“Київський фаховий коледж зв’язку”

Циклова комісія Комп’ютерної та програмної інженерії

ЗВІТ ПО ВИКОНАННЮ

ЛАБОРАТОРНОЇ РОБОТИ №8

з дисципліни: «Операційні системи»

Тема: “Збереження службових даних системи та її мережева конфігурація”

Виконали

студенти

групи РПЗ-03

Команда 6: Sichkar Maxim,

Brytyuk Bohdan

Kyiv 2023

The goal of the work:

1. Getting practical skills for working with the Bash command shell.

2. Familiarity with the basic structures for saving system data - processes, memory, log files and

kernel status message.

3. Acquaintance with the FHS standard.

4. Acquaintance with network configuration actions.

Material provision of classes

1. IBM PC type computer.

2. OS family Windows (Windows 7).

3. Virtual machine - Virtual Box (Oracle).

4. GNU/Linux operating system - CentOS.

5. Cisco network academy site netacad.com and its online Linux courses

**Tasks for preliminary preparation.**

Read the short theoretical information for the laboratory work and make a small dictionary

basic English terms for command assignments and their parameters.

**2. Study the materials of the online course of the Cisco Academy “NDG Linux Essentials”:**

- Chapter 13 - Where Data is Stored

- Chapter 14 - Network Configuration

**3. Take the test in the NDG Linux Essentials course on the following topics:**

- Chapter 13 Exam

- Chapter 14 Exam

**4. On the basis of the considered material, answer the following questions:**

**4.1. Explain the concept of "pseudo file system", why does the system need it?**

A pseudo file system is a file system that exists in memory and is used by an operating system to provide an interface to various system components and resources, such as the CPU, memory, and input/output devices. The term "pseudo" is used to indicate that this file system does not correspond to any physical device, but is instead a representation of the operating system's internal state.

One of the main reasons why an operating system needs a pseudo file system is to provide a unified interface to system components and resources, regardless of their physical location or type. By presenting all system components and resources as files or directories within a hierarchical file system, applications can access them using the same set of system calls and utilities that they use to access regular files.

Another reason why a pseudo file system is important is that it enables the operating system to manage system resources more efficiently. For example, the system can use a file in the pseudo file system to represent a hardware device or system parameter, and can then use standard file operations to control or query that device or parameter. This approach simplifies the implementation of device drivers and system utilities, and can help to reduce the overall complexity and overhead of the operating system.

**4.2. Why users don't go directly to the /proc directory so often, how can you get out of it get information?**

The /proc directory contains a lot of system information, and not all of it may be relevant to a particular user's needs. Additionally, the information in the /proc directory is often in a raw and unfiltered format, which can make it difficult for users to understand and use effectively.

Instead, users may use specific tools or commands that allow them to access and manipulate the information in the /proc directory more easily. For example, the top command can be used to display real-time information about system processes, or the sysctl command can be used to modify certain system settings.

In general, the information in the /proc directory is meant to be used by system administrators and advanced users who have a good understanding of how the system works. For everyday users, there are usually simpler and more user-friendly ways to access the information they need.

**4.3. What is the purpose of the files /proc/cmdline, /proc/meminfo and /proc/modules?**

The purpose of the files /proc/cmdline, /proc/meminfo, and /proc/modules are as follows:

/proc/cmdline: This file contains the command-line arguments that were passed to the Linux kernel when the system was booted. It provides information about the kernel parameters and boot options that are being used by the system. It is useful for troubleshooting system boot issues or for checking which kernel options are being used.

/proc/meminfo: This file provides detailed information about the system's memory usage. It contains information about the total amount of memory available, how much memory is being used, and how much memory is free. It also provides information about swap space usage, which is used when the system runs out of physical memory. This file is useful for monitoring system performance and diagnosing memory-related issues.

/proc/modules: This file lists all the kernel modules that are currently loaded in the system. A kernel module is a piece of code that can be loaded into the kernel at runtime to extend its functionality. This file is useful for checking which modules are loaded and for troubleshooting issues related to kernel modules.

**4.4. What is the purpose of the free command?**

The free command is a tool used in Linux and Unix operating systems to display the amount of free and used memory (both physical and swap memory) in the system. It provides a summary of the memory usage and statistics of the system's memory and is particularly useful for diagnosing and troubleshooting issues related to memory usage. The free command shows the total amount of memory available in the system, the amount of used memory, and the amount of free memory. It also shows information about the swap memory and the buffer and cache memory used by the system. The free command is a simple yet powerful tool for system administrators to monitor the memory usage of their systems and take appropriate action as needed.

