ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI: 10.21822/2073-6185-2024-51-2-53-61 Оригинальная статья /Original article

Анализ особенностей реализации атаки «сканирование портов» с использованием компьютера-«зомби»

Н.В. Болдырихин, М.В. Карпенко, И.А. Сосновский, Э.А. Ядрец
Донской государственный технический университет,
344003, г.Ростов-на-Дону, пл. Гагарина, 1, Россия

Резюме. Цель. Проанализировать особенности реализации атаки «сканирование портов» с использованием компьютера-«зомби» для сокрытия IP-адреса атакующей машины. **Метод.** В основе метода рассматривается компьютерное моделирование атаки «сканирование портов» с использованием виртуальной сетевой инфраструктуры. **Результат.** Проанализированы теоретические аспекты, связанные с реализацией атаки «сканирование портов» с использованием компьютера – «зомби». Указаны параметры, по которым выбирается в сети «зомби»-машина. Проведено компьютерное моделирование атаки «сканирование портов» с использованием виртуальной сетевой инфраструктуры. Приведены результаты моделирования, иллюстрирующие успешную реализацию атаки. Предложен простой способ противодействия данной атаке. **Вывод**. При реализации атаки «сканирование портов» с использованием утилиты Nmap можно получить много ценной информации, связанной с открытыми TCP-портами и службами, запущенными на атакуемых системах. Для обеспечения безопасности при проведении сканирования портов злоумышленники могут успешно использовать технологию маскировки IP-адреса атакующей машины посредством использования «зомби»-компьютера. Методика замены IP-адреса атакующего на IP -адрес «зомби»-машины является не только эффективной, но и безопасной для злоумышленников. За счет использования «зомби»-машины злоумышленник сканирует порты, не раскрывая свое реальное местоположение, что позволяет ему избежать правовых последствий, связанных с незаконной активностью в сети. Анализируя данные, полученные после сканирования, злоумышленник может получить информацию о том, какие порты открыты у целевого компьютера и составить карту уязвимостей атакуемой системы. В качестве способа защиты от рассмотренной атаки достаточно использовать брандмауэр Windows со стандартными настройками.

Ключевые слова: информационная безопасность, сетевые атаки, сканирование портов, утилита Nmap, подмена IP-адреса, компьютер- «зомби»

Для цитирования: Н.В. Болдырихин, М.В. Карпенко, И.А. Сосновский, Э.А. Ядрец. Анализ особенностей реализации атаки «сканирование портов» с использованием компьютера-«зомби». Вестник Дагестанского государственного технического университета. Технические науки. 2024; 51(2):53-61. DOI:10.21822/2073-6185-2024-51-2-53-61

Analysis of features of implementing a “Port scanning” attack using a “Zombie” computer

N.V. Boldyrikhin, M.V. Karpenko, I.A. Sosnovsky, E.A. Yadrets
Don State Technical University,
1 Gagarina Square, Rostov-on-Don 344003, Russia

Abstract. Objective. Analyze the implementation features of a “Port scanning” attack using a “Zombie” computer to hide the IP address of the attacking machine. **Method.** The method is based on computer simulation of a “port scanning” attack using a virtual infrastructure of the network. **Result.** Theoretical aspects related to the implementation of a “port scanning” attack using a “zombie” computer are analyzed. The parameters by which a “zombie” machine is

selected on the network are indicated. A computer simulation of a “port scanning” attack using a virtual infrastructure of the network was carried out. Simulation results illustrating the successful implementation of the attack are presented. A simple way to counter this attack is proposed. **Conclusion.** When implementing a port scanning attack using the Nmap utility, you can obtain a lot of valuable information related to open TCP ports and services running on the attacked systems. To ensure security when conducting port scanning, attackers can successfully use technology to mask the IP address of the attacking machine by using a “zombie” computer. The technique of replacing the attacker’s IP address with the IP address of a “zombie” machine is not only effective, but also safe for attackers. By using a “zombie” machine, the attacker scans ports without revealing his real location, which allows him to avoid legal consequences associated with illegal activity on the network. By analyzing the data obtained after scanning, an attacker can obtain information about which ports are open on the target computer and create a map of the vulnerabilities of the attacked system. As a way to protect against this attack, it is enough to use the Windows Firewall with standard settings.

