ZenSec

Master Active Directory Offensive Security

EXCLUSIVE GUIDE TO LAB CREATION

Set up your own offensive & defensive security virtual lab

www.zensec.org

CONTENTS

01
Authors & Introduction

Authors

Mateusz Jarzabek

I work as a Senior Offensive Security professional in EY's internal Purple Team, where I combine offensive and defensive techniques to help protect the firm.

I run zensec.org, a blog dedicated to helping others master Active Directory Offensive Security in a structured and practical way.

After struggling to connect the dots across scattered learning resources, I created ZenSec to provide clarity and structure to this complex topic.

Kacper Madej

I'm an aspiring cybersecurity practitioner. I hold OSCP certification, as well as CCNA, CompTIA Security+ (SY0-701), and SBT Blue Team Level 1.

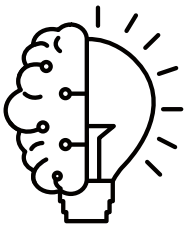
After graduating from a technical high school specializing in IT, I've been focused on developing both my networking and security skills through hands-on experience.

I enjoy building labs, testing real-world scenarios, and continuously challenging myself to grow.

My goal is to find a job in cybersecuirty and become a well-rounded security professional by combining offensive and defensive knowledge in practical, impactful ways.

Introduction

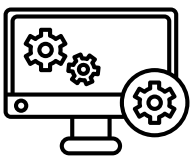
There are four things you need to consider when setting up your own offensive & deffensive cybersecurity lab. Whether your are setting it up at home or professionally.



01 Ideas, mission and objectives

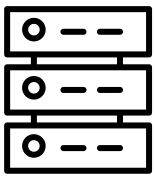
Creating a structured and versatile cybersecurity lab is one of the most effective ways to build practical skills and tackle real-world challenges.
Over the years, we've learned that the best labs are not only technically capable but also adaptable to a wide range of scenarios. That's exactly what the lab we are going to set up is designed to deliver.

From our experience, we know how cybersecurity filed can be overhelming and that's why this guide takes a structured approach, breaking down each step of the setup process. By the end, you'll not only have a functional lab but also the confidence to expand and adapt it as your skills grow and use cases multiply.



02 Virtualization platform

Choosing the right virtualization platform is important - it makes your work easier and can even determine the success of your lab.
In this guide, we will be using the latest version of VMware Workstation Pro, which has been available for free since November 2024. Instructions for installing it are provided later in the guide.



03 Machines and networking

Setting up the right virtual machines and configuring their networking is essential for creating a lab that is both functional and realistic. In this guide, we'll walk you through the configuration of four key machines: Ubuntu Server, Windows Server 2022, Windows 11, and Kali Linux.

All machines will be interconnected using a virtual network setup designed to replicate real-world scenarios. Additionally, the Kali machine will be configured with the flexibility to operate as either an internal or an external threat, allowing you to simulate a wide range of attack vectors against the lab network.

04 Solutions

To analyze, monitor, and secure your lab environment effectively, we'll integrate several powerful solutions. Wazuh XDR, Elasticsearch, and Kibana.

Wazuh provides real-time monitoring, threat detection, and incident response. It's lightweight, scalable, and perfect for understanding how to monitor and secure an environment proactively.

The Elasticsearch, and Kibana are a powerful open-source toolset for log management and analysis. They will help you centralize, visualize, and interpret data from your lab.

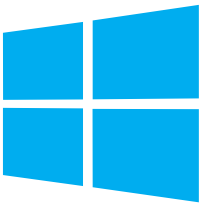
With this setup, you can simulate offensive and defensive scenarios while exploring roles like Security Analyst, Red Teamer, Threat Hunter, Detection Engineer, Security Researcher, Penetration Tester and so on.

02
Setting up machines

Setting up machines

Ubuntu Server

This is where we are going to have Wazuh XDR server and ELK stack installed, and other security solutions.



Windows Server 2022

This is going to be Active Directory Domain Controller. Here we also can set up any other custom services like Web server depending on our use case.

Windows 11

Domain joined Windows client is going to act as potential vector of attacks and pivoting scenarios.

Kali Linux

Kali Linux is going to act as internal/ external threat, depending on our network configuration.

2.1 VMWare Workstation Pro

Section Objective

- In this section we're going to install VMWare Workstation Pro
- Since VMware Workstation Pro is now available for free, we'll be using the Pro version instead of VMware Workstation Player.

01 Installation steps

- Access ***https://www.broadcom.com/***
- Click Support Portal -> go to portal (register/login with account)
- After logging expand dropdown Software (at the left of the screen), hit VMWare Cloud Foundation and click All Products
- Search for ***VMware Workstation Pro***
- On the left-hand menu, click My Downloads to access the list of available downloads under VMware Cloud Foundation, including VMware Workstation Pro.
- Find ***VMware Workstation Pro 17.0***, download newest release (17.6.2)
- Agree with Tems and Conditions and hit download icon
- Finally, launch the installer and proceed through the setup using the default settings, unless you have specific configuration preferences.

