Module:-COSA(Concept Of Operating System And Administration)
Date:- 31/10/2022

Assignment :- 05 **Name:- Prauthviraj Nikam**

NAGIOS:-

What is Nagios?

Nagios is an open source continuous monitoring tool which monitors network, applications and servers. It can find and repair problems detected in the infrastructure, and stop future issues before they affect the end users. It gives the complete status of your IT infrastructure and its performance.

Why Nagios?

Nagios offers the following features making it usable by a large group of user community:

- It can monitor Database servers such as SQL Server, Oracle, Mysql, Postgres
- It gives application level information (Apache, Postfix, LDAP, Citrix etc.).
- Provides active development.
- Has excellent support form huge active community.
- Nagios runs on any operating system.
- It can ping to see if host is reachable.

Benefits of Nagios

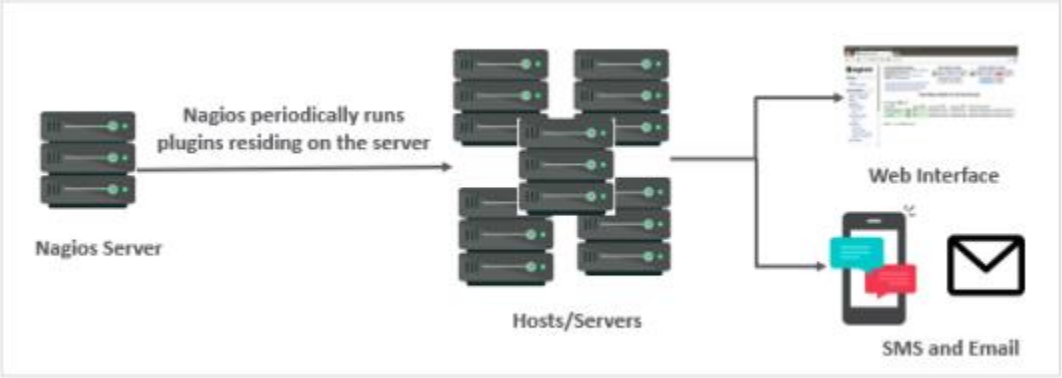
Nagios offers the following benefits for the users:

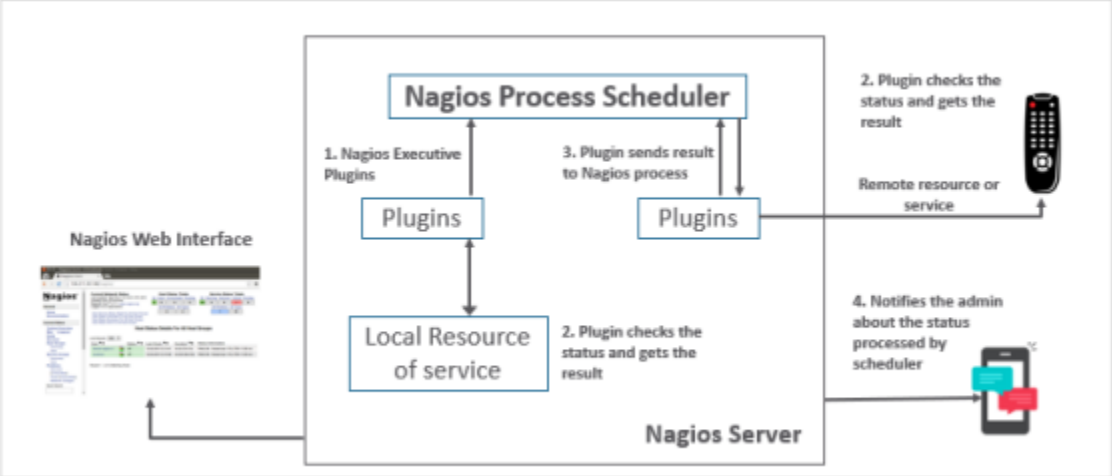
- It helps in getting rid of periodic testing.
- It detects split-second failures when the wrist strap is still in the “intermittent”stage.
- It reduces maintenance cost without sacrificing performance.
- It provides timely notification to the management of control and breakdown.

Nagios Architecture

The following points are worth notable about Nagios architecture:

- Nagios has server-agent architecture.
- Nagios server is installed on the host and plugins are installed on the remote hosts/servers which are to be monitored.
- Nagios sends a signal through a process scheduler to run the plugins on the local/remote hosts/servers. Plugins collect the data (CPU usage, memory usage etc.) and sends it back to the scheduler.
- Then the process schedules send the notifications to the admin/s and updatesNagios GUI.





