PROJECT

VIRTUAL HOMELAB

Performed By: Hardil Panwar

HOMELAB AIMS

I’d like to emphasise that this write-up is not intended to be a step-by-step walkthrough, especially regarding OS installs or VM creation. Instead, my purpose in writing is to share a high-level overview of the homelab. With that in mind, let’s get started.

Since my plans for the homelab involved gaining experience with various red/blue team tools and techniques, I designed my homelab with functionality in mind.

The homelab itself is a perpetual work in progress. That said, I’m proud of the functional, secure homelab framework I’ve constructed to this point.

TECHNOLOGY USED

1. VMWare

1.1. VMware is a leading provider of virtualization and cloud computing technology. It enables users to run multiple operating systems on a single physical machine, improving resource efficiency, security, and flexibility.

1.2. VMware is a virtualization platform that allows users to create and manage virtual machines (VMs).

1.3. It enables hardware abstraction, meaning multiple OS environments can run on the same hardware.

1.4. Commonly used in enterprise IT, cybersecurity labs, and cloud environments for testing, development, and security training.

2. Wazuh

2.1. Wazuh is a free and open-source security platform that unifies XDR and SIEM capabilities. It protects workloads across on-premises, virtualized, containerized, and cloud-based environments.

2.2. Wazuh helps organizations and individuals to protect their data assets against security threats. It is widely used by thousands of organizations worldwide, from small businesses to large enterprises.

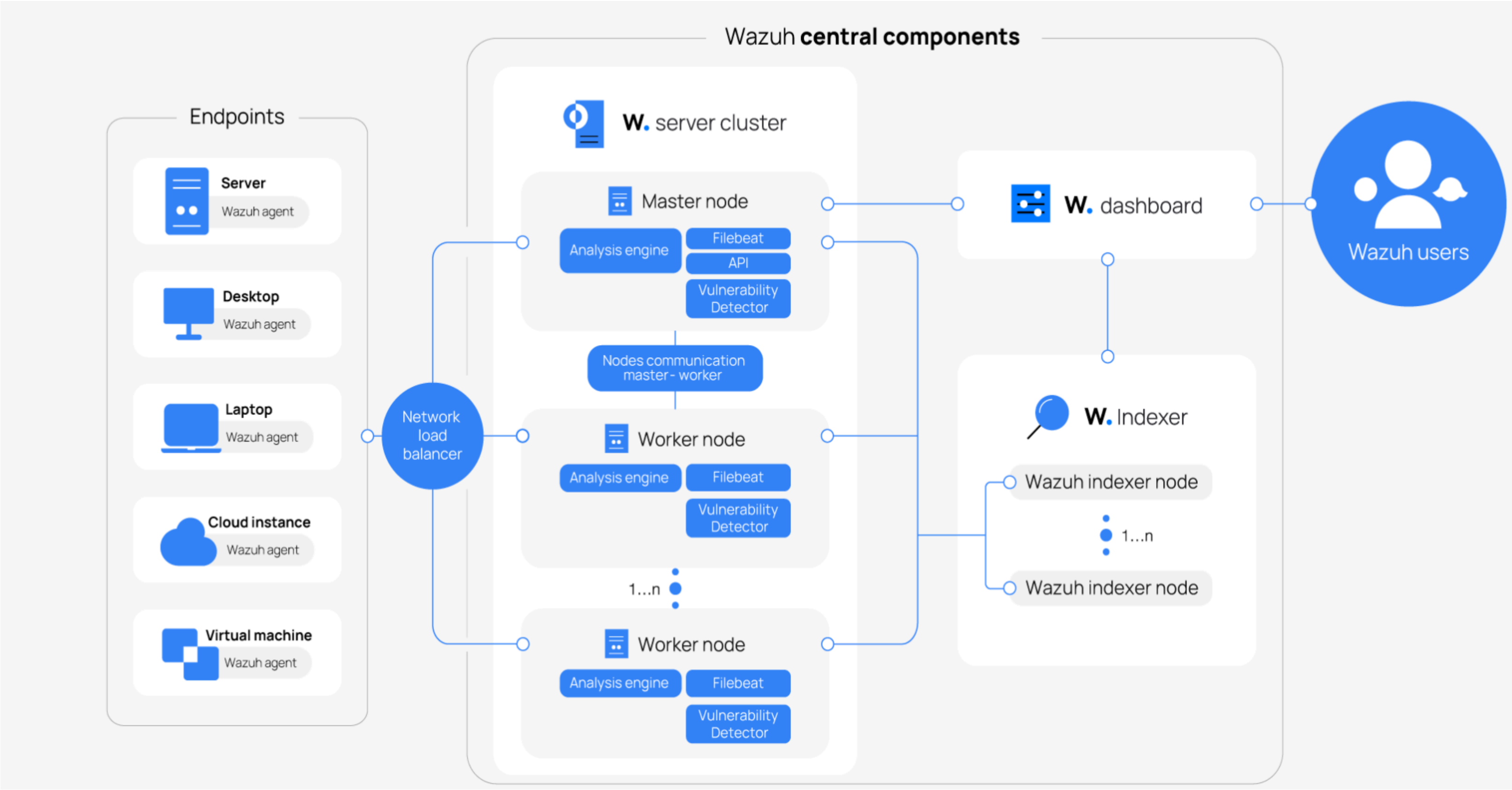
2.3. Wazuh has one of the largest open-source security communities in the world.

2.4. The solution is composed of a single universal agent and three central components: the **Wazuh server**, the **Wazuh indexer**, and the **Wazuh dashboard**.

2.5. The Wazuh architecture is based on agents, running on the monitored endpoints, that forward security data to a central server. Agentless devices such as firewalls, switches, routers, and access points are supported and can actively submit log data via Syslog, SSH, or using their API. The central server decodes and analyzes the incoming information and passes the results along to the Wazuh indexer for indexing and storage.

2.6. The **Wazuh indexer** cluster is a collection of one or more nodes that communicate with each other to perform read and write operations on indices. Small Wazuh deployments, which do not require processing large amounts of data, can easily be handled by a single-node cluster. Multi-node clusters are recommended when there are many monitored endpoints, when a large volume of data is anticipated, or when high availability is required.

