Научно-технические предложения по конфигурированию параметров службы доменных имен информационных систем в условиях сетевой разведки

М. С. Бодякин, e-mail: maksbody@mail.ru

Краснодарское высшее военное училища имени генерала армии С.М.Штеменко

Аннотация. *В настоящее время в области компьютерной безопасности особую актуальность набирают способы защиты информационных систем с использованием движущихся целей, основанные на конфигурировании (рандомизации, мутации) сетевых параметров, позволяющие предотвращать компьютерные атаки еще на их начальном этапе - этапе разведки. Использование этих способов дает возможность навязать противнику ложные сведения о реальной структуре и типологии информационной системы, предотвратив тем самым саму возможность осуществления компьютерной атаки.*

Ключевые слова: *информационная система, защита с использованием движущейся цели, сетевая разведка, система доменных имен.*

Введение

Большое количество компьютерных атак (КА) носит разведывательный характер с целью получения злоумышленником с помощью средств сетевой разведки (СР) информации о составе, структуре и алгоритмах функционирования информационных систем (ИС), являющейся объектом КА, а также об используемых средствах защиты ИС, что обусловлено статичностью их параметров.

В статически настроенной ИС узлы взаимодействуют через статические IP-адреса [1,2], поэтому противник посредством сетевой разведки (СР) может сканировать пространство IP-адресов, идентифицировать целевой список доменных имен или адресов после получения ответов и осуществлять КА с использованием целевого списка доменных имен или адресов. В сегментах ИС с применением средств защиты на основе конфигурирования IP-адресов, основанной на сопоставлении доменных имен, IP-адрес хоста постоянно меняется, и поэтому противник не может поддерживать целевой список IP-адресов. Однако, доменное имя хоста остается статичным, и поэтому злоумышленник может поддерживать доменную базу списка для

атаки [2]. Кроме того, ограниченная пространством IP-адресов перестановка сетевых адресов не может эффективно защитить от случайных сканирующих атак [3,4].

1. Материалы и результаты исследования

Разработан ряд научно-технических предложений по динамическому конфигурированию параметров ИС [5,6]. Однако, большинство из предложений, основанных на изменении сетевых адресов хостов, ограничены в возможностях в связи с конечным размером сетевого адресного пространства и полагаются на статическое доменное имя хоста для сопоставления с его динамическим адресом.

Таким образом, эти методы не обеспечивают в полной мере требуемый уровень защиты от злоумышленника, знающего доменное имя цели [7].

Разработанное научно-техническое предложение конфигурирования параметров службы доменных имен позволяет повысить результативность защиты за счет использования пространства доменных имен, емкость которого намного больше емкости адресного пространства IP-адресов, что значительно увеличивает сложность идентификации параметров ИС для злоумышленника.

На рис. 1 показана схема защищаемой с использованием конфигурирования параметров службы доменных имен ИС от СР, где все узлы соединены друг с другом посредством коммутатора.

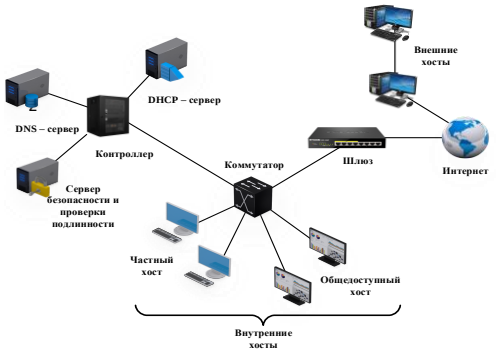


Рис. 1 Схема защищаемой ИС от СР с использованием конфигурирования параметров службы доменных имен

На представленной схеме коммутатор предназначен для изменения маршрутов следования и переправления пакетов, контроллер выступает центральным управляющим звеном над всеми коммутаторами сети, управляя их таблицами потоков и взаимодействуя с доверенным DNS-

сервером, DHCP-сервером и сервером безопасности и проверки подлинности.

