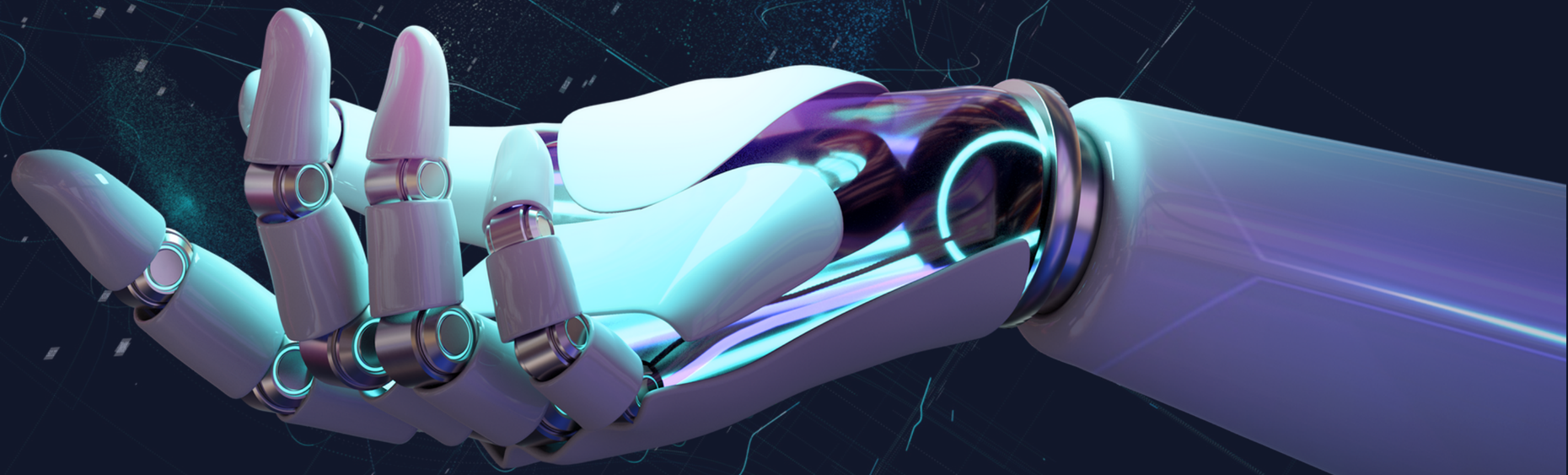
بسم الله الرحمن الرحيم

تثبيت واعداد Wazuh
وتثبيت واعداد Sysmon

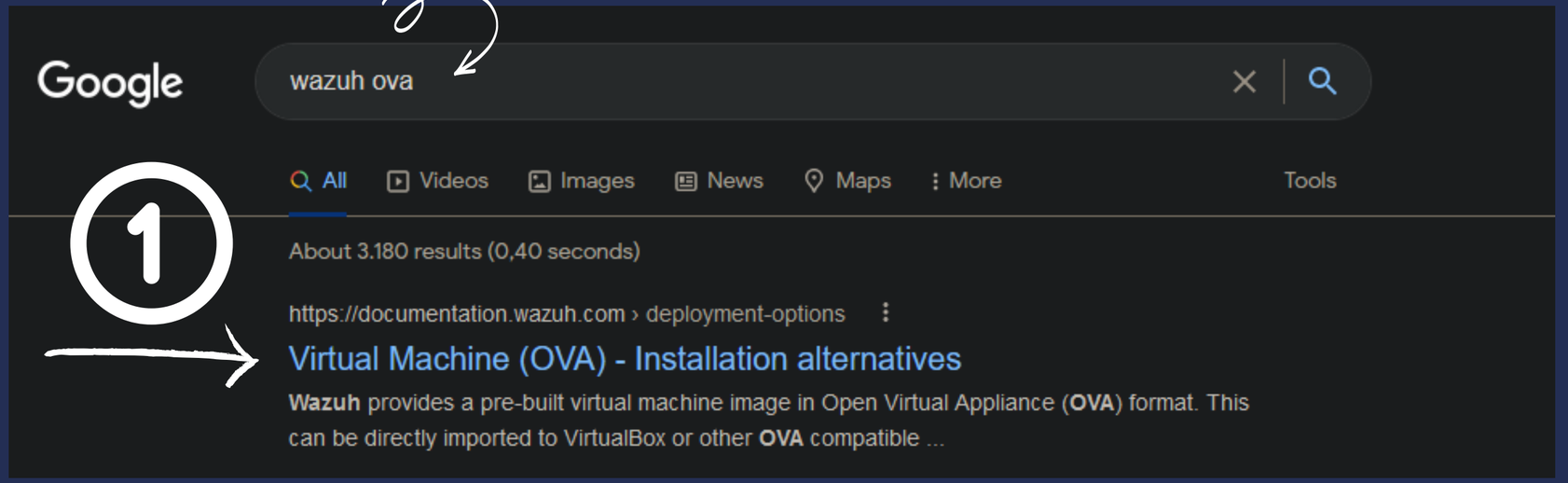
by:Abdulrahman.

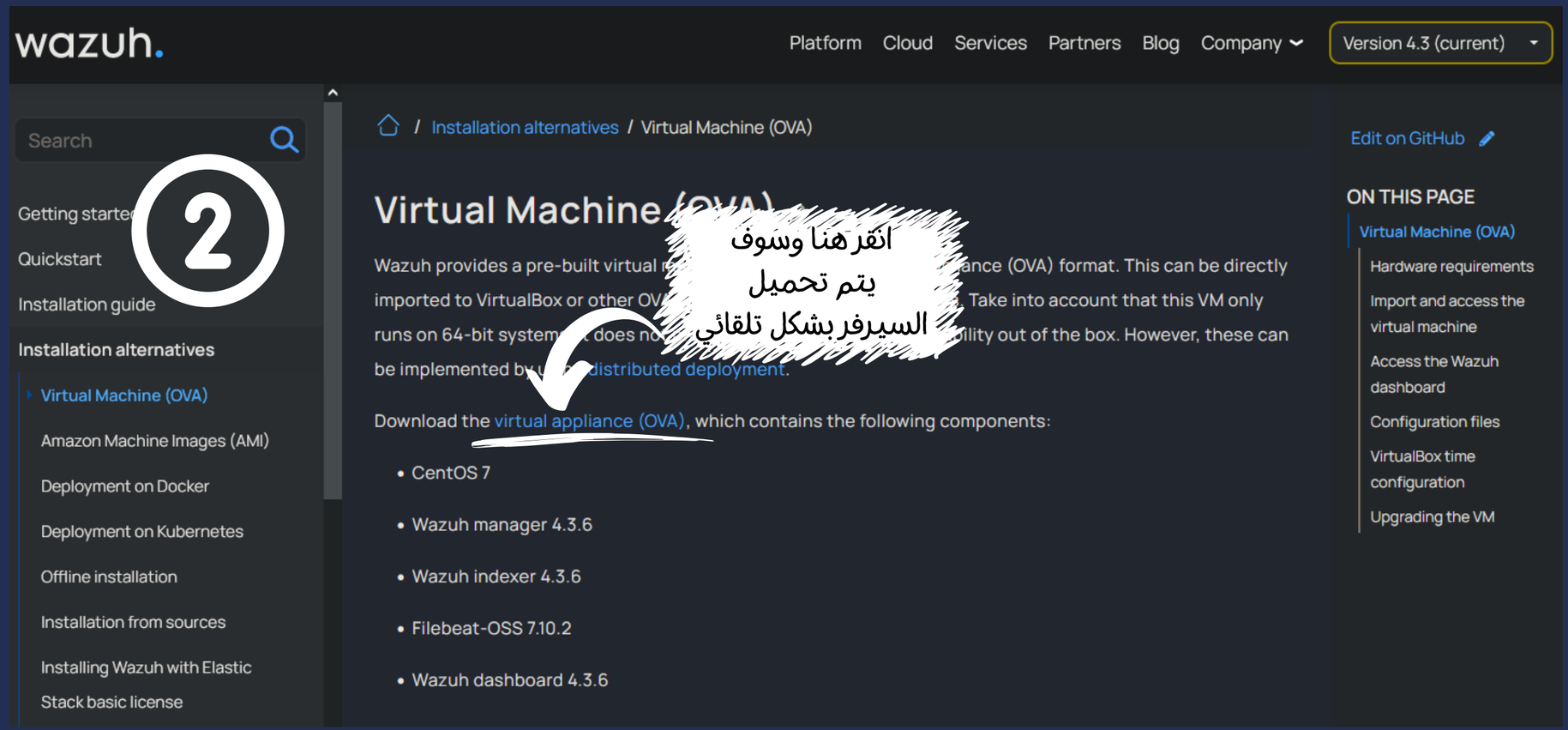


D1HM

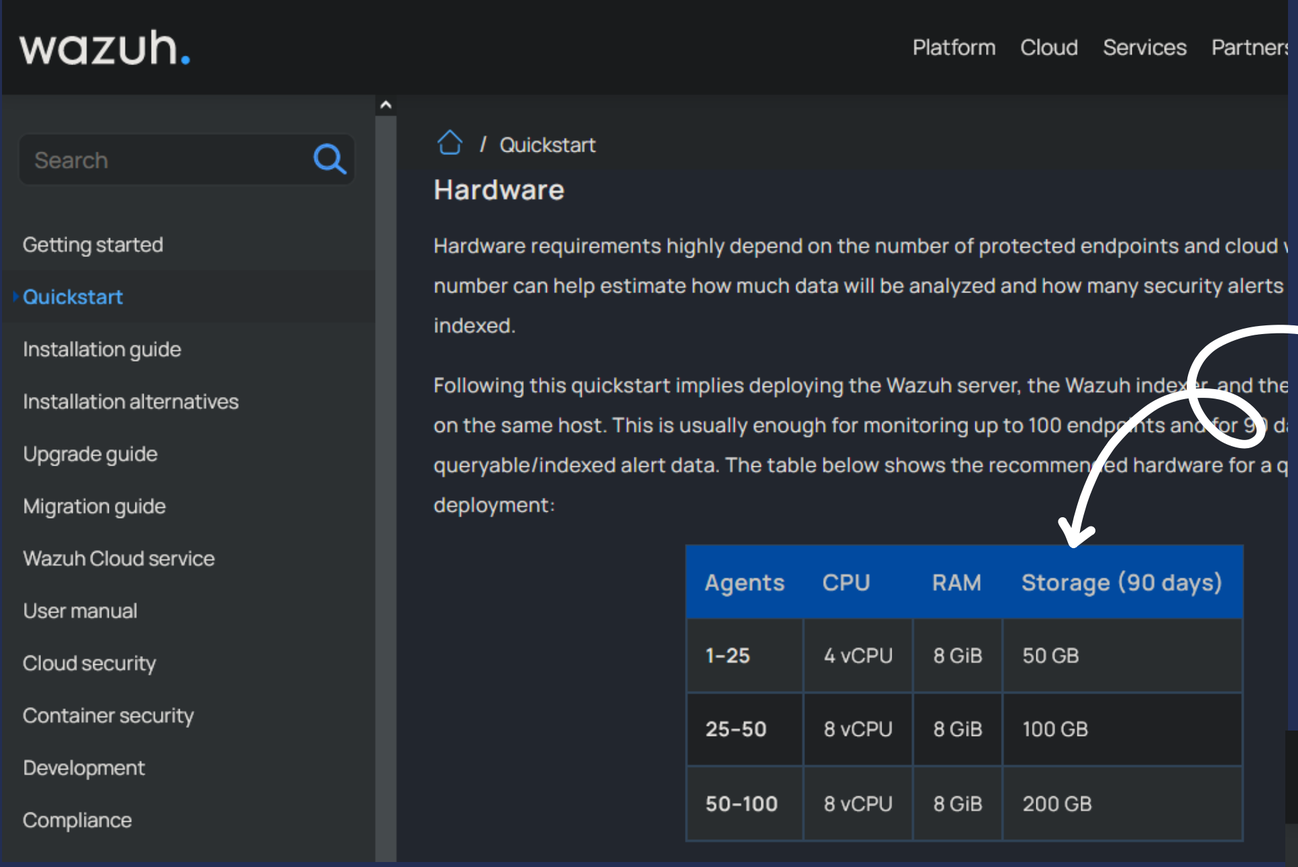
@D2HM5

شرح اعداد وتثبيت wazuh على virtualbox

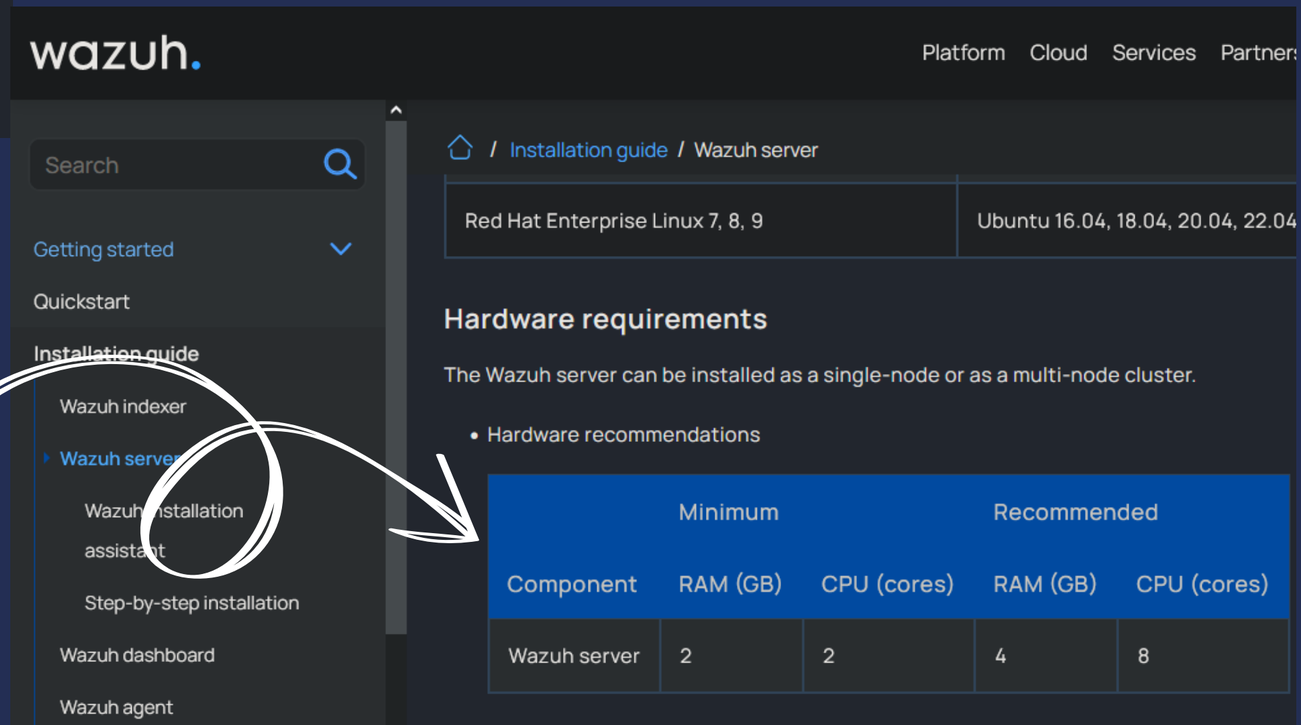




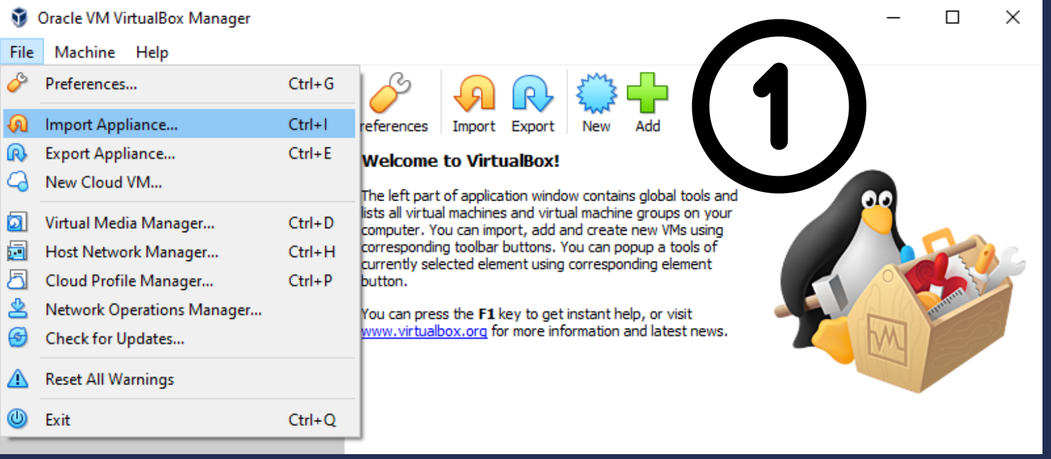
انقر هنا وسوف
يتم تحميل
السيرفر بشكل تلقائي

