TEST PROJECT IT NETWORK SYSTEMS ADMINISTRATION

WSC2015_TP39_ModuleA_actual

Submitted by: Module A group

Danny Meier CH
Andreas Strömgren SE
Toivo Pärnpuu EE
Jae Ha Lee KR
Jun Tian CN
Hamed Kargarzadeh IR
Karapet Kuyumjyan AM
Sujeet Kumar IN
Chin-Yu Yang TW
Semyon Ovsyannikov RU
Zoltán Sisák HU

CONTENTS

ISLAND A

CONTENTS

This Test Project proposal consists of the following document/file:

WSC2015_TP39_actual.docx

INTRODUCTION

The competition has a fixed start and finish time. You must decide how to best divide your time.

Please **carefully** read the following instructions!

When the competition time ends, please leave your station in a running state.

Please do not touch the VMware configuration as well as the configuration of the VM itself except the CD-ROM / HDD drives

PHYSICAL MACHINE (HOST)

FOLDER PATHS

Virtual Machines:	C:\VMs (Host)
ISO Images:	C:\ISO (Host)

LOGIN

Username:	skill39

DESCRIPTION OF PROJECT AND TASKS

You are a system engineer in a newly established company, which is developing mobile apps.

The task for you is to build a new IT-infrastructure for the company. The entirely network should be Linux based.

The employees should be able to send e-mails and also have access to the file shares.

You have also to set up a remote access VPN for road warriors, a web server for some web sites and a RADIUS server to authenticate users in the network.

The communication between clients and server should be always encrypted. Additional information is provided in the appendix.

PART 1

WORK TASK INSTALLATION (LNXRTR1, LNXSRV1, LNXSRV2)

Note: Please use the default configuration if you are not given the details.

The base Debian OS has been set up on lnxrtr1, lnxsrv1 and lnxsrv2.

WORK TASK SERVER LNXRTR1

- Configure the server with the hostname, domain and IP specified in the appendix
  - Install the services:
    - Routing
      - Enable routing
    - Firewall (iptables)
      - Allow the following services to lnxsrv1 from the external network:
        - HTTPS
        - DNS
        - FTPS
        - SMTPS
        - IMAPS
      - Allow RADIUS from DMZ network to internal network.
      - Allow traffic from internal network and DMZ network to external network.
      - Allow traffic from internal network to DMZ
      - Allow the following traffic from external to lnxrtr1
        - OpenVPN
        - Proxy (Nginx)
      - Allow all traffic from internal to lnxrtr1
      - All other traffic should be prohibited.
      - Configure source NAT for internet access from internal network.
      - Static NAT mappings
        - 192.168.10.150 <=> 32.54.87.114
      - DHCP
        - Scope for Internal network:
          Range: 172.17.20.100 – 172.17.20.150
          Netmask: /24
          Gateway: 172.17.20.1
          DNS: 192.168.10.150
        - DNS-Suffix: apps4you.com
        - Lnxclnt2 should always receive the following IP: 172.17.20.95
        - The clients should automatically register their name with the DNS servers after they have been assigned with an IP address by the DHCP server.
    - VPN (OpenVPN)
      - Configure VPN access to Internal network. External clients should connect to 32.54.87.115
      - Make sure that VPN clients can only access server lnxsrv2

  - Use address range 10.2.1.1 to 10.2.1.62 for VPN clients
  - For login create a user “vpn” with password “Skills39”
  - Use a certificate signed by lnxsrv2
- Proxy (Nginx)
  - Configure a reverse SSL proxy for www.apps4you.com website, which is hosted by lnxsrv1
  - For “www. apps4you.com”, HTTP access should be redirected to HTTPS automatically
    - Use a certificate signed by lnxsrv2
      Make sure no certificate warning is shown
    - Use Client-Certificate authentication for www.apps4you.com
      Allow only client certificates, which are signed by lnxsrv2

WORK TASK SERVER LNXSRV1

Note: Please use the default configuration if you are not given the details.

