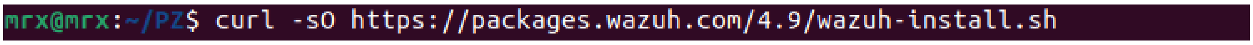
Практическая работа № 3: Wazuh

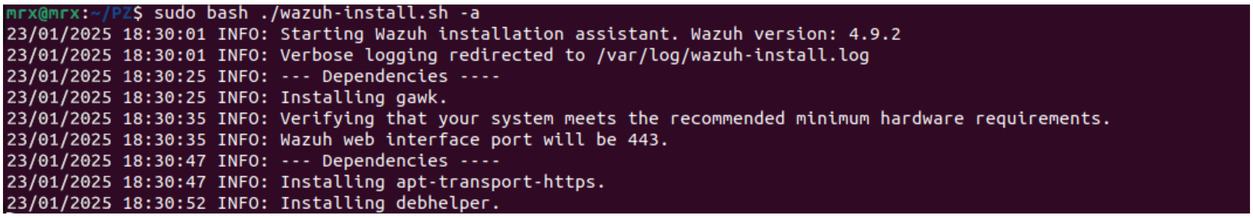
Выполнил Ионов Максим Сергеевич, группа ББМО-02-23

Ход работы

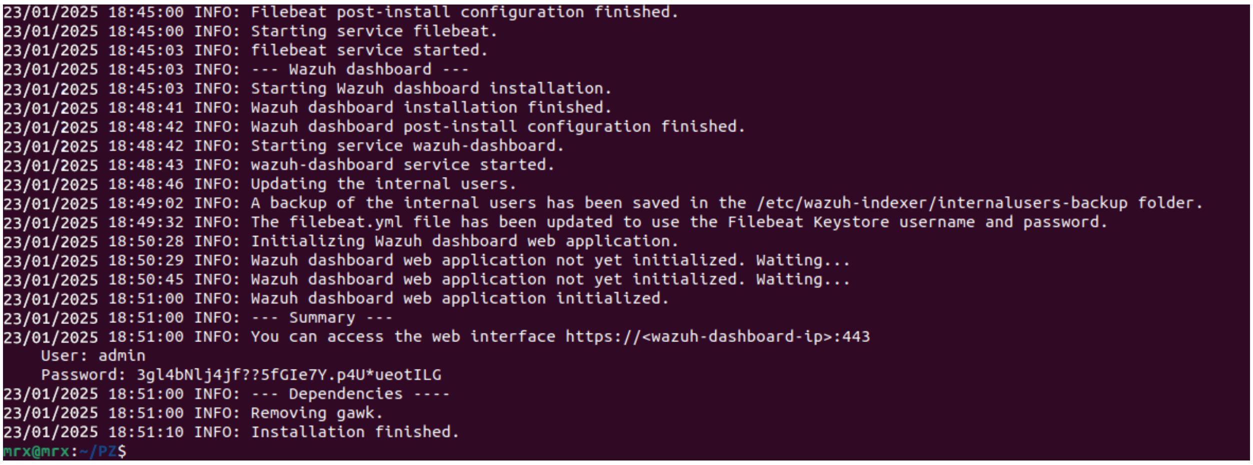
Устанавливаем сервер Wazuh на виртуальную машину



```
mrx@mrx:~/PZ$ curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
```

