World Skills Competition

Trade 39:

IT PC and Network Support

Day 4 Competition

- Network Security and Management –

Competitor Name: _____

Country Code: _____

WorldSkills Secretariat
Van Eedenstraat 9, 2012 EL Haarlem, The Netherlands
www.worldskills.org, Tel: +31 23 5311071, Fax:+31 23 5316360

CONTENTS

This Test Project proposal consists of the following documentation/files:

1. TP39_38FI_Day4_EN.doc

INTRODUCTION

You are working as a security specialist for a small company. The company is specialised in DMZ and Firewall solutions. You are employed by a customer to protect his network from any kind of attacks from the internet. A server should be setup with security rules implemented for the company employees. You are to implement the latest wireless technology for the customer. Your job is now to set up the project as written below.

DESCRIPTION OF PROJECT AND TASKS

It is recommended that you read the whole text before you start with your work.

Print the followings:

1. Configuration files for all configured CISCO devices.
2. A copy of the DHCP configured settings from Windows 2003 server.
3. A copy of the security template, trade39 showing ALL the settings configured.
4. A copy of the login_logout.log created under Special customer requirement.
5. A copy of the processes used in the Linux by using ps –ef. Make sure the processes name is visible on the printout.

Write down your station number and the name of the equipment on all printouts and put them in the envelope provided.

COMPANY-SERVER

- Setup the Windows2003 server starting with the pre-installed version. Administrator password is blank.
- The server name is win2003
- Setup the Administrator password as trade39 and change the Administrator name to wsc2005.

- Convert your server to Domain Controller using ADS (**A**ctive **D**irectory **S**ervices)
- Domain name is wsc2005.net
- Install the DHCP server to enable internal clients (wireless clients) to get IP settings.
- Disable the C$ share
- **Reboot the server after you have completed the Windows 2003 server Configuration.**

User accounts

Create the following users and organisation units.

Name	Username	Password	Organisation Unit
Jen Bell	jebe	123456_abcde	CEO
Jens Bielicke	jebi	123456_abcde	CEO
Kelvin Ng	keng	123456_abcde	EXP
Heinz Jakoubek	heja	123456_abcde	EXP
Tony Lee	tole	123456_abcde	ROOT
Raffaele Stefanelli	rast	123456_abcde	ROOT

Organisation Unit

Name: CEO

Name: ROOT Permissions see below

Name: EXP Permissions see below

Security Policies for the ROOT and EXP OU

The users in the EXP OU in the ADS have some policies:

- Set the default homepage (Internet Explorer) to www.wsc2005.net
- The default home page setting should not be changeable

The users in the ROOT OU in the ADS have one policy:

- Cannot modify the taskbar

Security Policies for all 3 OUs

- Configure the proxy settings for Internet Explorer.

Security policies

Create a new security template for the Windows 2003 Server. The name of the template is trade39. Apply this policy to the domain.

- The password cannot be changed before 5 days and is valid for 30 days. It should be in the minimum 6 characters and the last 5 used passwords do not work.
  After 5 incorrect logins the account will be deactivated for 10 minutes.

Special customer requirement

The customer has a special requirement. The requirement is shown below.

- Log all login and logout activities into the file C:\logs\login_logout.log
- The Sharename for (C:\logs) should not be listed in the network browser and the content of this directory should only be listed by the administrator

CLIENT

For testing purpose, the client will have two roles. It should be used firstly as an external client, using the VPN, and secondly as an internal client using the wireless network.
For marking, at the wireless LAN testing, the physical cable connecting to the ISP Router will be disconnected whereas at the VPN testing, experts will deactivate the wireless LAN card.

- Setup Windows XP on PC2 from the preinstalled version
- Over the wireless network, the client should use the ADS for logon purpose
- Administrator password is trade39
- Install and configure the wireless network card
- Create a short cut for the VPN connection on the desktop. The name of the Icon should be VPN.

LINUX SERVER

Use the DELL Power Edge 1800 Server as LINUX Server.

The Linux server is pre-installed. Install all the necessary packages using Debian apt-proxy.

Do NOT repartition the disk.

To access the Debian Installation Server (apt-proxy), set your computer to use the IP address 10.3.X.2/24 with default gateway in 10.3.X.1. Apt Server IP Address is 10.2.1.10:80. X is your workstation number

- Server name is debian
- Root password is **trade39**
- Domain name is **wsc2005.net**
- Install and configure LINUX as authenticated proxy server
- Username and password for the authenticated proxy server
    - Username: **wsc2005** / password: **proxy**
- Install and configure the server as a webserver and stored the content in /var/www directory
- The name of the website is www.wsc2005.net
- Make sure that the web server is secured and authenticated using SSL (HTTPS) with the following username and password.
    - Username: **wsc2005** / password: **web**
- Install and configure DNS service for the Linux Server
- You are to secure the DNS service. The chroot jail is the /var/dns directory.
- Create a simple start page (index) file showing the name of the web server
- The web server should be accessible from both networks (internal / external)
- To enhance security, you are to implement tripwire to detect changes in the file systems. You are to monitor any changes in the website.
- For IDS (Intrusion Detection System), you are to implement SNORT to detect intrusion to your system. As an added security, any ping packets greater than 650 bytes should be detected.

