Cybersecurity Analysis on Network Infrastructure Implemented in Microsoft Azure

Hector Manuel Herrera, David Gregorio Rubio Vizacaya, José Carlos Gallego Mina and Luis Alexis Plazas Gómez

Fundación Universitaria Los Libertadores / Universidad Distrital Francisco José de Caldas, Colombia

Abstract: This article presents a detailed analysis of cybersecurity in a network infrastructure deployed on Microsoft Azure. It reviews key configurations and components for optimal functioning in the cloud. By employing ethical hacking techniques and specialized tools, the article identifies vulnerabilities in the network and its individual elements. Importantly, it uses free software tools to pinpoint potential weaknesses in an Azure-implemented infrastructure, highlighting shortcomings that organizations using Azure might experience.

The analysis covers various aspects of network security, including firewall configurations, virtual network setups, and identity management. It emphasizes the importance of regular security assessments and updates to maintain a robust defense against potential threats. Additionally, the article discusses the role of encryption in protecting data both at rest and in transit, ensuring that sensitive information remains secure.

The test results determine the security level of the infrastructure, ensuring the integrity, confidentiality, and availability of information. Consequently, this analysis provides Microsoft Azure platform administrators with valuable security tools and guidance for deploying and securing cloud network infrastructures. By following the recommendations outlined in the article, administrators can enhance their security posture, mitigate risks, and protect their organization's data from cyber threats.

Keywords: Cybersecurity, Cloud infrastructure, Vulnerability analysis, Ethical Hacking, Microsoft Azure.

1. Introduction

For organizations, information has been and continues to be one of the most important assets. Consequently, it has become relevant to take the necessary measures to safeguard it from potential threats that could affect it economically, reputationally, and legally. As long as vulnerabilities exist and people can exploit them with the intention of demanding money or obtaining classified information, no company can be considered completely secure.

Additionally, there is a trend to migrate information, processes, and services to cloud platforms such as Microsoft Azure or Amazon AWS, among others. This fact can increase the vulnerability of information exposed on the Internet. The adoption of the cloud offers significant advantages, such as scalability and cost reduction, but also requires careful security management to protect sensitive data.

Currently, there are tools accompanied by ethical hacking techniques that allow identifying vulnerabilities and security gaps in different applications, servers, digital platforms, local networks, and cloud networks. These practices include penetration testing, vulnerability analysis, code reviews, and continuous monitoring. Furthermore, the implementation of robust security policies and constant staff training are essential to maintain the integrity and confidentiality of information.

2. Background

Cloud computing has positioned itself as one of the most used and popularized Internet technologies for today's organizations. Migrating their network infrastructure, applications, and computing services to the cloud can bring economic advantages of versatility, scalability, and ease of administration. In contrast, in an on-premise platform, the same benefits would be more

Received: December 2nd, 2024. Accepted: June 5th, 2025
DOI: 10.15676/ijeei.2025.17.2.5

difficult and costly to implement. However, having an entire information technology platform deployed on the Internet also exposes it and makes it more susceptible to security risks and cyberattacks (Muñoz-Calderón, 2020).

There are several cloud service models (Fuentes, 2014), such as:

- Cloud Software as a Service (SaaS): In cloud software as a service, the capability provided to the consumer consists of using the provider's applications running on a cloud infrastructure.
- Cloud Platform as a Service (PaaS): In cloud platform as a service, the capability provided to the consumer is to deploy onto the cloud infrastructure applications acquired or created by the consumer, which were developed using programming languages and tools supported by the provider.
- Cloud Infrastructure as a Service (IaaS): In cloud infrastructure as a service, the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources so that the consumer can deploy and run arbitrary software.

This last model, IaaS, will be used to implement and analyze cybersecurity and ethical hacking of the cloud platform. In this case, the shared responsibility model specifies the least amount of responsibility on the part of the cloud service customer (Evelin Pilar Díaz Rodríguez, 2022).

For platforms exposed in cloud services, the security risk is potentially higher due to having services exposed to the Internet, which implies vulnerability to cyberattacks, data loss, privacy breaches, service availability failures, among others (Mario Casasola Robles, cloudMIDDLEtrust, 2014).

The risks involved in implementing cloud platforms are analyzed according to Carrasco (2014), who studies the outsourcing of cloud computing services and the new challenges in computer security that this entails. He also analyzes the advantages of using these public cloud platforms and, above all, the disadvantages from the perspective of computer security.

Although the analysis will not be addressed in this document, it is recommended to validate computer security in applications and infrastructures implemented on cloud platforms, addressing the issue from a legal and responsibility standpoint, both for the organization contracting the cloud services and the provider offering the service (O, 2011).

Finally, regarding shared responsibility for penetration testing in the cloud, service level agreements and obligations of each party (client and provider) must be taken into account. In this case, the cloud provider is responsible for the physical security of the data centers, while the customer is responsible for protecting their data and applications stored in the cloud environment under the IaaS model (startechup, 2023).

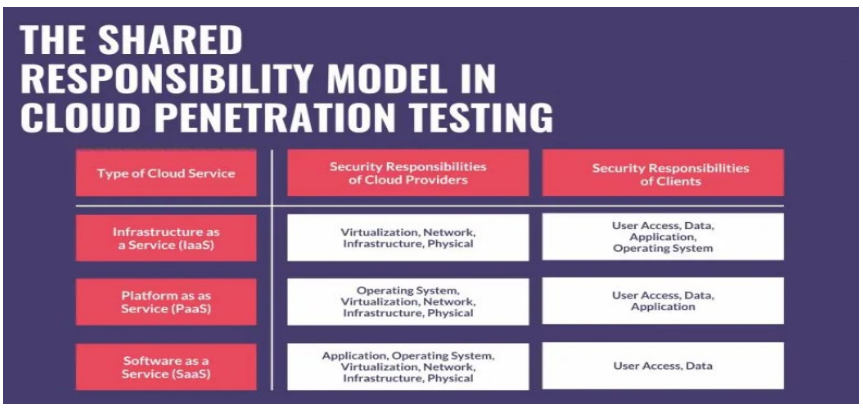


Figure 1. Shared responsibility model for cloud penetration testing. Source: (startechup, 2023)

Terms and Definitions

- **Azure**: Azure is a large collection of servers and network hardware running a complex set of distributed applications. These applications orchestrate the configuration and operation of the virtualized hardware and software on those servers. This platform is public and implemented in Microsoft's cloud (Microsoft, 2023).
- **Cloud Computing**: Cloud computing is the use of a network of remote servers connected to the Internet to store, manage, and process data, servers, databases, networks, and software that expose their services publicly over the Internet (Salazar, 2016).
- **ISO 27017 Standard**: ISO 27017 provides guidelines for implementing information security controls in cloud computing services, considering scenarios for both clients and providers of this type of service. This standard is based on the best practices for information security defined in ISO 27002 and complements information regarding cloud-specific controls (Bonfante, 2019).
- **ISO 27018 Standard**: ISO 27018 is the first international standard on cloud privacy. This standard is fundamentally based on laws and regulations issued in the European Union (Carlos Manuel Fernández, 2015).
- **NMAP**: NMAP is an open-source tool that allows for a series of scans within a network. This tool is cross-platform, providing network administrators and security consultants the ability to scan network ports and launch a series of scripts to detect potential vulnerabilities in the scanned equipment or network (Pereda, 2019).