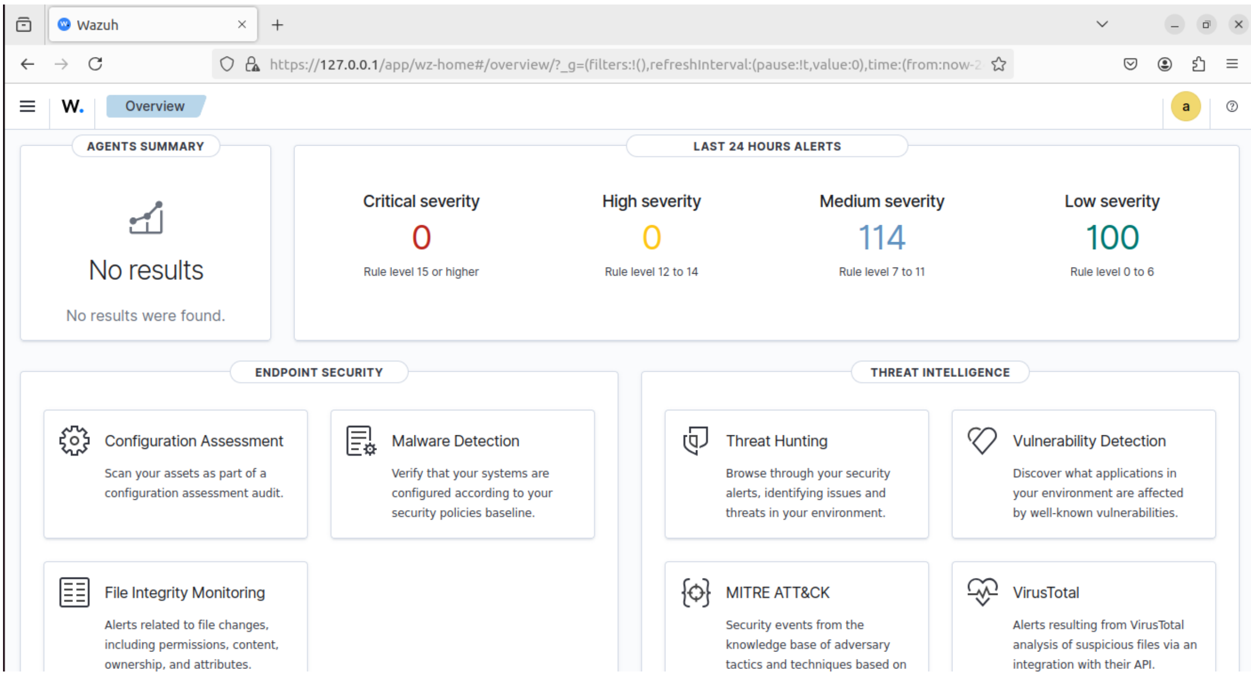


```
mrx@mrx:~/PZ$ sudo bash ./wazuh-install.sh -a
23/01/2025 18:30:01 INFO: Starting Wazuh installation assistant. Wazuh version: 4.9.2
23/01/2025 18:30:01 INFO: Verbose logging redirected to /var/log/wazuh-install.log
23/01/2025 18:30:25 INFO: --- Dependencies ----
23/01/2025 18:30:25 INFO: Installing gawk.
23/01/2025 18:30:35 INFO: Verifying that your system meets the recommended minimum hardware requirements.
23/01/2025 18:30:35 INFO: Wazuh web interface port will be 443.
23/01/2025 18:30:47 INFO: --- Dependencies ----
23/01/2025 18:30:47 INFO: Installing apt-transport-https.
23/01/2025 18:30:52 INFO: Installing debhelper.
```



```
23/01/2025 18:45:00 INFO: Filebeat post-install configuration finished.
23/01/2025 18:45:00 INFO: Starting service filebeat.
23/01/2025 18:45:03 INFO: filebeat service started.
23/01/2025 18:45:03 INFO: --- Wazuh dashboard ---
23/01/2025 18:45:03 INFO: Starting Wazuh dashboard installation.
23/01/2025 18:48:41 INFO: Wazuh dashboard installation finished.
23/01/2025 18:48:42 INFO: Wazuh dashboard post-install configuration finished.
23/01/2025 18:48:42 INFO: Starting service wazuh-dashboard.
23/01/2025 18:48:43 INFO: wazuh-dashboard service started.
23/01/2025 18:48:46 INFO: Updating the internal users.
23/01/2025 18:49:02 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
23/01/2025 18:49:32 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
23/01/2025 18:50:28 INFO: Initializing Wazuh dashboard web application.
23/01/2025 18:50:29 INFO: Wazuh dashboard web application not yet initialized. Waiting...
23/01/2025 18:50:45 INFO: Wazuh dashboard web application not yet initialized. Waiting...
23/01/2025 18:51:00 INFO: Wazuh dashboard web application initialized.
23/01/2025 18:51:00 INFO: --- Summary ---
23/01/2025 18:51:00 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: 3gl4bNlj4jf??5fGIe7Y.p4U*ueotILG
23/01/2025 18:51:00 INFO: --- Dependencies ----
23/01/2025 18:51:00 INFO: Removing gawk.
23/01/2025 18:51:10 INFO: Installation finished.
mrx@mrx:~/PZ$
```

Главная страница Wazuh



Wazuh
https://127.0.0.1/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-2
W.
Overview
a

AGENTS SUMMARY

No results

No results were found.

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	114	100
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Verify that your systems are configured according to your security policies baseline.