2.2 Kali Linux setup

Section Objective

- Download Kali Linux image
- Configure Kali Linux VM

01 Kali image

- Download image from the official site:
  https://www.kali.org/get-kali/#kali-installer-images

02 Kali configuration

- Create New Virtual Machine in VMWare Workstation PRO
- Select the Typical configuration option, then choose the Kali Linux image you previously downloaded.
- Continue with the installation by selecting a name for the virtual machine and specifying the installation location on your system.
- In the hardware configuration step, allocate 30 GB of disk space, 2 GB of RAM, and 2 CPU cores to the virtual machine for optimal performance.
- Once installation wizard is completed, Click Power on this VM
- Go through installation process - default values are fine in all cases
- Create new local user when asked

2.3 Ubuntu Server setup

Section Objective

- Download Ubuntu Server image
- Configure Ubuntu Server VM

01 Ubuntu Server image

- Download the image from the official site:
  https://ubuntu.com/download/server

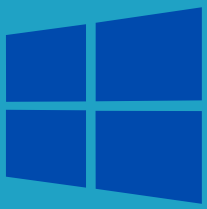
02 Ubuntu Server configuration

- Create New Virtual Machine in VMWare Workstation PRO
- Select the Typical configuration option, then choose the Ubuntu Server image you previously downloaded.
- Proceed with the installation by choosing a name for your virtual machine and selecting the location on your disk where the VM files will be stored.
- For disk space, I recommend allocating around 100 GB for testing purposes. This should be sufficient to store logs from approximately three days of testing with the firewall, XDR, and ELK stack, considering the needs of all the solutions involved. However, you can adjust the disk size based on your specific requirements.
- In the Customize Hardware section, I recommend allocating 4 GB of RAM for optimal performance (though 2 GB is the minimum required). and 2 CPU cores
- Once installation wizard is completed, Click Power on this VM
- Select Try or install Ubuntu Server
- Go through installation process - default values are fine in all cases
- Create new user when asked

2.4 Windows Server 2022

Section Objective

- Download Windows Server 2022 image
- Configure Windows Server 2022 VM



01 Windows Server 2022 image

- Download image from the official site:
  https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022

02 Windows Server 2022 configuration

- Create New Virtual Machine in VMWare Workstation PRO
- Select the Typical configuration option, then choose "I will install the operating system later." At the time of writing, there is a known bug with the installation process related to the license key. To work around this, we'll provide the operating system image at a later stage.
- Proceed with installation, select Microsoft Windows - Windows Server 2022, set VM Name and installation location.
- For hardware configuration, I recommend allocating 60 GB of disk space, 4 GB of RAM, and 2 CPU cores.
- Once installation wizard is completed, Provide .ISO downloaded in Virtual Machine settings, and click Power on this VM.
- Go through installation process - default values are fine in most cases
- Once asked for Operation system version select one with Desktop experience for ease of use, for example Windows Server 2022 Standard Evaluation (Desktop Experience)

2.5 Windows 11 setup

Section Objective

- Download Windows 11 image
- Configure Windows 11 VM

01 Windows 11 image

- Download ISO file from the official site:
  https://www.microsoft.com/en-us/software-download/windows11

02 Windows 11 configuration

- Create New Virtual Machine in VMWare Workstation PRO
- Select the Typical configuration option, then choose the Windows 11 image you downloaded.
- Proceed with the installation, select VM name and installation location.
- I suggest allocating 64 GB of disk space, 4 GB of RAM, and 2 CPU cores for the hardware configuration.
- Once installation wizard is completed, Click Power on this VM
- Go through installation process - default values are fine in most cases
- Once asked for version of Windows select Windows 11 Pro as other versions cannot be added to the Active Directory domain
- Select Set up for work or school
- Once asked do not login with Microsoft account, instead click Sign-in options and select Domain join instead, and create local user once asked

03
Setting up networking

3.1 Kali Linux network configuration

Section Objective

- Configure virtual machine settings
- Set IP address

01 VM settings

- Click on “Virtual Machine Settings”, then “Add”, and select “Network Adapter”
- First Network Adapter is going to be NAT
- Second Network Adapter is going to be VMnet2

02 IP settings

- We want to set IP address permamently
- We will set the IP to 10.0.0.5 and the default gateway to 10.0.0.1

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmcli con add type ethernet con-name "Wired connection 2" ifname eth1 ipv4.addresses 10.0.0.5/24 ipv4.gatewa
y 10.0.0.1 ipv4.method manual

Connection 'Wired connection 2' (c34ff256-ec37-4411-8f6c-ee2261c89979) successfully added.