Implementation of infrastructure in a cloud environment allows organizations to obtain advantages over On-Premises infrastructures, such as lower costs and ease of administration, among others. However, the security advantages remain to be validated when a cloud infrastructure is implemented for an organization (Guevara Jiménez, 2022).

Just like information in an On-Premise environment, information in cloud environments is also susceptible to attacks such as theft, hijacking, or damage. This underscores the importance of validating vulnerabilities that can be identified in these environments, the exposed risks, and considering measures to secure the environment along with the contained information. In this context, risks have been identified, their criticality ranges, associated vulnerabilities, and the platforms or clouds related to various organizations that have contracted them (Cuestas, 2019).

In the security evaluation of the main cloud platforms, including Azure, reasons are presented that rule out Oracle Cloud or Google Cloud due to configuration issues and an unfriendly interface, which can cause configuration errors, inadvertently opening security gaps that can eventually materialize security events. There is also a lack of clarity in the legal information of the service to be contracted, especially in Google's cloud. In contrast, Azure and AWS have a more user-friendly platform, free training content, and clarity in the terms and conditions and the legal aspects of the service to be contracted according to the region where it is implemented (Acevedo, 2022).

Security reports have been conducted where the security of cloud storage on the Microsoft Azure platform is analyzed, but these are focused on the detection and recovery from ransomware attacks, the impact of a materialized attack, recovery times, and recovery points. However, they do not identify other vulnerabilities to which this platform may be exposed (Trevejo, 2022).

Similarly, there is a description of the methodology and specifications for conducting intrusion tests in AWS cloud environments with attacks and identification of vulnerabilities, also using ethical hacking tools. Although the methodology is defined in this case, an analysis of the security level of the cloud platform is not conducted (Pavón, 2022).

For the vulnerability scanning process on the implemented platform, an audit plan can be viable as a methodological guide to follow, identifying threats, risks, and improvement actions associated with the contracted model (IaaS) and the implemented services, complemented by a remediation proposal. This evaluation, conducted independently and objectively, will allow identifying the security level of the evaluated system (Beatriz P. de Gallo, 2022).

Additionally, a similar methodology can be implemented that outlines the steps and procedures for conducting penetration tests on mobile applications in Google's public cloud. However, it does not expose the test results or the analysis of the detected security levels, but part of the methodology can be applied for the analysis of this article (Diego Jara, 2017).

3. Research methodology

For the development of this project, a quantitative methodology will be used, which will allow us to obtain concrete and reliable data to draw conclusions about the security of network infrastructure in a cloud environment on Microsoft Azure. The methodology used in this study will detail the devices to be analyzed, the techniques and programs with which the results will be analyzed.

Based on the conclusions obtained from the results, an assessment can be made regarding the security of a network implemented in the Azure cloud with the proposed infrastructure (see Figure 2). This quantitative approach is essential to ensure objectivity and accuracy in the security evaluation, allowing for the identification of specific vulnerabilities and areas for improvement.

Additionally, comparative analyses with other cloud platforms will be included to contextualize the findings and provide a more comprehensive view of the advantages and disadvantages of using Azure in terms of security. The implementation of this methodology will not only validate the security of the proposed infrastructure but also establish recommendations to strengthen data protection and network integrity in cloud environments.

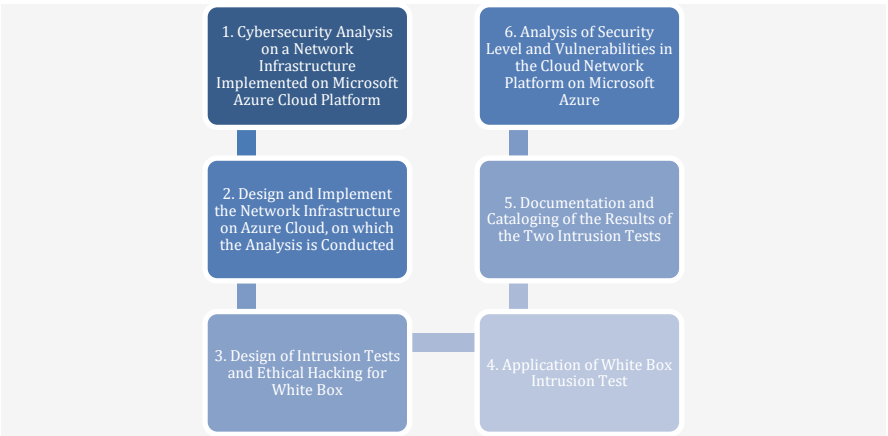


Figure 2. Steps of the Methodology Source: Own Elaboration

4. Results and discussion

Implementation of Infrastructure on Azure

In the implemented network architecture, the enabled servers and services correspond to standard services that are typically present in the technological platforms of any organization. These include HTTPS pages, file transfer services such as SFTP and SMB, databases like MSSQL Server and MySQL, and an environment composed of subnets and VPN access (see Figure 3, Table 1).

One of the advantages of implementing and deploying the infrastructure on a cloud platform is its agility and versatility. This allowed the proposed model to be deployed and configured in approximately 36 hours, making it ready for vulnerability exploration and analysis.

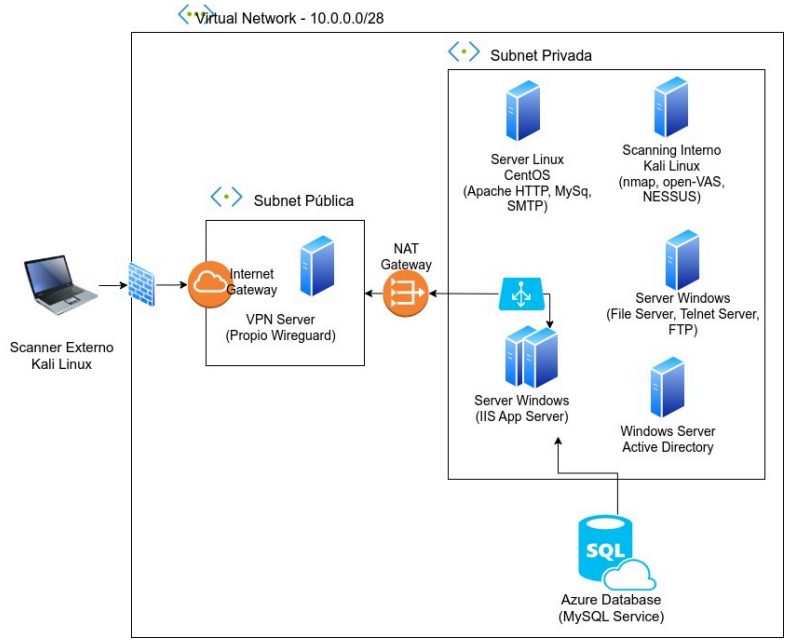


Figure 3. Network infrastructure design Source: own elaboration

Table 1. Inventory of the implemented infrastructure

SO	Exposed Services or Role	Exposed Ports	IP Address	Network (internal or external)
Kali Linux	Escáner	N/A	10.0.0.4/28	Internal
CentOS	HTTPS SFTP MYSQL SMTP	TCP 443 TCP 22 TCP 3306 TCP 25	10.0.0.6/28	Internal
Windows Server 2019	Directorio activo (proyect.com.dns)	TCP 3389	10.0.0.5/28	Internal
Windows Server 2016 datacenter	SFTP SMB HTTP RDP	TCP 22 TCP 445 TCP 80 TCP 3389	10.0.0.7/28	Internal
Windows Server 2019	SQL Server RDP	TCP 1433 TCP 3389	10.0.0.8/28	Internal
WINDVPN	Gateway RDP	TCP 3389	10.0.0.20/28	External/internal
Azure Virtual Network Gateway	VPN	N/A	N/A	External
NAT Gateway	N/A	N/A		Interna

Brief Description of the Implementation

1. Creation of the subscription in Microsoft Azure
2. Creation of the virtual network
3. Creation of subnets
4. Creation of servers and virtual machines

5. Creation and configuration of VPN
6. Public IP and VPN access tests

Intrusion Testing from Internal and External Scanning Machines

For the execution of the intrusion tests, two Linux scanning machines were prepared to use the NMAP and NESSUS tools. One of these machines is located outside the implemented infrastructure and will be used for the external or black-box intrusion test. The other machine is located within the internal network of the infrastructure implemented on Azure.
In the planning of the intrusion tests, a complete network scan will be performed to identify hosts, open ports, and exposed services, as well as their versions and operating systems. Additionally, exposed folders or files on web services will be identified.

