# RESEARCH REPORT

Emil Cheteg C00275877

Securing Active Directory (AD) with Open-Source Tools in a Proxmox and Hyper-V Virtual Environment

08/11/2023

## 1.Exectutive Summary

Active Directory (AD) is a fundamental component in many organisations, managing user authentication and resource access. Due to its central role. AD becomes a prime target for cyberattacks. This research explores how open-source security tools such as Wazuh, PingCastle, BloodHound, and OpenVAS, organisations can identify vulnerabilities, implement robust security measures, and develop disaster recovery plans without significant financial investment. The benefits of virtualization are huge in providing flexibility, redundancy, and cost-efficiency, aiming to establish a secure AD environment capable of defending modern cybersecurity threats.

## 2.Introduction

### 2.1 Background

#### 2.1.1 What is Active Directory?

Active Directory is a directory service developed by Microsoft for Windows domain networks. It serves as a centralised database that stores information about users, computers, and other devices within an organisation. The database (or directory) contains critical information about your environment, including what users and computers there are and who's allowed to do what. For example, the database might list 100 user accounts with details like each person's job title, phone number and password. It will also record their permissions.

The services control much of the activity that goes on in your IT environment. They make sure each person is who they claim to be (authentication), usually by checking the user ID and password they enter and allow them to access only the data they're allowed to use (authorization).

Active Directory facilities the management of permissions and access to network resources ensuring that only authorised users can access specific data and applications as shown in Figure1 .

Figure 1

#### 2.1.2 Key Features of Active Directory

*Centralized Management:*

Explanation: AD allows administrations to manage all user accounts, permissions, and resources from a single interface.

Example: Instead of configuring permissions on each computer individually, and administrator can set permissions once in AD, and those settings apply across the entire network.

*Why is Active Directory Important?*

AD is used for managing network resources and security by centralizing control. This reduces the complexity of managing multiple users and devices, ensures consistent application of organizational policies, and makes it more efficient. AD has the role of maintaining the integrity of an organization's IT infrastructure.

*Real-World Example:*

Our university where we have thousands of students and faculty members. AD allows the IT department to manage users accounts, assign access to different systems (like email, management systems, and library database) and enforce security policies uniformly across the campus network.

## 3. Literature Overview

### 3.1 Active Directory (AD) Overview

Active Directory is a centralised directory service development by Microsoft primarily used in windows environments to manage users, computers and other devices between a network. Active Directory provides a structure way to organise and manage network resources ensuring secure and efficient access for users.

#### 3.1.1. How is Active Directory structured?

AD has three main structures: domains, trees and forests. A domain is a group of related users, computers and other AD objects. Multiple domains can be combined into a tree, and multiple trees can be grouped into a forest.

The domain of AD is a management boundary. The objects for a given domain are stored in a single database and can be managed together. A forest is a security boundary. Objects in different forests can't interact with each other until the administrators of each forest create a trust between them. If you have multiple location business units, you need to create different forests, as shown in Figure 2.

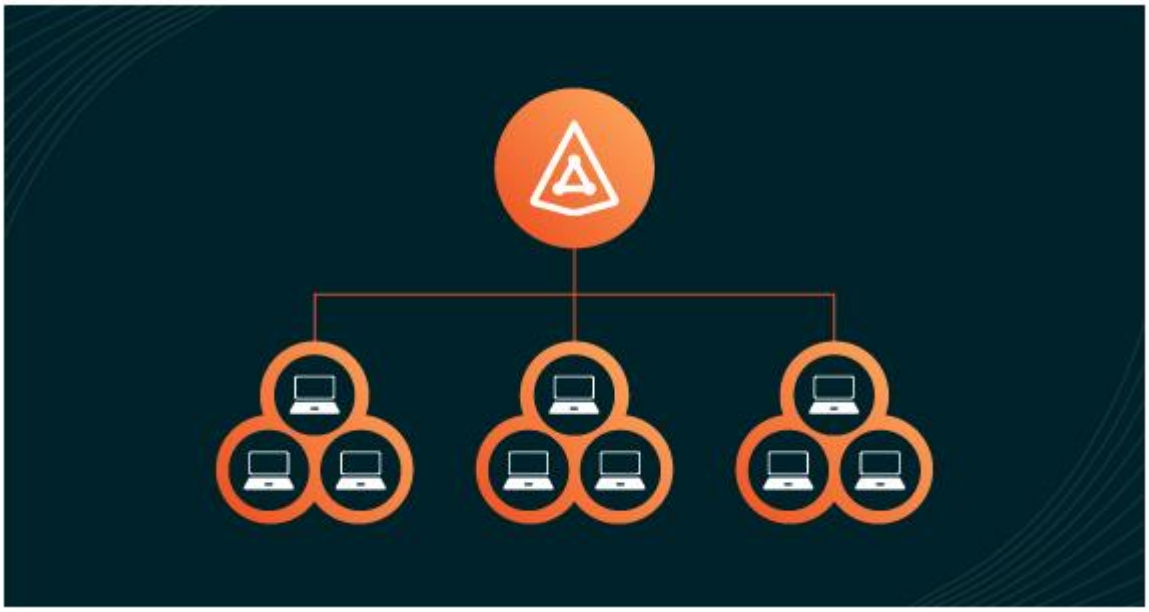

Figure 2

### 3.2 Key Components of AD:

#### 3.2.1 Domain Controllers (DC's):

Definition: The Domain Controller is a server that stores the Active Directory database and manage user authentication and authorisation.