File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

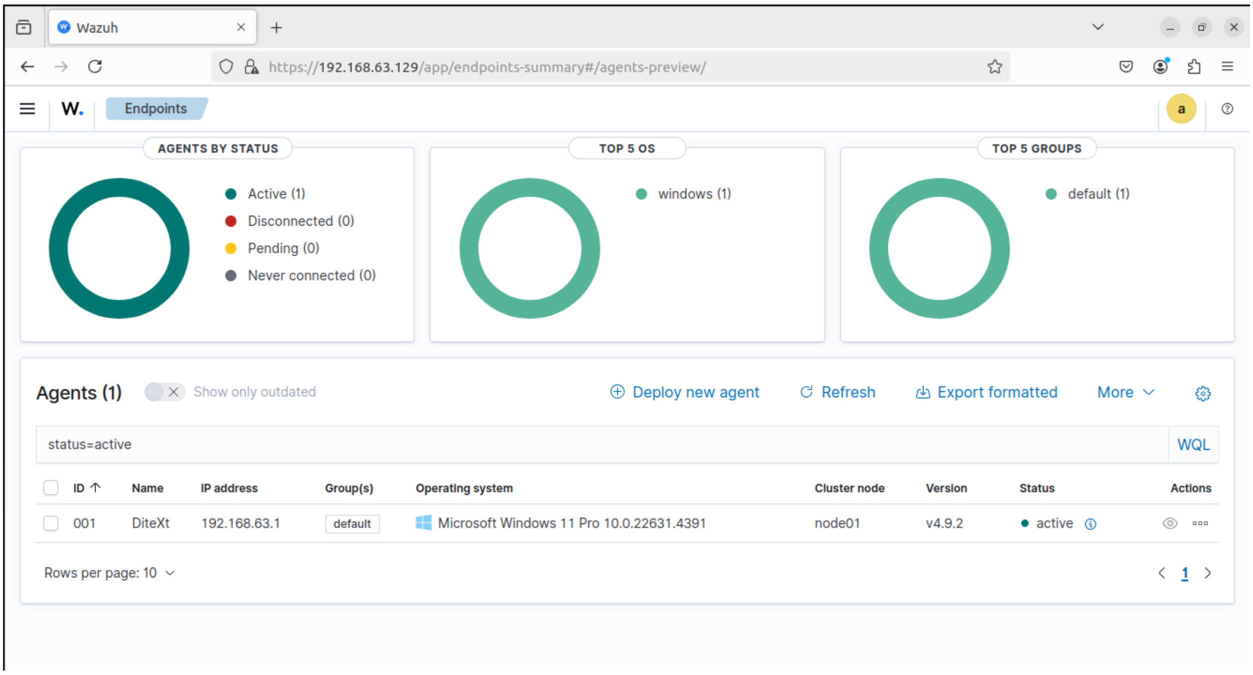
Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Security events from the knowledge base of adversary tactics and techniques based on

VirusTotal
Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.

Следуя официальной инструкциии от Wazuh устанавливаем агент на наш клиент и после видим его в системе

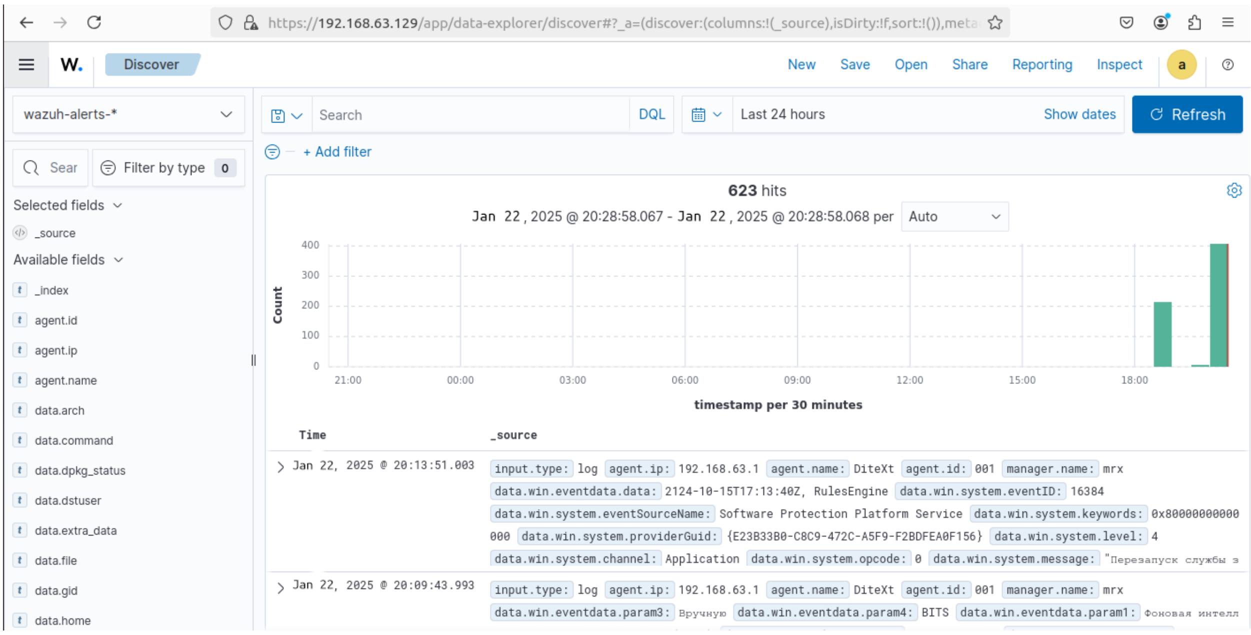


https://192.168.63.129/app/endpoints-summary#/agents-preview/

status=active

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	DiteXt	192.168.63.1	default	Microsoft Windows 11 Pro 10.0.22631.4391	node01	v4.9.2	active	

