролата се проверяват всички процеси за мониторинг и след това се спират (killall), като се възстановява оригиналната работа на мрежата.

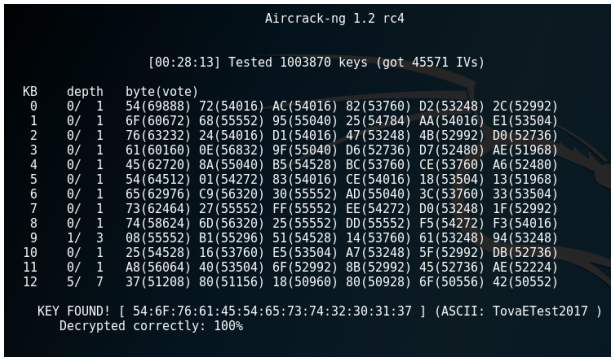
ЕКСПЕРИМЕНТАЛНИ РЕЗУЛТАТИ

С представеното приложение за тестване на устойчивостта на безжични мрежи са атакувани безжичните рутери за извличане на паролите им. Извършени са няколко типа атаки, като при всяка е измервано времето, за което се постига пълен достъп до атакуваната безжична мрежа.

1 атака: Атакуван WiFi рутер: D-link dir 615. Атаката е насочена към WEP парола 128 битова с максимум позволени 13 ASCII символа или 26 HEX.

Успешен резултат е постигнат за 56 минути, т.к. не беше генериран голям трафик от мобилно/и устройства. Използвани са модулите: airmon-ng, aircrack-ng и aireplay-ng.

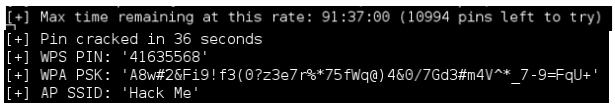
Успешният резултат е представен на фиг. 8.



Фиг. 8. *Паролата се извежда в ASCII и HEX код*

2 атака: Атакуван WiFi рутер tp-link wr740n. Атаката е насочена към wpa2 парола, но WPS е забранен.

Успешен резултат се постига за време между 2 часа и 10 часа, в зависимост от броя свързани устройства, дали WPS е забранен (трябва да се отключи), размера на трафика. Резултатът е представен на фиг. 9.



Фиг. 9. *Паролата при WPA2 е изведена*

В таблица 1 са представени резултатите от направените експерименти за атака към различни устройства, насочена към WPA2 парола, когато WPS е забранен.

Табл. 1*. Средно време за успешна атака на устройство*

Име на устройство	Тип	Средно време
TP-LINK WR740N	Wireless Router	6 часа
BiPAC 7404VGPX	AP	3 часа
ECB9500	Wireless Gigabit Client Bridge	4 часа
NP800n	Wireless Router	10 часа
WTM652	Router / Access Point	12 часа
LW310V2	Wireless Router	4 часа

3 атака: Атакуван WiFi рутер tp-link wr740n. Атаката е насочена към wpa2 парола, но е с WPS pixiedust.

Получава се или пина и паролата (фиг.10) или невалиден резултат (фиг.11).

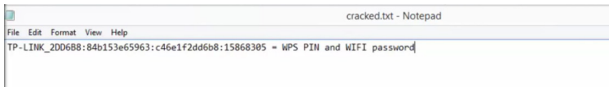
Фиг. 10. *Паролата при WPA2 + WPS pixiedust е изведена*

Фиг. 11. *Невалиден резултат при WPA2 + WPS pixiedust*

Успешен резултат се постига за време малко над 2 часа. При невалиден резултат се търси друг метод за атака.

4а атака: Атакуван WiFi рутер tp-link wr740n. Атаката е насочена към wpa2 парола, прилага се brute-force атака. Паролата е до 8 символа.