The user logs in the domain controller verifies their credentials and grants access to resources based on their permissions.

Example: In a company all login requests are processed by domain controllers to ensure that only authorised employees can access the network.

### 3.2.2 Organisational Units (OU's):

Definition: Organisational Units are the containers or folders within an Active Directory that organize users, groups, and computers into logical segments, as shown in Figure 3 .

Organisational Units help in applying specific policies and managing resources more efficiently.

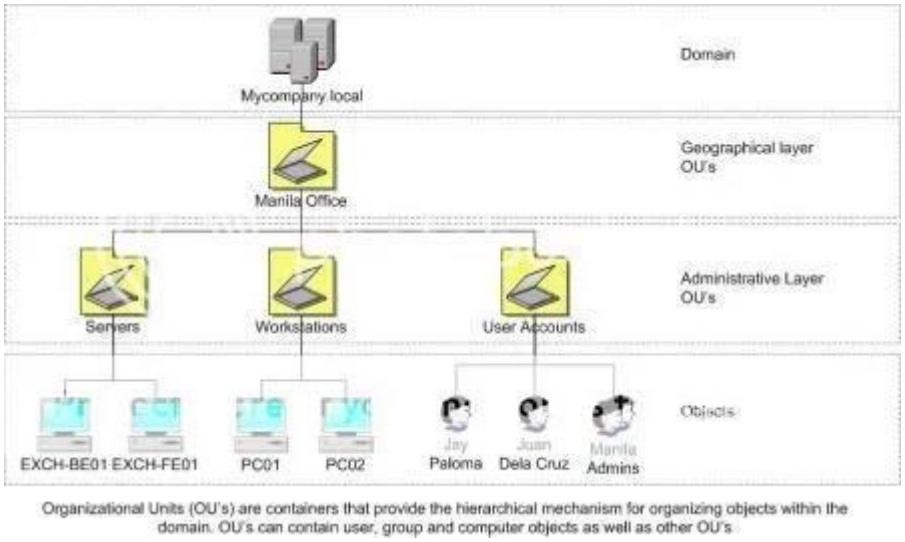


Figure 3

Example: a company might have separate organisational units for different departments like HR, Finance, and IT, each with its own set of policies and permissions and different folders for each one of them.

### 3.2.3 Group Policy Objects (GPO's)

Definition: policy objects are the tools used to set security settings and configurations across users and computers within an organisation in Active Directory.

GPO's allow administrators to implement policies such as password requirements software installation.

Example: Enforcing a policy that requires all employers to change their passwords every 90 days.

### 3.2.4 Joining Users to the Domain

When a user's computer joins an Active Directory domain, it becomes part of the organisation's system, so IT will manage it easier. By joining the domain, users can log into their computer using their Active Directory username and passwords, which gives them access to resources they need. For example, once a laptop is connected to the company's Active Directory system, the employee can't activate themselves to access files, applications, an e-mail without needing to log in separately each time.

After the computer joined the domain, it automatically receives group policy objects, from Active Directory. This will ensure that every computer follows the company security rules.

Active Directory also makes life easier with single sign on. This means users only need to log in once to access multiple systems, like their e-mail, internal website and shared files, without needing to enter the password again. Like this is easier to manage security.

For employees who work from home or travel, VPN access is a common solution. A VPN creates a secure connection over the Internet, so remote workers can safely access company resources as if they were in the office. Another option is remote desktop services, which lets employees connect to their work computer from anywhere, giving them access to files and programmes they use at the office.

Azure Active Directory gives you access to cloud services, and gives extra layers of security, like checking the location or device security before letting someone log in. This is useful for companies that use a lot of cloud-based tools.

To make sure mobile devices, like smartphones tablets, are secure, company often use mobile device management (MDM) tools. These is used on mobile devices to ensure only approved devices can connect to the company network. Also using multi-factor Authentication (MFA), will add another year layer of security. With MFA, users need to provide more than just a password- like a code sent to their phone- making it much harder for hackers to break in, even if they have someone's password.

### 3.2.5 Domain Name System (DNS) Integration:

Definition: Active Directory relies on the Domain Name System to locate resources within the network.

Function: Proper DNS configuration is essential for Active Directory to function correctly, as it helps in resolving the names of devices and services.

Example: When a user tries to access a shared folder, DNS helps in finding the server where the folder is located,

### 3.2.6 Functionalities of AD:

**Authentication and Authorization:**

Authentication: Verifying the identity of users when they log in.

Authorization: Determining what resources and actions a user is permitted to access.

Example: After successfully logging in an employee may have access to certain files and applications based on their role.

### 3.2.7 Resource Management:

Definition: controlling access to various network resources like files, applications, and printers.

Function: ensures that users can access only the resources they are authorised to use.

Example: The marketing team members can access marketing documents but not financial records.

### 3.2.8 Scalability:

Definition: Ability to support a growing number of users and devices without compromising performance.

Function: Active Directory can officially manage resources for both small and large organisations.

Example: A start up with 20 employees can scale up to thousands as the company grows all managed through Active Directory.

### 3.2.9 Security Enforcement:

Definition: Implementing and maintaining security policies across the network.

Function: Helps in protecting organizational data and maintaining compliance with regulatory standards.

