Assignment Report

*Setting up Syslog-ng on CentOS*

A write-up outlining the complete walk-through from setting up CentOS VM to installing and setting up a Syslog-ng server. Each task includes a brief introduction and the steps followed to complete that task.

Thanmai D L

11/2/2022

Table of Contents

[1. Setting Up A Linux Environment 2](#_Toc118215342)

[Steps involved in creating a CentOS 7 VM on Oracle VirtualBox: 2](#_Toc118215343)

[2. Port Scan using Nmap 3](#_Toc118215344)

[Steps to perform an open port scan: 3](#_Toc118215345)

[3. Creating a user in Linux 5](#_Toc118215346)

[The useradd command 5](#_Toc118215347)

[Steps to add a new user: 5](#_Toc118215348)

[4. Creating a New Directory and Modifying Permissions 6](#_Toc118215349)

[Switching to the newly created user: 6](#_Toc118215350)

[Steps to create a new directory and change file permissions 6](#_Toc118215351)

[5. Setting Up Syslog-ng Receiver 7](#_Toc118215352)

[Introduction to Syslog-ng 7](#_Toc118215353)

[Installing Syslog-ng on CentOS 7](#_Toc118215354)

[Steps to setup a Syslog-ng Receiver 8](#_Toc118215355)

# Setting Up A Linux Environment

CentOS is one of the most popular Linux distributions. It is an open-source operating system that provides an enterprise-class computing platform. The CentOS project oversees two versions of the distro – CentOS Linux and CentOS Stream. The main difference between them is that the former is downstream of Red Hat Enterprise Linux while CentOS Stream is the upstream version containing upcoming minor Red Hat updates.

### Steps involved in creating a CentOS 7 VM on Oracle VirtualBox:

* Download Linux distro from official [CentOS website](https://www.centos.org/download/)
* Download and Install latest version of [Oracle VM VirtualBox](https://www.virtualbox.org/wiki/Downloads)
* Setup CentOS on VirtualBox with the following configuration

CentOS VM setup


* Spin up the Linux VM and complete installing CentOS on the virtual machine
* Check for available updates



* Update CentOS



# Port Scan using Nmap

A port scan is a method for determining which ports on a network are open. As ports on a computer are the place where information is sent and received, port scanning is analogous to knocking on doors to see if someone is home. Running a port scan on a network or server reveals which ports are open and listening (receiving information), as well as revealing the presence of security devices such as firewalls that are present between the sender and the target. This technique is known as fingerprinting. It is also valuable for testing network security and the strength of the system’s security system. Due to this functionality, it is also a popular reconnaissance tool for attackers seeking a weak point of access to break into a computer.

A port scan sends a carefully prepared packet to each destination port number. The basic techniques that port scanning software is capable of include:

* **Vanilla** – It is a full connect scan, meaning it sends a SYN flag (request to connect) and upon receiving a SYN-ACK (acknowledgement of connection) response, sends back an ACK flag.
* **SYN Scan** – Also referred to as a half-open scan, it only sends a SYN, and waits for a SYN-ACK response from the target.
* **XMAS and FIN Scans** –In a FIN scan, an unsolicited FIN flag (used normally to end an established session) will be sent to a port. An XMAS scan simply sends a set of all the flags, creating a nonsensical interaction.