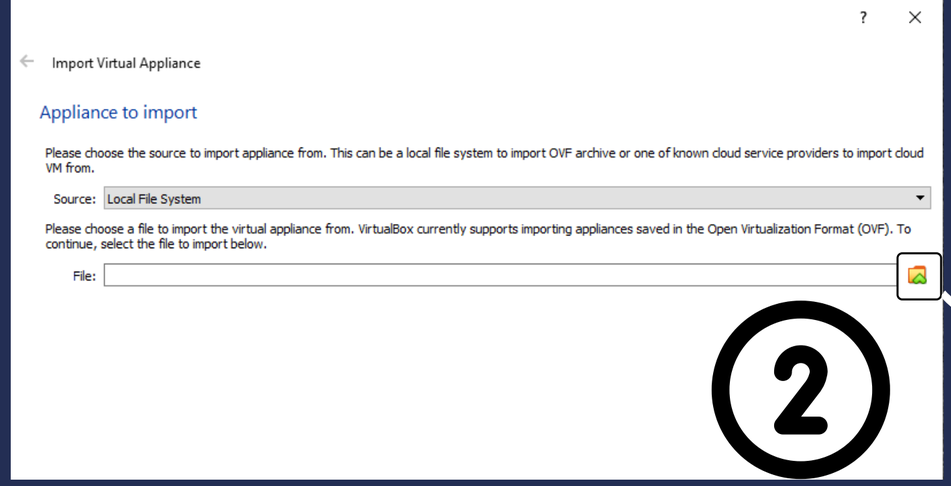


هنا يوضح استخدام السيرفر على مدار 90 يوم من حيث مساحه الهارديسك وقدرة المعالج والرامات وتدل "Agents" على عدد الاجهزه المستضافه على السيرفر

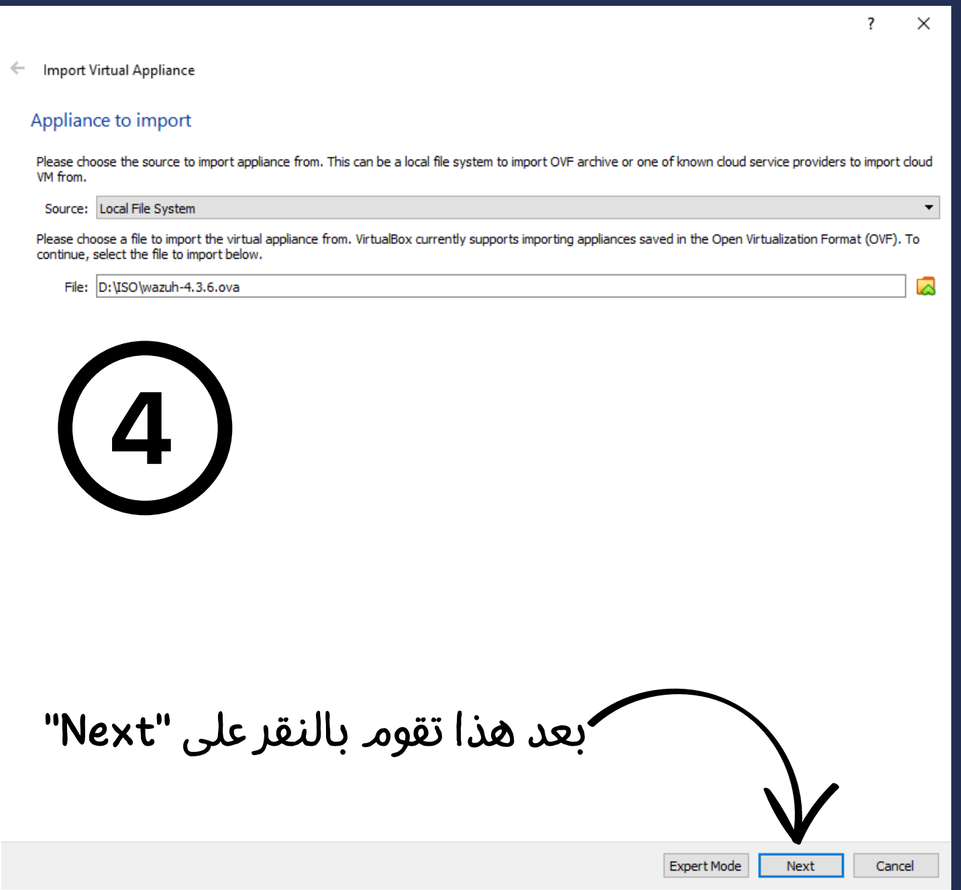


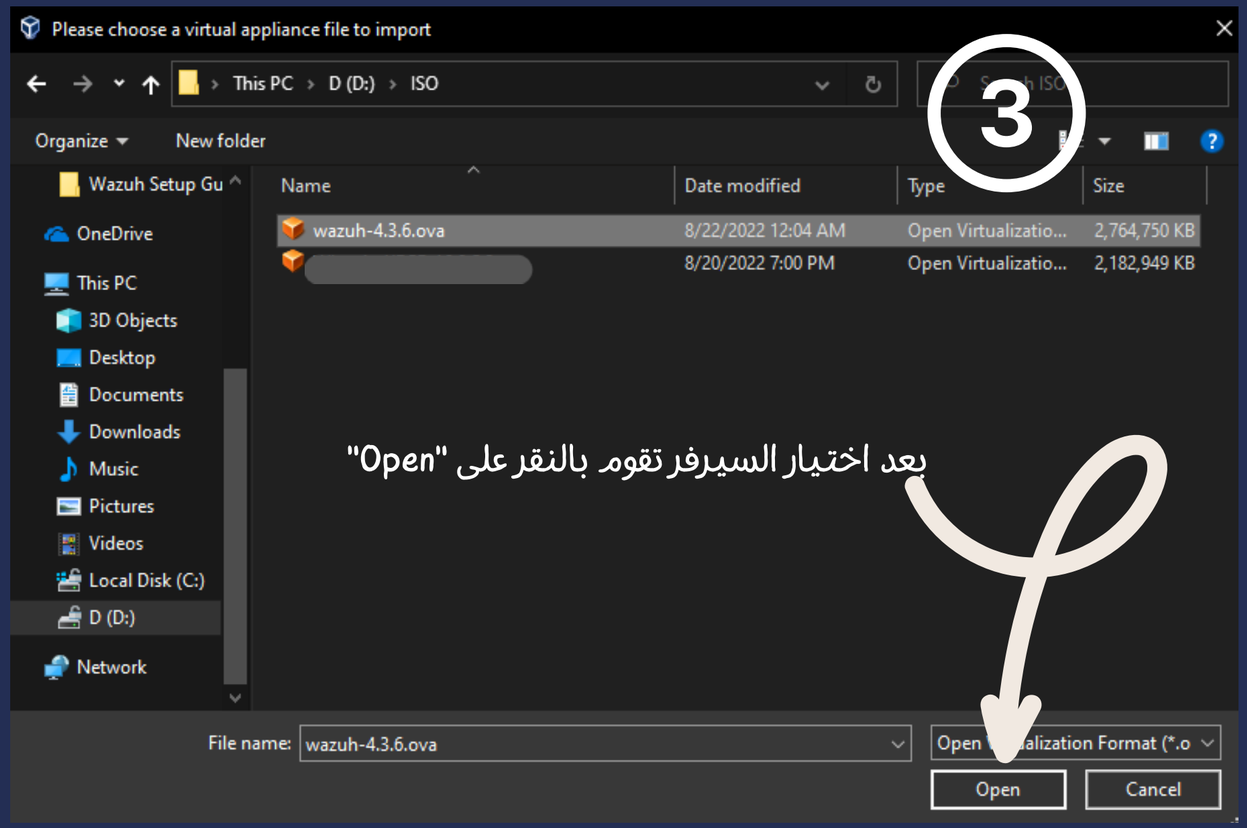
هنا يوضح الحد الادنى"Minimum" من حجم الرام والمعالج والاعداد الموصى به "Recommended" من حجم الرام والمعالج

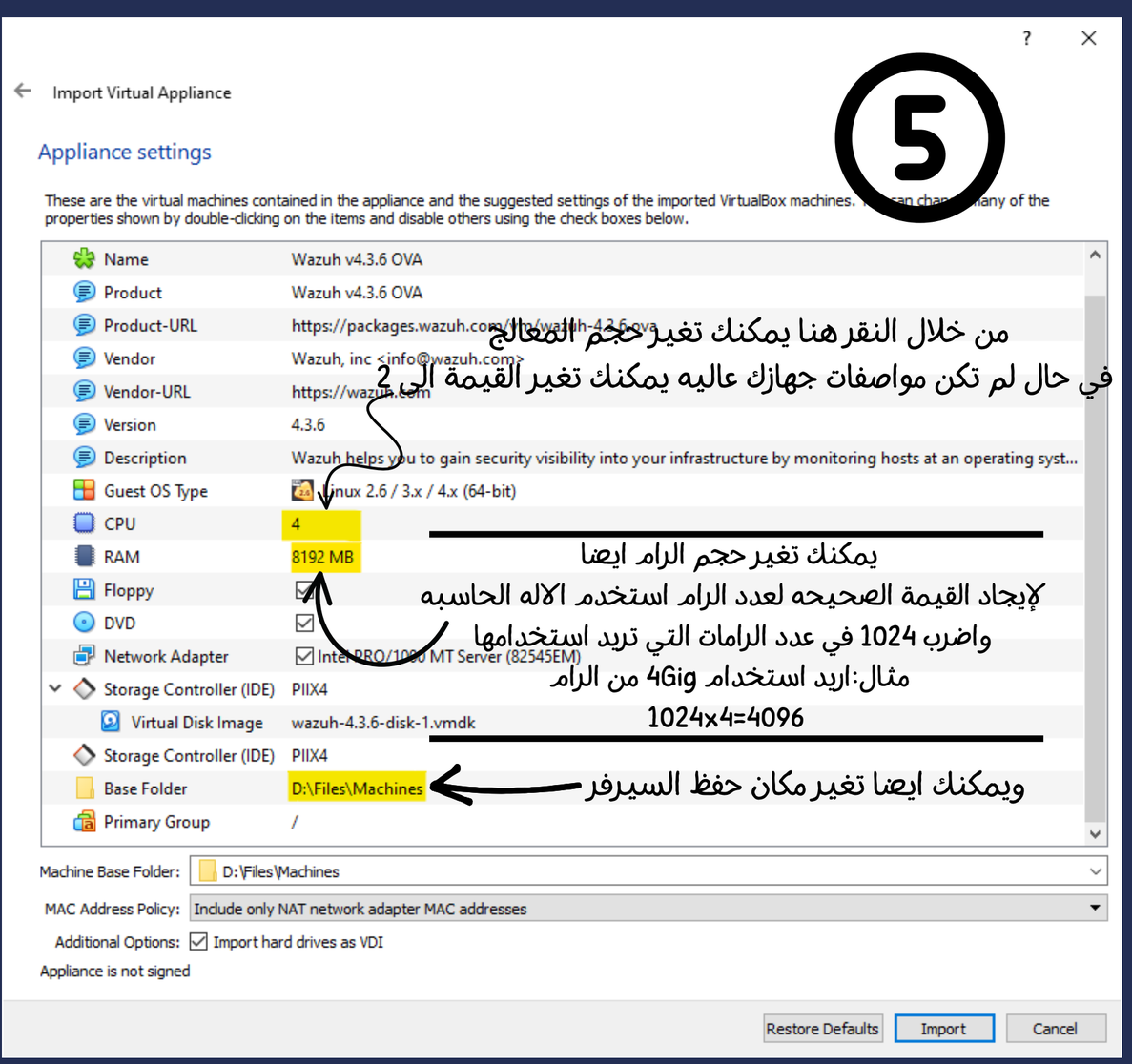


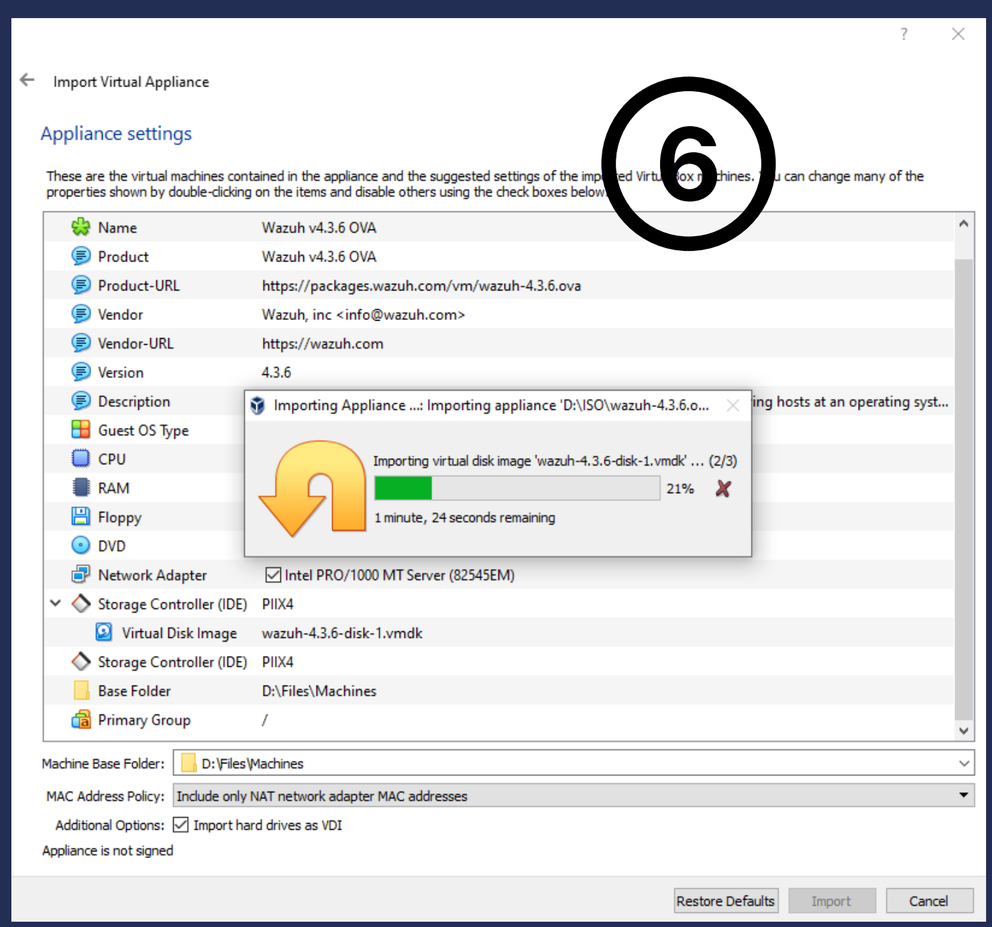


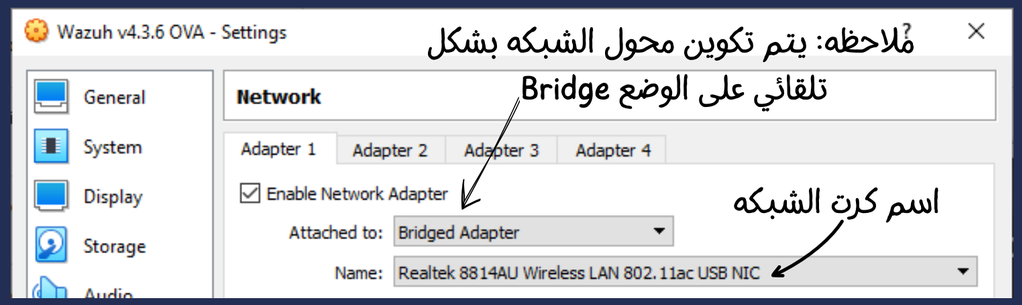
انقر هنا وسوف تنبثق لك نافذه وسوف تقوم بأختيار مكان السيرفر الذي تم تحميله مسبقا





