International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 15, Number 1 (2022), pp. 43-53
© International Research Publication House. http://www.irphouse.com

Sniffing Techniques and Its Application on the Network

Rosa M. Ramírez Rodríguez[1], Jenny A. Niño Rodríguez[2], Miguel A. Leguizamón[3]

[1]*Telematic Engineer, University Francisco José de Caldas, Colombia.*

[2]*Telematic Engineer, University Francisco José de Caldas, Colombia.*

[3]*Assistant Professor, University Francisco José de Caldas, Colombia.*

Abstract

Technology has undoubtedly been the main pillar of development in recent years, has allowed to generate confidential systems and transforming digital tools that ensure the integrity, availability, confidentiality, authenticity, and reliability of information. Digitalization forces companies to know in real time the status and behaviour of their networks, to determine not only possible bottlenecks but also vulnerabilities to data security, so it has monitoring systems that provide solutions, encryption services, data authentication, detection of attacks and intruders, security models.

The procedures and controls are performed and understood from a complete, accurate and updated base to which hackers want to obtain to analyse the security model and plan how to access and get privileged accounts and credentials.

Through this article we will approach some sniffing techniques, network monitoring tools and projects that seek to minimize the insecurity gaps in networks, both hybrid and cloud systems.

Keywords: Cybersecurity, Encryption, Intrusion detection, Man in the middle, sniffing

I. INTRODUCTION

The world of digitization brings with it many advantages when it comes to safeguarding information, but hackers are looking for ways to get ahead in order to gain access to servers and steal or hijack information for some kind of profit. For several decades systems have been created to strengthen security, but to date there is no tool that offers 100% security (recently, in the update of a monitoring tool hackers managed to access servers and install more programs that seek to seize the information) but there are many tools both cloud and hybrid that offer services and hosting of information.

It is important to have tools at hand to ensure data security and more than that, it is important to understand and know the ways in which vulnerabilities can be avoided.

This article is the product of research on sniffing techniques, it details the tools that allow us to ensure the quality of information and how in the midst of digitization new technologies offer intelligent tools.

II. SNIFFING

Before detailing the concept of sniffing, it is necessary to mention the concept of promiscuous mode, the promiscue mode is a mode for a wireless network interface controller

(WNIC) that makes the controller pass all the traffic that receives from the central processing unity (CPU) instead of passing only the wefts that the controller is Destiny to receive. This mode is normally use to track packets that takes place in a router or a computer connected to a concentrator (instead of a switch) or what is parto of a WLAN [1]

The **sniffing of packets** is a method of traffic collectiong on the network with the final purpose of review the traffic for its potential use. This method requires a device, a computer or a hardware packet sniffer. Besides how easy it is to get tools, software functionality that can capture all inbound and outbound traffic encourages attackers to use the technique to their advantage.

Due to the inactivity of the tools, they can simply collect information without modifying the network. [2]

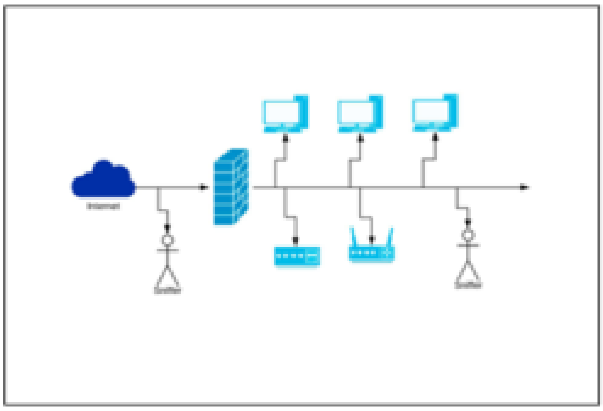


Fig 1. Sniffing process

The Packet tracing can be useful to increase network security. By monitoring traffic for clear text usernames and passwords, for example, you can detect potential security problems before any hacker.

Also, the remote traffic monitoring can help to ensure that all traffic is properly encrypted and is not sent to the open internet without encryption [3].

The Trackers can be used in wired networks, in this network the trackers can have access to the packets of each connected machine or limited by a switch. On the other hand, scanners can also be used in wireless networks, but they can only scan one channel at a time.

The active sniffing tecniques also including spoofing attacks, DHCP attacks and DNS poisoning, among others [4]

To understand a little more about packet sniffers, a brief explanation is presented: when we share a file, computers divide messages into packets. These packets are transmitted through Transmission Control Protocols / Internet Protocol (TCP / IP). Each packet is moved through the network application to the TCP layer and assigned a port number. Then the port migrates to the IP layer and receives the destination IP address. By having the exit and destination identifier, it travels through the internet in the hardware layer, the data is transported in network signals and when it reaches its destination the routing data is eliminated (port number, Ip address) and finally they acquire their digital format.

III. THERE ARE TWO TYPES OF ATTACKS:

Active: Active sniffing consists of injecting Address Resolution Protocols (ARP) into a network to flood the switch's Content Address Memory table (CAM). This, in turn, will redirect legitimate traffic to other ports, allowing the attacker to snoop on switch traffic [4]. There is a constant activity by the attacker for inject traffic into the Lan layer. As a result, they can get information and snoop on switching network traffic.

Passive: Passive sniffing involves only listening and is usually implemented in networks connected by hubs. In this type of network, the traffic is visible to all hosts. (4) An example of this is the voice over IP (VoIP)

IV. PACKET SNIFFER

A packet sniffer is a function that sniffs without altering the network packets in any way, it consists of two parts: a network adapter and software that is used in the network to observe or troubleshoot network traffic. [5] A sniffer is not a virus; therefore, it manages to reproduce itself, is controlled by a third party and is installed with or without consent.

During the scan, sniffers find packets that should not be part of the data or that are also retaining them in the data for reasons of intrusion, viruses, improper behaviour or any violation of policies. [6]

There are two ways to configure sniffers, we will begin by describing no filter, which means that all possible packets are captured and written to a local hard disk for later examination. The second is filter mode, which means that the parsers will only capture specific data items [7].

Fig 2. Sniffing by cookies

Sniffer packet types:

Hardware packet sniffers: A hardware packet sniffer is designed to be connected to and examine a network. This is useful when trying to view traffic for a specific network segment. By connecting directly to the physical network at the appropriate location, a hardware packet sniffer can ensure that no packets are lost due to filtering, routing, or other deliberate or inadvertent causes. A hardware packet tracker stores the collected packets or forwards them to a collector that records the data collected by the hardware packet tracker for later analysis [3].

Software packet sniffer: Although any network interface connected to a network can receive all passing network traffic, most are configured not to. A software packet sniffer changes this setting so that the network interface passes all network traffic to the stack. Once the configuration is ready, the functionality of a packet sniffer becomes a matter of separating, reassembling and registering all the software packages that pass through the interface, regardless of their destination addresses. Software packet sniffers pick up all traffic that flows through the physical network interface. That traffic is logged and used in accordance with the software's packet tracking requirements [3].

V. SNIFFING ATTACKS

To launch different attacks on the network, sniffing is executed in two ways, by using software programs or manually, some of them are detailed below.

