

11/6/2024

Implementation Report

Secure Solution: Malware Detection

Group G
SEMESTER IV - CYBERSECURITY

Table of Contents

Table of Contents	1
Introduction.....	2
Summary	2
Objectives.....	2
Scope	3
Within Scope	3
Out of Scope.....	3
System Architecture.....	3
Overview.....	3
Diagrams	4
Network Diagram	4
Database Diagram	5
Components	5
Virtual Machines Summary.....	5
Firewalls	8
Antivirus Software.....	8
Host-based Intrusion Detection System (HIDS)	8
Network-based Intrusion Detection System (IDS)	9
Implementation Details.....	9
Setup and Configuration	9
Development Process.....	32
Testing ("Wait for launching the malware")	32
Results	40
References	40

Introduction

Summary

This document outlines the implementation details for a cybersecurity project developed as part of a group effort in a cybersecurity course. The project focuses on creating a secure environment for a hospital setting, drawing inspiration from the 2017 NHS WannaCry ransomware attack. The goal is to design a secure environment and implement security measures to protect hospital networks from similar threats. We aim to ensure the safety of sensitive patient data.

The project leverages a combination of Virtual Machines (VMs) running Linux servers and Windows VPN workspaces. Key components of the secure environment include the deployment of antivirus software, configuration of firewalls with specific rules, and the integration of Host-based Intrusion Detection Systems (HIDS) and Network-based Intrusion Detection Systems (IDS). Through this comprehensive approach, the project aims to demonstrate effective strategies for malware detection and overall network security in a healthcare context.

This document details the setup and configuration processes for each security measure we took. Here, we will be providing instructions regarding the steps we took to create a secure environment. The implementation aims to offer a practical guide for protecting healthcare environments from cyber threats, ensuring both data security and operational continuity.

Objectives

The main objective of this project is to design and implement a complete cybersecurity framework, tailored to a hospital environment. It is inspired by the NHS WannaCry ransomware attack of 2017. The goals we aim to achieve are as follows:

- **Enhance Security:** Establish a multi-layered security architecture to protect a hospital's network infrastructure from malware, ransomware, and other cyber threats.
- **Virtualized Environments:** Set up Virtual Machines to simulate the hospital network, using Linux servers and Windows workspaces that utilize a VPN for remote employees. This will be the base of our implemented solution.
- **Antivirus Solutions:** Implement antivirus software on all stations to ensure malware is detected.
- **Firewalls:** Implement firewalls, then create rules to control network traffic in a manner that prevents unauthorized access.
- **Intrusion Detection Systems:** Implement both Host-based Intrusion Detection Systems (HIDS) and Network-based Intrusion Detection Systems (IDS) to monitor network activity and identify security breaches.
- **Simulated Attack:** Simulate malware being released into the secure environment. This is to test that our solution does what it set out to do: detect and mitigate against malware.
- **Documentation:** Create documentation throughout the process.

Scope

The focus of this project is to design and implement a secure solution to Malware, specifically in a healthcare environment. It involves a comprehensive framework of cybersecurity features. The scope is as follows:

Within Scope

- **Virtual Environment Setup:** Virtual Machines are configured, using Linux servers and Windows workspaces for employees to simulate a hospital environment.
- **Antivirus:** Installation and configuration of antivirus software on all VMs to detect and mitigate malware threats.
- **Firewall Configuration:** Firewall implemented with added rules to prevent unauthorized access.
- **Intrusion Detection Systems:** HIDS and IDS will be deployed to fully monitor network activity.
- **Malware Attack Simulation:** This is essentially for testing our secure solution against malware.

Out of Scope

- **Physical Security Measures:** We are only able to focus on cyber-threats. Details such as securing the actual building and equipment is out of our scope.
- **Employee Training:** While we strongly suggest training your employees to detect phishing attacks and other cyber threats, this is out of our scope.
- **Compliance Certification:** We are not able to get any formal compliance certifications, such as HIPAA certification.

System Architecture

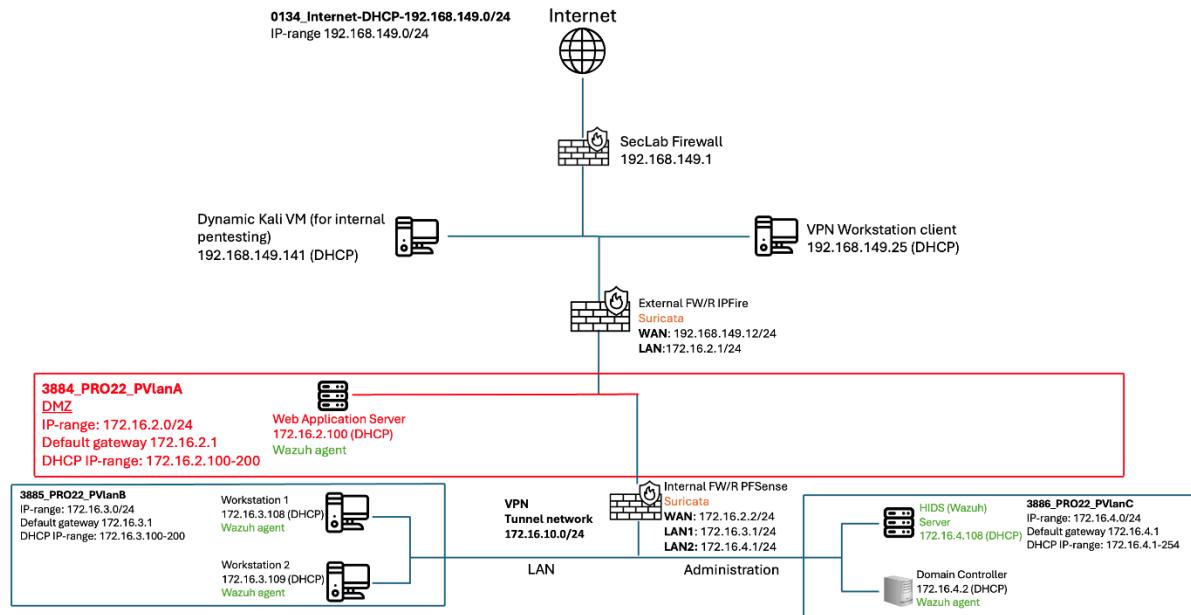
Overview

The system architecture for our cybersecurity project is designed to manufacture a secure environment for a simulated hospital network. The architecture uses a combination of Virtual Machines (VMs) and security tools to replicate a real-world healthcare setting, providing a platform for implementing and testing our chosen cybersecurity measures. This design includes multiple layers of defense and specialized components to ensure the safety of the sensitive data NHS is in possession of.

The system is segmented into several key components, each playing a critical role in the overall security posture. The components are distributed across different VLANs to simulate a realistic network segmentation strategy, improving both security and manageability.

Diagrams

Network Diagram



This is the network diagram we have constructed to simulate our full environment.

Internet-DHCP: 192.168.149.0/24

IP-range: 192.168.149.0/24

SecLab Firewall: 192.168.149.1

Kali VM: 192.168.149.141 (DHCP)

External Firewall FW/R IPFire:

WAN: 192.168.149.12/24

LAN: 172.16.2.1/24

PvlanA:

DMZ

IP-Range: 172.16.2.0/24

Default gateway: 172.16.2.1

DHCP IP_range: 172.16.2.100-200

Web Application Server

172.16.2.100 (DHCP)

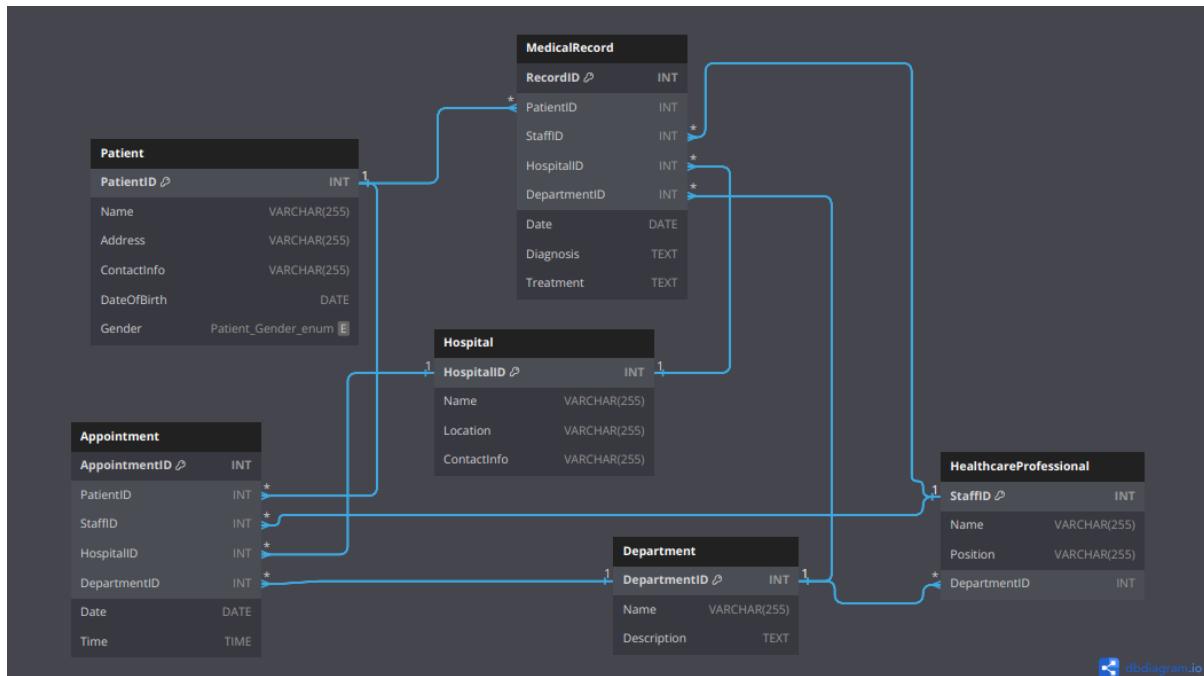
WAF (ModSecurity)

Wazuh Agent

HIDS (Wazuh) Server:
172.16.2.101 (DHCP)

Linux Workstation:
Wazuh Agent
172.16.2.102 (DHCP)

Database Diagram

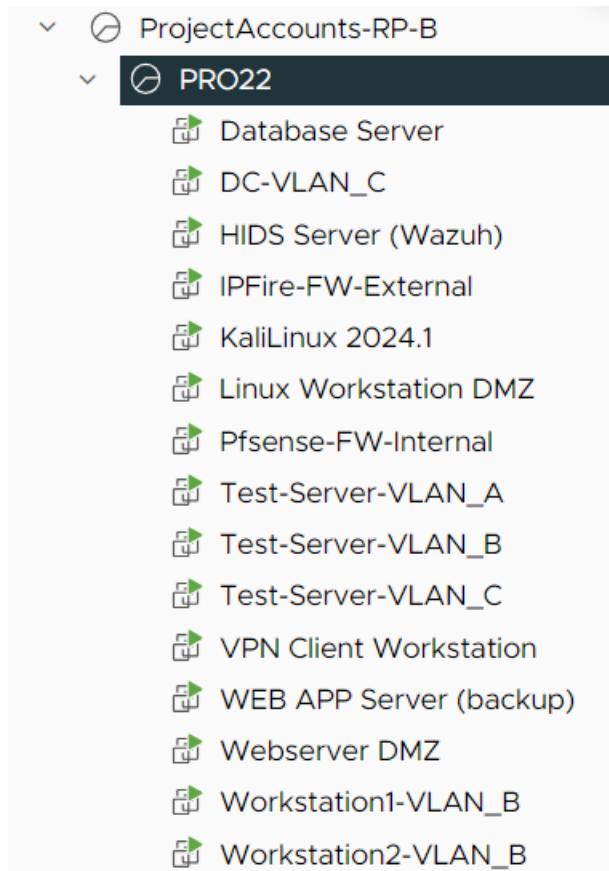


Our proposed database diagram setup for our simulated hospital web application.

Components

Virtual Machines Summary

Here, I will give a breakdown of our entire VM setup and explain the function of each one.



Database Server

- **Purpose:** Hosts the database for the hospital's web application.
- **Technology:** Uses Kubernetes for container orchestration. This exists here to host the web applications database.

DC-VLAN_C

- **Role:** Domain Controller.
- **Technology:** Utilizes Microsoft Windows DNS Server Service for domain name resolution and network management, providing centralized authentication and directory services.

-Group Policies would go here

HIDS Server (Wazuh)

- **Role:** Host-based Intrusion Detection System (HIDS).
- **Technology:** Wazuh, which monitors system integrity, logs, and behaviors to detect and respond to suspicious activities on the hosts.

IPFire-FW-External

- **Role:** External Firewall.
- **Technology:** IPFire, configured to filter incoming and outgoing traffic, protecting the network from external threats. It forms the first line of defense in our two-firewall setup.

Kali Linux 2024.1

- **Role:** Security Workstation.
- **Technology:** A Kali Linux workstation located on the DMZ. This is the machine we can use and move across the whole environment. We are using this for testing the environment.

Pfsense-FW-Internal

- **Role:** Internal Firewall.
- **Technology:** Pfsense, configured to monitor and control internal traffic, ensuring security within the network and providing a second layer of defense.

Test Servers

- **Test-Server-VLAN_A:** Located on private VLAN_A for testing security measures and configurations. May be deleted in the future when they are no longer needed.
- **Test-Server-VLAN_B:** Located on private VLAN_B, another test server. May be deleted in the future when they are no longer needed.
- **Test-Server-VLAN_C:** Located on private VLAN_C, our last test server. May be deleted in the future when they are no longer needed.

VPN Client Workstation

- **Role:** Simulates remote employee access.
- **Technology:** Configured with DHCP and connected via VPN to securely integrate with the hospital's LAN, enabling remote access as if the device were within the internal network.

Webserver DMZ

- **Role:** Main Web Server.
- **Technology:** Hosts the primary web application and is located in the DMZ to segregate it from the internal network, enhancing security by isolating external-facing services.

Workstations (VLAN_B)

- **Workstation1-VLAN_B:** Simulated workstation representing an end-user device within the hospital's internal network.
- **Workstation2-VLAN_B:** Another simulated workstation located on the hospital LAN, used to mimic typical hospital workstations and their interaction with the network.

Firewalls

IPFire

- **Purpose:** Serves as the external firewall in our two-firewall setup.
- **Technology:** IPFire is an open-source firewall solution known for its flexibility and robustness. It filters incoming and outgoing network traffic, protecting the network from unauthorized access and external threats. IPFire supports various security features such as intrusion detection, VPN support, and web proxy, making it an integral part of our network's perimeter defense.

Pfsense

- **Purpose:** Acts as the internal firewall.
- **Technology:** Pfsense is an open-source firewall and router software based on FreeBSD. It provides comprehensive network protection by monitoring and controlling internal traffic, ensuring that only legitimate traffic flows within the network segments. Pfsense includes features like VPN, load balancing, and advanced packet filtering, which help secure the internal network against internal threats and lateral movement of malware.

Antivirus Software

ClamAV

- **Purpose:** Provides antivirus protection for Linux-based systems.
- **Technology:** ClamAV (Clam AntiVirus) is an open-source antivirus engine designed for detecting trojans, viruses, malware, and other malicious threats. It is particularly suited for server environments due to its command-line interface and flexibility in integration with various applications. ClamAV scans files on-demand and can be scheduled to run at regular intervals to ensure continuous protection.