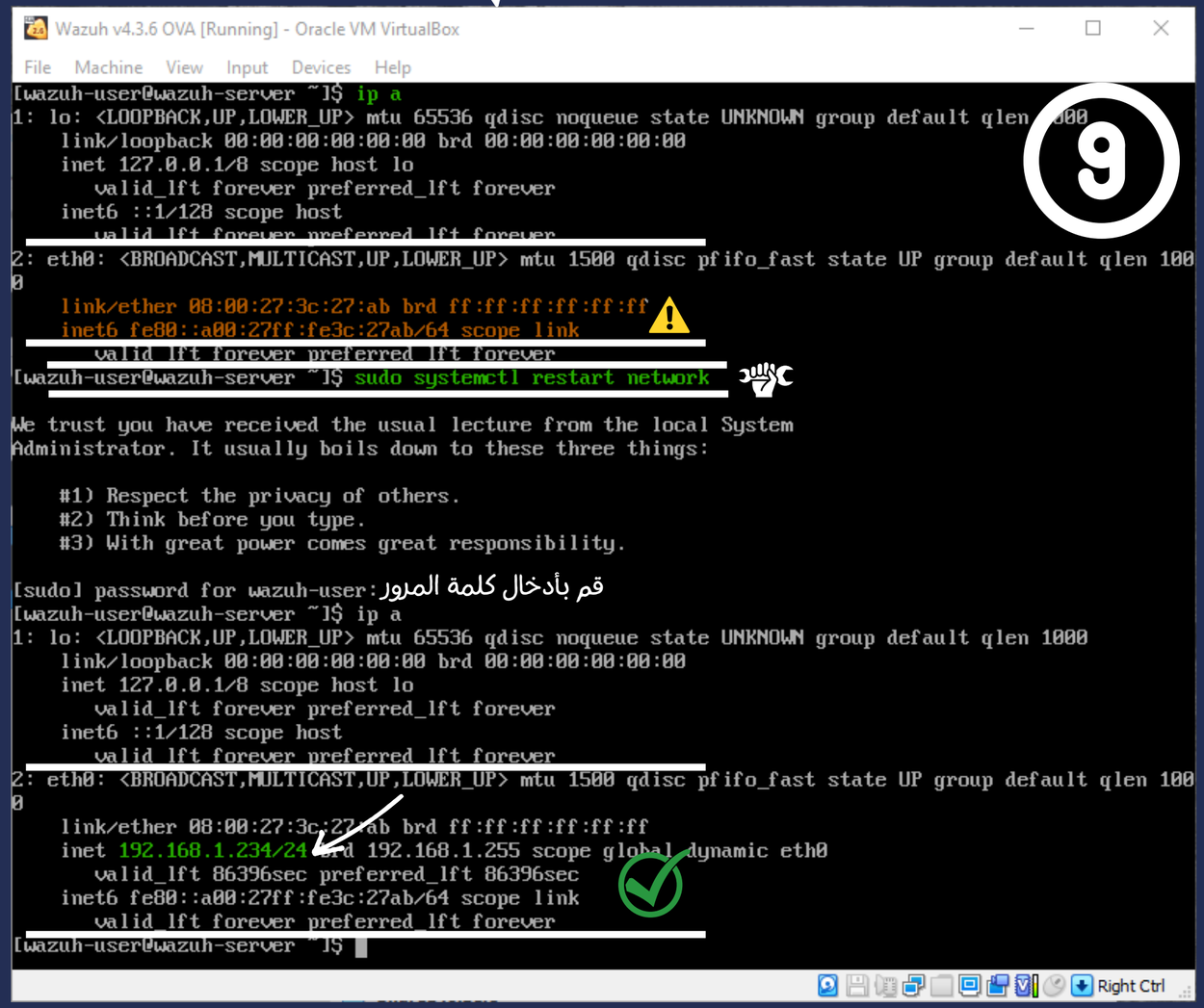

Import Virtual Appliance
Appliance settings
5
These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines.
properties shown by double-clicking on the items and disable others using the check boxes below.
Name Wazuh v4.3.6 OVA
Product Wazuh v4.3.6 OVA
Product-URL https://packages.wazuh.com/vm/wazuh-4.3.6.ova
Vendor Wazuh, inc <info@wazuh.com>
Vendor-URL https://wazuh.com
Version 4.3.6
Description Wazuh helps you to gain security visibility into your infrastructure by monitoring hosts at an operating syst...
Guest OS Type Linux 2.6 / 3.x / 4.x (64-bit)
CPU 4
RAM 8192 MB
Floppy
DVD
Network Adapter Intel PRO/1000 MT Server (82545EM)
Storage Controller (IDE) PIIX4
Virtual Disk Image wazuh-4.3.6-disk-1.vmdk
Storage Controller (IDE) PIIX4
Base Folder D:\Files\Machines
Primary Group /
Machine Base Folder: D:\Files\Machines
MAC Address Policy: Include only NAT network adapter MAC addresses
Additional Options: Import hard drives as VDI
Appliance is not signed
Restore Defaults
Import
Cancel
من خلال النقر هنا يمكنك تغير حجم المعالج
في حال لم تكن مواصفات جهازك عاليه يمكنك تغير القيمة الى 2
يمكنك تغير حجم الرام ايضا
لإيجاد القيمة الصحيحه لعدد الرام استخدم الاله الحاسبه
واضرب 1024 في عدد الرامات التي تريد استخدامها
مثال:اريد استخدام 4Gig من الرام
1024x4=4096
ويمكنك ايضا تغير مكان حفظ السيرفر

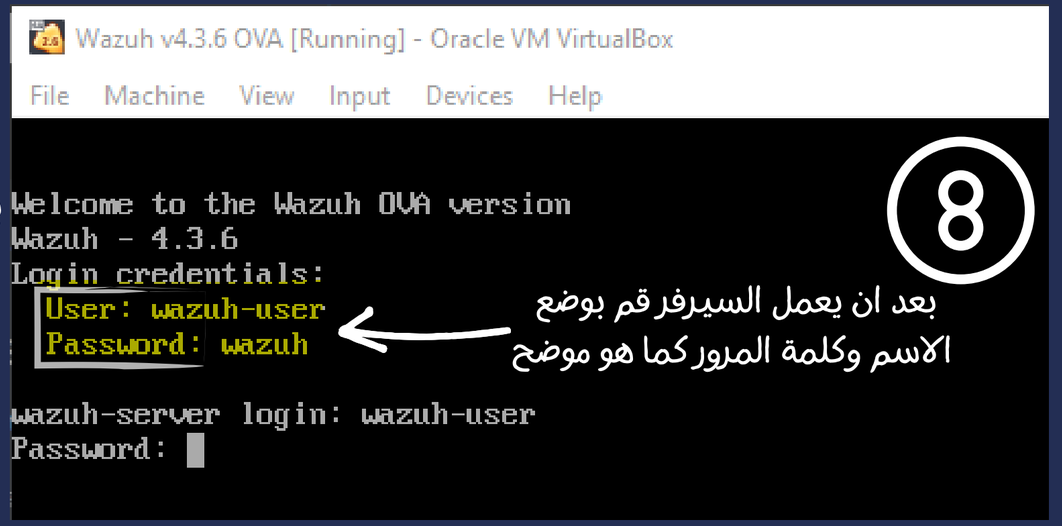

Import Virtual Appliance
Appliance settings
6
Name Wazuh v4.3.6 OVA
Product Wazuh v4.3.6 OVA
Product-URL https://packages.wazuh.com/vm/wazuh-4.3.6.ova
Vendor Wazuh, inc <info@wazuh.com>
Vendor-URL https://wazuh.com
Version 4.3.6
Description
Guest OS Type
CPU
RAM
Floppy
DVD
Network Adapter Intel PRO/1000 MT Server (82545EM)
Storage Controller (IDE) PIIX4
Virtual Disk Image wazuh-4.3.6-disk-1.vmdk
Storage Controller (IDE) PIIX4
Base Folder D:\Files\Machines
Primary Group /
Importing Appliance ...: Importing appliance 'D:\ISO\wazuh-4.3.6.o...
Importing virtual disk image 'wazuh-4.3.6-disk-1.vmdk' ... (2/3)
21%
1 minute, 24 seconds remaining
Machine Base Folder: D:\Files\Machines
MAC Address Policy: Include only NAT network adapter MAC addresses
Additional Options: Import hard drives as VDI
Appliance is not signed
Restore Defaults
Import
Cancel


Wazuh v4.3.6 OVA - Settings
General
System
Display
Storage
Audio
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Bridged Adapter
Name: Realtek 8814AU Wireless LAN 802.11ac USB NIC
ملاحظه: يتم تكوين محول الشبكه بشكل
تلقائي على الوضع Bridge
اسم كرت الشبكه

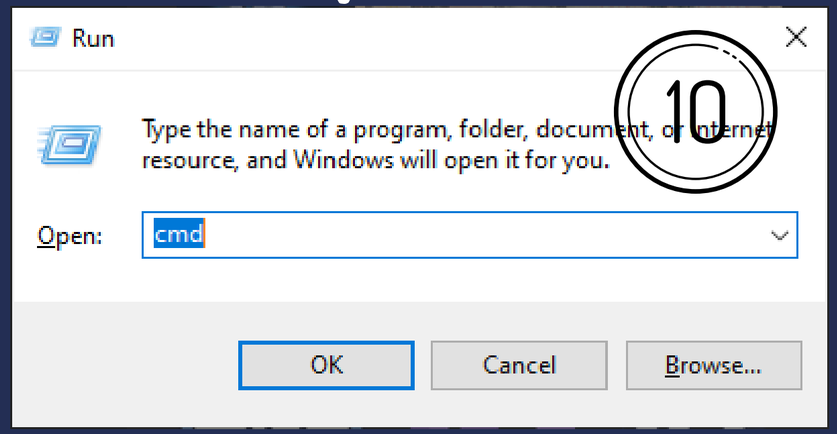

Oracle VM VirtualBox Manager
File Machine Help
Tools
New Settings Discard Start
Powered Off
Powered Off
Powered Off
Wazuh v4.3.6 OVA
Powered Off
General
Name: Wazuh v4.3.6 OVA
Operating System: Linux 2.6 / 3.x / 4.x (64-bit)
System
Base Memory: 8192 MB
Display
Video Memory: 16 MB
Graphics Controller: VBoxVGA
Preview
Wazuh v4.3.6 OVA
7
بعد ذلك قم بتسغيل السيرفر

لمعرفه عنوان السيرفر للدخول عليه من خلال متصفحك قم بكتابه الامر "ip a"
في حال لم يظهر لك اي عنوان كما هو موضح باللون البرتقالي قم بكتابه الأمر التالي
"sudo systemctl restart network"
بعد ذلك قم بكتابه كلمه المرور مره اخرى "wazuh" لمنح صلاحيه المسؤل من خلال الامر sudo

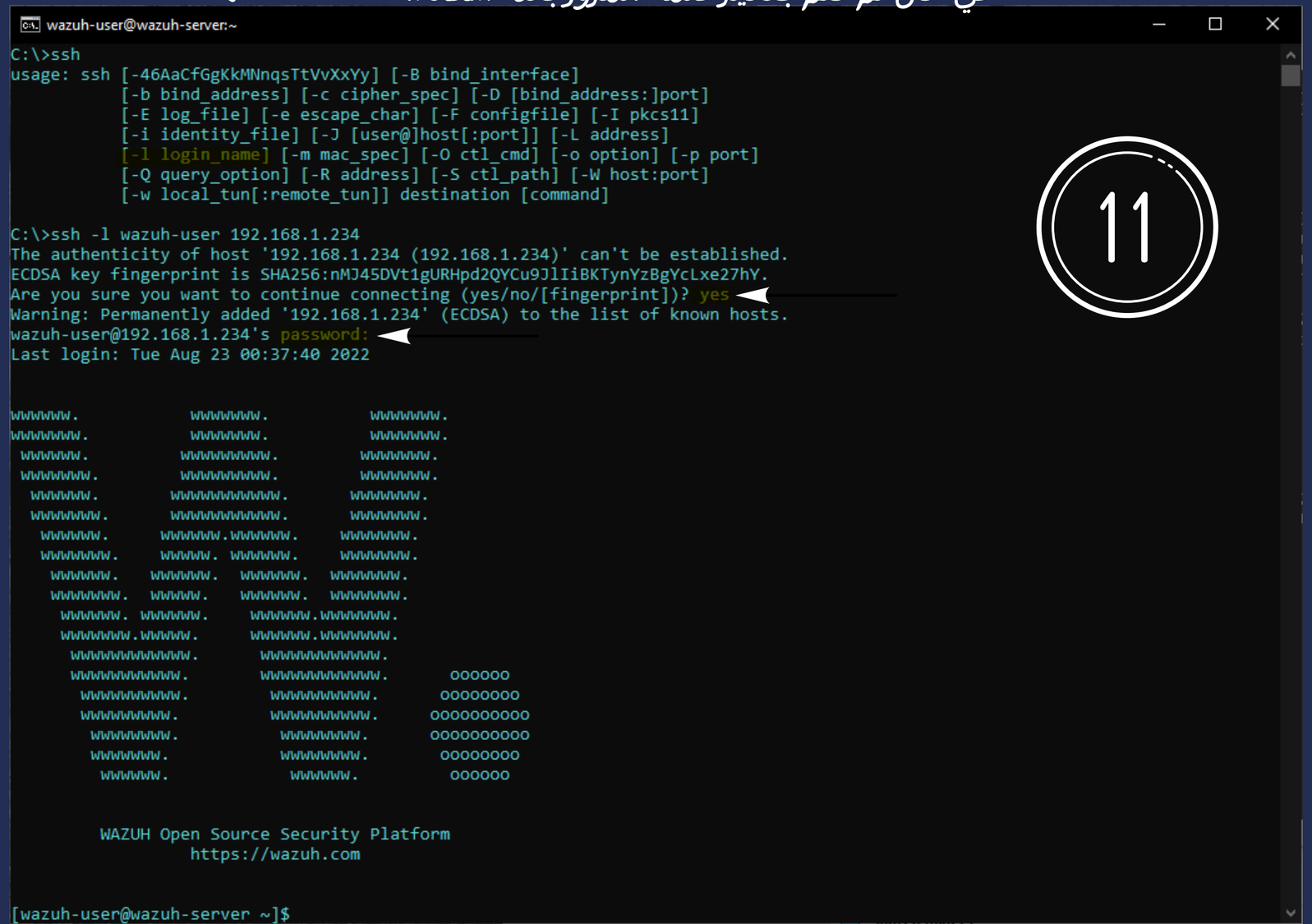




قم بتشغيل موجه الاوامر للاتصال بالسيرفر من خلال بروتوكول ssh لسهوله النسخ والصق لتشغيله من خلال الكيبورد "علامه الويندز + حرف R" بعد ذلك قم بكتابه cmd ثم "OK"