ARP attacks: The address resolution protocol works on the Lan to convert the given IP address into the corresponding MAC address. Knowing the Mac address, the response is cached for future use, the attacker takes advantage of this situation to pose as the owner of the IP address and sends false ARP responses. Attackers can even act as a router directing traffic to the legitimate user by configuring their machine, performing Dos and MITM attacks [8].

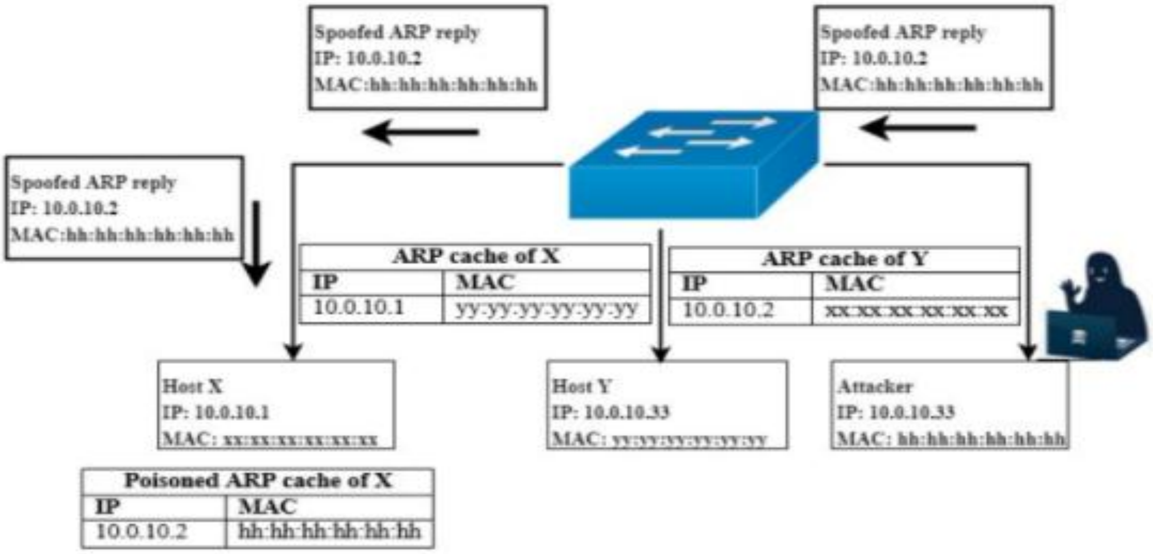


Fig 3. ARP attck

User Agent Fingerprinting: http packages provide system and application information thanks to the user agent that functions as a client on a network protocol. Thanks to the user agent, protocol violations can be detected and their recognition automated, device identification and device applications can be identified. The user agent is part of the http protocol, and the information it transmits can be captured when it is a flat file. When there are encryption protocols such as TLS / SSL, communication is secure [9].

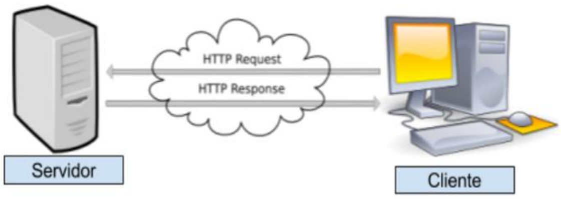


Fig 4. There is no https protocols.

Mac Attacks: Considering that the switch has limited memory, the attacker tends to flood the network device with numerous requests from different source Mac addresses in order to install itself and capture the sensitive information [8]

MITM: The attacker installs hardware posing as a trusted wireless network in order to trick unsuspecting victims into connecting to it and submitting their credentials [9n] MitM example: after managing to get in the middle of a communication the attacker creates similar domains (adds a letter at the end of both the sender domain and the recipient domain) to the original ones, maintains the same email subject and manages to spoof identities (Post5), being in the middle has the ability to read and changing the content before it reaches the recipient and finally gaining inside information. Based on this, the importance of taking security measures, auditing access records and using tools that identify fake domains is highlighted. [10]

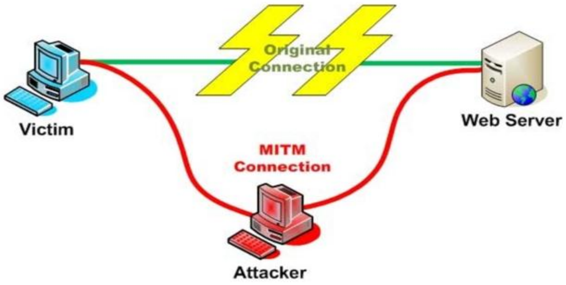


Fig 5. MITM attack man in the middle

DNS attacks: Impersonation of the domain name system. The attacker alters the DNS table, thus DNS directs its clients to a false IP address or redirects users to illicit websites (Post4). Mitigation with Secure DNS (DNSSEC), DNSCurve Security Proxy, Naïve Bayesian Algorithm, and K-nearest Neighboring [8]

DHCP Attacks: Flood DHCP requests through rogue server. To mitigate this attack, you should consider digital signatures and public key cryptography and know that the ports have a security function that restricts the unwanted entry of ports by limiting Mac addresses. Likewise, Cisco recommends the

DCHP Snooping table. which uses a database to filter unauthorized messages. (8) The ICMP protocol is very useful when diagnosing a network problem, if this protocol is disabled, DHCP will not be able to identify malicious requests. (Post6)

XSS attacks: In recent years, in order to navigate, many websites have a GDPR regulation, therefore, pop-up windows appear in which you request consent to use the data. but also a vulnerability was detected in which cross site scripting attacks were accepted. Hackers basically inject malicious code into your site and virtually hijack it. In this way, attackers use your blog, store or company website as a vehicle for their illegal activities. In general, these vulnerabilities are solved with patches and new updates [11].

Content Sniffing Attacks: They are malicious HTML content files or Javascript code which are embedded as Html but are not html. These attacks can be prevented from the server side if the file upload is prevented, however, the existing approaches to detecting sniffing attacks have several limitations, on the one hand, only a certain number of bytes are parsed and on the other hand the mechanisms used do not provide information on the impact of the malicious code. (Post3)

VI. SNIFFING TOOLS

It is important when purchasing a packet tracker to consider a tool capable of decoding administrative information, which shows valuable data such as port numbers, variables between which the packets travel and based on this generate a more robust analysis of the traffic. network. Today there are countless sniffers, they vary in their breadth and depth, the ability to analyze deep packet inspection.

Although the monitoring tools were designed to help network administrators detect network problems, certain bottlenecks, and view traffic, hackers also use them to scan a specific network and snoop on data. (Post 7)

There are many tools that collect network traffic activity. On Unix-like systems they use PCAP and for Windows systems they use libcap [12].

Next, we will explain the main tools used for network monitoring and intrusion detection.

Viewtify QoS: Before talking about this tool, it is necessary to cover two important concepts such as Log data wire Data and log data.

