



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

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

Отчёт по практической работе №3
по дисциплине «Система для сбора событий и логов»

Выполнил:
Евдокимов А.М.
Группа: ББМО-02-23

Москва - 2024

В данной практике я выбрал готовый вариант Wazuh Server

[illegible]

```

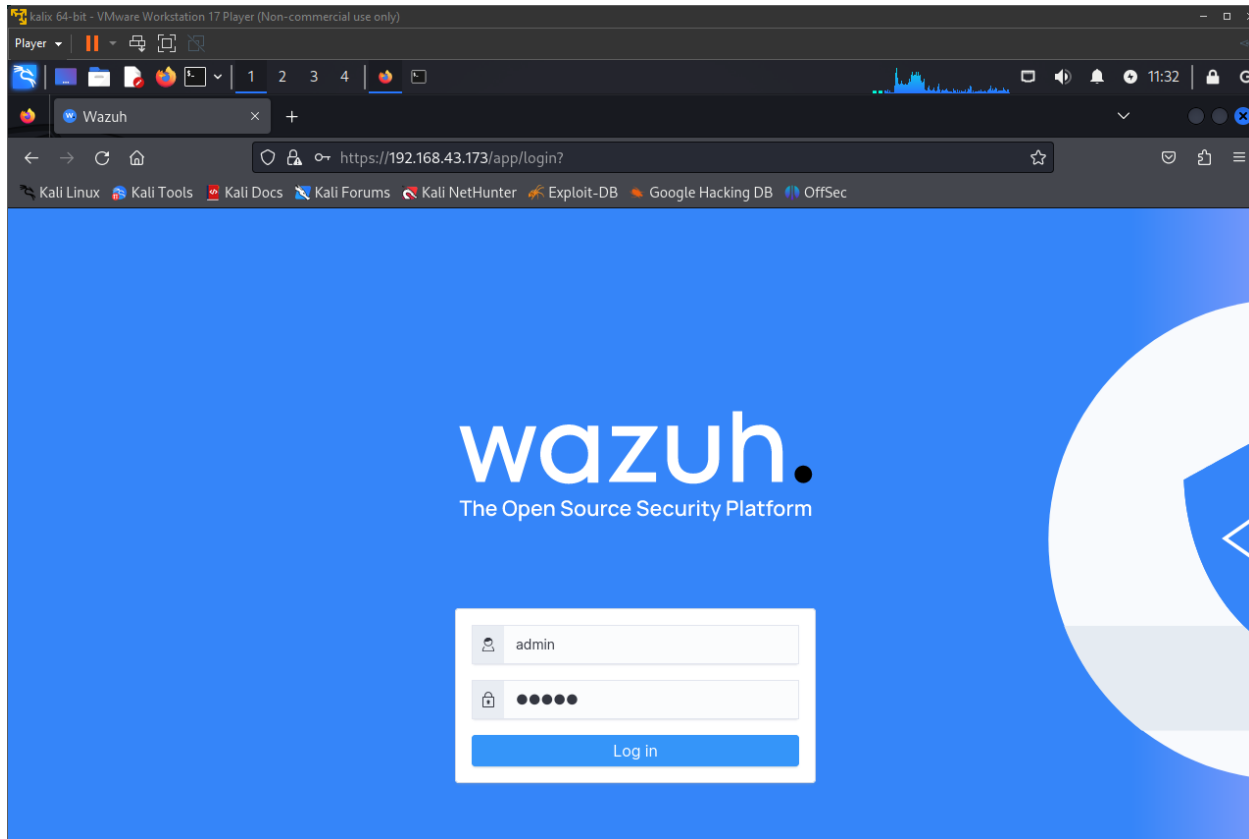
wazuh server - VMware Workstation 17 Player (Non-commercial use only)
Player  ▾  || ▾  🖨️  🖼️  🗑️
WWWWWWWWW.      WWWWWWWW.      0000000000
WWWWWWWWW.      WWWWWWWW.      00000000
WWWWWWW.        WWWWWW.        000000

WAZUH Open Source Security Platform
https://wazuh.com

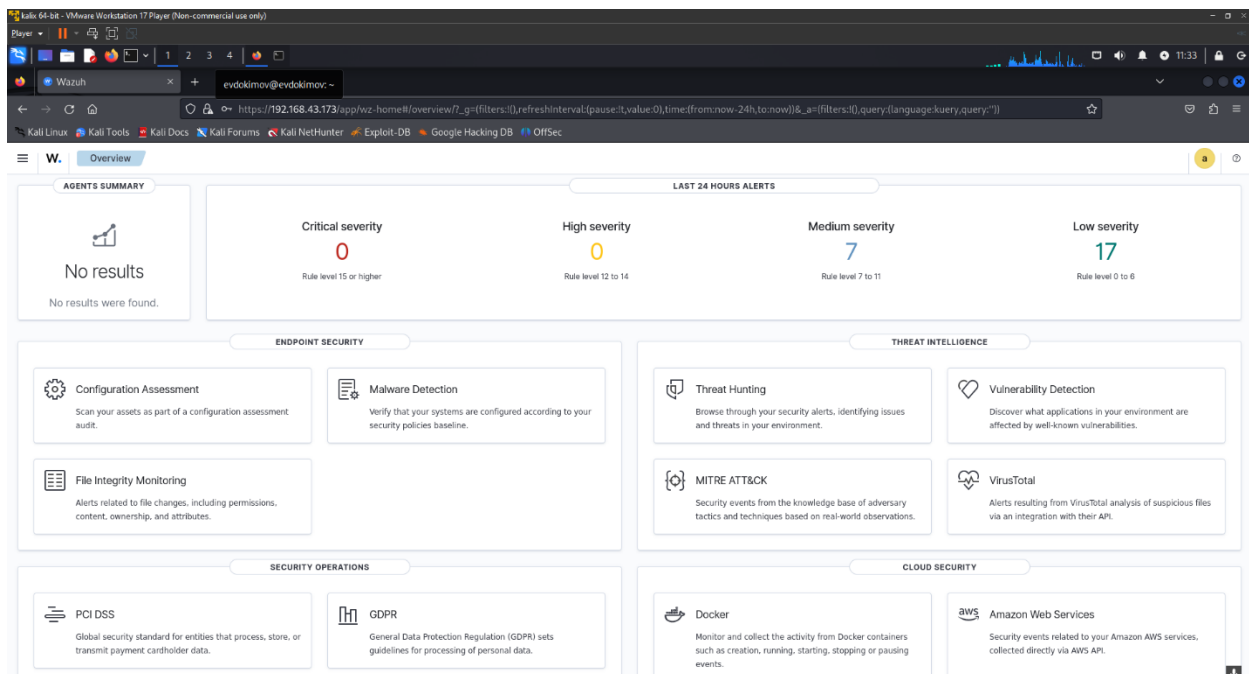
[wazuh-user@wazuh-server ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN gr
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast st
oup default qlen 1000
    link/ether 00:0c:29:bb:fc:62 brd ff:ff:ff:ff:ff:ff
    inet 192.168.43.173/24 brd 192.168.43.255 scope global dynamic eth0
        valid_lft 1738sec preferred_lft 1738sec
    inet6 fe80::20c:29ff:febb:fc62/64 scope link
        valid_lft forever preferred_lft forever
[wazuh-user@wazuh-server ~]$