2.7. The diagram below represents a Wazuh deployment architecture. It shows the solution components and how the Wazuh server and the Wazuh indexer nodes can be configured as clusters, providing load balancing and high availability.



3. Wazuh Agent

3.1. The Wazuh agent is a multi-platform component of the Wazuh solution and runs on the endpoints you want to monitor. It communicates with the Wazuh server, sending data in near real-time through an encrypted and authenticated channel. The Wazuh agent provides capabilities such as log data collection, file integrity monitoring, threat detection, security configuration assessment, system inventory, vulnerability detection, and incident response to enhance your endpoint security.

3.2. After installing the Wazuh agent on an endpoint, you need to enrol the Wazuh agent in the Wazuh manager.

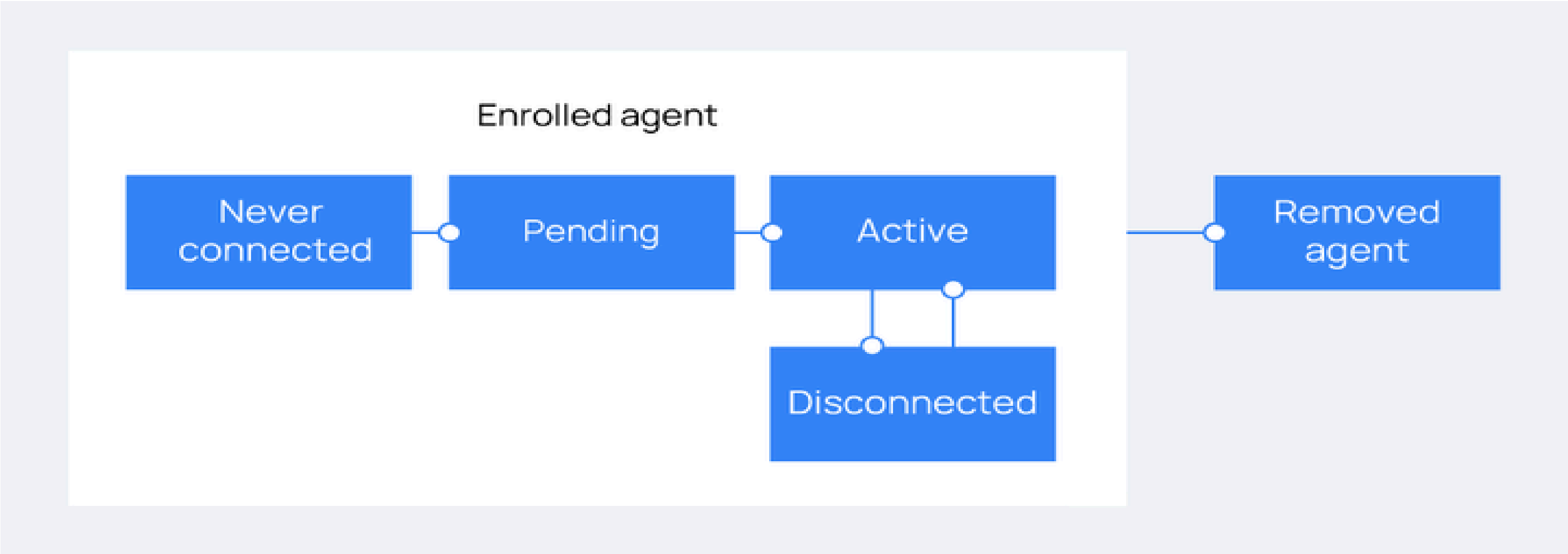
3.3. The two methods are available for enrolling Wazuh agents:

3.3.1. Enrollment via agent configuration: Once the IP address or FQDN (Fully Qualified Domain Name) of the Wazuh server has been set, the Wazuh agent can request the client key and import it automatically. This is the recommended enrollment method.

3.3.2. Enrollment via Wazuh server API: The user requests the client key from the Wazuh server API and then manually imports it to the Wazuh agent.

3.4. There are four different connection states that a Wazuh agent may be in at any given time, as shown in the image below:

3.4.1. Never connected: The Wazuh agent has been enrolled but has not yet connected to the Wazuh manager.



3.4.2. Pending: The authentication process has not been completed because the Wazuh manager received a request for connection from the Wazuh agent but has not received anything else. The Wazuh agent will be in this state one time in its life cycle after each startup. If the Wazuh agent persists in this state, it may indicate a connectivity issue.

3.4.3. Active: The Wazuh agent has successfully connected and can now communicate with the Wazuh manager.

3.4.4. Disconnected: The Wazuh manager will consider the agent disconnected if it does not receive any keep-alive messages within agents_disconnection_time (the default time is 10m).

4. Nessus

4.1. Tenable Nessus, the industry's most widely deployed vulnerability assessment solution helps to reduce an organization's attack surface and ensure compliance.

4.2. Tenable Nessus features high-speed asset discovery, configuration auditing, target profiling, malware detection, sensitive data discovery, and more.

4.3. Tenable Nessus supports more technologies than competitive solutions, **scanning** operating systems, network devices, hypervisors, databases, web servers, and critical infrastructure for vulnerabilities, threats, and compliance violations.

5. pfSense Firewall

5.1. The pfSense® Project is a free open-source customized distribution of FreeBSD tailored for use as a firewall and router entirely managed by an easy-to-use web interface. This web interface is known as the web-based GUI configurator, or WebGUI for short. No FreeBSD knowledge is required to deploy and use pfSense software.

5.2. The majority of users have never used FreeBSD outside of pfSense software. In addition to being a powerful, flexible firewalling and routing platform, pfSense software includes a long list of related features.

5.3. The pfSense software package system allows further expandability without adding bloat and potential security vulnerabilities to the base distribution.

5.4. pfSense software is a popular project with millions of downloads since its inception and hundreds of thousands of active installations. It has been proven successful in countless installations ranging from single computer protection in small home networks to thousands of network devices in large corporations, universities and other organisations.

