

**Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

Факультет безопасности информационных технологий

Дисциплина:

«Вычислительные сети и контроль безопасности в компьютерных сетях»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №7

«Сканирование уязвимостей»

Выполнили:

Чу Ван Доан, студент группы N3347



(подпись)

Чан Бао Линь, студентка группы N3346



(подпись)

Проверил:

Савков Сергей Витальевич, инженер факультета БИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

2025 г.

СОДЕРЖАНИЕ

Содержание.....	2
Введение.....	3
Задание.....	4
1. Проверка подключения и сетевого диапазона.....	5
1.1. Определить IP-адрес компьютера и маршрутизатора.....	5
2. Найти активные устройства.....	6
3. Сканирование портов и служб каждого хоста.....	7
4. Сканирование уязвимостей с помощью Nessus.....	7

ВВЕДЕНИЕ

Цель работы - Используя сетевой сканер nmap и сканер уязвимостей nessus, изучить основные методы анализа сетевой инфраструктуры .

Задание

- Подключиться к тестовому стенду, используя подключение Wi-Fi (параметры подключения взять из результатов выполнения ЛР2)
- Выполнить сканирование сети, на основе результатов сканирования сформировать карту сети
- Исследовать узлы сети на предмет открытых портов. Выполнить сканирование уязвимостей для сервисов на открытых портах.

Ход работы

1. Проверка подключения и сетевого диапазона

1.1. Определить IP-адрес компьютера и маршрутизатора.

```
root@chu-latitude-5510:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eno2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 74:78:27:2c:05:1c brd ff:ff:ff:ff:ff:ff
    altname enp0s31f6
    inet 192.168.31.231/24 brd 192.168.31.255 scope global dynamic noprefixroute eno2
        valid_lft 35509sec preferred_lft 35509sec
    inet6 fe80::c74e:a842:4e0c:9f07/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
4: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 52:54:00:73:f2:37 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
        valid_lft forever preferred_lft forever
6: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether d6:96:d8:a9:4d:af brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
7: doanlaptop: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue state UNKNOWN group default qlen 1000
    link/none
    inet 10.8.0.15/24 brd 10.8.0.255 scope global noprefixroute doanlaptop
        valid_lft forever preferred_lft forever
11: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 68:3e:26:09:87:f2 brd ff:ff:ff:ff:ff:ff
    altname wlp0s20f3
    inet 192.168.31.190/24 brd 192.168.31.255 scope global dynamic noprefixroute wlo1
        valid_lft 41612sec preferred_lft 41612sec
    inet6 fe80::3980:72be:e93e:862b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
root@chu-latitude-5510:~# ip route | grep default
default via 192.168.31.1 dev eno2 proto dhcp src 192.168.31.231 metric 100
default via 192.168.31.1 dev wlo1 proto dhcp src 192.168.31.190 metric 600
root@chu-latitude-5510:~#
```

Рисунок 1 – Определить IP-адрес компьютера и маршрутизатора.

Интерфейс, который мы используем: wlo1 (Wi-Fi)

IP-адрес вашего компьютера: 192.168.31.190

Маршрутизатор (шлюз по умолчанию): 192.168.31.1

Маска подсети: /24 (то есть 255.255.255.0)

Мы находимся во внутренней сети: 192.168.31.0/24

Информация	Значение
IP-адрес хоста	192.168.31.190
Маршрутизатор	192.168.31.1
Маска подсети	255.255.255.0 → /24
Сканируемая сеть	192.168.31.0/24

1.2. Найти активные устройства

`nmap -sn 192.168.31.0/24`

```
root@chu-latitude-5510:~# nmap -sn 192.168.31.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-24 13:07 MSK
Nmap scan report for _gateway (192.168.31.1)
Host is up (0.00056s latency).
MAC Address: C8:BF:4C:94:E2:C4 (Beijing Xiaomi Mobile Software)
Nmap scan report for 192.168.31.33
Host is up (0.0011s latency).
MAC Address: 50:E0:85:6A:16:20 (Intel Corporate)
Nmap scan report for 192.168.31.38
Host is up (0.0011s latency).
MAC Address: 50:E0:85:6A:16:20 (Intel Corporate)
Nmap scan report for 192.168.31.64
Host is up (0.046s latency).
MAC Address: 82:F4:D7:41:95:C0 (Unknown)
Nmap scan report for chu-latitude-5510 (192.168.31.190)
Host is up.
Nmap scan report for chu-latitude-5510 (192.168.31.231)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.36 seconds
root@chu-latitude-5510:~#
```