Keywords: information security, network attacks, port scanning, Nmap utility, IP address spoofing, zombie computer

For citation: N.V. Boldyrikhin, M.V. Karpenko, I.A. Sosnovsky, E.A. Yadrets. Analysis of features of implementing a “Port scanning” attack using a “Zombie” computer. Herald of Daghestan State Technical University. Technical Sciences. 2024; 51(2):53-61. DOI:10.21822/2073-6185-2024-51-2-53-61

Введение. На сегодняшний день интернет представляет из себя очень сложную структуру со множеством различных сетей, ресурсов и пользователей с их данными. Наряду с неоспоримыми преимуществами, которые предоставляют современные сетевые технологии, появилось много возможностей для злоумышленников, которые могут удаленно проникать в компьютеры, похищать данные пользователей и организаций, мешать нормальному функционированию информационных систем. В целом, проблема обеспечения информационной безопасности актуальна как никогда [1-10].

При использовании сетевых протоколов реализуется большое количество самых разных атак, в том числе позволяющих осуществить несанкционированный доступ к информации, захватить управление одним или несколькими компьютерами, распространить вредоносное программное обеспечение. Однако перед этим злоумышленник, как правило, изучает структуру сети, определяет компьютеры и серверы, их IP – адреса, какие установлены операционные системы, какие запущены службы и приложения [1-10]. Эти действия позволят выявить уязвимости, характерные для конкретных информационных систем и определить дальнейший вектор атаки. Для определения приложений и служб, запущенных на целевой машине, используют сканирование TCP-портов с помощью специальных утилит (например, Nmap). Открытый 20 и 21 порты свидетельствуют о запущенном протоколе FTP, 80 и 443 порты используют протоколы HTTP и HTTPS соответственно, открытый 23 порт позволяет удаленно подключаться по протоколу Telnet и т.д.

Следует отметить, что проведение атаки «сканирование портов» может привести к деанонимизации злоумышленника, поэтому для этих целей хакеры предпочитают использовать некоего посредника, с которого поступают запросы на целевую машину. Поскольку посредник не знает о том, что участвует в атаке, то его называют «зомби»-компьютером или «зомби»-машиной.

Постановка задачи. В рамках данного исследования поставлена задача рассмотреть теоретические и практические особенности реализации атаки «сканирование портов» с использованием компьютера-«зомби», проиллюстрировать реализацию атаки на основе специально созданной для этого виртуальной сетевой инфраструктуры, состоящей из трёх виртуальных машин, связанных сетью: атакующей машины, «зомби»-машины, и атакуемой машины.

Методы исследования. В качестве метода исследования использовался метод компьютерного моделирования атаки «сканирование портов» с использованием виртуальной сетевой инфраструктуры. Результаты исследований в данном случае ничем не отчаются от результатов, проводимых с использованием реального сетевого оборудования, при условии одинаковой конфигурации виртуальных и реальных машин.

Сама атака «сканирование портов» реализовывалась с помощью утилиты Nmap. Этот метод включает в себя отправку сообщения на TCP - порт и прослушивания ответа. Полученный ответ указывает на состояние порта: открытое или закрытое состояние. Nmap использует различные методы активного зондирования и может изменять параметры пакетов и использовать для анонимизации своей деструктивной деятельности в сети различные способы. Функционал, предоставляемый утилитой Nmap, достаточно широк.

В целом, существует два вида сканирования портов:

- вертикальное сканирование, предполагающее сканирование всех TCP – портов на одном компьютере;
- горизонтальное сканирование предполагающее сканирование одного TCP – порта на разных компьютерах, находящихся в сети.

Горизонтальное сканирование, как правило предшествует массовой атаке, а вертикальное нацелено на поиск уязвимостей на конкретной целевой машине. С помощью Nmap можно проводить оба вида сканирования. Также данная утилита дает возможность осуществлять поиск активных компьютеров в сети, проводить сканирование определенных портов, определять поддерживаемые IP-протоколы, идентифицировать операционные системы, обнаруживать межсетевые экраны, осуществлять подмену MAC-адреса атакующей машины и т.д.

В рамках данного исследования рассматривается процесс скрытного сканирования портов с использованием «зомби»-машины, от имени которой производится такое сканирование. Процесс «зомби» - сканирования заключается в первоначальном поиске «зомби» машины, IP - адрес которой используется для дальнейшего проведения атаки. Суть поиска такой машины заключается в отправке TCP-сегментов с установленными флагами SYN/ACK на предполагаемый «зомби»-компьютер. В свою очередь потенциальный «зомби» в соответствии с протоколом TCP должен отвечать на такие запросы сегментами с установленным флагом RST потому, что процессу установления соединения не предшествовал сегмент с флагом SYN.

При этом ID (идентификатор IP-пакета, переносящего сегмент) должен увеличиваться на одну единицу в каждом новом пакете. Если это условие не выполняется, то значит данный компьютер не подходит на роль «зомби». Обычно хорошо работают в качестве «зомби» компьютеры под управлением операционных систем Windows, MacOS, FreeBSD. Операционные системы OpenBSD, Solaris, Linux обладают иммунитетом против использования в роли «зомби». Однако в качестве жертвы «зомби»-сканирования может оказаться компьютер под управлением любой операционной системы.