На рис. 2 представлена блок-схема алгоритма, реализующая разработанное научно-техническое предложение, где приняты следующие обозначения:

n – максимальное допустимое значение количества IP-адресов узлов ИС;

$\{IP^d\}$ – множество всех IP-адресов узлов ИС, являющихся клиентами DHCP-сервера с IP-адресом IP^d_{dhcp}, где d – номер подсети DHCP-сервера d = 1, 2 … z, а z – максимальное количество подсетей;

[D] – массив памяти для хранения номера подсети DHCP-сервера;

t^d_{max} – максимальное значение времени аренды всех IP-адресов узлов подсети с номером d ИС;

CIP_m – идентификатор соединения между узлами ИС;

$[C_i]$ – массив памяти для хранения идентификаторов CIPm;

{TS} – множество идентификаторов санкционированных информационных потоков;

{MAC} – множество MAC-адресов сетевых устройств узлов ИС;

$[N_A]$ – массив памяти для хранения матрицы соответствия n-му IP-адресу узла ИС из множества IP-адресов l-го MAC-адреса из массива памяти MAC;

{DNS} – множество доменных имен узлов поддомена ИС, где k – максимальное допустимое значение количества доменных имен сетевых устройств поддомена k>>n;

u – номер поддомена, u=1, 2, …, U, где U – максимальное количество поддоменов;

IP^u_{DNS} –IP-адреса DNS-сервера поддомена u;

T^u_{max} – максимальное значение времени «жизни» всех доменных имен поддомена u;

[DP] – массив памяти для хранения номера поддомена;

$[N_P]$ – массив памяти для хранения матрицы соответствия n-му IP-адресу узла ИС из множества IP-адресов k-го доменного имени из множества {DNS}.

Задают исходные данные (см. блок 1 на рис. 2) $IP = \{IP_1, IP_2 \dots IP_n\}$ множество IP-адресов узлов ИС, являющихся DHCP-клиентами DHCP-сервера, где n – максимальное допустимое значение количества IP-адресов узлов ИС. Далее задают $C = \{CIP_1, CIP_2 \dots CIP_m\}$ множество соединений между узлами ИС, где CIP_m – идентификатор соединения между узлами ИС. После этого задают $MAC = \{MAC_1, MAC_2 \dots MAC_l\}$ множество MAC-адресов сетевых устройств узлов ИС, где l – максимальное количество сетевых устройств узлов ИС, массив памяти

N_A для хранения матрицы соответствия n-му IP-адресу узла ИС из множества IP-адресов l-го MAC-адреса из массива памяти MAC, также задают подмножества d в множестве IP-адресов узлов ИС $IP^d = \{IP^d_1, IP^d_2 \dots IP^d_n\}$, где d – номер подсети DHCP-сервера, d = 1, 2 … z, где z – максимальное количество подсетей, для каждого подмножества d предварительно задают IP-адреса DHCP-серверов IP^d_{dhcp}, где IP^d_{dhcp} – IP-адрес DHCP-сервера для подмножества d, $IP^d_{dhcp} \in IP^d$, массив памяти D = [1, 2, …, z] для хранения номера подсети DHCP-сервера.

Далее задают {DNS} – множество доменных имен узлов поддомена ИС, где k – максимальное допустимое значение количества доменных имен сетевых устройств поддомена k>>n, а также задают u – номер поддомена, u=1, 2, …, U, где U – максимальное количество поддоменов. После этого задают T^u_{max} – максимальное значение времени «жизни» всех доменных имен поддомена u, [DP] – массив памяти для хранения номера поддомена и $[N_P]$ – массив памяти для хранения матрицы соответствия n-му IP-адресу узла ИС из множества IP-адресов k-го доменного имени из множества {DNS}.

Подключают (см. блок 2 на рис. 2) сетевые устройства в ИС. Далее, после направления с сетевых устройств ИС сообщений на DHCP-сервер для получения IP-адресов, времени их аренды, номера подсети и других сетевых параметров, приема DHCP-сервером с IP-адресом IP^d_{dhcp} сообщений от сетевых устройств ИС, формируют (см. блок 3 на рис. 2) DHCP-сервером параметры синхронизации установленного часового пояса и времени, назначенные IP-адреса и другие сетевые параметры для узлов ИС в подсети d.

