Task #1

I found 10 critical vulnerabilities mostly related to OpenSSL. 77 high vulnerabilities, 67 medium, 5 low. Total 159 vulnerabilities.

Recommendations for troubleshooting - software update.

The OS is quite secure.

№ отчета	*66f0ac0f-f28c-4726-ad57-762a6582b986*
№ сканирования	*bb468abc-b2dd-4273-84fa-7ff09ba408aa*
Профиль	*Уязвимости*
Начало/завершение сканирования	*12.02.2025 1:57:54 / 12.02.2025 2:04:13*
Формирование отчета	*12.02.2025 2:30:57*

Уровень опасности	Найдено	Всего
Критический	10	5295
Высокий	77	10823
Средний	67	11258
Низкий	5	1231
Недоступно	0	1
Всего	159	28608

Task #2

1) Equipment manufacturer: Keenetic

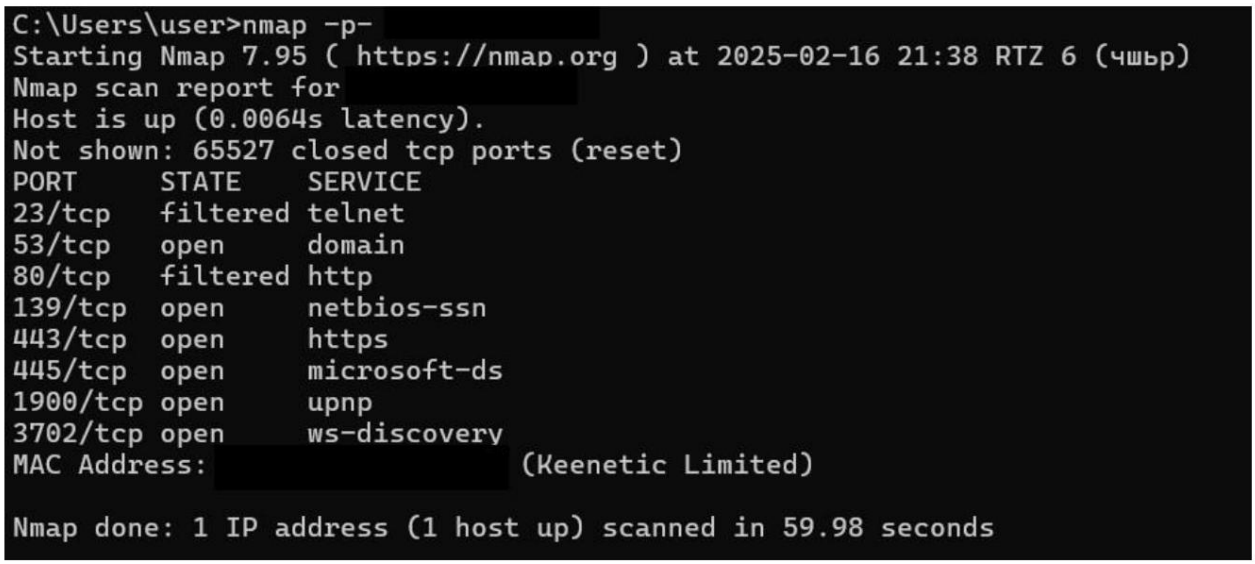
2) Operating system installed on the device: KeeneticOS

3) Open ports on the device: 7

4) Available services: Port
23 – telnet Port
53 – DNS Port
80 – HTTP Port
139 – netbios ssn Port
443 – HTTPS Port
445 – Microsoft-ds Port
1900 – upnp

5) Dangerous services: telnet, http, dns

6) ***Conclusion:*** using this test with the nmap utility, I identified vulnerabilities in my home router and eliminated them by closing the ports using the firewall settings telnet, http and doing dns filtering. Now the telnet and http ports are in "filtered" mode.



Task #3

1) Packets that are generated in my network: TCP, UDP, QUIC, TLS

2) I can say the following about the contents of the packages:

The main components of a packet in Wireshark are:

1. **Channel layer header (Layer 2):**
   - o **Ethernet Header:** Contains the source and destination MAC addresses, as well as the upper-layer protocol type.
2. **Network layer header (Layer 3):**
   - o **IP Header:** Includes source and destination IP addresses, protocol version (IPv4 or IPv6), packet time to live (TTL), and other service information.
3. **Transport layer header (Layer 4):**
   - o **TCP or UDP Header:** Contains source and destination ports, sequence numbers (for TCP), connection control flags, and checksums.
4. **Application layer data (Layer 7):**
   - o **Payload:** The actual data transferred by applications, such as the contents of HTTP requests and responses, FTP, SMTP, and other protocol data.

Analysis of package contents:

Wireshark provides detailed analysis of each packet layer, allowing you to:

- **Review protocol headers:** Study the information in detail, contained in the headers of various protocols, which helps in diagnosing network problems and understanding packet routing.
- **Analyze application data:** View and analyze data transmitted by applications, which is useful for debugging and security.

- **Use filters:** Apply filters to display only packets or protocols of interest, which simplifies the analysis of large volumes of traffic.

- **Monitor data streams:** Combine related packets into single streams to simplify the analysis of communication sessions, such as TCP sessions or HTTP requests, and answers.

3) I encountered multiple bad connections via TCP protocol