### Steps to perform an open port scan:

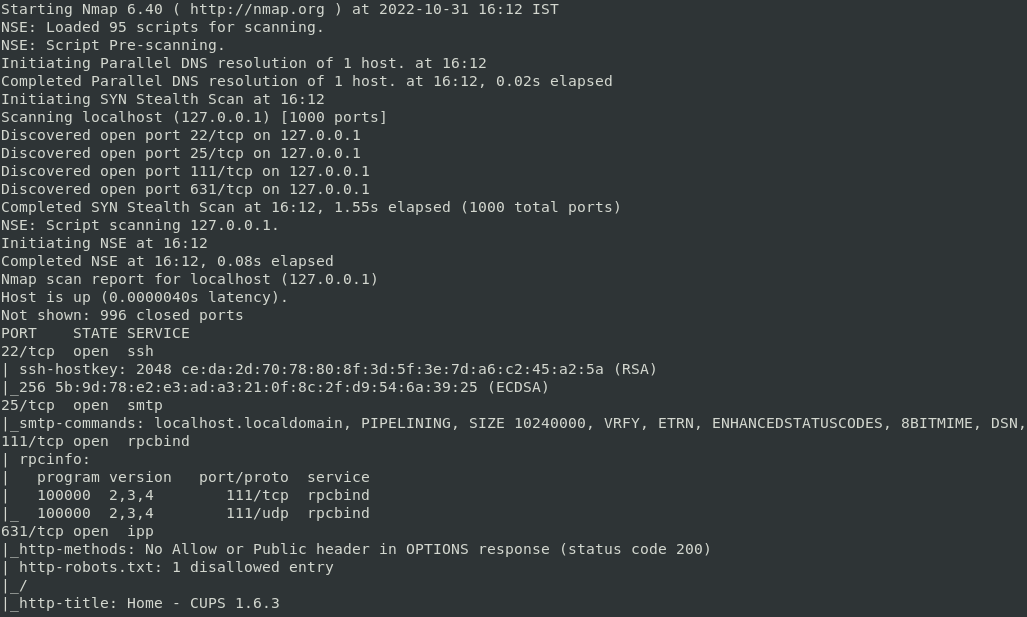
* Install Nmap port scanner tool using yum

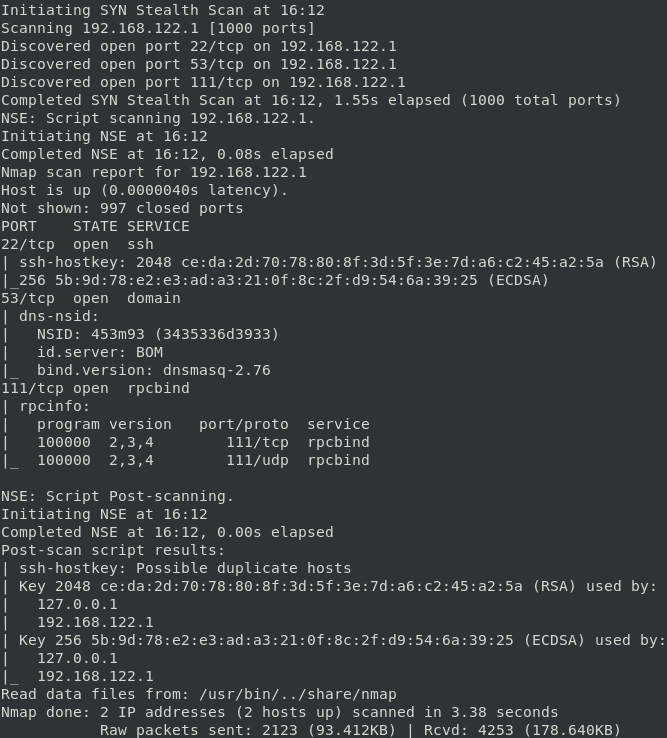


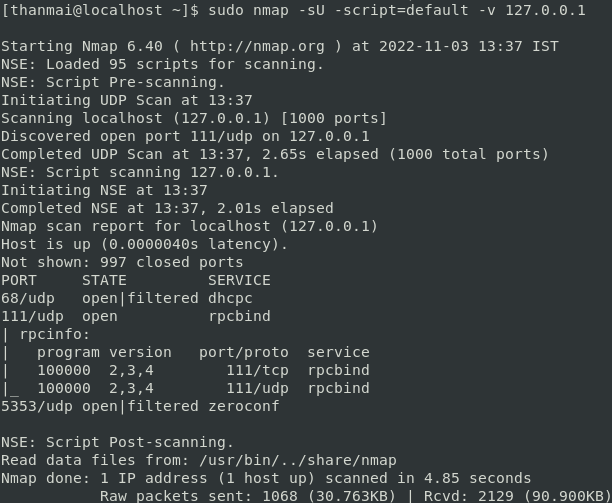
* Scanning the IPv4 and loopback address of VM using the default script



* Output of Port Scan







# Creating a user in Linux

Linux is a multi-user system, which means that more than one person can interact with the same system at the same time.

