электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 621.391

Работы общего и обзорного характера. Общая теория связи. Кибернетика (теория информации и теория сигналов применительно к электросвязи)
Оценка уязвимостей Voice-Over-IP протоколов

***Дербина Е.А.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

***Щербаков А.В.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Алёшин В.А., к.т.н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
v.aleshin@bmstu.net

Стек протоколов VoIP

Установление VoIP сеанса включает нагромождение различных протоколов, каждый из которых должен взаимодействовать правильно и надежно. Стек протоколов VoIP показан на рис. 1.

Рис. 1. Стек протоколов VoIP

Стек протоколов VoIP состоит из передачи сигналов (SIP — Session Initiation Protocol), описания сеанса (SDP — Session Description Protocol), обмена ключами (SDES

— Session Description Protocol Security Descriptions, MIKEY — Multimedia Internet KEYing и ZRTP — Z and Real-time Transport Protocol) и безопасных протоколов передачи данных (SRTP — Secure Real-time Transport Protocol).

Приведем некоторые основные понятия для дальнейшего изложения:

Передача сигналов: SIP (Session Initiation Protocol)

SIP является протоколом передачи сигналов прикладного уровня, используемым для создания, изменения и завершения сеансов с одним или несколькими участниками. Сеть SIP состоит из следующих объектов: оконечные устройства, прокси и/или сервер перенаправления, сервер местоположения и регистратор. Оконечные устройства или User Agents (UA) представляют телефонные устройства или модемы программного обеспечения.

Описание сеанса: SDP (Session Description Protocol)

SDP [2] — это формат для описания мультимедийных параметров сеанса в целях объявления сеанса, приглашения на сеанс, и т.д. Мультимедийный сеанс представляет собой ряд мультимедийных отправителей и получателей, а также потоков данных, протекающих между ними; один сеанс может состоять из нескольких мультимедийных потоков. Объявление сеанса состоит из описания сеансового уровня (детали, которые применяются ко всем мультимедийным потокам) и, дополнительно, нескольких описаний медиа-уровней.

Протокол передачи данных в реальном времени: RTP (Real-time Transport Protocol)

Протокол RTP [3] работает на прикладном уровне и используется при передаче трафика реального времени. Протокол RTP переносит в своём заголовке данные, необходимые для восстановления аудиоданных или видеоизображения в приёмном узле, а также данные о типе кодирования информации. В заголовке данного протокола, в частности, передаются временная метка и номер пакета. Эти параметры позволяют при минимальных задержках определить порядок и момент декодирования каждого пакета, а также интерполировать потерянные пакеты.

Установление и разрыв соединения не входит в список возможностей RTP, такие действия выполняются SIP.

Атаки и уязвимости

Отметим сценарии по реализации злоумышленником наиболее распространенных следующих угроз ИБ:

1. Атака «Отказ в обслуживании» (Denial of service)
2. Атака «Прослушивание» (Eavesdropping)
3. Атака «Подмена идентификатора вызывающего абонента» (Spoofing caller ID)
4. Атака «Подбор пароля» (Brute Force).

Для примеров атак мы используем физическую машину с Windows 8.1, две виртуальные машины Kali Linux и программную АТС, работающую на стандарте SIP — 3CX Phone System.

Атака «Отказ в обслуживании»

Как отмечено в работе [4], атака «Отказ в обслуживании» (DoS) нацелена на перевод сетевого элемента в состояние неработоспособности. К таким атакам обычно относят направление чрезмерно большого трафика на его интерфейсы. Распределенная DoS атака позволяет одному пользователю сети SIP воздействовать на большое количество сетевых узлов с тем, чтобы они передавали очень большой сетевой трафик на определенный узел сети («затопили» его). Во многих архитектурах прокси-серверы сети SIP взаимодействуют с публичной сетью Интернет, к которой подключено множество IP-терминалов. В результате, сеть SIP предоставляет возможность для распределенных DoS атак, что должно быть учтено разработчиками и операторами сетей SIP.

Злоумышленники могут создавать поддельные запросы, содержащие фальсифицированные IP-адреса источника и соответствующее поле заголовка Via [5]. Эти параметры идентифицируют ложный источник этих запросов, на который затем через агента пользователя или прокси-сервер SIP генерируется трафик, приводящий к DoS.

