**LOMBA KOMPETENSI SISWA**

SEKOLAH MENENGAH KEJURUAN

TINGKAT KABUPATEN KEBUMEN TH 2018

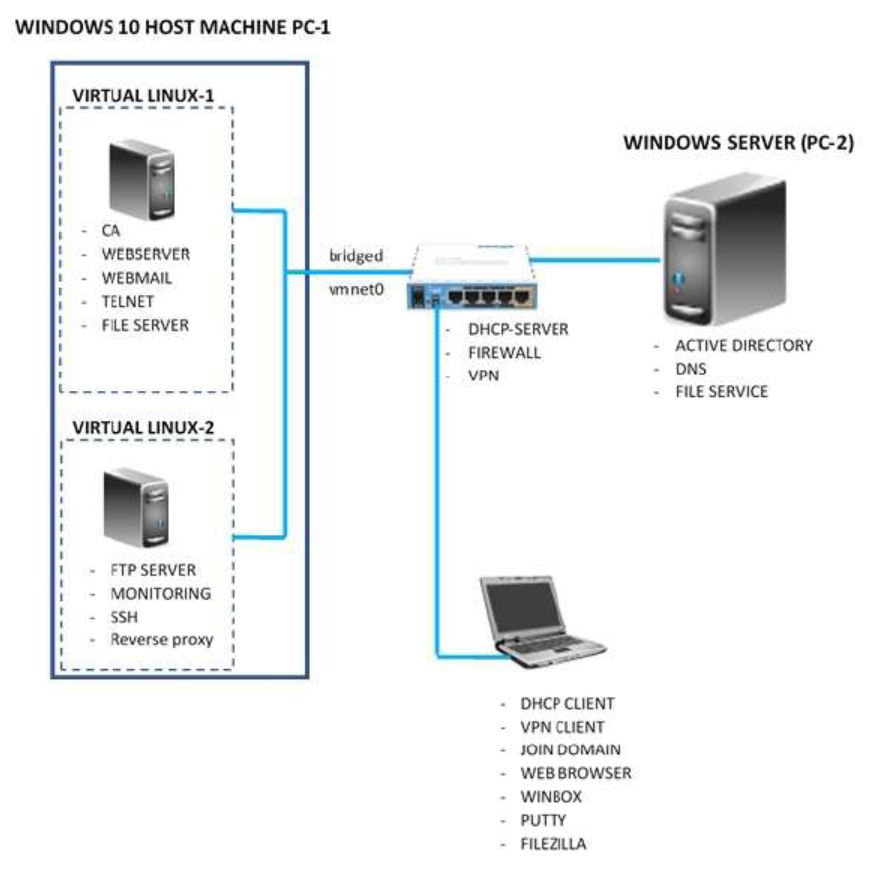


****

**IT NETWORK SYSADMIN**

**Soal Modul I Hari II**

**TOPOLOGI**



**CLIENT**

**RTR-PUSAT**

**Windows Server 2012 R2 (PC-2)**

**WINSRV**

1. Beri alamat IP dengan **IP Host Pertama** dari network **10.10.X.0/30**.

Dimana [X] = No Peserta

1. Aktifkan protocol **icmpv4** **tanpa mematikan** **FIREWALL** agar **WINSRV** bisa diping dari device lain.
2. Install **Active Directory Domain Service** dan **DNS Server** dengan domain **kebumen.net**
3. Konfigurasi **Active Directory User and Computer**

* Buat **Organizational Unit** (**OU**) pada **kebumen.net** dengan nama **kebumen**
* Buat group IT, MKT dan AKUTAN pada **OU** kebumen
* Buat 5 user baru **itX**, 5 user **mktX** dan 5 user **akutanX** dengan password sama yaitu **Kebumen-2018**. **[X] = 1-5**
* Masukkan user itX ke dalam group IT, user mktX ke dalam group MKT dan user akutanX ke dalam group AKUTAN.