بعد ذلك قم بكتابه الامر
"ssh -l wazuh-user <ip address>"
اسم المستخدم بعد ذلك عنوان الايبي الخاص بالسيرفر
بعد ذلك اكتب 'yes' بعد ذلك سيطلب منك كلمه المرور الخاصه باليوزر
في حال لم تقم بتغير كلمة المرور بعد "wazuh"



الان سوف نقوم بتغير كلمة المرور الافتراضيه للمستخدم لحماية السيرفر
نقوم بكتابه الامر "sudo passwd wazh-user"
ملاحظه:الامر sudo في كل مره تكتبه للمره الاوله يطلب من كلمة المرور
الخاصه بالمستخدم بعد ذلك ينفذ لك الامر
ويمنحك مده محدده في حال لم تقم بكتابه الامر sudo سوف يطلب منك ادخال كلمة المرور مره اخرى
في المثال الموضح في الاسفل استخدمت الامر sudo لمرات عديده والمده الزمنيه بين كل امر لم تكن
طويله لذلك كما هو موضح لم يطلب ادخال كلمة المرور الخاصة بالمستخدم وانما تم تنفيذ الامر بشكل
مباشر

ملاحظه: عند كتابه كلمة المرور كنوع من الامان لاتظهر كلمة المرور ولا تظهر عدد الخانات

```
[wazuh-user@wazuh-server ~]$ sudo passwd wazuh-user
Changing password for user wazuh-user.
New password: ادخل كلمة المرور الجديده
Retype new password: اعد ادخال كلمة المرور
passwd: all authentication tokens updated successfully.
[wazuh-user@wazuh-server ~]$
```

ملاحظه: تم وضع كلمة مرور افتراضيه للمستخدم Root
وهي "Wazuh" ويجب تغيرها لتأمين السيرفر

```
[root@wazuh-server ~]# sudo passwd root
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@wazuh-server ~]#
```

12

ملاحظه يوجد اكثر من اسم مستخدم وكلمة مرور
افتراضيه تستطيع تسجيل الدخول بها
سيتم تغيرها لاحقا للتأمين لوحة التحكم

للدخول لواجه الويب والوصول الى لوحة التحكم من خلال
المتصفح قم بكتابه رقم الايبي الخاص بالسيرفر
"https://<ip address>"
كما هو موضح في الصوره رقم 13
لمعرفه كيف معرفه الايبي في الاسفل صورة رقم 14

Access the Wazuh dashboard

Shortly after starting the VM, the Wazuh dashboard can be accessed from the web interface by using the following credentials:

```
URL: https://<wazuh_server_ip>
user: admin
password: admin
```

كلمة المرور واسم المستخدم
للدخول من خلال واجة الويب

14

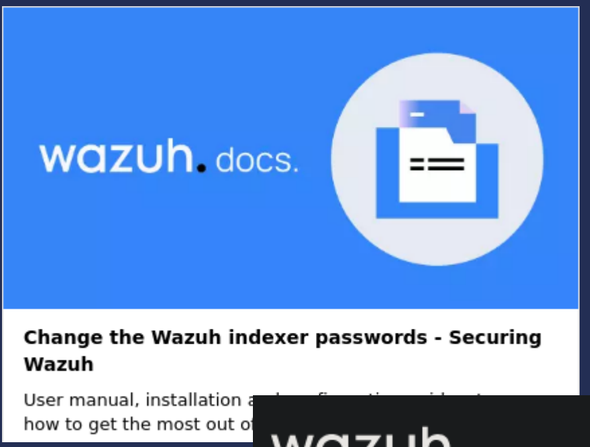
You can find `<wazuh_server_ip>` by typing the following command in the VM:

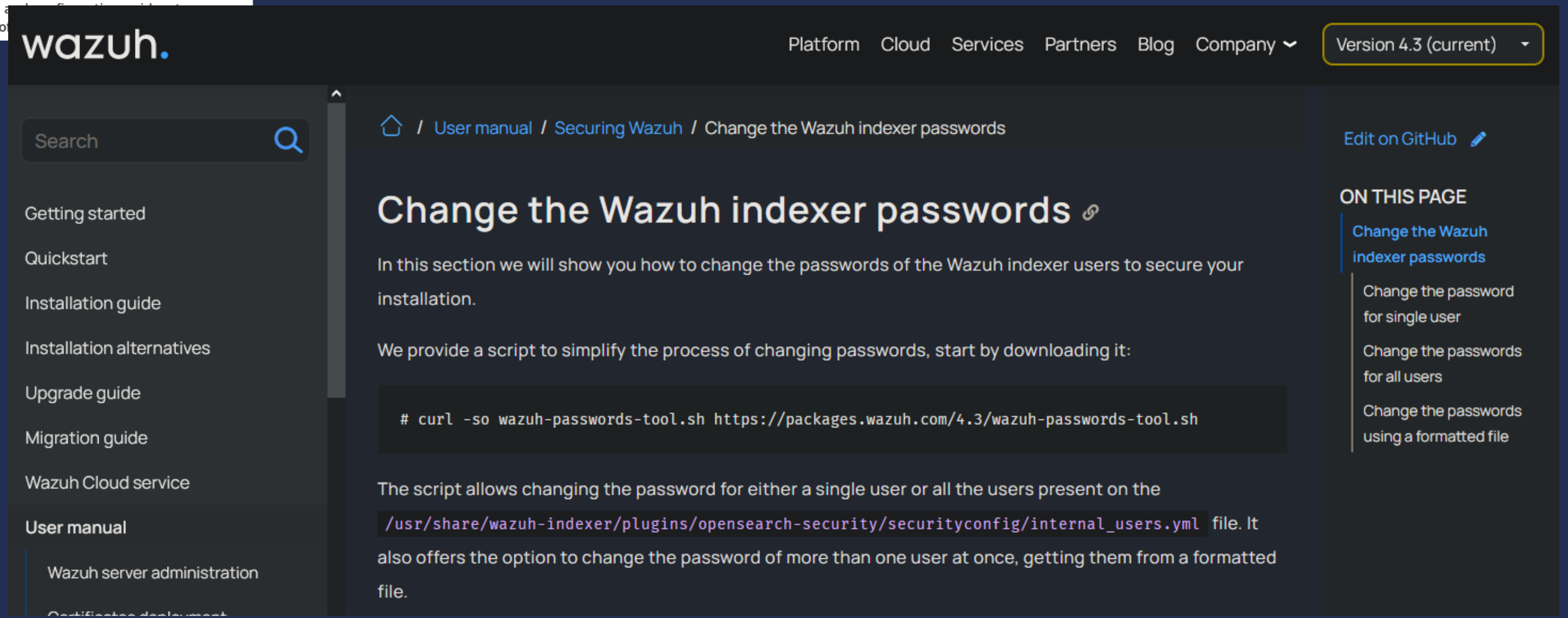
```
ip a
```

لمعرفه عنوان الايبي الخاص بالسيرفر

الان سنقوم بتغير كلمات المرور المستخدمين الخاصه بالدخول للوحة التحكم لتأمينها
من خلال موجه الاوامر 'CMD' بأستخدام بروتوكول "SSH" وذلك لسهوله النسخ واللصق
يمكنك معرفه كيفيه الاتصال من خلال النظر للصورتين في الاعلى
رقم 10,11

سنقوم بأستخدام سكربت يساعدنا في عملية تغير كلمات المرور ويمكن من خلاله
تغير جميع كلمات المرور الخاصه بلوحة التحكم دفعة واحده وانشاء كلمات مرور
عشوائيه او تغير كلمات المرور بشكل محدد





سنقوم بتحميل السكربت من خلال الامر التالي

curl -so wazuh-passwords-tool.sh https://packages.wazuh.com/4.3/wazuh-passwords-tool.sh

ثم نقوم بكتابه الامر "chmod +x wazh-passwords-tool.sh"

لتغير جميع كلمات مرور المستخدمين وانشاء كلمات مرور عشوائيه قم بأستخدام الامر

"sudo ./wazuh-passwords-tool.sh -a"

لتغير كلمة المرور لمستخدم واحد فقط

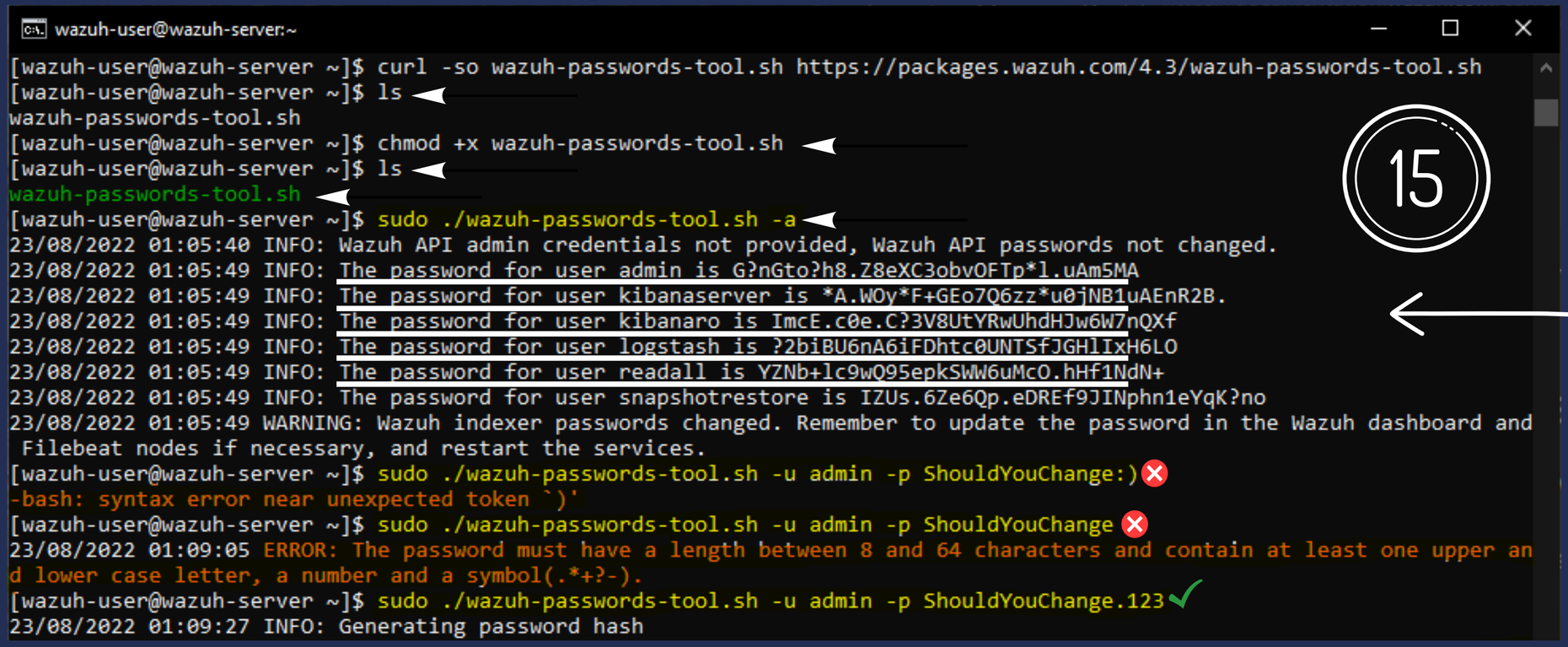
"sudo ./wazuh-passwords-tool.sh -u اسم المستخدم -p كلمه المرور الجديده"

ملاحظه: في حال اردت تغير كلمة مرور بشكل محدد يرجى مراعاة انه لا يسمح

بأستخدام جميع الرموز وانما يسمح بالرموز التاليه فقط . * ? + -

ويجب ان تكون كلمه المرور بين 8 خانات الى 64 خانه ويجب ان تكون مكونه من احرف صغيره وكبيره ورموز وارقام

وتم تضليل الاخطاء باللون البرتقالي للتوضيح



15

كما هو موضح تمت طباعة كل اسم ويقابله كلمه المرور التي تم انشائها بشكل عشوائي

لتغير جميع كلمات المرور بشكل عشوائي وطباعتها في ملف قم بكتابه الامر التالي
"sudo ./wazuh-passwords-tool.sh -a -gf اسم الملف الذي تريد انشائه واضافة كلمات السر داخله

```
[wazuh-user@wazuh-server ~]$ sudo ./wazuh-passwords-tool.sh -a -gf passwords.txt
24/08/2022 22:30:58 INFO: Wazuh API admin credentials not provided, Wazuh API passwords not changed.
24/08/2022 22:31:10 INFO: The password for user admin is w.DMSZuDptjNCT49R9bmegrm5W9AMV5+
24/08/2022 22:31:10 INFO: The password for user kibanaserver is L0?xD0G5kxdW.2FIjiTfiID+7D+LIH7y
24/08/2022 22:31:10 INFO: The password for user kibanaro is Rok7PWRZW2Pc?EWsleYFj9oZyL3RflgW
24/08/2022 22:31:10 INFO: The password for user logstash is t0HWFCHcb5*aQP*d5y?EaiEAAMAjshkY
24/08/2022 22:31:10 INFO: The password for user readall is BBoS7ZWGgbTqfKmyh?ucSKt4JcHdK.SQ
24/08/2022 22:31:10 INFO: The password for user snapshotrestore is xjZLGb0rMYEs.1i2HPn3.wV5jvhgbo9X
24/08/2022 22:31:10 WARNING: Wazuh indexer passwords changed. Remember to update the password in the Wazuh dashboard and
 Filebeat nodes if necessary, and restart the services.
[wazuh-user@wazuh-server ~]$ ls
passwords.txt  wazuh-passwords-tool.sh
[wazuh-user@wazuh-server ~]$ cat passwords.txt
cat: passwords.txt: Permission denied
[wazuh-user@wazuh-server ~]$ sudo cat passwords.txt
# Admin user for the web user interface and Wazuh indexer. Use this user to log in to Wazuh dashboard
  indexer_username: 'admin'
  indexer_password: 'w.DMSZuDptjNCT49R9bmegrm5W9AMV5+'

# Wazuh dashboard user for establishing the connection with Wazuh indexer
  indexer_username: 'kibanaserver'
  indexer_password: 'L0?xD0G5kxdW.2FIjiTfiID+7D+LIH7y'
```