Execution of Scanning Tests

For the vulnerability analysis with NMAP and NESSUS, each host in the infrastructure and the entire network will be analyzed individually. It is necessary to update and download the vulnerability databases before using the scanning tools. For the external scanning test, the public connection exposing the Azure VPN will be analyzed using the URL (azuregateway-99ba0077-0633-4763-b424-e8197bd83633-9ad228ae9961.vpn.azure.com) or the public IP 4.227.194.97. In the internal test, the vulnerability scan will be directed towards the internal network address of the implemented environment, which in this case is 10.0.0.0/28.

External Scanning Test with NMAP

The commands used for the vulnerability analysis with NMAP in the external scan from Kali Linux are parameterized to generate an output file in XML format (see Figure 4, 5, and 6), which will later be converted to HTML format for easier reading.

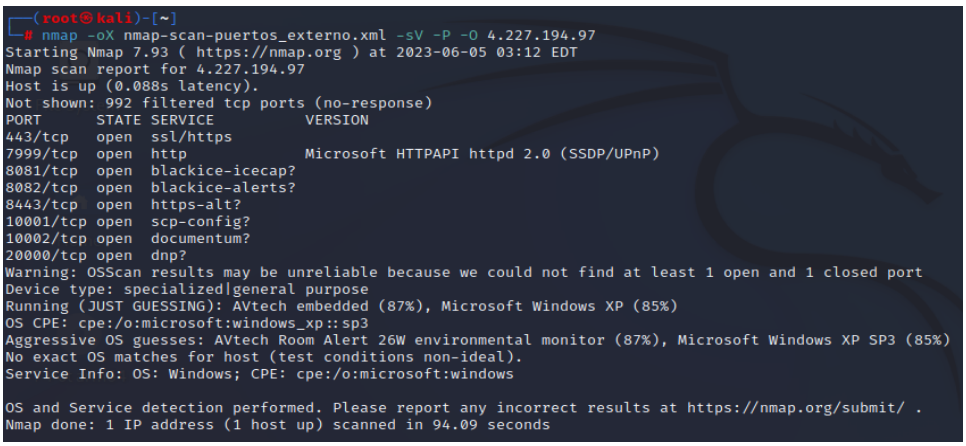


Figure 4. Identification of ports, services and operating system Source: own elaboration

During the scan, several open ports were found, including: 443, 7999, 8081, 8082, 8443, 10001, 10002, and 20000. These ports can be exploited to compromise the security of services, gain unauthorized access to system resources, infiltrate the system, and escalate privileges to take control of the server.

To minimize the exposure of unnecessary ports for VPN connection, it is recommended to:

1. Enable and configure a firewall as the first line of defense in the network.
2. Update the firmware of network components.
3. Block the ICMP protocol.
4. Perform periodic network scans.
5. Use VLANs for network segregation.

6. Implement IPS (Intrusion Prevention System).
7. Utilize UTM (Unified Threat Management).
8. Implement WAF (Web Application Firewall).

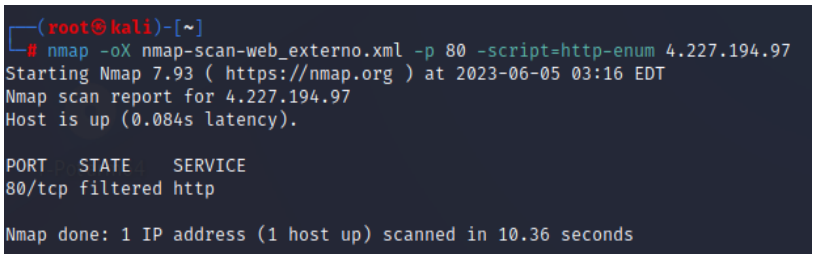


Figure 5. Identification of Web files or folders Source: own elaboration

In this case, the scan results do not provide any information that could be used by an attacker.

Figure 6. Identify vulnerabilities with NMAP + Vulscan Source: own elaboration

During this analysis, several CVEs were identified on hosts not associated with the subscription. Below are some examples:

- *CVE-2013-3174*: DirectShow in Windows systems allows remote attackers to execute arbitrary code through a crafted GIF file. This vulnerability, also known as the "DirectShow Arbitrary Memory Overwrite Vulnerability" (CVE, 2023), can be mitigated by applying updates provided by Microsoft.
- *CVE-2013-3154*: The signature update functionality in Windows Defender on Microsoft Windows 7 and Windows Server 2008 R2 relies on an incorrect path name. This allows local users to gain privileges through a Trojan horse application in the top-level %SYSTEMDRIVE% directory. This vulnerability is known as the "Microsoft Windows 7 Defender Inadequate Path Name Vulnerability" (CVE, 2023). To mitigate this vulnerability, it is crucial to update the operating system with the updates provided by Microsoft.
- *CVE-2009-3555*: The TLS protocol, and the SSL 3.0 protocol and possibly earlier versions, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, various Cisco products, and other products, do not properly associate renegotiation handshakes with an existing connection. This allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context. This issue is known as the "plain text injection attack" or the "Project Mogul" problem (CVE, 2023). To mitigate this vulnerability, the OpenSSL project should be updated to the latest version available, which at the time of this documentation is 1.0.2.

To mitigate these vulnerabilities, it is essential to apply the security updates provided by the respective vendors. Additionally, conducting regular security audits to identify and remediate potential system vulnerabilities is recommended. Implementing additional security measures, such as properly configuring firewalls and intrusion prevention systems (IPS), can also help protect systems from potential attacks.

External Scanning Test with NESSUS

The NESSUS application is executed through a web browser, configuring the external scan to the public IP address of VPN access (see Figure 7). During the external scanning process, Nessus identifies several vulnerabilities, classifying them by level of criticality (see Figure 8). These vulnerabilities can range from configuration issues to security flaws that could be exploited by attackers.

The scan with NESSUS includes a detailed assessment of each vulnerability, providing information on the potential impact and recommendations for mitigation. The tool analyzes various aspects of security, such as port exposure, service configuration, and the presence of outdated software. At the end of the scan, Nessus generates vulnerability reports in PDF format, which are essential for evaluation and planning corrective measures (tenable, 2023).

These reports allow system administrators to quickly identify critical areas that require immediate attention. Additionally, the detailed documentation facilitates the implementation of appropriate security solutions, such as software updates, service reconfiguration, and the application of security patches. Using NESSUS in external scanning is a fundamental practice for maintaining the integrity and security of the network infrastructure.