┌──(root㉿kali)-[/home/kali]
└─# sudo nmcli con up "Wired connection 2"

Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/5)
```

3.2 Ubuntu Server network configuration

Section Objective

- Configure virtual machine settings
- Set IP address

01 VM settings

- Click on "Virtual Machine Settings", then "Add", and select "Network Adapter"
- First Network Adapter is going to be NAT
- Second Network Adapter is going to be VMnet2

02 IP settings

- The route tells the system that traffic destined for the 10.0.0.0/24 network should be sent through the gateway 10.0.0.1
- ens37 is configured with a static IP address (10.0.0.10/24)

```
ebook@ebook:~$
ebook@ebook:~$
ebook@ebook:~$ sudo nano /etc/netplan/50-cloud-init.yaml
```

```
network:
  version: 2
  ethernets:
    ens33:
      dhcp4: true
    ens37:
      dhcp4: false
      addresses:
        - 10.0.0.10/24
      routes:
        - to: 10.0.0.0/24
          via: 10.0.0.1
          metric: 100
```

```
ebook@ebook:~$ sudo netplan apply
ebook@ebook:~$
```

Network configuration file should look like this

3.3 Windows Server 2022 network configuration

Section Objective

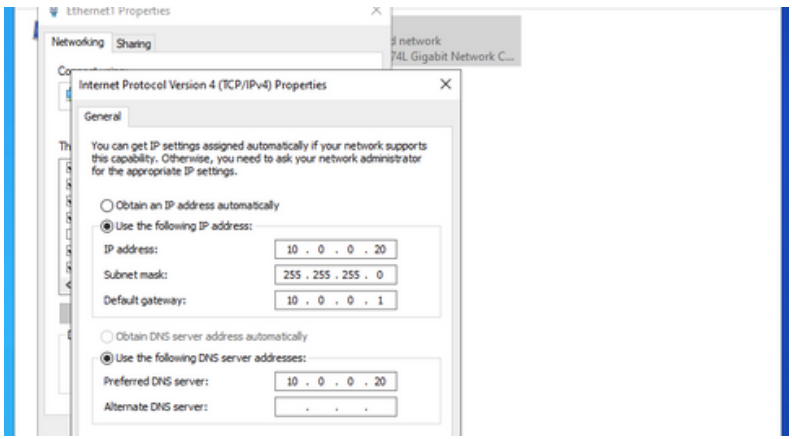
- Configure virtual machine settings
- Set IP address

01 VM settings

- Click on "Virtual Machine Settings", then "Add", and select "Network Adapter"
- First Network Adapter is going to be NAT
- Second Network Adapter is going to be VMnet2

02 IP settings

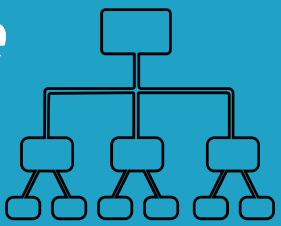
- search in windows serach bar for network connections, right click on newly created adapter, select Internet Protocol Version 4 -> Properties and provide network details in our case, it will be:



3.4 Active Directory Domain Services configuration

Section Objective

- Install and Promote Windows Server to a Domain Controller
- Create and Manage Domain Users



01 Install Active Directory Domain Services

- Server manager -> Mange -> Add roles and features, you can go with default values till Server Roles and select Active Directory Domain Serveices, and till the end you can go with defaults, and hit install
- After the installation is complete, click the flag icon in server manager, and then hit "Promote this server to a domain controller"
- then Add new forest and enter Root domain name (can be something like ebook.lab)

02 Create user account

- After the server restarts and the installation is complete, you can finish the setup by creating a new user account.
- Click Server Manager -> Tools -> Active Directory Users and Computers, expand your domain and right click on Users and New -> User -> enter user details (in our case James@ebook.lab)

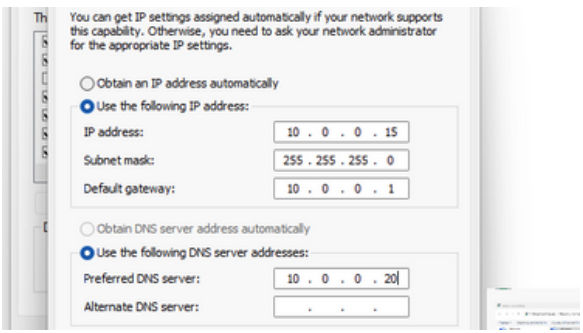
3.5 Windows 11 network configuration and domain

Section Objective

- Set IP address
- Join to a previously created domain

01 Setting IP address

- search in windows serach bar for network connections, right click on newly created adapter(most likely ethernet 1), select Internet Protocol Version 4 -> Properties and provide network details for lab, it will be:



02 Joining a Domain

- In windows search bar type Access work or school, hit enter, click blue connect button, once asked for email address click below option "Join this device to a local Active Directory domain", type your domain, and provide credentials of domain administrator
- Once asked for user provide user created in Active directory configuration in our case James and select Standard User account type, click next and restart the computer

04
Setting up Elastic Stack

4.1 Installing Elasticsearch

Section Objective

- Install Elasticsearch on Ubuntu Server
- Reset password

01 Installing Elasticsearch

- Change directory to opt with:
  cd /opt
- Install Elasticsearch with wget:

```
ebook@ebook:/opt$ sudo wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.17.0-amd64.deb
```

- now we need to unpack it and install:

```
ebook@ebook:/opt$ sudo dpkg -i elasticsearch-8.17.0-amd64.deb
```

- You gonna be prompted with eleastic superuser password, you don't have to copy it, you can reset it later on your own, with the eleastic-reset-passwrod binary, in order to do it proceed with those commands:

```
ebook@ebook:/opt$ sudo /bin/systemctl daemon-reload
ebook@ebook:/opt$ sudo /bin/systemctl enable elasticsearch.service
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /usr/lib/systemd/system/elasticsearch.service.
ebook@ebook:/opt$ sudo /bin/systemctl start elasticsearch.service
ebook@ebook:/opt$ sudo /usr/share/elasticsearch/bin/elasticsearch-reset-password  -u elastic -i
This tool will reset the password of the [elastic] user.
You will be prompted to enter the password.
Please confirm that you would like to continue [y/N]y


Enter password for [elastic]:
passwords must be at least [6] characters long
Try again.
Enter password for [elastic]:
Re-enter password for [elastic]:
Password for the [elastic] user successfully reset.
ebook@ebook:/opt$
```

- **-u flag is used to specify user, -i is for interactive password reset (so you can type it manually)**

4.2 Elasticsearch Configuration

Section Objective

- Edit Elasticsearch configuration file
- Set proper IP address and port number

01 Configuring Elasticsearch

- First we need to edit elasticsearch configuration file
- In order to do it we need to change user to root with ***sudo su***
- Now we can change directory with ***cd /etc/elasticsearch***
- Now we can open configuration file with a built in text editor
  nano elasticsearch.yml
- We want to change three things in this file - IP address and Port numbers
- To achieve this, we'll need to uncomment and modify two elements, as shown in the screenshot, and add third element (transport.port):

```
# ---------------------------------- Network -----------------------------------
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: 10.0.0.10
transport.port: 9400
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9201
#
# For more information, consult the network module documentation.
```

- To save this file you need to press ctrl+o, and to exit text editor press ctrl+x
- We changed IP address to 10.0.0.10 and port number to 9201
- Normally we could leave port number as default which is 9200 and transport port as 9300 but later in this ebook we will need those port to run Wazuh XDR

4.3 Elasticsearch Configuration Verification

Section Objective

- Restart Elasticsearch service
- Verify that everything works

01 Restarting Elasticsearch

- After we changed configuration file we need to restart the elasticsearch service

```
root@ebook:/etc/elasticsearch# sudo /bin/systemctl restart elasticsearch.service
root@ebook:/etc/elasticsearch#
```

02 Ensuring Everything Is Working Correctly

- To verify if elasticsearch works we can use ***curl*** command

```
root@ebook:/etc/elasticsearch# curl -k -u elastic:elastic https://10.0.0.10:9201
{
  "name" : "ebook",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "Fb-I0vstSo-aGt6SIziuOQ",
  "version" : {
    "number" : "8.17.0",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "2b6a7fed44faa321997703718f07ee0420804b41",
    "build_date" : "2024-12-11T12:08:05.663969764Z",
    "build_snapshot" : false,
    "lucene_version" : "9.12.0",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

- here you need to specify your previously set password

  elastic:<your password>

- If your output matches the screenshot, it indicates that everything is working correctly

4.4 Kibana Installation

Section Objective

- Download Kibana package
- Unpack and Install Kibana

01 Installing Kibana

- First we need to change directory to opt with ***cd /opt***
- now we can download kibana with wget

```
root@ebook:/opt# wget https://artifacts.elastic.co/downloads/kibana/kibana-8.17.0-amd64.deb
--2025-05-28 13:48:05--  https://artifacts.elastic.co/downloads/kibana/kibana-8.17.0-amd64.deb
Resolving artifacts.elastic.co (artifacts.elastic.co)... 34.120.127.130, 2600:1901:0:1d7::
Connecting to artifacts.elastic.co (artifacts.elastic.co)|34.120.127.130|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 345323288 (329M) [application/vnd.debian.binary-package]
Saving to: ‘kibana-8.17.0-amd64.deb’

kibana-8.17.0-amd64.deb                 100%[=============================================================

2025-05-28 13:48:56 (6.49 MB/s) - ‘kibana-8.17.0-amd64.deb’ saved [345323288/345323288]

root@ebook:/opt#
```