```

Авторизация



Веб-интерфейс Wazuh



Теперь готовимся установить агент на другой ВМ

kalix 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Player ▾ | 1 2 3 4 | 11:47

Wazuh Deploying Wazuh agents


https://192.168.43.173/app/endpoints-summary#/agents-preview/deploy


Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec


W. Endpoints Deploy new agent

Deploy new agent

✓ **Select the package to download and install on your system:**

**LINUX**
☐ RPM amd64 ☐ RPM aarch64
☒ DEB amd64 ☐ DEB aarch64

**WINDOWS**
☐ MSI 32/64 bits

**macOS**
☐ Intel
☐ Apple silicon

[For additional systems and architectures, please check our documentation.](#)

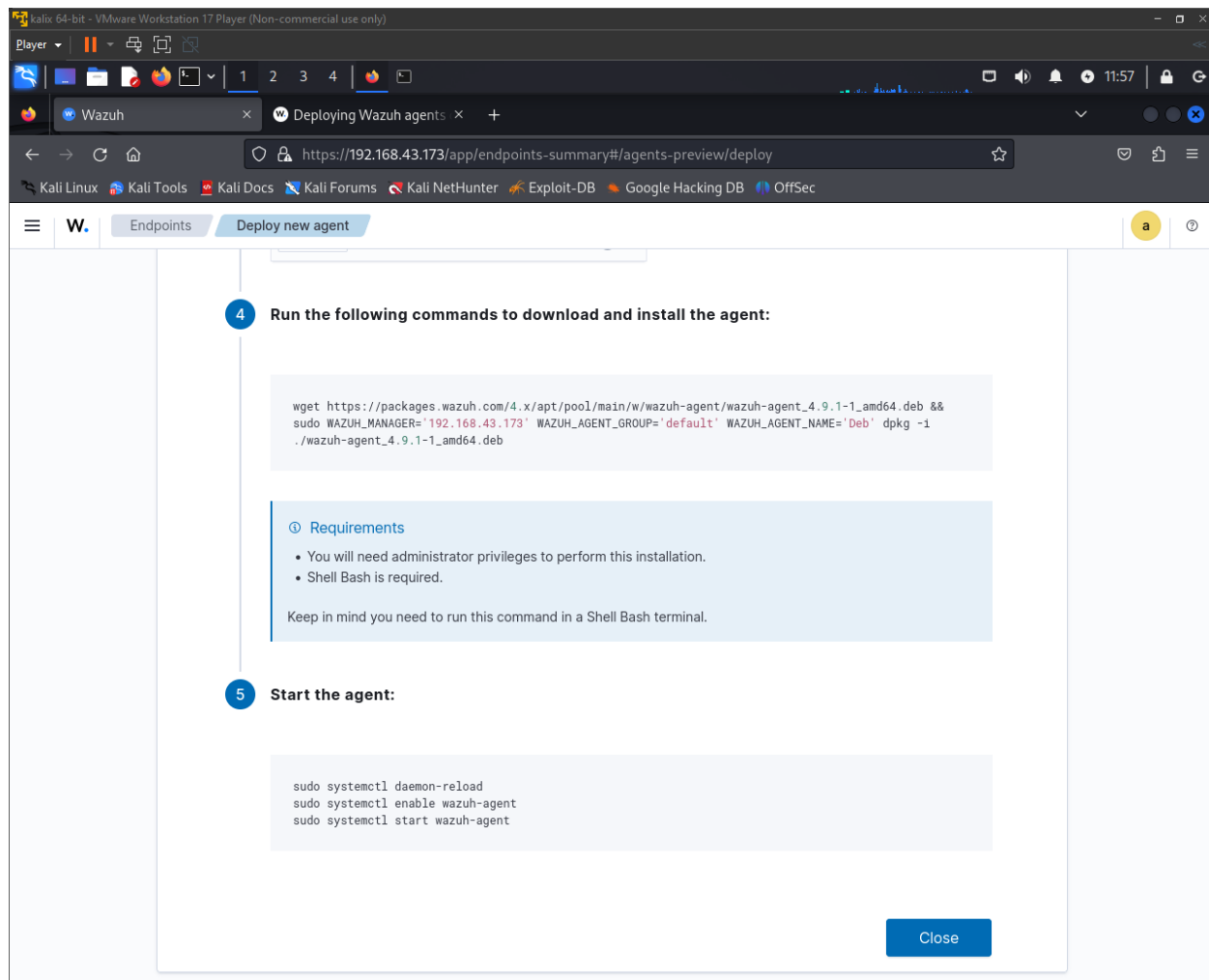
✓ **Server address:**

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

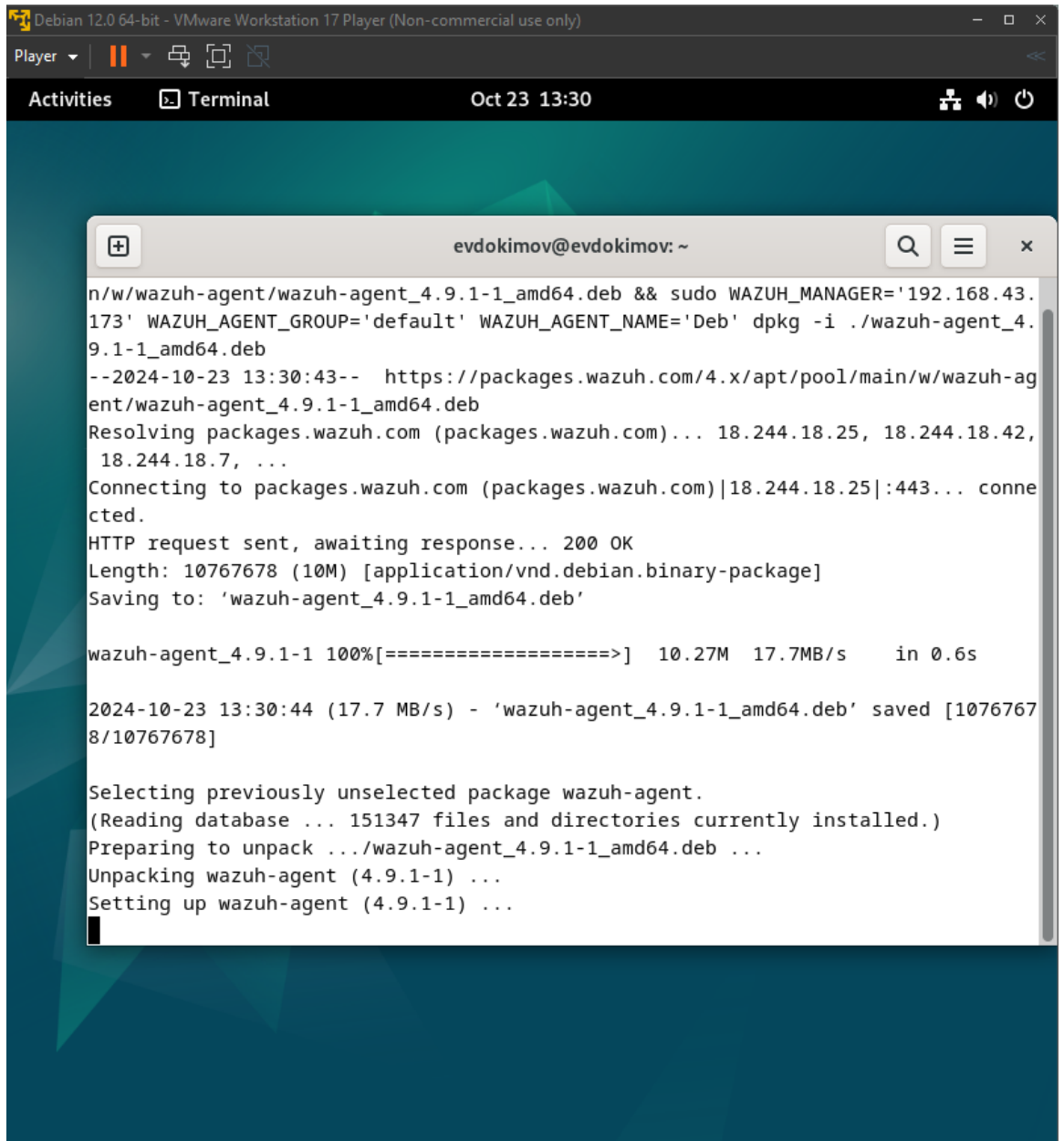
Assign a server address [?](#)