For all CISCO devices set cisco as the enable password. You need to implement local login authentication for all Cisco devices. Username is wsc2005 and Password is trade39

PIX FIREWALL

Use the CISCO PIX 515E Firewall

Do NOT use the PDM (Web Interface) to configure the PIX.

- Configure all the interfaces of the PIX firewall.
- Configure for SSH access only from Linux server.
- Configure NAT to translate all internal IP addresses to DMZ and public IP addresses so as to enable the internal network to access network resources in DMZ and external zone.
- Configure a static NAT to ensure that external clients could access the web server hosted by the Linux machine in the DMZ zone.
- Configure PIX firewall to detect any intrusion and send alarm to Linux syslog server.
- Install the VPN Server
- Enable VPN connection from the external network
- Use Protocol IPSEC/L2TP with CHAP and MS-CHAP for Windows XP clients
- Use pre-shared key for authentication (use the key: **trade39**)
- Username for VPN Login is **admin** / password is **trade39**
- The range of the VPN IP address start 192.168.0.240/28
- Close the following TCP ports (4000 – 5000) for outside interface

ISP ROUTER

Use the Cisco 2600 Router (use the router that stays directly under the PIX Firewall in the rack) The Router should simulate an ISP.

- Enable the HTTP Service on the Router

- Enable the loop back interface to simulate internet use the following address (200.30.10.40/24)
- Implement a time-based ACL to allow internal clients to access Internet during Weekdays 08:00 to 19:00.

INHOUSE LAN-SWITCH

Use the Cisco catalyst 2950 switch (use the switch that stays directly below your ISP Router located in the rack). The switch has to implement the following security feature:

- Configure port security on the first 3 ports as shown in the table below such that when any violation is being detected in these interfaces, it shall result in the ports being shutdown automatically.

Connect and configure the following ports

Port Number	Interface
1	Windows 2003 Server
2	Wireless Access Point
3	PIX Firewall
4	Not shutdown. Access mode
5 -24	All shut down

Network Address

Use the IP addresses given below:

Device	IP Address
Windows 2003 Server	192.168.0.1/24
Wireless access point	192.168.0.10/24
PIX Firewall (internal)	192.168.0.2/24
PIX (DMZ)	200.20.10.2/24
PIX Firewall (outside)	200.10.10.2/24
ISP Router fa0/0	200.10.10.1/24
ISP Router fa0/1	200.30.10.2/24
Windows XP Client	200.30.10.1/24
Linux Server	200.20.10.1/24
LINUX address translation outside interface	200.10.10.10/24

WIRELESS ACCESS POINT

Use the Cisco Aironet 1200 Wireless Access Point. The Wireless Access Point has to be configured as described:

- Configure IP address as given
- Configure WPA authentication with pre-shared key (Trade-39xx) where **xx** represent your station ID
- Configure SSID as **WSC2005xx** where **xx** represent your station ID
- Do not broadcast SSID
- Configure MAC address authentication for the access point. Allow only the MAC address of the wireless card provided.
- Configure the channel number of your wireless LAN access point. The channel numbers of the access point are as follows:

Station ID	Channel
1 /4/7/10/13/16/19	1
2/5/8/11/14/17/20	7
3/6/9/12/15/18	13

PRINTER CONNECTION

- Connect the Printer to the Windows server
- Allow all users to use the Printer.

INSTRUCTIONS TO THE COMPETITOR

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

At the final of day 4, you should create 3 short and simple handwritten activity log documents:

- For Windows 2003 server activities (max 1 page)
- For Linux server activities (max 1 page)
- For Firewall (PIX) activities (max 1 page)

You can decide which tasks to begin with and how many details to include in your log documents.