1. Konfigurasi **DNS** sebagai berikut :

* Buat **reverse zone** untuk Network seluruh **Network** yang ada.
* Buat subdomain sebagai berikut :

|  |  |  |
| --- | --- | --- |
| **Subdomain** | **Host** | **IP Address** |
| router.kebumen.net | RTR-PUSAT | 10.10.X.Y |
| internal.kebumen.net | LINUX-1 | 20.20.X.Y |
| info.kebumen.net | LINUX-1 | 20.20.X.Y |
| mail.kebumen.net | LINUX-1 | 20.20.X.Y |
| pesan.kebumen.net | LINUX-1 | 20.20.X.Y |
| smb.kebumen.net | LINUX-1 | 20.20.X.Y |
| [ftp.kebumen.net](ftp://ftp.kebumen.net) | LINUX-2 | 30.30.X.Y |
| www.kebumen.net | LINUX-2 | 30.30.X.Y |
| cacti.kebumen.net | LINUX-2 | 30.30.X.Y |

[X] = No Peserta, [Y] = IP Host, pastikan DNS reply from IP yang sesuai

1. Buat folder pada drive **C:\** dengan nama KEBUMEN kemudian buat beberapa folder lagi didalamnya dengan nama : IT, MKT, AKUTAN
2. Lakukan Share folder read/write

* KEBUMEN untuk semuanya
* IT untuk Group IT
* MKT untuk Group MKT
* AKUTAN untuk Group AKUTAN
* Pastikan user yang tidak termasuk kedalam group tidak dapat mengakses

1. Konfigurasi user agar setiap login terdapat drive **Z:** sesuai dengan nama usernya. **Contoh it1 (\\10.10.X.Y\kebumen\IT)(Z:)**
2. Install **DFS (Distributes File System)**

* Buat **DFS Namespace** dengan nama **“anggota”**
* Buat folder baru pada **namespace anggota**

**IT** untuk **\\WINSRV\IT**

**MKT** untuk **\\WINSRV\MKT**

**AKUTAN** untuk **\\WINSRV\AKUTAN**

1. Lakukan konfigurasi Group Policy Management (GPM) agar setiap kali user login terdapat drive **Y:** sesuai namanya usernya. **Contoh it1 (Y:)**

**Mikrotik Routerboard**

**RTR-PUSAT**

1. Ubah identity menjadi **RTR-PUSAT**
2. IP Address

Beri alamat IP dengan **IP Host Terakhir** sesuai dengan networknya, sebagai berikut

|  |  |  |
| --- | --- | --- |
| **Interface** | **IP Network** | **Terkoneksi ke -** |
| Ether1 | 10.10.X.0/30 | WINSRV |
| Ether2 | 20.20.X.0/30 | LINUX-1 |
| Ether2 | 30.30.X.0/30 | LINUX-2 |
| Ether3 | 192.168.X.0/25 | CLIENT (LAPTOP) |

**[X] = No Peserta**

1. DHCP Server

* Buat DHCP Server untuk **CLIENT (Laptop)** sebagai DHCP Client
* Interface DHCP Server adalah interface yang menuju ke **CLIENT (Laptop)**
* Gunakan seluruh IP Host dalam subnet **192.168.X.0/25** sebagai IP DHCP, kecualikan IP interfacenya sendiri
* Pastikan Client mendapatkan IP Address, netmask, gateway dan DNS yang sesuai.