- Configure the server with the hostname, domain and IP specified in the diagrams shown in appendix
- Install the services
  - Configure PAM to authenticate against the radius server on the lnxsrv2
    - Use shared secret “Skills39”
  - Webserver (Apache2)
    - Install apache2 including php5
    - Enable HTTPS
      - Use a certificate signed by lnxsrv2
        - Make sure no certificate warning is shown
  - Create websites “www.apps4you.com” and “intranet.apps4you.com”
  - Make sure “intranet.apps4you.com” is protected by authentication
    - Use radius server to authenticate users
    - Allow users from “user20” to “user39”
    - Configure /webdav for WebDAV
      - Create and use /data/webdav directory
      - “/webdav” directory should be accessible only from the Internal network
    - Show on both websites the website name (the fully qualified domain name) and the current date and time (client time or server time)
    - As a basic security measure, make sure Apache2 doesn´t expose any protocol header and footer information (e.g. version, OS, …).
  - DNS (bind)
    - Make sure both websites are resolvable to 32.54.87.114 (intranet.apps4you.com) and 32.54.87.115 (www.apps4you.com) from the Internet, which has been already mapped to lnxsrv1’s IP address on lnxrtr1.
      - Requests from internal networks (Internal) for both websites should be resolvable to the internal IP addresses of lnxsrv1 and lnxrtr1 instead of 32.54.87.114 / 32.54.87.115
    - Avoid the DNS server from being used as resolver from the Internet for any Internet domain name except for its own. For example, if a client on the Internet queries for the IP of, say, www.google.com, the DNS server will not perform the query for it, but it will for www.apps4you.com.
      - For queries from the internal clients, it will perform regardless of the domain name.

        - Set up DNS firewall to lie using Response Policy Zones (RPZ)
            - Users should not be able to open malicious websites.
            - The user should be redirected to a landing page hosted on lnxsrv1.
                - The landing page should display the following message: *"WARNING: The website you are attempting to visit has been marked as harmful, therefore the access to it has been denied"*
            - Malicious domains:
                - download.malware.com
                - abcd.bad.net
                - dangerous.org
                - site.is.malicious.net
                - virus1.net - virus10.net
- FTP (proftpd)
    - Enable FTPS
        - Use a certificate signed by lnxsrv2
        - Use implicit encryption
    - Create a FTP user account for each website of the webserver
        - User "apps4you" with password "Skills39"
        - User "intranet" with password "Skills39"
    - Make sure the users are jailed in their respective website document root directories.
    - Make sure file transfer to the server is possible.
- Mail
    - You may use any software for the mail server. Functional testing will be applied.
    - Make sure user20 to user30 have access via IMAPS and SMTPS
    - Use certificates signed by lnxsrv2 for SSL/TLS encryption
    - Use Client Certificate Authentication in addition for IMAP and SMTP services
    - Create a mailing list it@apps4you.com
        - user20 to user29 should be in the mailing list
    - user21 is not allowed to send e-mails (via SMTP)
    - Before you finish your project make sure you send an email message from user20 to user30 and another message from user30 to user20. Send also a message from user20 to the mailing list
    - Do not delete these email messages
- Install Fail2ban and configure it to block FTP and HTTP access for 1 minute, after 3 failed login attempts.

WORK TASK SERVER LNXSRV2

Note: Please use the default configuration if you are not given the details.

- Configure the server with the hostname, domain and IP specified in the appendix
- Configure the disk and partitions
    - Add three virtual disks with a size of your choosing.
      If you will be asked about administrator permissions just click 'no' (this will work as expected)
    - Use the three virtual disks to create a software RAID 5.
    - Mount it as /data
- Install the services
    - File sharing (Samba)
        - Share "internal"
            - Path is /data/internal
            - Give access only to users "user1" to "user10"
            - Make sure the share is not shown in the network browser of the clients
        - Share "public"
            - Path is /data/public
            - Enable read-only access to everyone
    - CA (openssl)
        - Configure as CA
        - CA attributes should be set as follows
            - Country code is set to BR
            - Organization is set to Apps4you
        - Create a root CA certificate
        - Store all CA related files in /ca and make sure the CA key is only accessible by root.
          (You are allowed to put everything in /ca or to use subfolders within /ca)
    - RADIUS (freeradius)
        - Create 100 local UNIX users with password "Skills39"
            - Username: user[1-100]
            - These users should not be able to login locally
        - Authenticate users against /etc/passwd file

PART 2

WORK TASK INSTALLATION (LNXCLNT1, LNXCLNT2)

Note: Please use the default configuration if you are not given the details.