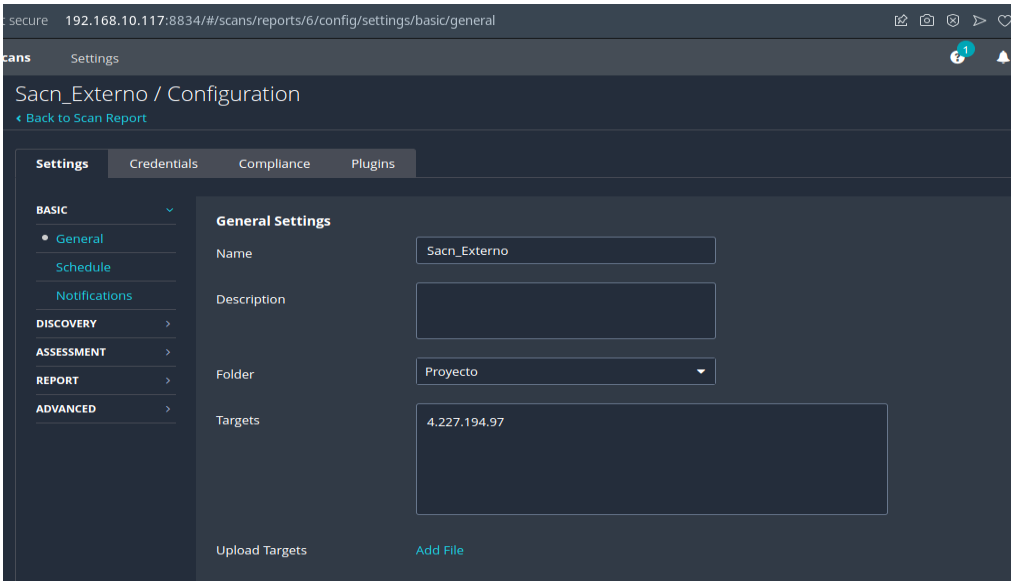


Figure 7. Nessus External Scan Settings Source: own elaboration

To conduct a vulnerability analysis using the Nessus tool, it is necessary to create a project. In this project, you must assign a name and specify an IP address or a range of IP addresses to be analyzed as the target. This process allows Nessus to identify and evaluate potential vulnerabilities present in the systems and services associated with the selected IP addresses. Proper configuration of the project is crucial to ensure that the analysis is thorough and accurate, providing detailed information on security risks and recommended mitigation measures.

The result of this vulnerability analysis found that the server certificate is unreliable. This certificate does not have a known public certification authority, and the criticality level of this finding is medium, associated with ID 51192.

To mitigate this vulnerability, it is recommended to generate the certificate with a recognized certification authority, such as GOGETSSL, or issue an SSL certificate authenticated by the internal PKI issuing CA. Subsequently, the certificate should be assigned to the RDP store and the personal store, the default SSL certificate should be removed, and the server should be restarted.

Another finding was the identification of the operating systems of some machines in the infrastructure. Although the criticality level of this finding is low, it represents a risk as it reveals information about the infrastructure or tenant shared with other customers of the Azure platform.