1. Firewall

* Lakukan konfigurasi firewall agar **RTR-PUSAT** tidak dapat di ping dari manapun
* Lakukan konfigurasi firewall agar semua device yang melakukan ping ke **RTR-PUSAT** masuk kedalam **address list** dengan nama “**tukang ping**”

1. VPN Server

* Buat **PPPoE Server** sebagai server VPN untuk **CLIENT (Laptop)**
* Buat **IP Pool** untuk **PPPoE** server dengan nama pool “**pppoe-pool**” **rang IP** = **25.25.25.25** sampai **25.25.25.50**
* Buat user PPPoE dengan nama user “**pesertaX**” password “**kebumen2018”**

**[X] = No Peserta**

* Interface **PPPoE** diarahkan ke interface yang menuju client

**WINDOWS 10 HOST MACHINE PC-1**

**LINUX-1**

1. Beri alamat IP dengan **IP Host pertama** dari network **20.20.X.0/30.**

**[X] = No Peserta**

1. Buat 10 user baru dengan nama **user1** s.d. **user10** password **“kebumen-2018”**

Keterangan : **user1** sampai **user5** tidak memiliki home directory. user lainnya memiliki.

1. Konfigurasi CA (openssl)

* Install Openssl
* Country = ID
* Province = Jawa Tengah
* City = Kebumen
* Organization = lks kebumen
* Buat Root CA
* Simpan certificate di directory **/cert**

1. Web server http dan https (apache2)

* Buatlah secure website **http://info.kebumen.net** dan **http://internal.kebumen.net**
* Isi konten web **http://info.kebumen.net** dengan kode html berikut

**<html>**

**<h1> Welcome to website info kebumen </h1>**

**</html>**

* Isi konten web **http://internal.kebumen.net** dengan kode html berikut

**<html>**

**<h1> Selamat datang di website internal kebumen </h1>**

**</html>**

* Website **http://internal.kebumen.net** hanya dapat diakses dengan **autentikasi** dari **username** dan **password user1 s.d.** **user5**
* Kedua website dapat diakses dari client dengan protocol **HTTPs**, menggunakan Certificate **CA** yang telah dibuat sebelumnya dan tanpa ada peringatan pada web browser client.
* Buat virtual webpages untuk **user6 s.d.** **user10**. **Contoh http://info.kebumen.net/~user6**

1. Mail Server (Postfix dan Courier-imap)

* Install postfix dan courier-imap
* Gunakan domain **mail.kebumen.net** sebagai **system mail name**
* Buat 2 user dengan nama **ani** dan **budi** dengan password **kebumen-2018**
* Pastikan **ani** dan **budi** bisa saling mengirim pesan
* Pesan yang telah terkirim jangan dihapus

1. Web mail (squirrelmail)

* Install squirrelmail
* Gunakan domain **pesan.kebumen.net** untuk mengaksesnya

1. SSH

* Install SSH sebagai pengganti telnet yang tidak ada di debian 8.7
* Ubah nomer port default menjadi 23
* Buat agar user root tidak bisa login
* Buat user baru dengan nama **“akses”** password **“kebumen-2018”**
* Pastikan user akses bisa login dan memiliki hak akses setara dengan root
* Pastikan bisa digunakan sebagai protocol melakukan upload conten dari client

1. File Server (samba)

* Buat file server dengan paket aplikasi **samba**
* Arahkan samba ke folder **/home**
* Hanya ijinkan **user6** sampai **user10** saja yang bisa mengakes samba. User lainnya tidak bisa
* Buat agar user yang login hanya bisa menyimpan file pada foldernya masing-masing

**LINUX-2**

1. Beri alamat IP dengan **IP Host pertama** dari network **30.30.X.0/30. [X] = No Peserta**
2. Buat 5 user baru dengan **adduser** nama **user11** sampai **user15**

password **“kebumen-2018”**

1. FTP Server (proftpd)

* Install Proftpd
* Gunakan domain **ftp.kebumen.net** untuk melakukan akses ftp dari client
* Lakukan konfigurasi secure ftp (**FTPs**) menggunakan **CA** yang ada di **LINUX-1**
* Pastikan jika **user11** sampai **user15** login akan langsung mengarah ke **folder**nya masing-masing
* Pastikan bisa mengupload file dari client ke directorynya menggunakan protocol ftp