WORK TASK LNXCLNT1

Note: Please use the default configuration if you are not given the details.

- Install the base OS and use Gnome for the GUI.
- Configure the client with the hostname, domain and IP specified in the appendix
- Make sure the client can connect to lnxsrv2 (via lnxrtr1) through VPN
- Make sure the root CA certificate of lnxsrv2 is trusted
- Make sure the client certificate is installed
- Install FileZilla FTP client
- Install Icedove mail client
  - Configure mailbox of user20
  - Install Enigmail
  - Create Private/Public keys for encryption with gnupg (RSA 1024)
    - Use Skills39 as passphrase
  - Make sure user20 can send encrypted mails to user30
- Make sure the client can access samba shares.

WORK TASK LNXCLNT2

Note: Please use the default configuration if you are not given the details.

- Install the base OS and use Gnome for the GUI
- Configure the client with the hostname, domain and IP specified in the appendix
- Make sure the root CA certificate of lnxsrv2 is trusted
- Make sure the client certificate is installed
- Install Icedove mail client
  - Configure mailbox of user30
  - Install Enigmail
  - Create Private/Public keys for encryption with gnupg (RSA 1024)
    - Use Skills39 as passphrase
  - Make sure user30 can send encrypted mails to user20
- Make sure the client can access the internal share.
  - Mount the internal SMB share to /mnt/internal on boot using fstab
- Install Cadaver (WebDAV client)

APPENDIX

SPECIFICATIONS

LNXSRV1

IP	192.168.10.150/25 (eth0)
Hostname	lnxsrv1
User name	root
Admin Password	Skills39

LNXSRV2

IP	172.17.20.50/24 (eth0)
Hostname	lnxsrv2
User name	root
Admin Password	Skills39

LNXRTR1

Internal IP	172.17.20.1/24 (eth0)
External IP	32.54.87.115/29 (eth1)
DMZ IP	192.168.10.129/25 (eth2)
VPN network	10.2.1.0/26
Hostname	lnxrtr1
User name	root
Admin Password	Skills39