6. Kali-Linux

6.1. Kali Linux (formerly known as BackTrack Linux) is an open-source, Debian-based Linux distribution that allows users to perform advanced penetration testing and security auditing. It runs on multiple platforms and is freely available and accessible to both information security professionals and hobbyists.

6.2. This distribution has several hundred tools, configurations, and scripts with industry-specific modifications that allow users to focus on tasks such as computer forensics, reverse engineering, and vulnerability detection, instead of dealing with unrelated activities.

6.3. This distribution is specifically tailored to the needs of experienced penetration testers, so therefore all documentation on this site assumes prior knowledge of and familiarity with, the Linux operating system in general.

7. Windows Server 2022

7.1. Windows Server is the platform for building an infrastructure of connected applications, networks, and web services, from the workgroup to the data center. Windows Server bridges on-premises environments with Azure, adding additional layers of security while helping you modernize your applications and infrastructure.

8. Flare VM

8.1. A collection of software installation scripts for Windows systems that allows to easily set up and maintain a reverse engineering environment on a virtual machine (VM).

8.2. FLARE-VM was designed to solve the problem of reverse engineering tool curation and relies on two main technologies: **Chocolatey and Boxstarter**.

8.2.1. Chocolatey is a Windows-based Nuget package management system, where a "package" is essentially a ZIP file containing PowerShell installation scripts that download and configure a specific tool.

8.2.2. Boxstarter leverages Chocolatey packages to automate the installation of software and create repeatable, scripted Windows environments.

9. Splunk

9.1. Splunk Enterprise is a software product that enables you to search, analyze, and visualize the data gathered from the components of your IT infrastructure or business.

9.2. Splunk Enterprise takes in data from websites, applications, sensors, devices, and so on. After you define the data source, Splunk Enterprise indexes the data stream and parses it into a series of individual events that you can view and search.

9.3. Most users connect to Splunk Enterprise with a web browser and use Splunk Web to administer their deployment, manage and create knowledge objects, run searches, create pivots and reports, and so on.

9.4. There are three main stages in the Splunk data pipeline: data collection, data indexing, and finally, search and analysis.

9.4.1. Data Collection

9.4.1.1. The first stage of the Splunk data pipeline is data collection. Splunk can ingest data from a wide variety of sources, including files, directories, network events, and APIs. It supports common data formats such as CSV, JSON, and XML, as well as custom formats. Data collection is typically performed using forwarders, which are lightweight agents that can be installed on any machine that generates data. Learn more in the Splunk Components section below.

9.4.2. Data Indexing

9.4.2.1. Once data is collected, it moves on to the indexing stage. Splunk indexes the data by parsing it into individual events and extracting relevant fields, such as timestamps, source types, and host information. This process enables efficient searching and analysis of the data later on.

9.4.3. Data Searching and Analysis

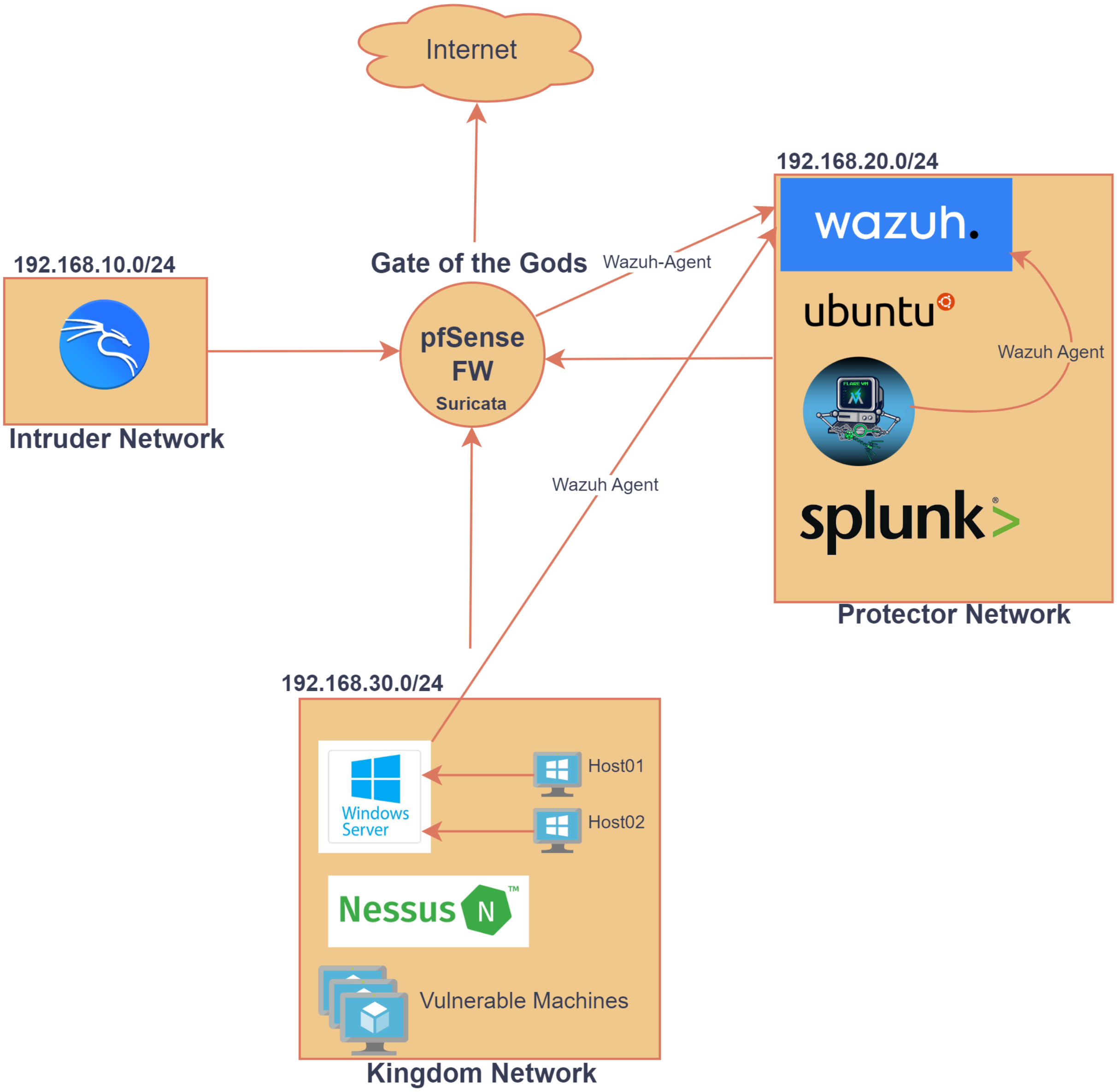
9.4.3.1. After data is indexed, it can be searched and analyzed using Splunk's powerful search language, the Search Processing Language (SPL). SPL allows users to perform a wide range of operations on the data, such as filtering, aggregation, correlation, and statistical analysis. Users can create custom reports, dashboards, and alerts based on the results of their searches and analyses.