Чтобы проверить уязвимость компьютера к использованию его в роли «зомби» - достаточно просто запустить Nmap с параметрами IdleScan. Утилита Nmap автоматически проверит указанный компьютер и сообщит о возможности использования его в роли «зомби».

На рис. 1, 2 проиллюстрирован процесс «зомби»-сканирования. Сначала сканирующий компьютер отправляет на «зомби»-компьютер TCP-сегмент с установленными флагами SYN/ACK. «Зомби» отвечает сегментом с флагом RST. Сканирующий компьютер запоминает при этом ID пакета, полученного от «зомби» (рис.1).

Далее сканирующий компьютер отправляет на целевую машину сегмент с установленным флагом SYN, предлагая установить TCP-соединение. Однако в заголовке сетевого уровня IP-пакета, указывается IP-адрес не сканирующего компьютера, от которого реально пришел пакет, а IP-адрес «зомби»-машины.

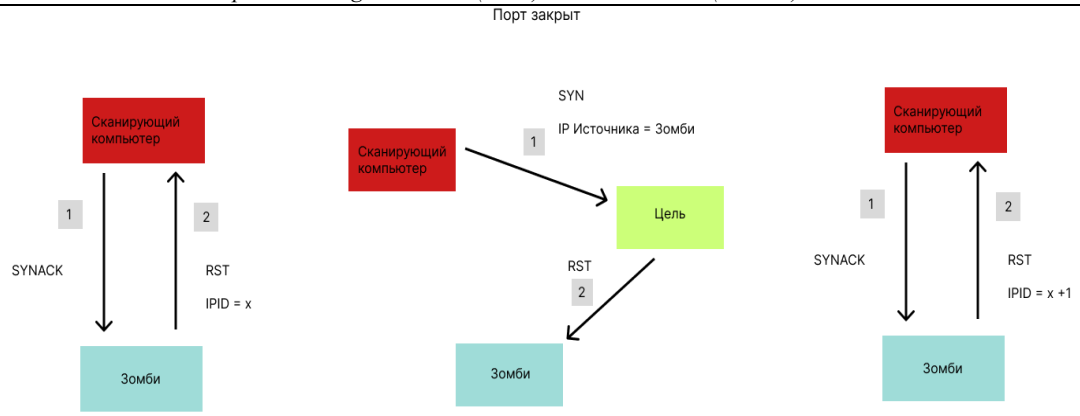

Рис. 1. Иллюстрация работы «зомби»-сканирования при закрытом состоянии порта на целевой машине

Fig. 1. Illustration of how zombie scanning works when the port is closed on the target machine

Если порт целевого компьютера, закрыт, то тогда будет отправлен сегмент с флагом RST от целевого компьютера на «зомби»-машину, поскольку от её имени была попытка установки соединения. При получении пакета с сегментом RST, «зомби»-машина его просто проигнорирует и ID её пакетов не изменится.

После этого сканирующий компьютер отправляет на «зомби»-машину TCP-сегмент с установленными флагами SYN/ACK. В ответ «зомби»-машина пришлет сегмент с флагом RST, а ID пакета, пришедшего от «зомби», увеличится на единицу, что и будет свидетельствовать о закрытом состоянии порта целевой машины.

Рис. 2. Иллюстрация работы «зомби»-сканирования при открытом порте

Fig. 2. Illustration of zombie scanning with an open port

В случае открытого порта на целевой машине, в ответ на сканирующий зарос от атакующей машины она ответит сегментом с флагами SYN/ACK на компьютер «зомби». Однако компьютер «зомби» не посылал запрос на создание соединения, поэтому он ответит целевой машине сегментом с флагом RST (рис. 2).

При этом значение ID пакета «зомби»-машины увеличится на единицу. Далее, сканирующий компьютер, как и в предыдущем случае, отправляет на «зомби»-машину TCP-сегмент с установленными флагами SYN/ACK. В ответ «зомби»-машина пришлет сегмент с флагом RST, а ID пакета, пришедшего от «зомби», увеличится на 2, что и будет свидетельствовать об открытом состоянии порта целевой машины. Таким образом, если ID пакета «зомби»-машины увеличивается на 1, по сравнению с исходным состоянием, значит порт целевой машины закрыт, если на 2, то порт открыт.

Обсуждение результатов. Для моделирования данной атаки использовался стенд, состоящий из 3 виртуальных машин, две из которых являлись машинами под управлением ОС семейства Windows, а именно Windows 10 и одна с системой Ubuntu. С машины под управлением Ubuntu с IP-адресом 192.168.63.131 осуществлялась атака, Windows-машины с адресами 192.168.63.136 и 192.168.63.137 использовались в качестве «зомби» и целевой машины соответственно.