TCPDUMP:-

The “tcpdump” is a packet analyzer and used to diagnose and analyze network issues. It captures the network traffic going through your device and looks over it. The “tcpdump” tool is a powerful tool to troubleshoot network issues. It comes with many options, which makes it a versatile command-line utility to fix network issues.

The above command will be used for Debian-based distributions such as Ubuntu and LinuxMint. For “Redhat” and “CentOS,” use

CMD:-

dnf install tcpdump

Wireshark :-

What is Wireshark?

Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

Uses of Wireshark:

Wireshark can be used in the following ways:

1. It is used by network security engineers to examine security problems.
2. It allows the users to watch all the traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyze dropped packets.
6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

What is a packet?

A packet is a unit of data which is transmitted over a network between the origin and the destination. Network packets are small, i.e., maximum **1.5 Kilobytes for Ethernet packets and 64 Kilobytes for IP packets**. The data packets in the Wireshark can be viewed online and can be analyzed offline.

Functionality of Wireshark:

Wireshark is similar to tcpdump in networking. **Tcpdump** is a common packet analyzer which allows the user to display other packets and TCP/IP packets, being transmitted and received over a network attached to the computer. It has a graphic end and some sorting and filtering functions. Wireshark users can see all the traffic passing through the network.

Wireshark can also monitor the unicast traffic which is not sent to the network's MAC address interface. But, the switch does not pass all the traffic to the port. Hence, the promiscuous mode is

not sufficient to see all the traffic. The various network taps or **port mirroring** is used to extend capture at any point.

Port mirroring is a method to monitor network traffic. When it is enabled, the switch sends the copies of all the network packets present at one port to another port.

What is color coding in Wireshark?

The packets in the Wireshark are highlighted with **blue**, **black**, and **green color**. These colors help users to identify the types of traffic. It is also called as **packet colorization**. The kinds of coloring rules in the Wireshark are **temporary rules** and **permanent rules**.

- The temporary rules are there until the program is in active mode or until we quit the program.
- The permanent color rules are available until the Wireshark is in use or the next time you run the Wireshark. The steps to apply color filters will be discussed later in this topic.

Features of Wireshark

- It is multi-platform software, i.e., it can run on Linux, Windows, OS X, FreeBSD, NetBSD, etc.
- It is a standard three-pane packet browser.
- It performs deep inspection of the hundreds of protocols.
- It often involves live analysis, i.e., from the different types of the network like the Ethernet, loopback, etc., we can read live data.
- It has sort and filter options which makes ease to the user to view the data.
- It is also useful in VoIP analysis.
- It can also capture raw USB traffic.
- Various settings, like timers and filters, can be used to filter the output.
- It can only capture packet on the PCAP (an application programming interface used to capture the network) supported networks.
- Wireshark supports a variety of well-documented capture file formats such as the PcapNg and Libpcap. These formats are used for storing the captured data.
- It is the no.1 piece of software for its purpose. It has countless applications ranging from the tracing down, unauthorized traffic, firewall settings, etc.

Iperf:-

What is iperf?

Iperf is a command-line tool that allows you to test the bandwidth, any way you like. Unlike online speed tests, you have to provide both server and client. In other words, when doing an online speed test, you connect to a server on the Internet, owned by the provider of the test (like Ookla). Then, the application measures the network performance between you and such a server. Instead, with iperf, you have to set up your own iperf server. Don't worry, you don't need special hardware, you only need to run a command from your prompt. In fact, you can have both the server and the client on the same computer.

The advantage of running your own server is predictability. You know where the server is, and you may repeat the test in the future. That's not the case with online services, where they allocate you a server dynamically. This means you won't be able to reproduce the same test in the future if you do an online speed test. Since you place the server whenever you want, you can also have it on your internal network and thus test internal links.

Getting iperf

The sable version of iperf is iperf3. It is free software (BSD license) you can download from iperf.fr. In a rush? Here is a quick link to the download page. You will find an iperf for any operating system and architecture you need. In this guide, we are using iperf3 on Windows (64 bit), but the tutorial on how to use iperf is the same for any OS.

If you are on Windows like me, you will get a compressed ZIP file. Extract it, and if you want to do things faster copy its content into `C:\Windows\System32`. This way, you will always have iperf3 at hand as a command on the prompt. If you don't do that, you will need to move to the folder where you have iperf before you can give the command.

How to use iperf

Once we have iperf, we need to learn how to use it. As we mentioned above, we need to run both server and client. The server will keep listening, accepting client connections. Thus, this is the first thing we need to do. Running the server is as simple as writing `iperf3 -s` in the prompt (`-s` stands for server). The first time you do that, on Windows, it will ask you network permission. Of course, flag the permissions and click **Allow access**.