10. Vulnerable Machines

10.1. Metasploitable 2 – A deliberately vulnerable Linux-based VM designed for practicing penetration testing and Metasploit exploitation.

10.2. VulnHub VMs – Various intentionally vulnerable machines available for free to practice exploitation.

LOGICAL TOPOLOGY



This Lab is inspired by the book 'A Song Ice and Fire'.
I've created three distinct networks i.e.,

1. Intruder Network: 192.168.10.0/24
2. Protector Network: 192.168.20.0/24
3. Kingdom Network: 192.168.30.0/24

Intruder Network:

This network contains a Kali-Linux machine which will be performing attacks. The machine is intruding on different networks collecting information and silently performing attacks.

Kingdom Network:

This network contains different types of machines i.e.,

- Windows Server 2022: DC-server
- Vulnerable machines like Metasploitable2
- Nessus: Hand of the King
- Host machines connected to Windows Server: Weakling

DC-server has Wazuh-Agent installed and sends logs to Wazuh-server which is placed in its dedicated network for security purposes.

For practice purposes, I have also added Vulnerable machines like Metasploitable2.

Hand of the King will be used for the vulnerability scanning and I will be using it to learn different methods to secure the systems and learn how different techniques can exploit the vulnerabilities.

I have added host machines i.e., Weakling (Windows 7), as it contains a lot of vulnerabilities. This can be used to learn Red Teamwork.

Protector Network:

As the name suggests, this network contains different machines which will be used to protect the Kingdom Network. This network contains different types of security machines i.e.,

- Wazuh SIEM : Wazuh-server
- Ubuntu machine : Protector’s Base
- FlareVM: Protector Analysis Lab (also Nika)
- Splunk : Splunk-server

Wazuh-server will be used as the main SIEM tool which will be performing different analyses like File Integrity Monitoring, Malware Detection, Vulnerability Management and more. It will be getting all the logs from the pfSense Firewall, Windows Server 2022 from Kingdom Network, and FlareVM will also send the logs.

The Protector's Base machine will behave like a Wazuh’s Security base. It means I will be using this machine to access the Dashboard of the Wazuh. That is the whole purpose of this machine.

I have installed FlareVM on my Protector Analysis Lab. This machine will be used for malware analysis. It has all the tools which are required to perform the analysis.

Splunk-server is installed on this network. I have installed Universal Forwarder in the DC-server machine from the Kingdom network. But, I will be actively using the Wazuh-server. However, I am planning to make Splunk-server a fully-fledged warrior for the analysis work too, just like Wazuh-server.

pfSense Firewall:

At the heart of all this is the pfSense Firewall. I named it Gate of the Gods. It has Suricata added to it. It will be actively used to provide different networks with the required network access.

STORYTIME

The Kingdom: Defending the Realm
In the heart of the digital world lies KingdomNetwork, a thriving domain where data flows like lifeblood, powering the kingdom’s operations. But with every kingdom comes the threat of invaders — malicious forces aiming to breach the gates and disrupt the peace.

The Gate of the Gods: The Kingdom’s First Line of Defense
At the edge of the kingdom stands an unyielding fortress — Gate of the Gods, a powerful sentinel known to mortals as pfSense. This gate carefully controls who may enter and who must be turned away, inspecting every traveller and messenger seeking passage.

- WAN (The Outlands): The wild, unpredictable internet.
- LANs (The Inner Kingdom): The core of the realm, housing loyal subjects (hosts and servers).

Within the gate resides a powerful oracle: Wazuh-agent, installed directly within the fortress. It listens to every log, detects anomalies, and raises the alarm at the first sign of trouble — serving as both the chronicler and protector of the kingdom.

The Royal Guard: Suricata, the Vigilant Sentinel
Patrolling the walls of the Gate of the Gods is Suricata, a tireless sentinel watching every packet like a hawk. It scans for suspicious patterns and intrusions, feeding its observations directly to Wazuh, which deciphers and analyzes the threats.

The Royal Library: The Kingdom’s Living Memory
Instead of ancient scrolls and dusty tomes, the kingdom relies on the Wazuh-server as its living archive. Every event, from login attempts to firewall decisions, is meticulously logged and analyzed. Wazuh serves as both historian and investigator, ready to reveal hidden dangers lurking in past events.

The Palace and Its People: The Heart of the Kingdom
The DC-server acts as the royal palace, coordinating the efforts of the realm. The connected hosts diligently serve the kingdom, but without careful oversight, they might accidentally invite malicious influences — making continuous monitoring essential.

The Dark Forest: Home of the Intruder
Beyond the Gate of the Gods lies the Intruder, a rogue warrior wielding the tools of chaos — Kali Linux. This adversary launches relentless attacks, probing the defences and seeking vulnerabilities. Yet with every failed attempt, the kingdom learns, evolves, and fortifies itself further.

The Council of War: The Kingdom’s Strategic Mind
When danger strikes, the kingdom assembles its council:

- **Wazuh-server** (The All-Seeing Oracle): Collects and analyzes logs, detects threats, and orchestrates the defensive response.

- **Hand of the King** (The Royal Guard): Regularly scans the infrastructure, identifying vulnerabilities so that the kingdom can shore up its defences before enemies exploit them.