Для проведения атаки использовалась утилита Nmap. Также использовалась программа Wireshark для анализа трафика и иллюстрации проведения атаки.

На рис. 3 приведено окно программы Wireshark, иллюстрирующее процесс отправки пакетов, содержащих TCP-сегмент с флагом SYN/ACK для проверки пригодности компьютера с адресом 192.168.63.136 к роли «зомби».

На рис. 3 видно, что «зомби»-машина отвечает на запросы атакующей машины и ID каждого такого пакета с ответом идет по порядку, что также является обязательным условием для реализации данной атаки.

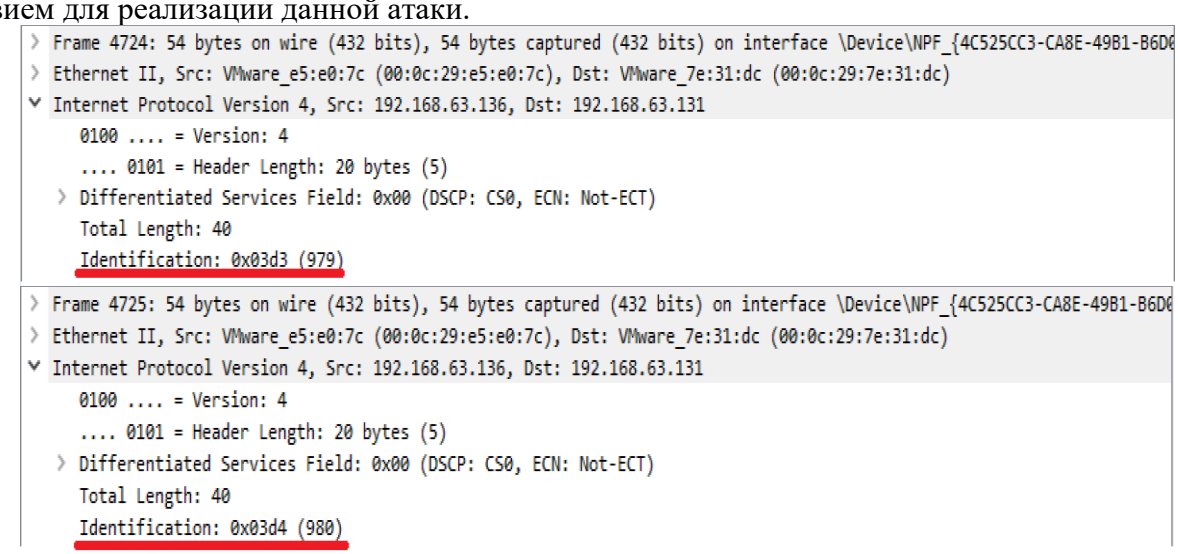

Рис. 3. Отображение ID пакетов, следующих друг за другом
Fig. 3. Displaying packet IDs following one another

После нахождения «зомби»-машины, происходит атака непосредственно целевого компьютера со стороны атакующей машины. На цель отправляются пакеты, содержащие TCP-сегмент с флагом SYN, причём в пакете производится с замена исходного IP-адреса атакующей машины 192.168.63.131 на IP-адрес «зомби»-машины 192.168.63.136.

На рис. 4 приведено окно программы Wireshark, иллюстрирующее процесс сканирования портов.

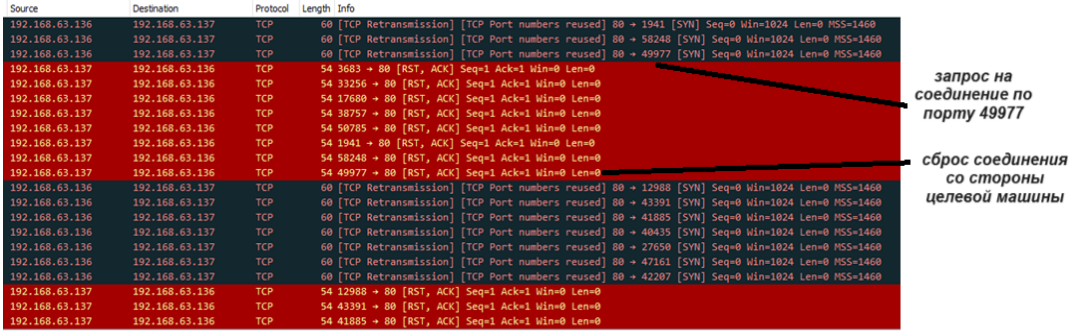

Рис. 4. Результат сканирования портов с подменой IP адреса
Fig. 4. Result of port scanning with IP address spoofing

Для примера рассмотрим запрос атакующей машины 192.168.63.131 к целевой машине 192.168.63.137 на соединение по порту 49977. Поскольку истинный адрес атакующей машины подменен, то в программе Wireshark этот запрос просматривается как запрос от «зомби»-машины с адресом 192.168.63.136 (рис. 4).