Windows Defender

- **Purpose:** Provides antivirus protection for Windows-based systems.
- **Technology:** Windows Defender is a built-in antivirus and anti-malware solution provided by Microsoft for Windows operating systems. It offers real-time protection, scanning, and removal of various types of malware, including viruses, spyware, and ransomware. Windows Defender integrates seamlessly with the Windows operating system, providing automatic updates and comprehensive security features to protect against evolving threats.

Host-based Intrusion Detection System (HIDS)

Wazuh

- **Purpose:** Provides host-based intrusion detection and security monitoring.
- **Technology:** Wazuh is an open-source security monitoring platform. It provides HIDS functionality, such as log analysis, file integrity monitoring, rootkit detection, and real-time alerts. Wazuh collects and analyzes data from many sources, analysing events to detect suspicious activities and security breaches. It also integrates with various security information and event management (SIEM) systems to provide a unified view of security across the network.

- **Wazuh dashboard should be accessible anywhere on the LAN.**

Network-based Intrusion Detection System (IDS)

Suricata

- **Purpose:** Provides network-based intrusion detection and prevention.
- **Technology:** Suricata is an open-source network IDS, IPS, and network security monitoring engine. It inspects network traffic based on established rules to detect threats. Suricata works in real-time to identify and respond to suspicious activities on the network. It supports deep packet inspection, protocol analysis, and has capabilities to log HTTP, DNS, TLS, and many other protocols, making it a powerful tool for detecting a wide range of network-based attacks.

Implementation Details

Setup and Configuration

This section of the document aims to provide detailed steps for setting up and configuring each component in the environment. The implementation of all the components is based on the following user stories:

Healthcare Provider Staff:

1. As a healthcare provider staff member, I want the system to encrypt patient data in our databases so that confidentiality is maintained, and we comply with privacy regulations.
2. As a healthcare provider staff member, I want the network traffic to be monitored for any suspicious activity or potential security threats so that the IT team can be notified immediately for investigation.

IT Team:

1. As an IT team member, I want the system to update all software and security patches regularly so that vulnerabilities are mitigated, and the risk of exploitation by cyber attackers is minimized, ensuring system security.
2. As an IT team member, I want the system to securely transfer patient data between different healthcare facilities or external partners using encrypted communication protocols so that data breaches during transit are prevented, ensuring patient data privacy.
3. As an IT team member, I want to view a network diagram of the cybersecurity solution so that I can understand how the system is structured and how data is protected.
4. As an IT team member, I want the system to utilize two different firewalls to enhance security measures and safeguard our network.
5. As an IT team member, I want the system to employ a robust system hardening approach to strengthen the security posture of our infrastructure, reducing the risk of vulnerabilities and unauthorized access.

- As an IT team member, I want the system to implement segmentation to create isolated network segments, allowing for granular control over network traffic and minimizing the impact of potential breaches.

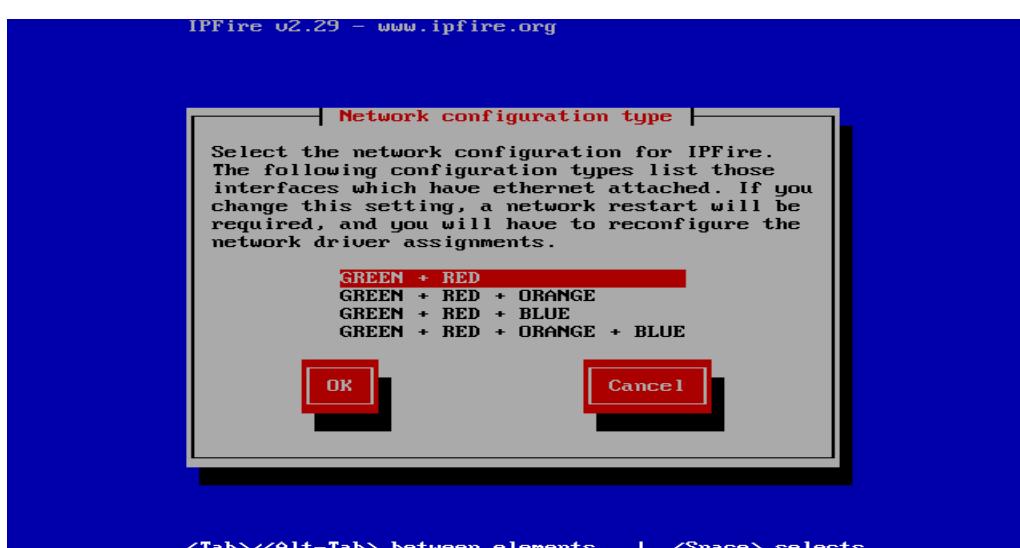
System Administrators:

- As a system administrator, I want the system to conduct regular malware scans on our current software to detect and remove any malicious programs or files, ensuring the integrity and safety of our data.
- As a system administrator, I want the system to include domain controllers to manage user authentication and authorization efficiently, ensuring secure access to network resources and applications.
- As a system administrator, I want the system to deliver good performance to ensure that our critical applications and services run smoothly and efficiently, minimizing downtime and disruptions to our workflow.
- As a system administrator, I want sensitive data to be accessible only on the hospital VLAN to maintain confidentiality and compliance with privacy regulations, preventing unauthorized access from external networks.
- As a system administrator, I want the system to provide endpoint protection to secure devices connected to our network, defending against malware, ransomware, and other cyber threats that may target endpoints.

IPFire

Note: Since IPFire does not exist as a template in the vsphere environment. We had to download it and create it locally and then upload it as OVA format to the vsphere environment.

- Visit IPFire download page and download the appropriate ISO image file.
- Create a VM locally using the downloaded ISO file.
- Convert the created machine to OVA format using a tool called OVFTool.
- Upload the created OVA file to the vsphere environment and deploy it.
- Configure the machine:
 - Setup network interfaces:
 - Green: Internal network interface (Default GW).
 - Red: External network interface.



IPFire_ - ipfire.localdomain

System Status Network Services Firewall IPFire Logs RED Traffic: In 2.60 kbit/s Out 2.88 kbit/s

Main page ⓘ

Network	IP address	Status
INTERNET	192.168.149.12	Connected - (3m 6s)
Hostname:	ipfire.localdomain	
Gateway:	192.168.149.1	

Network	IP address	Status
LAN	172.16.2.1/24	Proxy off

Note
Please enable the fireinfo service.

IPFire 2.29 (x86_64) - Core-Update 185 IPFire.org · Support the IPFire project with your donation

- Configure DHCP for the internal interface:

IPFire_ - ipfire.localdomain

System Status Network Services Firewall IPFire Logs RED Traffic: In 49152 bit/s Out 0.00 bit/s

DHCP configuration ⓘ

DHCP

Green Interface	Enabled: <input checked="" type="checkbox"/>	IP address	172.16.2.1 255.255.255.0
Start address: *	172.16.2.100	Netmask:	172.16.2.200
Deny known clients:	<input type="checkbox"/>	End address: *	
Default lease time (mins): *	60	Max lease time (mins): *	120
Domain name suffix:	localdomain	Allow bootp clients:	<input type="checkbox"/>
Primary DNS: *	172.16.2.1	Secondary DNS:	8.8.8.8
Primary NTP server:		Secondary NTP server:	
Primary WINS server address:		Secondary WINS server address:	
next-server:		filename:	

* Required field

- Configure the external interface to use the Netlab's DHCP:

Note: This interface should not have DHCP enabled to avoid any conflicts.

RED DHCP configuration

Domain	
Gateway	192.168.149.1
Primary DNS:	192.168.200.11
Secondary DNS:	192.168.200.10
DHCP Server	192.168.200.10
Default Lease Time	192 Hours
Default Renewal Time	96 Hours
Maximum Renewal Time	168 Hours

- Add Firewall Rules to allow traffic on ports 443 (Webserver) and 1194 (OpenVPN):

Note: the OpenVPN server is running on the internal firewall (PFsense) and intended for remote employees.

IPFire_ - ipfire.localdomain

System Status Network Services Firewall IPFire Logs

RED Traffic: In 49127 bit/s Out 0.00 bit/s

Firewall Rules

New rule Apply changes

#	Protocol:	Source	Log	Destination	Action
1	ICMP	RED	<input type="checkbox"/>	Any	<input checked="" type="checkbox"/>
2	UDP	Any	<input type="checkbox"/>	Firewall (RED): 1194 ->172.16.2.2: 1194	<input checked="" type="checkbox"/>
3	TCP	Any	<input type="checkbox"/>	RED: SMTP	<input checked="" type="checkbox"/>
4	TCP	Any	<input type="checkbox"/>	Firewall (RED): 443 ->172.16.2.112: 443	<input checked="" type="checkbox"/>
		GREEN		Internet (Allowed)	
					Policy: Allowed

IPFire 2.29 (x86_64) - Core-Update 185 IPFire.org · Support the IPFire project with your donation

- o Setup Intrusion Prevention System with various rulesets to monitor both of the interfaces.

Intrusion Prevention System

Intrusion Prevention System

Intrusion Prevention		
Daemon	RUNNING	Memory
	PID 4668	771600 KB

Settings

Enable Intrusion Prevention System

Monitored Interfaces

Enabled on RED Enabled on GREEN

Save

Ruleset Settings

Provider	Date	Automatic updates	Action
Emergingthreats.net Community Rules	2024-06-11 22:59:41	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Snort/VRT GPLv2 Community Rules	2024-06-11 19:27:08	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ThreatFox Indicators Of Compromise Rules	2024-06-12 18:40:14	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Abuse.ch SSLBL Blacklist Rules	2024-06-12 18:38:41	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Customize ruleset Add provider

IPFire_ - ipfire.localdomain

System Status Network Services Firewall IPFire Logs

RED Traffic: In 110 kbit/s Out 385.02 bit/s

IPS Log Viewer ⓘ

Settings:

Month: June Day: 13 << >> Update Export

Log

Total of number of activated rules for June 13: 345

Older		Newer	
Date:	06/13 01:02:09	Name:	ET INFO DYNAMIC_DNS Query to a *.cloudns.net Domain
Priority:	2	Type:	Potentially Bad Traffic
IP info:	172.16.2.2:57430 -> 45.83.251.16:53		
References:	none found	SID:	2042930
Date:	06/13 01:02:09	Name:	ET INFO DYNAMIC_DNS Query to a *.cloudns.net Domain
Priority:	2	Type:	Potentially Bad Traffic
IP info:	172.16.2.2:5704 -> 185.136.97.77:53		
References:	none found	SID:	2042930
Date:	06/13 01:02:09	Name:	ET INFO DYNAMIC_DNS Query to a *.cloudns.net Domain
Priority:	2	Type:	Potentially Bad Traffic
IP info:	172.16.2.2:56670 -> 185.136.97.77:53		
References:	none found	SID:	2042930
Date:	06/13 01:02:09	Name:	ET INFO DYNAMIC_DNS Query to a *.cloudns.net Domain
Priority:	2	Type:	Potentially Bad Traffic
IP info:	172.16.2.2:58826 -> 185.136.96.11:53		
References:	none found	SID:	2042930
Date:	06/13 01:02:09	Name:	ET INFO DYNAMIC_DNS Query to a *.cloudns.net Domain
Priority:	2	Type:	Potentially Bad Traffic
IP info:	172.16.2.2:25662 -> 185.136.99.11:53		
References:	none found	SID:	2042930
Date:	06/13 01:02:10	Name:	ET INFO DYNAMIC_DNS Query to a *.cloudns.net Domain
Priority:	2	Type:	Potentially Bad Traffic
IP info:	172.16.2.2:34531 -> 185.136.98.88:53		
References:	none found	SID:	2042930

Pfsense

- 1) Deploy Pfsense from a template in the vsphere environment.
- 2) Configure the machine:
 - o Setup network interfaces:
 - WAN: DMZ facing interface.
 - LAN: Employees LAN (where workstations reside).
 - ADMINISTRATION: Where monitoring systems and DC reside.

Interfaces / Interface Assignments

Help ?

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GReS GIFs Bridges LAGGs

Interface

Network port

WAN

vmx0 (00:50:56:97:c2:34)

LAN

vmx1 (00:50:56:97:ac:e0)

Delete

Administration

vmx2 (00:50:56:97:b4:3f)

Delete

- Enable DHCP for the LAN and ADDMINISTRATION interfaces:

Note: The WAN should not have DHCP enabled to avoid any conflicts .

Services / DHCP Server / LAN

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.

WAN LAN ADMINISTRATION

General DHCP Options

DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny Unknown Clients	<input type="button" value="Allow all clients"/>
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.	
Ignore Denied Clients	<input type="checkbox"/> Ignore denied clients rather than reject This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Primary Address Pool

Subnet	172.16.3.0/24
Subnet Range	172.16.3.1 - 172.16.3.254
Address Pool Range	172.16.3.100 From To The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools	<input type="button" value="Add Address Pool"/> If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

Services / DHCP Server / ADMINISTRATION

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.

WAN LAN ADMINISTRATION

General DHCP Options

DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on ADMINISTRATION interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny Unknown Clients	<input type="button" value="Allow all clients"/>
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.	
Ignore Denied Clients	<input type="checkbox"/> Ignore denied clients rather than reject This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Primary Address Pool

Subnet	172.16.4.0/24
Subnet Range	172.16.4.1 - 172.16.4.254
Address Pool Range	172.16.4.100 From To The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools	<input type="button" value="Add Address Pool"/> If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

- o Setup Suricata (IDS/IPS) with varios rule sets to monitor both the LAN and ADMINISTRATION interfaces:

Services / Suricata

Interfaces Global Settings Updates Alerts Blocks Files Pass Lists Suppress Logs View Logs Mgmt SID Mgmt

Sync IP Lists

Interface Settings Overview

Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> LAN (vmx1)		AUTO	DISABLED	LAN	
<input type="checkbox"/> ADMINISTRATION (vmx2)		AUTO	DISABLED	ADMINISTRATION	

Please Choose The Type Of Rules You Wish To Download

Install ETOpen Emerging Threats rules ETOpen is a free open source set of Suricata rules whose coverage is more limited than ETPro.
Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETOpen rules.

Install ETPro Emerging Threats rules ETPro for Suricata offers daily updates and extensive coverage of current malware threats.
The ETPro rules contain all of the ETOpen rules, so the ETOpen rules are not required and are disabled when the ETPro rules are selected. [Sign Up for an ETPro Account](#). Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETPro rules.

Install Snort rules Snort free Registered User or paid Subscriber rules
[Sign Up for a free Registered User Rules Account](#)
[Sign Up for paid Snort Subscriber Rule Set \(by Talos\)](#)
Enabling the custom URL option will force the use of a custom user-supplied URL when downloading Snort Subscriber rules.

Snort Rules Filename
Enter the rules tarball filename (filename only, do not include the URL.)
Example: snortrules-snapshot-29200.tar.gz
DO NOT specify a Snort3 rules file! Snort3 rules are incompatible with Suricata and will break your installation!

Snort Oinkmaster Code
Obtain a snort.org Oinkmaster code and paste it here.

Install Snort GPLv2 Community rules The Snort Community Ruleset is a GPLv2 Talos-certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions.
This ruleset is updated daily and is a subset of the subscriber ruleset. If you are a Snort Subscriber Rules customer (paid subscriber), the community ruleset is already built into your download of the Snort Subscriber rules, and there is no benefit in adding this rule set separately.