Рисунок 2 – Найти активные устройства

Результат: Обнаружено 6 активных устройств (host)

IP	Предполагаемое устройство	MAC-адрес
192.168.31.1	Роутер (Шлюз, Xiaomi)	C8:BF:4C:94:E2:C4
192.168.31.33	Устройство Intel	50:E0:85:6A:16:20
192.168.31.38	Тот же MAC, что и у .33 → возможно, виртуальная машина?	50:E0:85:6A:16:20
192.168.31.64	Неизвестно	82:F4:D7:41:95:C0
192.168.31.190	Ваш компьютер (через Wi-Fi, интерфейс wlo1)	
192.168.31.231	Ваш компьютер (через LAN, интерфейс eno2)	

Мы выберем другие IP-адреса, кроме вашего, для дальнейшего анализа, например:

192.168.31.33

192.168.31.38

192.168.31.64

1.3. Сканирование портов и служб каждого хоста.

```
sudo nmap -sS -sV -O -Pn 192.168.31.33
```

```
sudo nmap -sS -sV -O -Pn 192.168.31.38
```

```
root@chu-latitude-5510:~# sudo nmap -sS -sV -O -Pn 192.168.31.33
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-24 13:09 MSK
Nmap scan report for 192.168.31.33
Host is up (0.00040s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
7070/tcp  open  ssl/realserver?
MAC Address: 98:FA:9B:A4:D9:BE (LCFC(HeFei) Electronics Technology)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.99 seconds
root@chu-latitude-5510:~# sudo nmap -sS -sV -O -Pn 192.168.31.38
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-24 13:10 MSK
Nmap scan report for 192.168.31.38
Host is up (0.00027s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
7070/tcp  open  ssl/realserver?
MAC Address: 98:FA:9B:A4:D9:BE (LCFC(HeFei) Electronics Technology)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.92 seconds
root@chu-latitude-5510:~#
```

Рисунок 3 – Сканирование портов и служб каждого хоста.

Хост	ОС	Открытые порты	Описание сервиса
192.168.31.33	Linux 4.x–5.x	tcp/7070	SSL service (realserver?)
192.168.31.38	Linux 4.x–5.x	tcp/7070	SSL service (realserver?)

2. Сканирование уязвимостей с помощью Nessus

Скачайте и установите Nessus: <https://www.tenable.com/downloads/nessus>

```
sudo dpkg -i Nessus-*.deb
```

```
sudo systemctl start nessusd
```