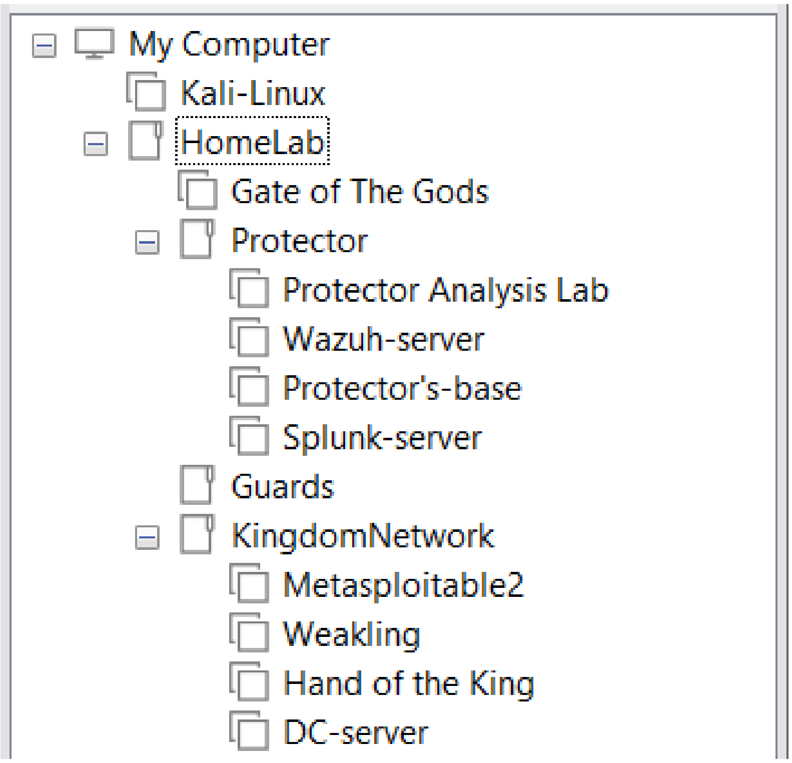
A Living, Evolving Kingdom

The Kingdom grows stronger with every threat it faces. The Gate of the Gods stands resilient, Suricata guards the walls, and Wazuh-server keeps vigilant watch over the entire realm — ensuring no danger goes unnoticed.

At the helm of this ever-evolving digital kingdom is Hardil, the sovereign architect — learning, building, and defending his realm with unwavering dedication.