- Now we can unpack and install kibana with dpkg command:

```
root@ebook:/opt# dpkg -i kibana-8.17.0-amd64.deb
Selecting previously unselected package kibana.
(Reading database ... 88221 files and directories currently installed.)
Preparing to unpack kibana-8.17.0-amd64.deb ...
Unpacking kibana (8.17.0) ...
Setting up kibana (8.17.0) ...
Creating kibana group... OK
Creating kibana user... OK
Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how to disable
7/production.html#openssl-legacy-provider
Created Kibana keystore in /etc/kibana/kibana.keystore
root@ebook:/opt#
```

4.5 Kibana Setup

Section Objective

- Setup Kibana
- generate token and copy with tmux

01 Kibana Setup

- First we need to generate Kibana enrollement token with:

/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana

```
root@ebook:/opt# sudo /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana
eyJ2ZXIiOiI4LjE0LjAiLCJhZHIiOlsiMTAuMC4wLjEwOjkyMDEiXSwiZmdyIjoiMTg5ZGEyODk3MTYxNGJmODllNzU1NTdiOWJhOWViOTA1ZWU5MDA4NzZ
InpZZ3ZGNWNCbDZnTVFJMTNGWHp0OjhOaHlzcUJBUzB1OUZ0UEhnV3I0RkEifQ==
root@ebook:/opt#
```

- We need to copy this token to move to the next step
- Unfortunately Ubuntu Server doesn't come with copy function
- In order to copy this token I recommend installing tmux:

  sudo apt install tmux
- now we can enter tmux session with command: ***tmux***
- now generate token again and press:

  ctrl +b + [
- now to copy this token hold: ***ctrl + space***, and use arrows
- lastly press ***ctrl + w***
- now we can paste the token with: ***ctrl +b +]***

02 Kibana Setup continuation

- now we can run kibana setup binary and paste the token

```
root@ebook:/opt# /usr/share/kibana/bin/kibana-setup
Native global console methods have been overridden in production environment.
? Enter enrollment token: eyJ2ZXIiOiI4LjE0LjAiLCJhZHIiOlsiMTAuMC4wLjEwOjkyMDEiXSwiZmdyIjoiMTg5ZGEyODk3
U0OTExOTc4OTQ5ZCIsImtleSI6IjA0ZzJGNWNCbDZnTVFJMTNIbnhBOkJhUjJLLTBYUlkyZ0NSVHNLbWMwelEifQ==

✔ Kibana configured successfully.

To start Kibana run:
  bin/kibana
root@ebook:/opt#
```

4.6 Kibana Configuration

Section Objective

- Setup Kibana
- generate token and copy with tmux

01 Kibana Configuration

- In order to finish setting up kibana we need to edit Kibana's configuration file

```
root@ebook:/opt# nano /etc/kibana/kibana.yml
root@ebook:/opt#
```

- In this file we need to uncomment server.port and leave it as default (5601)
- We also need to uncomment server.host and change it to 10.0.0.10
- File should look like this:

```
 GNU nano 7.2                                                  /etc/kibana/kibana.yml *
# For more configuration options see the configuration guide for Kibana in
# https://www.elastic.co/guide/index.html

# ==================== System: Kibana Server ====================
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid va
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: 10.0.0.10

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
```

- Save file with ***ctrl + o***, and exit text editor with ***ctrl + x***

02 Starting Kibana Service

- Lastly we need to enable and start kibana service

```
root@ebook:/opt# sudo systemctl enable kibana.service
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /usr/lib/systemd/system/kibana.serv
root@ebook:/opt#
root@ebook:/opt# sudo systemctl start kibana.service
root@ebook:/opt# _
```

4.7 Enable PowerShell Advanced Logging

Section Objective

- Enable PowerShell Advanced Logging on Computers in Active Directory domain

01 Enabling PS advanced logging

- in Windows Server search bar Group Policy Management, expand your forest (for example ebook.lab) -> Domains -> ebook.lab -> right click on Group Policy Objects -> New GPO -> enter a name like "Logging" -> right click Edit
- Go to: Computer Configuration > Policies -> Administrative Templates > Windows Components > Windows PowerShell
- Double click on "Turn on Powershell Script Block logging" - set it to enabled and also select "Log script block invocation start / stop events" -> click Apply
- Enable Module logging -> Double-click on "Turn on Powershell Module logging" Set it to enabled -> specify modules that we want to log -> Click on "Show" under options section -> type * wildcard symbol which means all modules
- Now open Server Manager -> Tools → AD Users and Computers ->right-click on ebook.lab -> New -> Organizational Unit -> name it for example Logging
- Now go to Computers in the same window, right click on our Win11 → move → and move it to the newly created OU
- Now type in search bar Group Policy Management → expand forest etc. → right-click on ebook.lab → click "Link an Existing GPO...", select Logging GPO and close the window
- Lastly open command prompt on Win11 and type ***gpupdate /force to*** enforce policy changes

4.8 Configuring Windows 11 for Log Forwarding [1]

Section Objective

- Install winlogbeat
- Configure winlogbeat to send logs from windows 11 to elasticsearch