Доступ к веб-интерфейсу: <https://localhost:8834>

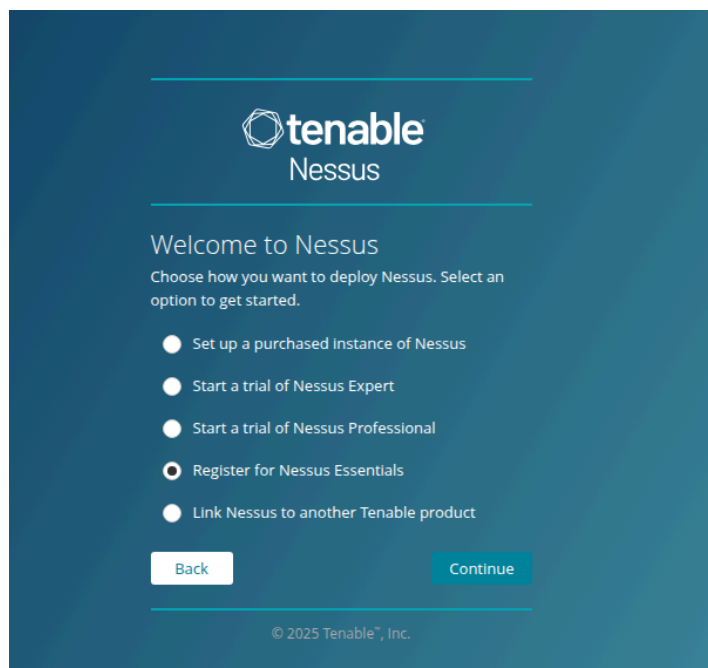


Рисунок 4 – Интерфейс Nessus

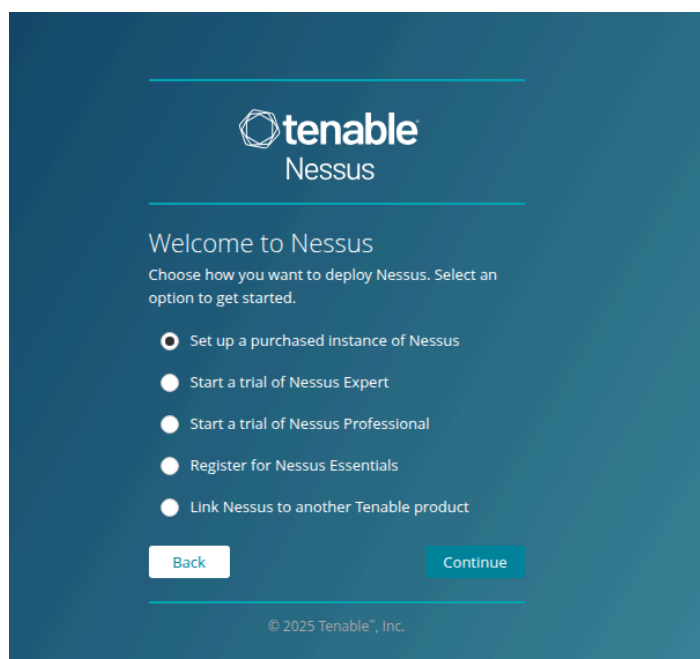
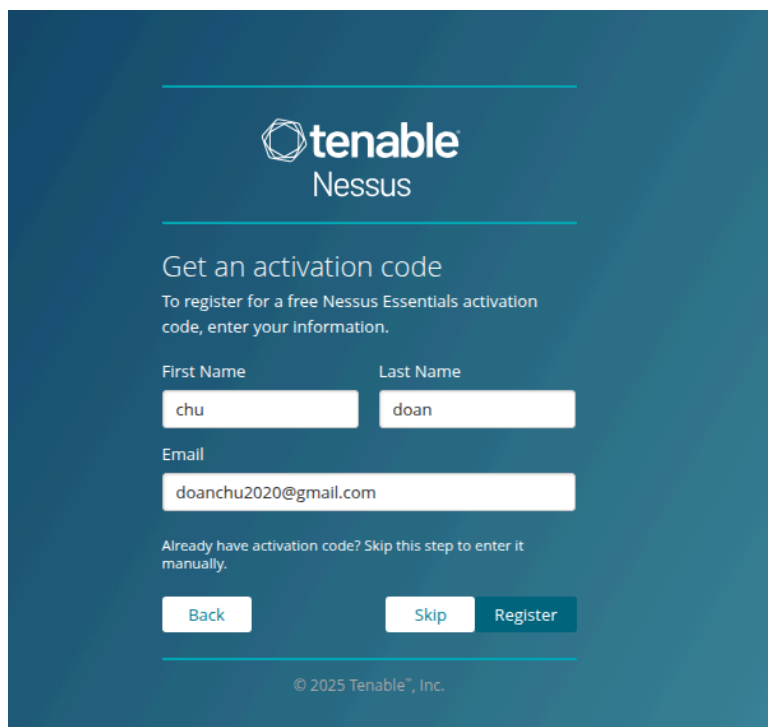