16

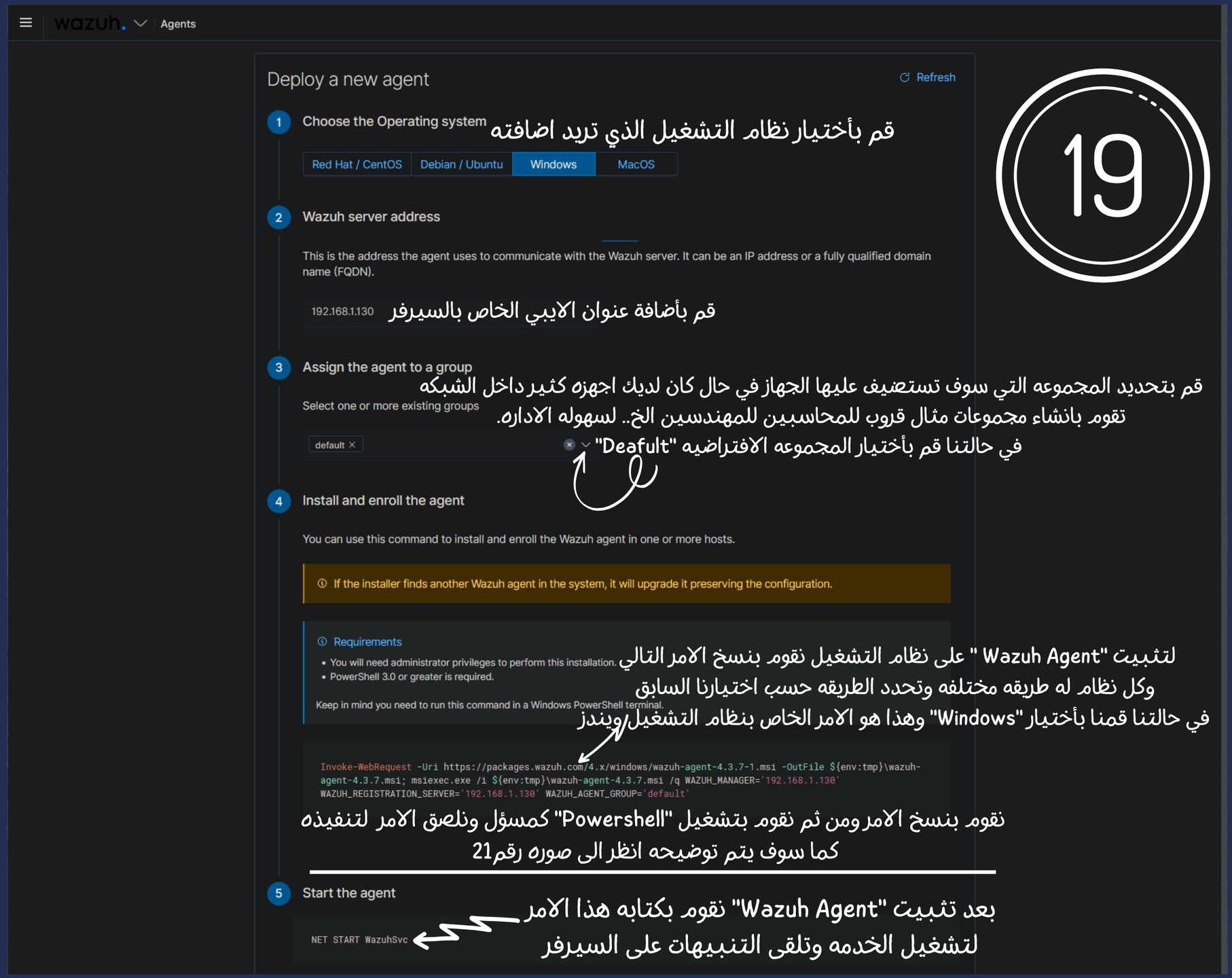
لطباعة الملف الذي تم انشائه ويحتوي
على كلمات المرور و اسماء المستخدمين

تتم اضافة كلمات المرور واسم المستخدم داخل الملف بالطريقة التاليه

17

يمكنك نسخ اسم المستخدم وكلمه المرور من خلال الملف الذي تم انشائه
وتسجيل الدخول الى لوحة التحكم من خلال المتصفح كما تم الشرح مسبقا في الاعلى في الصورة رقم 13

بعد تسجيل الدخول ستظهر لوحة التحكم بالشكل التالي
نقوم بالنقر على "Add agent" لأستضافه نظام تشغيل على السيرفر



قم بأختيار نظام التشغيل الذي تريد اضافته

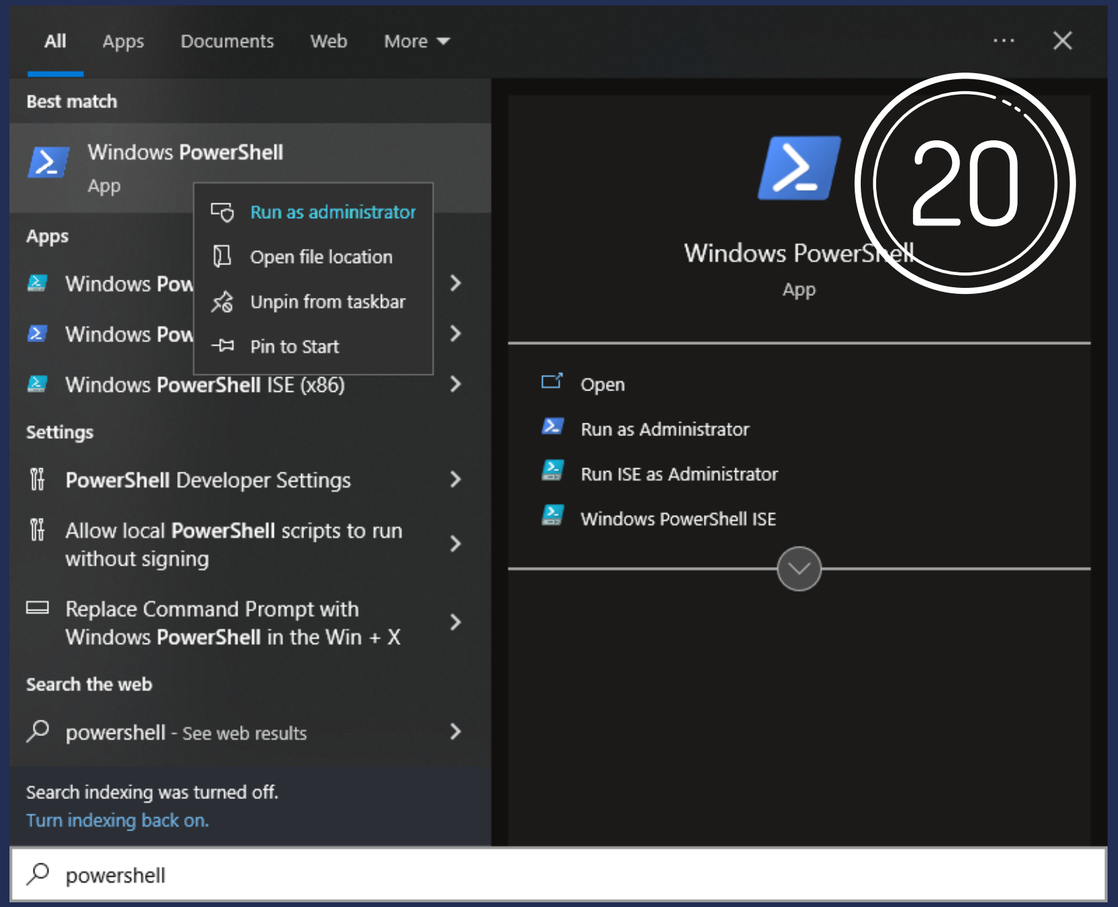
قم بأضافة عنوان الايبي الخاص بالسيرفر

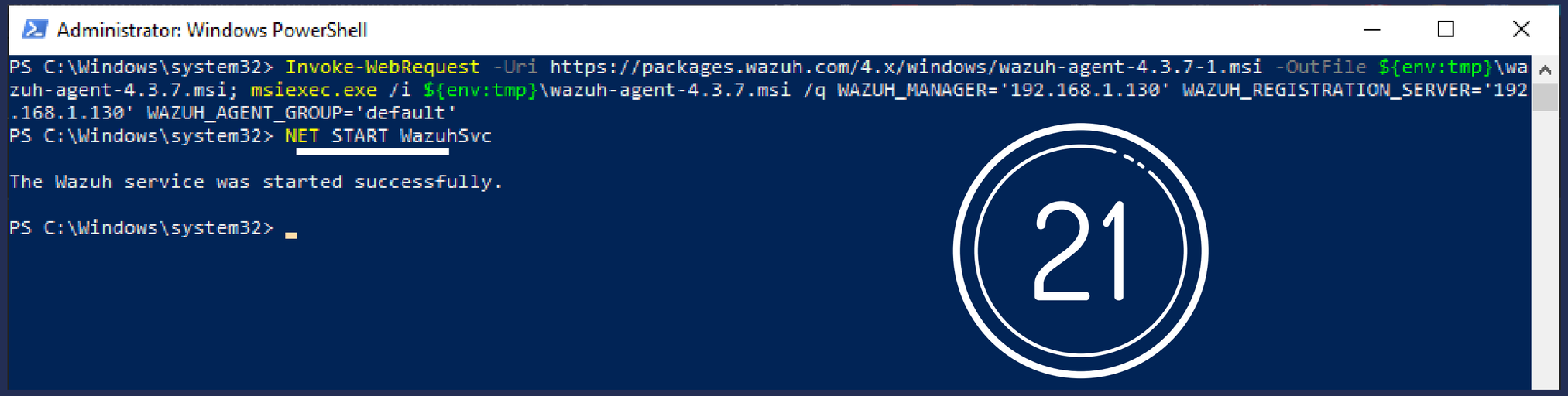
قم بتحديد المجموعه التي سوف تستضيف عليها الجهاز في حال كان لديك اجهزه كثير داخل الشبكه
تقوم بانشاء مجموعات مثال قروب للمحاسبين للمهندسين الخ.. لسهوله الاداره.
في حالتنا قم بأختيار المجموعه الافتراضيه "Deafult"

لتثبيت "Wazuh Agent " على نظام التشغيل نقوم بنسخ الامر التالي
وكل نظام له طريقه مختلفه وتحدد الطريقه حسب اختيارنا السابق
في حالتنا قمنا بأختيار "Windows" وهذا هو الامر الخاص بنظام التشغيل ويندز

نقوم بنسخ الامر ومن ثم نقوم بتشغيل "Powershell" كمسؤل ونلصق الامر لتنفيذه
كما سوف يتم توضيحه انظر الى صوره رقم21

بعد تثبيت "Wazuh Agent" نقوم بكتابه هذا الامر
لتشغيل الخدمه وتلقى التنبيهات على السيرفر


All
Apps
Documents
Web
More
Best match
Windows PowerShell
App
Run as administrator
Open file location
Unpin from taskbar
Pin to Start
Apps
Windows Pow
Windows Pow
Windows PowerShell ISE (x86)
Settings
PowerShell Developer Settings
Allow local PowerShell scripts to run without signing
Replace Command Prompt with Windows PowerShell in the Win + X
Search the web
powershell - See web results
Search indexing was turned off.
Turn indexing back on.
Windows PowerShell
App
Open
Run as Administrator
Run ISE as Administrator
Windows PowerShell ISE
powershell


Administrator: Windows PowerShell
PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.3.7-1.msi -OutFile ${env:tmp}\wazuh-agent-4.3.7.msi; msiexec.exe /i ${env:tmp}\wazuh-agent-4.3.7.msi /q WAZUH_MANAGER='192.168.1.130' WAZUH_REGISTRATION_SERVER='192.168.1.130' WAZUH_AGENT_GROUP='default'
PS C:\Windows\system32> NET START WazuhSvc
The Wazuh service was started successfully.
PS C:\Windows\system32>
21

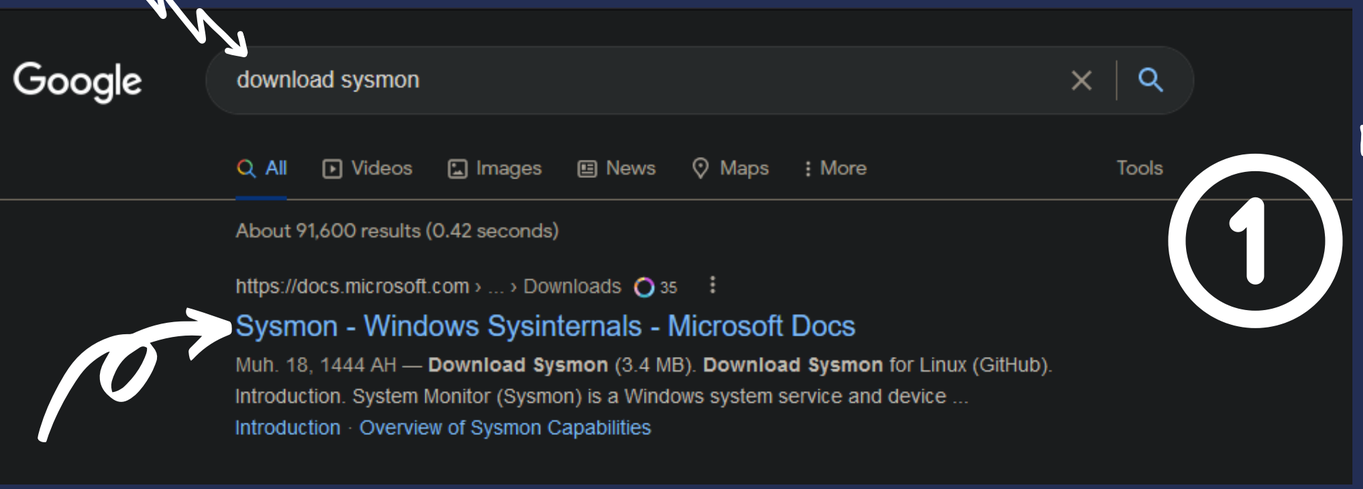
قم بالرجوع الى الصفحه الرئيسيه في لوحة التحكم وقم بتحديث الصفحه وسوف يظهر لك انه تم اضافة جهاز الى السيرفر

لتحديث السيرفر نقوم بكتابه الامر 'sudo su' اولا ومن ثم كلمه مرور المستخدم للوصول للمستخد المسؤل لتتمكن من تحديث موارد النظام بعد ذلك نقوم بكتابه الامر التالي 'yum update'