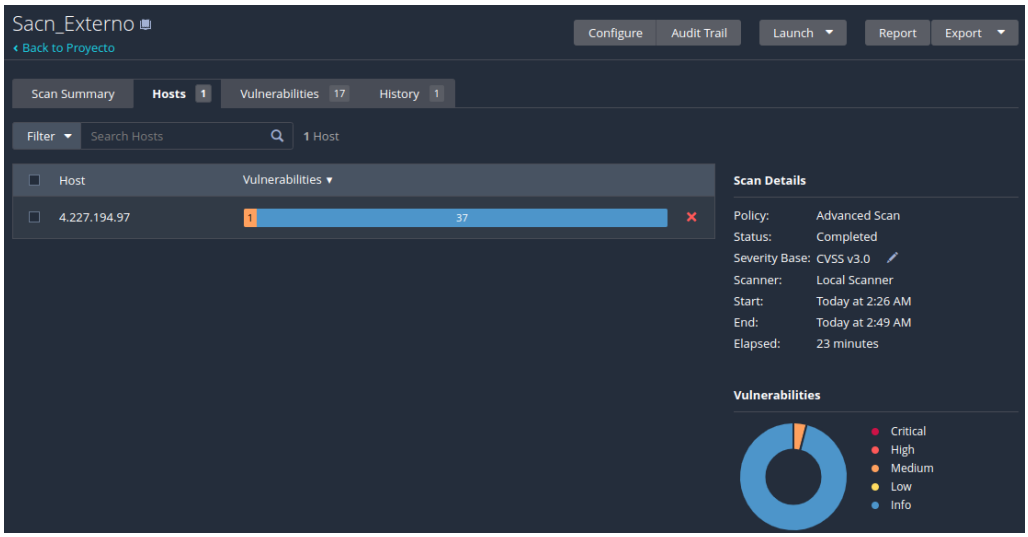


Figure 8. External scanning process with Nessus Source: own elaboration

Internal Scan Test with NMAP

For the vulnerability analysis with NMAP in the internal scan from Kali Linux, parameterized commands were used to generate an output file in XML. This file is subsequently converted to HTML format to facilitate reading (see Figure 9, 10, and 11). As in the external scan, this process allows identifying possible vulnerabilities and evaluating the security of the internal infrastructure.

```
┌──(root㉿kali)-[/home/kaliuser]
└─# nmap -oX nmap-scan-puertos_interno.xml -sV -P -O 10.0.0.0/28
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-05 05:53 UTC
Nmap scan report for 10.0.0.1
Host is up (0.00057s latency).
All 1000 scanned ports on 10.0.0.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 12:34:56:78:9A:BC (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

Figure 9. Identification of ports, services and operating system Source: own elaboration

Through this network vulnerability analysis, not only were the ports identified, but also information about some servers. The ports found were: 22, 53, 80, 88, 135, 139, 389, 443, 445, 3306, 4674, 593, 636, 3268, 3269, 3389, and 5357. The information obtained includes the operating system and some services exposed by these ports, such as OPENSSH, MYSQL, and APACHE. Identifying these ports and services is crucial, as each can represent a potential attack vector if not properly managed.

The exposure of these ports can be minimized through operating system hardening tasks. Hardening involves applying additional security configurations and removing unnecessary services to reduce the attack surface. This can include disabling unused ports, implementing firewalls, and applying security patches.

To prevent information from being obtained from Apache, the file /etc/apache2/conf-available/security.conf should be modified. In this file, the directives ServerTokens

OS and ServerSignature On should be changed to ServerTokens Prod and ServerSignature Off. After making these modifications, the changes should be saved. These configurations ensure that Apache does not reveal information about the server version and other details that could be used by attackers to exploit specific vulnerabilities.

To address the OpenSSH vulnerability, the file located at /etc/ssh/sshd_config can be edited, adding DebianBanner no at the end of the file. The changes should be saved, and the service restarted with the command systemctl restart sshd. This configuration hides the Debian banner displayed when connecting via SSH, which can prevent attackers from obtaining information about the operating system and the version of OpenSSH used, thus making it more difficult to plan targeted attacks.

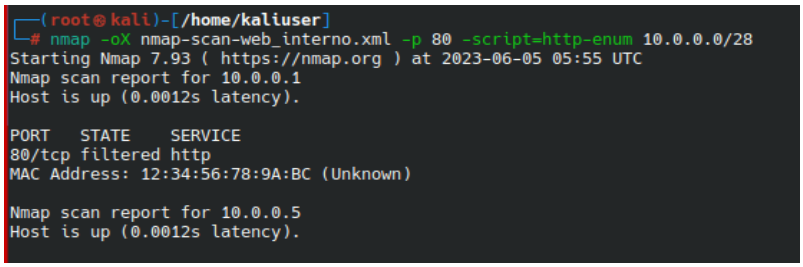


Figure 10. Identifying folders or files on Web servers Source: own elaboration

When performing the port analysis on the internal network, information about some ports and a directory was obtained. This analysis is crucial for identifying potential entry points that attackers could exploit. The exposed port, from which directory information is being acquired, is port 80 on IP 10.0.0.6, corresponding to the Linux CentOS application server. Port 80 is used by the HTTP protocol, which transmits data in plain text, potentially allowing attackers to intercept and access sensitive information.

This vulnerability can be mitigated by applying correct configurations to the HTTP service or, alternatively, migrating the service to HTTPS. Migrating to HTTPS involves using an SSL/TLS certificate, which encrypts the communication between the server and clients, thus protecting the transmitted information. Additionally, it is advisable to review and adjust the security configurations of the web server to minimize the exposure of unnecessary data and services.

Figure 11. Identifying vulnerabilities with NMAP + Vulscan Source: own elaboration

This analysis revealed several vulnerabilities, including:

- CVE-2006-5229: OpenSSH portable 4.1 on SUSE Linux, and possibly on other platforms and versions with limited configurations, allows remote attackers to determine valid usernames through timing discrepancies, where responses take longer for valid usernames than for invalid ones, as demonstrated by sshtime. Note: As of 20061014, it appears that this issue depends on the use of manually configured passwords that cause delays when processing /etc/shadow due to a higher number of rounds (CVE, 2023). Mitigation: It is recommended to update the OPENSSH project to address this vulnerability. Updating OpenSSH to the latest version ensures that security patches are applied, correcting this and other known vulnerabilities, thereby improving the overall security of the system.
- CVE-2012-5975: The SSH USERAUTH CHANGE REQUEST function in SSH Tectia Server 6.0.4 to 6.0.20, 6.1.0 to 6.1.12, 6.2.0 to 6.2.5, and 6.3.0 to 6.3.2 on UNIX and Linux, when old-style password authentication is enabled, allows remote attackers to bypass authentication through a manipulated session involving blank password entries, as

demonstrated by a root login session from a modified OpenSSH client with an input_userauth_passwd_changereq call added in sshconnect2.c (CVE, 2023). Mitigation: This vulnerability can be addressed by disabling old-style password authentication. Disabling old-style password authentication and using more secure authentication methods, such as SSH keys, significantly reduces the risk of brute force attacks and other authentication bypass methods.

- CVE-2005-2573: The mysql_create_function function in sql_udf.cc for MySQL 4.0 before 4.0.25, 4.1 before 4.1.13, and 5.0 before 5.0.7-beta, when running on Windows, uses an incomplete blacklist in a directory traversal check, allowing attackers to include arbitrary files via the backslash () character (CVE, 2023). Mitigation: This vulnerability is resolved by migrating MySQL to version 4.0. Upgrading MySQL to a newer version not only fixes this specific vulnerability but also provides additional performance and security improvements that protect against a wide range of threats.

Internal Scan Test with NESSUS