Рисунок 5 – Интерфейс Nessus



The image shows the Tenable Nessus registration page. At the top is the Tenable Nessus logo. Below it, the heading "Get an activation code" is followed by the instruction "To register for a free Nessus Essentials activation code, enter your information." The form contains three input fields: "First Name" with the value "chu", "Last Name" with the value "doan", and "Email" with the value "doanchu2020@gmail.com". Below these fields is a link that says "Already have activation code? Skip this step to enter it manually." At the bottom of the form are three buttons: "Back", "Skip", and "Register". The "Register" button is highlighted in a darker blue. At the very bottom, there is a copyright notice: "© 2025 Tenable™, Inc."

tenable
Nessus

Get an activation code

To register for a free Nessus Essentials activation code, enter your information.

First Name Last Name

chu doan

Email

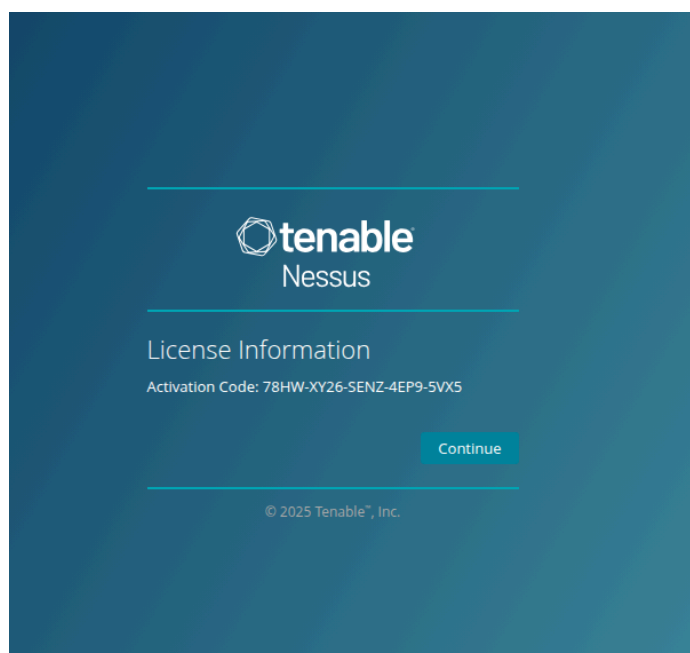
doanchu2020@gmail.com

Already have activation code? Skip this step to enter it manually.

Back Skip Register

© 2025 Tenable™, Inc.

Рисунок 6 – Register



The image shows the Tenable Nessus license information screen. At the top is the Tenable Nessus logo. Below it, the heading "License Information" is followed by the text "Activation Code: 78HW-XY26-SENZ-4EP9-5VX5". At the bottom right of the form is a "Continue" button. At the very bottom, there is a copyright notice: "© 2025 Tenable™, Inc."

tenable
Nessus

License Information

Activation Code: 78HW-XY26-SENZ-4EP9-5VX5

Continue

© 2025 Tenable™, Inc.

Рисунок 7 – Register

tenable
Nessus

Create a user account

Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username *

Password *

Back Submit

© 2025 Tenable®, Inc.

Рисунок 8 – Create account

tenable
Nessus

Initializing

Please wait while Nessus is initializing.

Downloading plugins...

© 2025 Tenable®, Inc.