22

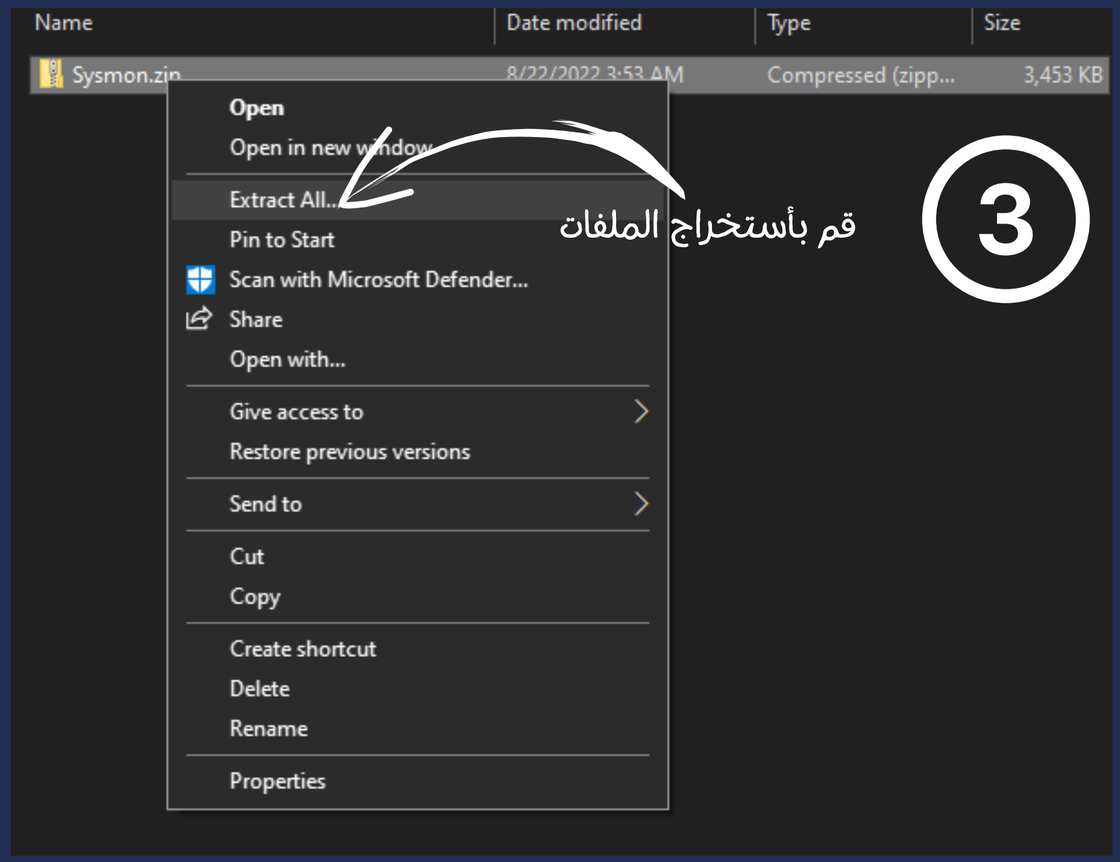
23

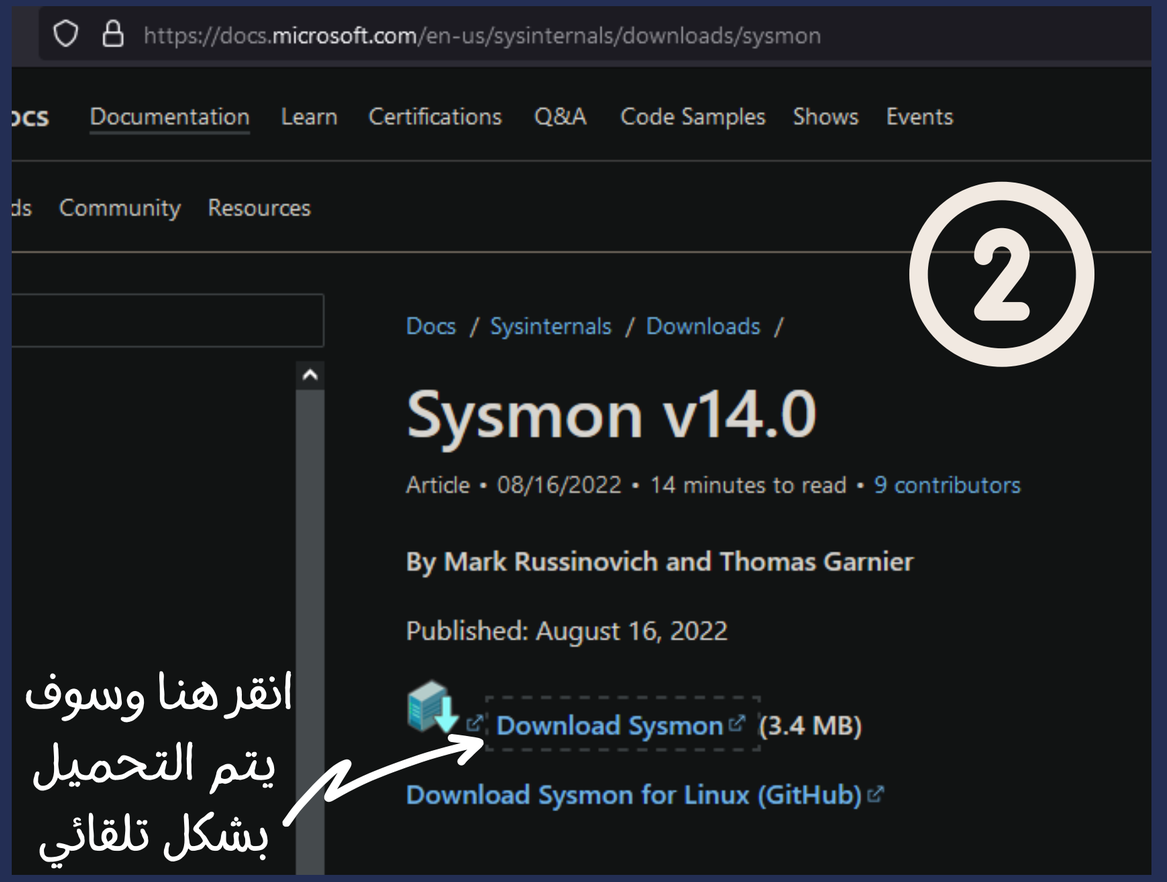
شرح أعداد وتثبيت sysmon



Sysmon

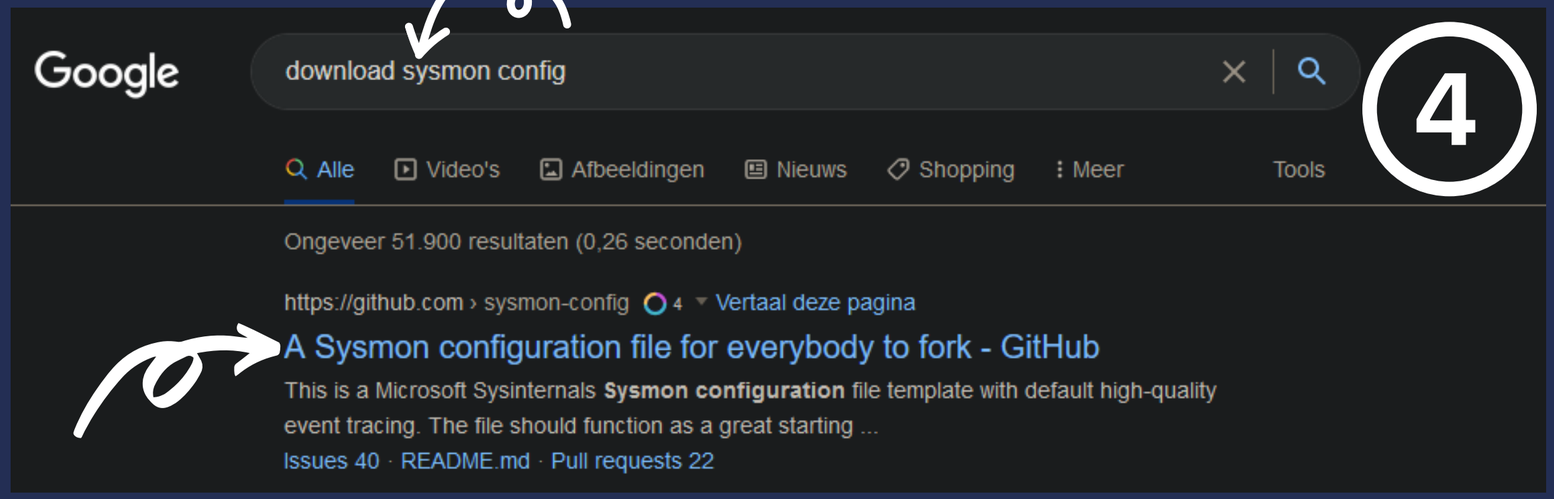
هي اداة من سلسة اداوات Sysinternals وهي الان تابعه لشركة Microsoft
تقوم الاداة بتسجيل وتحليل نشاط النظام لتحديد الانشطه الضاره
او الغير طبيعيه ومن خلال تثبيت هذه الاداه وارسال مخرجاتها
الى سيرفر Wazuh فسوف نزيد من قدرة تحليل السجل "Logs" لدينا
وبالتالي زيادة احتمالية اكتشاف التهديدات .

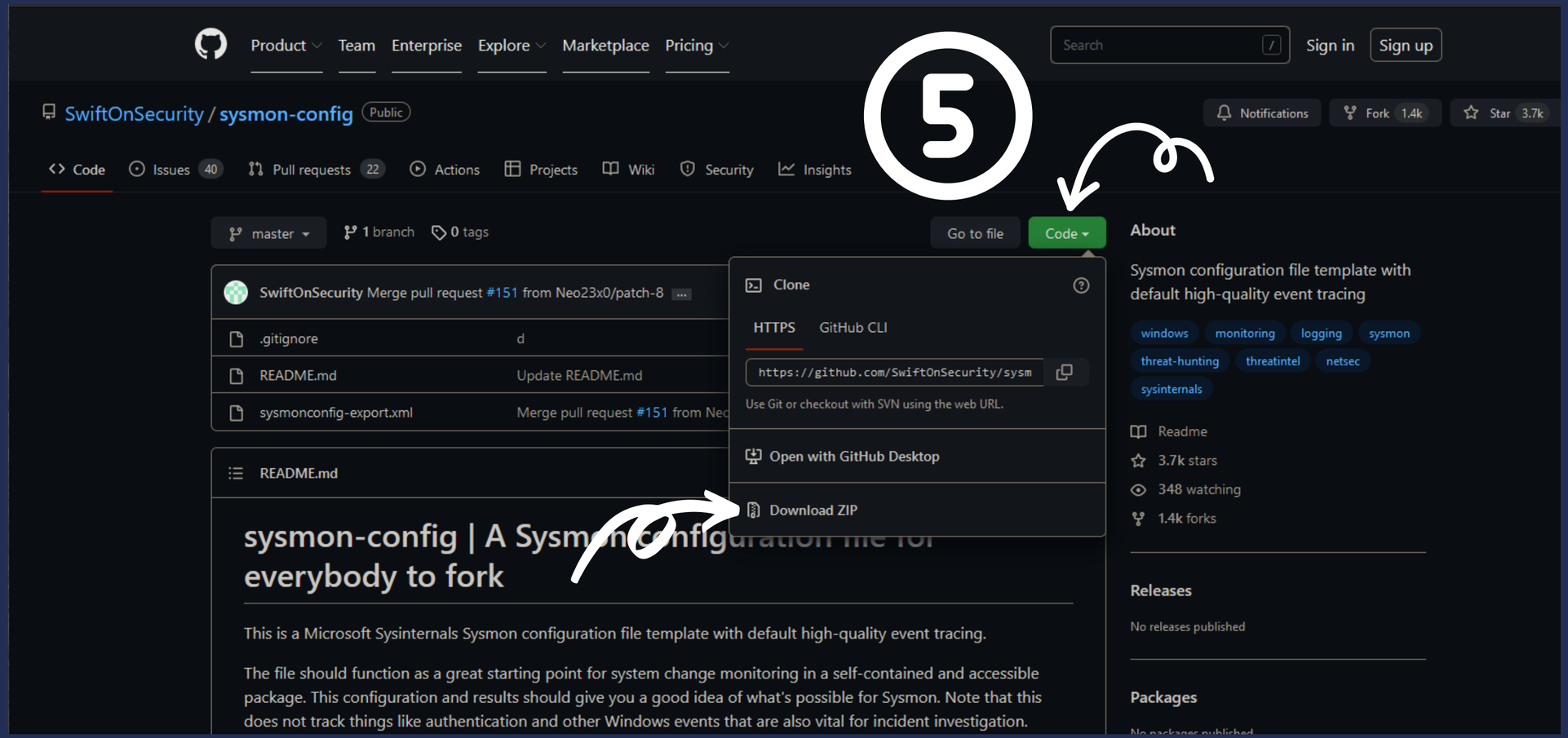




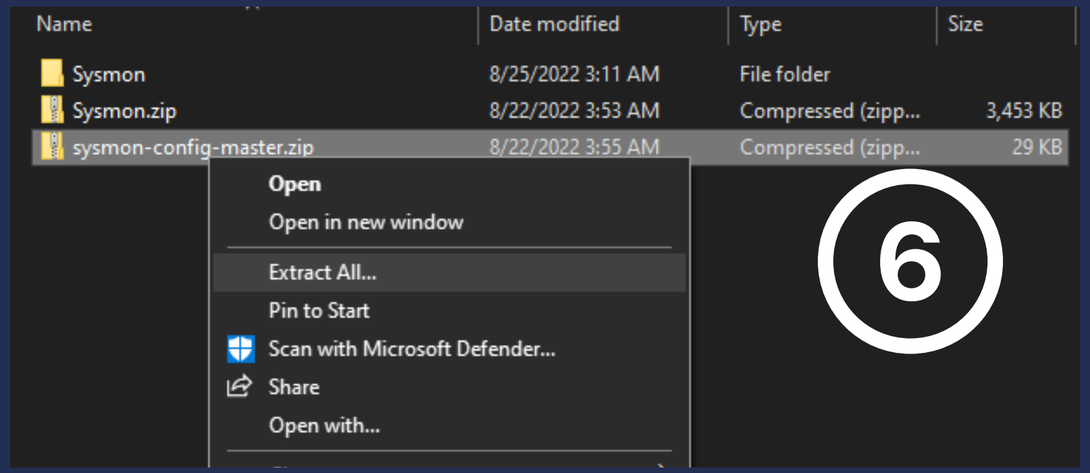
Sysmon Config

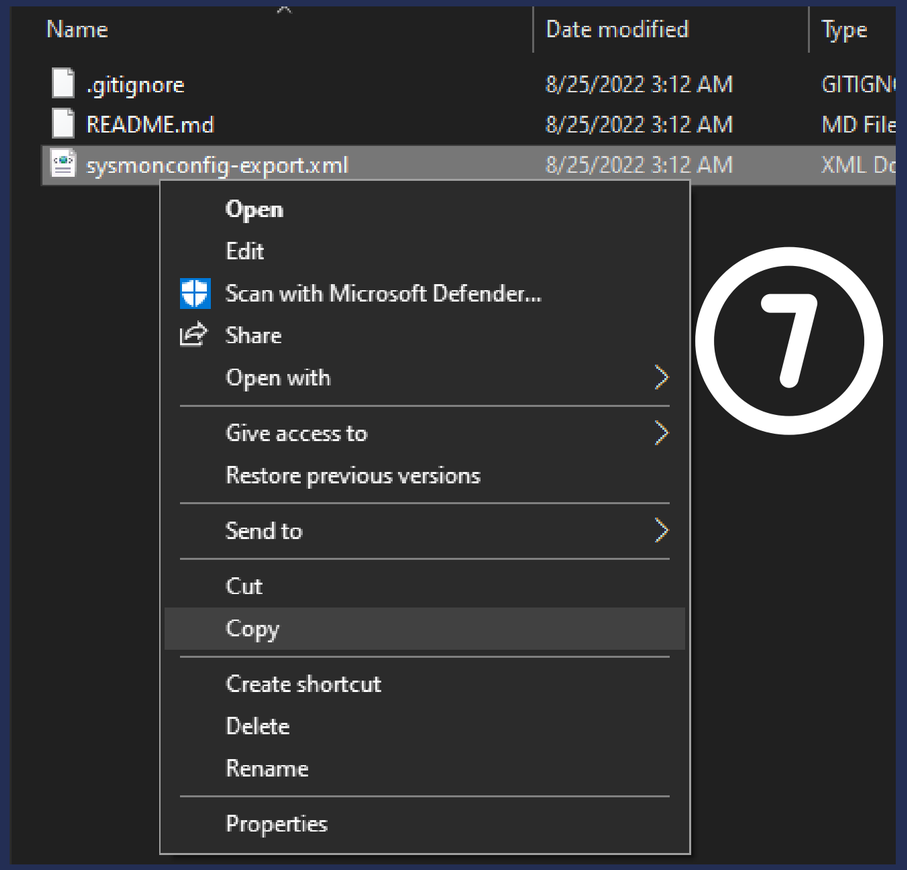
وهو ملف بصيغة xml يتحكم في كيفية عمل sysmon
ويمكنك انشاء ملف تكوين خاص بك بحيث تتحكم فيما يتم تسجيله او استبعاده في حالتنا سوف نقوم بتحميل ملف جاهز