Для примера атаки «Отказ в обслуживании» воспользуемся инструментом inviteflood, который позволяет отправлять запросы INVITE на SIP порты/прокси и SIP телефоны.

На рис. 2 показано, что после получения 2129120 запросов на звонок, SIP телефон X-lite выдал программную ошибку.

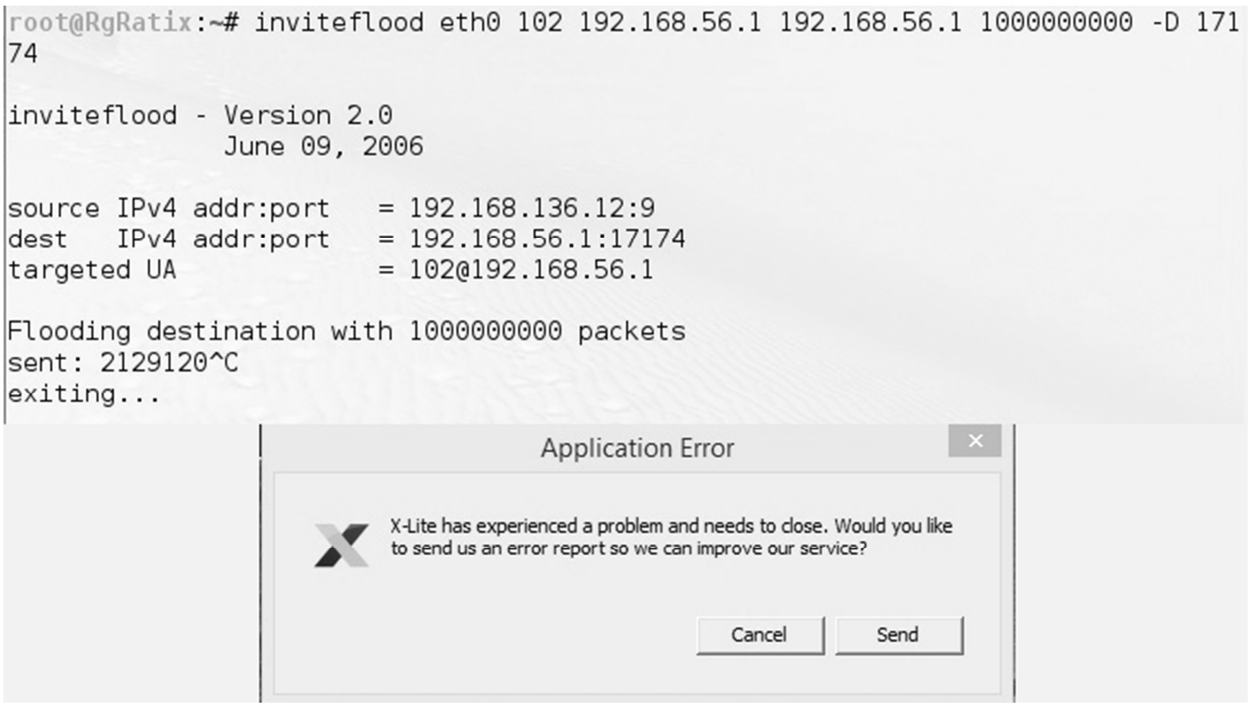

Рис. 2. Атака «Отказ в обслуживании»

Атака «Прослушивание» (Eavesdropping)

Прослушивание (Eavesdropping) — атака, которая возникает, когда злоумышленник мониторит или прослушивает трафик сети при передаче и затем может выявить все незащищенные данные. Важно понимать, что если для прослушивания обычных телефонных переговоров (телефонные системы с коммутацией каналов) необходимо иметь специальное оборудование и доступ в здание телефонной компании, то все, что необходимо для прослушивания в IP-сети — это сниффер для сбора данных, которые передаются. В основном это происходит в следствии того, что TCP/IP (Transmission Control Protocol/Internet Protocol) разрабатывался как открытая архитектура для передачи нешифрованного трафика по сетям.

Чтобы привести пример атаки «Прослушивание», одна из виртуальных машин будет пытаться подслушать разговор, устанавливаемый по SIP протоколу, между второй виртуальной и физической машинами.

Мы будем использовать сценарий, представленный на рис. 3.