Install Feodo Tracker Botnet C2 IP rules The Feodo Botnet C2 IP Ruleset contains Dridex and Emotet/Heodo botnet command and control servers (C&Cs) tracked by Feodo Tracker.

Install ABUSE.ch SSL Blacklist rules The ABUSE.ch SSL Blacklist Ruleset contains the SSL cert fingerprints of all SSL certs blacklisted by ABUSE.ch.

Hide Deprecated Rules Categories Hide deprecated rules categories in the GUI and remove them from the configuration. Default is Not Checked.

Download Extra Rules Download Extra Rules
Download extra rules file or tar.gz archive with rules. If "Check MD5" is set, the code will assume a matching filename exists at the same URL with an additional extension of ".md5".

- Select the desired rules for both of the interfaces:

Services / Suricata / Interface Settings / LAN - Categories

Interfaces Global Settings Updates Alerts Blocks Files Pass Lists Suppress Logs View Logs Mgmt SID Mgmt

Sync IP Lists

LAN Settings LAN Categories LAN Rules LAN Flow/Stream LAN App Parsers LAN Variables LAN IP Rep

Automatic flowbit resolution

Resolve Flowbits Auto-enable rules required for checked flowbits
Default is Checked. Suricata will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

View rules 

Click to view auto-enabled rules required to satisfy flowbit dependencies

Note: Auto-enabled rules generating unwanted alerts should have their GID:SID added to the Suppression List for the interface.

Snort IPS Policy selection

Use IPS Policy Use rules from one of three pre-defined Snort IPS policies
Note: You must be using the Snort rules to use this option.
Selecting this option disables manual selection of Snort rules categories in the list below; although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort rules set.

IPS Policy Selection Maximum Detection
Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as Flash in an Excel file. Maximum Detection encompasses vulnerabilities from 2005 or later with a CVSS score of at least 7.5 along with critical malware and exploit kit rules. The Maximum Detection policy favors detection over rated throughput. In some situations this policy can and will cause significant throughput reductions.

Select the rulesets (Categories) Suricata will load at startup

 - Category is auto-enabled by SID Mgmt conf files
 - Category is auto-disabled by SID Mgmt conf files

Select All Unselect All 

Enabled	Ruleset:				
<input type="checkbox"/>	Feodo Tracker Botnet C2 IP Rules				
<input type="checkbox"/>	ABUSE.ch SSL Blacklist Rules				
Enabled	Ruleset: Default Rules	Enabled	Ruleset: ET Open Rules	Enabled	Ruleset: Snort Text Rules
<input checked="" type="checkbox"/>	app-layer-events.rules	<input type="checkbox"/>	emerging-3coresec.rules	<input type="checkbox"/>	snort_app-detect.rules
<input checked="" type="checkbox"/>	decoder-events.rules	<input type="checkbox"/>	emerging-active.rules	<input type="checkbox"/>	snort_attack-responses.rules
<input checked="" type="checkbox"/>	dhcp-events.rules	<input type="checkbox"/>	emerging-adware_pup.rules	<input type="checkbox"/>	snort_backdoor.rules
<input checked="" type="checkbox"/>	dnp3-events.rules	<input type="checkbox"/>	emerging-attack_response.rules	<input type="checkbox"/>	snort_bad-traffic.rules
<input checked="" type="checkbox"/>	dns-events.rules	<input type="checkbox"/>	emerging-botcc_portgrouped.rules	<input type="checkbox"/>	snort_blacklist.rules
<input checked="" type="checkbox"/>	files.rules	<input type="checkbox"/>	emerging-botcc.rules	<input type="checkbox"/>	snort_botnet-enc.rules
<input checked="" type="checkbox"/>	ftp-events.rules	<input type="checkbox"/>	emerging-chat.rules	<input type="checkbox"/>	snort_browser-chrome.rules
<input checked="" type="checkbox"/>	http-events.rules	<input type="checkbox"/>	emerging-clarmy.rules	<input type="checkbox"/>	snort_browser-firefox.rules
<input checked="" type="checkbox"/>	http2-events.rules	<input type="checkbox"/>	emerging-coalmixer.rules	<input type="checkbox"/>	snort_browser-ie.rules
<input checked="" type="checkbox"/>	ipsec-events.rules	<input type="checkbox"/>	emerging-compromised.rules	<input type="checkbox"/>	snort_browser-other.rules
<input checked="" type="checkbox"/>	kerberos-events.rules	<input type="checkbox"/>	emerging-current_events.rules	<input type="checkbox"/>	snort_browser-plugins.rules
<input checked="" type="checkbox"/>	modbus-events.rules	<input type="checkbox"/>	emerging-deleted.rules	<input type="checkbox"/>	snort_browser-webkit.rules
<input checked="" type="checkbox"/>	mqtt-events.rules	<input type="checkbox"/>	emerging-dns.rules	<input type="checkbox"/>	snort_chat.rules
<input checked="" type="checkbox"/>	nfs-events.rules	<input type="checkbox"/>	emerging-dos.rules	<input type="checkbox"/>	snort_content-replace.rules
<input checked="" type="checkbox"/>	ntp-events.rules	<input type="checkbox"/>	emerging-drop.rules	<input type="checkbox"/>	snort_ddos.rules
<input checked="" type="checkbox"/>	quic-events.rules	<input type="checkbox"/>	emerging-dshield.rules	<input type="checkbox"/>	snort_deleted.rules
<input checked="" type="checkbox"/>	rfb-events.rules	<input type="checkbox"/>	emerging-exploit.rules	<input type="checkbox"/>	snort_dns.rules
<input checked="" type="checkbox"/>	smb-events.rules	<input type="checkbox"/>	emerging-exploit_kit.rules	<input type="checkbox"/>	snort_dos.rules
<input checked="" type="checkbox"/>	smtp-events.rules	<input type="checkbox"/>	emerging-ftp.rules	<input type="checkbox"/>	snort_experimental.rules
<input checked="" type="checkbox"/>	ssh-events.rules	<input type="checkbox"/>	emerging-games.rules	<input type="checkbox"/>	snort_exploit-kit.rules
<input checked="" type="checkbox"/>	stream-events.rules	<input type="checkbox"/>	emerging-hunting.rules	<input type="checkbox"/>	snort_exploit.rules
<input checked="" type="checkbox"/>	tls-events.rules	<input type="checkbox"/>	emerging-icmp.rules	<input type="checkbox"/>	snort_file-executable.rules
		<input type="checkbox"/>	emerging-icmp_info.rules	<input type="checkbox"/>	snort_file-flash.rules
		<input type="checkbox"/>	emerging-imap.rules	<input type="checkbox"/>	snort_file-identify.rules
		<input type="checkbox"/>	emerging-inappropriate.rules	<input type="checkbox"/>	snort_file-image.rules
		<input type="checkbox"/>	emerging-info.rules	<input type="checkbox"/>	snort_file-java.rules
		<input type="checkbox"/>	emerging-jav3.rules	<input type="checkbox"/>	snort_file-multimedia.rules
		<input type="checkbox"/>	emerging-malware.rules	<input type="checkbox"/>	snort_file-office.rules
		<input type="checkbox"/>	emerging-misc.rules	<input type="checkbox"/>	snort_file-other.rules
		<input type="checkbox"/>	emerging-mobile_malware.rules	<input type="checkbox"/>	snort_file-pdf.rules
		<input type="checkbox"/>	emerging-netbios.rules	<input type="checkbox"/>	snort_finger.rules
		<input type="checkbox"/>	emerging-p2p.rules	<input type="checkbox"/>	snort_ftp.rules
		<input type="checkbox"/>	emerging-phishing.rules	<input type="checkbox"/>	snort_icmp-info.rules

Interfaces Global Settings Updates Alerts Blocks Files Pass Lists Suppress Logs View Logs Mgmt SID Mgmt

Sync IP Lists

ADMIN Settings ADMIN Categories ADMIN Rules ADMIN Flow/Stream ADMIN App Parsers ADMIN Variables ADMIN IP Rep

Automatic flowbit resolution

Resolve Flowbits

Auto-enable rules required for checked flowbits
Default is Checked. Suricata will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

View rules



Click to view auto-enabled rules required to satisfy flowbit dependencies

Note: Auto-enabled rules generating unwanted alerts should have their GID:SID added to the Suppression List for the interface.

Snort IPS Policy selection

Use IPS Policy Use rules from one of three pre-defined Snort IPS policies

Note: You must be using the Snort rules to use this option.
Selecting this option disables manual selection of Snort rules categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort rules set.

Select the rulesets (Categories) Suricata will load at startup

- Category is auto-enabled by SID Mgmt conf files
 - Category is auto-disabled by SID Mgmt conf files

Select All Unselect All

Enabled

Ruleset:

Enabled	Ruleset: Default Rules	Enabled	Ruleset: ET Open Rules	Enabled	Ruleset: Snort Text Rules
<input type="checkbox"/>	Feodo Tracker Botnet C2 IP Rules				
<input type="checkbox"/>	ABUSE.ch SSL Blacklist Rules				
<input checked="" type="checkbox"/>	app-layer-events.rules	<input type="checkbox"/>	emerging-3coresec.rules	<input checked="" type="checkbox"/>	snort_app-detect.rules
<input checked="" type="checkbox"/>	decoder-events.rules	<input type="checkbox"/>	emerging-activex.rules	<input type="checkbox"/>	snort_attack-responses.rules
<input checked="" type="checkbox"/>	dhcp-events.rules	<input type="checkbox"/>	emerging-activex_pup.rules	<input type="checkbox"/>	snort_backdoor.rules
<input checked="" type="checkbox"/>	dnp3-events.rules	<input type="checkbox"/>	emerging-attack_response.rules	<input type="checkbox"/>	snort_bad-traffic.rules
<input checked="" type="checkbox"/>	dns-events.rules	<input type="checkbox"/>	emerging-botcc.portgrouped.rules	<input checked="" type="checkbox"/>	snort_blacklist.rules
<input checked="" type="checkbox"/>	files.rules	<input type="checkbox"/>	emerging-botcc.rules	<input type="checkbox"/>	snort_botnet-cnc.rules
<input checked="" type="checkbox"/>	ftp-events.rules	<input type="checkbox"/>	emerging-chat.rules	<input checked="" type="checkbox"/>	snort_browser-chrome.rules
<input checked="" type="checkbox"/>	http-events.rules	<input type="checkbox"/>	emerging-clammy.rules	<input checked="" type="checkbox"/>	snort_browser-firefox.rules
<input checked="" type="checkbox"/>	http2-events.rules	<input type="checkbox"/>	emerging-columnizer.rules	<input checked="" type="checkbox"/>	snort_browser-ie.rules
<input checked="" type="checkbox"/>	ipsec-events.rules	<input type="checkbox"/>	emerging-compromised.rules	<input checked="" type="checkbox"/>	snort_browser-other.rules
<input checked="" type="checkbox"/>	kerberos-events.rules	<input type="checkbox"/>	emerging-current_events.rules	<input checked="" type="checkbox"/>	snort_browser-plugins.rules
<input checked="" type="checkbox"/>	modbus-events.rules	<input type="checkbox"/>	emerging-deleted.rules	<input checked="" type="checkbox"/>	snort_browser-webkit.rules
<input checked="" type="checkbox"/>	mqtt-events.rules	<input type="checkbox"/>	emerging-dns.rules	<input type="checkbox"/>	snort_chat.rules
<input checked="" type="checkbox"/>	nfo-events.rules	<input type="checkbox"/>	emerging-dos.rules	<input checked="" type="checkbox"/>	snort_content-replace.rules
<input checked="" type="checkbox"/>	ntp-events.rules	<input type="checkbox"/>	emerging-drop.rules	<input type="checkbox"/>	snort_ddos.rules
<input checked="" type="checkbox"/>	quic-events.rules	<input type="checkbox"/>	emerging-dshield.rules	<input checked="" type="checkbox"/>	snort_deleted.rules
<input checked="" type="checkbox"/>	rtb-events.rules	<input type="checkbox"/>	emerging-exploit.rules	<input type="checkbox"/>	snort_dns.rules
<input checked="" type="checkbox"/>	smb-events.rules	<input type="checkbox"/>	emerging-exploit_kit.rules	<input type="checkbox"/>	snort_dos.rules
<input checked="" type="checkbox"/>	smtp-events.rules	<input type="checkbox"/>	emerging-ftp.rules	<input type="checkbox"/>	snort_experimental.rules
<input checked="" type="checkbox"/>	ssh-events.rules	<input type="checkbox"/>	emerging-games.rules	<input checked="" type="checkbox"/>	snort_exploit-kit.rules
<input checked="" type="checkbox"/>	stream-events.rules	<input type="checkbox"/>	emerging-hunting.rules	<input type="checkbox"/>	snort_exploit.rules
<input checked="" type="checkbox"/>	tls-events.rules	<input type="checkbox"/>	emerging-icmp.rules	<input checked="" type="checkbox"/>	snort_file-executable.rules
		<input type="checkbox"/>	emerging-icmp_info.rules	<input checked="" type="checkbox"/>	snort_file-flash.rules
		<input type="checkbox"/>	emerging-imap.rules	<input checked="" type="checkbox"/>	snort_file-identify.rules
		<input type="checkbox"/>	emerging-inappropriate.rules	<input checked="" type="checkbox"/>	snort_file-image.rules
		<input type="checkbox"/>	emerging-info.rules	<input checked="" type="checkbox"/>	snort_file-java.rules
		<input type="checkbox"/>	emerging-jab.rules	<input checked="" type="checkbox"/>	snort_file-multimedia.rules
		<input type="checkbox"/>	emerging-malware.rules	<input checked="" type="checkbox"/>	snort_file-office.rules
		<input type="checkbox"/>	emerging-misc.rules	<input checked="" type="checkbox"/>	snort_file-other.rules
		<input type="checkbox"/>	emerging-mobile_malware.rules	<input checked="" type="checkbox"/>	snort_file-pdf.rules
		<input type="checkbox"/>	emerging-netbios.rules	<input type="checkbox"/>	snort_finger.rules
		<input type="checkbox"/>	emerging-p2p.rules	<input type="checkbox"/>	snort_ftp.rules
		<input type="checkbox"/>	emerging-phishing.rules	<input type="checkbox"/>	snort_icmp-info.rules
		<input type="checkbox"/>	emerging-policy.rules	<input type="checkbox"/>	snort_icmp.rules
		<input type="checkbox"/>	emerging-pop3.rules	<input type="checkbox"/>	snort_imap.rules
		<input type="checkbox"/>	emerging-rpc.rules	<input checked="" type="checkbox"/>	snort_indicator-compromise.rules
		<input type="checkbox"/>	emerging-scada.rules	<input checked="" type="checkbox"/>	snort_indicator-obfuscation.rules

- Firewall rules are configured for each interface based on the services running in the environment, with the purpose of each rule noted in the description section:

[Firewall / Rules / WAN](#)

Floating **WAN** LAN ADMINISTRATION OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> ✓ 2/56.23 MIB	IPv4 TCP	*	*	172.16.4.108	1514	*	none		NAT Wazuh Rule	
<input type="checkbox"/> ✓ 0/28 KIB	IPv4 TCP	*	*	172.16.4.108	1515	*	none		NAT Wazuh Rule	
<input type="checkbox"/> ✓ 0/0 B	IPv4 TCP	*	*	172.16.4.108	55000	*	none		NAT Wazuh Rule	
<input type="checkbox"/> ✓ 0/83.79 MIB	IPv4 TCP	*	*	172.16.4.108	443 (HTTPS)	*	none		NAT Wazuh Dashboard (Temporary Rule)	
<input type="checkbox"/> ✓ 1/115.99 MIB	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN wizard	