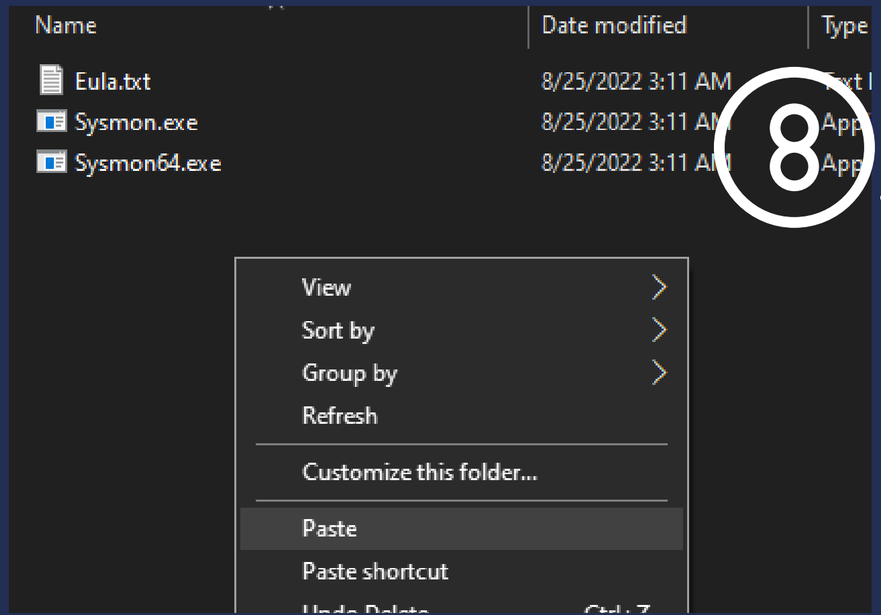




بعد ذلك قم بأستخراج الملفات ونسخ الملف
"sysmonconfig-export.xml"
كما هو موضح في الصورة رقم 7



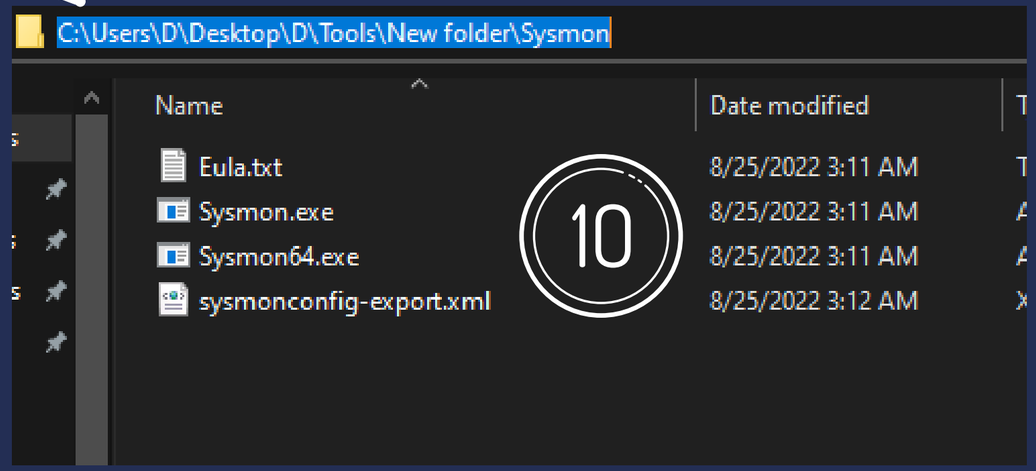


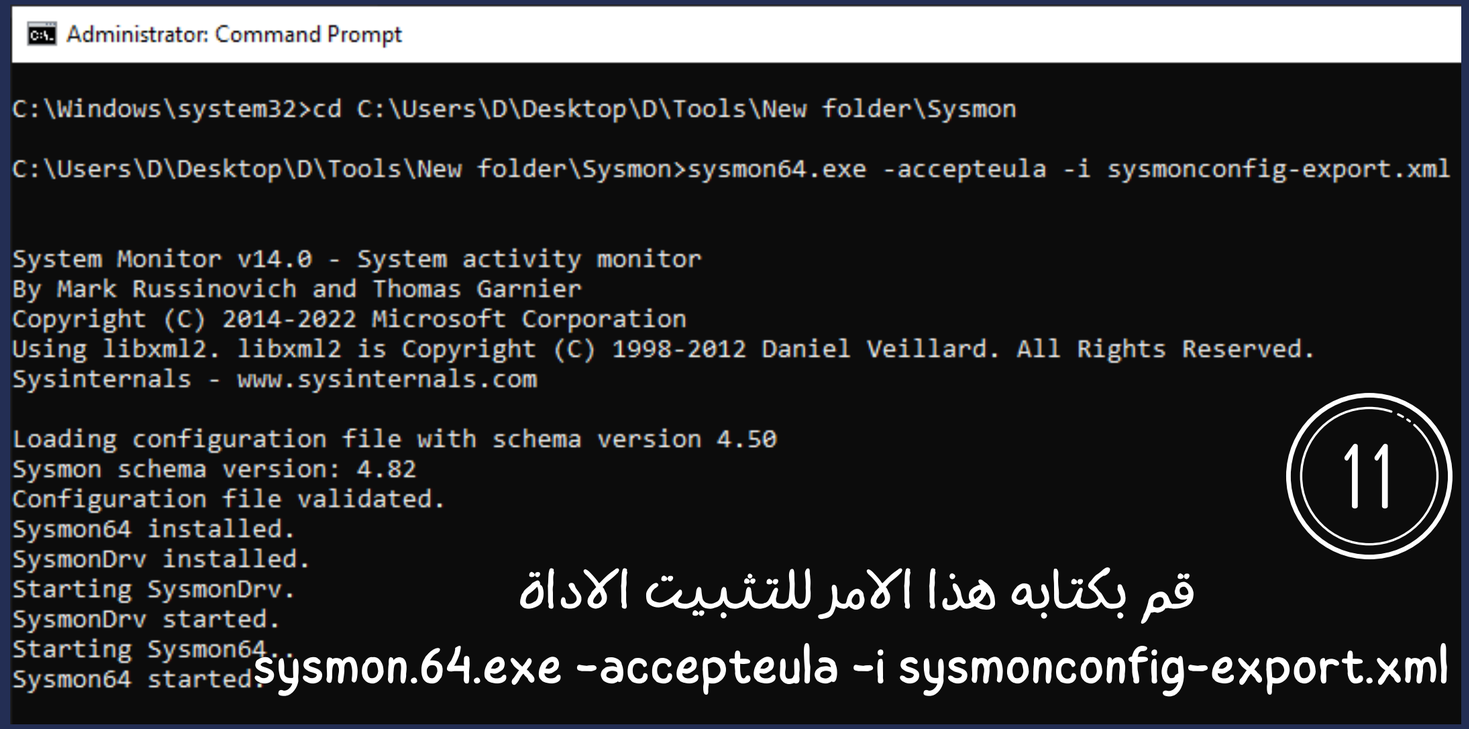


بعد ذلك قم بلصق الملف الذي تم نسخه
الى المجلد الذي يحتوي على اداة sysmon
كما هو موضح في الصورة رقم 8

قم بتشغيل موجه الاوامر "CMD" كمسؤل

قم بنسخ مسار الملف الذي يحتوي
اداة sysmon وملف التكوين sysmonconfig



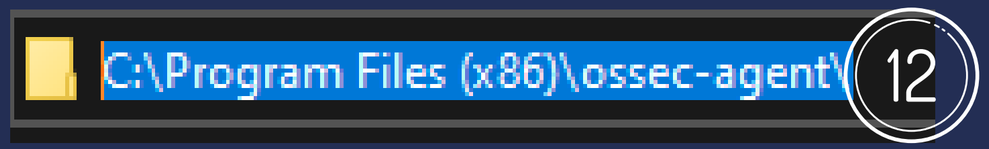


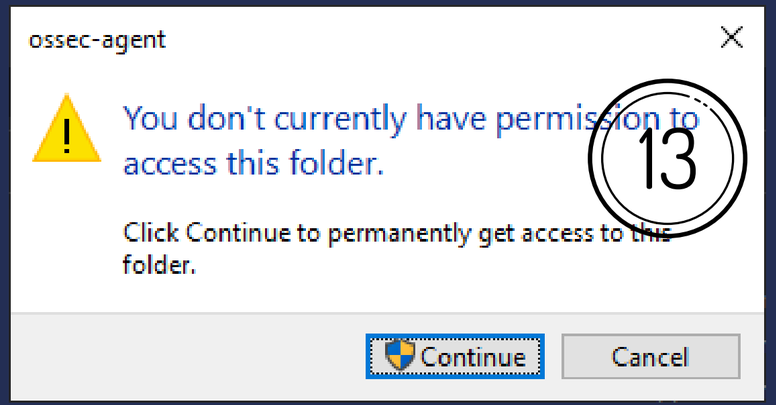
قم بكتابه هذا الامر للتثبيت الاداة

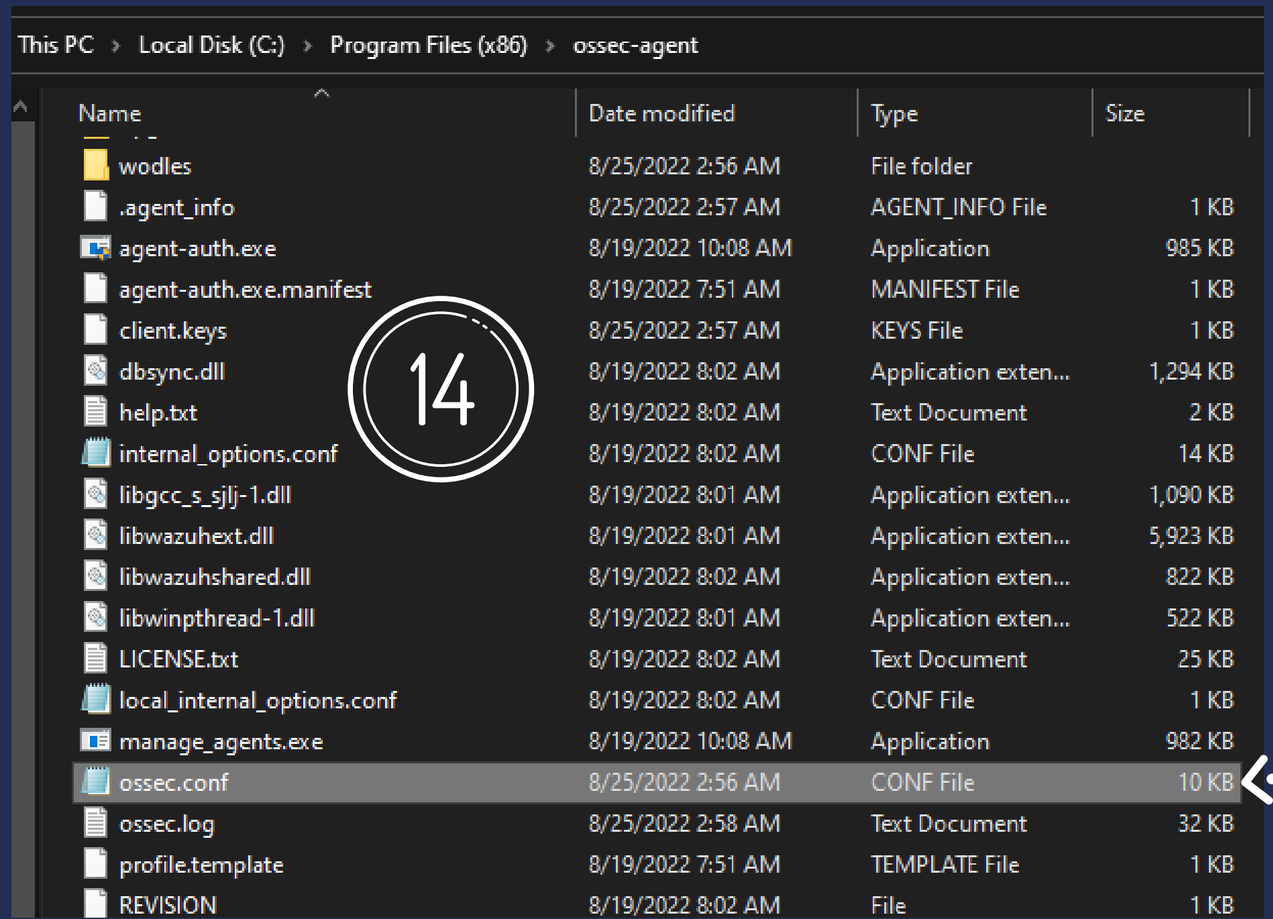
sysmon.64.exe -accepteula -i sysmonconfig-export.xml

الان سوف نقوم باعداد عميل wazuh لاستقبال ماسوف يتم تسجيله من خلال sysmon

قم بالذهاب الى هذا المسار وهو المكان الذي تم تثبيت Wazuh agent داخله
"القرص c \ البرامج والملفات (86x) \ اسم الملف الذي يحتويه wazuh agent"
قد يختلف المسار بأختلاف مكان التثبيت حاول الوصول الى الملف ossec-agent
وسوف تضهر نافذه كما هو موضح في الصوره رقم 13 انقر على متابعه "Continue"