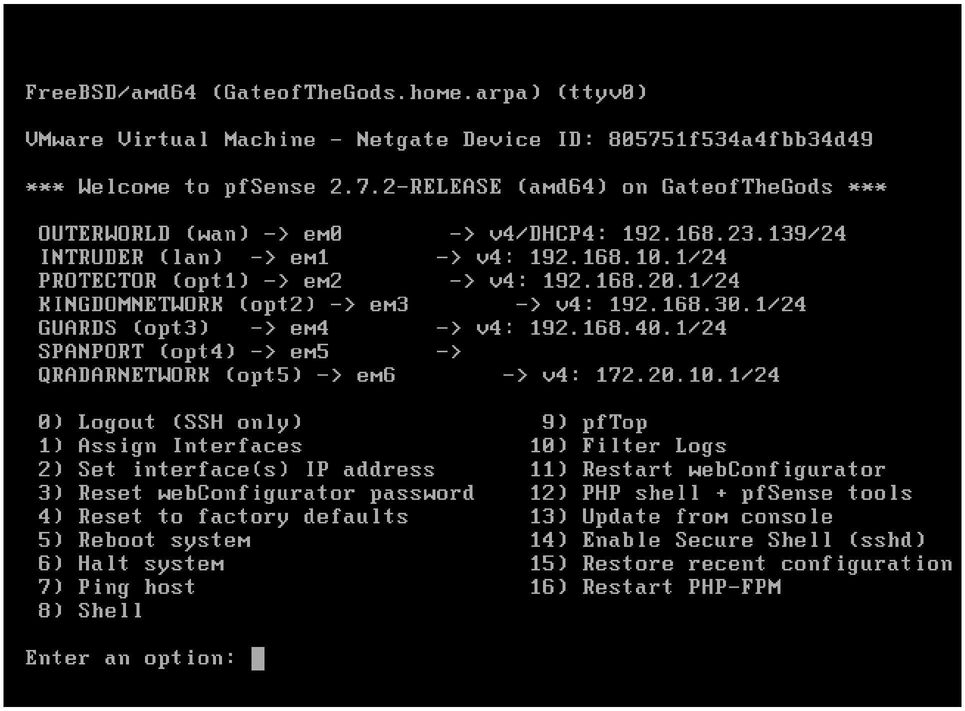
SCREENSHOTS

- **Vmware**



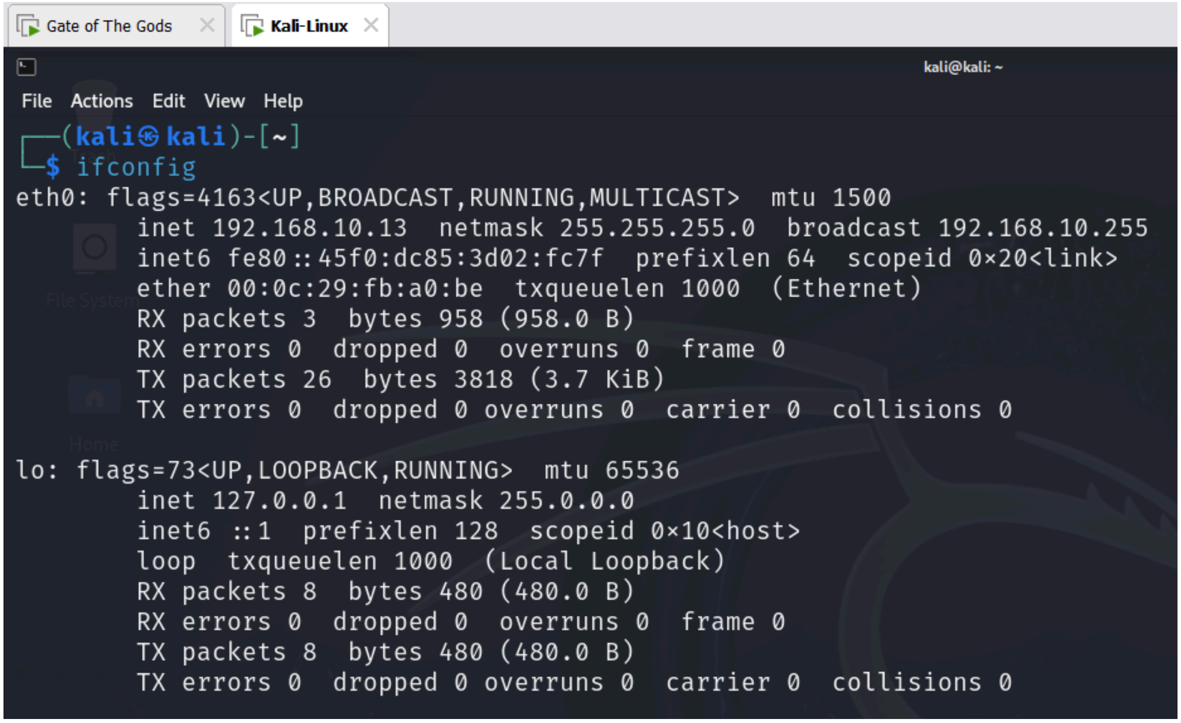
- My Computer
  - Kali-Linux
  - HomeLab
    - Gate of The Gods
    - Protector
      - Protector Analysis Lab
      - Wazuh-server
      - Protector's-base
      - Splunk-server
    - Guards
    - KingdomNetwork
      - Metasploitable2
      - Weakling
      - Hand of the King
      - DC-server

- **Gate of the Gods**



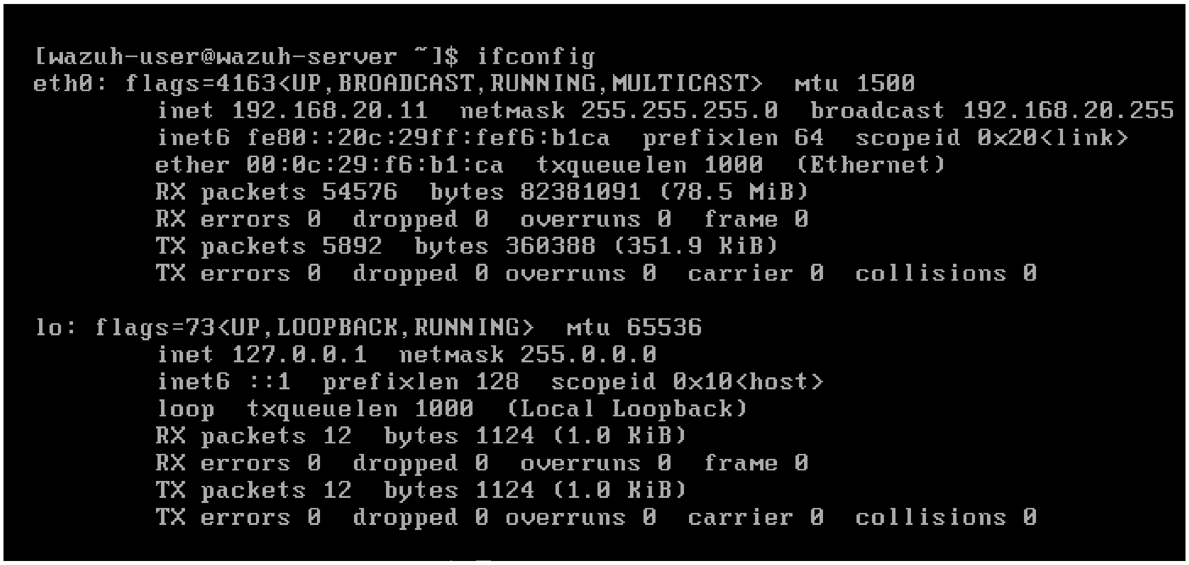
```
FreeBSD/amd64 (GateofTheGods.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 805751f534a4fbb34d49

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on GateofTheGods ***

 OUTERWORLD (wan) -> em0        -> v4/DHCP4: 192.168.23.139/24
 INTRUDER (lan)  -> em1        -> v4: 192.168.10.1/24
 PROTECTOR (opt1) -> em2        -> v4: 192.168.20.1/24
 KINGDOMNETWORK (opt2) -> em3        -> v4: 192.168.30.1/24
 GUARDS (opt3)   -> em4        -> v4: 192.168.40.1/24
 SPANPORT (opt4) -> em5        ->
 QRADARNETWORK (opt5) -> em6        -> v4: 172.20.10.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: █
```