☐ Remember server address

3 **Optional settings:**



Разворачиваем агент на второй ВМ



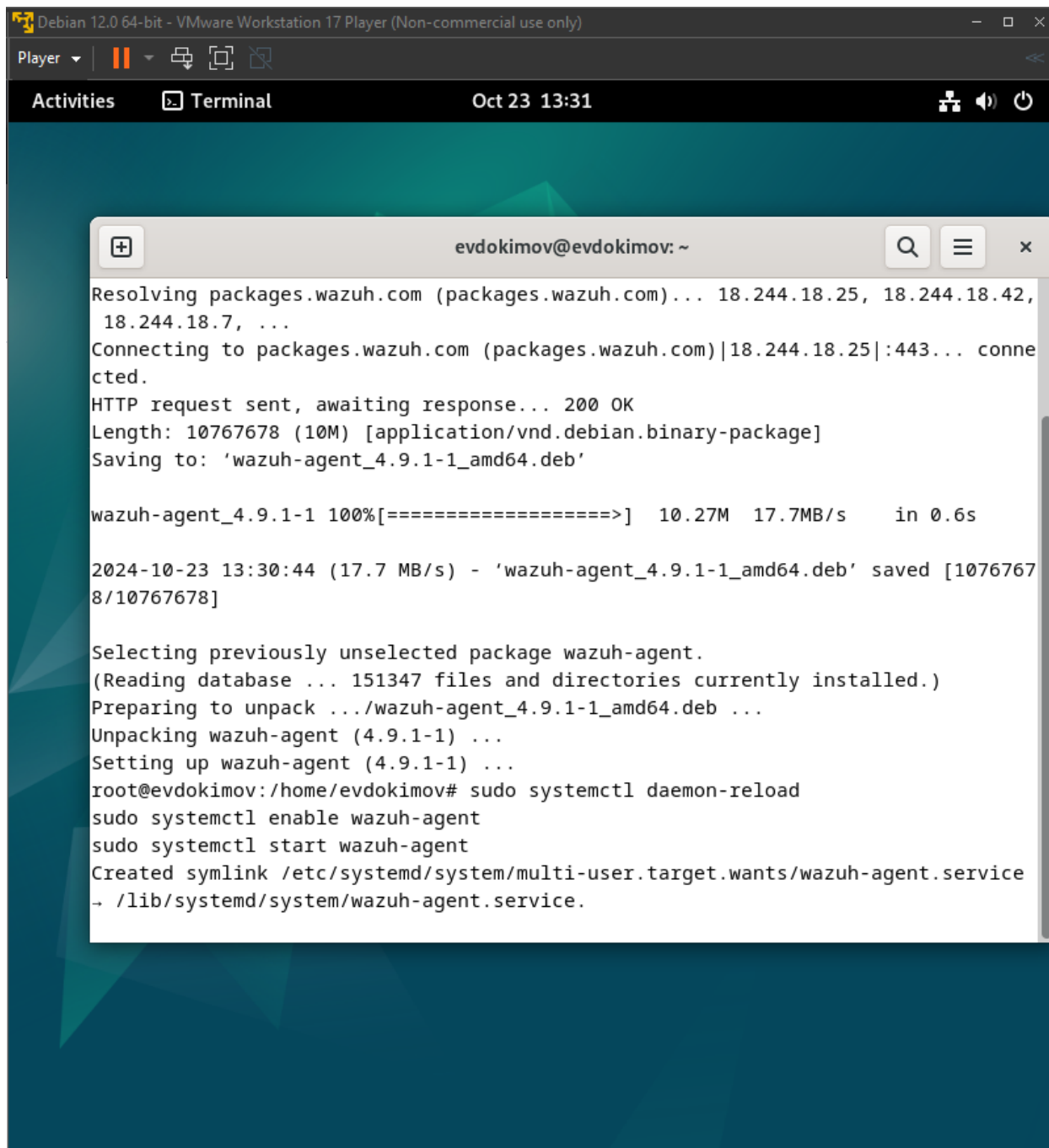
```
Debian 12.0 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player | || | |
Activities | Terminal | Oct 23 13:30 | [Icons]

evdokimov@evdokimov: ~
n/w/wazuh-agent/wazuh-agent_4.9.1-1_amd64.deb && sudo WAZUH_MANAGER='192.168.43.173' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='Deb' dpkg -i ./wazuh-agent_4.9.1-1_amd64.deb