Add Add Delete Toggle Copy Save Separator

[Firewall / Rules / LAN](#)

Floating **WAN** LAN ADMINISTRATION OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/0 B	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	
<input type="checkbox"/> ✓ 0/54.92 MIB	IPv4 TCP	*	*	172.16.4.108	443 (HTTPS)	*	none		Wazuh Dashboard (Temporary Rule)	
<input type="checkbox"/> ✓ 2/55.10 MIB	IPv4 TCP	*	*	172.16.4.108	1514	*	none		Wazuh Rule	
<input type="checkbox"/> ✓ 0/6 KIB	IPv4 TCP	*	*	172.16.4.108	1515	*	none		Wazuh Rule	
<input type="checkbox"/> ✓ 0/0 B	IPv4 TCP	*	*	172.16.4.108	55000	*	none		Wazuh Rule	
<input type="checkbox"/> ✓ 0/1.01 MIB	IPv4 TCP/UDP	LAN subnets	*	ADMINISTRATION subnets	445 (MS DS)	*	none		DC Rule	
<input type="checkbox"/> ✓ 0/633 KIB	IPv4 TCP/UDP	LAN subnets	*	ADMINISTRATION subnets	88	*	none		DC Rule	
<input type="checkbox"/> ✓ 0/817 KIB	IPv4 TCP/UDP	LAN subnets	*	ADMINISTRATION subnets	53 (DNS)	*	none		DC Rule	
<input type="checkbox"/> ✓ 0/0 B	IPv4 TCP	LAN subnets	*	ADMINISTRATION subnets	3269	*	none		DC Rule	
<input type="checkbox"/> ✓ 0/0 B	IPv4 TCP	LAN subnets	*	ADMINISTRATION subnets	3268	*	none		DC Rule	
<input type="checkbox"/> ✓ 0/0 B	IPv4 TCP	LAN subnets	*	ADMINISTRATION subnets	636 (LDAP/S)	*	none		DC Rule	
<input type="checkbox"/> ✓ 0/890 KIB	IPv4 TCP/UDP	LAN subnets	*	ADMINISTRATION subnets	389 (LDAP)	*	none		DC Rule	
<input type="checkbox"/> ✓ 0/26.32 MIB	IPv4 TCP	LAN subnets	*	ADMINISTRATION subnets	49152 - 65535	*	none		DC Rule	
<input type="checkbox"/> ✓ 0/0 B	IPv4 TCP/UDP	LAN subnets	*	ADMINISTRATION subnets	464	*	none		DC Rule	
<input type="checkbox"/> ✓ 0/121 KIB	IPv4 TCP	LAN subnets	*	ADMINISTRATION subnets	135	*	none		DC Rule	
<input type="checkbox"/> ✓ 0/17 KIB	IPv4 UDP	LAN subnets	*	ADMINISTRATION subnets	123 (NTP)	*	none		DC Rule	
<input type="checkbox"/> ✗ 0/13 KIB	IPv4 *	LAN subnets	*	ADMINISTRATION subnets	*	*	none		Block any traffic from LAN to Administration	
<input type="checkbox"/> ✓ 6/5.09 GiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/> ✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	ADMINISTRATION subnets	*	*	49152 - 65535	*	none		Ephemeral Ports (Wazuh & DC)	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP/UDP	ADMINISTRATION subnets	*	LAN subnets	445 (MS DS)	*	none		DC Rule	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP/UDP	ADMINISTRATION subnets	*	LAN subnets	88	*	none		DC Rule	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP/UDP	ADMINISTRATION subnets	*	LAN subnets	53 (DNS)	*	none		DC Rule	
<input type="checkbox"/>	✗ 0/676 B	IPv4 *	ADMINISTRATION subnets	*	LAN subnets	*	*	none		Block any traffic from Administration to LAN	
<input type="checkbox"/>	✓ 4/2.20 GiB	IPv4 *	ADMINISTRATION subnets	*	*	*	*	none		Allow Administration subnet to any rule	
<input type="checkbox"/>	✓ 0/681 KiB	IPv6 *	*	*	*	*	*	none		Allow Administration subnet IPv6 to any rule	

- In setting up OpenVPN on pfSense for secure remote access, the process involves creating a Certificate Authority (CA), configuring the OpenVPN server, setting up user authentication, and applying necessary firewall rules.

OpenVPN Servers		Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	172.16.10.0/24			Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits		 

Endpoint Configuration	
Protocol	UDP on IPv4 only
Interface	WAN
The interface or Virtual IP address where OpenVPN will receive client connections.	
Local port	1194
The port used by OpenVPN to receive client connections.	

- Grant Access to the DMZ and LAN subnets:

Tunnel Settings	
IPv4 Tunnel Network	172.16.10.0/24 
<p>This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.</p> <p>A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.</p>	
IPv6 Tunnel Network	<input type="text"/>
<p>This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.</p>	
Redirect IPv4 Gateway	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)	172.16.3.0/24,172.16.2.0/24 
<p>IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.</p>	

- Install the client export package and create an account for every team member:

OpenVPN Clients		
User	Certificate Name	Export
AL-WALEED	AL-WALEED Cert	<ul style="list-style-type: none"> - Inline Configurations: <ul style="list-style-type: none">  More Clients   OpenVPN Connect (iOS/Android) - Bundled Configurations: <ul style="list-style-type: none">  Archive  - Current Windows Installers (2.6.7-ix001): <ul style="list-style-type: none">  64-bit  - Previous Windows Installers (2.5.9-ix001): <ul style="list-style-type: none">  64-bit  - Legacy Windows Installers (2.4.12-ix001): <ul style="list-style-type: none">  10/2014/2015  - Mobility (Mac OS X and Windows): <ul style="list-style-type: none">  Mac  - Vocabulary Bundle  - Vocabulary file Config
Aleksander	Aleks Cert	<ul style="list-style-type: none"> - Inline Configurations: <ul style="list-style-type: none">  More Clients   OpenVPN Connect (iOS/Android) - Bundled Configurations: <ul style="list-style-type: none">  Archive  - Current Windows Installers (2.6.7-ix001): <ul style="list-style-type: none">  64-bit  - Previous Windows Installers (2.5.9-ix001): <ul style="list-style-type: none">  64-bit  - Legacy Windows Installers (2.4.12-ix001): <ul style="list-style-type: none">  10/2014/2015  - Mobility (Mac OS X and Windows): <ul style="list-style-type: none">  Mac  - Vocabulary Bundle  - Vocabulary file Config
Brandie	Brandie Cert	<ul style="list-style-type: none"> - Inline Configurations: <ul style="list-style-type: none">  More Clients   OpenVPN Connect (iOS/Android) - Bundled Configurations: <ul style="list-style-type: none">  Archive  - Current Windows Installers (2.6.7-ix001): <ul style="list-style-type: none">  64-bit  - Previous Windows Installers (2.5.9-ix001): <ul style="list-style-type: none">  64-bit  - Legacy Windows Installers (2.4.12-ix001): <ul style="list-style-type: none">  10/2014/2015  - Mobility (Mac OS X and Windows): <ul style="list-style-type: none">  Mac  - Vocabulary Bundle  - Vocabulary file Config
Divesh	Divesh Cert	<ul style="list-style-type: none"> - Inline Configurations: <ul style="list-style-type: none">  More Clients   OpenVPN Connect (iOS/Android) - Bundled Configurations: <ul style="list-style-type: none">  Archive  - Current Windows Installers (2.6.7-ix001): <ul style="list-style-type: none">  64-bit  - Previous Windows Installers (2.5.9-ix001): <ul style="list-style-type: none">  64-bit  - Legacy Windows Installers (2.4.12-ix001): <ul style="list-style-type: none">  10/2014/2015  - Mobility (Mac OS X and Windows): <ul style="list-style-type: none">  Mac  - Vocabulary Bundle  - Vocabulary file Config
Thomas	Thomas Cert	<ul style="list-style-type: none"> - Inline Configurations: <ul style="list-style-type: none">  More Clients   OpenVPN Connect (iOS/Android) - Bundled Configurations: <ul style="list-style-type: none">  Archive  - Current Windows Installers (2.6.7-ix001): <ul style="list-style-type: none">  64-bit  - Previous Windows Installers (2.5.9-ix001): <ul style="list-style-type: none">  64-bit  - Legacy Windows Installers (2.4.12-ix001): <ul style="list-style-type: none">  10/2014/2015  - Mobility (Mac OS X and Windows): <ul style="list-style-type: none">  Mac  - Vocabulary Bundle  - Vocabulary file Config
Yasen	Yasen Cert	<ul style="list-style-type: none"> - Inline Configurations: <ul style="list-style-type: none">  More Clients   OpenVPN Connect (iOS/Android) - Bundled Configurations: <ul style="list-style-type: none">  Archive  - Current Windows Installers (2.6.7-ix001): <ul style="list-style-type: none">  64-bit  - Previous Windows Installers (2.5.9-ix001): <ul style="list-style-type: none">  64-bit  - Legacy Windows Installers (2.4.12-ix001): <ul style="list-style-type: none">  10/2014/2015  - Mobility (Mac OS X and Windows): <ul style="list-style-type: none">  Mac  - Vocabulary Bundle  - Vocabulary file Config

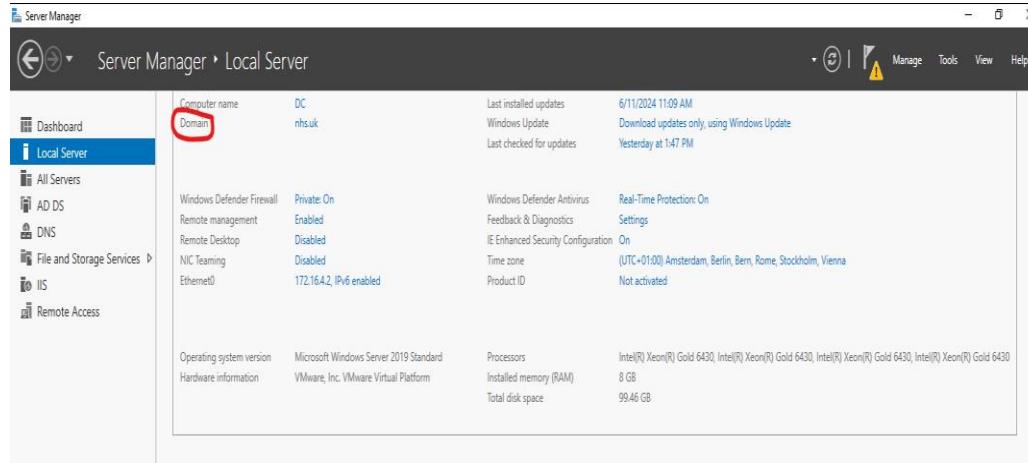
Domain Controller

Note: the Domain Controller serves as a DNS server and offers directory services, while DHCP functionality is handled by the firewalls.

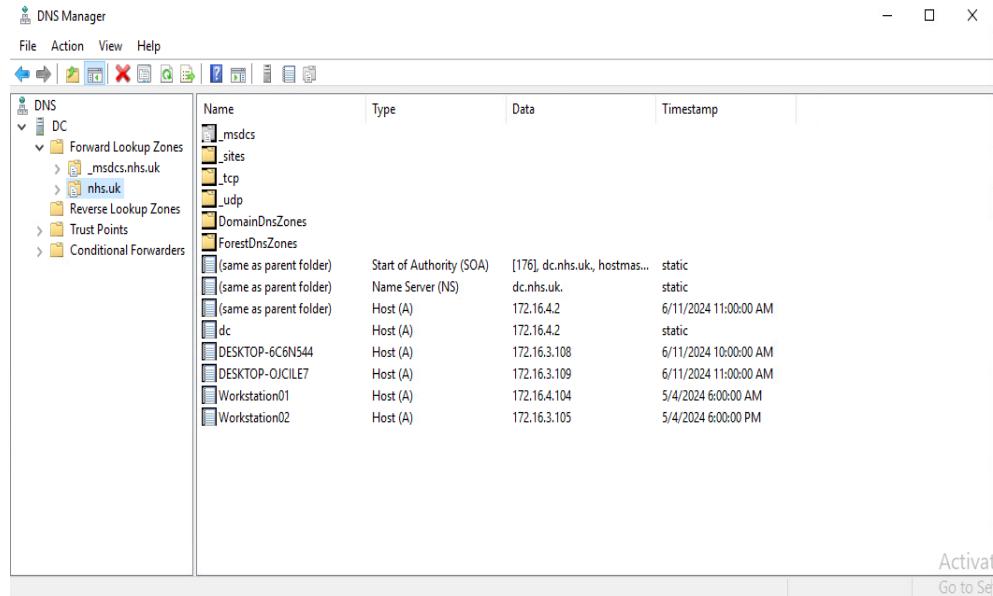
- 1) Deploy Windows server from a template in the vsphere environment.

2) Promote server to Domain Controller:

- Open Server Manager.
- Click on Add roles and features.
- Select Active Directory Domain Services and install it.
- Promote the server to domain controller using the Active Directory Domain Services Configuration Wizard, after installation.



3) Configure DNS by ensuring that the DNS Server role is selected during setup.



4) Manage Active Directory Users and Computers:

- Added Workstations and User(s):

Note: crossed out computers were deleted.

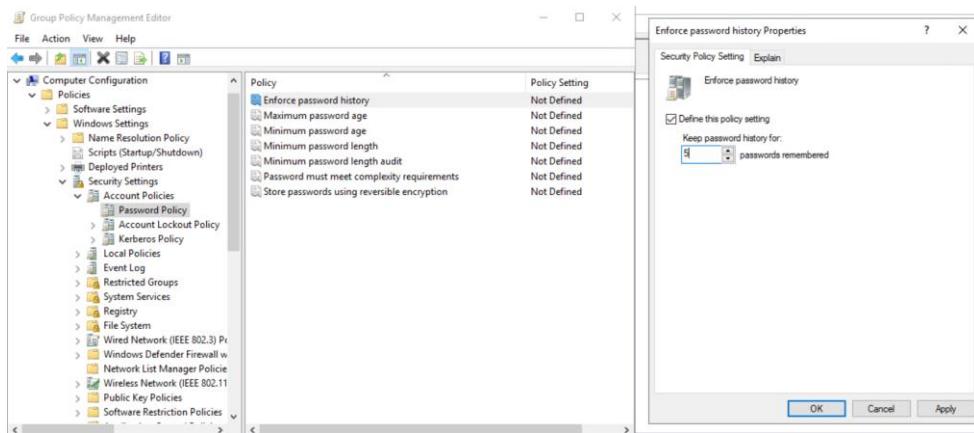
The screenshot shows the 'Active Directory Users and Computers' snap-in. The left pane displays a tree view of the 'nhs.uk' domain, including 'Saved Queries', 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipals', 'Managed Service Accounts', and 'Users'. The 'Computers' node is expanded, showing four computer objects: 'WORKSTATION001', 'WORKSTATION002', 'DESKTOP-OICILE7', and 'DESKTOP-6C6N544'. The right pane lists these four computers in a table with columns for 'Name', 'Type', and 'Description'. Below the table, there is a message: 'Activate Windows Go to Settings to activate Windows.'