**4.5. Why are log files needed, give examples of their use?**

Log files are used to record events and activities in a system or application. They serve as a historical record of what happened in a system or application, which can be used for troubleshooting, analysis, and auditing purposes.

Here are some examples of the use of log files:

System Administration: System logs are used by system administrators to diagnose and troubleshoot problems in the operating system, network devices, and other system components. They can also be used to monitor the performance of the system and ensure that it is running smoothly.

Application Monitoring: Application logs are used to monitor the activity of an application and identify errors or issues that occur. This can help developers and system administrators to diagnose and fix problems with the application.

Security: Security logs are used to track activity on a system or application and identify potential security threats. They can be used to detect unauthorized access attempts, malware infections, and other security breaches.

Compliance: Log files are often required for compliance purposes, such as in the case of financial institutions, healthcare providers, and government agencies. These organizations need to maintain detailed records of their activities to comply with regulations and laws.

**4.6. What is the purpose of the /var/log/dmesg file?**

The /var/log/dmesg file contains the output of the dmesg command, which is used to display the kernel's ring buffer. The ring buffer contains messages that the kernel generates during the boot process and while the system is running, including information about hardware and driver initialization, system messages, and errors.

The purpose of the /var/log/dmesg file is to provide a persistent record of the messages generated by the kernel, which can be useful for troubleshooting issues related to hardware, device drivers, and system configuration. The file can be viewed using a text editor or the dmesg command, and is often examined by system administrators and developers to diagnose system problems or identify areas where performance can be improved.

**4.7. What is FHS designed for?**

FHS stands for Filesystem Hierarchy Standard, and it is a set of guidelines for the directory and file structure of Linux and other Unix-like operating systems. The purpose of FHS is to provide a standardized directory structure across different Linux distributions, allowing software developers and system administrators to write and manage software that can run on any compliant system.

The FHS defines a set of directories and their contents, specifying what types of files should be stored in each directory. For example, the /bin directory should contain essential command-line utilities, while the /var directory should contain variable data that changes frequently during the system's operation, such as log files and spool directories.

By adhering to the FHS, Linux distributions can ensure that applications and system services can locate important files in their expected locations, making it easier to manage and troubleshoot the system. It also makes it easier for users to find and organize their files, as they know where to look for specific types of files and data.

**4.8. What are the main commands in Linux for viewing and configuring the network**

There are several commands in Linux for viewing and configuring the network. Here are some of the main ones:

ifconfig: This command is used to view and configure network interfaces. It shows information about the current network configuration and allows you to configure settings such as IP address, netmask, and gateway.

ip: This command is a more modern replacement for ifconfig and is used to view and configure network interfaces as well as routing tables and other network settings.

netstat: This command is used to view active network connections, open ports, and other network statistics.

ping: This command is used to test network connectivity by sending ICMP packets to a specified host or IP address.

traceroute: This command is used to trace the path of packets from your computer to a specified host or IP address, showing the network hops along the way.

route: This command is used to view and modify the routing table, which determines how network traffic is routed between different networks.

iptables: This command is used to configure the Linux firewall, including setting rules for inbound and outbound traffic.

ss: This command is similar to netstat, but provides more detailed information about active network connections.

nmcli: This command is used to view and configure network connections using the NetworkManager service.

5. Prepare the initial version of the report electronically:

- Title page, topic and purpose of the work

- Glossary of terms

- Answers to p. 4.1 and p. 4.5 from tasks for preliminary preparation

**Progress.**

1. Initial work in CLI mode in Linux OS of the Linux family:

1.1. Start the VirtualBox virtual machine, select CentOS and run it. Log in

under user: CentOS, password for login: reverse (if you run LR in 401 aud.) and run terminal.

1.2. Start the Ubuntu\_PC virtual machine (if you are doing the LR tasks through the netacad academy)

1.3. Start your Linux family operating system (if you are working on your own PC and its installed) and launch the terminal.