Уязвимости по умолчанию



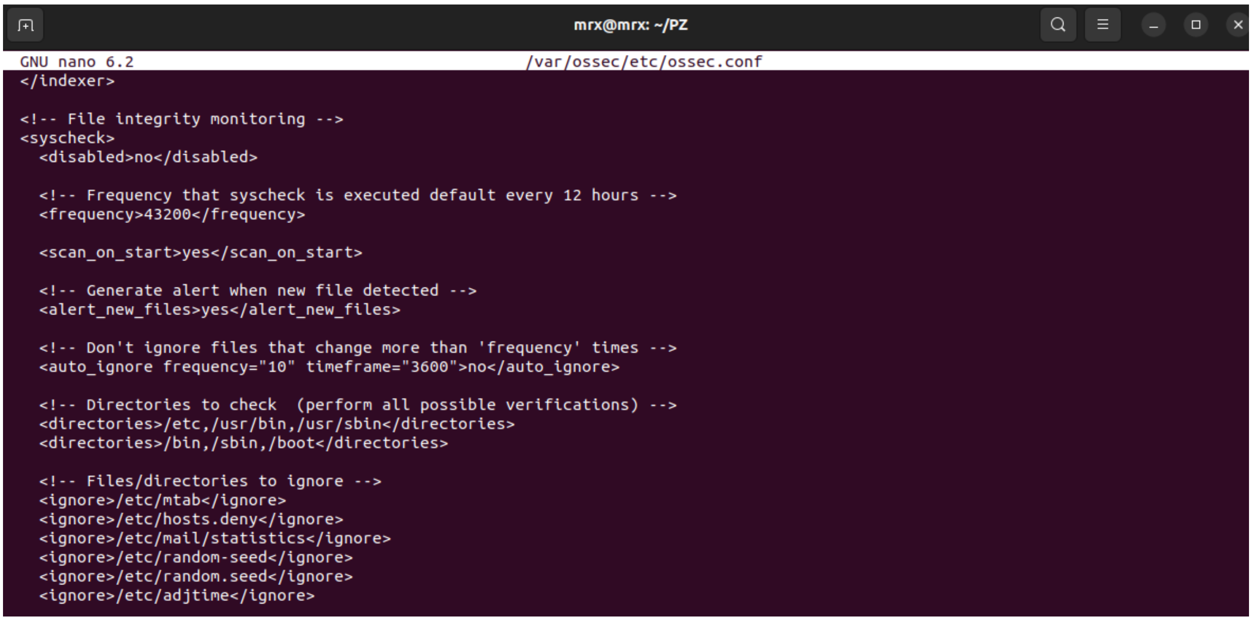
https://192.168.63.129/app/data-explorer/discover#?_a=(discover:(columns:!(_source),isDirty:!f,sort:!()),meta