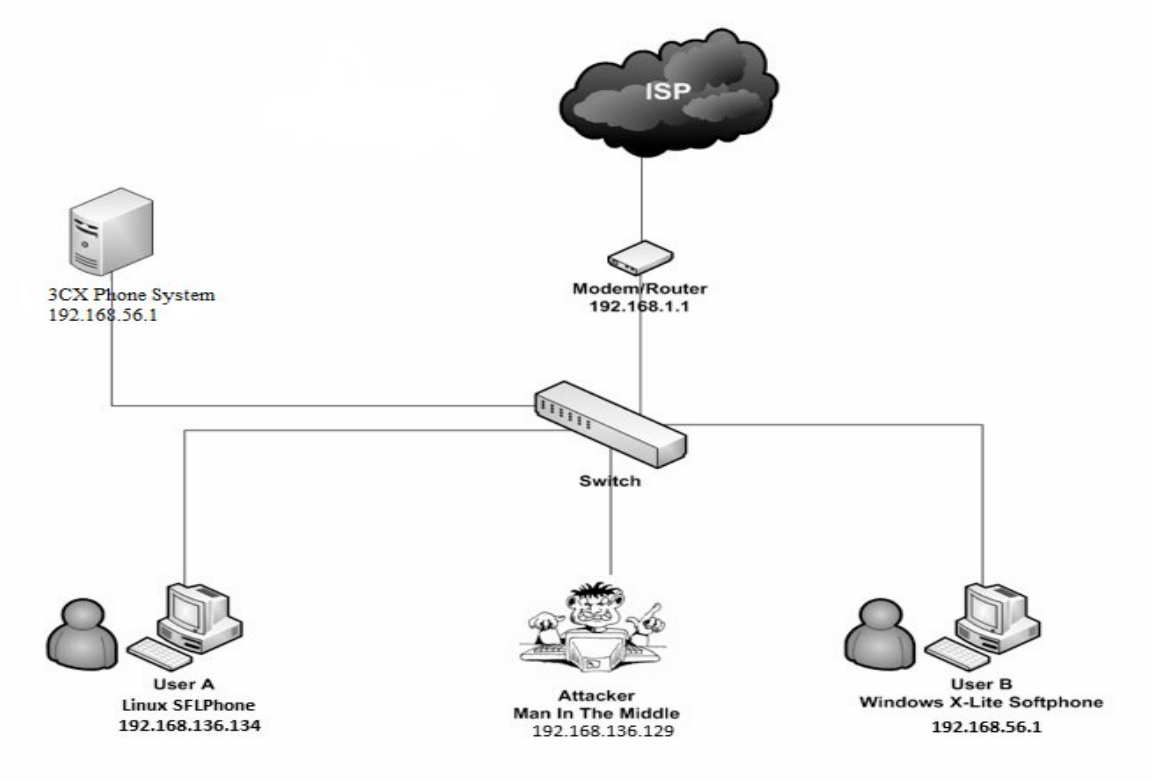

Рис. 3. Сценарий атаки «Подслушивание»

Для реализации этого сценария нам необходимо провести атаку «Человек посередине», которая потребует следующие шаги:

1. ARP-Poisoning
2. Сниффинг трафика
3. Расшифровка данных RTP в аудио файл.

Чтобы реализовать ARP-Poisoning воспользуемся утилитой Arpspoof, которая показана на рис. 4.

```
root@RgRatix:~# arpspoof -t 192.168.136.134 192.168.56.1
0:c:29:95:d1:9c 0:c:29:cb:3e:9e 0806 42: arp reply 192.168.56.1 is-at 0:c:29:95:
d1:9c
0:c:29:95:d1:9c 0:c:29:cb:3e:9e 0806 42: arp reply 192.168.56.1 is-at 0:c:29:95:
d1:9c
```

Рис. 4. Утилита Arpspoof

Оставим Arpspoof работать на фоне для проведения ARP-Poisoning и перейдем к следующему пункту.

Для сниффинга трафика и расшифровки данных RTP в аудиофайл используем Wireshark, что наглядно видно на рис. 5 и рис. 6 соответственно.