01 Installing Winlogbeat

- Install this lightweight agent from this link:
  https://www.elastic.co/downloads/beats/winlogbeat
- You can download it to your main operating system and move to win11 VM
- Now unzip it, I'll extract it to Program Files
- Now we need to install winlogbeat as a service, in order to do that we need to open PowerShell with administrative privileges
- move to the proper directory, in my case:
  cd C:\program files\winlogbeat-9.0.1-windows-x86_64
- run this command to allow running scripts:
  Set-ExecutionPolicy Unrestricted
- run this ps script:
  .\install-service-winlogbeat.ps1

02 Configuring Winlogbeat

- Still in the same directory, we need to create keystore for password:
  .\winlogbeat.exe keystore create
  .\winlogbeat.exe keystore add ES_PWD (and type your elastic pass)
- Lastly open winlogbeat.yml (located in the same directory) with any text editor
- Continuation on the next page...

4.8 Configuring Windows 11 for Log Forwarding [2]

Section Objective

- Configure winlogbeat.yml file

02 Configuring Winlogbeat Continuation

- Our configuration file that we previously opened should look like this

```
winlogbeat.event_logs:
  - name: Security
    event_id: 4688, 4697, 4720, 4726, 4732

  - name: Windows PowerShell
    event_id: 400, 403

  - name: Microsoft-Windows-PowerShell/Operational
    event_id: 4103, 4104, 4105, 4106
```

```
setup.kibana:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify and additional path, the scheme is required: http://localhost:5601/p
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "http://10.0.0.10:5601"
  ssl.verification_mode: none
```

```
# ------------------------------ Elasticsearch Output ------------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["https://10.0.0.10:9201"]

  # Protocol - either `http` (default) or `https`.
  protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "${ES_PWD}"
  ssl.verification_mode: none

  # Pipeline to route events to security, sysmon, or powershell pipelines.
  pipeline: "winlogbeat-%{[agent.version]}-routing"
```

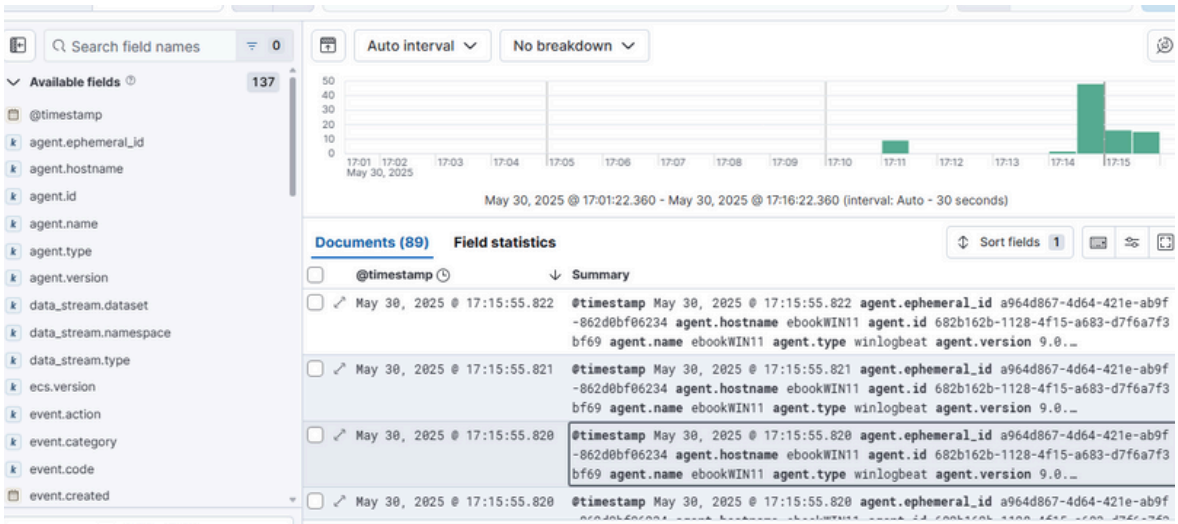
4.8 Verifying successful log forwarding

Section Objective

- Run winlogbeat test in cmd
- verify if logs are sent properly in kibana

01 Running winlogbeat test

- Open cmd and go to winlogbeat location, then run:
  winlogbeat.exe test config
  winlogbeat.exe test output
  winlogbeat.exe setup
  net start winlogbeat
- now open browser and go to:
  http://10.0.0.10:5601 ***(our kibana instance)***
- and now we should see some logs already ingested:



05
Setting up Wazuh XDR

5.1 Wazuh Indexer (Engine)

Section Objective

- Install Wazuh Indexer on Ubuntu Server
- Configure Indexer

01 Installing Indexer

- Create directory for our install script and config file:
  mkdir /opt/wazuh && cd /opt/wazuh
- Download the Wazuh installation assistant and the configuration file:
  curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
  curl -sO https://packages.wazuh.com/4.9/config.yml
- Edit ./config.yml and replace IP values with ubuntu server IP (10.0.0.10)
- Run the Wazuh installation assistant with the option --generate-config-files to generate the Wazuh cluster key, certificates, and passwords necessary for installation:
  bash wazuh-install.sh --generate-config-files
- Run the Wazuh installation assistant with the option --wazuh-indexer and the node name to install and configure the Wazuh indexer:
  bash wazuh-install.sh --wazuh-indexer node-1
- Run the Wazuh installation assistant with option --start-cluster on any Wazuh indexer node to load the new certificates information and start the cluster:
  bash wazuh-install.sh --start-cluster
- Run the following command to get the admin password:
  tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | grep -P "\'admin\'" -A 1
- Now test it, if its working it will produce json output:
  curl -k -u admin:<ADMIN_PASSWORD> https://10.0.0.10:9200

Common Problem:

- There is a common problem with wazuh-indexer that prevents it from working, to workaround it we need to use:

mkdir -p /var/log/wazuh-indexer/tmp && touch /var/log/wazuh-indexer/gc.log && chmod -R 777 /var/log/wazuh-indexer

5.2 Wazuh Manager (Server)

Section Objective

- Install Wazuh Manager on Ubuntu Server
- Configure Manager

01 Installing Manager

- Run the installation with the --wazuh-server parameter, using the name defined in config.yml (default: wazuh-1):

  bash wazuh-install.sh --wazuh-server wazuh-1

- It installs wazuh manager, filebeat and is doing a couple other things

```
31/05/2025 09:55:27 INFO: --- Wazuh server ---
31/05/2025 09:55:27 INFO: Starting the Wazuh manager installation.
31/05/2025 09:58:23 INFO: Wazuh manager installation finished.
31/05/2025 09:58:23 INFO: Wazuh manager vulnerability detection configuration finished.
31/05/2025 09:58:23 INFO: Starting service wazuh-manager.
31/05/2025 09:58:48 INFO: wazuh-manager service started.
31/05/2025 09:58:48 INFO: Starting Filebeat installation.
31/05/2025 09:59:09 INFO: Filebeat installation finished.
31/05/2025 09:59:11 INFO: Filebeat post-install configuration finished.
31/05/2025 09:59:15 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
31/05/2025 09:59:48 INFO: Starting service filebeat.
31/05/2025 09:59:52 INFO: filebeat service started.
31/05/2025 09:59:52 INFO: Installation finished.
root@ebook:/opt/wazuh# _
```

5.3 Wazuh Dashboard

Section Objective

- Install Wazuh Dashboard on Ubuntu Server
- Configure Wazuh Dashboard

01 Installing Dashboard

- Run the installation with the --wazuh-dashboard parameter, using the name defined in the config.yml file (default: dashboard):

  bash wazuh-install.sh --wazuh-dashboard dashboard

```
root@ebook:/opt/wazuh# bash wazuh-install.sh --wazuh-dashboard dashboard
31/05/2025 10:06:28 INFO: Starting Wazuh installation assistant. Wazuh version: 4.9.2
31/05/2025 10:06:28 INFO: Verbose logging redirected to /var/log/wazuh-install.log
31/05/2025 10:06:41 INFO: Verifying that your system meets the recommended minimum hardware requirements.
31/05/2025 10:06:41 INFO: Wazuh web interface port will be 443.
31/05/2025 10:06:49 INFO: --- Dependencies ----
31/05/2025 10:06:49 INFO: Installing debhelper.
31/05/2025 10:08:13 INFO: Wazuh repository added.
31/05/2025 10:08:14 INFO: --- Wazuh dashboard ----
31/05/2025 10:08:14 INFO: Starting Wazuh dashboard installation.
31/05/2025 10:09:36 INFO: Wazuh dashboard installation finished.
31/05/2025 10:09:36 INFO: Wazuh dashboard post-install configuration finished.
31/05/2025 10:09:36 INFO: Starting service wazuh-dashboard.
31/05/2025 10:09:38 INFO: wazuh-dashboard service started.
31/05/2025 10:10:02 INFO: Initializing Wazuh dashboard web application.
31/05/2025 10:10:03 INFO: Wazuh dashboard web application initialized.
31/05/2025 10:10:03 INFO: --- Summary ---
31/05/2025 10:10:03 INFO: You can access the web interface https://10.0.0.10:443
    User: admin
    Password: 4M7DDMm5*EY?t.BEclTuFH04?vMXopOY
31/05/2025 10:10:03 INFO: Installation finished.
root@ebook:/opt/wazuh# _
```

- If you want to access all of your passwords for wazuh you can use:
  tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt

- Now wazuh will be accessible with this URL:
  https://10.0.0.10
- You can login with admin credentials