2. Work through all the command examples presented in the labs of the NDG Linux Essentials course - Lab 13: Where Data is Stored and Lab 14: Network Configuration. Create a table to describe these teams\*\*\*

The name of the command Its purpose and functionality su Change the current user to root ls /proc View the contents of the /proc system directory (root access rights are required for this)

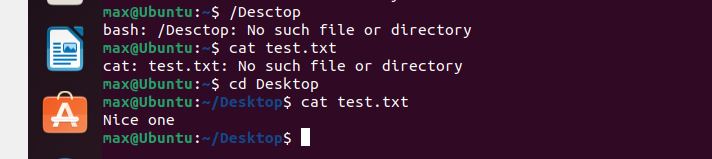
\*\*\*Screenshots of the execution of commands in the terminal may not be presented, it is enough to briefly describe the commands

in the table.

3. Perform practical tasks in the terminal (show screenshots):

- this lab used the cat command, explore its capabilities and describe for

what tasks it is intended for;



- demonstrate examples when the cat command is used to create a file, view

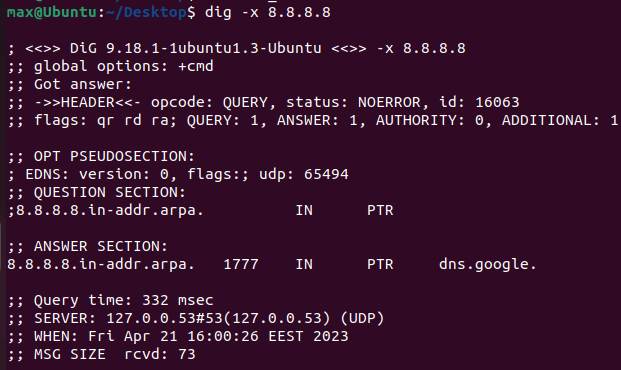
file contents, forwarding information to another file, gluing several files into one;



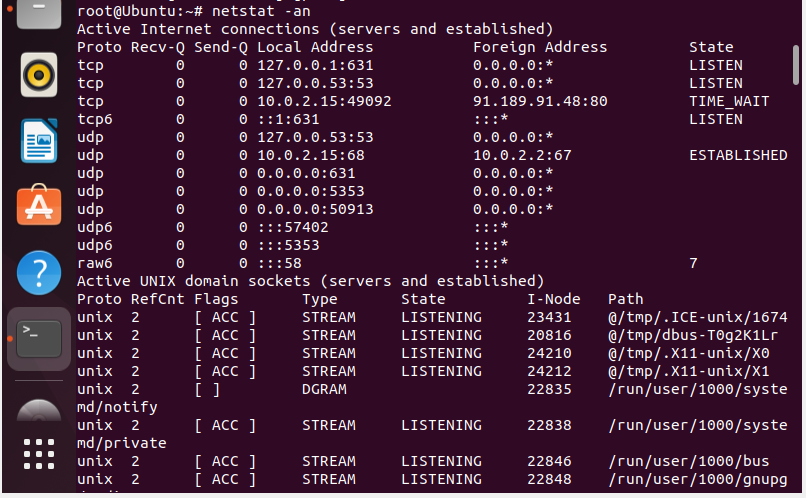
- what parameters of the cat command should be used to number the lines of the file, to display non-printing characters, remove empty lines?



- describe the capabilities of the dig command and give examples;



- describe the capabilities of the netstat command and give examples;.



**Control questions**

1. **How are cat and tac commands related to each other?**

The cat and tac commands are related to each other in that they both deal with files and file contents, but they differ in the order in which they display the contents

The cat command (short for "concatenate") is used to display the contents of one or more files in sequential order. For example, the command cat file1.txt file2.txt will display the contents of file1.txt followed by the contents of file2.txt.

The tac command (short for "reverse concatenate") is similar to cat, but it displays the contents of files in reverse order. For example, the command tac file1.txt file2.txt will display the contents of file2.txt followed by the contents of file1.txt.

1. **What does the ss team do?**

The "ss" command in Linux is used for showing detailed information about network sockets, network connections, and network statistics. It is used to display information about both TCP and UDP connections. The "ss" command stands for "socket statistics" and is used as an alternative to the older "netstat" command. The ss team is responsible for maintaining and improving the "ss" command in Linux.

1. **What is the difference between ps --forest and pstree commands?**

Both ps --forest and pstree commands display the process hierarchy in a tree-like structure, but there are some differences between them:

ps --forest is a command that needs to be executed in the terminal, while pstree is a standalone command.

ps --forest is part of the ps command, which is a widely used command in Linux for viewing information about running processes, while pstree is a standalone command that is specifically designed for displaying the process hierarchy in a tree-like structure.

ps --forest provides more detailed information about the processes, such as the parent process ID and the user running the process, while pstree only displays the process name and its descendants.

ps --forest is more flexible in terms of the information it displays and the options it provides for customizing the output, while pstree is a more simplified and easy-to-use command for quickly visualizing the process hierarchy.