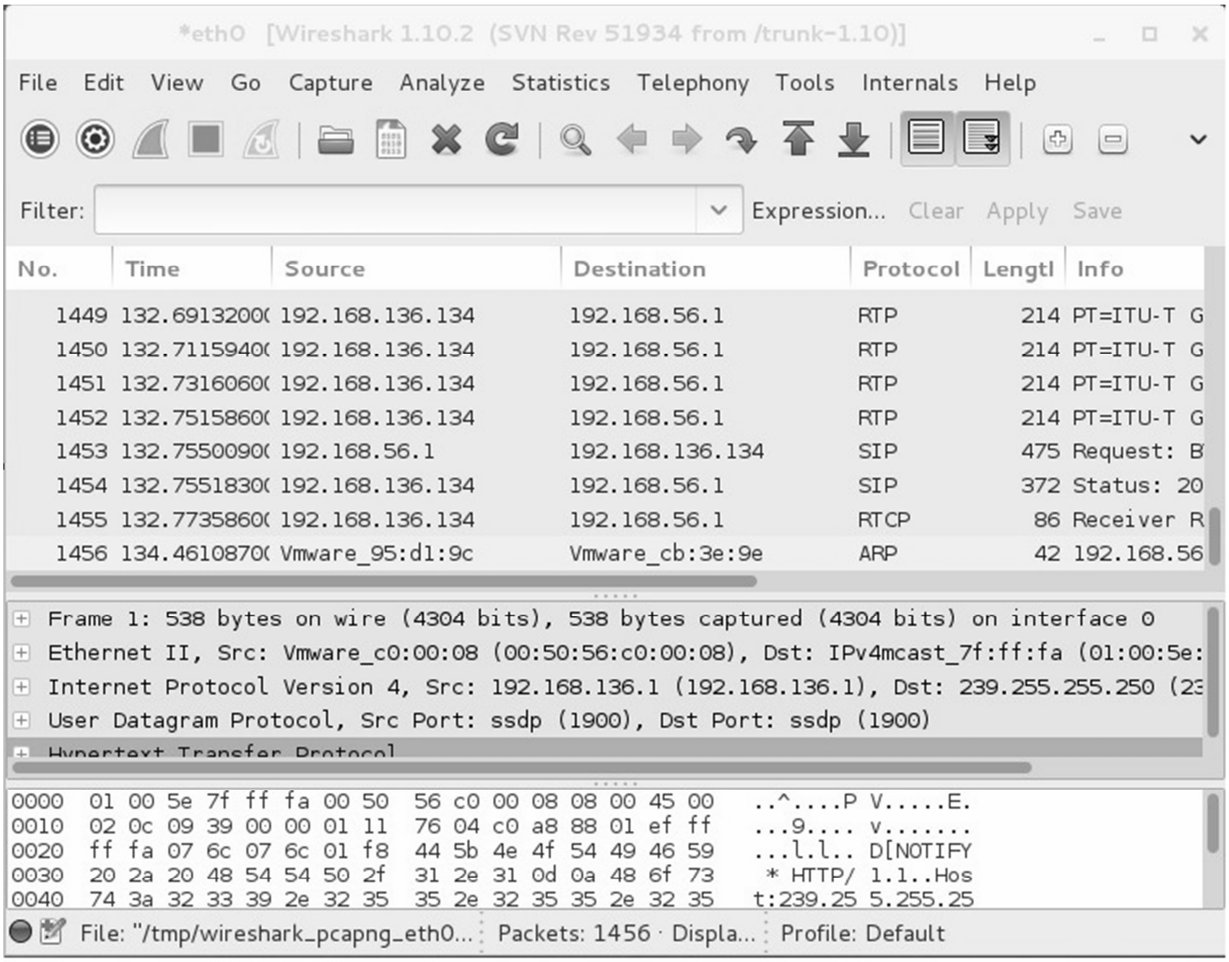

Рис. 5. Перехват RTP пакетов (сниффинг трафика) при помощи Wireshark

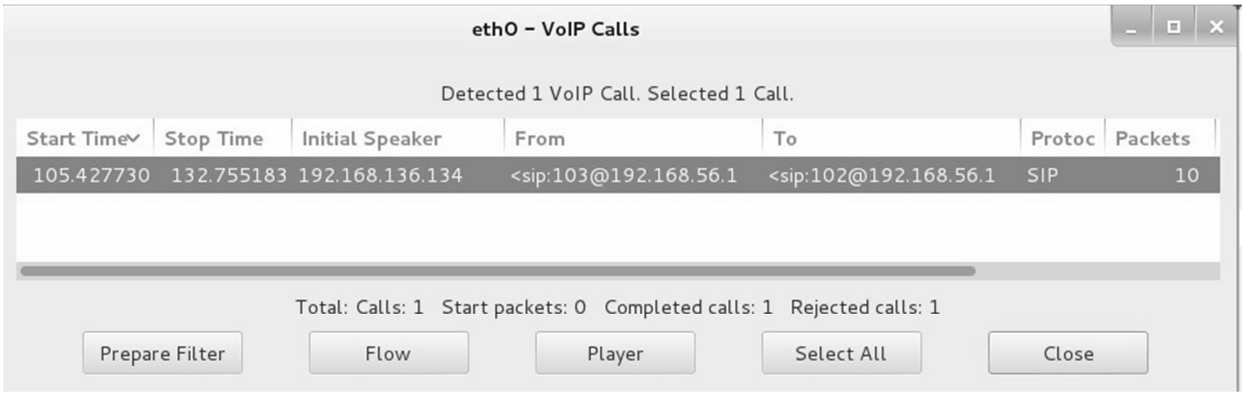

Рис. 6. Расшифровка захваченного разговора в аудиофайл при помощи Wireshark

Атака «Подмена идентификатора вызывающего абонента» (Spoofing caller ID)

Атака на SIP, вызываемая неаутентифицированным ID пользователя, которая

позволяет злоумышленнику отключить механизмы аутентификации, а также обмануть участника SIP в создании разделенного ключа со злоумышленником или заставить протокол преждевременно отключиться.

Приведем пример подмены caller ID. Для этого воспользуемся вспомогательным модулем Metalsploit — Sip_invite_spoof. Как видно из рис. 7, в результате работы с Metalsploit абоненту «102» приходит вызов от несуществующего пользователя «The Metalsploit has you» с фиктивным IP 0.0.0.0.

