IE2012 – Systems and Network Programming

Assignment

This case study is designed to provide you with hands-on experience in a virtual Linux environment, covering essential skills for Linux administration. You will learn core concepts, configure essential services, and gain practical experience through a series of tasks.

Deliverables (descriptive explanation given at the end of the assignment):

- A virtual machine image containing a configured Linux environment.
- A detailed report documenting your activities, steps taken, and configurations achieved for each topic.

1. Basics of Linux Environments

Objectives:

- Understand the core components of a Linux system.
- Navigate the Linux file system using the command line.
- Learn basic Linux commands for file manipulation, system information retrieval, and user management.

Tasks:

1. **Virtual Machine Setup:**
   Install a virtual machine software like VirtualBox (https://www.virtualbox.org/wiki/Downloads) or VMware Workstation Player (https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html). Download a Linux distribution like Ubuntu or CentOS (https://ubuntu.com/download/desktop, https://www.centos.org/download/). Create a virtual machine with appropriate resource allocation and install the chosen Linux distribution.
2. **Command Line Introduction:** Access your virtual machine and log in with the new created user credentials. Learn basic navigation commands like cd, ls, pwd, mkdir, and rmdir. Practice file manipulation commands like cp, mv, cat, and more.
3. **System Information and User Management:** Use commands like uname -a, cat /proc/version, df -h, and free -m to retrieve system information. Explore user management commands like id, whoami, passwd, and useradd to understand user accounts and permissions.

2. DHCP, DNS and NTP Services

Objectives:

- Understand the functionalities of DHCP, DNS, and NTP services.
- Configure and manage these services on a Linux system.

Tasks:

1. **DHCP (Dynamic Host Configuration Protocol):** Research DHCP and its role in network configuration. Learn how to install and configure a DHCP server like isc-dhcp-server on your Linux machine. Simulate a small network environment with your virtual machine and configure it to obtain an IP address automatically from the DHCP server.
2. **DNS (Domain Name System):** Understand the role of DNS in resolving hostnames to IP addresses. Learn how to configure a DNS server like BIND on your Linux machine. Configure your virtual machine to use your local DNS server or a public DNS server like Google DNS (8.8.8.8).
3. **NTP (Network Time Protocol):** Learn the importance of accurate system time. Install and configure an NTP client on your Linux machine to synchronize time with an NTP server on the internet.

3. Shell Scripting and Security

Objectives:

- Learn the basics of shell scripting in Linux.
- Understand and configure security tools like SSH, iptables, and Access Control Lists (ACLs).

Tasks:

1. **Shell Scripting:** Learn the basics of shell scripting syntax, control flow statements (if, else, for, while), and functions. Create simple shell scripts to automate the following tasks
    i. Write a script to automate a report that captures key system details every day. This script can be scheduled to run using cron jobs. Get System Information such as *Date, Uptime, Free memory and Disk Usage*. Create a report file at the location with the file name as mentioned below.
    Destination directory : /home/user/system_reports

    ii. Write a script to automate the backup of a critical directory (/home/user/documents) containing important files. This script can be scheduled to run periodically. Make sure to name the backup file with the date.
    Source directory : /home/user/documents
    Destination directory : /home/user/backup/documents

2. **SSH (Secure Shell):** Understand the importance of secure remote access. Configure SSH server on your Linux machine for secure remote login using tools like sshd. Connect to your virtual machine remotely using an SSH client from another computer and take necessary screenshots.

3. **iptables and ACLs:** Learn how to manage network traffic using firewalls and iptables rules. Define basic firewall rules using iptables to allow specific ports and services while blocking unwanted traffic. Define rules (ACL or iptable) to implement the following security measures.

    i. Web Server Security: Allow incoming traffic only on port 80 (HTTP) and port 443 (HTTPS) for your web server. Block all other incoming traffic by default.
    ii. Remote Administration Access: Allow SSH access (port 22) only from specific IP addresses of your trusted machines used for administration. This restricts remote access attempts to authorized sources.
    iii. Allow Specific Applications: If you know the port numbers used by specific applications you want to allow (like a video conferencing app using port 443), you can create an ACL rule to permit traffic only for those ports.
    iv. Allow Pings (ICMP Echo Request): This basic rule allows ping requests (ICMP Echo Request) to your machine, which can be helpful for troubleshooting network connectivity.
    v. Printer Server Access: For a printer server, allow printing traffic (port 9100) only from specific IP addresses within your local network. Block all external access to the printer server to prevent unauthorized printing.

4. Best practices

Objectives:

- Understand security aspects of network interface configuration.

Tasks:

1. Implement and explain 5 best practices to be implemented after installing Linux in a machine, to ensure the security aspects of network interface configuration.

Final Deliverables of the assignment:

Prepare a report document including the following results / confirmations done under each Topic.

1. Document the installation process for the virtual machine and Linux distribution.
2. Test 15 basic Linux commands you learned with a brief description of their functionality and add screenshots of them when executed in the terminal.
3. Document the configuration steps for DHCP, DNS, and NTP services on your virtual machine with screenshots demonstrating successful configuration of these services.
4. Add screenshots of the scripts written (both) and copy the text separately and add into the documentation of the report.
5. Document the the configuration steps for SSH server, iptables and ACLs.
6. Add screenshots of the rules written in the firewall (or in iptable) and copy the text separately and add into the documentation of the report.
7. Document the implementation of best practices to ensure the security aspects of network interface configuration.

Mark distribution of the assignment:

1. VM installation steps - (5)
2. Basic navigation commands (cd, ls, pwd etc) and File manipulation commands (-a, cat /proc/version, df -h) - (5)
3. 15 basic Linux commands with brief descriptions - (10)
4. DHCP installation steps (5)
5. DNS installation steps (5)
6. NTP installation steps (5)
7. System details script with all variables and cron job (Date, Uptime, Free memory and Disk Usage) (15)
8. Backup script with cron job (15)
9. Connecting to VM remotely using an SSH client from another computer (5)
10. 5 iptable rules with screen shots (2*5)
11. Implementing 5 best practices in a Linux based environment (4*5)