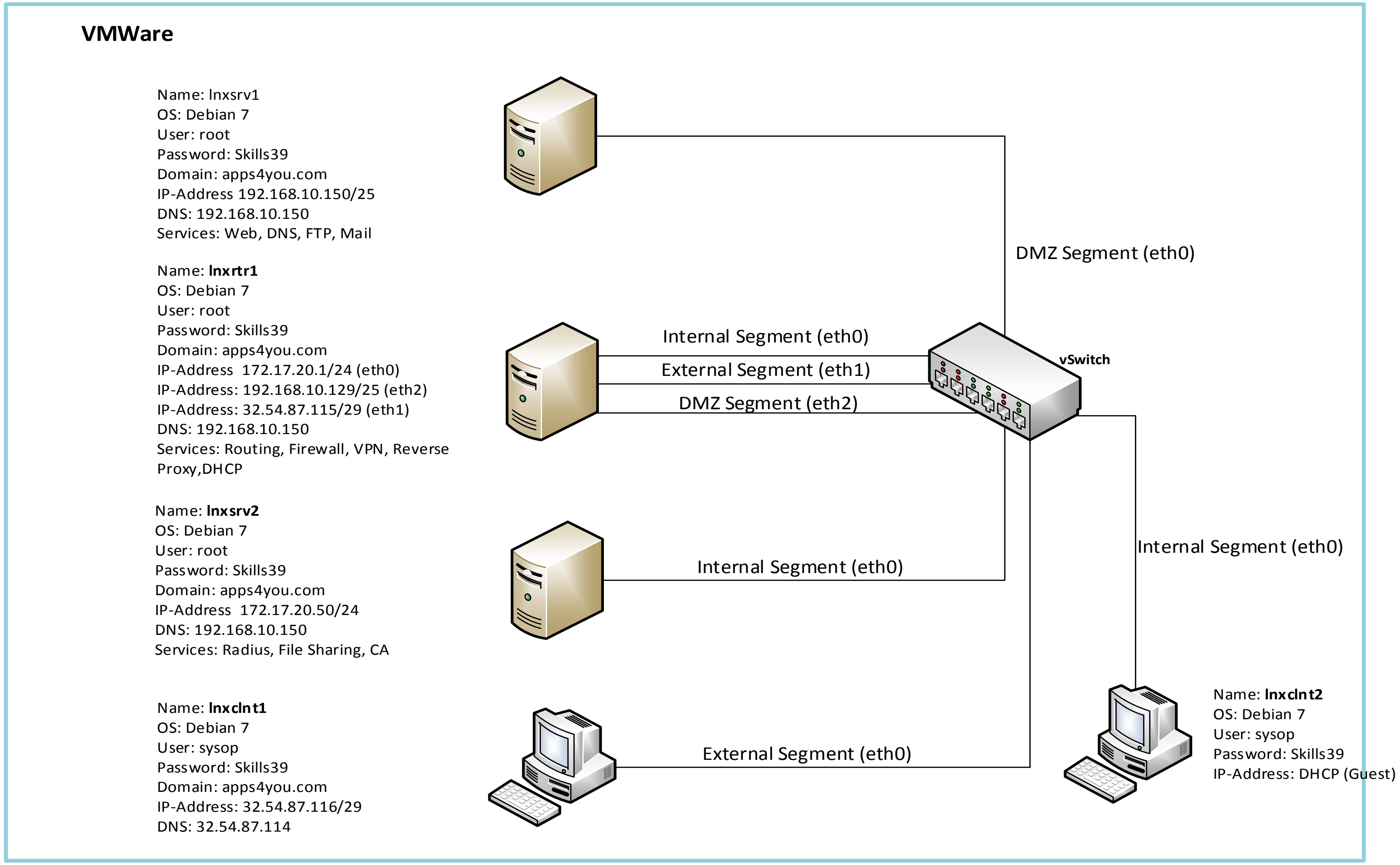
LNXCLNT1

IP	32.54.87.116/29 (eth0)
Hostname	lnxclnt1
User name	sysop
Admin Password	Skills39

LNXCLNT2

Internal IP	DHCP client
Hostname	lnxclnt2
User name	sysop
Admin Password	Skills39

NETWORK SPECIFICATION



Name: lnxsrv1
OS: Debian 7
User: root
Password: Skills39
Domain: apps4you.com
IP-Address 192.168.10.150/25
DNS: 192.168.10.150
Services: Web, DNS, FTP, Mail