Устанавливают (см. блок 4 на рис. 2) на DHCP-сервере соответствия MAC- и IP-адресов в подсети d и запоминают (см. блок 5 на рис. 2) его в массиве памяти N_A.

Далее направляют (см. блок 6 на рис. 2) значения параметров синхронизации установленного часового пояса и времени, назначенные IP-адреса и другие сетевые параметры для узлов ИС в подсети d на контроллер. В качестве контроллера выступает один из узлов ИС с предустановленным специальным программным обеспечением, содержащий массивы памяти для хранения таблиц соответствия значений IP-адресов узлов ИС и доменных имен в текущей и последующих конфигурациях. Контроллер взаимодействует с DHCP и DNS серверами, а также штатными средствами защиты ИС. Он осуществляет прием сообщений от средств защиты о факте воздействия средств СР, прием и хранение сетевых параметров узлов ИС, а также выдачу команд на прекращение аренды текущих сетевых параметров узлов, формирование и назначение новых и выдачу более неактуальных

средствам СР на их запросы после очередного цикла реконфигурации параметров ИС. Контроллер осуществляет взаимодействие с несколькими подсетями ИС и не принадлежит ни одной из них.

После этого направляют (см. блок 7 на рис. 2) значения параметров синхронизации установленного часового пояса и времени, назначенные IP-адреса и другие сетевые параметры для узлов ИС в подсети d на DNS сервер.

Затем формируют (см. блок 8 на рис. 2) DNS имена для узлов ИС для u-го поддомена ИС.

Устанавливают (см. блок 9 на рис. 2) соответствие IP-адресов и DNS имен узлов ИС и запоминают (см. блок 10 на рис. 2) данное соответствие в массиве памяти $[N_P]$.

Далее направляют (см. блок 11 на рис. 2) сформированные DNS имена и время их «жизни» T^u на контроллер, где его запоминают (см. блок 12 на рис. 2) и направляют (см. блок 13 на рис. 2) IP-адреса для подсети d, а DNS имена для поддомена u узлам ИС и задают (см. блок 14 на рис. 2) каждую соответствующую пару IP-адреса и DNS имени узлам ИС.

Устанавливают (см. блок 15 на рис. 2) сетевые соединения между узлами ИС. После чего назначают (см. блок 16 на рис. 2) установленным соединениям идентификаторы соединения между узлами ИС.

Далее принимают (см. блок 17 на рис. 2) из канала связи пакет сообщений и выделяют (см. блок 18 на рис. 2) из заголовка идентификатор информационного потока и сравнивают (см. блок 19 на рис. 2) его с предварительно заданными идентификаторами санкционированных информационных потоков.

В случае, если идентификатор информационного потока принадлежит (см. блок 19 на рис. 2) предварительно заданными идентификаторам санкционированных информационных потоков, то определяют (см. блок 20 на рис. 2) является ли сообщение запросом к DNS. Если данное сообщение является запросом к DNS, то направляют (см. блок 21 на рис. 2) в ответ DNS имя и IP-адрес, для чего производят поиск соответствия, запрашиваемого DNS имени рекурсивным либо итеративным методом, в зависимости от настроек DNS – сервера. Затем передают (см. блок 22 на рис. 2) пакет получателю и принимают из канала связи следующий пакет сообщения. Если данное сообщение не является запросом к DNS, то сразу передают пакет получателю.

В обратном случае, если идентификатор информационного потока не принадлежит предварительно заданными идентификаторам санкционированных информационных потоков, то направляют (см. блок

23 на рис. 2) запрос на контроллер на конфигурирование IP-адресов и DNS имен узлов ИС.