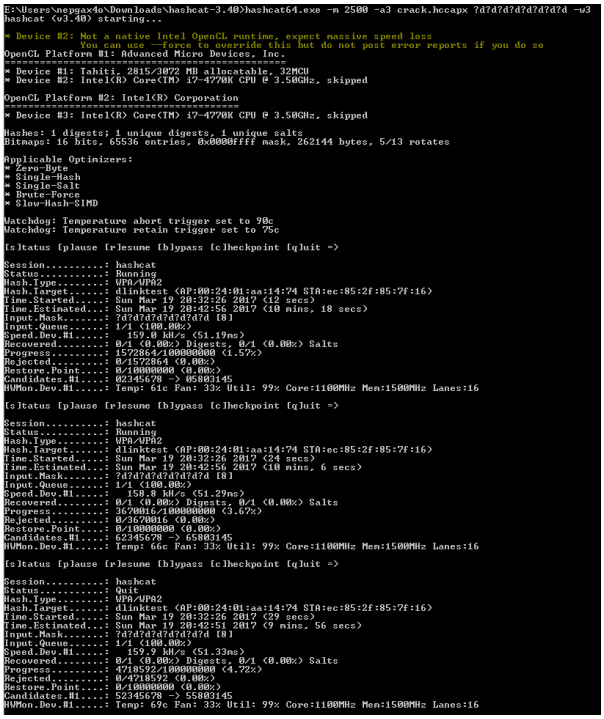
Подходите за списъка с евентуални пароли са два: да се използва password list или default-ен такъв за рутерите. Повечето рутери идват от производителя с дълга парола, която ползвателя не сменя. Така 99% от всичките възможни пароли се намират във вградения файл rockyou на Kali Linux. 5. В cracked.txt се получват съответно PIN-а и паролата (фиг.12). Успешен резултат се постига за време 86 минути, защото паролата беше в списъка.



Фиг. 12. *Паролата, получена с brute-force атака*

4б атака: Атакуван WiFi рутер tp-link wr740n. Атаката е насочена към wpa2 парола, прилага се brute-force атака. Паролата е до 8 символа. С алтернатива на предложеното в доклада решение hashcat, която работи и под Windows. Резултат е постигнат за 10 минути (фиг. 13).

Направеното сравнение на бързодействието на двете решения при използване на един и същ хардуер е в полза на популярното решение hashcat (8 пъти по-бързо). И в двата случая търсената парола беше в обхождания списък с пароли. Прилагането на маска при търсенето на пароли значително ускорява процеса и при двете решения, но съотношението на времената за намиране на паролата при равни други условия се запазва.



Фиг. 13. *Brute-force атака с hashcat*

Простият принцип на работа на предложеното приложение не би се забелязал от повечето потребители, защото по-голяма част от устройствата се свързват директно към фалшивата мрежа, която има само за цел да присвои паролата от оригиналната мрежа.

ЗАКЛЮЧЕНИЕ

За да бъде една мрежа достатъчно ефективно предпазена, тя трябва да бъде подготвена да отговори на потенциалните заплахи на практика. Тази необходимост все повече засилва нуждата от използването на софтуерни средства като представената разработка. С предложеното решение може да се помогне за усъвършенстване и тестване на защитата на всяка една безжична мрежа, но и да се даде възможност за извършването на тестове и симулации в реално време, максимално доближаващи се до реалните условия, при които мрежата ще функционира в критични за нейната сигурност моменти.

В настоящият доклад са представени и резултати от експерименти, които доказват ефективността на предложеното софтуерно средство за изследване уязвимостта в сигурността при безжични мрежи. Неговата модулна реализация позволява в бъдеще да се имплементират и други видове популярни атаки, които не са насочени само към безжичните мрежи.

REFERENCE

[1]WiFi Alliance, https://www.wi-fi.org/.(last visit on 01.10.2017)

[2]A. Sebbar, SE. Boulahya, G. Mezzour, M. Boulmalf, An Empirical Study of WIFI Security and Performance in Morocco - WarDriving in Rabat., ICEIT'2016, DOI: 10.1109/EITech.2016.7519621, 2016.

[3]Ar Kar Kyaw, Zhuang Tian, Brian Cusack, Wi-Pi: a study of WLAN security in Auckland City, IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.8, , pp. 68-80, 2016.

[4]Wigle Wifi Wardriving 2.24 Released, https://wigle.net/.(last visit on 01.10.2017)

[5]How To Pentest Your WPA/WPA2 WiFi With Kali Linux, https://www.pentestingshop.com/how-to-pentest-your-wpawpa2-wifi-with-kali-linux/./.(last visit on 01.10.2017)

[6]Wi-Fi Security and Pentesting, http://www.pentesteracademy.com. (last visit on 01.10.2017)

[7]Wireless Security - Wi-Fi Pen Testing, https://www.tutorialspoint.com/wireless_security/wireless_security_wifi_pen_testing.htm. (last visit on 01.10.2017)