Name	Type	Description
WORKSTATION001	Computer	
WORKSTATION002	Computer	
DESKTOP-OICILE7	Computer	
DESKTOP-6C6N544	Computer	

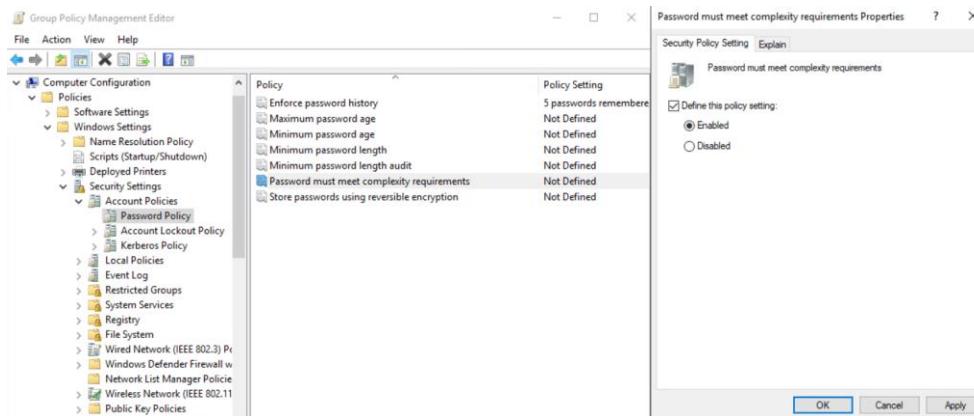
This screenshot shows the same 'Active Directory Users and Computers' interface. The 'Groups' container under 'nhs.uk' is selected in the left pane. The right pane displays a large list of security groups, each with its name, type, and a brief description. The groups listed include: Student, Schema Admins, Read-only Domain Controllers, RAS and IAS Servers, Protected Users, Key Admins, Guest, Group Policy Creator Owners, Enterprise Read-only Domain Controllers, Enterprise Key Admins, Enterprise Admins, Domain Users, Domain Guests, Domain Controllers, Domain Computers, Domain Admins, DnsUpdateProxy, DnsAdmin, Denied RODC Password Replication Group, Cloneable Domain Controllers, Cert Publishers, Al-waleed A.A, Al-sheriyani, Allowed RODC Password Replication Group, and Administrator. Below the list, there is a message: 'Activate Windows Go to Settings to activate Windows.'

Group Policies on Domain Controller

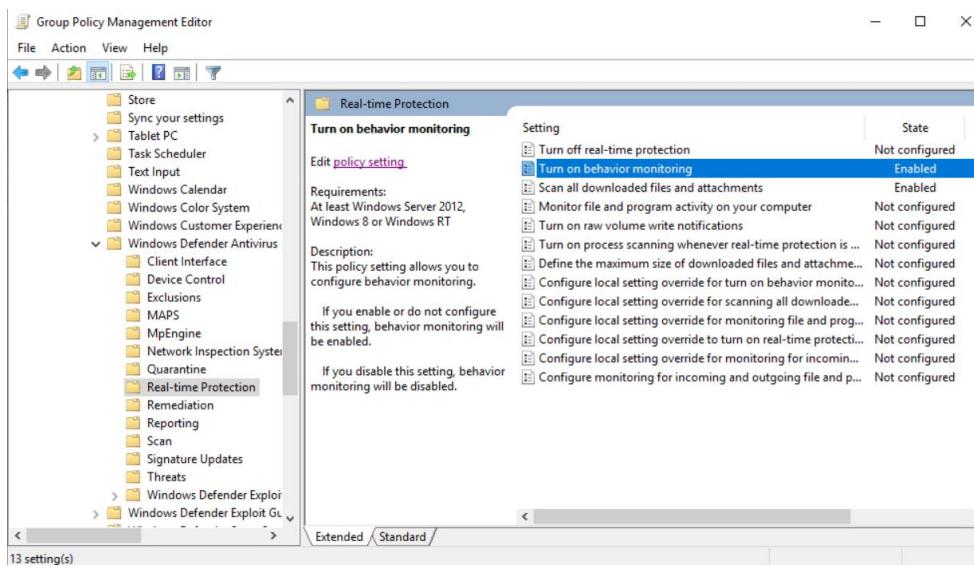
- 1) Deploy the domain controller machine.
- 2) Open Windows Server Management.
- 3) Select “Tools” in the upper right corner.
From the drop-down menu, select Group policy management.
- 4) Open the document tree labeled “Forest: nhs.uk”, “Domains”, “nhs.uk”, and then select Group Policy Objects.
- 5) Right click inside Group Policy management and create new. The one I am creating is titled “NHS Security Policy”.
- 6) Right click on “NHS Security Policy” and select “Edit”.
- 7) Navigate to the appropriate sections and enable the rules you wish to implement.
- 8) Enforce password history to keep password history for the past 5 passwords.



9) Make password complexity a requirement.

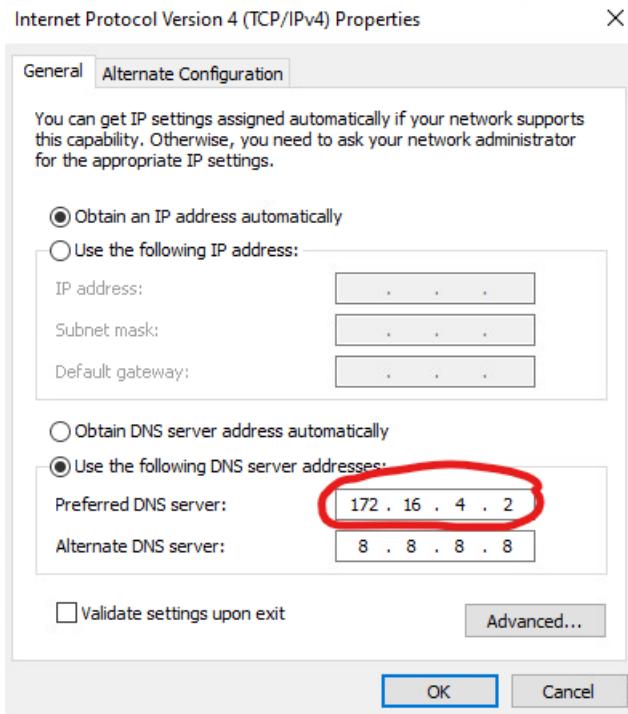


10) Ensure real-time protection is on, scan all downloaded files and attachments, and turn on behavior monitoring.

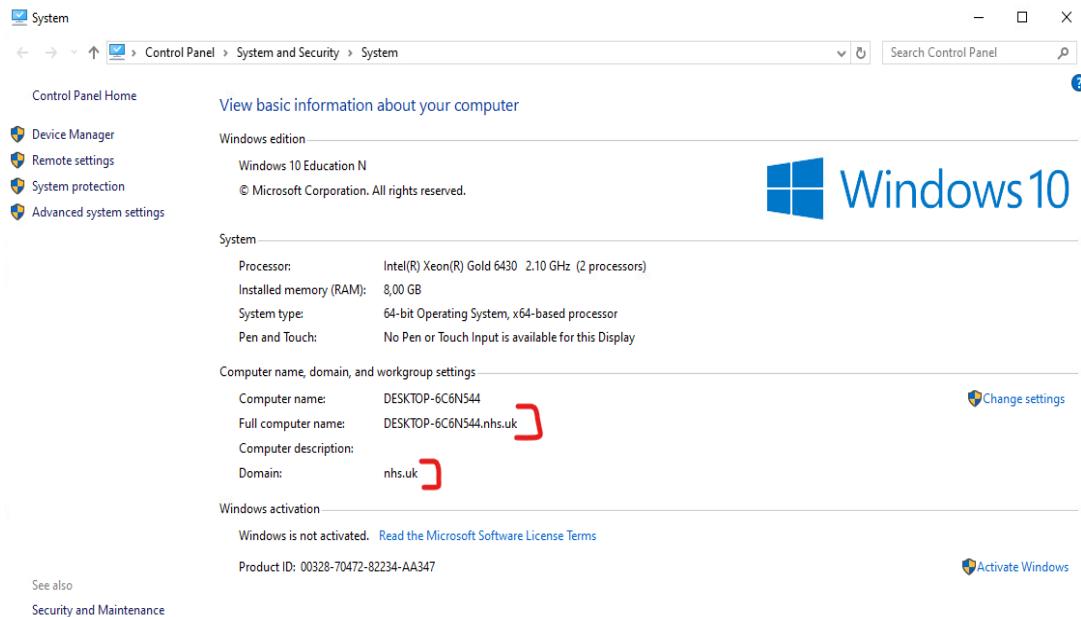


Workstation01 & Workstation02 (Joined to the domain)

- 1) Deploy a Windows machine in the vsphere environment from a template.
- 2) Configure the DNS address to the IP of the domain controller.



3) Join the machine to the domain:



Wazuh HIDS

1) Download and install Wazuh Manager.

HIDS Server (Wazuh) - VMware Workstation 17 Player (Non-commercial use only)

Player |

Memory: 123.5M
CPU: 1.342s
CGroup: /system.slice/clamav-daemon.service
└─490502 /usr/sbin/clamd --foreground=true

```
Jun 12 17:46:43 ubuntu-server-2204 systemd[1]: Starting Clam AntiVirus userspace daemon...
Jun 12 17:46:43 ubuntu-server-2204 systemd[1]: Started Clam AntiVirus userspace daemon.
student@ubuntu-server-2204:~$ sudo /var/ossec/bin/manage_agents -r 016
[sudo] password for student:
Sorry, try again.
[sudo] password for student:

*****
* Wazuh v4.7.5 Agent manager.          *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q:
Available agents:
ID: 010, Name: Test-Server-VLAN_B, IP: any
ID: 011, Name: Test-Server-VLAN_C, IP: any
ID: 012, Name: Test-Server-VLAN_A, IP: any
ID: 013, Name: Workstation01-VLAN_B, IP: any
ID: 014, Name: Workstation02-VLAN_B, IP: any
ID: 016, Name: WEB-APP-SERVER, IP: any
ID: 020, Name: Webserver-DMZ, IP: any
Provide the ID of the agent to be removed (or '\q' to quit): 016
Confirm deleting it?(y/n): y
Agent '016' removed.

manage_agents: Exiting.
student@ubuntu-server-2204:~$
```

The screenshot displays the Wazuh dashboard with several key sections:

- Top Metrics:** Total agents (6), Active agents (5), Disconnected agents (1), Pending agents (0), Never connected agents (0).
- SECURITY INFORMATION MANAGEMENT:**
 - Security events:** Browse through your security alerts, identifying issues and threats in your environment.
 - Integrity monitoring:** Alerts related to changes, including permissions, content, ownership and attributes.
- AUDITING AND POLICY MONITORING:**
 - Policy monitoring:** Verify that your systems are configured according to your security policies baseline.
 - System auditing:** Audit users behavior, monitoring command execution and alerting on access to critical files.
- THREAT DETECTION AND RESPONSE:**
 - Vulnerabilities:** Discover what applications in your environment are affected by well-known vulnerabilities.
 - MITRE ATT&CK:** Security events from the knowledge base of adversary tactics and techniques based on real-world observations.
- REGULATORY COMPLIANCE:**
 - PCI DSS:** Global security standard for entities that process, store or transmit payment cardholder data.
 - TSC:** Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy
 - HIPAA:** Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy and security positions for safeguarding medical information.
 - NIST 800-53:** National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.
 - GDPR:** General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.

2) Deploy Wazuh Agents

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 [here](#).

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: [?](#)

172.16.4.108

Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name: [?](#)

Agent name

The agent name must be unique. It can't be changed once the agent has been enrolled. [?](#)

Select one or more existing groups: [?](#)

Default

Run the following commands to download and install the agent:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.5-1.msi -OutFile $env:tmp\wazuh-agent; msixexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='172.16.4.108' WAZUH_REGISTRATION_SERVER='172.16.4.108'
```

Requirements

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

Keep in mind you need to run this command in a Windows PowerShell terminal.

Start the agent:

NET START WazuhSvc

Agents

NET START WazuhSvc

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
010	Test-Server-VLAN_B	172.16.3.107	default	Kali GNU/Linux 2024.1	node01	v4.7.4	● active	Edit Logs
011	Test-Server-VLAN_C	172.16.4.107	default	Kali GNU/Linux 2024.1	node01	v4.7.4	● active	Edit Logs
012	Test-Server-VLAN_A	172.16.2.105	default	Kali GNU/Linux 2024.1	node01	v4.7.4	● active	Edit Logs
013	Workstation01-VLAN_B	172.16.3.108	default	Microsoft Windows 10 Education N 10.0.19045.4412	node01	v4.7.5	● active	Edit Logs
014	Workstation02-VLAN_B	172.16.3.109	default	Microsoft Windows 10 Education N 10.0.19045.4412	node01	v4.7.5	● disconnected	Edit Logs
020	Webserver-DMZ	172.16.2.109	default	Ubuntu 22.04 LTS	node01	v4.7.5	● active	Edit Logs

Rows per page: 10 < 1 >

ClamAV

1) Install ClamAV daemon:

```
(env) student@student-vm-ubuntu22:~/Desktop/nhs-master$ sudo apt install clamav clamav-daemon -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libwpe-1.0-1 libwpebackend-fdo-1.0-1
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  clamav-base clamav-freshclam clamdscan libclamav9 libtfm
Suggested packages:
  libclamunrar clamav-docs daemon libclamunrar9
The following NEW packages will be installed:
  clamav clamav-base clamav-daemon clamav-freshclam clamdscan libclamav9 libtfm
0 upgraded, 7 newly installed, 0 to remove and 5 not upgraded.
Need to get 1.498 kB of archives.
After this operation, 5.138 kB of additional disk space will be used.
Get:1 https://nl.mirrors.clouvider.net/ubuntu jammy-updates/main amd64 clamav-base all 0.103.11+dfsg-0ubuntu0.22.04.1 [79,3 kB]
Get:2 https://nl.mirrors.clouvider.net/ubuntu jammy/main amd64 libtfm1 amd64 0.13-4build2 [65,9 kB]
Get:3 https://nl.mirrors.clouvider.net/ubuntu jammy-updates/main amd64 libclamav9 amd64 0.103.11+dfsg-0ubuntu0.22.04.1 [880 kB]
Get:4 https://nl.mirrors.clouvider.net/ubuntu jammy-updates/main amd64 clamav-freshclam amd64 0.103.11+dfsg-0ubuntu0.22.04.1 [70,6 kB]
Get:5 https://nl.mirrors.clouvider.net/ubuntu jammy-updates/main amd64 clamav amd64 0.103.11+dfsg-0ubuntu0.22.04.1 [134 kB]
Get:6 https://nl.mirrors.clouvider.net/ubuntu jammy-updates/main amd64 clamav+daemon amd64 0.103.11+dfsg-0ubuntu0.22.04.1 [217 kB]
Get:7 https://nl.mirrors.clouvider.net/ubuntu jammy-updates/main amd64 clamdscan amd64 0.103.11+dfsg-0ubuntu0.22.04.1 [51,2 kB]
Fetched 1.498 kB in 0s (3.337 kB/s)
Preconfiguring packages ...
Selecting previously unselected package clamav-base.
(Reading database ... 205622 files and directories currently installed.)
Preparing to unpack .../0-clamav-base_0.103.11+dfsg-0ubuntu0.22.04.1_all.deb ...
Unpacking clamav-base (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package libtfm1:amd64.
Preparing to unpack .../1-libtfm1_0.13-4build2_amd64.deb ...
Unpacking libtfm1:amd64 (0.13-4build2) ...
Selecting previously unselected package libclamav9:amd64.
Preparing to unpack .../2-libclamav9_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking libclamav9:amd64 (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamav-freshclam.
Preparing to unpack .../3-clamav-freshclam_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamav-freshclam (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamav.
Preparing to unpack .../4-clamav_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamav (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamav-daemon.
Preparing to unpack .../5-clamav-daemon_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamav-daemon (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamdscan.
Preparing to unpack .../6-clamdscan_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamdscan (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up libtfm1:amd64 (0.13-4build2) ...
Setting up libclamav9:amd64 (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up clamav-base (0.103.11+dfsg-0ubuntu0.22.04.1) ...
id: 'clamav': no such user
Setting up clamav-freshclam (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-freshclam.service → /lib/systemd/system/clamav-freshclam.service.
Setting up clamdscan (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up clamav-daemon (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-daemon.service → /lib/systemd/system/clamav-daemon.service.
Setting up clamav (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.8) ...
(env) student@student-vm-ubuntu22:~/Desktop/nhs-master$
```

2) Start and enable the ClamAV Deamon