The NESSUS application is run through a web browser, configuring the internal scan to the local network address (see Figure 12). During the internal scan process, the Nessus application identifies several vulnerabilities for each of the hosts located on the internal network, categorizing them by criticality level (see Figure 13). Nessus classifies vulnerabilities into categories such as critical, high, medium, and low, allowing for prioritization of corrective actions based on the risk level. Upon completion of the Nessus scan, vulnerability reports are generated in PDF format for evaluation. These detailed reports provide a solid basis for planning and executing mitigation measures, thereby improving the security posture of the internal network.

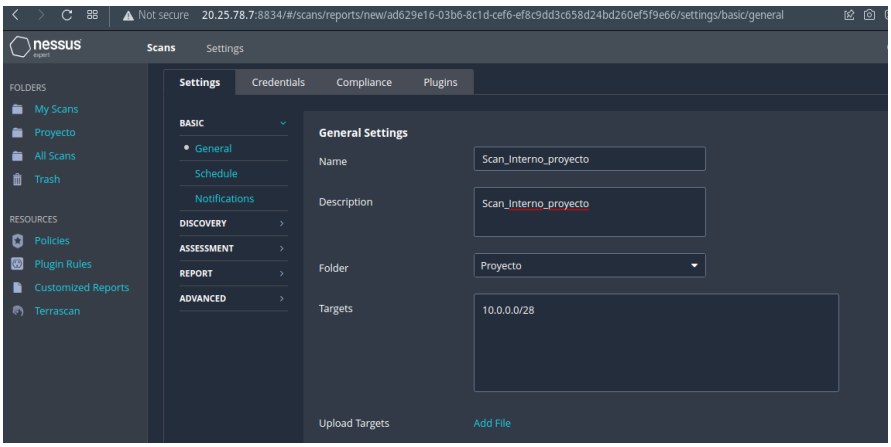


Figure 12. Internal scan configuration with Nessus Source: own elaboration

The result of this vulnerability analysis found that the server certificate is unreliable. This certificate does not have a known public certification authority, and the criticality level of this finding is medium, associated with ID 51192. An unreliable certificate can allow attackers to intercept and manipulate communication between the server and clients, potentially leading to the exposure of sensitive data and identity spoofing attacks. To mitigate this vulnerability, it is crucial to obtain certificates from a recognized certification authority, ensuring the authenticity and integrity of communications.

Another vulnerability found is that the daemon processes on the remote host are associated with programs that have been manually installed. This finding has a low priority and is associated with ID 33851. Manually installed domain processes may not follow best security practices and could introduce uncontrolled vulnerabilities into the system. To mitigate this vulnerability, native package management tools of the operating system should be used to manage the

installation, updates, and removal of software. This ensures that the installed packages are verified and maintained by the community or the operating system provider, reducing the risk of introducing malicious or insecure software.

Figure 13. Internal scan process with Nessus Source: own elaboration

Internal Analysis of Microsoft Azure

Automatically, and through Microsoft Defender for Cloud, which is native to the Azure platform, a security analysis of all instances implemented in the subscription is generated. Microsoft Defender for Cloud provides continuous security assessment, identifying vulnerabilities and misconfigurations in real-time. This allows system administrators to take proactive measures to protect their cloud resources. For example, for the Windows Server with Active Directory role, the following security issues are reported (see Table 2): Vulnerabilities in an Active Directory server can be especially critical, as this server manages the authentication and authorization of users and services on the network. Identifying and correcting these issues is essential to maintaining the integrity and security of the entire IT infrastructure.

Table 2. Shows Azure security results

Recommendation	Description	Remediation
Virtual machines must encrypt temporary disks, caches, and data flows between compute and storage resources.	Temporary disks and data caches are not encrypted, and data is not encrypted when flowing between compute and storage resources. Use Azure Disk Encryption to encrypt all these data.	To enable disk encryption on your virtual machines, follow the provided encryption instructions.
The Log Analytics agent must be installed on virtual machines.	Defender for Cloud collects data from your Azure virtual machines (VMs) to monitor security vulnerabilities and threats. The data is collected via the Log Analytics agent, which reads various security-related configurations and event logs from the machine for analysis.	To learn various ways to install and configure your Log Analytics agent, refer to the instructions.

Source: own elaboration

Analysis of the External Instruction or Black Box Test Results

The external scan with NMAP does not reflect vulnerable ports exposed on the public IP address of the VPN (see Figure 14). This indicates that, at first glance, the VPN configuration does not present open ports that can be directly exploited from the outside, which is a good indication of perimeter security. Regarding exposed folders or web services, NMAP does not identify any. This suggests that there are no visible or accessible web services from the public IP, reducing the risk of web-based attacks.

However, in the joint analysis of NMAP with VULSCAN on the public address of the VPN, multiple exposed systems with known vulnerabilities are identified, as evidenced in the generated report (see Figure 15). This finding is crucial, as although the ports are not directly exposed, vulnerabilities in the systems can be exploited by attackers to gain unauthorized access or cause service interruptions. VULSCAN complements NMAP by providing detailed information about known vulnerabilities associated with the detected systems, allowing for a deeper risk assessment.

Recommendations: To mitigate these risks, it is essential to apply security patches and updates to all systems identified with vulnerabilities. Additionally, additional security measures should be implemented, such as network segmentation and the use of advanced firewalls, to protect critical systems and limit unauthorized access.

Ports

The 992 ports scanned but not shown below are in state: **filtered**

- 992 ports replied with: **no-response**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
443	tcp	open	https	syn-ack			
7999	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP
8081	tcp	open	blackice-icecap	syn-ack			
8082	tcp	open	blackice-alerts	syn-ack			
8443	tcp	open	https-alt	syn-ack			
10001	tcp	open	scp-config	syn-ack			
10002	tcp	open	documentum	syn-ack			
20000	tcp	open	dnp	syn-ack			

Remote Operating System Detection

- Used port: **443/tcp** (**open**)
- OS match: **AVtech Room Alert 26W environmental monitor** (**87%**)
- OS match: **Microsoft Windows XP SP3** (**85%**)

Figure 14. VPN Exposed Ports Source: own elaboration