Wire data: it is cable data, it is data from the data that is extracted from IP traffic. In general terms, it refers to the operation of the network, to the transactions between applications, devices, client and infrastructure component. For example, in teleworking issues it allows to know the time that an employee was connected, the calls he made, the time of availability and occupation. A piece of information that every company or organization is interested in having on its side in terms of productivity and quality.

Log data: they are the records of the user's activities in the operating system or footprint that the connected elements have left and that are recorded in a file. This tool allows the integration of any log in any format thanks to Smart data broker. If a log analysis is required and there is no standardization of the log record format, this process may be a bit delayed.

Viewtify Qos is a solution that allows you to monitor and control the traffic of business networks, which has advanced analytics, TCP protocol optimization and “traffic shaping”. It provides real-time information about the network environment. Broadly speaking, its architecture has three layers [13]:

- Viewtisight: provides answers to questions that arise from the operational part or areas of the company. Together with the analytics component, it allows to provide other anomaly detection, correlation and forecasting functionalities.
- Viewtilog; allows the integration of data from any source and manufacturer into Viewtisight, in any format (SNMP, Netflow, Syslog, WMI, API, CDRs, etc.), automatically, simplifying the operations of organizations, both in the IT, OT and IoT.
- Viewtimon is a probe capable of collecting all wire data, providing visibility of applications, network KPIs and quality of experience measures. And it is that, with the sniffer configuration, packet captures can be made uninterruptedly with a high retention rate

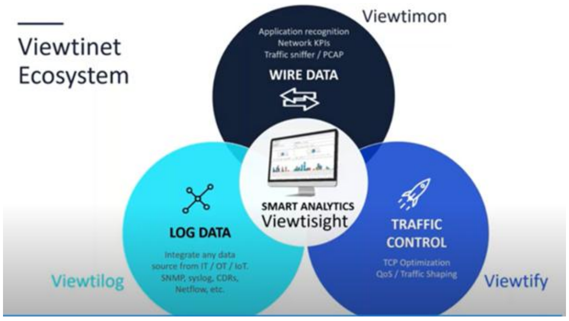
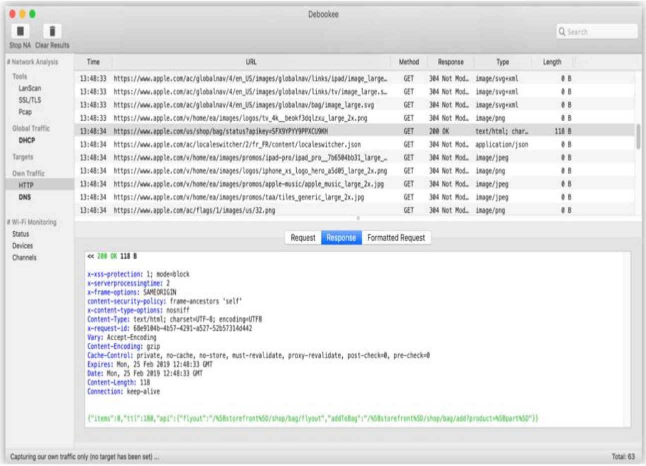


Fig 6. Viewtinet arquitecture

Wireshark: is a network protocol analyzer that is used to analyze data packets on a network. The analysis can be done in many aspects such as time, origin and destination, protocol, etc. Wireshark has many features like filtering, searching based on given criteria, and dumping data in many formats for analysis. The data is analyzed to identify the IP addresses of all hosts on the network and to identify the protocols used for data transfer between nodes. [14]

Based on this definition, it is possible to show that the tool provides us with the facility to take confidential information with a malicious purpose by providing attacks, by obtaining vulnerable data (IP addresses, Hostnames or host names, routers and transmission routes, data where most transmitted on the network circulate in plain text, including FTP, Telnet, email, among others)

DEBOOKEE: is a payment tool to analyze and monitor the network. This tool is capable of intercepting the traffic of multiple devices. The methods used by this tool are completely independent of the devices used. This means that the traffic of phones, laptops and even tablets can be monitored using the tool. The SSL / TLS decryption strategy used by Debookee is known to support secure layer communication. This tool allows you to see not only the traffic of the pc, but also to see the raw data of the mobiles or IOT things with the network Analysis module [15].



Time	URL	Method	Response	Type	Length
13:48:33	https://www.apple.com/ac/globalnav/4/en_US/images/globalnav/links/ipad/image_large…	GET	304 Not Mod…	image/svg+xml	0 B
13:48:33	https://www.apple.com/ac/globalnav/4/en_US/images/globalnav/links/tv/image_large.s…	GET	304 Not Mod…	image/svg+xml	0 B
13:48:33	https://www.apple.com/ac/globalnav/4/en_US/images/globalnav/bag/image_large.svg	GET	304 Not Mod…	image/svg+xml	0 B
13:48:33	https://www.apple.com/v/home/ea/images/logos/tv_4k__beokf3dqlzxu_large_2x.png	GET	304 Not Mod…	image/png	0 B
13:48:34	https://www.apple.com/us/shop/bag/status?apikey=SFX9YPYY9PPXCU9KH	GET	200 OK	text/html; char…	118 B
13:48:34	https://www.apple.com/ac/localeswitcher/2/fr_FR/content/localeswitcher.json	GET	304 Not Mod…	application/json	0 B
13:48:34	https://www.apple.com/v/home/ea/images/promos/ipad-pro/ipad_pro__7b6504bb31_large_…	GET	304 Not Mod…	image/jpeg	0 B
13:48:34	https://www.apple.com/v/home/ea/images/logos/iphone_xs_logo_hero_a5d05_large_2x.png	GET	304 Not Mod…	image/png	0 B
13:48:34	https://www.apple.com/v/home/ea/images/promos/apple-music/apple_music_large_2x.jpg	GET	304 Not Mod…	image/jpeg	0 B
13:48:34	https://www.apple.com/v/home/ea/images/promos/taa/tiles_generic_large_2x.jpg	GET	304 Not Mod…	image/jpeg	0 B
13:48:34	https://www.apple.com/ac/flags/1/images/us/32.png	GET	304 Not Mod…	image/png	0 B

```
<< 200 OK 118 B

x-xss-protection: 1; mode=block
x-serverprocessingtime: 2
x-frame-options: SAMEORIGIN
content-security-policy: frame-ancestors 'self'
x-content-type-options: nosniff
Content-Type: text/html; charset=UTF-8; encoding=UTF8
x-request-id: 68e9104b-4b57-4291-a527-52b57314d442
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: private, no-cache, no-store, must-revalidate, proxy-revalidate, post-check=0, pre-check=0
Expires: Mon, 25 Feb 2019 12:48:33 GMT
Date: Mon, 25 Feb 2019 12:48:33 GMT
Content-Length: 118
Connection: keep-alive


{"items":0,"ttl":180,"api":{"flyout":"/%5Bstorefront%5D/shop/bag/flyout","addToBag":"/%5Bstorefront%5D/shop/bag/add?product=%5Bpart%5D"}}
```

Capturing our own traffic only (no target has been set) …

Total: 63

Fig 7. Environment Debooke’s tool

TCPDUMP: it is a network tracker which requires less system resources, fixes different errors, tracks network problems and monitors activities. There is a separate Windows port called WinDump, tcpdump is the source for the libpcan / winPcap packet capture library, which is used by Nmap and other tools. It doesn't require a heavy desktop to run, making it a favorite tool for sysadmins. Tcpdump captures all traffic through a library called libcap and then dumps it directly to your screen. The data is exported to a third party tool for analysis, tcpdump cannot read the pcap files it captures [12]. Tcpdump has the ability to capture packets directly from the wire, examine individual packets or script, its outputs can be manipulated by scripts. One of the disadvantages is that it has no concept of state and does not provide any ability to interpret application layer protocols [16].

