Task #1 Research of local indicators

1. To conduct a system security audit, you need to install special software:

• if you have Windows OS installed, go to the FSTEC of Russia website and download the ScanOVAL software and a vulnerability database. If you have any questions about the software, please refer to the operating instructions provided by the software operator;

• if you have Linux OS installed, download Lynis, The vulnerability database is included in the software.

4. Conduct an audit of the system using the example from the lecture.

5. What vulnerabilities did you find - there will definitely be at least 5. What recommendations did you

Can you give some advice on how to eliminate them?

6. Draw conclusions about the level of security of the operating system.

Solution:

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.

ScanOVAL ОТЧЁТ

№ 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 Research of network indicators

1. Download and install nmap software (zenmap).
2. Analyze the access point installed at your home. To do this, determine the default gateway address using the ipconfig command for Windows and ip route for Linux.
3. Check the availability of the default gateway using the ping command: ping 'ip address default gate' (for example, ping 192.168.0.1).
4. Run nmap (zenmap) program and execute the command nmap -sV 'ip address default gate' -p-. Here 'ip address default gate' is ping 192.168.0.1 from the example above.
5. Answer the following questions:

• Who is the manufacturer of the equipment?
• What operating system is installed on the device?
• How many ports are open on the device?
• What services are available?
• Are there any dangerous services? How to find out: copy the name of the service and its version, check in search engine.

6. Draw conclusions about the level of protection of your device.

Solution:

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
139 port – netbios ssn
Port 443 – HTTPS
Port 445 – Microsoft-ds
1900 port – 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.

```
C:\Users\user>nmap -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 21:38 RTZ 6 (чшьр)
Nmap scan report for
Host is up (0.0064s latency).
Not shown: 65527 closed tcp ports (reset)
PORT     STATE    SERVICE
23/tcp   filtered telnet
53/tcp   open     domain
80/tcp   filtered http
139/tcp  open     netbios-ssn
443/tcp  open     https
445/tcp  open     microsoft-ds
1900/tcp open     upnp
3702/tcp open     ws-discovery
MAC Address:                  (Keenetic Limited)

Nmap done: 1 IP address (1 host up) scanned in 59.98 seconds
```

Task #3 Network traffic analysis

1. Install Wireshark. The tool will be needed to collect network traffic and its subsequent analysis.
2. After installing Wireshark, restart your system.
3. After rebooting, at the beginning of work, launch Wireshark.
4. Enable data collection via the network interface and start working.
5. Go to any sites, look at various resources. Collect information for no more than 5 minutes, then turn off information collection and save the packet log.
6. When working with Wireshark, please refer to the instructions.
7. Start analysis:

• What packets are generated on your network?
• What can you say about the contents of the packages?
• What suspicious information have you encountered?

8. Draw conclusions.

Solution:

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