ческого университета. 2017. Т. 20. № 17. С. 71-73.

9. Обухов А.В., Ляшева С.А., Шлеймович М.П. Методы автоматического распознавания автомобильных номеров// Вестник Чувашского университета. 2016. №3. С.201-208.

10.Гизатуллин З.М., Гизатуллин Р.М., Назметдинов Ф.Р., Набиев И.И. Повышение помехоустойчивости электронных средств при электромагнитных воздействиях по сети электропитания // Журнал радиоэлектроники: электронный журнал. – 2015. – №6.- С. 2.

11.Белоусов А.О., Газизов Т.Р., Заболоцкий А.М. Многопроводная микрополосковая линия как модальный фильтр для защиты от сверхкоротких импульсов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2015. – №3. – С. 124-128.

12. Газизов А.Т., Заболоцкий А.М., Газизов Т.Р. Разложение сверхкороткого импульса в структурах с лицевой связью // Известия высших учебных заведений. Физика. – 2017. – №3. – С. 70-75.

13. Белоусов А.О., Заболоцкий А.М., Газизов Т.Р. Экспериментальное подтверждение модельной фильтрации в многопроводной микрополосковой линии // Доклады Томского государственного университета систем управления и радиоэлектроники. 2016. – №3. – С. 51-54.

Д. Шкирдов

МЕТОД ЛОВУШЕК ДЛЯ СОСТАВЛЕНИЯ ЧЕРНЫХ СПИСКОВ АТАКУЮЩИХ АДРЕСОВ

(Самарский университет)

Ни для кого не секрет, что в современном мире киберпреступления активно развиваются. Сетевые ловушки являются относительно новым способом борьбы с постоянно развивающимися сценариями атак. Сетевая ловушка (она же honeypot) –это система, представляющая из себя приманку для злоумышленника. Она обычно состоит из компьютера, программ и информации, которые вместе симулируют поведение реальной системы, являющейся частью сети. Сама ловушка изолирована и контролируется, и кажется содержит информацию или ресурс, представляющий ценность для злоумышленников [1]. Добросовестным пользователям нет смысла подключаться к такой системе, поэтому наблюдение за попытками получить доступ к ловушке и активностью в ней позволяет получить сведения об уровне угроз реальной системе. Информация, полученная в результате работы ловушки сетевых служб, систематизируется и анализируется.

Для обнаружения и анализа аномальной сетевой активности IP адресов была создана инфраструктура, основанная на понятии ловушки(приманки). В качестве ловушки используется сервер с установленным на нём программным

обеспечением [2]. Данное программное обеспечение реализует ряд популярных интернет-сервисов, приведенных в Таблице 1.

Таблица 1 – основные сервисы на сервере-ловушке

Программное обеспечение	Протокол или служба
Asterisk	Интернет-телефония
Apache, Nginx	HTTP, веб-сервис
Devecot, Exim	Электронная почта
Mysql	Базы данных mysql
Samba	Служба доступа к сетевым ресурсам
Squid	Web Proxy
OpenSSH-server	Безопасное удаленное управление, ssh
Vsftpd	Протокол передачи файлов, ftp
Bind9	Сервис доменных имен, DNS
iptables	Межсетевой экран

Установленные на сервере-ловушке сервисы были выбраны из расчета их популярности и потенциальных возможностей их взлома.

Для повышения точности анализа данных были установлены подобные сервера в других частях мира. Сервера установлены в Самаре, Крыму, Ростове-на-Дону, а также США. Данные сервера не наполнялись информацией, в поисковые системы не передавались, доменные имена не присваивались. Именно поэтому любые запросы к данному сервису можно считать, как аномальную сетевую активность.

Целью данной работы является анализ поступающих запросов: определяется частота запросов на сервисы, их тип, количество атакующих IP-адресов, их географическое местоположение и сравнение полученных данных.

В ходе эксперимента каждый сервис на каждом сервере анализировался следующим образом, на примере сервиса SIP-телефонии: Было выявлено два типа атак:

- Попытки дозвониться на внутренний номер с целью поиска номера для дальнейшего подбора пароля
- Попытки подбора пароля к внутренним номерам

Проводился анализ IP-адресов, которые отправляли запросы на несколько серверов-ловушек.

Таблица 2 - Количество уникальных IP-адресов, совпавших между серверами-ловушками.

	США	**Крым**	**Ростов-на Дону**	**Самара**
США	353	59%	23%	18%
Крым	304	468	45%	32%
Ростов-на-Дону	148	281	444	27%
Самара	160	279	304	691

Составлялся черный список атакующих IP-адресов, в который входили IP-адреса атаковавших сразу два и более серверов и отправивших 3 и более запросов, а также производился анализ исходя из их географического местоположения.

В черный список для SIP-телефонии вошло 1063 IP-адреса. После анализа их географического местоположения можно сделать вывод, что среди атакующих, 85% IP-адресов расположены в странах НАТО.

Литература

1. Bao, J. Research on network security of defense based on Honeypot [Текст] / Bao, J., Ji C., Gao M. // Computer Application and System Modeling (ICCASM), 2010 International Conference on. – IEEE, 2010. – Т. 10. – С. V10-299-V10-302.

2. Sukhov A. M. Analysis of Internet service user audiences for network security problems / A.M. Sukhov, E.S. Sagatov, A.V. Baskakov //Telecommunication Technologies (ISTT), 2014 IEEE 2nd International Symposium on. – IEEE, 2014. – С. 214-219.