Рисунок 9 – Download plugins

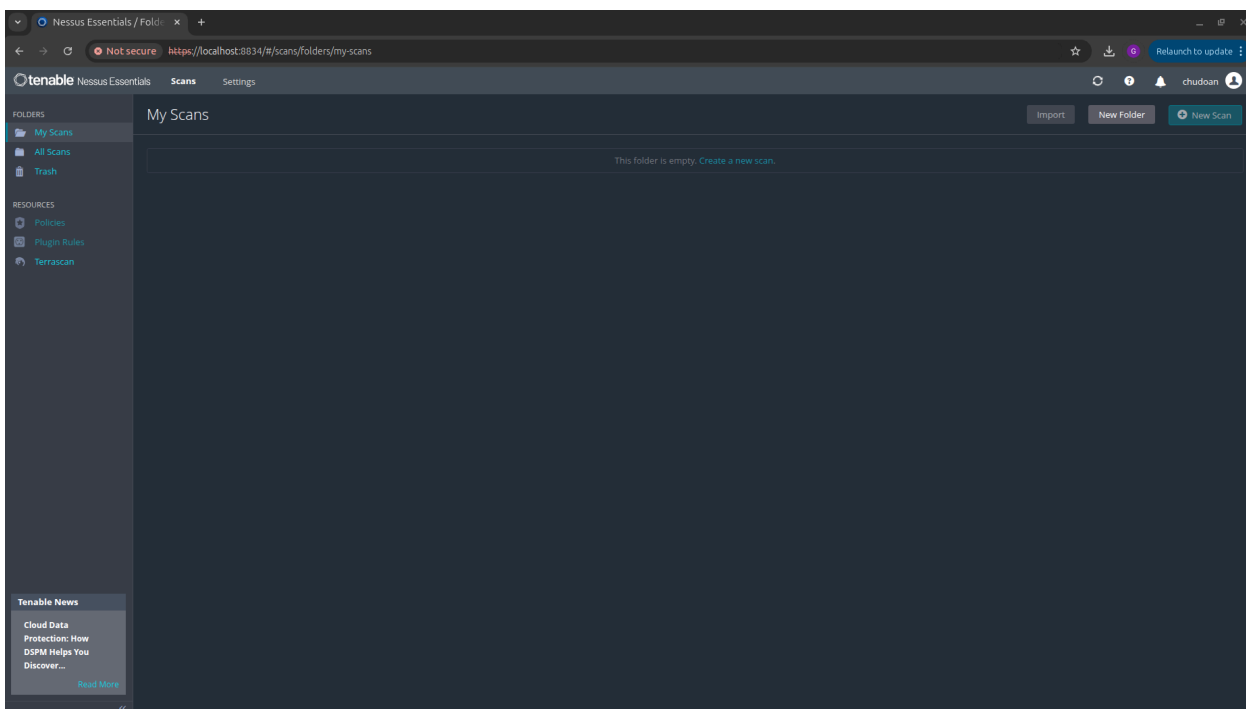


Рисунок 10 – Интерфейс Nessus Essentials

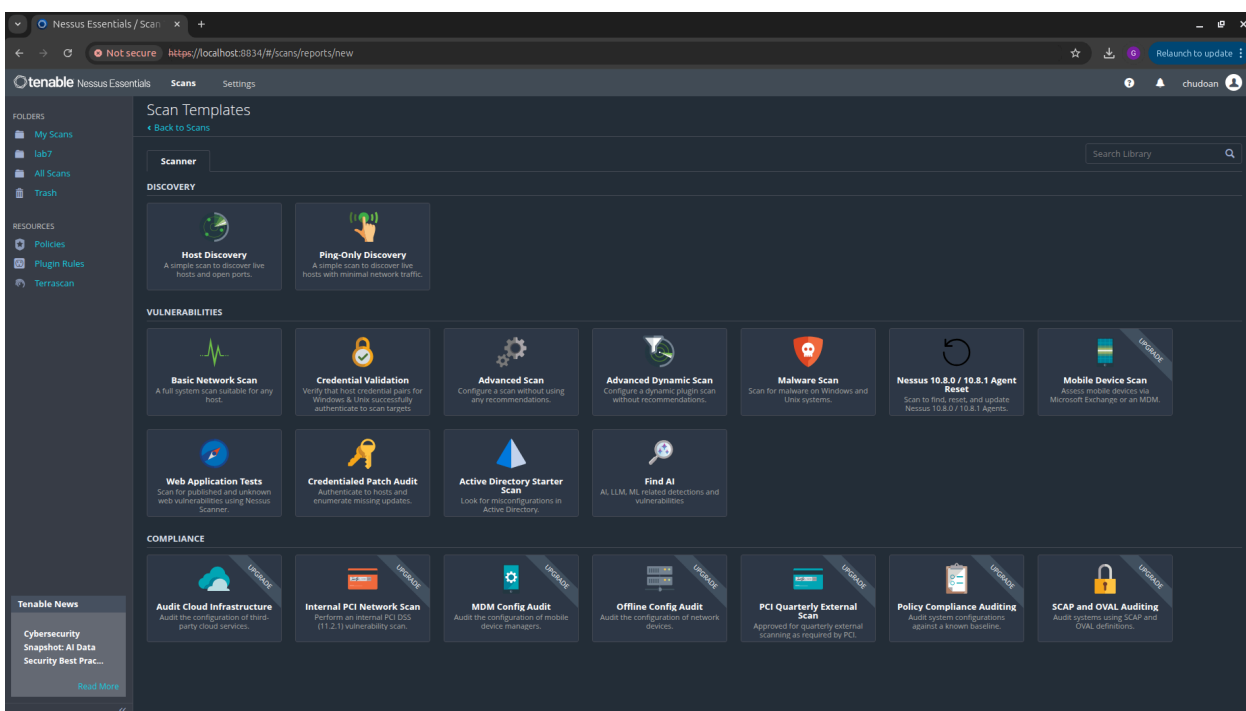


Рисунок 11 – Create new scan

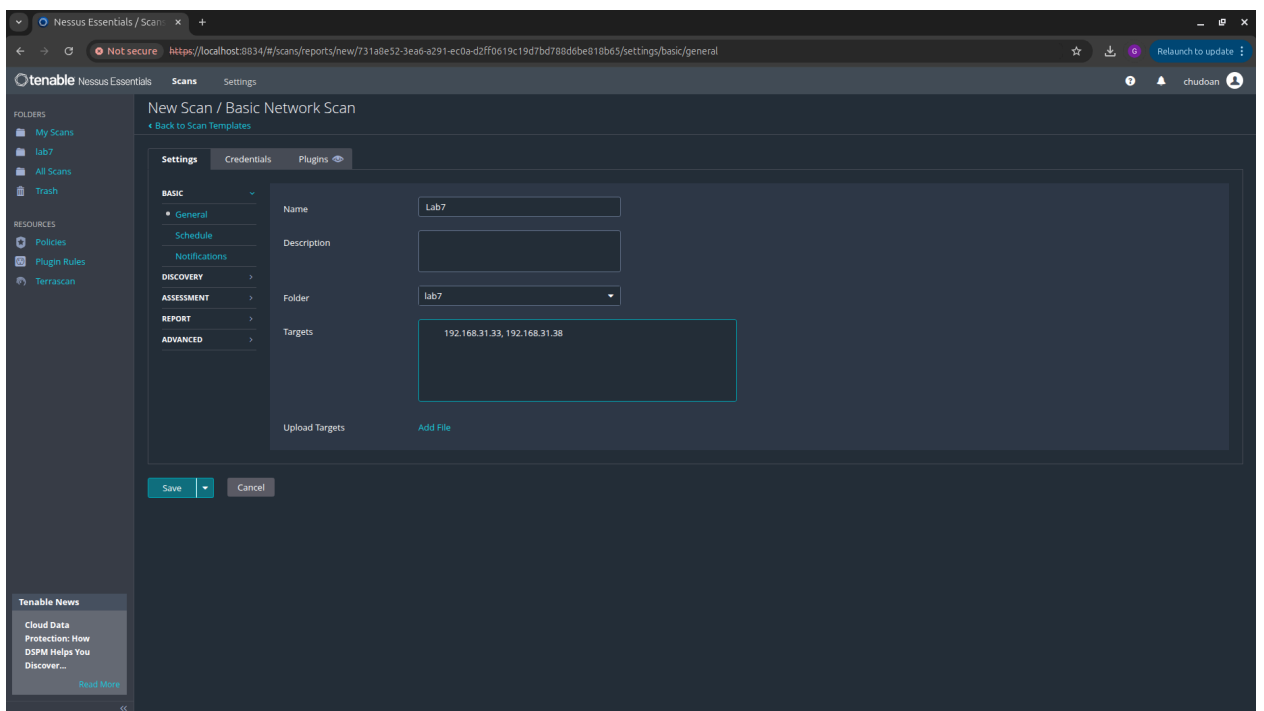


Рисунок 12 – Create new scan

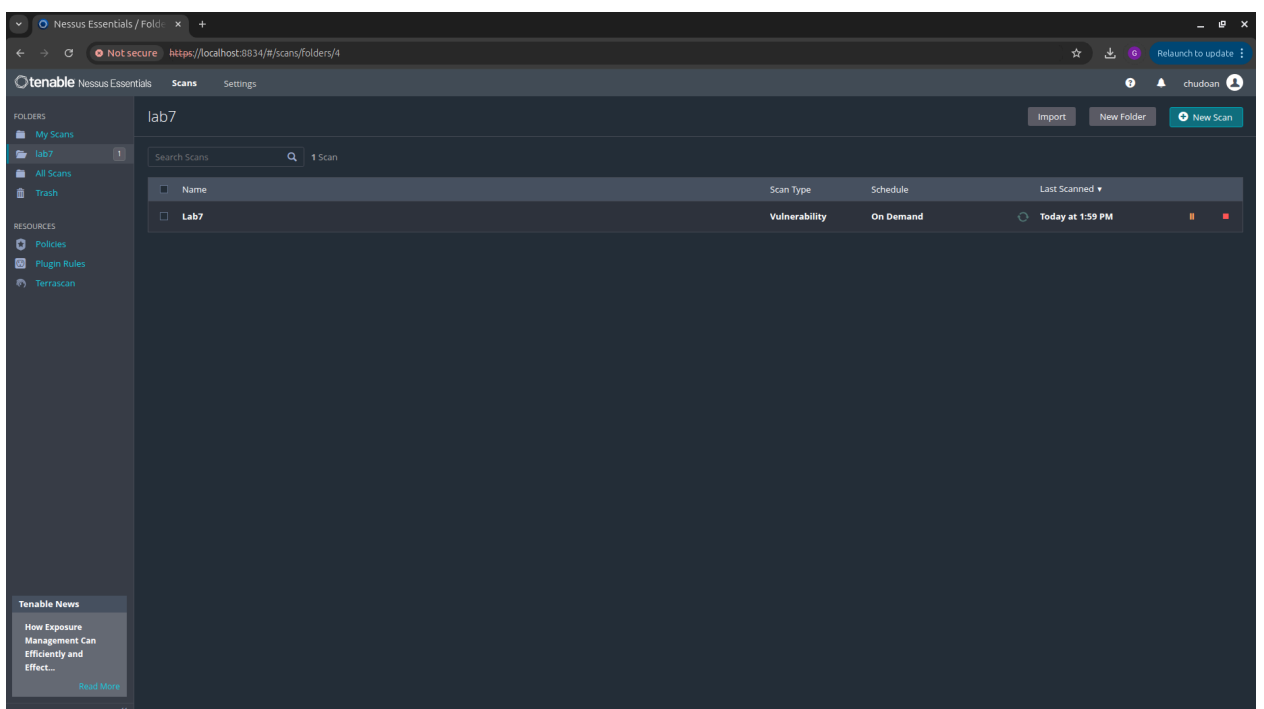


Рисунок 13 – Scan

Vulnerabilities 12

Sev	CVSS	VPR	EPSS	Name	Family	Count
LOW	2.1	2.2	0.0037	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Device Type	General	1
INFO				Ethernet Card Manufacturer Detection	Misc.	1
INFO				Ethernet MAC Addresses	General	1
INFO				mDNS Detection (Local Network)	Service detection	1
INFO				Nessus Scan Information	Settings	1
INFO				Nessus SYN scanner	Port scanners	1
INFO				OS Fingerprints Detected	General	1
INFO				OS Identification	General	1
INFO				TCP/IP Timestamps Supported	General	1
INFO				Traceroute Information	General	1

Host Details

Host: 192.168.31.33

IP: 192.168.31.33
 MAC: 98:FA:9B:A4:D9:BE
 OS: Linux Kernel 2.6
 Start: Today at 1:59 PM
 End: Today at 2:01 PM
 Elapsed: 2 minutes
 KB: Download

Vulnerabilities

Donut chart showing severity distribution: Critical (0), High (0), Medium (0), Low (1), Info (11).