--2024-10-23 13:30:43-- https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.9.1-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 18.244.18.25, 18.244.18.42, 18.244.18.7, ...
Connecting to packages.wazuh.com (packages.wazuh.com)|18.244.18.25|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10767678 (10M) [application/vnd.debian.binary-package]
Saving to: 'wazuh-agent_4.9.1-1_amd64.deb'

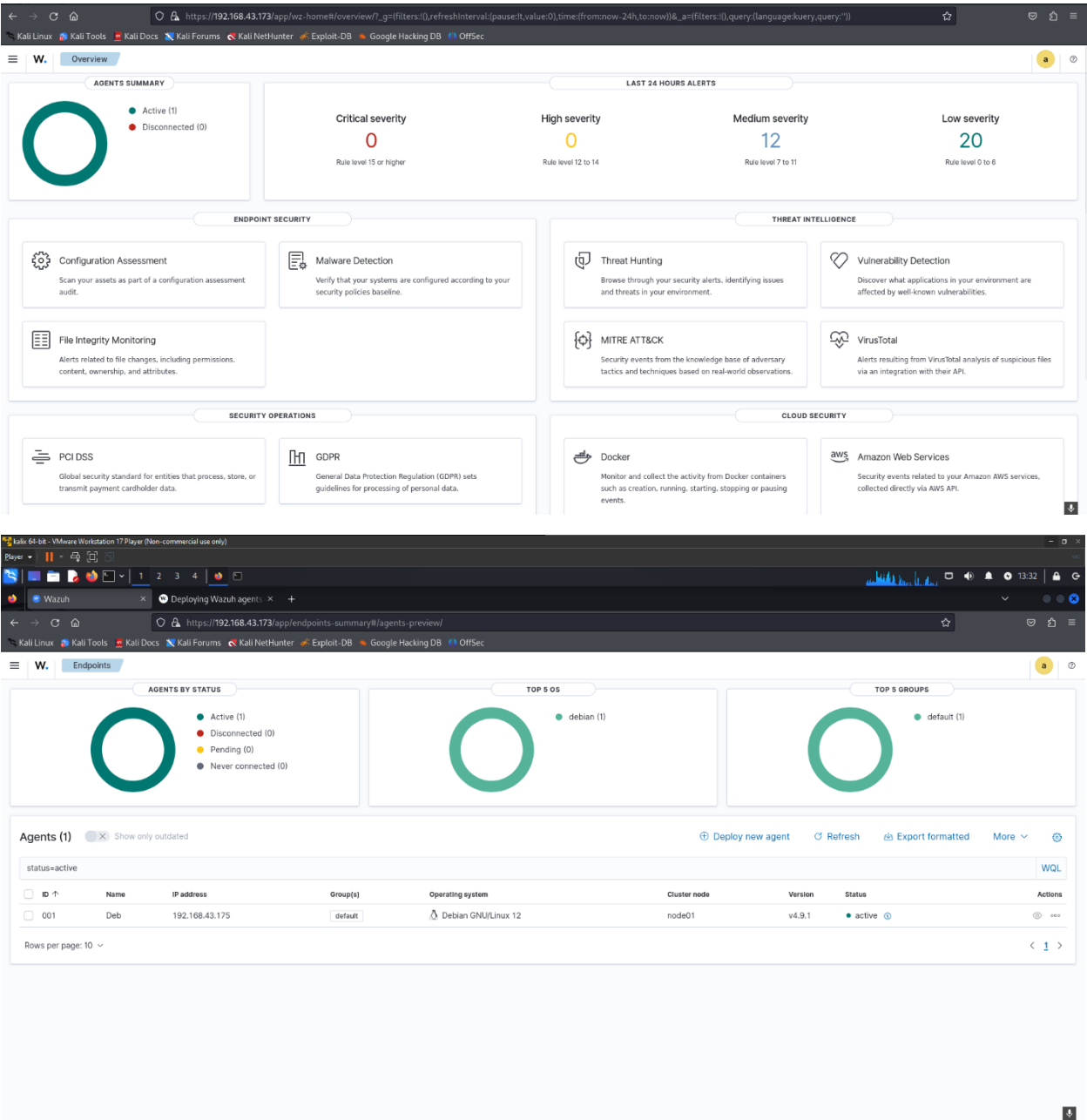
wazuh-agent_4.9.1-1 100%[=====>] 10.27M 17.7MB/s in 0.6s

2024-10-23 13:30:44 (17.7 MB/s) - 'wazuh-agent_4.9.1-1_amd64.deb' saved [10767678/10767678]

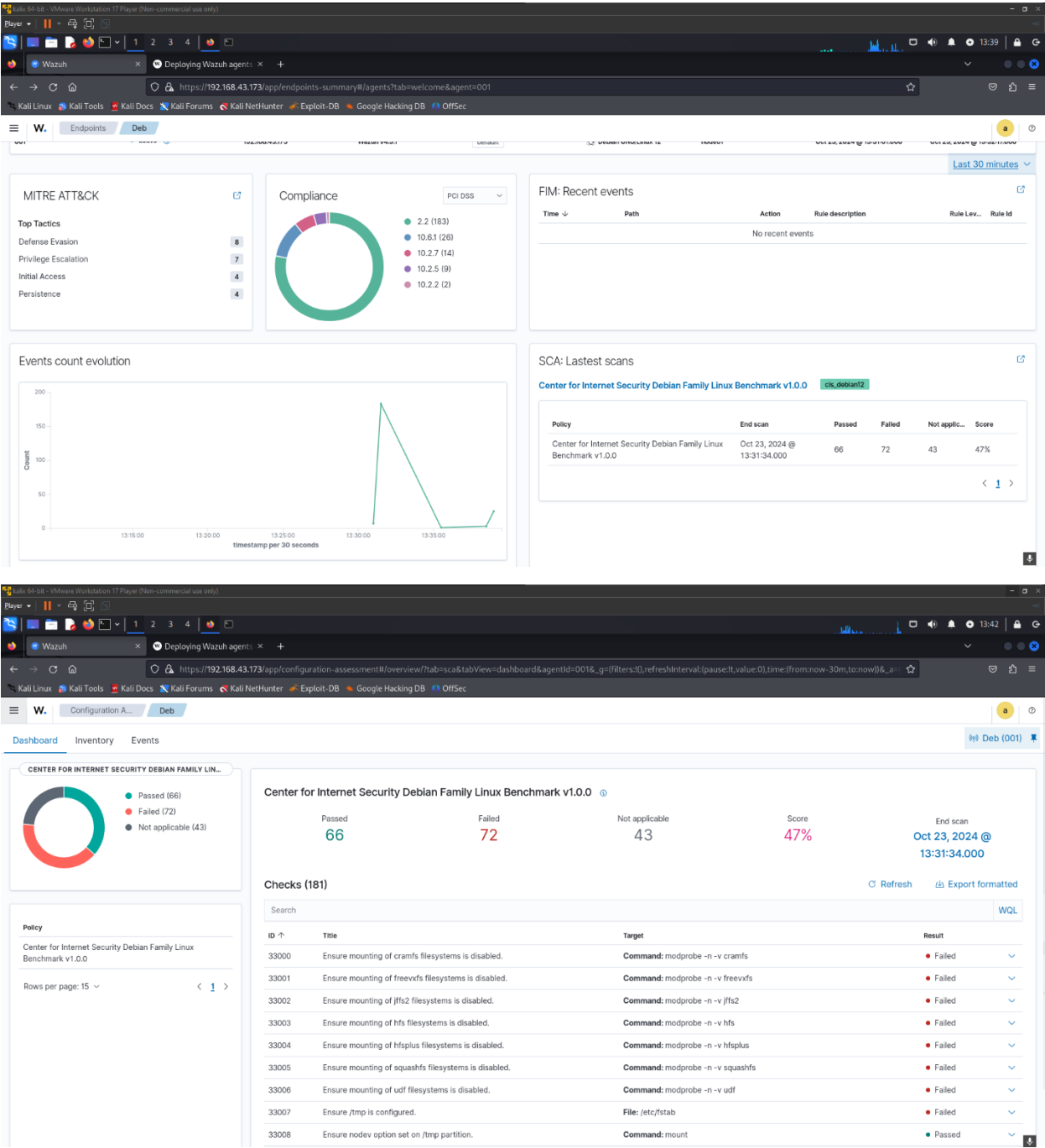
Selecting previously unselected package wazuh-agent.
(Reading database ... 151347 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.9.1-1_amd64.deb ...
Unpacking wazuh-agent (4.9.1-1) ...
Setting up wazuh-agent (4.9.1-1) ...
```