После осуществления такой атаки можно получить информацию по всем портам, которые были открыты на атакуемой машине (рис. 5), что позволит злоумышленникам в дальнейшем осуществить атаку на какую-либо службу, которая использует тот или иной порт и получить над ней контроль.

```
Nmap scan report for 192.168.63.137
Host is up (0.053s latency).
Not shown: 65522 closed|filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5040/tcp  open  unknown
5357/tcp  open  wsdapi
7680/tcp  open  pando-pub
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
MAC Address: 00:0C:29:AF:34:D8 (VMware)
```

Рис. 5. Результат проведенного сканирования
Fig. 5. The result of the scan

No.	Time	Source	Destination	Protocol	Length	Info
4558	216.782081	192.168.63.136	192.168.63.137	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 80 → 19722 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4559	216.782095	192.168.63.136	192.168.63.137	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 80 → 2372 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4560	216.782173	192.168.63.136	192.168.63.137	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 80 → 25566 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4561	216.782189	192.168.63.136	192.168.63.137	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 80 → 25242 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4562	216.782204	192.168.63.136	192.168.63.137	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 80 → 31415 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4563	216.782255	192.168.63.136	192.168.63.137	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 80 → 18918 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4564	216.782255	192.168.63.136	192.168.63.137	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 80 → 32468 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4565	216.782292	192.168.63.136	192.168.63.137	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 80 → 58770 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4566	216.782319	192.168.63.136	192.168.63.137	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 80 → 13363 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4567	216.782561	192.168.63.136	192.168.63.137	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 80 → 1475 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4568	216.782561	192.168.63.136	192.168.63.137	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 80 → 51166 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4569	216.782561	192.168.63.136	192.168.63.137	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 80 → 30284 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4570	216.782561	192.168.63.136	192.168.63.137	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 80 → 63684 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4571	216.782652	192.168.63.136	192.168.63.137	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 80 → 63789 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4572	216.782652	192.168.63.136	192.168.63.137	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 80 → 9437 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4573	216.782652	192.168.63.136	192.168.63.137	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 80 → 48663 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Рис. 6. Трафик, поступающий на «зомби» - машину при включенном брандмауэре на атакуемой машине
Fig. 6. Traffic arriving at a “zombie” machine when the firewall is enabled on the attacked machine

Однако избежать сканирования портов компьютера можно довольно просто: использование брандмауэра Windows со стандартными настройками позволяет блокировать подозрительный трафик (рис. 6, 7).

На рис. 6 видны запросы, поступающие с атакующей машины на целевую от имени «зомби». Также видно, что атакуемая машина не отвечает. Эту ситуацию иллюстрирует рис. 7, на котором показан трафик атакуемой машины.

No.	Time	Source	Destination	Protocol	Length	Info
7606	15.206625	192.168.63.136	192.168.63.137	TCP	60	80 → 42496 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7607	15.206701	192.168.63.136	192.168.63.137	TCP	60	80 → 23015 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7608	15.206701	192.168.63.136	192.168.63.137	TCP	60	80 → 21088 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7609	15.206701	192.168.63.136	192.168.63.137	TCP	60	80 → 62833 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7610	15.206746	192.168.63.136	192.168.63.137	TCP	60	80 → 25068 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7611	15.206794	192.168.63.136	192.168.63.137	TCP	60	80 → 47600 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7612	15.206794	192.168.63.136	192.168.63.137	TCP	60	80 → 63989 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7613	15.206814	192.168.63.136	192.168.63.137	TCP	60	80 → 18019 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7614	15.206829	192.168.63.136	192.168.63.137	TCP	60	80 → 8671 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Рис. 7. Трафик, поступающий на атакуемую машину
Fig. 7. Traffic arriving at the attacked machine

На рис. 8 приведен результат сканирования портов утилитой Nmap при включенном брандмауэре на целевой машине. Видно, что попытка сканирования не достигла результата.