1. **In which directories are system settings stored?**

System settings are stored in various directories in Linux, including:

/etc: This directory contains system-wide configuration files for various applications, as well as system startup and shutdown scripts.

/usr: This directory contains read-only data for applications and other system files, including system-wide configuration files.

/var: This directory contains variable data, such as log files, spool files, and other temporary files created by system applications.

/bin: This directory contains essential executable binaries that are required for the system to function properly.

/sbin: This directory contains system binaries that are typically used by the system administrator for system maintenance tasks.

/lib: This directory contains shared library files that are required for system programs and applications to run.

/usr/local: This directory contains locally installed software and data that is not part of the base Linux distribution.

1. **In which directories can you find the programs installed in the system and available to the user?**

In Linux, the programs installed in the system are usually stored in directories such as:

/usr/bin: This directory contains user binaries (executable programs) for general use. These programs are usually available to all users on the system.

/usr/sbin: This directory contains system administration binaries (executable programs) that are usually intended for use by the system administrator. These programs are not usually available to regular users.

/usr/local/bin: This directory contains locally installed user binaries. Programs installed in this directory are not part of the default system installation and are installed by the system administrator.

/usr/local/sbin: This directory contains locally installed system administration binaries. Programs installed in this directory are not part of the default system installation and are installed by the system administrator.

/bin: This directory contains essential system binaries (executable programs) that are required for the system to function properly. These programs are usually available to all users on the system.

/sbin: This directory contains essential system administration binaries (executable programs) that are required for the system to function properly. These programs are not usually available to regular users.

/opt: This directory is used for optional software packages that are not part of the default system installation.

1. **In which directories can you find installed system programs and programs intended for execution superuser?**

System programs and programs intended for execution by the superuser are typically located in directories that are not accessible to regular users. The most common directories where these programs can be found are:

/bin: This directory contains essential system utilities and programs that are necessary for the system to boot and run.

/sbin: This directory contains system administration utilities and programs that are used by the system administrator to manage the system.

/usr/sbin: This directory contains system administration utilities and programs that are not essential for the system to boot and run, but are still necessary for system administration tasks.

/usr/bin: This directory contains user-level programs and utilities that are not essential for the system to run, but are available to all users.

/usr/local/sbin: This directory contains locally installed system administration utilities and programs that are not part of the standard distribution.

/usr/local/bin: This directory contains locally installed user-level programs and utilities that are not part of the standard distribution.

1. **Explain the purpose of the ping, ifconfig, traceroute commands.**

ping: The ping command is used to check the connectivity between two devices over an IP network. It sends packets to the destination device and waits for a response. If a response is received, it means that the connection is alive and functioning properly. The ping command is often used for troubleshooting network issues and for testing the network connection between two devices.

ifconfig: The ifconfig command is used to configure network interfaces on a Linux system. It displays information about the current network configuration, such as IP addresses, netmasks, and network interfaces. It can also be used to configure network settings, such as IP addresses and netmasks, as well as to bring up or down network interfaces.

traceroute: The traceroute command is used to trace the route that packets take from one device to another over an IP network. It works by sending packets with increasing TTL (Time To Live) values and observing the route that the packets take as they are discarded by intermediate devices. This allows network administrators to identify network congestion or other issues that may be affecting network performance.

1. **What are network interfaces called in Linux?**

Network interfaces in Linux are commonly referred to as network adapters, network cards, or simply NICs (Network Interface Cards). In Linux, network interfaces are typically named in the format of ethX, where X is a number representing the interface number (e.g. eth0, eth1, eth2, etc.). However, newer versions of Linux may use different naming conventions, such as enpXsY, where X represents the type of interface (e.g. en for Ethernet), and Y represents the slot number.

1. **How to display the parameters of only one network interface using the ifconfig command (eg eth1) and not all?**

To display the parameters of a specific network interface, such as eth1, you can use the following command:

ifconfig eth1

This command will display the configuration information for eth1 only, rather than showing all available network interfaces.

**Conclusion:** Preservation of service data of the system and its network configuration are important components of the security and efficiency of the computer system.

Saving system service data may include saving configuration files, databases, log files, and other important data. This data may be needed to debug the system, recover from a failure, or ensure system security.