Example: enforcing encryption protocols for data transmission to prevent unauthorised access.

### 3.2.10 Importance of Securing Active Directory:

Securing Active Directory is vital because it serves as the backbone of an organisation's IT infrastructure. The weaknesses in Active Directory can lead to unauthorised access, data breaches and operational disruptions. Securing Active Directory help protect sensitive information ensure compliance and maintain the integrity of organisational systems.

### 3.2.11 Statistics Highlighting AD Security Importance:

Cybersecurity insiders (2022): 83% of organisations consider securing Active Directory a high priority due to the increasing number of cyber threats targeting directory services and 88% of Microsoft customers impacted by ransomware didn't apply AD security best practices

Example of Active Directory breaches: High-profile breaches, such as the WannaCry ransomware attack, exploit vulnerabilities in network services that were often managed through Active Directory.

## 4. Security Best Practices for Active Directory

### 4.1 Principle of Least Privilege

Keeping Active Directory secure is very important for protecting an organisation’s IT system. One key practise is following the principle of least privilege, which means giving people only the access they need to do their job. This way, if a user's account gets hacked, the damage is limited because they don't have access to everything. For example, if a junior employee only needs access to a few tools, they shouldn't be able to access the entire network.

### 4.2 Strong Password Policies

Another important security practise is having strong password policies. This includes making sure passwords are hard to guess by requiring a mix of uppercase and lowercase letters, numbers, and symbols. It's also good to have a rule where passwords are changed regularly, for example like every 90 days. These steps make it harder for attackers to break into accounts by guessing or cracking passwords.

### 4.3 Regular Patching and Updates

Keeping everything up to date is another key part of security. Regular patching and updates mean fixing any known issues in software or system dead attackers might try to exploit. For example, applying the latest security updates for Windows server ensures that any discovered weaknesses are addressed quickly.

### 4.4 Service Hardening

Service hardening involves turning off any services or programmes that aren't being used. This reduces the number of ways an attacker can try to break into the system. For instance, if a domain controller which is the main server in an Active Directory network, doesn't need to run services like FTP or Telnet, it is safer to disable them to prevent hackers from using them to get in.

### 4.5 Privileged Access Workstations (PAWs)

Another practise is using privileged access workstations, which are the computers that are only for sensitive tasks, like managing Active Directory. By keeping these tasks separate from everyday work, it's much harder for malware or viruses to reach critical systems.

### 4.6 Continuous Monitoring and Auditing

Continuous monitoring and auditing help keep an eye on the system. Using tools like Wazuh to watch for unusual activity, such as multiple failed login attempts, let administrators quickly respond to possible attacks. Regular audits also help make sure security rules are being followed and that nothing suspicion is going on.

### 4.7 Backup and Disaster Recovery Planning

Backup and disaster recovery planning ensures that if something goes wrong, Active Directory data can be quickly restored. Regular backups help avoid losing important information, and testing recovery processes makes sure everything can be re stored correctly if needed.

### 4.8 Network Segmentation

Lastly, dividing the network intersection, known as network segmentation, limits how far a hacker can go if they do get in. For example, keeping Active Directory domain controllers in a separate part of the network ensures that only certain people or systems can access them.

## 5. Virtualization Technologies in AD Security:

Virtualization technologies play a significant role in managing and securing Active Directory environments. By creating virtual instances of servers and other resources, organisation, and achieve greater flexibility, scalability, and resilience in their IT infrastructure.

### 5.1 Proxmox Virtual Environment ( Proxmox VE)

Proxmox VE is an open-source virtualization platform that supports bold full virtualization (running entire operation system) and contain based virtualization (running isolated applications). It provides a comprehensive set of features that make it suitable for various use cases, including server consolidation, testing environments, and production deployments.