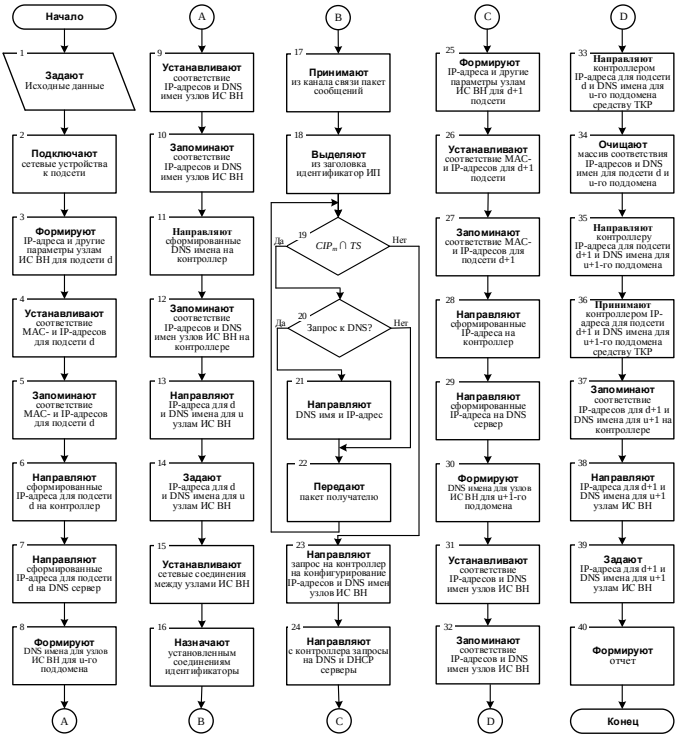


Рис. 2. Блок-схема последовательности действий, реализующая научно-технические предложение по защите ИС от СР на основе конфигурирования доменных имен

После чего, контроллером направляют (см. блок 24 на рис. 2) запросы на DNS и DHCP серверы о прекращении T^u времени «жизни» всех доменных имен поддомена u формировании параметров для поддомена u+1 и t^d времени аренды всех IP-адресов узлов подсети с номером d ИС и формировании параметров для подсети d+1.

Далее, после направления с контролера сообщений на DHCP-сервер для получения IP-адресов, времени их аренды, номера подсети и других сетевых параметров, приема DHCP-сервером с IP-адресом IP^{d+1}_{dhcp} сообщений от сетевых устройств ИС, формируют (см. блок 25 на рис. 2) DHCP-сервером параметры синхронизации установленного

часового пояса и времени, назначенные IP-адреса и другие сетевые параметры для узлов ИС в подсети d+1.

Устанавливают (см. блок 26 на рис. 2) на DHCP-сервере соответствия MAC- и IP-адресов в подсети d+1 и запоминают (см. блок 27 на рис. 2) его в массиве памяти N_A.

Затем направляют (см. блок 28 на рис. 2) значения параметров синхронизации установленного часового пояса и времени, назначенные IP-адреса и другие сетевые параметры для узлов ИС в подсети d+1 на контроллер.

После этого направляют (см. блок 29 на рис. 2) значения параметров синхронизации установленного часового пояса и времени, назначенные IP-адреса и другие сетевые параметры для узлов ИС в подсети d+1 на DNS сервер.

На DNS сервере формируют (см. блок 30 на рис. 2) DNS имена для узлов ИС для u+1-го поддомена ИС.

Устанавливают (см. блок 31 на рис. 2) соответствие IP-адресов и DNS имен узлов ИС и запоминают (см. блок 32 на рис. 2) данное соответствие в массиве памяти [NP] для поддомена u+1.

Далее направляют (см. блок 33 на рис. 2) контроллером IP-адреса для подсети d и DNS имена для u-го поддомена средству СР, вводя его тем самым в заблуждение, и очищают (см. блок 34 на рис. 2) массив соответствия IP-адресов и DNS имен для подсети d и u-го поддомена

После этого направляют (см. блок 35 на рис. 2) сформированные DNS имена и время их «жизни» T^u на контроллер.

Принимают (см. блок 36 на рис. 2) контроллером IP-адреса для подсети d+1 и DNS имена для u+1-го поддомена, запоминают (см. блок 37 на рис. 2) их и направляют (см. блок 38 на рис. 2) IP-адреса для подсети d+1, а DNS имена для поддомена u+1 узлам ИС и задают (см. блок 39 на рис. 2) каждую соответствующую пару IP-адреса и DNS имени узлам ИС и формируется отчет.