SolarWinds Network Performance Monitor: Scalability and ease of use provides a complete view of your network, so you can quickly detect, diagnose, and resolve network performance problems and avoid downtime. Additionally, the system uses minimal bandwidth, requiring low overhead on the Orion platform nodes and servers.

With the probes installed, SolarWinds can view and collect metadata from all network traffic, logging and displaying response times, data volumes, and transactions to locate slowdowns and flag any problems. Facing some user experiences create a packet roadmap in order to find the location of bottlenecks.

This administration tool suffered an attack last December 2020, cybercriminals managed to break into SolarWinds internal network and altered various versions of its Orion solution to add Sunburst malware. That malware was found in every update released between March and June 2020, and more seriously, no SolarWinds customer was aware (or at least did not report) it until nine months had passed. In fact, it wasn't until December 15 that SolarWinds released a new version of Orion that could stand up to the attack. The problem is that not only was Sunburst [16]. This malware is not complex or particularly aggressive, but it was in charge of collecting the information that allowed attackers to select the target customers they considered most interesting: US government agencies and companies such as Microsoft or FireEye. [17]

Promqry3 : Is a Microsoft antisniffing tool that can be used to detect network interfaces running in promiscuous mode. Promqry can determine if a Windows-based device has promiscuous mode network interfaces, which may be a sign that a network sniffer is running on the system. This tool works by enumerating the interfaces in promiscuous mode on the local machine requesting information about the state of the interface through WinAPI. To scan external machines, a range of IP addresses can be specified, then these addresses are checked using a ping query, and if the host is running / connected, the tool tries to connect to the host with a Remote Procedure Call (RPC) and checks the state of the interface to find out if promiscuous mode is used. [18]

PcapWT, an efficient packet extraction tool for large traces. PcapWT provides a quick search for packages by indexing an original trace using a wavelet tree structure. Additionally, pcapWT supports multithreading to avoid synchronous I / O and locking system calls used for file processing and is particularly efficient on SSD machines. PcapWT shows notable performance improvements compared to traditional tools like tcpdump and newer tools like pcapIndex in terms of index data size and packet extraction time. [19]

Sonarwan: it is a system that has a PyShark library, open source that has two programs: wrapper and Tshark. Wrapper provides a compatible interface to use another program: tshark, which is basically a wireshark without a graphical interface. Pyshark supports live capture at time x.

Sonarwan receives traffic capture files in a “pcap” format that come from devices that are on the network. If there are several files, it takes them as a single capture and in the output describes scenarios and behaviours that the network had. It has three main components: environment (stage), handlers (manipulators) and tools (tools). Sonarwan can associate the package not only with the device, but also with an application and even a service that was consumed [9].

VII. AT THE CLOUD LEVEL WE MENTION THE FOLLOWING TOOLS:

Amazon CloudWatch: Collects monitoring and operations data in the form of logs, metrics, and events, providing an overview of the status of operations, and allows data from all applications and services running on the server to be correlated on one platform. Users can define alarms and automate actions based on defined thresholds and learning algorithms. The service is provided in the cloud or also in hybrid cloud architectures (in order to monitor local resources), it integrates Amazon AWS services (21). This tool can automatically learn and distinguish the web-based applications it hosts, and detect latency anomalies for each application based on its own state, this in light and real time.

NetApp Cloud Insights: With this tool the user can monitor, optimize and protect the resources both those that are in public clouds and those that are in private centers. In addition to this, it detects problems and limits downtime, manages resources and detects Ransomware with actionable intelligence. Provides seamless navigation of Kubernetes clusters to identify performance issues and resource constraints in either the cluster or backup infrastructure. This tool also has the ability to learn automatically [22].

Orizon Boost & Optimize Applications: Optimize and manage the performance of technology infrastructures by identifying and correcting problems. Through the analysis and monitoring of the operation of hardware and software, it provides a global vision of all systems and infrastructure. It operates in 5 phases, the first is data capture, secondly, it produces a census of the processes and detections according to a period of time. The analysis and detection of improvement opportunities is the third Phase. In the fourth phase is the follow-up and finally verifies the alignment of all the proposed objectives. It has improvements to its graphical interface and will include artificial intelligence and maching learning algorithms [23].

Dynatrace Cloud infrastructure monitoring: Add artificial intelligence to the monitoring of technology infrastructures in the cloud to ensure easy implementation and have practical information. Provides complete visibility into the infrastructure layer in public, private, and hybrid cloud environments. In the future, it will generate a Davis artificial intelligence engine that includes improved algorithms and the ability to integrate information from other solutions such as IBM or Citrix. It also monitors containers at Web scale with a Cloud Infrastructure Monitoring solution [24].

HPE OneSphere: Hybrid cloud management platform based on a software-as-a-service (SaaS) solution. Thanks to this, both developers and IT staff can create hybrid clouds capable of supporting traditional and native cloud applications. It enables organizations to integrate Amazon Web Services and Microsoft Azure public clouds and virtual data centers. Supports provisioning of enterprise-grade Kubernets clusters within AWS.

It provides a catalog of application services that integrates different public and private cloud services. Allows you to import legacy operating system images, as well as cloud-hosted application images. It also enables detailed analytics to track, categorize, and report on cloud costs across multiple clouds.

HPE has a solution called Consumtion Analtycs, which is an interactive online portal that helps monitor, manage and optimize IT services based on consumption, facilities and cloud computing [25].

Microsoft Azure Monitor: Provides advanced analytics and machine learning to monitor application performance and proactively identify issues to respond to alerts. It has a solution that collects, examines and manages telemetric data. It suggests a centralized space to identify network errors, spikes in CPU usage, memory leaks in code, and other issues before they affect the business.

The data is classified according to two criteria, metrics (numerical values that describe some aspect of a system at a given moment, support real-time scenarios) and records (contain different types of data organized in groups with different types of properties).

With Intelligent Insights powered by artificial intelligence, you can analyze, correlate, and monitor data from different sources [26].

Oracle Management Cloud: The protection, monitoring and administration of applications is provided by a set of services, these are characterized by machine learning and big data techniques for the operational data set.

It has 7 modules [27]:

- Log Analytics: Write log queries and analyze information about machine data in real time.
- Application Performance Monitoring: Enables IT and development teams to troubleshoot application-related problems based on information.
- Infrastructure Monitoring: Through a single platform the status of an entire infrastructure is examined.
- IT Analytics: shows a total vision of the performance, availability and capacity of applications and investments in the structures.
- Orchestration: Implemented for the automation of

executed tasks and hyperloading by calling third-party REST endpoints, scripts or automation frameworks.