623 hits

Jan 22, 2025 @ 20:28:58.067 - Jan 22, 2025 @ 20:28:58.068 per Auto

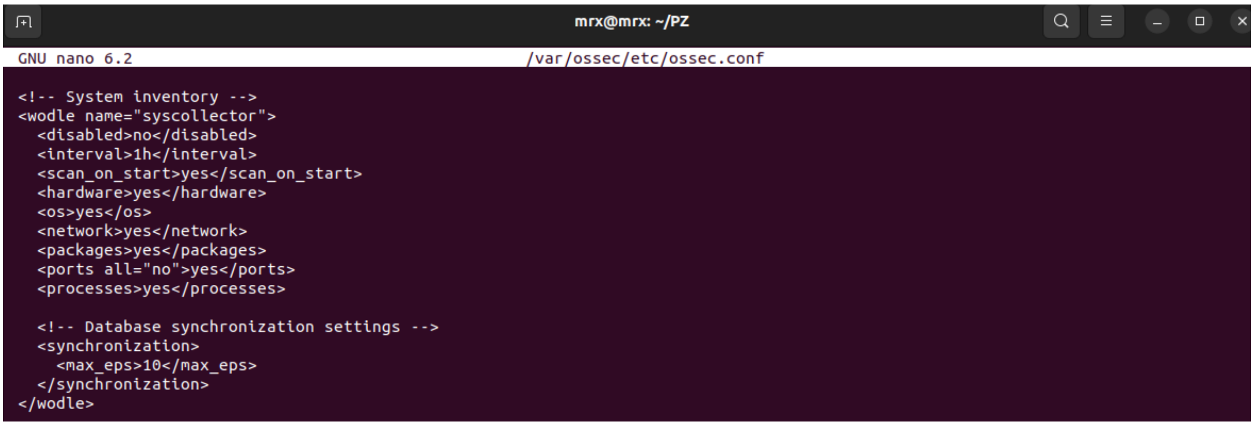
```
Time                         _source
Jan 22, 2025 @ 20:13:51.003  input.type: log agent.ip: 192.168.63.1 agent.name: DiteXt agent.id: 001 manager.name: mrx
                             data.win.eventdata.data: 2124-10-15T17:13:40Z, RulesEngine data.win.system.eventID: 16384
                             data.win.system.eventSourceName: Software Protection Platform Service data.win.system.keywords: 0x80000000000
                             000 data.win.system.providerGuid: {E23B33B0-C8C9-472C-A5F9-F2BDFEA0F156} data.win.system.level: 4
                             data.win.system.channel: Application data.win.system.opcode: 0 data.win.system.message: "Перезапуск службы з
Jan 22, 2025 @ 20:09:43.993  input.type: log agent.ip: 192.168.63.1 agent.name: DiteXt agent.id: 001 manager.name: mrx
                             data.win.eventdata.param3: Вручную data.win.eventdata.param4: BITS data.win.eventdata.param1: Фоновая интелл
```

Настройка для проверки целостности файлов



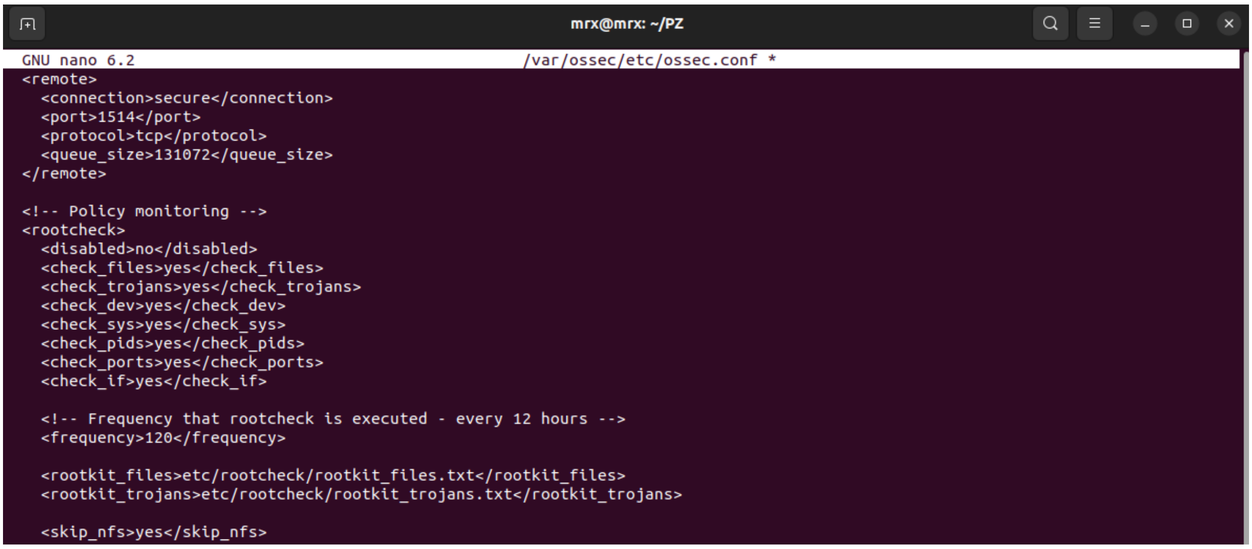
```
GNU nano 6.2                                 /var/ossec/etc/ossec.conf
</indexer>

<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <scan_on_start>yes</scan_on_start>

  <!-- Generate alert when new file detected -->
  <alert_new_files>yes</alert_new_files>

  <!-- Don't ignore files that change more than 'frequency' times -->
  <auto_ignore frequency="10" timeframe="3600">no</auto_ignore>

  <!-- Directories to check  (perform all possible verifications) -->
  <directories>/etc,/usr/bin,/usr/sbin</directories>
  <directories>/bin,/sbin,/boot</directories>

  <!-- Files/directories to ignore -->
  <ignore>/etc/mtab</ignore>
  <ignore>/etc/hosts.deny</ignore>
  <ignore>/etc/mail/statistics</ignore>
  <ignore>/etc/random-seed</ignore>
  <ignore>/etc/random.seed</ignore>
  <ignore>/etc/adjtime</ignore>
```