Результативность полученного технического решения была проверена путем программной реализации предложения и проведения имитационного моделирования. Суть моделирования – оценка результативности конфигурирования параметров сегмента ИС в условиях идентификации противником IP-адресов узлов и DNS имен.

Моделирование исследуемого процесса осуществлялось в среде EVE–NG. Схема сегмента ИС для проведения моделирования приведена на рис. 3 и включает следующие элементы: 1 – сервер защиты с предустановелнным СПО защиты; 2- рабочие станции (ОС Windows 10); 3 - средство СР (ОС Kali Linux 2020.2); 4 – FTP-сервер; 5 - коммутационное оборудование (коммутатор).

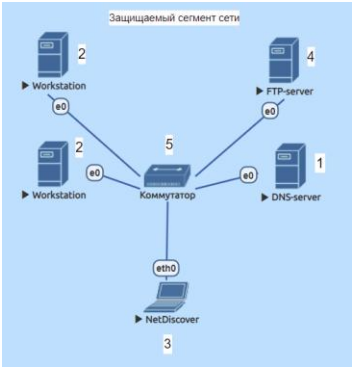
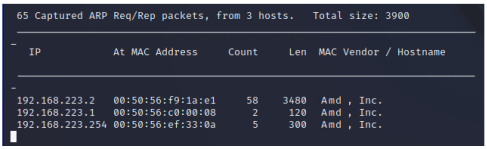


Рис. 3. Схема сегмента ИС для проведения моделирования процесса конфигурирования параметров в условиях СР

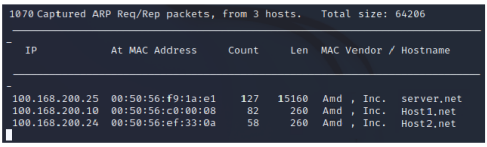
В качестве средства конфигурирования параметров ИС применен свободно распространяемый динамический DNS-сервер с открытым исходным кодом (в виде СПО), который позволяет конфигурировать параметры ИС [8, 9]. В качестве средства СР использовано автоматизированное рабочее место (АРМ) с предустановленной операционной системой Kali Linux. Для оценки возможности идентификации параметров ИС [10] смоделировано применение противником многофункционального сетевого сканера NetDiscover, экранная форма интерфейса которого приведена на рис. 3. Средство СР Netdiscover способно функционировать в 2-х режимах: активном и пассивном. В активном – средство направляет запросы в виде пакетов сообщений для идентификации DNS имен и IP-адресов, в пассивном – только анализирует транзитные пакеты сетевого трафика между абонентами и коммутационным оборудованием.

На рис. 4 приведены экранные формы, отображающие оценку результативности разработанного научно-технического предложения на различных этапах моделирования.

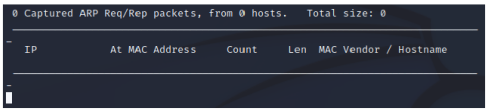
В ходе первого этапа моделирования параметры ИС были идентифицированы средством СР без противодействия со стороны средства защиты (динамического DNS-сервера), осуществлялась идентификация только IP-адресов ИС. Средство СР функционировало в активном режиме, направляя сканирующие запросы на узлы ИС. Из рис. 4 видно, что противник идентифицировал всех абонентов защищаемой сети за 65 принятых пакетов.



а



б



в

Рис. 4. Экранная форма, отображающая результаты идентификации параметров ИС средством NetDiscover в ходе моделирования (а-первый этап, б – второй этап, в – третий этап)

В ходе второго этапа моделирования осуществлялась идентификация средствами СР IP-адресов и DNS имен узлов ИС. Средство СР функционировало в пассивном режиме, только на прием пакетов от узлов ИС. Конфигурирование параметров ИС осуществлялось с применением средства защиты (динамического DNS-сервера), изменяющего IP-адреса и маску подсети узлов сегмента ИС с частотой, большей, чем цикл СР (сетевого сканирования). Это увеличивало время идентификации параметров ИС, однако все IP-адреса и DNS имена узлов были вскрыты. Из рис. 4 видно, что средство СР идентифицировало все узлы ИС перехватив 1070 пакетов.