### The useradd command

Only root or users with sudo privileges can use the useradd command to create new user accounts. When invoked, useradd creates a new user account according to the options specified on the command line and the default values set in the /etc/default/useradd file.

Text

Description automatically generated

### Steps to add a new user:

* Create new user using useradd with default option

Text

Description automatically generated



* + The command adds an entry to the /etc/passwd, /etc/shadow, /etc/group and /etc/gshadow files
  + To be able to log in as the newly created user, a password needs to be set

Graphical user interface, text

Description automatically generated with medium confidence

# Creating a New Directory and Modifying Permissions

A new directory is created from the command line using the mkdir command. The mkdir stands for 'make directory'.

### Switching to the newly created user:

* Switch user to avglinuxenjoyer



* After switching to avglinuxenjoyer



### Steps to create a new directory and change file permissions

* Creating a new directory named test folder



* + An escape character (“\”) is used to escape a special character (whitespace)
* Default permission assigned to the newly created directory



* Changing file permissions using chmod command and verifying the changes



# Setting Up Syslog-ng Receiver

In computing, syslog is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the type of system generating the message, and is assigned a severity level.

Computer system designers may use syslog for system management and security auditing as well as general informational, analysis, and debugging messages. A wide variety of devices, such as printers, routers, and message receivers across many platforms use the syslog standard. This permits the consolidation of logging data from different types of systems in a central repository. Implementations of syslog exist for many operating systems.

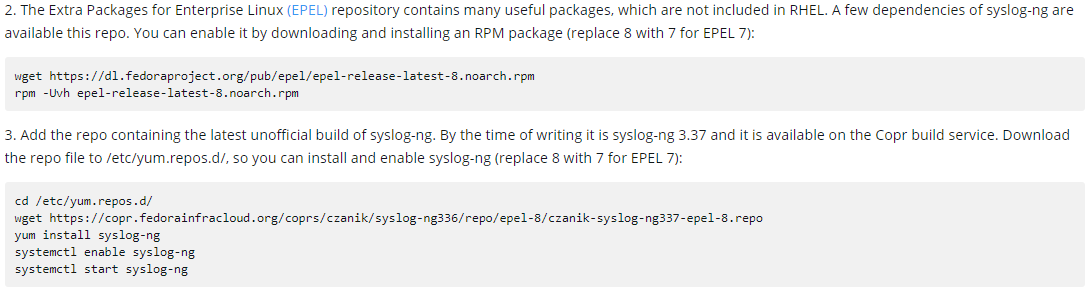
When operating over a network, syslog uses a client-server architecture where a syslog server listens for logs messages coming from clients.

### Introduction to Syslog-ng

The syslog-ng Open-Source Edition (syslog-ng OSE) application is a flexible and highly scalable system logging application that is ideal for creating centralized and trusted logging solutions. Among others, syslog-ng OSE offers features such as:

* + Secure and reliable log transfer
  + Disk-based message buffering
  + Secure logging using TLS
  + Flexible data extraction and processing
  + Filter and classify
  + Parse and rewrite
  + IPv4 and IPv6 support and more.

### Installing Syslog-ng on CentOS



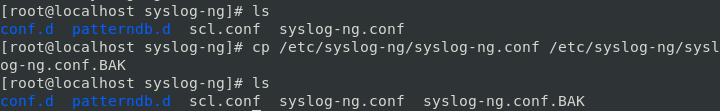
### Steps to setup a Syslog-ng Receiver

* Check status of syslog-ng

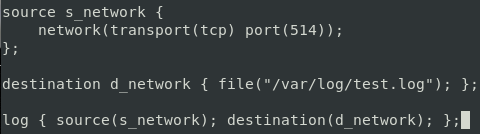
Text

Description automatically generated

* Syslog-ng receiver configuration
  + Creating a backup of default syslog-ng.conf file (/etc/syslog-ng)



* + Editing syslog-ng.conf file by adding the following configurations



* + Reloading syslog-ng service



* + Checking port status of port 514 using netstat command



Graphical user interface, text, application, email

Description automatically generated

* Testing the syslog-ng server
  + Pushing sample messages



* + Verifying messages received by syslog server