Настройка выявление уязвимостей



```
GNU nano 6.2                                 /var/ossec/etc/ossec.conf

<!-- System inventory -->
<wodle name="syscollector">
  <disabled>no</disabled>
  <interval>1h</interval>
  <scan_on_start>yes</scan_on_start>
  <hardware>yes</hardware>
  <os>yes</os>
  <network>yes</network>
  <packages>yes</packages>
  <ports all="no">yes</ports>
  <processes>yes</processes>

  <!-- Database synchronization settings -->
  <synchronization>
    <max_eps>10</max_eps>
  </synchronization>
</wodle>
```

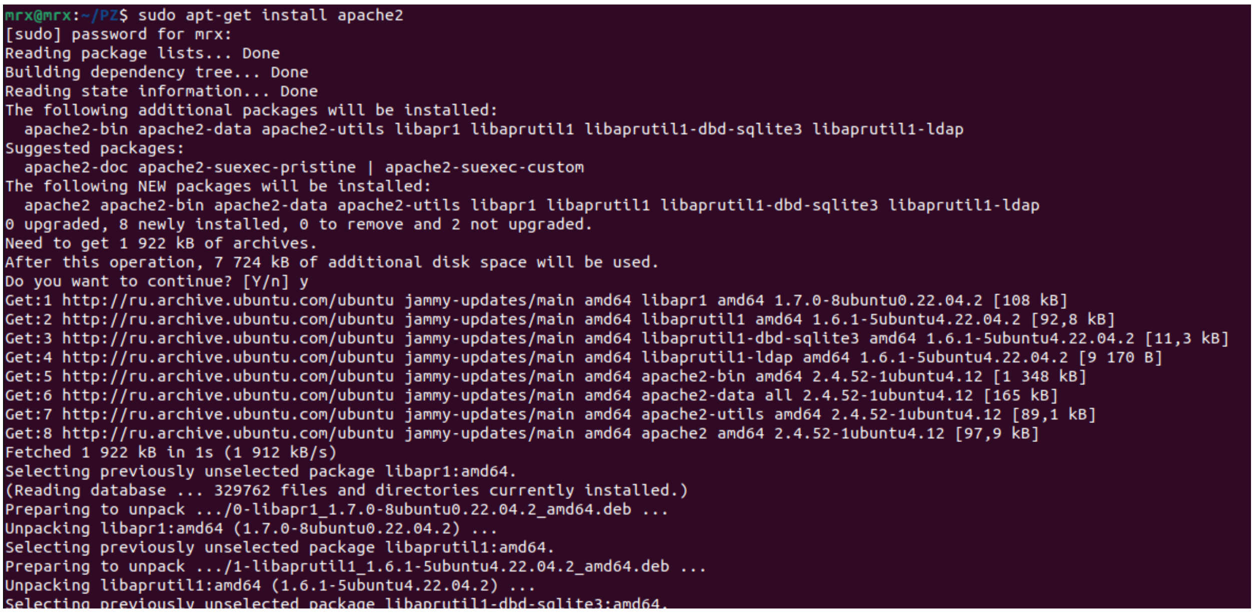
Настройка скрытых процессов



```
GNU nano 6.2                                 /var/ossec/etc/ossec.conf *
<remote>
  <connection>secure</connection>
  <port>1514</port>
  <protocol>tcp</protocol>
  <queue_size>131072</queue_size>
</remote>

<!-- Policy monitoring -->
<rootcheck>
  <disabled>no</disabled>
  <check_files>yes</check_files>
  <check_trojans>yes</check_trojans>
  <check_dev>yes</check_dev>
  <check_sys>yes</check_sys>
  <check_pids>yes</check_pids>
  <check_ports>yes</check_ports>
  <check_if>yes</check_if>

  <!-- Frequency that rootcheck is executed - every 12 hours -->
  <frequency>120</frequency>

  <rootkit_files>etc/rootcheck/rootkit_files.txt</rootkit_files>
  <rootkit_trojans>etc/rootcheck/rootkit_trojans.txt</rootkit_trojans>

  <skip_nfs>yes</skip_nfs>
```