В ходе третьего этапа моделирования параметров ИС (IP-адреса и DNS имена) конфигурировались средством защиты после выявления активности средств СР. Средство СР функционировало как в активном, так и в пассивном режимах. Высокая интенсивность конфигурирования параметров ИС динамическим DNS-сервером с сохранением информационного обмена между узлами за счет использования DNS-имен, позволила обеспечить невозможность вскрытия параметров средством СР.

Заключение

Таким образом, результаты проведенного моделирования показали, что в разработанном способе, в отличие от известных, обеспечивается расширение области применения, повышение результативности и снижение ресурсоемкости защиты. Расширение области применения обеспечивается за счет того, что конфигурирование параметров ИС производят в рамках задаваемого диапазона подсетей без разрыва критически важных соединений за счет организации сетевого взаимодействия посредством DNS имен. Конфигурирование DNS имен узлов ИС производится в пределах нескольких поддоменов, что в совокупности с изменением IP-адресов значительно усложняет процедуру вычисления противником алгоритма функционирования средств защиты и затрудняет идентификацию параметров ИС.

Литература

1. RFC 791. Internet protocol (IP). 1981. [Электронный ресурс]: база данных. – URL: https://tools.ietf.org/html/rfc791 (дата обращения: 15.12.2022).
2. RFC 1035. Domain names implementation and specification (DNS). 1987. [Электронный ресурс]: база данных. – URL: https://tools.ietf.org/html/rfc1035 (дата обращения: 15.12.2022).
3. Душкин, А. В. Способ повышения эффективности распознования несанкционированных воздействий на ИТКС. / А. В. Душкин, В. Н. Похващев, С. П. Соколовский // Информация и безопасность. – 2010. – Т. 13. – № 1. – С. 97-102.
4. Результаты анализа способов компрометации средств защиты информации / А. Л. Гаврилов [и др.] // Технические и технологические системы: Материалы девятой Международной научной конференции «ТТС-17», Краснодар, 22–24 ноября 2017 года / Кубанский государственный технологический университет, Краснодарское высшее военное авиационное училище летчиков имени А.К. Серова - 2017. – Т1 - С. 117-121.
5. Патент № 2696330 C1 Российская Федерация, МПК G06F 21/50, G06F 21/60, H04L 9/00. Способ защиты вычислительных сетей: № 2018128075 : заявл. 31.07.2018 : опубл. 01.08.2019 / В. В. Барабанов, А. А. Ефремов, Р. В. Максимов [и др.]; заявитель Краснодарское высшее военное училище имени генерала армии С.М. Штеменко Министерство обороны Российской Федерации.
6. Соколовский, С.П. Поиск новых технических решений по маскированию структуры вычислительных сетей на основе динамического конфигурирования их параметров / С. П. Соколовский, И. С. Ворончихин, А. Д. Гритчин // Решетневские чтения : Материалы

XXIII Международной научно-практической конференции, посвященной памяти генерального конструктора ракетно-космических систем академика М.Ф. Решетнева. В 2-х частях, Красноярск, 11–15 ноября 2019 года - 2019. – Т2 - С. 447-448.

7. Поддержка принятия управленческих решений в сфере информационной безопасности в терминах теории игр / С. П. Соколовский [и др.] // Вестник Воронежского института ФСИН России. – 2018. – № 2. – С. 46-54.

8. Душкин, А. В. Способ распознавания вредоносных воздействий на информационную систему / А. В. Душкин, В. Н. Похващев, С. П. Соколовский // Телекоммуникации. – 2011. – № 10. – С. 25-28.

9. Соколовский, С. П. Применение адаптивных нечетких систем в вопросах разработки средств выявления несанкционированных воздействий на информацию / С. П. Соколовский, Н. А. Усов // Информатика: проблемы, методология, технологии : материалы XVI Международной научно-методической конференции, Воронеж, 11–12 февраля 2016 года . - 2016. – С. 259-264.

10. Душкин, А. В. Нейросетевая реализация модуля выявления НСД на ИТКС специального назначения / А. В. Душкин, С. П. Соколовский // Информация и безопасность. – 2010. – Т. 13. – № 1. – С. 123-126.