- Security Monitoring and Compliance: integrates capabilities based on SIEM and UEBA machine learning.
- Configuration and Compliance: By means of industry standard benchmarks and thanks to maching Learning applied to application metrics, operating systems and logs, it solves violations.

VIII. PREVENTION MEASURES:

• Attacks are increasingly sophisticated, unknown in nature, and the only way to detect them is to use different layers of cyber defense. Layered defense requires coordination and the use of Artificial Intelligence to aid in real-time detection and response, and to isolate compromised parts of our infrastructure. [28]

• Companies must be faster detecting and responding to threats, and this can be achieved using advanced cloud-native incident management tools (SIEM) and automated response solutions (SOAR), assisted by intelligence technology. artificial and machine learning. [29]

• Have or hire a Security Operations Center (SOC) It is also important to configure a SOC internally for future security incidents or partner with a managed service provider that has a SOC that can help monitor and manage security 24 hours a day. day to reduce the risk of a leak. A SOC tracks user behavior and looks for unusual activity using artificial intelligence and machine learning; manage vulnerabilities; and verifies and validates that security solutions are working properly, are up-to-date and generate security alarms. [29]

• Involve artificial intelligence in security systems to anticipate an attack and optimize time in front of the threat [30].

• Browse only websites that are encrypted with the "HTTPS-" [5]

• Network administrators should scan and observe their network bandwidth monitoring or device auditing at regular intervals to detect any questionable traffic or activity [9].

• Vulnerability management plan and quickly apply patches released by IT vendors to avoid incidents. [1j]

• You must have Backup solutions, no cybersecurity strategy will work without a business continuity and disaster recovery plan because, in the face of a serious security incident, it will allow the company to recover activity. [29]

• It is not only necessary to protect the infrastructures and the network. You also have to protect all devices by investing in EDR, threat detection and response solutions at the endpoint level. [25]

• Use of encryption tools, adding the MAC address of the gateway permanently to the ARP cache, changing to SSH, https instead of http and so on. (two)

• Connections are currently very fast thanks to the implementation of 5g technologies, but it is still vulnerable to network attacks due to the nature of wireless technology. Forensic analysis of the network is necessary to analyze and defend against these attacks. Network forensic analysis refers to a technology that analyzes all actions that are performed on the network and analyzes and responds to attacks by analyzing packets.

WHAT NEW TECHNOLOGIES OFFER FOR THE FUTURE FOR SECURITY?

Cyberattacks and data leaks have skyrocketed since the outbreak of COVID. In the face of advanced cyber threats, it is important to have a consistent structure to detect, monitor, manage and protect the corporate network, capable of minimizing the time to detect an intrusion. (intrusion detection system)

Not only do you have to protect the infrastructure and network, you have to invest in the devices, investing in EDR solutions, threat detection and response at the endpoint level. [29]

SD WAN: Future 5g deployments and IOT growth will make old networks less and less useful as a way to manage everything. Network administrators can fight back as security is increasingly integrated into SD WAN services. SD-WAN is a centralized management of WAN networks, usually closely related to cloud computing and security (post2). SD WAN offers agile technology and responds perfectly (31). An SD WAN tracks the origin of an attack in order to mitigate it (Post1), offers traffic control, prioritization and intelligent routing for key applications and an overall improvement of the end-user experience of IaaS and SaaS applications, firewalls specifics, network translations [NAT], encryption and DDoS protection [32].

Artificial Intelligence: Artificial intelligence today can pinpoint anomalies for a security analyst to investigate, saving resources such as time and costs [33]. This technology is expected to accurately detect and remediate attacks in real time in the future. The AI learns traffic patterns, thus suggesting security policies. Machine learning is used to discover threats and stop them before any attack is carried out.

Artificial intelligence is capable of identifying fraud and anticipating it by analyzing multiple risk indicators and attack patterns. The most recent implementation was by a bank, with the AI a digital profile is created in each transaction, if a cybercriminal has the credentials and wants to carry out an operation, the AI is able to identify the differences, generate an alert and thus block said transaction . This service is offered from the cloud. [9]

Artificial intelligence can be vulnerable to attacks, it is programmed to make models more autonomous, but a hacker can intervene in the programming of this in order to change its purpose. By virtue of the way they learn they can be attacked and controlled by an adversary.

Companies that use artificial intelligence to prevent attacks: Microsoft, chronicle, splunk, SQRRL, Blackberry, Demisto [34]. AI is a feature, not a business. You will play a role in solving a specific problem. But not all problems can be solved with AI.

Quantum Computing: Any security measure can be compromised at any time as long as the right conditions exist, but with quantum computing it will be possible to create more secure systems. In general, for some classical encryption systems prime numbers are factored, but with quat (subatomic participles) said in factoring, the algorithms will be much more efficient thanks to quantum mechanics. If a third party intercepted the information during the creation of the secret key, the process itself would be altered, so the system would reveal the intruder. Interlacing is another property that is used to transmit information securely and without a transmission medium. And the encoding is done under safe conditions thanks to the processing power and exponential speed. [35]

Neuro cybersecurity: The human element is an important factor when it comes to an attack since a hacker can control attention, manipulate perception and memory without the victim being aware of this. There have been many scenarios where a person clicks on a malicious link or performs some kind of transfer without question.

The brain develops effective strategies, such as building an illusion of continuity or anticipating events to face dangers or threats, there are some mental algorithms that work to be able to act and protect itself. The brain of each possible victim is in charge of constructing reality with incomplete data, and thanks to the context and its own catalog of experiences, it completes images, develops emotions, makes decisions in the event of a cyberattack and even categorizes people.

Neurocybersecurity provides a different approach to trying to solve one of the great problems in the digital age, cyberattacks. [36]

Pktmon: Microsoft has quietly added a built-in network packet sniffer to the Windows 10 October 2018 Update, and it has gone unnoticed since its release.

This packet tracker is a program that monitors network activity flowing through a computer at the individual packet level.

This can be used by network administrators to diagnose network problems, see what types of programs are being used on a network, or even listen to network conversations sent via clear text.

While Linux users always had the tcpdump tool to perform network tracing, Windows users have had to install third-party programs such as Microsoft Network Monitor and Wireshark.

This all changed when Microsoft released the October 2018 Update, as Windows 10 now comes with a new "Packet Monitor" program called pktmon.exe.

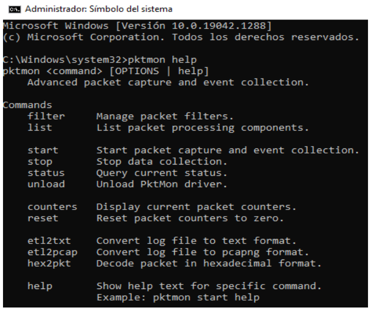
This program has a description of "Monitor internal packet propagation and packet drop reports", which indicates that it is designed to diagnose network problems.