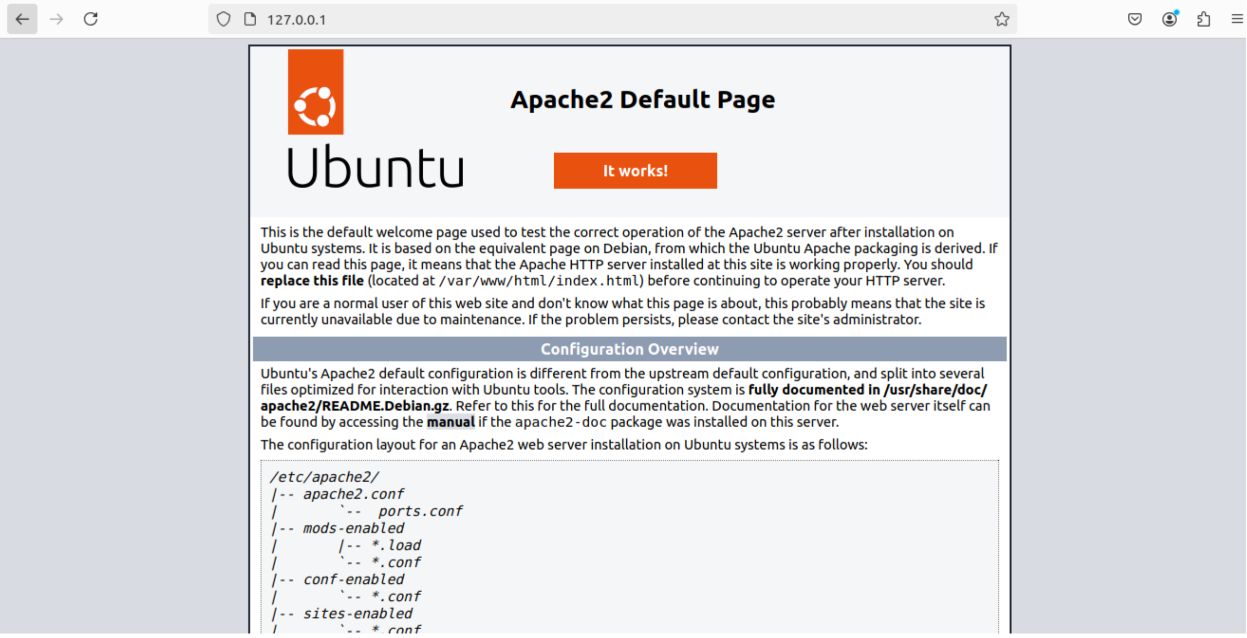
SQL-инъекции

Установка Apache



```
mrx@mrx:~/PZ$ sudo apt-get install apache2
[sudo] password for mrx:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
0 upgraded, 8 newly installed, 0 to remove and 2 not upgraded.
Need to get 1 922 kB of archives.
After this operation, 7 724 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapr1 amd64 1.7.0-8ubuntu0.22.04.2 [108 kB]
Get:2 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1 amd64 1.6.1-5ubuntu4.22.04.2 [92,8 kB]
Get:3 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-5ubuntu4.22.04.2 [11,3 kB]
Get:4 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-ldap amd64 1.6.1-5ubuntu4.22.04.2 [9 170 B]
Get:5 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-bin amd64 2.4.52-1ubuntu4.12 [1 348 kB]
Get:6 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-data all 2.4.52-1ubuntu4.12 [165 kB]
Get:7 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-utils amd64 2.4.52-1ubuntu4.12 [89,1 kB]
Get:8 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2 amd64 2.4.52-1ubuntu4.12 [97,9 kB]
Fetched 1 922 kB in 1s (1 912 kB/s)
Selecting previously unselected package libapr1:amd64.
(Reading database ... 329762 files and directories currently installed.)
Preparing to unpack .../0-libapr1_1.7.0-8ubuntu0.22.04.2_amd64.deb ...
Unpacking libapr1:amd64 (1.7.0-8ubuntu0.22.04.2) ...
Selecting previously unselected package libaprutil1:amd64.
Preparing to unpack .../1-libaprutil1_1.6.1-5ubuntu4.22.04.2_amd64.deb ...
Unpacking libaprutil1:amd64 (1.6.1-5ubuntu4.22.04.2) ...
Selecting previously unselected package libaprutil1-dbd-sqlite3:amd64.
```

Главная страница Apache



Apache2 Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

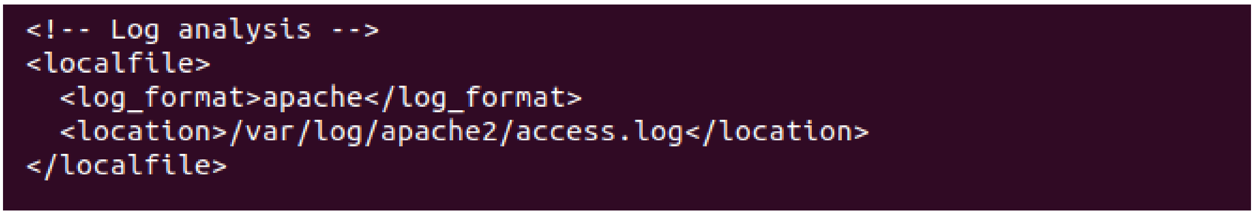
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