EQUIPMENT, MACHINERY, INSTALLATIONS AND MATERIALS REQUIRED

You have the following equipment at your disposal:

Software CDs

- Windows 2003 Server with SP1
- Printer driver
- Wireless LAN USB Card
- Cisco Equipment

Hardware

- DMZ (LINUX) Server is DELL Power Edge 1800
- Windows 2003 Server is DELL Optiplex GX280
- Windows XP Client is DELL Optiplex GX280
- 1 Cisco PIX Firewall
- 1 Cisco Router
- 1 Cisco Switch
- 1 Cisco Aironet 1200 Wireless Access Point
- 1 Wireless LAN USB card
- 1 Printer

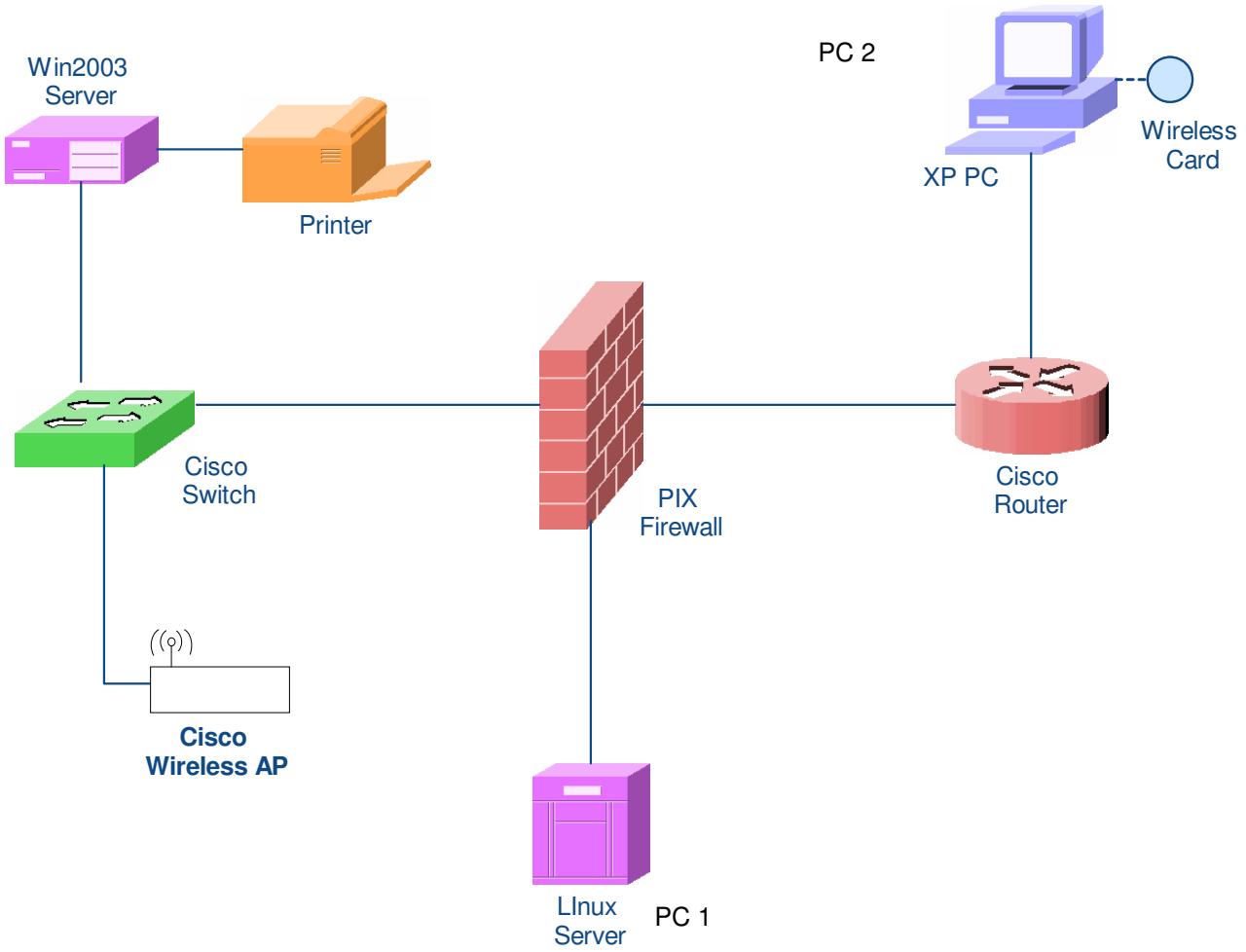
Cable

- USB Printer cable
- 3 crossover cables
- 3 straight through cables
- 2 rollover cables
- 1 RJ45-RS232 adapter

MARKING

Working System	1.6
Microsoft Server	3.0
Windows XP Client	3.2
Linux	6.0
PIX Firewall	6.0
ISP Router	1.0
LAN Switch	1.0
IP Address setup	0.7
WLAN Access Point	2.0
Printer	0.5
Total	25.0

OTHER



WorldSkills Secretariat
Van Eedenstraat 9, 2012 EL Haarlem, The Netherlands
www.worldskills.org, Tel: +31 23 5311071, Fax:+31 23 5316360