- **Kali-Linux**



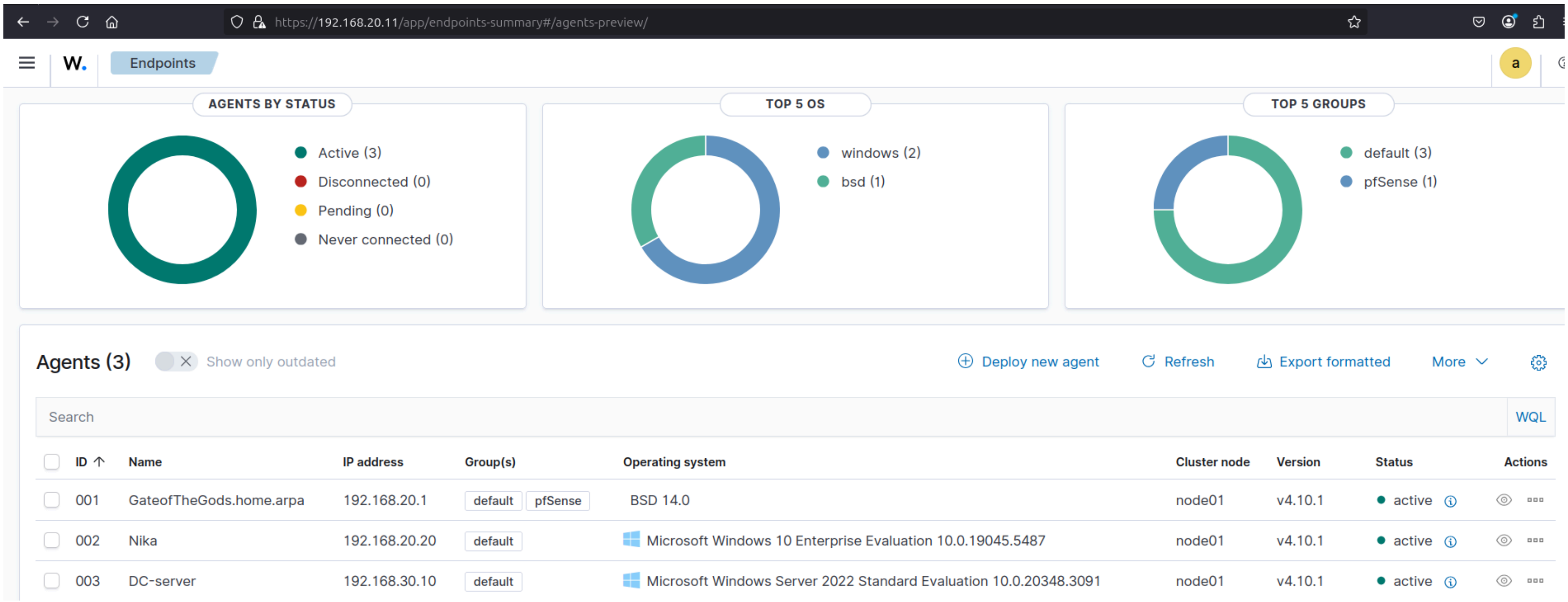
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.13  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::45f0:dc85:3d02:fc7f  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:fb:a0:be  txqueuelen 1000  (Ethernet)
        RX packets 3  bytes 958 (958.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26  bytes 3818 (3.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- **Wazuh-server**



```
[wazuh-user@wazuh-server ~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.20.11  netmask 255.255.255.0  broadcast 192.168.20.255
        inet6 fe80::20c:29ff:fef6:b1ca  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:f6:b1:ca  txqueuelen 1000  (Ethernet)
        RX packets 54576  bytes 82381091 (78.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5892  bytes 360388 (351.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 12  bytes 1124 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 1124 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- **Protector’s Base (Ubuntu machine)**



https://192.168.20.11/app/endpoints-summary#/agents-preview/

W. Endpoints

AGENTS BY STATUS

- ● Active (3)
- ● Disconnected (0)
- ● Pending (0)
- ● Never connected (0)

TOP 5 OS

- ● windows (2)
- ● bsd (1)

TOP 5 GROUPS

- ● default (3)
- ● pfSense (1)

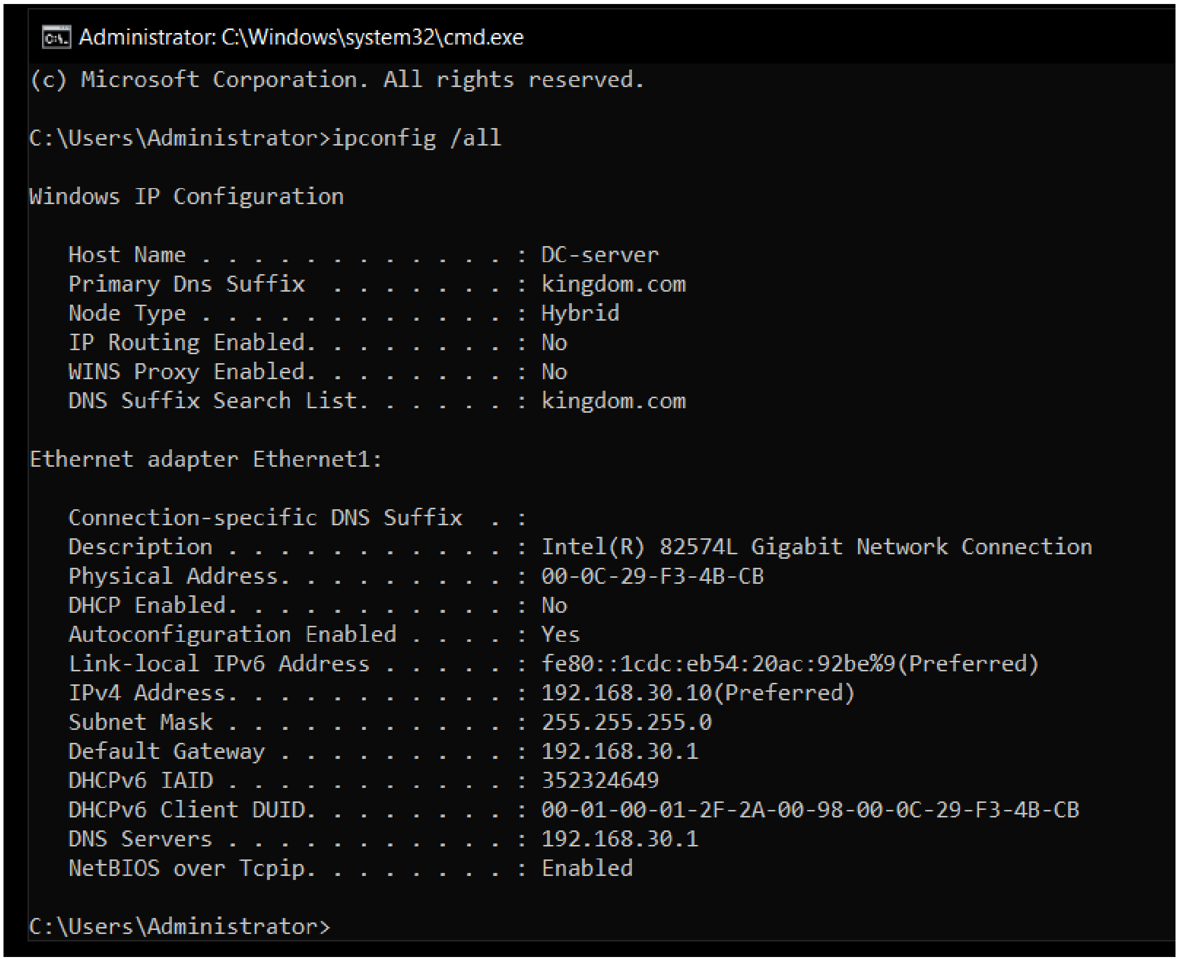
Agents (3) Show only outdated

Deploy new agent | Refresh | Export formatted | More

Search | WQL

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	GateofTheGods.home.arpa	192.168.20.1	default pfSense	BSD 14.0	node01	v4.10.1	● active	
002	Nika	192.168.20.20	default	Microsoft Windows 10 Enterprise Evaluation 10.0.19045.5487	node01	v4.10.1	● active	