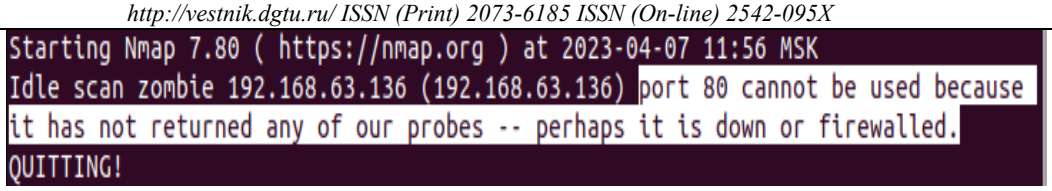

Рис. 8. Результат сканирования портов с включенным брандмауэром
Fig. 8. The result of a port scan with the firewall enabled

Вывод. В результате исследования была достигнута поставленная цель, которая заключалась в анализе особенностей реализации атаки «сканирование портов» с использованием компьютера-«зомби» для сокрытия IP-адреса атакующей машины.

На основе данного анализа выявлены следующие факты:

- реализация атаки достаточно проста;
- сведения, получаемые злоумышленником, дают возможность строить дальнейшую стратегию нападения с учетом выявленных уязвимостей на основе информации о состоянии портов целевой машины;
- использование брандмауэра Windows на целевой машине позволяет противодействовать сканированию портов.

Следует отметить, что использование брандмауэра Windows помогает так же избежать использование компьютера в качестве «зомби». Однако с поиском «зомби»-машин у злоумышленников проблем нет, поскольку в сети достаточно устройств, которые не защищены брандмауэром, например, сетевые принтеры или сетевые видеокамеры.

Библиографический список:

1. Andersson A. Standardizing information security – a structurational analysis / Andersson A., Hedström K., Karlsson F. // Information & Management. 2022. Vol. 59. Iss. 3. 103623. DOI:10.1016/j.im.2022.103623.
2. Vedadi A. Herd behavior in information security decision-making / Vedadi A., Warkentin M., Dennis A. // Information & Management. 2021. Vol. 58. Iss. 8. 103526. DOI:10.1016/j.im.2021.103526.
3. Stallings W. Computer security: principles and practice / Stallings W. — Boston. Pearson. 2012. 182 p.
4. Мирошниченко Е.Л. Разработка модели сбора информации о состоянии защищаемой системы для решения задач управления системой обнаружения, предупреждения и ликвидации последствий компьютерных атак / Мирошниченко Е.Л., Калач А.В, Зенин А.А. // Вестник Воронежского института ФСИН России. 2020. № 1. С. 102-107.
5. Шелухин О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) / Шелухин О.И., Сакалема Д.Ж., Филинова А.С.. — М: Горячая линия—Телеком. 2013. 220 с.
6. Chandola V. Anomaly detection: A survey / Chandola V., Banerjee A., Kumar V. // ACM Computing Surveys (CSUR). Article 15. 2009. Vol. 41. No. 3. pp. 15:1-15:58. DOI:10.1145/1541880.1541882.
7. Boldyrikhin N. Controlling the Resources of the Intrusion Detection System at Network Objects Monitoring / Boldyrikhin N., Safaryan O., Razumov P., Porksheyan V., Smirnov I., Korochentsev D., Cherckesova L., Romanov A. // ICCAIS 2020 - 3rd International Conference on Computer Applications and Information. 2020. 9096741. DOI:10.1109/ICCAIS48893.2020.9096741.
8. Boldyrikhin N. Features of the Practical Implementation of the Method for Managing Observations of the State of Monitored Objects in Intrusion Detection SystemsN / Boldyrikhin N., Safaryan O., Korochentsev D., Reshetnikova I., Alferova I. and Manakova A. // Applied Sciences. 2023. Vol. 13. No. 3. 1831. DOI:10.3390/app13031831.
9. Макаренко С.И. Анализ стандартов и методик тестирования на проникновение / Макаренко С.И., Смирнов Г.Е. // Системы управления, связи и безопасности. 2020. № 4. С. 44-72.
10. Khraisat A. Survey of intrusion detection systems: Techniques, datasets and challenges / Khraisat A., Gondal I., Vamplew P., Kamruzzaman J.// Cybersecurity. 2019. Vol.2. DOI: 10.1186/s42400-019-0038-7.
11. Alazab A. Using response action with intelligent intrusion detection and prevention system against web application malware / Alazab A., Hobbs M., Abawajy J., Khraisat A., Alazab M. // Information Management & Computer Security. 2014. Vol. 22. pp. 431–449.
12. Agrawal S. Survey on Anomaly Detection using Data Mining Techniques / Agrawal S., Agrawal J. // Procedia Computer Science. 2015. Vol. 60. pp. 708–713. DOI: 10.1016/j.procs.2015.08.220.
13. Abbasi A. On Emulation-Based Network Intrusion Detection Systems / Abbasi A., Wetzels J., Bokslag W., Zambon E., Etalle S. // In RAID 2014: Research in Attacks, Intrusions and Defenses. Lecture Notes in Computer Science. 2014; Vol. 8688, pp. 384–404.