```
MITRE CVE - https://cve.mitre.org:
[CVE-2013-3661] The EPATHOBJ::bFlatten function in win32k.sys in Microsoft Windows XP SP2 and SP3,
[CVE-2013-3660] The EPATHOBJ::pprFlattenRec function in win32k.sys in the kernel-mode drivers in M
[CVE-2013-3174] DirectShow in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows V
[CVE-2013-3173] Buffer overflow in win32k.sys in the kernel-mode drivers in Microsoft Windows XP S
[CVE-2013-3172] Buffer overflow in win32k.sys in the kernel-mode drivers in Microsoft Windows XP S
[CVE-2013-3171] The serialization functionality in Microsoft .NET Framework 2.0 SP2, 3.5, 3.5 SP1,
[CVE-2013-3167] win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows
[CVE-2013-3154] The signature-update functionality in Windows Defender on Microsoft Windows 7 and
[CVE-2013-3138] Integer overflow in the TCP/IP kernel-mode driver in Microsoft Windows Vista SP2,
```

Figure 15. Systems detected over the VPN Source: own elaboration

As observed in the previous analysis, multiple systems are identified that are not implemented within the contracted infrastructure or subscription. This confirms that Microsoft

Azure has not fully segregated environments for different clients, sharing the same tenant. This situation represents a significant security risk for the contracted environment, as the lack of proper isolation can allow vulnerabilities or misconfigurations in one client to affect others. Additionally, resource sharing can facilitate lateral attacks, where an attacker compromising one system can move laterally to other systems within the same tenant.

In the results of the external analysis conducted with Nessus, only one vulnerability is reported on the public IP of the VPN related to the certificate used for the service, which is self-signed (see Figure 16). Self-signed certificates are not trusted by default, as they are not validated by a recognized certification authority. This can allow man-in-the-middle attacks, where an attacker can intercept and modify traffic between the client and the server. To mitigate this risk, it is necessary for the certificate to be signed by an official certification authority, ensuring the server's authenticity and protecting communication from interception and tampering.

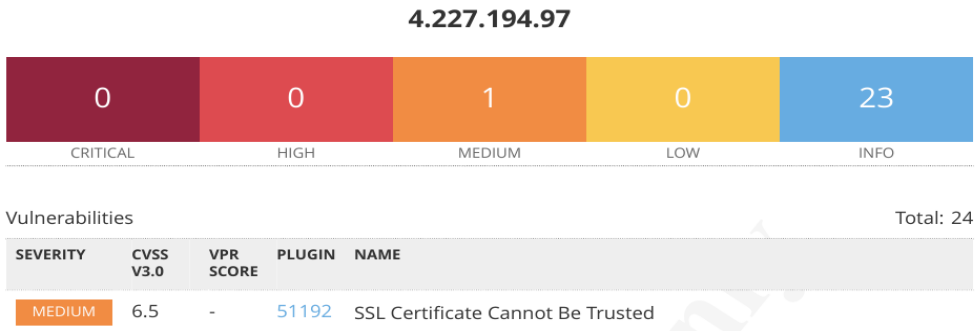


Figure 16. Result of the external analysis carried out with Nessus Source: own elaboration

Analysis of the Internal Instruction or White Box Test

The identification of ports, services, and operating systems with NMAP primarily focuses on Windows systems, detecting open ports for configured services. For example, for the Active Directory server, ports such as LDAP, NETBIOS, and KERBEROS are identified, among others. These ports are essential for communication and authentication within a Windows network, and their correct configuration is crucial for the security and functionality of the environment. Additionally, NMAP not only identifies open ports but also provides detailed information about the versions of the services running. This information is vital for security assessment, as outdated versions may contain known vulnerabilities that could be exploited by attackers.

10.0.0.5

Address

- 10.0.0.5 (ipv4)
- 12:34:56:78:9A:BC (mac)

Ports

The 987 ports scanned but not shown below are in state: **filtered**

- 987 ports replied with: **no-response**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
53	tcp	open	domain	syn-ack	Simple DNS Plus		
88	tcp	open	kerberos-sec	syn-ack	Microsoft Windows Kerberos		server time: 2023-06-05 05:53:37Z
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
389	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP		Domain: proyect.com.dns0., Site: Default-First-Site-Name
445	tcp	open	microsoft-ds	syn-ack			
464	tcp	open	kpasswd5	syn-ack			
593	tcp	open	ncacn_http	syn-ack	Microsoft Windows RPC over HTTP	1.0	
636	tcp	open	tcpwrapped	syn-ack			
3268	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP		Domain: proyect.com.dns0., Site: Default-First-Site-Name
3269	tcp	open	tcpwrapped	syn-ack			
3389	tcp	open	ms-wbt-server	syn-ack	Microsoft Terminal Services		
5357	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP

Remote Operating System Detection

Unable to identify operating system.

- Used port: **53/tcp (open)**

Figure 17. Ports and version of services on Windows server Source: self made

In this specific case, NMAP also shows the domain name and the operating system of the machine, as seen in Figure 17. NMAP's ability to identify specific details about the operating system and domain is particularly useful for system administrators, as it provides a more comprehensive view of the network environment. With this information, informed decisions can be made regarding patch management and updates, as well as the implementation of additional security measures to protect critical systems.

To prevent a port scan from revealing this information, hardening of the operating systems should be performed, following the manufacturer's recommendations as applicable.

In the identification of web folders or files for Linux CentOS and Windows Server application servers, TCP port 80 was detected open, exposing the HTTP service in addition to the configured HTTPS. Specifically, on the Linux CentOS server, exposed folders were also identified (see Figure 18).

10.0.0.6 / centos1.internal.cloudapp.net

Address

- 10.0.0.6 (ipv4)
- 12:34:56:78:9A:BC (mac)

Hostnames

- centos1.internal.cloudapp.net (PTR)

Ports

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack			
	http-enum	/icons/: Potentially interesting folder w/ directory listing					

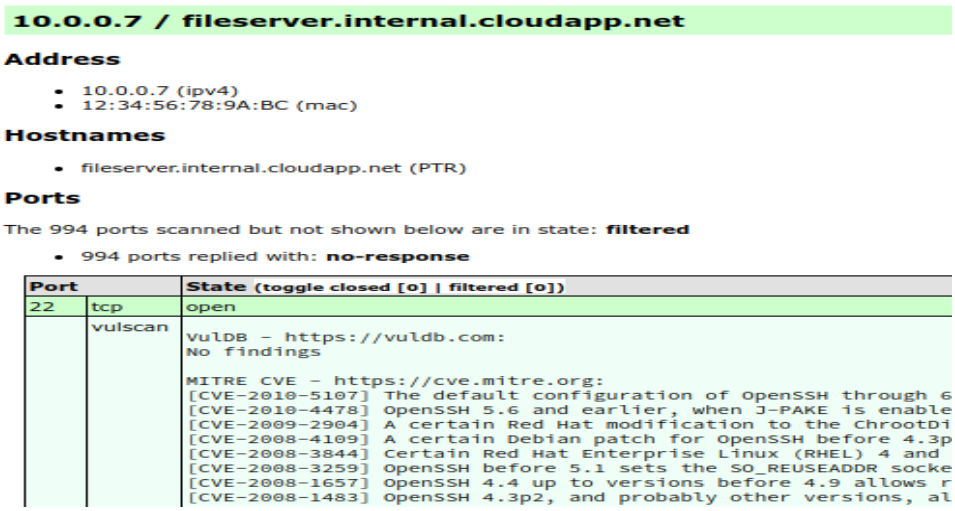
Figure 18. Exposed HTTP folders on Linux CentOS Source: Own elaboration

The results of the vulnerability scan test with NMAP along with VULSCAN provided detailed information about the exposed services on all deployed servers (Linux and Windows). For example, for the Windows server with the Fileserver role, vulnerabilities associated with the OpenSSH service used to provide the SFTP service were identified (see Figure 19). These vulnerabilities can allow an attacker to exploit weaknesses in the OpenSSH service to gain unauthorized access or disrupt the service. It is crucial to keep the OpenSSH service updated and apply recommended security configurations to mitigate these risks.

Similarly, the analysis conducted with Nessus for the same server reported six vulnerabilities related to the SSH service, associated with TLS protocol versions, as well as weak ciphers and algorithms (see Figure 20). Outdated versions of TLS and weak encryption algorithms can be exploited by attackers to intercept and decrypt sensitive communications. To mitigate these risks, it is recommended to upgrade to more secure versions of TLS and disable weak ciphers and algorithms. Additionally, it is important to follow security best practices for SSH configuration, such as using key-based authentication and restricting access to authorized users.

Preventing the occurrence of this type of vulnerability involves keeping the SSH service version updated to the latest release. Software updates typically include security patches that address known vulnerabilities, significantly reducing the risk of exploitation. Additionally, it is crucial to enable only the most robust encryption ciphers and communication algorithms, such as AES and SHA-256, while disabling weaker ones like DES and MD5. Robust ciphers and algorithms provide greater resistance against brute force and cryptanalysis attacks, ensuring secure communication.

Disabling weak ciphers and algorithms is essential to avoid security breaches that attackers could exploit. Weak algorithms may be vulnerable to various attack techniques, such as side-channel attacks and collision attacks, which can compromise the integrity and confidentiality of data. By eliminating these weak points, the security of the SSH service is strengthened, reducing the attack surface and making it more difficult for attackers to carry out an attack.



10.0.0.7 / fileserver.internal.cloudapp.net

Address

- 10.0.0.7 (ipv4)
- 12:34:56:78:9A:BC (mac)

Hostnames

- fileserver.internal.cloudapp.net (PTR)

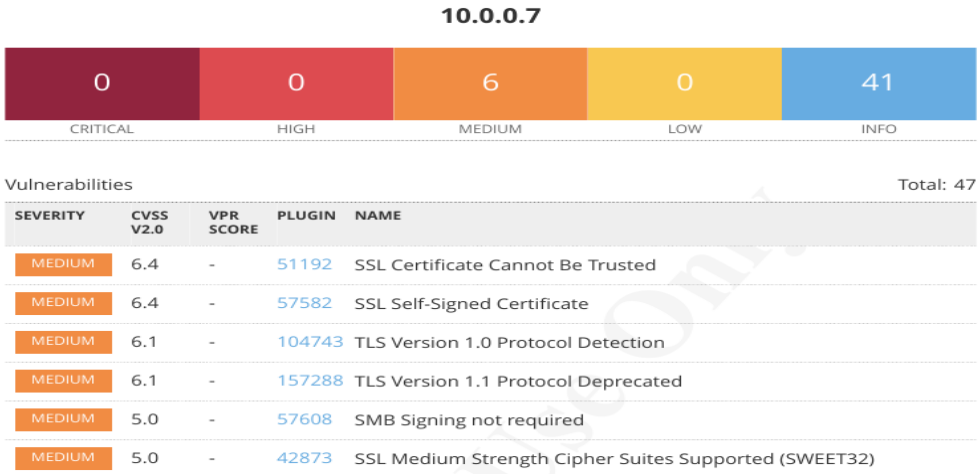
Ports

The 994 ports scanned but not shown below are in state: **filtered**

- 994 ports replied with: **no-response**

Port		State (toggle closed [0] | filtered [0])
22	tcp	open
	vulscan	VulDB - https://vuldb.com: No findings MITRE CVE - https://cve.mitre.org: [CVE-2010-5107] The default configuration of OpenSSH through 6 [CVE-2010-4478] OpenSSH 5.6 and earlier, when J-PAKE is enable [CVE-2009-2904] A certain Red Hat modification to the ChrootDi [CVE-2008-4109] A certain Debian patch for OpenSSH before 4.3p [CVE-2008-3844] Certain Red Hat Enterprise Linux (RHEL) 4 and [CVE-2008-3259] OpenSSH before 5.1 sets the SO_REUSEADDR socke [CVE-2008-1657] OpenSSH 4.4 up to versions before 4.9 allows r [CVE-2008-1483] OpenSSH 4.3p2, and probably other versions, al