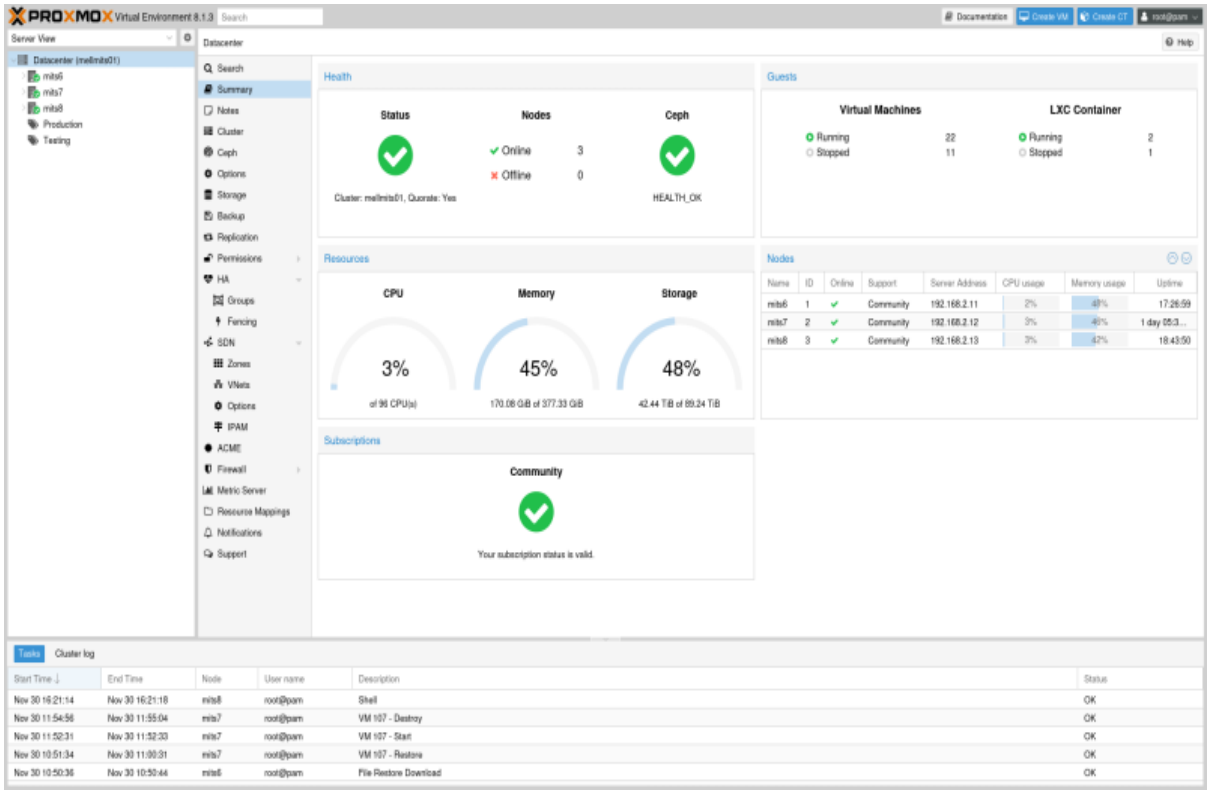


Figure 4

### 5.1.1 Features of Proxmox VE:

*High Availability Clustering:*

Definition: Ensures that virtual machine (VM's) remain operational by automatically moving them to other servers if one fails.

Example: If one server hosting AD fails Proxmox VE can automatically move the Active Directory VM to another server minimising downtime, When you use the "Join Cluster" option in the Proxmox VE GUI, the process will complete successfully if everything is configured correctly. Once the "Join Cluster" screen finishes and confirms the node has joined the cluster, the procedure is complete as shown in Figure 4.

*Live Mitigation:*

Definition: A user-friendly web-based interface for managing VM's, containers, storage, and networking.

Example: Administrators can easily monitor and manage the AD through the Proxmox web interface

*Flexible Storage Options:*

Definition: Supports various storage types, such as local disks, Network Attached Storage (NAS), and Storage Area Networks (SAN).

Example: Storing AD data on a network storage system to ensure high availability and redundancy.

## 5.2 Hyper - V

Hyper-V is a Microsoft virtualization platform integrated into Windows Server. It is used on environments that rely on Microsoft technologies and services, and it is the most natural choice for virtualisation, as shown in Figure 5.