NMAP:-

What is Nmap?

Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.

Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

Gordon Lyon (pseudonym Fyodor) wrote Nmap as a tool to help map an entire network easily and to find its open ports and services.

Nmap has become hugely popular, being featured in movies like The Matrix and the popular series Mr. Robot.

Why use Nmap?

There are a number of reasons why security pros prefer Nmap over other scanning tools.

First, Nmap helps you to quickly map out a network without sophisticated commands or configurations. It also supports simple commands (for example, to check if a host is up) and complex scripting through the Nmap scripting engine.

Other features of Nmap include:

- Ability to quickly recognize all the devices including servers, routers, switches, mobile devices, etc on single or multiple networks.
- Helps identify services running on a system including web servers, DNS servers, and other common applications. Nmap can also detect application versions with reasonable accuracy to help detect existing vulnerabilities.
- Nmap can find information about the operating system running on devices. It can provide detailed information like OS versions, making it easier to plan additional approaches during penetration testing.
- During security auditing and vulnerability scanning, you can use Nmap to attack systems using existing scripts from the Nmap Scripting Engine.
- Nmap has a graphical user interface called Zenmap. It helps you develop visual mappings of a network for better usability and reporting

NESSUS:-

Nessus is one of the many vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks. This article will focus on this vulnerability scanner, discussing the fundamentals that one needs to have before getting started with the tool, the different scanning capabilities that it provides, what it takes to run the tool and how results appear once scans are complete.

Nessus products brief

Nessus is sold by Tenable Security. The tool is free for non-enterprise use; however, for enterprise consumption, there are options that are priced differently. The following are the available options at your disposal:

1. **Tenable.io** is a subscription-based service available here. It allows different teams to share scanners, schedules, scan policies and scan results. Tenable also contains what was previously known as Nessus Cloud, which used to be Tenable's Software-as-a-Service solution. Tenable.io also allows for the customization of workflows for effective vulnerability management.
2. **Nessus Agents** provide a flexible way of scanning hosts within your environment without necessarily having to provide credentials to hosts. The agents enable scans to be carried out even when the hosts are offline. The application areas of these agents are wide. Consider environments that lack traditional malware protection, such as antivirus solutions — the overhead these agents exert within hosts is quite small. Here, agents take up minimal system resources within the hosts they are installed in, whilst still providing adequate malware protection.
3. **Nessus Professional** is the most commonly-deployed vulnerability assessment solution across the industry. This solution helps you perform high-speed asset discovery, target profiling, configuration auditing, malware detection, sensitive data discovery and so much more. Nessus Professional runs on client devices such as laptops and can be effectively used by your security departments within your organization.
4. **Nessus Manager** is used to provide the capabilities of the Nessus Professional solution along with numerous additional vulnerability management and collaboration features. However, Nessus Manager is no longer sold as of February 1st, 2018. This solution was used within organizations to collaborate and share information between different departments within the

organization. It provided the ability to monitor company assets as well as devices in hard-to-reach environments.

These products discussed above offer multiple services that range from Web application scanning to mobile device scanning, cloud environment scanning, malware detection, control systems auditing (including SCADA and embedded devices) and configuration auditing and compliance checks.

Fundamentals of the Nessus vulnerability scanner

For us to appreciate the capabilities Nessus offers, we need to understand some fundamentals. We will first discuss the user interface and take a look at how to install Nessus on Linux and Windows Operating Systems.

1. Installation on Linux

The downloadable installer can be found here for Linux-based systems. You need to make sure you know the distribution of Linux you are running in order to choose which installer to download. For instance, this article covers the Debian file system that Kali Linux is based on, so we will be downloading the *.deb installer file. We are also running a 64-bit version of Kali Linux; you'll need to find out the architecture you are running.

As of the writing of this article, the latest version of Nessus is 8.0.0.

Once the package file has been downloaded, you may install it from within the Linux terminal using the command below:

$ sudo dpkg -i Nessus-8.0.0-debian6_i386.deb

If you are using any other version of Linux, use the commands below:

For RedHat version 6:

 # rpm -ivh Nessus-<version number>-es6.x86_64.rpm

For FreeBSD version 10:

 # pkg add Nessus-<version number>-fbsd10-amd64.txz

After installation on your Linux system, be sure to start up the Nessus daemon as shown below:

For Red Hat, CentOS, Oracle Linux, Fedora, SUSE and FreeBSD, use the command below:

 # service nessusd start

For Debian/Kali and Ubuntu, use the command below:

 # /etc/init.d/nessusd start