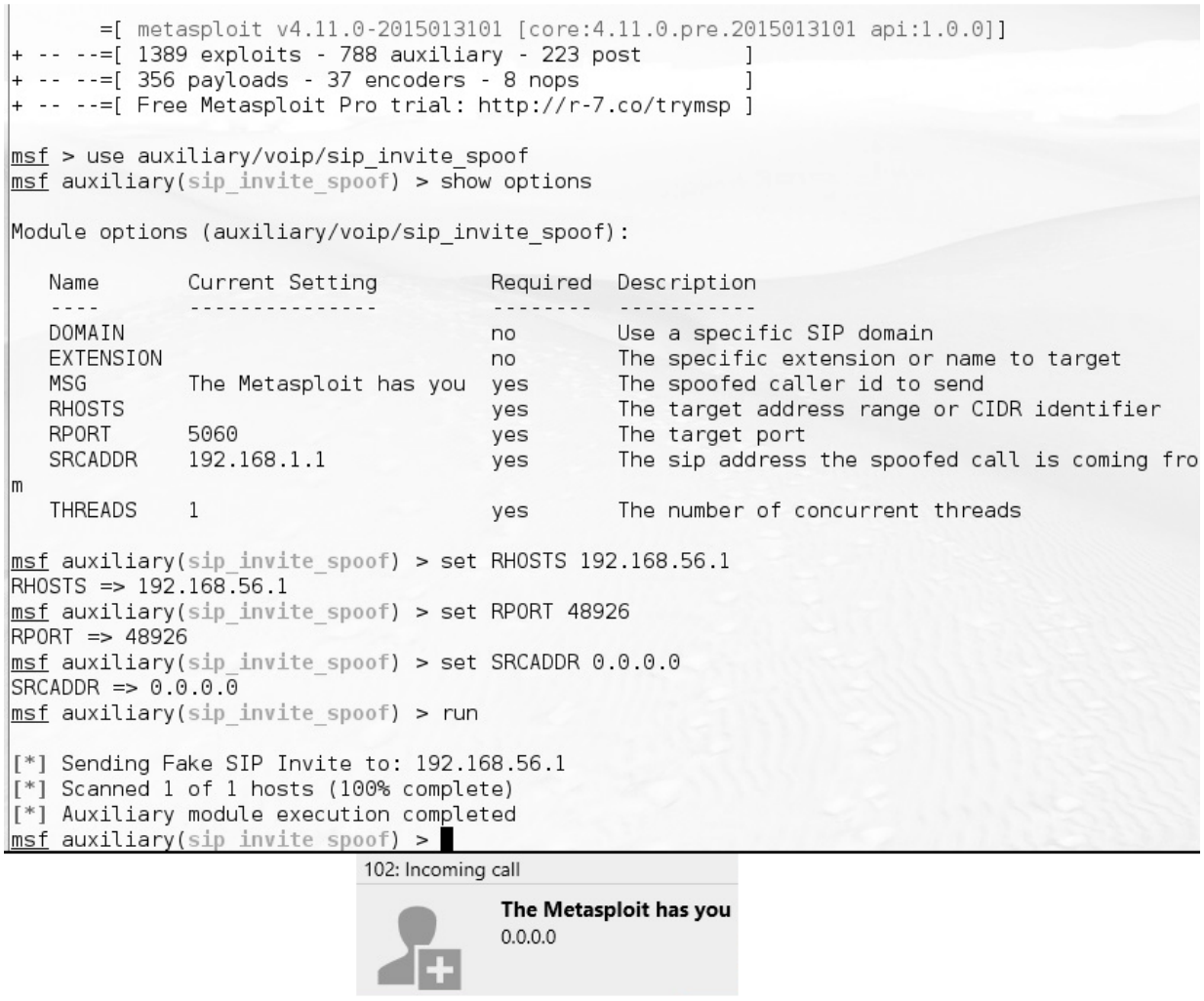

Рис. 7. Подмена caller ID

Атака «Подбор пароля» (Brute Force)

Пример подбора пароля к SIP аккаунту. Для этого нам понадобится воспользоваться тремя инструментами: SIPDump, SIPCrack и Johny The Reaper. SIPDump позволяет нам захватить ответ на верную аутентификацию, из которого мы можем узнать

caller ID и хэш пароля. Johny the Reaper мы используем для составления словаря паролей и SIPCracker для подбора пароля. Выполненную атаку можно видеть на рис. 8.

```
root@RgRatix:~# john --incremental=digits -stdout=5 >/tmp/sipcrack
Warning: MaxLen = 8 is too large for the current hash type, reduced to 5
words: 111110  time: 0:00:00:00 DONE (Mon Mar 16 21:58:58 2015)  w/s: 740733  current: 89092
root@RgRatix:~# sipcrack -w /tmp/sipcrack auth.txt

SIPcrack 0.2  ( MaJoMu | www.codito.de )
----------------------------------------

* Found Accounts:

Num     Server          Client          User    Hash|Password

1       192.168.136.129 192.168.56.1    101     f5df2254c79c21cf9e33d30c2b73eedf
* Generating static MD5 hash... 747909caf056bd17f39412e5d652702a
* Loaded wordlist: '/tmp/sipcrack'
* Starting bruteforce against user '101' (MD5: '0ff9e3d424806c733df95ff831a45602')
* Tried 8760 passwords in 0 seconds

* Found password: '54321'
* Updating dump file 'auth.txt'... done
```

Рис. 8. Brute Force

Заключение