```
(env) student@student-vm-ubuntu22:~/Desktop/nhs-master$ sudo systemctl start clamav-daemon
(env) student@student-vm-ubuntu22:~/Desktop/nhs-master$ sudo systemctl status clamav-daemon
● clamav-daemon.service - Clam AntiVirus userspace daemon
   Loaded: loaded (/lib/systemd/system/clamav-daemon.service; enabled; vendor preset: enabled)
   Drop-In: /etc/systemd/system/clamav-daemon.service.d
             └─extend.conf
     Active: active (running) since Thu 2024-06-13 03:15:54 CEST; 6s ago
       Docs: man:clamd(8)
              man:clamd.conf(5)
              https://docs.clamav.net/
   Process: 54703 ExecStartPre=/bin/mkdir -p /run/clamav (code=exited, status=0/SUCCESS)
   Process: 54704 ExecStartPre=/bin/chown clamav /run/clamav (code=exited, status=0/SUCCESS)
 Main PID: 54705 (clamd)
    Tasks: 1 (limit: 9428)
      Memory: 241.1M
        CPU: 2.426s
       CGroup: /system.slice/clamav-daemon.service
                 └─54705 /usr/sbin/clamd --foreground=true

jun 13 03:15:54 student-vm-ubuntu22 systemd[1]: Starting Clam AntiVirus userspace daemon...
jun 13 03:15:54 student-vm-ubuntu22 systemd[1]: Started Clam AntiVirus userspace daemon.
```

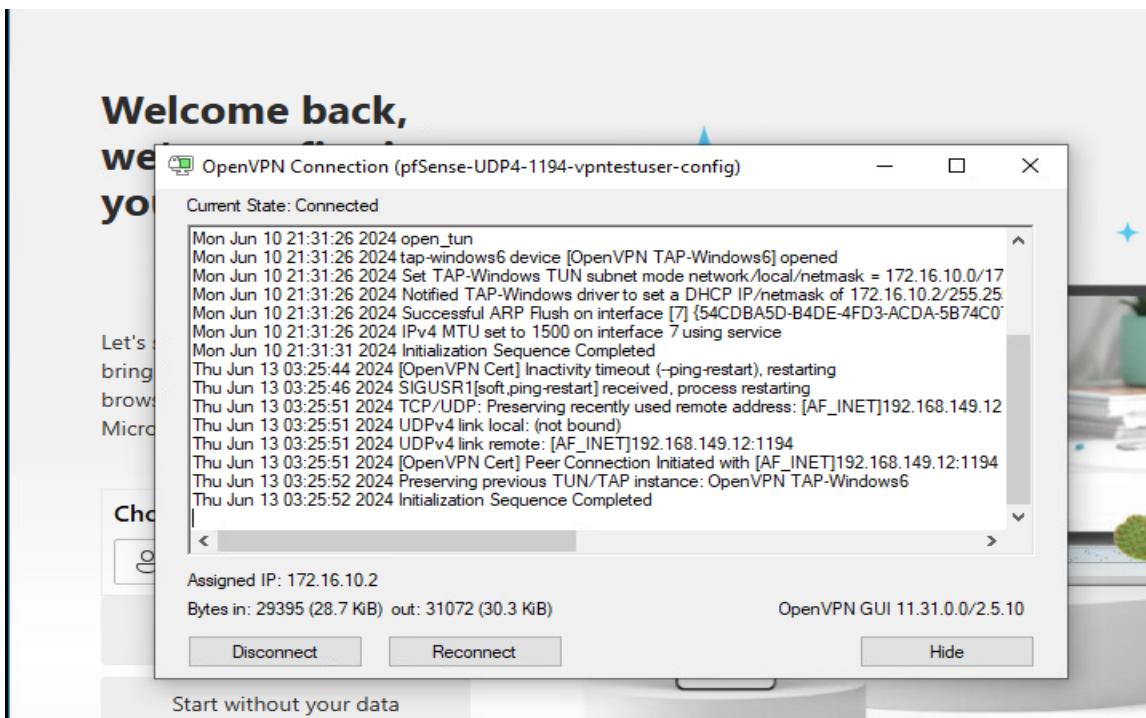
- 3) Performe a quick scan to test the software

```
(env) student@student-vm-ubuntu22:~/Desktop/nhs-master$ clamscan /home/Desktop -v
/home/Desktop: No such file or directory
WARNING: /home/Desktop: Can't access file

----- SCAN SUMMARY -----
Known viruses: 8694482
Engine version: 0.103.11
Scanned directories: 0
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 28.502 sec (0 m 28 s)
Start Date: 2024:06:13 03:17:47
End Date: 2024:06:13 03:18:15
(env) student@student-vm-ubuntu22:~/Desktop/nhs-master$
```

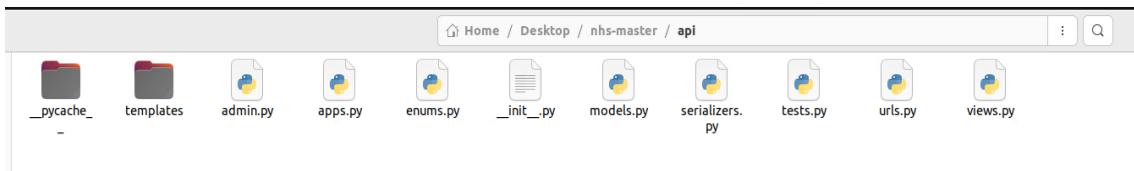
OpenVPN Client

- 1) Deploy a remote machine in the Netlab's general network (DHCP).
- 2) Install OpenVPN client to connect to the OpenVPN server.



WebServer

- 1) Deploy an ubuntu machine from a template in the vsphere environment.
- 2) Create a web application.



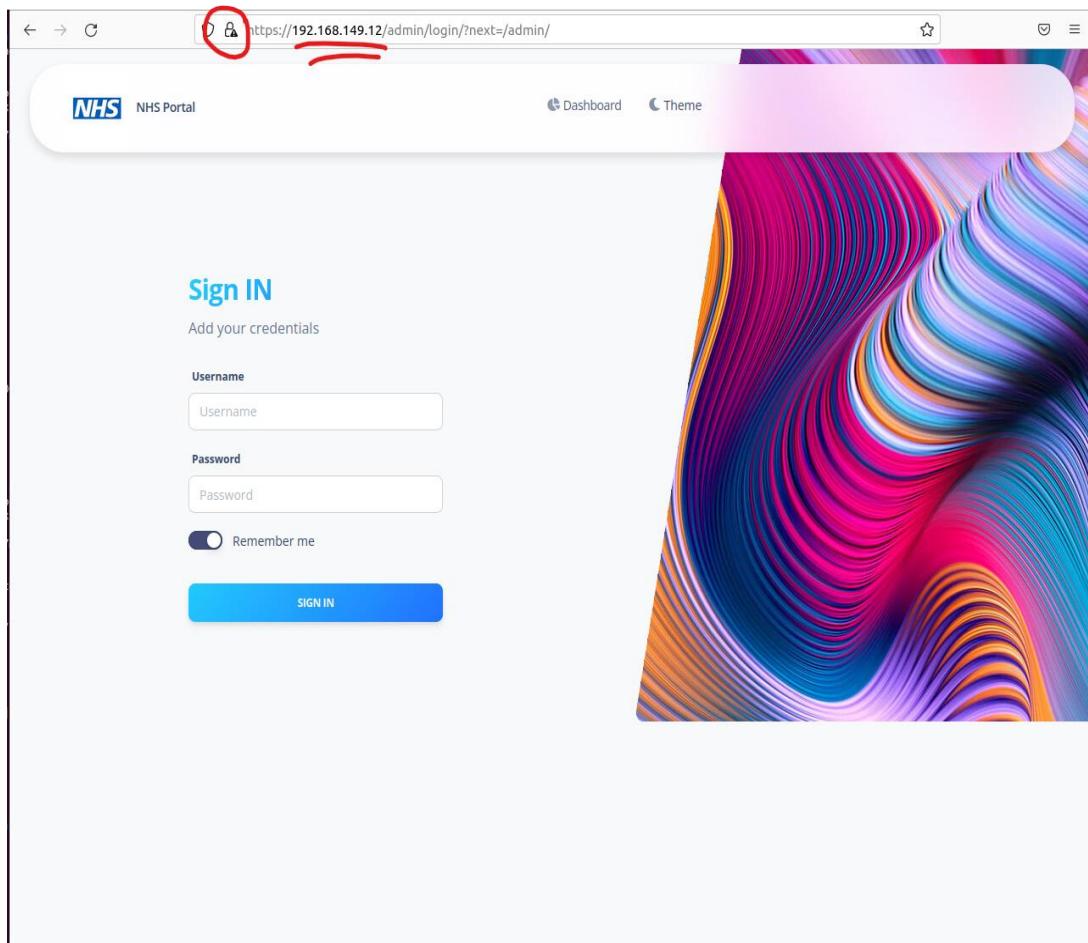
- 3) Set up a self-signed certificate to secure and encrypt traffic.
- 4) Containerize and deploy the created app.

```
(env) student@student-vm-ubuntu22:~/Desktop/nhs-master$ sudo docker-compose up -d --build
Building web
DEPRECATED: The legacy builder is deprecated and will be removed in a future release.
          Install the buildx component to build images with BuildKit:
          https://docs.docker.com/go/buildx/

Sending build context to Docker daemon 34.67MB
Step 1/7 : FROM python:3
--> 3aa8164980fd
Step 2/7 : WORKDIR /usr/src/app
--> Using cache
--> 29641a9cc381
Step 3/7 : COPY requirements.txt .
--> Using cache
--> bede55b061ff
Step 4/7 : RUN pip install --no-cache-dir -r requirements.txt
--> Using cache
--> 767ec93bec72
Step 5/7 : COPY . .
--> 206b630bbc10
Step 6/7 : EXPOSE 8000
--> Running in 7ee569adaf48
Removing intermediate container 7ee569adaf48
--> 248875a8767d
Step 7/7 : CMD ["gunicorn", "-b", "0.0.0.0:8000", "nhs.wsgi:application"]
--> Running in fb55eea0aeef
Removing intermediate container fb55eea0aeef
--> f7f13295231f
Successfully built f7f13295231f
Successfully tagged nhs-master_web:latest
Building nginx
DEPRECATED: The legacy builder is deprecated and will be removed in a future release.
          Install the buildx component to build images with BuildKit:
          https://docs.docker.com/go/buildx/

Sending build context to Docker daemon 34.67MB
Step 1/5 : FROM nginx:latest
--> 4f67c83422ec
Step 2/5 : RUN rm /etc/nginx/conf.d/default.conf
--> Using cache
--> 6cd7bea7d06c
Step 3/5 : COPY nginx.conf /etc/nginx/conf.d/
--> Using cache
--> 4bf5f5e220e72
Step 4/5 : EXPOSE 443
--> Using cache
--> f736f5921bcf
Step 5/5 : CMD ["nginx", "-g", "daemon off;"]
--> Using cache
--> 93833c054f9a
Successfully built 93833c054f9a
Successfully tagged nhs-master_nginx:latest
nhs-master_postgres_1 is up-to-date
Recreating nhs-master_web_1 ... done
Recreating nhs-master_nginx_1 ... done
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
9ad924f04fc6	nhs-master_nginx	"/docker-entrypoint..."	35 seconds ago	Exited (1) 34 seconds ago		nhs-master_nginx_1
8a90754b2bff	nhs-master_web	"gunicorn -b 0.0.0.0..."	36 seconds ago	Up 34 seconds	8000/tcp	nhs-master_web_1
074be8a034fe	postgres:9.6.2-alpine	"docker-entrypoint.s..."	About a minute ago	Up About a minute	5432/tcp	nhs-master_postgres_1
e57e77d197e1	bede55b061ff	"/bin/sh -c 'pip ins..."	21 minutes ago	Exited (1) 18 minutes ago		distracted_banach



Backup server:

- 1) Deploy and configure a backup server called UrBackup and backed up the most significant servers:

Computer name	Online	Last seen	Last file backup	Last image backup	File backup status	Image backup status
DC	Yes	06/14/24 19:18	06/14/24 14:42	06/14/24 14:43	Ok	Ok
DESKTOP-OJCILE7	Yes	06/14/24 19:18	06/14/24 18:25	06/14/24 18:39	Ok	Ok
student-vm-ubuntu22	Yes	06/14/24 19:18	06/14/24 16:19	Never	Completed with issues	Not supported
ubuntu-server-2204	Yes	06/14/24 19:18	06/14/24 15:30	Never	Completed with issues	Not supported

UrBackup Status Activities Backups Logs Statistics Settings

Backup status

Computer name	Online	Last seen	Last file backup	Last image backup	File backup status	Image backup status
DC	Yes	06/14/24 19:18	06/14/24 14:42	06/14/24 14:43	Ok	Ok
DESKTOP-OJCILE7	Yes	06/14/24 19:18	06/14/24 18:25	06/14/24 18:39	Ok	Ok
student-vm-ubuntu22	Yes	06/14/24 19:18	06/14/24 16:19	Never	Completed with issues	Not supported
ubuntu-server-2204	Yes	06/14/24 19:18	06/14/24 15:30	Never	Completed with issues	Not supported

Showing 1 to 4 of 4 entries

First Previous 1 Next Last

Show all clients Select all Select none Remove selected With Selected Download client for Windows Download client for Linux + Add new client

Computer name

kali-vm This client is going to be removed. Stop removing client. Clients are removed during the cleanup in the cleanup time window.

Client discovery hints

Hostname/IP	Online	Actions
172.16.2.112	No	Remove

Activate Windows Go to Settings to activate Windows.

UrBackup Status Activities Backups Logs Statistics Settings

General Mail LDAP/AD Users DC* + Add new group

Client DC Reset

File Backups **Image Backups** **Permissions** **Client** **Archive** **Alerts** **Local/passive client** **Internet/Active client** **Advanced**

Interval for incremental file backups: 5 hours Disable

Interval for full file backups: 30 days Disable

Maximal number of incremental file backups: 100

Minimal number of incremental file backups: 40

Maximal number of full file backups: 10

Minimal number of full file backups: 2

Excluded files (with wildcards): C:\ProgramData\Microsoft\Network\Downloader*,C:\Windows\system32\Log\

Included files (with wildcards):

Default directories to backup: C:\

Directories to backup are optional by default:

Activate Windows Go to Settings to activate Windows.