Vulnerabilities 11

Sev	CVSS	VPR	EPSS	Name	Family	Count
LOW	2.1	2.2	0.0037	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Device Type	General	1
INFO				Ethernet Card Manufacturer Detection	Misc.	1
INFO				Ethernet MAC Addresses	General	1
INFO				Nessus Scan Information	Settings	1
INFO				Nessus SYN scanner	Port scanners	1
INFO				OS Fingerprints Detected	General	1
INFO				OS Identification	General	1
INFO				TCP/IP Timestamps Supported	General	1
INFO				Traceroute Information	General	1

Host Details

Host: 192.168.31.38

IP: 192.168.31.38
 MAC: 98:FA:9B:A4:D9:BE
 OS: Linux Kernel 2.6
 Start: Today at 1:59 PM
 End: Today at 2:01 PM
 Elapsed: 2 minutes
 KB: Download

Vulnerabilities

Donut chart showing severity distribution: Critical (0), High (0), Medium (0), Low (1), Info (10).

№	Название уязвимости	Уровень	IP 192.168.31.3	IP 192.168.31.38	Краткое описание
1	ICMP Timestamp Request Remote Date Disclosure	Низкий	✓	✓	Утечка времени системы через ICMP — может использоваться при атаке.

2	Common Platform Enumeration (CPE)	Инфо	✓	✓	Определение ОС и используемого ПО.
3	Device Type	Инфо	✓	✓	Определение типа устройства (ПК, маршрутизатор и т. д.).
4	Ethernet Card Manufacturer Detection	Инфо	✓	✓	Утечка информации о производителе сетевой карты.
5	Ethernet MAC Addresses	Инфо	✓	✓	Утечка MAC-адреса.
6	mDNS Detection (Local Network)	Инфо	✓	✗	Обнаружение mDNS-служб в локальной сети.
7	Nessus Scan Information	Инфо	✓	✓	Утечка информации о сканировании.
8	Nessus SYN scanner	Инфо	✓	✓	Сканирование открытых TCP-портов.
9	OS Fingerprints Detected	Инфо	✓	✓	Определение "отпечатков" операционной системы.
10	OS Identification	Инфо	✓	✓	Идентификация операционной системы.
11	TCP/IP Timestamps Supported	Инфо	✓	✓	Указывает на поддержку TCP timestamps системой.
12	Traceroute Information	Инфо	✓	✓	Утечка информации о маршруте пакетов.

ЗАКЛЮЧЕНИЕ

В результате выполнения лабораторной работы №7 с использованием инструмента Nessus было проведено сканирование двух хостов с IP-адресами 192.168.31.33 и 192.168.31.38. Сканирование выявило ряд уязвимостей, преимущественно информационного характера. Единственная уязвимость с уровнем угрозы "Low" — ICMP Timestamp Request Remote Date Disclosure — присутствует на обоих хостах и может быть использована злоумышленниками для определения системного времени, что потенциально способствует проведению атак с вычислением временных сдвигов.

Большинство обнаруженных уязвимостей связаны с утечкой информации о системе, таких как MAC-адреса, тип устройства, операционная система, поддержка TCP/IP timestamps и информация о маршрутизации. Эти данные могут быть использованы для дальнейшего этапа атаки — разведки (reconnaissance).

Следует отметить, что:

- Обе системы имеют схожий профиль уязвимостей, за исключением mDNS Detection, обнаруженной только на хосте 192.168.31.33.
- Ни одна из систем не имеет критических или высокоопасных уязвимостей, что свидетельствует об относительно хорошем уровне базовой защиты.