Были выполнены атаки, такие как «Отказ в обслуживании» (Denial of service), «Прослушивание» (Eavesdropping), «Подмена идентификатора вызывающего абонента» (Spoofing caller ID), «Подбор пароля» (Brute Force) с использованием ОС Kali Linux. Результатом выполнения данных атак является наличие уязвимостей в VoIP протоколах. Представленные нами примеры атак можно использовать для тестирования на проникновение в различные VoIP системы с целью оценки их безопасности.

Список литературы

1. Gupta P., Shmatikov V. Security Analysis of Voice-over-IP Protocols // 20th IEEE Computer Security Foundations Symposium. CSF '07. Italy, Venice, 2007. С. 49-63. DOI: 10.1109/CSF.2007.31.
2. Andreasen F., Baugher M., Wing D. Session Description Protocol (SDP) Security Descriptions for Media Streams. Режим доступа: http://www.ietf.org/rfc/rfc4568.txt (дата обращения 05.03.2015).
3. Schulzrinne H., Casner S., Frederick R., Jacobson V. RTP: A Transport Protocol for Real-Time Applications. Режим доступа: http://www.ietf.org/rfc/rfc3550.txt (дата обращения 05.03.2015).
4. Бельфер Р.А. Сети и системы связи (технологии, безопасность): учеб. пособие по дисциплине «Сети и системы связи»: электронное учебное издание. М.: МГТУ им. Н.Э. Баумана, 2012. 738 с.

5. Гольдштейн Б.С., Зарубин А.А., Саморезов В.В. Протокол SIP: справочник. СПБ.: БХВ-Петербург, 2014. 456 с