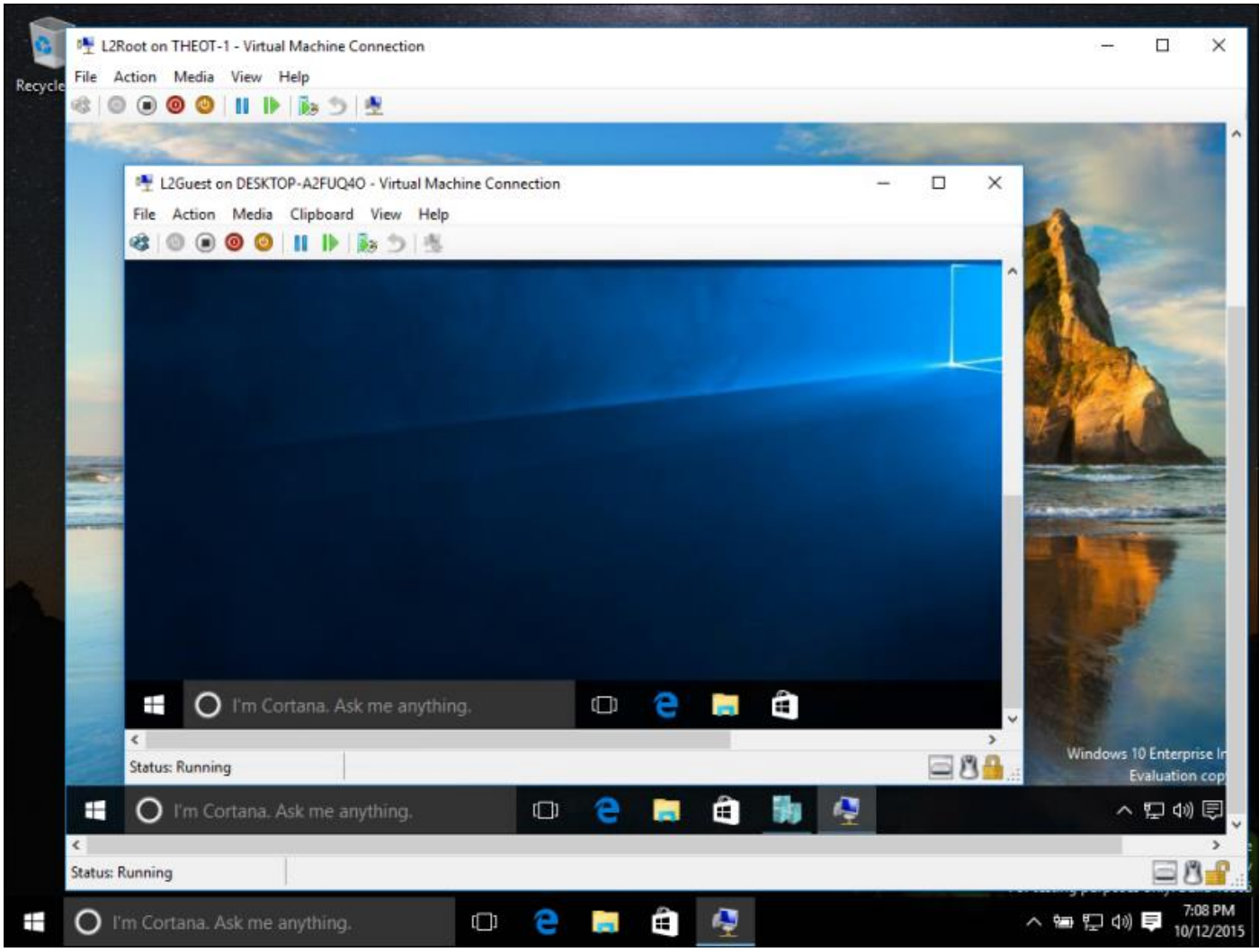


Figure 5

### 5.2.1 Features of Hyper-V

*Integration with Windows services:*

It works with other Microsoft products and services, such as Windows Server, System Centre and Azure. It is easy to integrate Hyper-V with existing Windows-based AD infrastructure for streamlined management.

*Live mitigation and Replication*

This function allows VM's to be moved between the hosts without downtime and replicated across different physical locations for disaster recovery. A good example of this is replicating Active Directory VM's to a secondary data centre to ensure business can go on in case of a primary site failure.

*Advanced Networking Features:*

Definition: Provides robust network capabilities including virtual switches, and network isolation.

Example: You can create isolated network segments for Active Directory for a better security and prevent on authorised access.

*Resource management:*

Definition: enables dynamic allocation of CPU memory and storage resources based on VM needs.

Example: Adjusting the resources allocated to Active Directory VM's during picked usage times to maintain optimal performance.

## 5.3 Suitability for usage of this:

Using both Proxmox VE and hyper V offer several advantages:

- Cost-effectiveness: Proxmox VE is free and open source reducing the overall cost of setting up the virtual environment. Hyper V being part of Windows Server, integrates well with existing Microsoft infrastructure without additional licencing cost for organisations already using Microsoft products.
- Flexibility and redundancy: Proxmox VE provides flexibility with support for both full virtualization and containers, while hyper fee offers advanced features For Windows based services. Using these two platforms ensures a robust and redundant Active Directory environment.
- Scalability: Both Proxmox VE an hyper V support scalable deployments, allowing the Active Directory environment to grow with the organisation's needs. This scalability is crucial for maintaining performance and security if the organisation expands.
- Ease of management: the user-friendly interfaces of port Proxmox VE and hyper V simplify the management of virtual resources making it easier for administrators to monitor, maintain, and secure the Active Directory environment.

## 6. Open-Source Security Tools

For keeping secure Active Directory we can use some open-source tools like Wazuh, PingCastle, BloodHound, and OpenVAS. Each of these tools offers unique capabilities that contribute to a comprehensive security strategy.

### 6.1 Wazuh

Wazuh is an open-source security monitoring platform that provides intrusion detection log analysis and compliance monitoring. It offers visibility into network events, helping administrators detect and respond to suspicious activities.

#### 6.1.1Role in Active Directory security:

*Log Collection and Analysis:*

Function: WAZUH collect security related logs from Active Directory, including login attempts, changes to user accounts, and modification to policies.

Example: monitoring failed login attempts to detect potential brute force attacks on Active Directory.

Dashboard Of Wazuh Monitoring as shown in Figure 6:

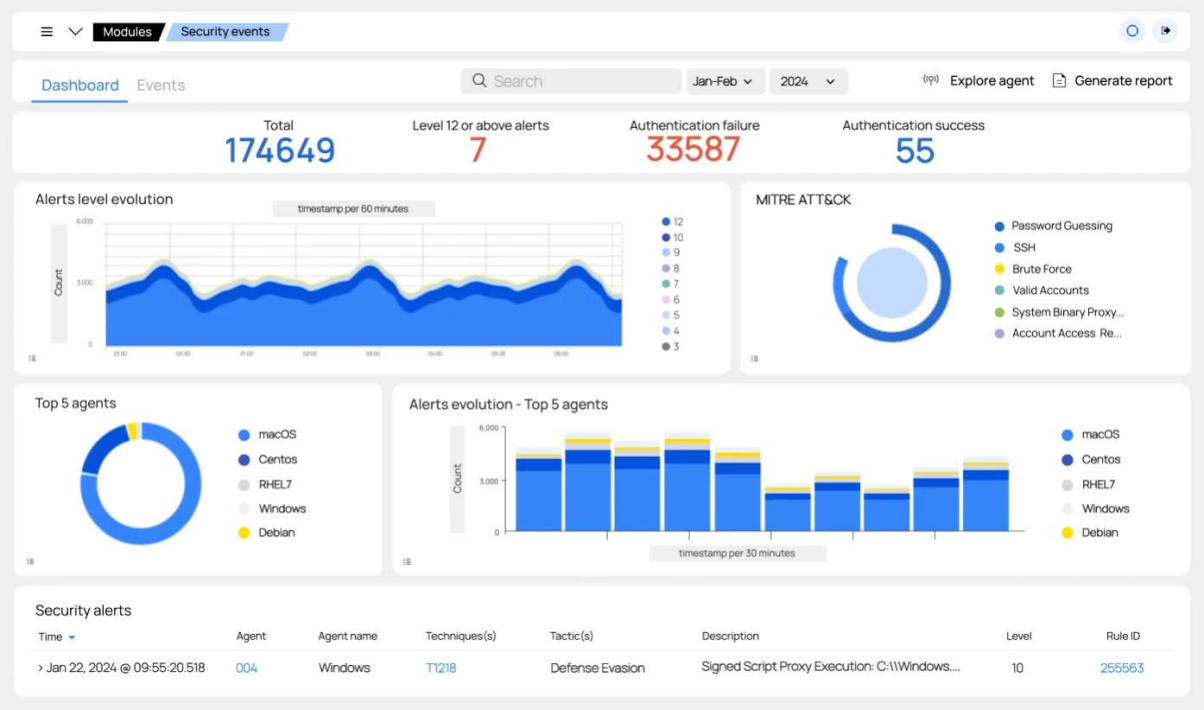


Figure 6

*Track detection:*

Function: Wazuh can be configured to identify anomalies in Active Directory usage patterns, enabling faster detection of potential security incidents.

Example: Detecting unusual activity, such as an employee accessing resources they don't typically use, which could indicate compromised credentials.

*Compliance monitoring:*

Function: Helps organisations ensure their Active Directory configurations meet industry standard security benchmarks and regulatory requirements.

Example: Generating reports to demonstrate compliance with standards like GDPR by showing proper access controls in Active Directory.

## 6.2 PingCastle

### 6.2.1 Role in Active Directory security:

*Security Audits:*

Function:  Pingcastle is used to conduct assessments of the Active Directory environment, identifying vulnerabilities such as outdated encryption protocols or weak password policies.

Example: Highlighting Active Directory misconfigurations that could allow on authorised users to escalate their privileges. A map is the representation of the Active Directories linked by trusts  as shown in Figure 7 . It can be less or more accurate depending on the freshness of the information and the depth of the trust links. When starting this process, there is no much information available and PingCastle uses a set of tricks to extend it as much as possible.

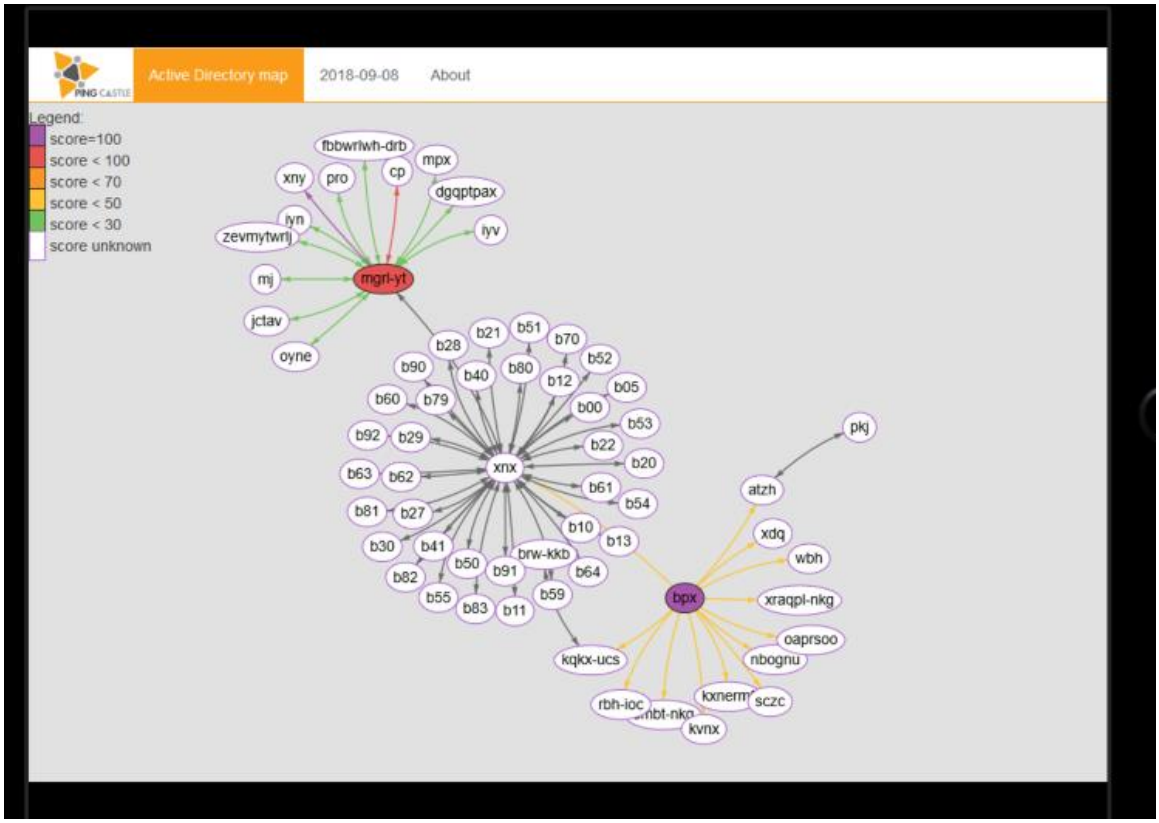


Figure 7

*Risk prioritisation:*

Function: Generates risk scores based on the severity of detected vulnerabilities, helping administrators prioritise their security.