5.4 Wazuh Agent + Sysmon (Windows 11) [1]

Section Objective

- Configure Sysmon logging on win11
- Install Wazuh Agent on win11

01 Installing and Configuring Sysmon

- Download sysmon zip from this link:
  https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
- Extract sysmon to newly created 'sysmon' folder in program files:
  Right click -> exctract all -> C:\program files\sysmon
- Download sysmon configuration file from this link:
  https://wazuh.com/resources/blog/emulation-of-attack-techniques-and-detection-with-wazuh/sysmonconfig.xml
- Move this config file to ***c:\program files\sysmon***
- Open cmd, and go to c:\program files\sysmon and run:
  Sysmon64.exe -accepteula -i sysmonconfig.xml

```
c:\Users\James\Desktop\Sysmon>Sysmon64.exe -accepteula -i sysmonconfig-export.xml


System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.

c:\Users\James\Desktop\Sysmon>
```

5.4 Wazuh Agent + Sysmon (Windows 11) [2]

Section Objective

- Configure Sysmon logging on win11
- Install Wazuh Agent on win11

02 Installing and Configuring Wazuh Agent

- Open PowerShell and use this command to download lightweight agent that will monitor your pc:

Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.9.2-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='10.0.0.10' WAZUH_AGENT_NAME='windows11'

- You will need administrator privileges to execute this command, and powershell 3.0 or greater
- Now start the service:

Start-Service WazuhSvc

- In order to add sysmon to the wazuh agent config file:
- Go to ***C:\Program files(x86)\ossec-agent***
- open ***ossec.conf*** with notepad and add these four lines:

```
<localfile>
  <location>Microsoft-Windows-Sysmon/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
```

- Lastly restart Wazuh Agent service:

Restart-Service WazuhSvc

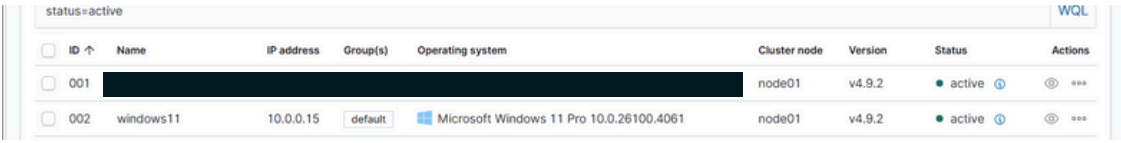
5.4 Verifying if everything works

Section Objective

- Log into Wazuh
- Check if it logs Sysmon

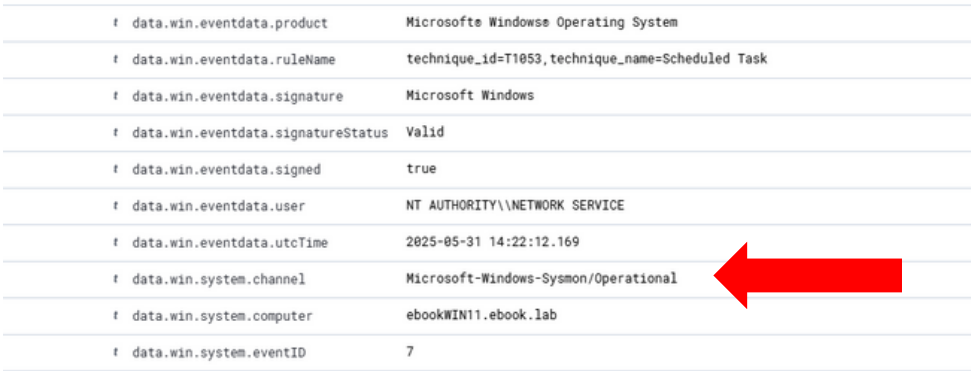
01 Logging into Wazuh

- Open any browser on windows 11 and browse to:
  https://10.0.0.10
- login with admin:<Admin Password>
- Click on Overview, you should see windows 11
  (don't mind my second PC, you should see only win11)



02 Looking for Sysmon logs

- Now go to Discover and sift through logs and look for some sysmon logs



06
Summary

Summary

This ebook was created with one clear mission: to help you build a structured, versatile cybersecurity lab that mirrors real-world conditions and supports both offensive and defensive skill development.

From our experience, diving into cybersecurity without a clear learning path can feel overwhelming. That's why we focused on clarity, structure, and practicality — guiding you step-by-step through the setup process while also leaving room for future growth.

We walk you through the process of choosing a virtualization platform (leveraging VMware Workstation Pro), deploying four core machines (Ubuntu Server, Windows Server 2022, Windows 11, and Kali Linux), and configuring a realistic virtual network. This setup allows you to simulate a range of attack and defense scenarios in a controlled environment.

To bring the lab to life, we integrate solutions like Wazuh XDR, Elasticsearch, and Kibana — giving you visibility into system activity, detection capabilities, and incident response workflows. These tools provide a foundation for learning modern blue team practices while also supporting red team testing.

Whether you're aiming to become a Red Teamer, Security Analyst, Detection Engineer, or just want to get hands-on with cybersecurity concepts, this lab is designed to grow with you.