После настройки убедились, что агент настроен. И доступна машина для мониторинга



Система имеет встроенный детектор уязвимостей



Wazuh

Deploying Wazuh agent: x +

https://192.168.43.173/app/configuration-assessment#/overview?tab=sca&redirectPolicy=cis_debian12&agentId=0016_g=(filters:[])&refreshInterval:(pause:0,value:0)&time:(from:now-24h,to:now)

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

Policy

Center for Internet Security Debian Family Linux Benchmark v1.0.0

Rows per page: 15

ID	Title	Target	Result
33010	Ensure noexec option set on /tmp partition.	Command: mount	Passed
33011	Ensure separate partition exists for /var.	Command: mount	Failed

Rationale

Since the /var directory may contain world-writable files and directories, there is a risk of resource exhaustion if it is not bound to a separate partition.

Remediation

For new installations, during installation create a custom partition setup and specify a separate partition for /var For systems that were previously installed, create a new partition and configure /etc/fstab as appropriate.

Description

The /var directory is used by daemons and other system services to temporarily store dynamic data. Some directories created by these processes may be world-writable. Note: When modifying /var it is advisable to bring the system to emergency mode (so auditd is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multiuser mode.

Check (Condition: all)

- cmount -> r15+ on /var type ext4

Compliance

cis: 1.1.6

cis_csc_v7: 5.1

mmmc_v2.0: AC.1.002,CM.2.061,SC.3.180

iso_27001-2013: A.8.1.3,A.14.2.5

mitre_techniques: T1110,T1003,T1081,T1097,T1178,T1072,T1067,T1495,T1019,T1177,T1485,T1486,T1491,T1488,T1487,T1490,T1146,T1148,T1015,T1133,T1200,T1076,T1051,T1176,T1501,T1087,T1098,T1139,T1197,T1092,T1136,T1011,T1147,T1130,T1174,T1053,T1106,T1206,T1503,T1214,T1187,T1208,T1142,T1075,T1201,T1145,T1184,T1537,T1078,T1077,T1134,T1017,T1088,T1175,T1190,T1210,T1525,T1215,T1086,T1055,T1505,T1035,T1218,T1169,T1100,T1047,T1084,T1028,T1156,T1196,T1530,T1089,T1073,T1157,T1054,T1070,T1037,T1036,T1096,T1034,T1150,T1504,T1494,T1489,T1198,T1165,T1492,T1080,T1209,T1112,T1058,T1173,T1137,T1539,T1535,T1506,T1138,T1044,T1199

nist_sp_800-53: AU-2,CM-1,CM-2,CM-6,CM-7,IA-5,IA-6,SC-20,SC-21

pcl_dss_v3.2.1: 2.2

33012

Ensure separate partition exists for /var/tmp.

Command: mount

Failed

Wazuh

Deploying Wazuh agent: x +

https://192.168.43.173/app/configuration-assessment#/overview?tab=sca&redirectPolicy=cis_debian12&agentId=0016_g=(filters:[])&refreshInterval:(pause:0,value:0)&time:(from:now-24h,to:now)

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

Document Details

View surrounding documents

View single document

TableJSON

f _index

wazuh-alerts-4x-2024.10.23

f agent.id

001

f agent.ip

192.168.43.175

f agent.name

Deb

f data.sca.check.compliance.cis

6.2.10

f data.sca.check.compliance.cis_csc_v7

4.6

f data.sca.check.compliance.mmc_v2

AC.2.008

f data.sca.check.compliance.iso_27001-2013

A.9.2.3

f data.sca.check.compliance.mitre_techniques

T1019,T1098,T1017,T1043,T1175,T1136,T1094,T1482,T1048,T1190,T1210,T1133,T1046,T1145,T1076,T1484,T1489,T1105,T1095,T1072,T1190,T1085,T1028,T1112,T1058,T1198,T1209

f data.sca.check.description

Any account with UID 0 has supervisor privileges on the system.

f data.sca.check.file

/etc/passwd

f data.sca.check.id

33180

f data.sca.check.rationale

This access must be limited to only the default root account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in item 5.6 Ensure access to the su command is restricted.

f data.sca.check.remediation

Remove any users other than root with UID 0 or assign them a new UID if appropriate.

f data.sca.check.result

passed

f data.sca.check.title

Ensure root is the only UID 0 account.

f data.sca.policy

Center for Internet Security Debian Family Linux Benchmark v1.0.0

f data.sca.scan.id

1689233944

f data.sca.type

check

f decoder.name

sca

Wazuh Configuration Assistant (Wazuh) interface showing a list of documents and a detailed view of a document.

Document Details

Field	Value
data.sca.check.title	Ensure root is the only UID 0 account.
data.sca.policy	Center for Internet Security Debian Family Linux Benchmark v1.0.0
data.sca.scan_id	1689233944
data.sca.type	check
decoder.name	sca
id	1729704701.703670
input.type	log
location	sca
manager.name	wazuh-server
rule.cis	6.2.10
rule.cis_csc_v7	4.6
rule.description	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure root is the only UID 0 account.
rule.freetimes	66
rule.gdpr	IV.35.7.d
rule.groups	sca
rule.id	19008
rule.iso_27001-2013	A.9.2.3
rule.level	3
rule.mail	false
rule.mitre_techniques	T1019, T1068, T1017, T1043, T1175, T1136, T1094, T1482, T1048, T1190, T1210, T1133, T1046, T1145, T1076, T1494, T1489, T1051, T1095, T1072, T1199, T1065, T1028, T1112, T1058, T1198, T1209
rule.nist_800_53	CM.1
rule.pci_dss	2.2
rule.tsc	CC7.1, CC7.2
timestamp	Oct 23, 2024 @ 13:31:41:643

Создание проверки целостности файлов

```
evdokimov@evdokimov: /var
GNU nano 7.2 ossec.conf *
<!-- 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>

  <!-- Enable attribute change monitoring -->
  <auto_ignore>no</auto_ignore>
  <alert_new_files>yes</alert_new_files>

  <!-- 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>
```

Настройка выявлений уязвимостей в соответствии с документацией

```
evdokimov@evdokimov: /var
GNU nano 7.2 ossec.conf *
<vulnerability-detector>
  <enabled>yes</enabled>
  <interval>5m</interval>
  <min_full_scan_interval>10m</min_full_scan_interval>
  <run_on_start>yes</run_on_start>

  <!-- Ubuntu OS vulnerabilities -->
  <provider name="canonical">
    <enabled>yes</enabled>
    <os>trusty</os>
    <os>xenial</os>
    <os>bionic</os>
    <os>focal</os>
    <os>jammy</os>
    <update_interval>1h</update_interval>
  </provider>

  <!-- Debian OS vulnerabilities -->
  <provider name="debian">
    <enabled>yes</enabled>
    <os>buster</os>

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

Выявление скрытых процессов