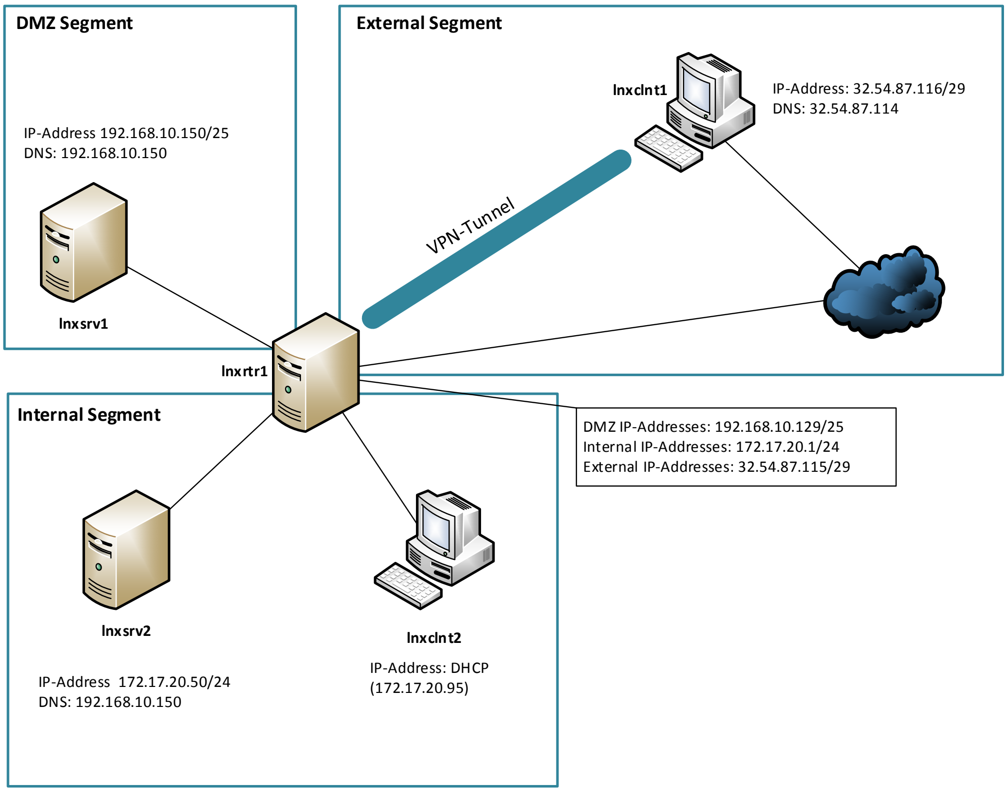
Name: **lnxrtr1**
OS: Debian 7
User: root
Password: Skills39
Domain: apps4you.com
IP-Address 172.17.20.1/24 (eth0)
IP-Address: 192.168.10.129/25 (eth2)
IP-Address: 32.54.87.115/29 (eth1)
DNS: 192.168.10.150
Services: Routing, Firewall, VPN, Reverse Proxy,DHCP

Name: **lnxsrv2**
OS: Debian 7
User: root
Password: Skills39
Domain: apps4you.com
IP-Address 172.17.20.50/24
DNS: 192.168.10.150
Services: Radius, File Sharing, CA

Name: **lnxclnt1**
OS: Debian 7
User: sysop
Password: Skills39
Domain: apps4you.com
IP-Address: 32.54.87.116/29
DNS: 32.54.87.114

Name: **lnxclnt2**
OS: Debian 7
User: sysop
Password: Skills39
IP-Address: DHCP (Guest)

LOGICAL TOPOLOGY DIAGRAM


DMZ Segment
IP-Address 192.168.10.150/25
DNS: 192.168.10.150
lnxsrv1
External Segment
lnxclnt1
IP-Address: 32.54.87.116/29
DNS: 32.54.87.114
VPN-Tunnel
lnxrtr1
Internal Segment
DMZ IP-Addresses: 192.168.10.129/25
Internal IP-Addresses: 172.17.20.1/24
External IP-Addresses: 32.54.87.115/29
lnxsrv2
IP-Address 172.17.20.50/24
DNS: 192.168.10.150
lnxclnt2
IP-Address: DHCP
(172.17.20.95)

INSTRUCTIONS

INSTRUCTIONS TO THE COMPETITOR

- Do not bring any materials with you to the competition.
- Mobile phones and any electric devices are prohibited.
- Do not disclose any competition material / information to any person during each day’s competition.
- Read the whole competition script prior to starting your work.
- Be aware of different tasks attract a percentage of the overall mark. Plan your time carefully.

EQUIPMENT, MACHINERY, INSTALLATIONS AND MATERIALS REQUIRED

LOCAL WORKSTATION:

- VMware workstation and WMware tools preinstalled
- VMs are preconfigured
- lnxrtr1 and lnxsrv1
  - 1x Disk 10GB
  - 1GB RAM
  - 1 CPU core
  - 1 network card
- lnxsrv2
  - 1x Disk 10GB
  - 2x Disk 5GB
  - 1GB RAM
  - 1 CPU core
  - 1 network card
- lnxclnt1 and lnxclnt2
  - 1x Disk 10GB
  - 2GB RAM
  - 1 CPU core
  - 1 network card
- Additional software:
  - Operating System (Debian 7) (DVD1-10)
  - Debian 7 sources (DVD1-8)
  - Divers for peripherals