Figure 19. Vulnerabilities detected in the OpenSSH service on Windows Source: Own elaboration



10.0.0.7

0	0	6	0	41
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 47

SEVERITY	CVSS V2.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.4	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	-	57582	SSL Self-Signed Certificate
MEDIUM	6.1	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.1	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.0	-	57608	SMB Signing not required
MEDIUM	5.0	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)

Figure 20. Vulnerabilities associated with the OpenSSH service identified in Nessus Source: Own elaboration

According to the results obtained, it is evident that conducting a cybersecurity analysis on a network infrastructure deployed on Microsoft Azure significantly contributes to cybersecurity research by offering a detailed approach to identifying vulnerabilities through ethical hacking techniques and specialized tools. By using free software, it democratizes access to advanced security evaluation methods, allowing researchers and organizations with limited resources to perform effective analyses. This practical and replicable approach not only provides a clear method for evaluating the security of cloud networks but also establishes a solid foundation for future research in identifying and mitigating vulnerabilities in cloud environments.

Additionally, the article provides practical recommendations to improve security posture and mitigate risks, applicable not only to Azure but also to other cloud platforms. By addressing firewall configurations, virtual network setups, and identity management, it offers a comprehensive view of cloud security. This underscores the importance of a holistic security strategy that addresses multiple attack vectors, significantly contributing to research in security methodologies.

Finally, the emphasis on encryption to protect data both at rest and in transit, along with the importance of regular security assessments and updates, highlights the need for a proactive approach to security management. These elements are essential for research in encryption techniques and continuous evaluation methodologies. Overall, the article not only provides a detailed analysis of security in Azure but also offers practical tools and recommendations to enhance security in cloud infrastructures.

5. Conclusions

In conclusion, the cybersecurity analysis conducted on a network infrastructure deployed on Microsoft Azure proves to be a valuable tool for cybersecurity research. By utilizing ethical hacking techniques and specialized tools, vulnerabilities are identified in a detailed and precise manner. This approach not only provides a clear and replicable method for evaluating the security of cloud networks but also establishes a solid foundation for future research in identifying and mitigating vulnerabilities in cloud environments.

Furthermore, the practical recommendations offered in the article to improve security posture and mitigate risks are applicable not only to Azure but also to other cloud platforms. By addressing firewall configurations, virtual network setups, and identity management, it offers a comprehensive view of cloud security. This underscores the importance of a holistic security strategy that addresses multiple attack vectors, significantly contributing to research in security methodologies.

Finally, the emphasis on encryption to protect data both at rest and in transit, along with the importance of regular security assessments and updates, highlights the need for a proactive approach to security management. These elements are essential for research in encryption techniques and continuous evaluation methodologies. Overall, the article not only provides a detailed analysis of security in Azure but also offers practical tools and recommendations to enhance security in cloud infrastructures, benefiting administrators and professionals in the field of cybersecurity.

6. References

[1]. Acevedo, N. Q. (2022). Seguridad y privacidad en la Nube, fortalezas y vulnerabilidades: Recomendaciones para tener en cuenta con los proveedores de servicios de la nube. *Universidad de Los Andes*.

[2]. Beatriz P. de Gallo1, H. B.-G. (2022). Auditoría de vulnerabilidades de seguridad de una arquitectura de procesamiento analítico basada en Azure. *SEDICI Univercida nacional de la Plata*.

[3]. Bonfante, L. E. (2019). Recomendaciones De Seguridad Para Los Servicios De Computación En La Nube, A Partir De Los Estándares Y Modelos De Seguridad De La Información.

[4]. Carlos Manual Fernandez, M. R. (2015). Privacidad elevada en la nube.

[5]. Carrasco, U. D. (2014). Los Problemas Estructurales En El Planteamiento De La Ciberseguridad. *Dialnet*.

[6]. Cuestas, J. A. (2019). Meta-Analisis De Vulnerabilidades Y Gestión Del Riesgo En Arquitecturas Cloud. *Universidad Católica De Colombia*.

[7]. CVE. (2023). *CVE*. Recuperado el 08 de 06 de 2023, de https://cve.mitre.org/cgi-bin/cvename.cgi.

[8]. Diego Jara, P. C. (2017). Propuesta metodológica de evaluación de seguridad para aplicaciones deMobile Cloud Computing. Obtenido de https://publicaciones.ucuenca.edu.ec/ojs/index.php/maskana/article/view/1974/1411.

[9]. Evelin Pilar Díaz Rodríguez, J. A. (2022). Propuesta Arquitectura De Seguridad Para Organizaciones Que Utilicen Los Principales Modelos De Servicios De Informática En La Nube.

[10]. Fuentes, N. L. (2014). COMPUTACIÓN EN LA NUBE. *Mundo Fesc*, 46 -51.

[11]. Guevara Jimenez, D. M. (2022). Diseño de una plataforma cloud basado en IAAS para un empresa de seguros.
[12]. Mario Casasola Robles (cloudMIDDLEtrust), M. S. (2014). *La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo.* Toluca, Mexico: CIDE.
[13]. Microfost. (02 de 03 de 2023). *¿Cómo funciona Azure?* Obtenido de https://learn.microsoft.com: https://learn.microsoft.com/es-es/azure/cloud-adoption-framework/get-started/what-is-azure.
[14]. Muñoz-Calderón, P. F.-M. (2020). Computación en la nube, la infraestructura como servicio frente al modelo On-Premise.
[15]. BRAVO, R. H. (2011). *Cloud Computing and Security: Clearing the Clouds to Protect Personal Data*. DIALNET, pp. 43–58.
[16]. Pavón, A. S. (2022). Metodología a seguir para realizar tests de intrusión sobre entornos AWS. Obtenido de https://upcommons.upc.edu/bitstream/handle/2117/379436/Metodologia_a_seguir_al_realizar_un_test_de_intrusión_sobre_entornos_AWS-Alejandro%20Silva.pdf?sequence=2.
[17]. Pereda, A. G. (2019). Pruebas de penetración y análisis de vulnerabilidades.
[18]. Salazar, V. H. (2016). Seguridad y protección de la Información en la Nube de Cómputo.
[19]. startechup. (2 de marzo de 2023). *PRUEBAS DE PENETRACIÓN EN LA NUBE: ¿QUÉ NECESITA SABER?* Recuperado el 27 de mayo de 2023, de https://www.startechup.com/es/blog/cloud-penetration-testing/#:~:text=Las%20pruebas%20de%20penetración%20en%20la%20nube%2C%20también%20conocidas%20como,que%20puedan%20abusar%20los%20hackers
[20]. tenable. (2023). *NESSUS*. Recuperado el mayo de 2023, de https://es-la.tenable.com/products/nessus.
[21]. Trevejo, L. A. (2022). *Plan de continuidad de negocio de un file server ante un ataque de malware en Cloud.* Universidad Europea. Obtenido de https://titula.universidadeuropea.com/bitstream/handle/20.500.12880/2157/TFM_Talavera%20Luis.pdf?sequence=1&isAllowed=y.

Hector Manuel Herrera, Electronics and Telecommunications Engineer, Master's in Information and Communications Sciences, PhD student in engineering at the Francisco Jose de Caldas District University. Associate professor in the Systems Engineering program at the Los Libertadores University Foundation. A researcher in the field of cybersecurity and data analytics, he has over three years of experience identifying, analyzing, and proposing methodologies, tools, and standards for solving problems faced by organizations' information systems**.**

David Gregorio Rubio Vizacaya, Sistems Ingenieer and information security especialist, whit conolegde in network infraestructure, develoment lenguajes, operative sistems, data bases and cloud infraestructure. I have 14 years working in information tecnologies, in last ten years I have performed administrator platform role and infraestructur leader in a Colombian IT company.

José Carlos Gallego Mina is an experienced systems engineer and information security specialist with a distinguished eight-year track record. His expertise focuses on security software implementation, complemented by extensive knowledge of networks, databases, and cloud infrastructure management. His professional profile aligns with the need to address complex challenges in the field of cybersecurity, providing robust and strategic solutions.

Luis Alexis Plazas Gómez, PhD Candidate at Universidad Cuauhtémoc, Aguascalientes Campus; Master's Degree in Education; Specialization in University Teaching; Specialization in Software Engineering; Systems Engineer; member of the Applied Research Group in Signals and Systems (GUIAS) at Fundación Universitaria Los Libertadores