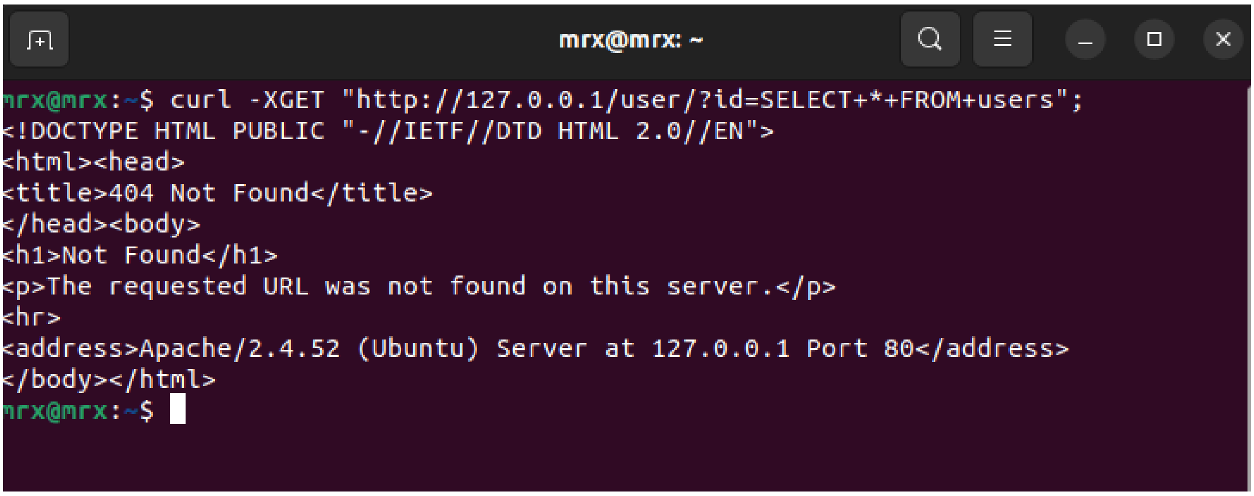
```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

Настройка для мониторинга файлов сервера Apache



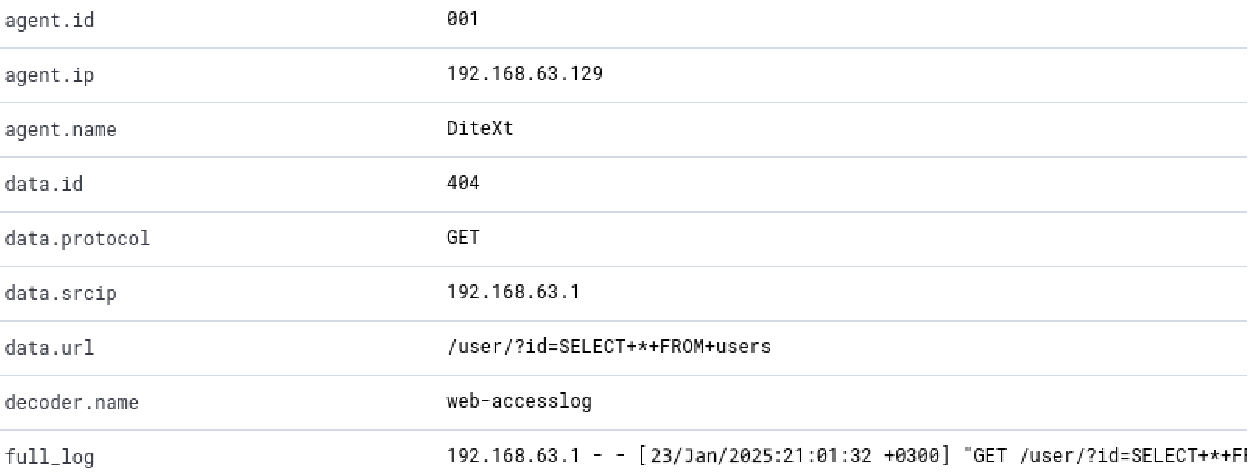
```
<!-- Log analysis -->
<localfile>
  <log_format>apache</log_format>
  <location>/var/log/apache2/access.log</location>
</localfile>
```

Имитируем атаку



```
mrx@mrx:~$ curl -XGET "http://127.0.0.1/user/?id=SELECT+*+FROM+users";
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.52 (Ubuntu) Server at 127.0.0.1 Port 80</address>
</body></html>
mrx@mrx:~$ 
```

Отчет о работе



agent.id	001
agent.ip	192.168.63.129
agent.name	DiteXt
data.id	404
data.protocol	GET
data.srcip	192.168.63.1
data.url	/user/?id=SELECT+*+FROM+users
decoder.name	web-accesslog
full_log	192.168.63.1 - - [23/Jan/2025:21:01:32 +0300] "GET /user/?id=SELECT+*+F