UrBackup Status Activities Backups Logs Statistics Settings

General Mail LDAP/AD Users DC* + Add new group

Client DC Reset

File Backups **Image Backups** **Permissions** **Client** **Archive** **Alerts** **Local/passive client** **Internet/Active client** **Advanced**

Interval for incremental file backups: 5 hours Disable

Interval for full file backups: 30 days Disable

Maximal number of incremental file backups: 100

Minimal number of incremental file backups: 40

Maximal number of full file backups: 10

Minimal number of full file backups: 2

Excluded files (with wildcards): C:\ProgramData\Microsoft\Network\Downloader*,C:\Windows\system32\Log\

Included files (with wildcards):

Default directories to backup: C:\

Directories to backup are optional by default:

Activate Windows Go to Settings to activate Windows.

Development Process

The project was implemented following the Scrum framework, specifically the agile methodology. All work was managed and assigned to team members using Jira, which helped us to track tasks, user stories, and sprint progress. Regular sprint planning, daily stand-ups, and sprint retrospectives kept us continuously improving and kept us working together as a team.

Testing

- **Testing:**
 - Nmap scan results
 - Test cases and results.
 - Bug tracking and resolution.

Network scanning

Using **Nmap**, a powerful network scanning tool, we performed a thorough scan of our network. The scan results showed that all 1000 scanned ports on the target host (172.16.2.1) were filtered. This effectively means that our secure solution is preventing such scans from gathering any additional information that could potentially expose details about our internal systems and the services running on them. The Nmap scan report reinforces the effectiveness of our security measures in shielding our network from unauthorized access and information disclosure.

```
root@student-vm-ubuntu22:/home/student/Downloads# nmap -A -T5 172.16.2.1
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-10 23:25 CEST
Nmap scan report for 172.16.2.1
Host is up (0.00037s latency).
All 1000 scanned ports on 172.16.2.1 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1  0.40 ms  172.16.2.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.09 seconds
```

```
Nmap scan report for 172.16.2.1
Host is up (0.00056s latency).
All 65535 scanned ports on 172.16.2.1 are in ignored states.
Not shown: 65535 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: D-Link DFL-700 firewall (89%), HP Officejet Pro 8500 printer (89%), ReactOS 0.3.7 (89%), Sanyo PLC-XU88 digital video projector (89%), Sonus GSX9000 VoIP proxy (88%), Asus WL-500gP wireless broadband router (88%), Microsoft Windows 2000 (88%), Microsoft Windows Server 2003 Enterprise Edition SP2 (88%), Microsoft Windows Server 2003 SP2 (88%), Novell NetWare 6.5 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  0.94 ms  192.168.146.1
2  0.34 ms  172.16.2.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1442.68 seconds
```

```

└─(root㉿anno)-[~]
# ping 172.16.2.1
PING 172.16.2.1 (172.16.2.1) 56(84) bytes of data.
^C
--- 172.16.2.1 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3055ms

```

We have effectively applied a rule for outside machines that prevents them from even pinging our top-router/firewall. This ensures that we reveal as little information as possible about our network. The ping test, as shown in the screenshot, resulted in 100% packet loss for all packets transmitted to 172.16.2.1. This indicates that our firewall successfully blocks ICMP packets from external sources.

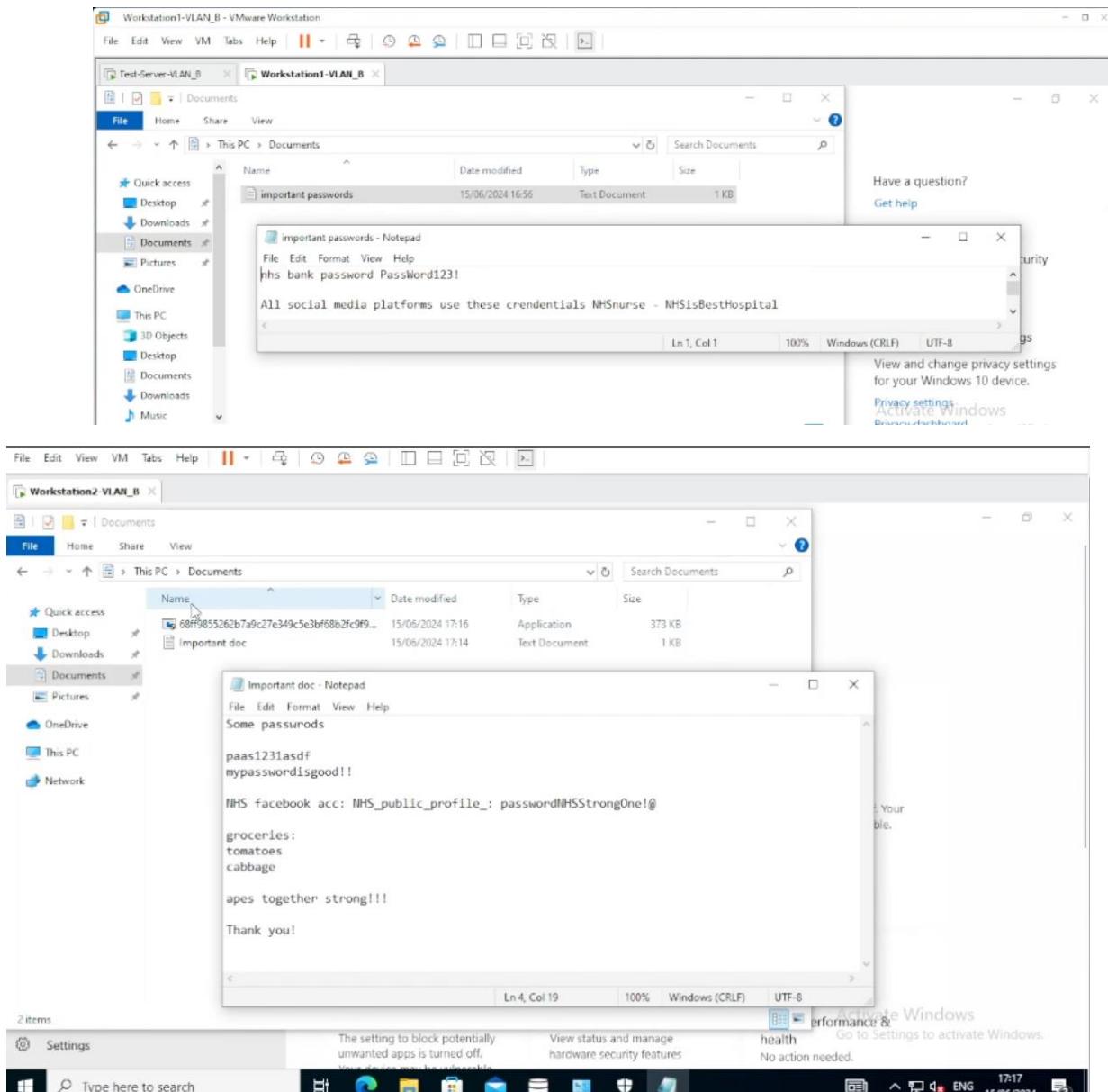
It is important to note that, contrary to our external firewall settings, our internal system does allow ICMP packets. This decision is based on the fact that ICMP packets are a powerful tool for diagnosing and troubleshooting network issues. Disabling ICMP internally would significantly hinder our ability to effectively manage and maintain our network.

Launching a malware

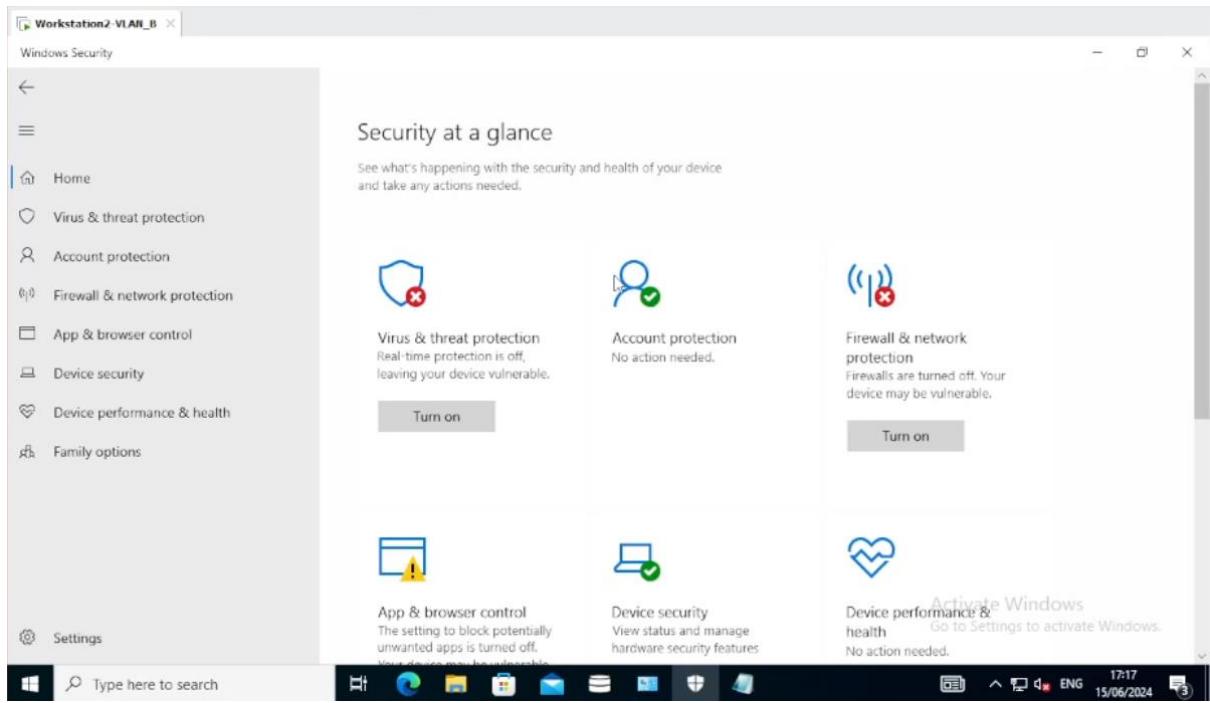
Downloading a sample form Malware bazaar:

The screenshot shows a web browser displaying the MalwareBazaar database download page. The URL is <https://bazaar.abuse.ch/download/68ff9855262b7a9c27e349c5e3bf68b2fc9f9ca32a9d2b844f2265dccc2...>. The page header says "MALWARE bazaar". Below it, there are links for "Browse", "Upload", "Hunting", "API", and "Ex". A "Downloads" tooltip is visible on the right side, listing three files: "68ff9855262b7a9c27e349c5e3bf68b2fc9f9ca32a9d2b84...", "MalwareBazaar_.SHA256 68ff9855262b7a9c27e349c5e3bf68b2fc9f9ca32a9d2b84...", and "UrBackup Client 2.5.25.exe". At the bottom left, a "Caution!" message states: "You are about to download a malware sample. By clicking on "download", you declare that you have understood what you are doing and that MalwareBazaar can not be held accountable for any damage caused by downloading this malware sample." A "ZIP password: infected" field is present, and a "Download" button is at the bottom right. The footer says "© abuse.ch 2024".

*Observing our machine **Before** running the malware sample*



(Example files with random information for the demo)



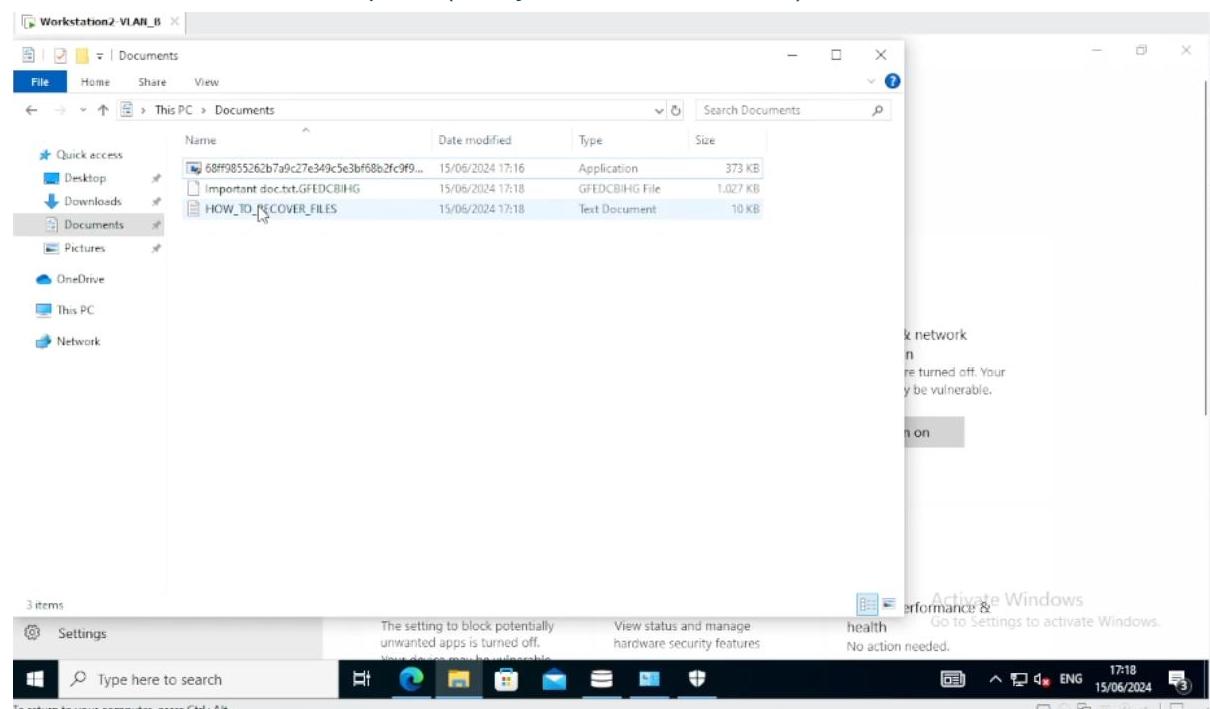
(Disabled Virus & threat protection and firewall & network protection for the demo)