Example: Is focusing on fixed high-risk vulnerabilities first, such as disabling unused admin accounts that are on security threats.

*Health check reports:*

Function: Provide detailed report that outlines the current state of Active Directory security.

Example: A report indicating that certain Active Directory domains are not replicating properly, which could lead to potential security gaps.

## 6.3 BloodHound

### 6.3.1 Role in Active Directory Security:

*Attack Path Virtualisation:*

Function: Bloodhound creates graphical representation of Active Directory relationships, making it easier to understand how permission and connections can be abused.

Example: Visualising how a user in the finance department could potentially gain access to IT resources through shared group memberships.

The Bloodhound cyber security tool then analyses the data and produces visualizations of attack paths in the domain. An example version of attack paths  as shown in Figure 8 :

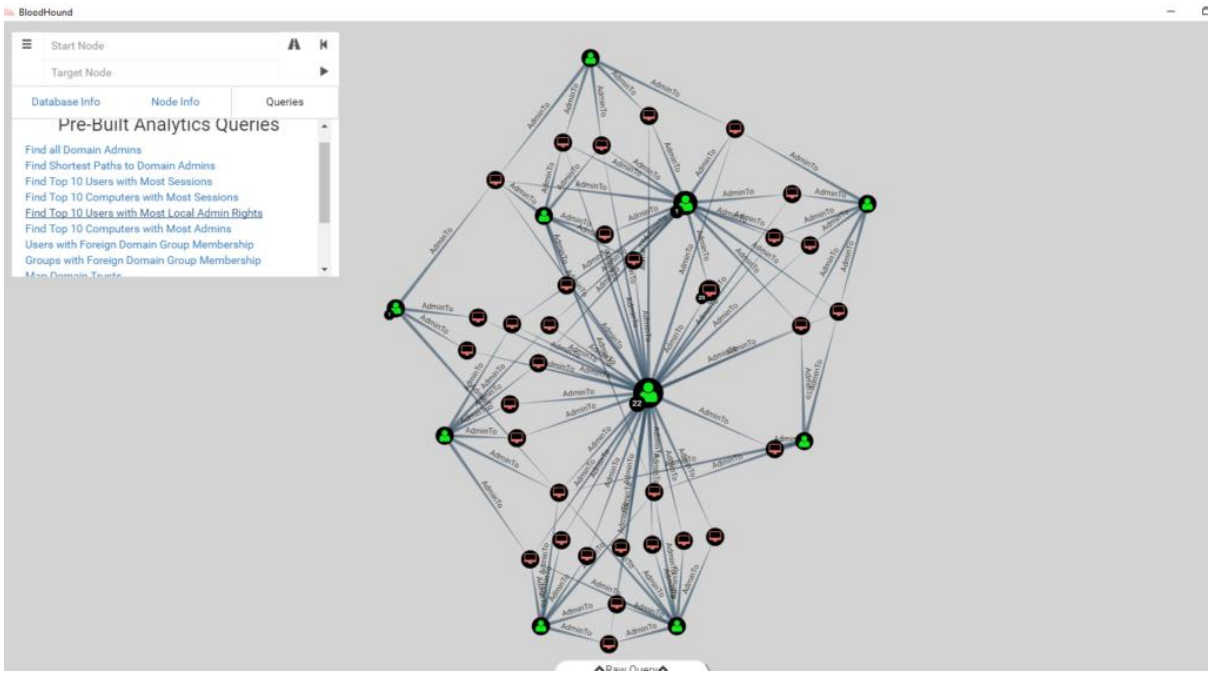


Figure 8

*Privilege escalation detection:*

Function: Identifies potential points were attackers could escalate their privileges within Active Directory, allowing for preset the security measure.

Example: Detecting accounts with excessive privileges that could be targeted to gain broader access to the network.

*Permission analysis:*

Function: maps out user and group permissions to identify areas where access controls can be tightened.

Example: Discovering that some users have access to sensitive data that is not necessary for their roles, enabling administrators toremove unnecessary permissions.

## 6.4 OpenVAS

### 6.4.1 Role in Active Directory Security:

*Vulnerability Assessment:*

Function: OpenVAS scans Active Directory servers and related infrastructure to identify vulnerabilities such as unpatched software, misconfigured services, or exposed ports.

Example: Detecting outdated version of software on Domain Controllers that are at risk to be exploited by attackers. The Greenbone Community Edition dashboard lets you filter vulnerability scan results interactively. You can view the detected vulnerabilities and sort them by their severity as shown in Figure 9.