Similar to the Windows 'netsh trace' command, it can be used to perform a full inspection of data packets being sent through the computer. [37]

Any machine that communicates over the network has at least one network adapter. All the components between this adapter and an application form a network stack - a collection of network components that process and move network traffic. In traditional scenarios, the network stack is small and all packet routing and switching occurs on external devices. [38]

Having said the above, a machine with a network adapter is taken to exemplify the use of this command a bit:

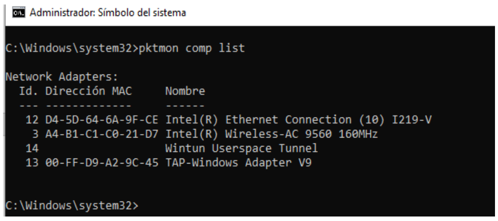
1. The command prompt must be run with administrator privileges.
2. Execute the pktmon help command to display the list of options offered by this Pktmon.



```
Microsoft Windows [Versión 10.0.19042.1288]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>pktmon help
pktmon <command> [OPTIONS | help]
    Advanced packet capture and event collection.

Commands
    filter     Manage packet filters.
    list       List packet processing components.

    start      Start packet capture and event collection.
    stop       Stop data collection.
    status     Query current status.
    unload     Unload PktMon driver.

    counters   Display current packet counters.
    reset      Reset packet counters to zero.

    etl2txt    Convert log file to text format.
    etl2pcap   Convert log file to pcapng format.
    hex2pkt    Decode packet in hexadecimal format.

    help       Show help text for specific command.
               Example: pktmon start help
```

Fig 8. Options list PKtMon

3. In this case, we want to list the interfaces available for packet capture, the command pktmon comp list is entered, this command details the id, MAC address and name of the interface available to monitor.

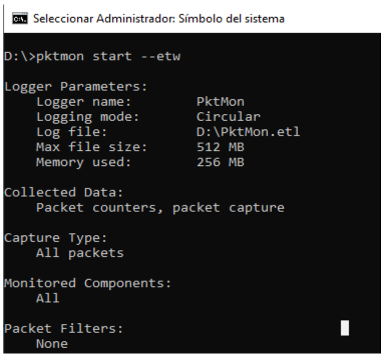


```

C:\Windows\system32>pktmon comp list

Network Adapters:
  Id. Dirección MAC     Nombre
  --- -------------     ------
   12 D4-5D-64-6A-9F-CE Intel(R) Ethernet Connection (10) I219-V
    3 A4-B1-C1-C0-21-D7 Intel(R) Wireless-AC 9560 160MHz
   14                   Wintun Userspace Tunnel
   13 00-FF-D9-A2-9C-45 TAP-Windows Adapter V9


C:\Windows\system32>
```

Fig 9. List of available interfaces

4. To initialize the monitoring of the available interfaces, execute the command pktmon start –etw, in addition

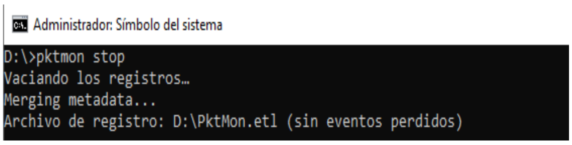
to executing the monitoring, it returns information on the name and size of the created file.



```
D:\>pktmon start --etw

Logger Parameters:
    Logger name:        PktMon
    Logging mode:       Circular
    Log file:           D:\PktMon.etl
    Max file size:      512 MB
    Memory used:        256 MB

Collected Data:
    Packet counters, packet capture

Capture Type:
    All packets

Monitored Components:
    All

Packet Filters:
    None
```

Fig 10: Monitoring initialization information

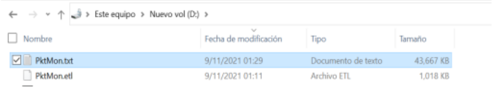
5. When executing the pktmon stop command, the traffic statistics of the interface are obtained, leaving a file on the disk drive where pktmon was started:



```
D:\>pktmon stop
Vaciando los registros…
Merging metadata...
Archivo de registro: D:\PktMon.etl (sin eventos perdidos)
```

Fig 11: Pktmon detention

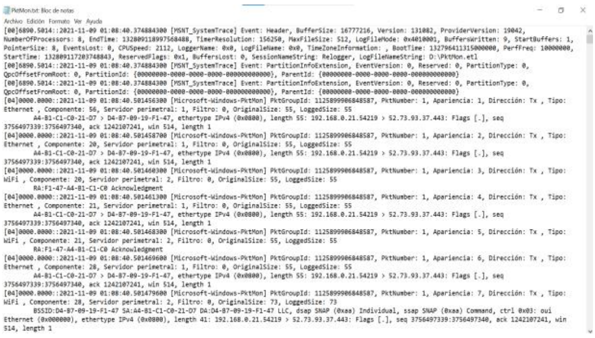
6. To finish the example of the use of pktmon, the interface traffic statistics are read, it is possible to convert the PktMon.etl file to text format and execute it from the console (CMD) with the command pktmon format PktMont. etl -o PktMon.txt, renaming the file "PktMon.txt" whose location is on the same drive where the original PktMon.etl file is initially located.



☐ Nombre	Fecha de modificación	Tipo	Tamaño
☑ PktMon.txt	9/11/2021 01:29	Documento de texto	43,667 KB
PktMon.etl	9/11/2021 01:11	Archivo ETL	1,018 KB