003	DC-server	192.168.30.10	default	Microsoft Windows Server 2022 Standard Evaluation 10.0.20348.3091	node01	v4.10.1	● active	

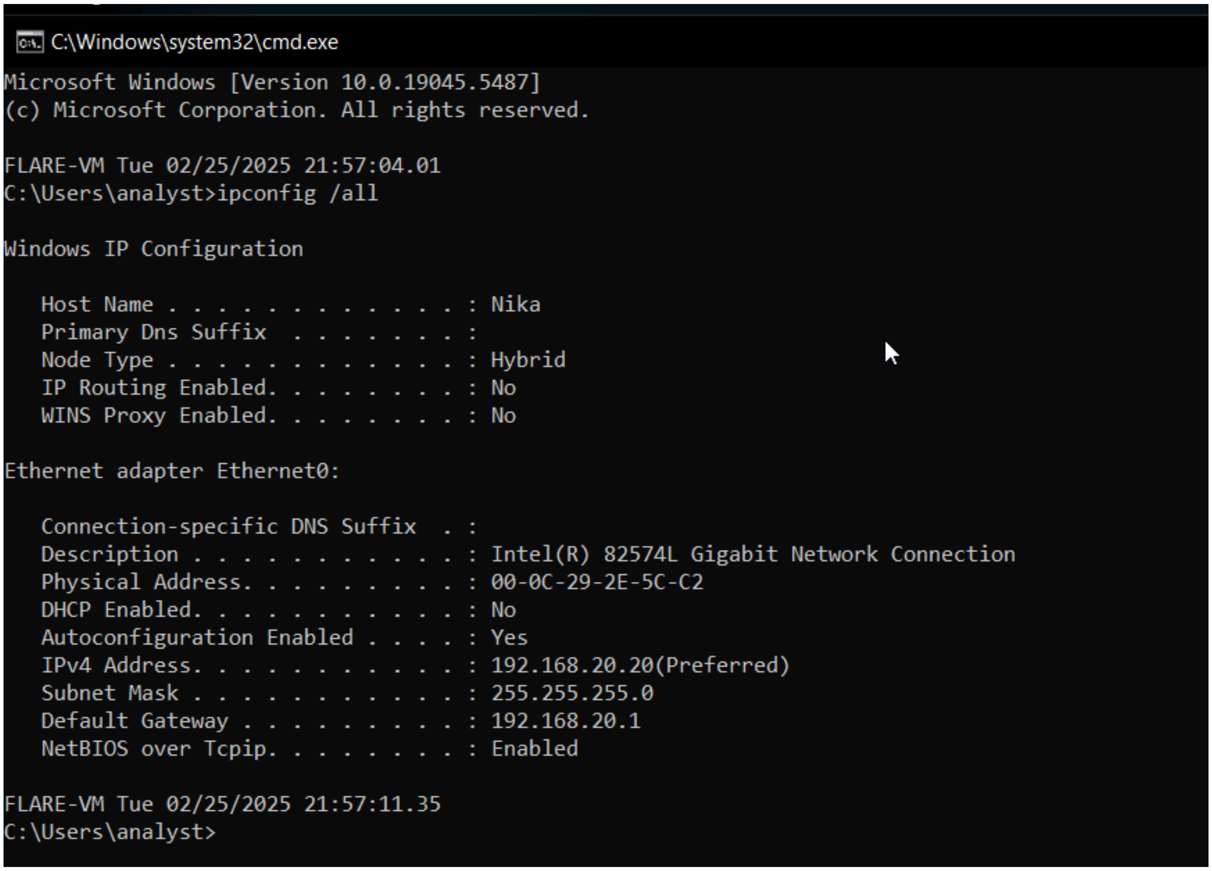
- **DC-server**



Administrator: C:\Windows\system32\cmd.exe

```
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DC-server
   Primary Dns Suffix  . . . . . . . : kingdom.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : kingdom.com

Ethernet adapter Ethernet1:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-F3-4B-CB
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::1cdc:eb54:20ac:92be%9(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.30.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.30.1
   DHCPv6 IAID . . . . . . . . . . . : 352324649
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2F-2A-00-98-00-0C-29-F3-4B-CB
   DNS Servers . . . . . . . . . . . : 192.168.30.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Administrator>
```

- **FlareVM (Nika)**



C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

FLARE-VM Tue 02/25/2025 21:57:04.01
C:\Users\analyst>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Nika
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-2E-5C-C2
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.20.20(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.20.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

FLARE-VM Tue 02/25/2025 21:57:11.35
C:\Users\analyst>
```

`

REFERENCES

FlareVM: https://github.com/mandiant/flare-vm/blob/main/README.md
Windows Server:
https://learn.microsoft.com/en-us/windows-server/get-started/get-started-with-windows-server
Kali-Linux: https://www.kali.org/docs/introduction/what-is-kali-linux/#kali-linux-features
Nessus: https://docs.tenable.com/nessus/10_8/Content/PDF/Nessus_10_8.pdf
pfSense: https://docs.netgate.com/pfsense/en/latest/general/index.html