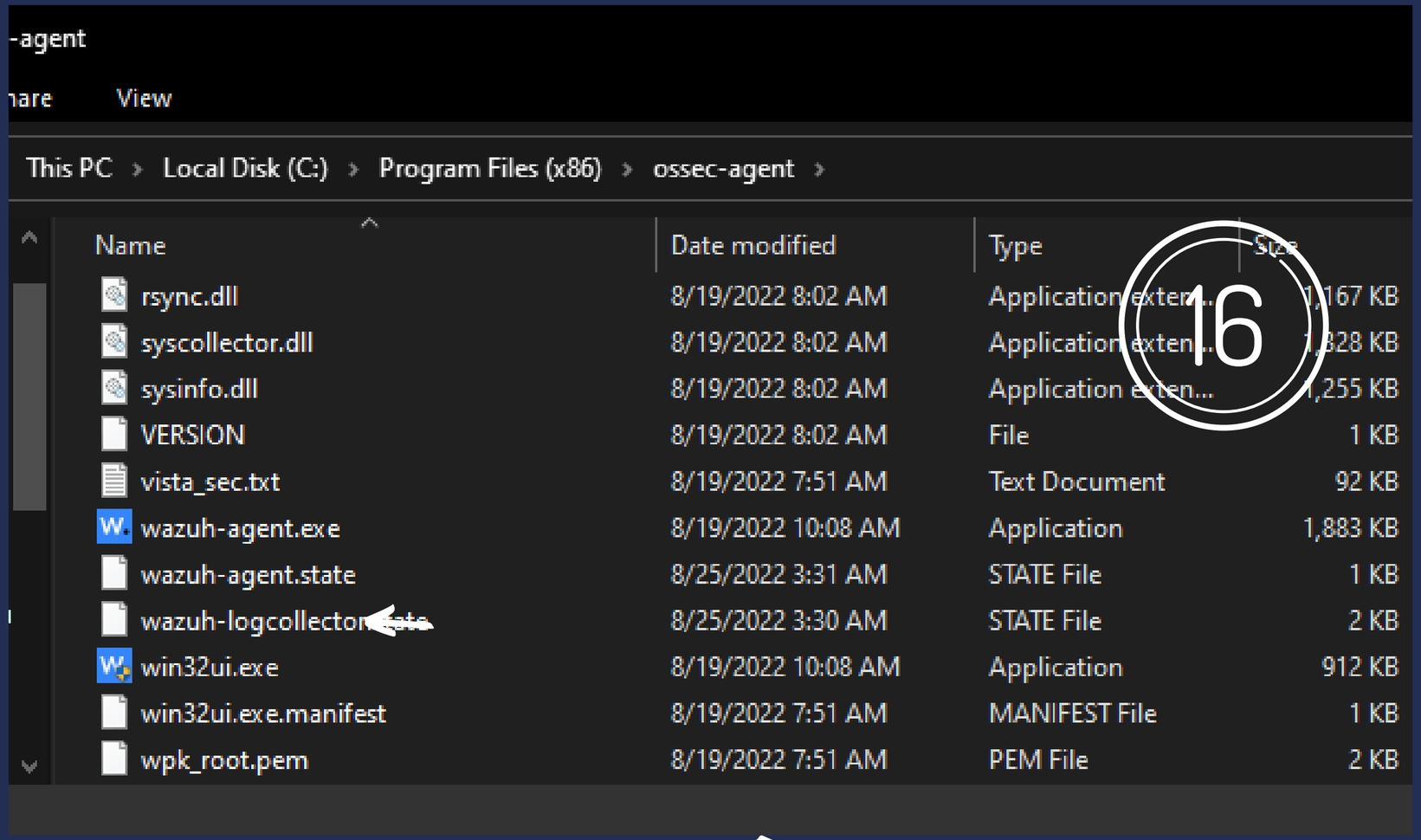


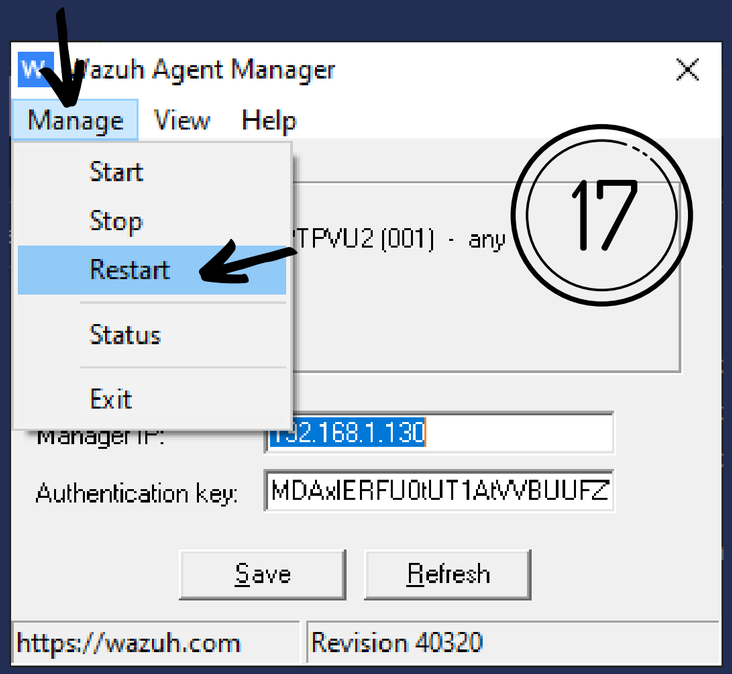
بعد ذلك ابحث عن ملف بأسم "ossec.conf" وقم بفتحه
بأستخدام المفكره او اي برنامج يستخدم لتحرير النصوص

بعد الوصول الى الملف كما هو موضح في الصوره رقم 14
قم بأضافة مايلي مع مراعاة مكان الاضافة

‹localfile›
location›Microsoft-Windows-›
‹Sysmon/Operational‹/location
‹log_format›eventchannel‹/log_format›
‹localfile/›

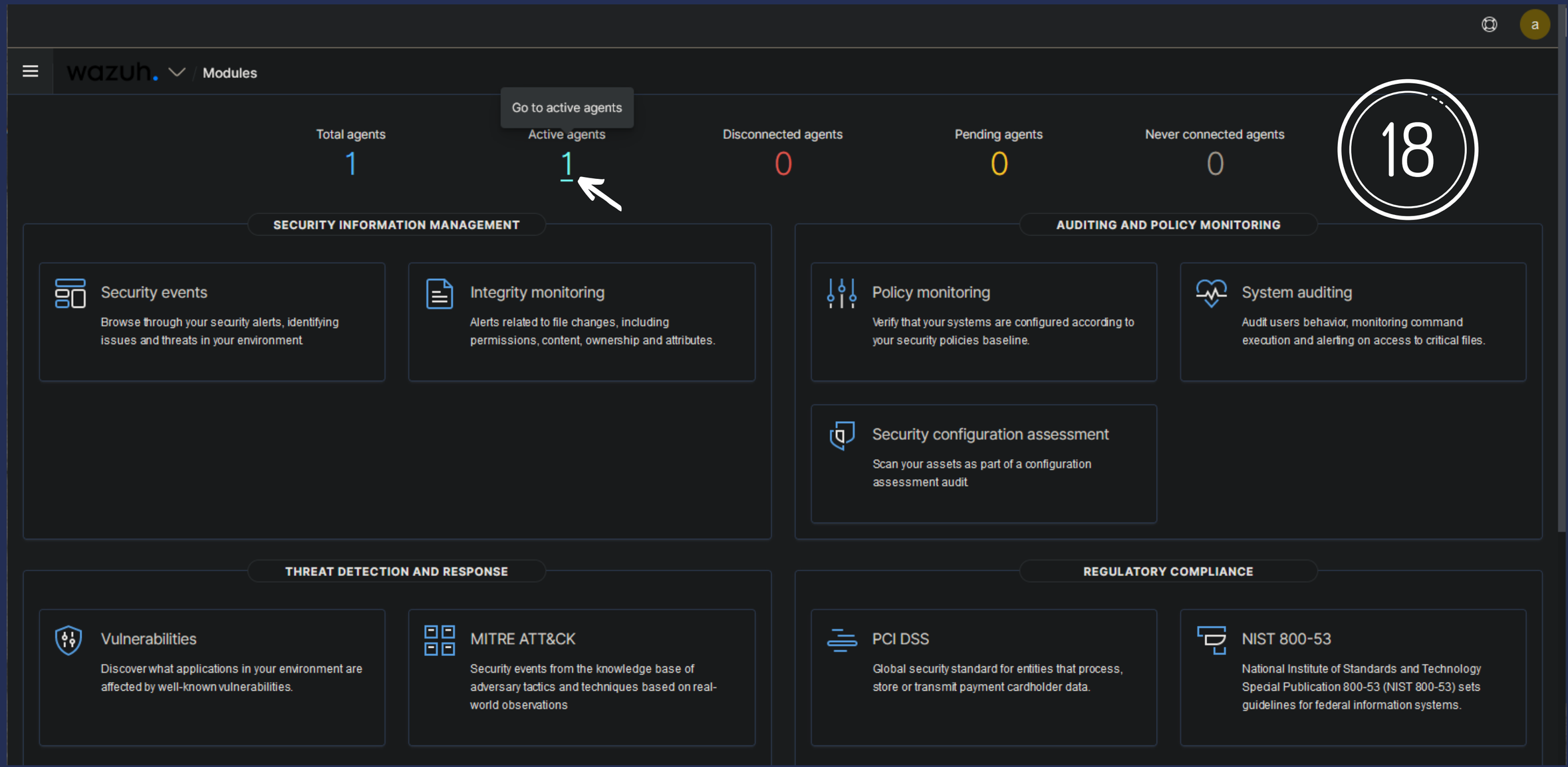
بعد ذلك نقوم بالرجوع للملف الذي يحتوي Wazuh agent
كما تم توضيحه سابقا في الصوره رقم 12

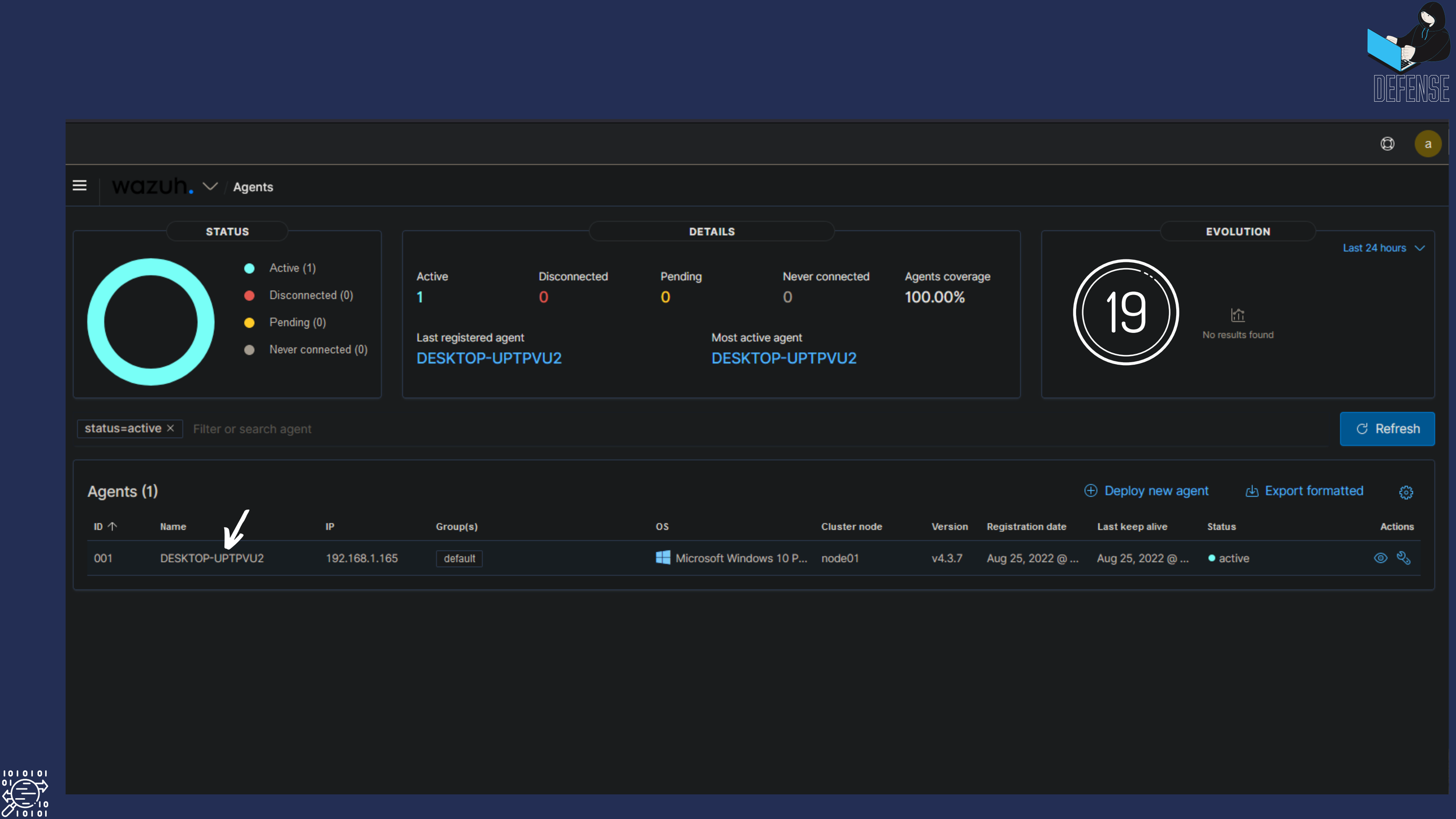




بعد ذلك نقوم بتشغيل 'Win32ui.exe'
ونقوم بعمل اعاده تشغيل لـ Wazuh Agent كما هو موضح
في الصورة رقم 17

قم بالروجوع للوحة التحكم الخاصه بسيرفر wazuh من خلال
المتصفح ومن ثم العملاء النشطين واختار الجهاز المستضاف
كما هو موضح صوره رقم 19 لترى التنبيهات والخ..




wazuh.
Agents
STATUS
Active (1)
Disconnected (0)
Pending (0)
Never connected (0)
DETAILS
Active
1
Disconnected
0
Pending
0
Never connected
0
Agents coverage
100.00%
Last registered agent
DESKTOP-UPTPVU2
Most active agent
DESKTOP-UPTPVU2
EVOLUTION
Last 24 hours
19
No results found
status=active
Filter or search agent
Refresh
Agents (1)
Deploy new agent
Export formatted
ID
Name
IP
Group(s)
OS
Cluster node
Version
Registration date
Last keep alive
Status
Actions
001
DESKTOP-UPTPVU2
192.168.1.165
default
Microsoft Windows 10 P...
node01
v4.3.7
Aug 25, 2022 @ ...
Aug 25, 2022 @ ...
active

اكتشف واستمتع

wazuh. / Agents / DESKTOP-UPTPVU2

DESKTOP-UPTP... | Security events | Integrity monitoring | SCA | Vulnerabilities | MITRE ATT&CK | More... | Inventory data | Stats | Configuration

ID	Status	IP	Version	Groups	Operating system	Cluster node	Registration date	Last keep alive
001	active	192.168.1.165	Wazuh v4.3.7	default	Microsoft Windows 10 Pr...	node01	Aug 25, 2022 @ 02:57:24.000	Aug 25, 2022 @ 03:35:46.000

Last 24 hours

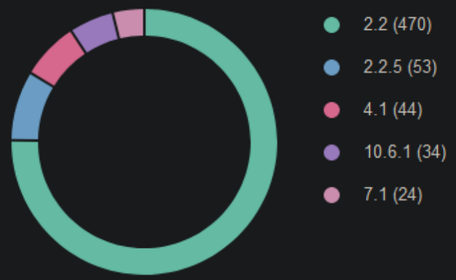
MITRE

Top Tactics

Defense Evasion	17
Persistence	17
Privilege Escalation	17
Initial Access	15
Impact	4

Compliance

PCI DSS



- 2.2 (470)
- 2.2.5 (53)
- 4.1 (44)
- 10.6.1 (34)
- 7.1 (24)

FIM: Recent events

Time	Path	Action	Rule description	Rule Level	Rule Id
No recent events					

ملاحضه:ليس بالضروره ان تكون جميع التنبيهات
دليل على وجود نشاط ضار

Events count evolution

SCA: Last scan

Benchmark for Windows audit | sca_win_audit

This document provides a way of ensuring the security of the Windows systems.

Pass	Fail	Total checks	Score
22	10	71	68%

Start time: Aug 25, 2022 @ 03:32:52.000 | Duration: < 1s