Fig 12: Pktmon files location

Opening the PktMon.txt file displays captured packets and event tracing for Windows :



```
[00]6890.5014::2021-11-09 01:08:40.374884300 [MSNT_SystemTrace] Event: Header, BufferSize: 16777216, Version: 131082, ProviderVersion: 19042,
NumberOfProcessors: 8, EndTime: 132809118997568488, TimerResolution: 156250, MaxFileSize: 512, LogFileMode: 0x4010001, BuffersWritten: 9, StartBuffers: 1,
PointerSize: 8, EventsLost: 0, CPUSpeed: 2112, LoggerName: 0x0, LogFileName: 0x0, TimeZoneInformation: , BootTime: 132796411315000000, PerfFreq: 10000000,
StartTime: 132809117203748843, ReservedFlags: 0x1, BuffersLost: 0, SessionNameString: Relogger, LogFileNameString: D:\PktMon.etl
[00]6890.5014::2021-11-09 01:08:40.374884300 [MSNT_SystemTrace] Event: PartitionInfoExtension, EventVersion: 0, Reserved: 0, PartitionType: 0,
QpcOffsetFromRoot: 0, PartitionId: {00000000-0000-0000-0000-000000000000}, ParentId: {00000000-0000-0000-0000-000000000000}
[00]6890.5014::2021-11-09 01:08:40.374884300 [MSNT_SystemTrace] Event: PartitionInfoExtension, EventVersion: 0, Reserved: 0, PartitionType: 0,
QpcOffsetFromRoot: 0, PartitionId: {00000000-0000-0000-0000-000000000000}, ParentId: {00000000-0000-0000-0000-000000000000}
[04]0000.0000::2021-11-09 01:08:40.501456300 [Microsoft-Windows-PktMon] PktGroupId: 1125899906848587, PktNumber: 1, Apariencia: 1, Dirección: Tx , Tipo:
Ethernet , Componente: 56, Servidor perimetral: 1, Filtro: 0, OriginalSize: 55, LoggedSize: 55
        A4-B1-C1-C0-21-D7 > D4-B7-09-19-F1-47, ethertype IPv4 (0x0800), length 55: 192.168.0.21.54219 > 52.73.93.37.443: Flags [.], seq
3756497339:3756497340, ack 1242107241, win 514, length 1
[04]0000.0000::2021-11-09 01:08:40.501458700 [Microsoft-Windows-PktMon] PktGroupId: 1125899906848587, PktNumber: 1, Apariencia: 2, Dirección: Tx , Tipo:
Ethernet , Componente: 20, Servidor perimetral: 1, Filtro: 0, OriginalSize: 55, LoggedSize: 55
        A4-B1-C1-C0-21-D7 > D4-B7-09-19-F1-47, ethertype IPv4 (0x0800), length 55: 192.168.0.21.54219 > 52.73.93.37.443: Flags [.], seq
3756497339:3756497340, ack 1242107241, win 514, length 1
[04]0000.0000::2021-11-09 01:08:40.501460300 [Microsoft-Windows-PktMon] PktGroupId: 1125899906848587, PktNumber: 1, Apariencia: 3, Dirección: Tx , Tipo:
WiFi , Componente: 20, Servidor perimetral: 2, Filtro: 0, OriginalSize: 55, LoggedSize: 55
        RA:F1-47-A4-B1-C1-C0 Acknowledgment
[04]0000.0000::2021-11-09 01:08:40.501461300 [Microsoft-Windows-PktMon] PktGroupId: 1125899906848587, PktNumber: 1, Apariencia: 4, Dirección: Tx , Tipo:
Ethernet , Componente: 21, Servidor perimetral: 1, Filtro: 0, OriginalSize: 55, LoggedSize: 55
        A4-B1-C1-C0-21-D7 > D4-B7-09-19-F1-47, ethertype IPv4 (0x0800), length 55: 192.168.0.21.54219 > 52.73.93.37.443: Flags [.], seq
3756497339:3756497340, ack 1242107241, win 514, length 1
[04]0000.0000::2021-11-09 01:08:40.501468300 [Microsoft-Windows-PktMon] PktGroupId: 1125899906848587, PktNumber: 1, Apariencia: 5, Dirección: Tx , Tipo:
WiFi , Componente: 21, Servidor perimetral: 2, Filtro: 0, OriginalSize: 55, LoggedSize: 55
        RA:F1-47-A4-B1-C1-C0 Acknowledgment
[04]0000.0000::2021-11-09 01:08:40.501469600 [Microsoft-Windows-PktMon] PktGroupId: 1125899906848587, PktNumber: 1, Apariencia: 6, Dirección: Tx , Tipo:
Ethernet , Componente: 28, Servidor perimetral: 1, Filtro: 0, OriginalSize: 55, LoggedSize: 55
        A4-B1-C1-C0-21-D7 > D4-B7-09-19-F1-47, ethertype IPv4 (0x0800), length 55: 192.168.0.21.54219 > 52.73.93.37.443: Flags [.], seq
3756497339:3756497340, ack 1242107241, win 514, length 1
[04]0000.0000::2021-11-09 01:08:40.501479600 [Microsoft-Windows-PktMon] PktGroupId: 1125899906848587, PktNumber: 1, Apariencia: 7, Dirección: Tx , Tipo:
WiFi , Componente: 28, Servidor perimetral: 2, Filtro: 0, OriginalSize: 73, LoggedSize: 73
        BSSID:D4-B7-09-19-F1-47 SA:A4-B1-C1-C0-21-D7 DA:D4-B7-09-19-F1-47 LLC, dsap SNAP (0xaa) Individual, ssap SNAP (0xaa) Command, ctrl 0x03: oui
Ethernet (0x000000), ethertype IPv4 (0x0800), length 41: 192.168.0.21.54219 > 52.73.93.37.443: Flags [.], seq 3756497339:3756497340, ack 1242107241, win
514, length 1
```

Fig 13. Monitoring results

IX. CONCLUSION

From the above it is evident that the fight against sniffers is a permanent issue and that more sophisticated techniques are constantly being developed for their detection, but at the same time models are being created for their violation, which causes a constant struggle between the defender and the attacker.

However, it is essential and important for any security administrator to have sufficient knowledge of all available sniffer detection tools and attack techniques that a thief may use to breach network security and to understand the outcome of using their tools and how far they may go in the face of such an attack.

On the other hand, it is worth highlighting that because of the different attacks that have been generated in the history of networks, companies are already implementing greater security in their systems, with new, more robust technologies looking to protect their information, which leads to an imbalance in the fight between protection and the attack in favor of the network administrator.

At present there are some advanced and simple solutions that can be applied to minimize the impact of a sniffer, mainly the segmentation of the network either physically or through smart hubs that prevent any traffic not destined for them from reaching the network card.

REFERENCES

[1] S.Shirtharth, D. Prince Winston, A Comparative Analysis between Two Countermeasure Techniques to Detect DDoS with Sniffers in a SCADA Network, Science Direct,2015,21,179-186, Available in: https://www.sciencedirect.com/science/article/pii/S221201731500314X

[2] Aayush Pradhan, Rejo Mathew Solutions to Vulnerabilities and Threats in Software Defined Networking (SDN), Science Direct, 2020,171,2581-2589

[3] Packet Sniffing [Web Site]*Paessler 2021 [Access June 12, 2021] Available in: https://www.paessler.com/it-explained/packet-sniffing

[4] Cyware,A quick guide to sniffing attacks [Web Site]* Cyware[Updated October 6, 2021, accessed June 13, 2021.] Available in https://cyware.com/news/a-quick-guide-to-sniffing-attacks-44edd76b/

[5] Ajay Ohri, Sniffing and Spoofing: Important Points to know in 2021[Web Site]* JIGSAW ACADEMY;2020[Updated December 28, 2020, accessed May 29, 2021] Available in: https://www.jigsawacademy.com/blogs/cyber-security/sniffing-and-spoofing/

[6] Pankaj Shinde,Thaksen J. Parvat, DDoS Attack Analyzer: Using JPCAP and WinCap, Science Direct,

2016,79,781-784 Available in: https://www.sciencedirect.com/science/article/pii/S1877050916002349

[7] Kaspersky, What is a Packet Sniffer? [Web Site]* Kasperky,2021[Accessed April 28, 2021], Available in: https://www.kaspersky.com/resource-center/definitions/what-is-a-packet-sniffer

[8] Jeyanthi Nagamalai - Prabadevi. B A Review on Various Sniffing Attacks and its Mitigation Techniques, Vellore India. 2018,12:1117-1125

[9] Bond,Federico Itzcovich,Ivan, Detection of behavior patterns in network traffic [Web Site]* Technological Institute of Buenos Aires.2016[Accessed May 15, 2021] Available in: https://ri.itba.edu.ar/bitstream/handle/123456789/1236/Informe%20PF.pdf?sequence=1&isAllowed=y