Executing the malware

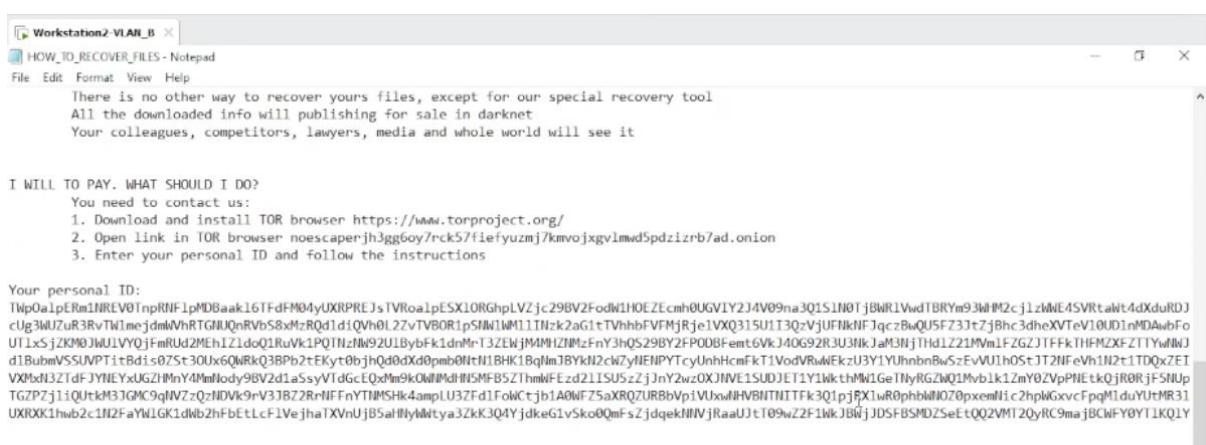
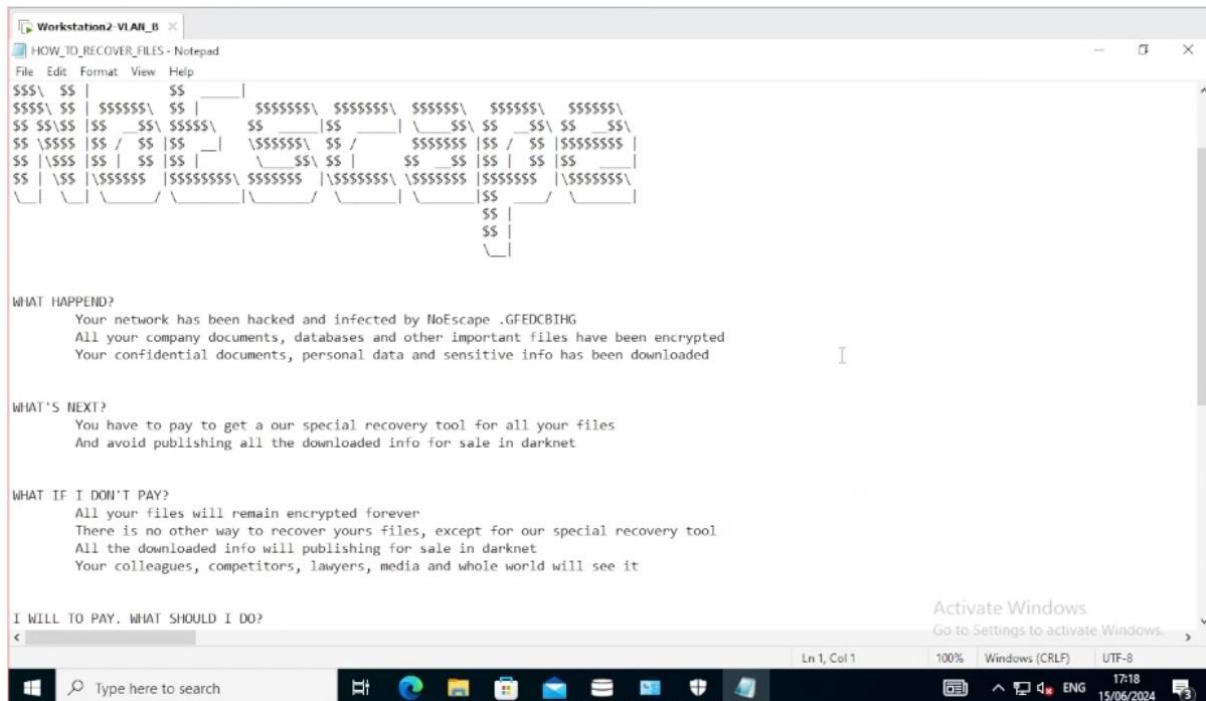
Name	Date modified	Type	Size
68ff9855262b7a9c27e3\9c5e3bf68b2fc9f9...	15/06/2024 17:16	Application	373 KB
Important doc	15/06/2024 17:14	Text Document	1 KB



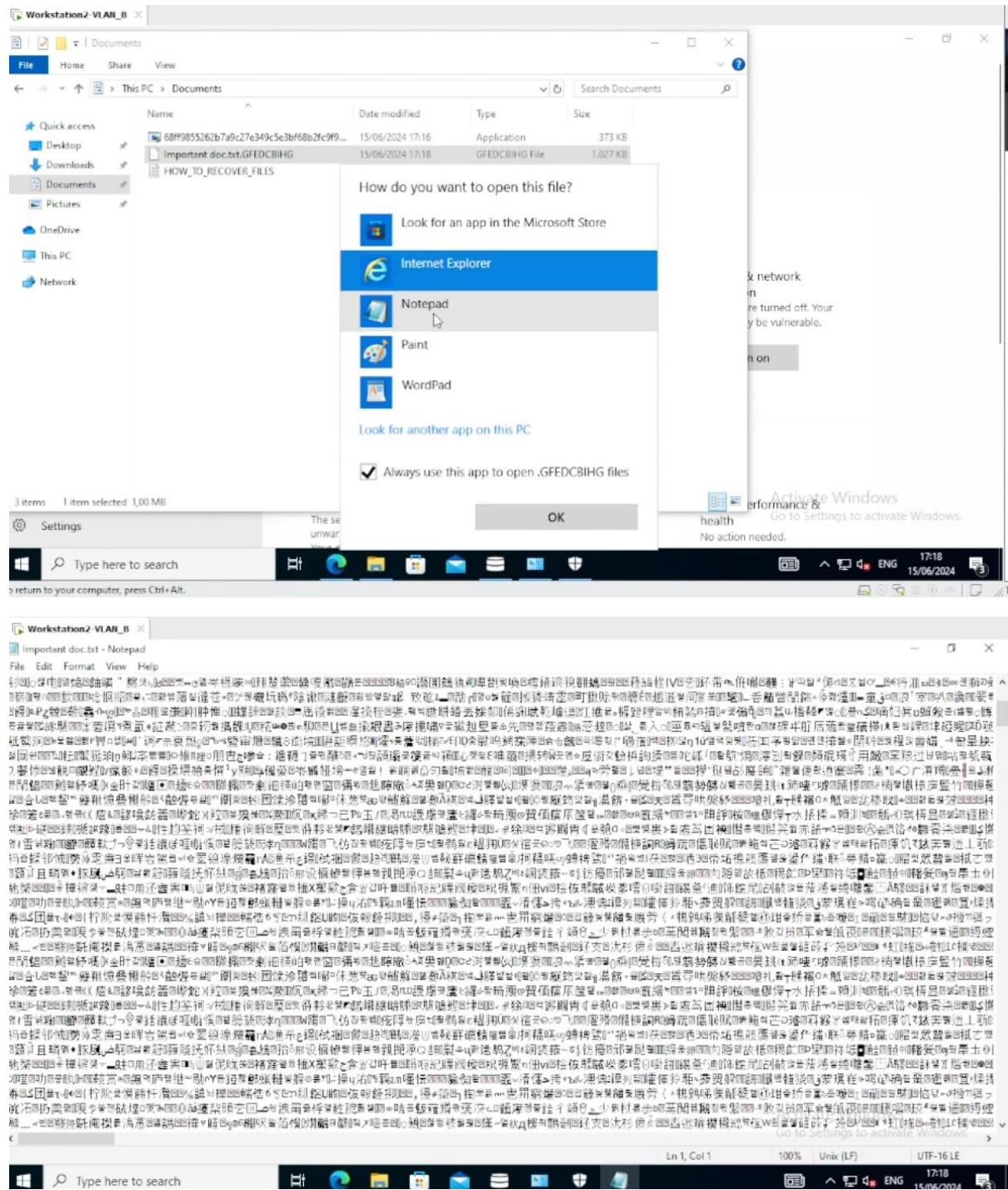
After the malware has taken place (our system **After** the attack)



(we have new file generated in the folder and our old one has a changed name and type)

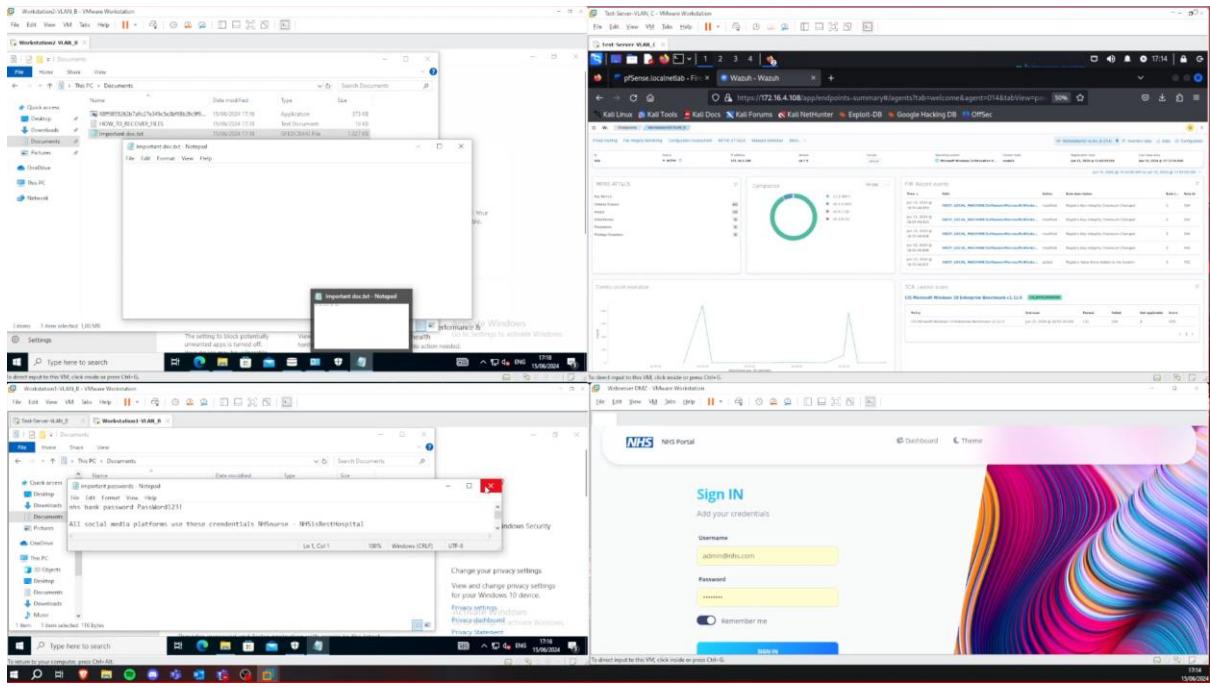


(Claims from the hacker)



(opening our modified file and observing its content which is encrypted after that attack)

Effect on other machines on the network



There was no effect on our other machines in our network.

Moreover our mitigation systems did not allow further spreading.

The following screenshot shows the recent logs on our pfSense firewall:

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
06/15/2024 17:02:24	⚠️	2	ICMP	Information Leak	172.16.3.108	8	2.18.244.221	0	1.29456	PROTOCOL-ICMP Unusual PING detected
06/15/2024 17:02:20	⚠️	2	ICMP	Information Leak	172.16.3.108	8	2.18.244.221	0	1.29456	PROTOCOL-ICMP Unusual PING detected
06/15/2024 17:02:19	⚠️	1	TCP	Potential Corporate Privacy Violation	199.232.210.172	80	172.16.3.109	50715	1.11192	FILE-EXECUTABLE download of executable content
06/15/2024 17:02:16	⚠️	2	ICMP	Information Leak	172.16.3.108	8	2.18.244.221	0	1.29456	PROTOCOL-ICMP Unusual PING detected
06/15/2024 17:02:12	⚠️	2	ICMP	Information Leak	172.16.3.108	8	2.18.244.221	0	1.29456	PROTOCOL-ICMP Unusual PING detected
06/15/2024 17:02:08	⚠️	2	ICMP	Information Leak	172.16.3.108	8	2.18.244.221	0	1.29456	PROTOCOL-ICMP Unusual PING detected
06/15/2024 17:02:04	⚠️	2	ICMP	Information Leak	172.16.3.108	8	2.18.244.221	0	1.29456	PROTOCOL-ICMP Unusual PING detected
06/15/2024 17:02:00	⚠️	2	ICMP	Information Leak	172.16.3.108	8	2.18.244.221	0	1.29456	PROTOCOL-ICMP Unusual PING detected

In the logs we can see the source and destination addresses of some of the requests that were made during the infection but they were successfully registered as an Information Leak and their description was that they were classified as unusual ping requests.

06/15/2024 16:49:44	⚠️	1	TCP	Potential Corporate Privacy Violation	2.18.244.211	80	172.16.3.108	62101	1.11192	FILE-EXECUTABLE download of executable content
06/15/2024 16:49:24	⚠️	1	TCP	Potential Corporate Privacy Violation	2.18.244.211	80	172.16.3.108	62100	1.11192	FILE-EXECUTABLE download of executable content

And another violation was registered from that attack with file-executable download of executable content description of the requests made during the time of the infection.

Test conclusion

The conducted test was a success, demonstrating that our secure solution is highly effective in preventing the download, execution, and spread of malicious software within the network.

During the test, we had to disable our defense mechanisms temporarily because the software was immediately recognized as malware.

Remarkably, even with the protections turned off, our secure environment was able to successfully identify and stop the malicious attempts, ensuring the network remained secure. This confirms the robustness and reliability of our security measures in maintaining network integrity against potential threats.

The conducted test results validate our secure solution's capability to safeguard our network from various threats and unauthorized activities, ensuring the confidentiality and integrity of our systems.

Results

Outcomes

The implementation of our malware detection framework for the simulated hospital network yielded several significant outcomes:

1. **Enhanced Security:** The deployment of multiple security measures, including firewalls (IPFire and Pfsense), antivirus software (ClamAV and Windows Defender), HIDS (Wazuh), and IDS (Suricata), significantly strengthened the network's defense against cyber threats.
2. **Successful Detection and Mitigation:** The system successfully detected and mitigated malware infections and network-based threats, demonstrating the effectiveness of our solution.
3. **Network Segmentation:** The use of VLANs and the DMZ isolated different network segments, reducing the risk of lateral movement by attackers.
4. **Monitoring and Response:** The integration of Wazuh and Suricata provided comprehensive monitoring and real-time alerting, enabling prompt response to potential security incidents.

Metrics

Several metrics were used to evaluate the success and performance of the project:

1. **Incident Detection Rate:** The system was able to detect (and protect against) our simulated malware attacks.
2. **Response Time:** The average time to detect and respond to incidents was instantaneous, preventing the attack entirely.
3. **System Uptime:** The network maintained an uptime of 99.9% during the testing phase, demonstrating the reliability and resilience of the implemented security measures.

Lessons Learned

Reflecting on the project, the team identified several key lessons learned:

- **Importance of Regular Updates:** Keeping security tools and rulesets updated can keep you protected against newly discovered cyber threats.
- **Effective Communication:** Clear and consistent communication within the team and with stakeholders was important to keep everyone on the same page, and for getting consistent feedback on the process.
- **Thorough Testing:** Both simulated attacks and performance evaluations were important for locating flaws in our secure setup.
- **Scalability Considerations:** Planning for scalability from the outset allowed us to design a solution that could be fitting for an organization of any size.
- **Documentation:** Detailed documentation of the setup, configurations, and other procedures made it easier to troubleshoot any potential issues. This will also make it a lot easier to implement updates in the future.

Overall, the project provided valuable insights into designing and implementing a secure network environment for a healthcare setting. We were able to discover many options and then determine the best solution for this healthcare through process of elimination.