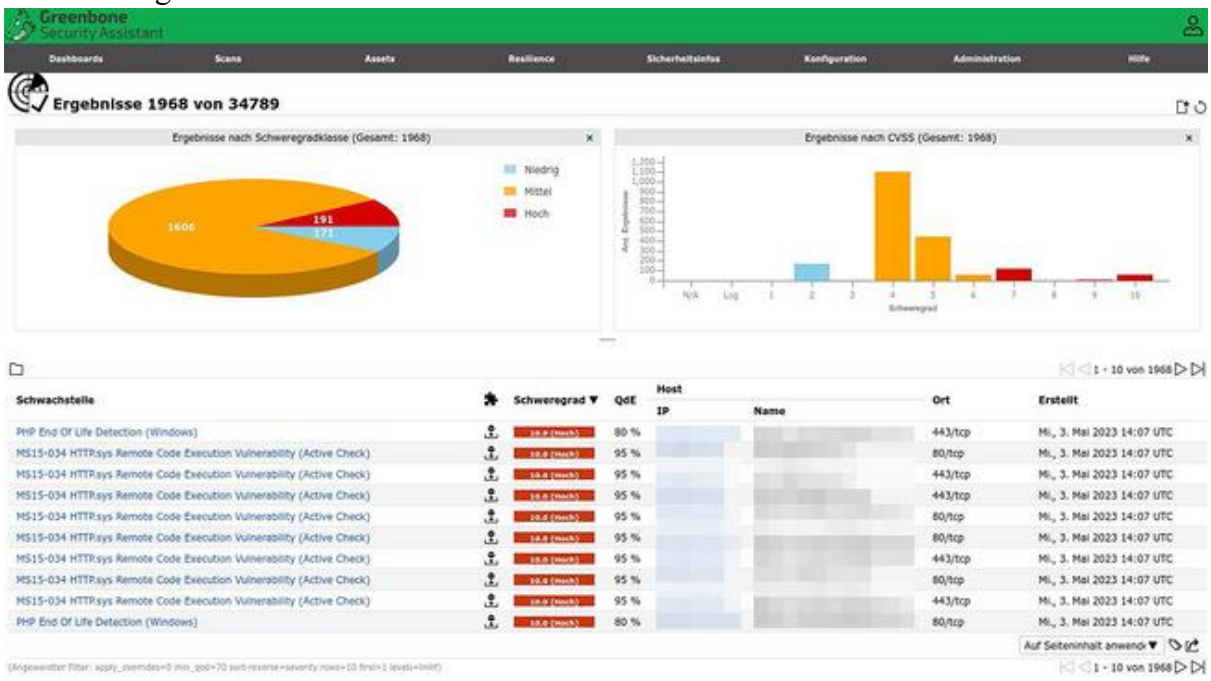


Figure 9

In

*Security reporting:*

Function: Provide report on identified vulnerabilities, including descriptions, severity levels, and recommended fixes.

Example: A report listing multiple vulnerabilities in the network's DNS configuration, and the steps to remediate each issue.

*Regular scanning:*

Function: Allows for schedule scouts to ensure that the Active Directory environment remains secure overtime by identifying new vulnerabilities as they arise.

Example: Setting up weekly scans to detect and display new vulnerability promptly, maintaining a secure Active Directory environment.

## 6.5 Integration of security tools:

These open-source tools work very well to provide a multi-layered security approach for Active Directory environments. Wazuh offers continuous monitoring and threat detection, PingCastle provide comprehensive security audits, BloodHound visualise potential attack pads, and open VAS identifies and helps remediate vulnerabilities. Together, they form a robust framework that enhances Active Directory security without significant financial investment. Together they create a strong framework that boosts Active Directory security with minimal cost.

# 7. References


(2024) *What is Active Directory?* Available at: https://www.quest.com/solutions/active-directory/what-is-active-directory.aspx (Accessed: 03 November 2024).

*Active directory security best practices* (2023) *Netwrix*. Available at: https://www.netwrix.com/active-directory-best-practices.html (Accessed: 07 November 2024).

Devry, J. (2024) Zero trust in active directory: A practical guide, Cybersecurity Insiders. Available at: https://www.cybersecurity-insiders.com/a-practical-guide-to-applying-zero-trust-principles-to-active-directory-for-microsoft-on-premises-and-hybrid-environment-protection/ (Accessed: 07 November 2024).

*Active directory organizational unit design principles* (2011) *Jay Paloma's Tech and Music Blog*. Available at: https://jpaloma.wordpress.com/2011/01/19/active-directory-organizational-unit-design-principles/ (Accessed: 07 November 2024).

Wazuh (2024) *Open source XDR. open source siem.*, *Wazuh*. Available at: https://wazuh.com/ (Accessed: 07 November 2024).

*Map* (2019) *PingCastle*. Available at: https://www.pingcastle.com/documentation/map/ (Accessed: 07 November 2024).

Warren, J. (2023) *Attack path mapping with bloodhound ad*, *Domain Attacks with BloodHound AD*. Available at: https://blog.netwrix.com/2023/01/20/bloodhound-active-directory-html/ (Accessed: 07 November 2024).

Iainfoulds (2024) *Active directory domain services overview*, *Microsoft Learn*. Available at: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (Accessed: 07 November 2024).

*Open vulnerability assessment system (openvas)* (2023) *Federal Office for Information Security*. Available at: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/Tools/OpenVAS/OpenVAS_node.html (Accessed: 07 November 2024).

*Main page* (2024) *Proxmox VE*. Available at: https://pve.proxmox.com/wiki/Main_Page (Accessed: 07 November 2024).

Scooley (2024) *Introduction to hyper-V on windows*, *Microsoft Learn*. Available at: https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/ (Accessed: 07 November 2024).