[10] Montalbano Elizabeth, ‘Ultimate’ MiTM Attack Steals $1M from Israeli Startup [Web Site]* threatpost,2019 [Updated December 5, 2019, Accessed June 14, 2021] Available in: https://threatpost.com/ultimate-mitm-attack-steals-1m-from-israeli-startup/150840/

[11] Schüring, Tobias Attacks XSS: How to protect yourself, you the customers and you the business [Web Site]* Raidboxes,2020 [Updated January 23, 2020, Accessed April 20, 2021] Available in: https://raidboxes.io/es/blog/security/xss-attacken-verhindern/

[12] Watson Jon, 11 Best packet sniffing [Web Site]* Watson Jon,2021[Updated January 4, 2021, accessed May 29, 2021] Available in https://www.comparitech.com/net-admin/packet-sniffer-network-analyzers/

[13] Viewtinet, Network Observability & Optimization[Web Site]*Viewtinet,2020[Accessed May 12, 2021] Available in https://viewtinet.com/

[14] Sai Kiran, R.N. Kamakshi Devisetty .Building a Intrusion Detection System for IoT Environment using Machine Learning Techniques, Science Direct, 2020,171,2372-2379

[15] Iwaxx Sárl,Debooke[Web Site].Debooke,2019[Updated February 28, 2019, accessed June 18, 2021] Available in:

[16] https://docs.debookee.com/_/downloads/en/latest/pdf/

[17] Sanders Chris, Smith Jason, Applied Network Security Monitoring - Collection, Detection, and Analysis,Syngress,2014,[Web Site]* Girne, Northern Cyprus, 2018,[Access July 20, 2021] Available in: https://ieeexplore.ieee.org/document/8319360

[18] Peisert Sean, Schneier,Bruce, Okhravi Hamed,Massacci Fabio, Benzel Terri, Landwehr Carl, Mannan Mohammad, Perspectives on the SolarWinds Incident, IEEE Xplore,2021,19,7-13

[19] Marcin Gregorczyk, Piotr Zorawski, Piotr Nowakowski, Krzysztof Cabaj, Wojciech Mazurczyk, Sniffing Detection Based on Network Traffic Probing and Machine Learning,2020,8.

[20] Young Hwan Kim, konow Roberto,Dujovne Diego,Turletti Thierry, Dabbous Walid, Navarro Gonzalo, PcapWT: An efficient packet extraction tool for large volume network traces, Computer Networks,2015,79,91-102

[21] Bond,Federico Itzcovich,Ivan, Detection of behavior patterns in network traffic [Web Site]*Technological Institute of Buenos Aires. 2016 [Access May 15, 2021] Available in: https://ri.itba.edu.ar/bitstream/handle/123456789/1236/Informe%20PF.pdf?sequence=1&isAllowed=y

[22] Amazon Cloud Watch [Web Site]*AWS,2021[Access April 13, 2021] Available in: https://aws.amazon.com/es/cloudwatch/

[23] Netapp, Cloud Insights: monitor, optimize and protect your resources in the cloud [Web Site]* NetApp,2021[Accessed April 14, 2021] Available in https://www.netapp.com/es/cloud-services/cloud-insights/

[24] Mar Orizon Boost & Optimize Applications [Internet]*2021 March. [Access April 16, 2021] Available in https://www.informacion.es/empresas-en-alicante/2021/03/09/orizon-banca-rendimiento-tecnologicas-39543220.html

[25] Dynatrace, Dynatrace Cloud Infrastructure Monitoring [Internet]* Dynatrace,2018, [Updated December 4, 2021; Access April 16, 2021] Available in https://www.dynatrace.com/

[26] Microsoft.com,Azure Monitor Overview [Web Site]* Wren Brian, 2019 [Access April 4, 2021] Available in: https://docs.microsoft.com/en-us/azure/azure-monitor/overview

[27] Microsoft.com,Azure Monitor Overview [Web Site]* Wren Brian, 2019 [Access April 4, 2021] Available in: https://docs.microsoft.com/en-us/azure/azure-monitor/overview

[28] Oracle, Oracle Management Clud Solution [Web Site]* Oracle, 2016 [Access April 23,2021] Available in: https://www.oracle.com/us/solutions/cloud/oracle-management-cloud-brief-2714883.pdf

[29] Garcia, Vanesa. 5 pillars for the new cybersecurity. Byte TI [Online magazine] *July, 2021 [Accessed August 14, 2021] -1, Available in https://revistabyte.es/actualidad-it/ciberseguridad-5-pilares/

[30] Garcia, Vanesa. 10 recommendations to improve the cybersecurity posture of the company. Byte TI [Online magazine]*July, 2021 [Access July 16, 2021]1,Available in: https://revistabyte.es/ciberseguridad/ciberseguridad-recomendaciones/

[31] Drafting Byte Ti, 6 trends and technologies that will shape cybersecurity in 2021 [Online magazine]

December, 2020 [Access June 17, 2021], Available in: https://revistabyte.es/ciberseguridad/6-tendencias-en-ciberseguridad/

[32] Colt ,How the SD WAN is changing the networks and where it is going [Online magazine]* March, 2021 [Access April 4, 2021] Available in https://revistabyte.es/wp-content/uploads/2021/03/ES_Jan-21_SD-WAN-campaign_whitepaper.pdf

[33] Colt Techology Services, Why SD WAN Makes Sense for Multi-Cloud Infrastructure [Web Site]* January, 2021[Access April 3, 2021] Available in https://www.colt.net/es/resources/por-que-la-sd-wan-tiene-sentido-para-la-infraestructura-multinube/

[34] O'flaherty, Kate O'flaherty, AI: A new route for cyber-attacks or a way to prevent them? [Web Site]* March, 2021[Updated March 22, 2019; Access April 07, 2021] Available in: https://www.information-age.com/ai-a-new-route-for-cyber-attacks-or-a-way-to-prevent-them-123481083/

[35] Gottsegen, Gordon Machine Learning Cybersecurity: How It Works And Companies To Know [Web Site], builtin 2020 [Updated January 8, 2021, Accessed May 5, 2021] Available in: https://builtin.com/artificial-intelligence/machine-learning-cybersecurity

[36] Faro, Ismael Quantum computing, What is it and how to work from it? Spain, Byte, 2021

[37] Mosqueda, María L. Neurocybersecurity [Web Site]* Techherox [Access July 17, 2021] Available in: https://www.techherox.com/

[38] Abrams, Lorenzo Built-in Packet Tracker Comes to Windows 10 [Online magazine]* March, 2020 [Access September 2, 2021] Available in https://www.bleepingcomputer.com/news/microsoft/windows-10-quietly-got-a-built-in-network-sniffer-how-to-use/

[39] Microsoft, Packet Monitor (Pktmon) [Web Site]* October, 2021[Updated October 27, 2021; Access November 07, 2021] Available in: https://docs.microsoft.com/en-us/windows-server/networking/technologies/pktmon/pktmon