14. Khraisat A. An Anomaly Intrusion Detection System Using Discovery and Data Mining. Lecture Notes in Computer Science. Springer: Cham, Switzerland. 2018. Vol. 11154. DOI: 10.1007/978-3-030-04503-6_14.
15. Ананьин Е.В. Формализованная модель обнаружения сканирования портов. / Ананьин Е.В., Кожевникова И.С., Лысенко А.В., Никишова А.В. // Молодой ученый. 2016. № 23 (127). С. 9-12.
16. Шаханова М.В. Разработка системы защиты от атаки сканирования сетевых портов / Шаханова М.В., Солоненко Д.Ю., Шаханова Э.С. // Международный журнал информационных технологий и энергоэффективности. 2023. Т. 8. № 5-1 (31). С. 67-74.
17. Вехова Л.Д. Сканирование UDP\TCP портов средствами языка программирования Python 3 / Вехова Л.Д. // Системный администратор. 2022. № 6 (235). С. 64-67.
18. Кожевникова И.С. Анализ методов обнаружения аномалий для обнаружения сканирования портов /Кожевникова И.С. // Молодой ученый. 2017. № 14 (148). С. 31-34.
19. Сагатов Е.С. Разработка программных комплексов для противодействия сканированию портов / Сагатов Е.С., Майхуб С., Сухов А.М., Баймяшкин М.А. // Состояние и перспективы развития современной науки по направлению «Информационная безопасность». Сборник статей II Всероссийской научно-технической конференции. Федеральное государственное автономное учреждение "Военный инновационный технополис "ЭРА". Анапа. 2020. С. 70-79.
20. Макатерчик А.В. Экспериментальное исследование сайтов компаний и организаций Республики Беларусь на предмет сканирования портов на компьютерах посетителей / Макатерчик А.В., Маликов В.В. // Управление информационными ресурсами. Материалы XVII Международной научно-практической конференции. Минск, 2021. С. 225-226.
21. Андриянов Е.А. Методы сканирования ЭВМ в вычислительных сетях /Андриянов Е.А., Бирюков М.А., Соколов О.Д., Козлов И.И., Кульнев Д.В. // LXVII Международные научные чтения (памяти В.Л. Гинзбурга). Сборник статей Международной научно-практической конференции. 2020. С. 4-6.
22. Кожевникова И.С. Анализ методов обнаружения аномалий при сканировании портов / Кожевникова И.С., Пасюк А.О., Ананьин Е.В. // Сборник статей «Материалы научной сессии». 2017. С. 591-596.

References:

1. Andersson A. Standardizing information security – a structurational analysis / Andersson A., Hedström K., Karlsson F.. Information & Management. 2022; 59(3). 103623. DOI:10.1016/j.im.2022.103623.
2. Vedadi A. Herd behavior in information security decision-making / Vedadi A., Warkentin M., Dennis A. *Information & Management*. 2021; 58(8). 103526. DOI:10.1016/j.im.2021.103526.
3. Stallings W. Computer security: principles and practice. *Stallings W. Boston. Pearson.* 2012;182.
4. Miroshnichenko E.L. Development of a model for collecting information about the state of the protected system to solve problems of managing a system for detecting, preventing and eliminating the consequences of computer attacks / Miroshnichenko E.L., Kalach A.V., Zenin A.A. *Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia*. 2020;1:102-107. (In Russ).
5. Shelukhin O.I. Detection of intrusions into computer networks (network anomalies) / O.I. Shelukhin, D.Zh. Sakalema, A.S. Filinova. M: Hotline-Telecom. 2013; 220. (In Russ).
6. Chandola V. Anomaly detection: A survey / Chandola V., Banerjee A., Kumar V. *ACM Computing Surveys (CSUR). Article 15*. 2009; 41(3):15:1-15:58. DOI:10.1145/1541880.1541882.
7. Boldyrikhin N. Controlling the Resources of the Intrusion Detection System at Network Objects Monitoring / Boldyrikhin N., Safaryan O., Razumov P., Porksheyan V., Smirnov I., Korochentsev D., Cherckesova L., Romanov A. // ICCAIS 2020 - 3rd International Conference on Computer Applications and Information. 2020. 9096741.DOI:10.1109/ICCAIS48893.2020.9096741.
8. Boldyrikhin N. Features of the Practical Implementation of the Method for Managing Observations of the State of Monitored Objects in Intrusion Detection SystemsN / Boldyrikhin N., Safaryan O., Korochentsev D., Reshetnikova Alferova I. and Manakova A. *Applied Sciences*. 2023;13(3):1831. DOI:10.3390/app13031831.
9. Makarenko S.I. Analysis of standards and methods of penetration testing / Makarenko S. I., Smirnov G.E. *Control, communication and security systems.* 2020;4: 44-72. (In Russ).
10. Khraisat A. Survey of intrusion detection systems: Techniques, datasets and challenges / Khraisat A., Gondal I., Vamplew P., Kamruzzaman J. *Cybersecurity.* 2019;2. DOI: 10.1186/s42400-019-0038-7.
11. Alazab A. Using response action with intelligent intrusion detection and prevention system against web application malware / Alazab A., Hobbs M., Abawajy J., Khraisat A., Alazab M. *Information Management & Computer Security*. 2014; 22:431–449.
12. Agrawal S. Survey on Anomaly Detection using Data Mining Techniques / Agrawal S., Agrawal J. *Procedia Computer Science.* 2015; 60:708–713. DOI: 10.1016/j.procs.2015.08.220.
13. Abbasi A. On Emulation-Based Network Intrusion Detection Systems / Abbasi A., Wetzels J., Bokslag W., Zambon E., Etalle S. *In RAID 2014: Research in Attacks, Intrusions and Defenses. Lecture Notes in Computer Science*. 2014; 868: 384–404.