```
evdokimov@evdokimov: /var
GNU nano 7.2 ossec.conf *
<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>43200</frequency>

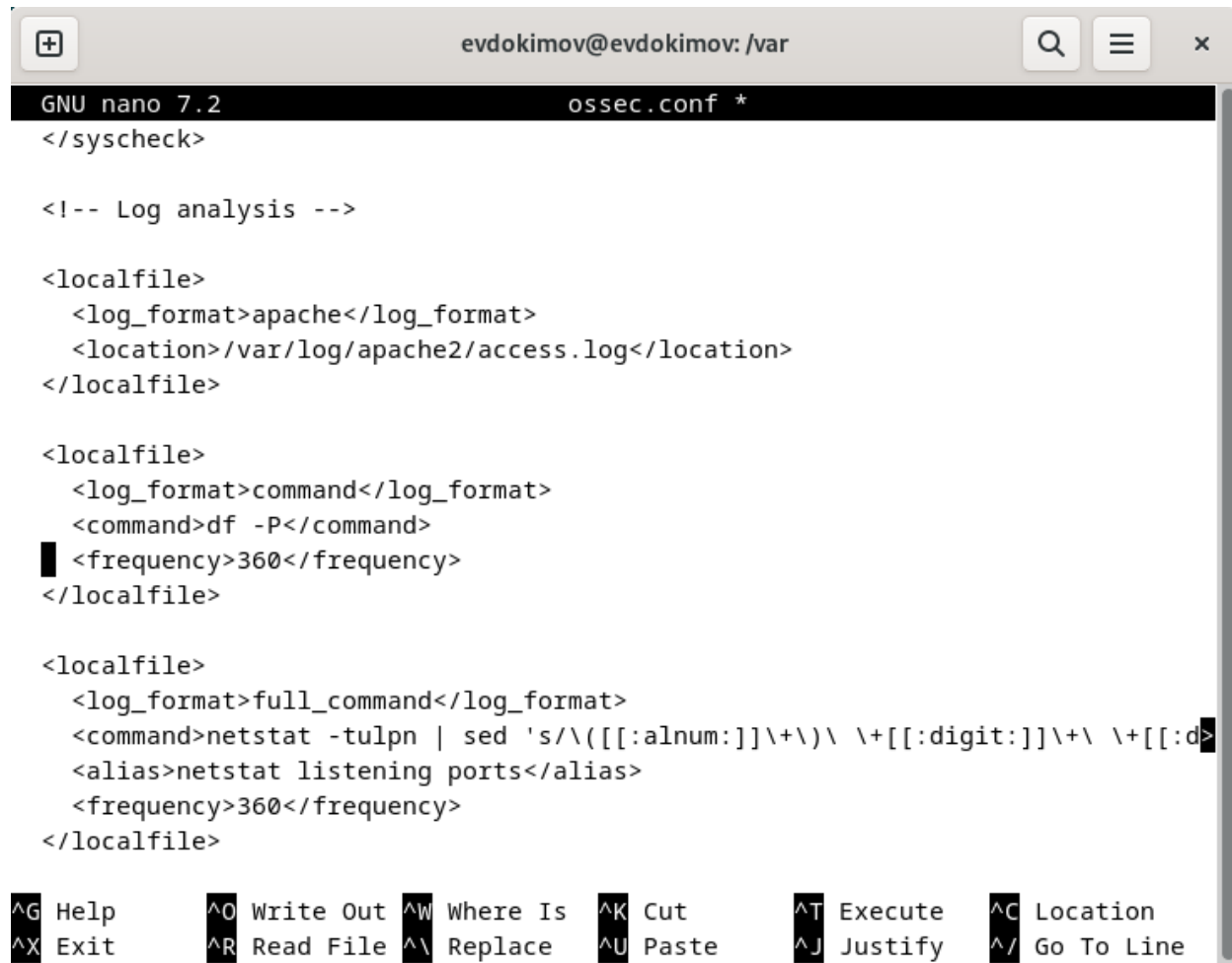
  <rootkit_files>etc/shared/rootkit_files.txt</rootkit_files>
  <rootkit_trojans>etc/shared/rootkit_trojans.txt</rootkit_trojans>

  <skip_nfs>yes</skip_nfs>

  <ignore>/var/lib/containerd</ignore>
  <ignore>/var/lib/docker/overlay2</ignore>
</rootcheck>

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

Выявление SQL-инъекций



```
evdokimov@evdokimov: /var
GNU nano 7.2 ossec.conf *
</syscheck>

<!-- Log analysis -->

<localfile>
  <log_format>apache</log_format>
  <location>/var/log/apache2/access.log</location>
</localfile>

<localfile>
  <log_format>command</log_format>
  <command>df -P</command>
  <frequency>360</frequency>
</localfile>

<localfile>
  <log_format>full_command</log_format>
  <command>netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+([[:digit:]]\+\ \+([[:d>
  <alias>netstat listening ports</alias>
  <frequency>360</frequency>
</localfile>

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

Проверка работы настроенных механизмов

SQL injection