14. Khraisat A. An Anomaly Intrusion Detection System Using Discovery and Data Mining. Lecture Notes in Computer Science. Springer: Cham, Switzerland. 2018. Vol. 11154. DOI: 10.1007/978-3-030-04503-6_14.
15. Ananyin E.V. Formalized port scan detection model. Ananyin E.V., Kozhevnikova I.S., Lysenko A.V., Nikishova A.V. *Young scientist.* 2016; 23 (127): 9-12. (In Russ).
16. Shakhanova M.V. Development of a protection system against network port scanning attacks / Shakhanova M.V., Solonenko D.Yu., Shakhanova E.S. *International Journal of Information Technologies and Energy Efficiency*. 2023; 8(5-1 (31):67-74. (In Russ).
17. Vekhova L.D. Scanning UDP\TCP ports using the Python 3 programming language / Vekhova L.D. *System Administrator.* 2022; 6 (235): 64-67. (In Russ).
18. Kozhevnikova I.S. Analysis of anomaly detection methods for port scanning detection / Kozhevnikova I.S. *Young scientist*. 2017;14 (148): 31-34. (In Russ).
19. Sagatov E.S. Development of software systems to counteract port scanning / Sagatov E.S., Maykhub S., Sukhov A.M., Baymyashkin M.A. State and prospects for the development of modern science in the direction of "Information Security". Collection of articles of the II All-Russian Scientific and Technical Conference. Federal State Autonomous Institution "Military Innovative Technopolis "ERA". Anapa. 2020; 70-79. (In Russ).
20. Makaterchik A.V. Experimental study of websites of companies and organizations of the Republic of Belarus for scanning ports on visitors' computers / Makaterchik A.V., Malikov V.V. Information resource management. Materials of the XVII International Scientific and Practical Conference. Minsk, 2021; 225-226. (In Russ).
21. Andriyanov E.A., Biryukov M.A., Sokolov O.D., Kozlov I.I., Kulnev D.V. Methods for scanning computers in computer networks. LXVII International scientific readings (in memory of V.L. Ginzburg). Collection of articles of the International Scientific and Practical Conference. 2020; 4-6. (In Russ).
22. Kozhevnikova I.S., Pasyuk A.O., Ananyin E.V. Analysis of anomaly detection methods when scanning ports. *Collection of articles "Materials of the scientific session*". 2017; 591-596. (In Russ).

Сведения об авторах:

Болдырихин Николай Вячеславович, кандидат технических наук, доцент кафедры «Кибербезопасность информационных систем»; boldyrikhin@mail.ru

Карпенко Михаил Владиславович, магистрант; karpenkomihail15@gmail.com

Сосновский Иван Александрович, кандидат технических наук, доцент кафедры «Кибербезопасность информационных систем»; sosnovskiy_dgtu@mail.ru

Ядрец Эдуард Александрович, магистрант; xperia1058@gmail.com

Information about the authors:

Nikolay V. Boldyrikhin, Cand.Sci. (Eng.), Assoc. Prof., Department of Cybersecurity of Information Systems; boldyrikhin@mail.ru

Mikhail V. Karpenko, Master's Student; karpenkomihail15@gmail.com

Ivan A. Sosnovsky, Cand.Sci. (Eng.), Assoc. Prof., Department of Cybersecurity of Information Systems; sosnovskiy_dgtu@mail.ru

Eduard A. Yadrets, Master's Student; xperia1058@gmail.com

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 08.01.2024.

Одобрена после рецензирования / Reviced 30.01.2024.

Принята в печать /Accepted for publication 30.01.2024.