1. Monitoring (cacti)

* Install cacti
* Gunakan domain **cacti.kebumen.net** untuk mengaksesnya
* Lakukan konfigurasi untuk memonotoring **RTR-PUSAT**
* Monitoring meliputi : Eternet, Memory, CPU
* Pastikan telah mengaktifkan protocol **snmp** pada **RTR-PUSAT**

1. SSH

* Ubah nomer port default menjadi 2018
* Buat agar user root tidak bisa login
* Buat user baru dengan nama **“remote”** password **“kebumen-2018”**
* Pastikan user akses bisa login dan memiliki hak akses setara dengan root
* Pastikan bisa digunakan sebagai protocol melakukan upload conten dari client

1. Reverse Proxy (nginx)

* Install nginx
* Konfigurasi secure reverse proxy **https://www.kebumen.net**
* Reverse proxy bertugas untuk mengambil konten dari website **info.kebumen.net** dan menampilkannya ke client yang mengakses **https://www.kebumen.net**

**CLIENT**

1. Pengkabelan

* Lakukan pengkabelan (cabling) sesuai gambar topologi, menggunakan kabel yang sudah disiapkan.
* Hubungkan CLIENT dengan RTR-PUSAT, RTR-PUSAT dengan PC1 dan PC2, sesuai gambar topologi.

1. DHCP client

* Lakukan pengaturan network adapter, agar client (laptop) mendapatkan IP DHCP dari RTR-PUSAT
* Pastikan IP yang diterima adalah IP valid yang benar (IP Address, Subnetmask, Gateway dan DNS
* Jika IP telah dianggap benar, cobalah untuk mengakses seluruh device yang ada di jaringan
* Cobalah juga mengakses service-service dari semua server yang telah dibuat
* Lakukan troubleshooting secara mandiri jika ternyata client belum bisa mengakses device dan service yang ada pada jaringan

1. VPN Client

* Lakukan koneksi VPN ke VPN Server (PPPOE) yang telah dibuat di RTR-PUSAT
* Buatlah koneksi baru (broadband connection) agar client bisa melakukan dial-up ke VPN Server
* Pastikan client bisa login ke VPN Server (broadband connection) dengan usename dan password yang telah dibuat di VPN Server
* Pastikan Client mendapat IP dari VPN Server, dan dapat mengakses device serta service yang telah dibuat di jaringan

1. Join Domain

* Lakukan join domain ke ADDS pada WINSRV-A
* Pastikan client bisa login dengan user-user yang telah dibuat di ADDS server

1. Pengujian Service Server dari Client

* Pastikan client bisa mengakses service semua server yang telah dibuat
* Pengujian service dilakukan dengan program aplikasi web browser, putty, winbox, windows explorer, dan program lain yang diperlukan
* Lakukan troubleshooting secara mandiri manakala ada device atau service yang tidak bisa diakses dari client

1. Remote Access (Putty- Winbox)

* Client dapat melakukan remote access dengan menggunakan winbox maupun putty
* Remote access dilakukan untuk melakukan konfigurasi maupun pemeriksaan service sesuai kebutuhan
* Konfigurasi semua perangkat dalam jaringan bisa dilakukan dari client, baik secara GUI maupun CLI

**KETENTUAN KHUSUS**

1. Kerjakan seluruh pekerjaan sesuai dengan prosedur yang benar.
2. Urutan pekerjaan adalah sebagai berikut :
3. Lakukan Instalasi sistem operasi dan program aplikasi yang diperlukan.
4. Lakukan instalasi pengkabelan dan pengaturan mode network adapter pada Vmware (Konfigurasi Layer 1).
5. Lakukan pemberian alamat IP pada semua Server, Client dan Router (Konfigurasi Layer 3). Pastikan Client terkoneksi ke semua Server dan Router. Pastikan Client bisa ping reply ke semua IP Server dan Router, sesuai dengan gambar topologi.
6. Lakukan konfigurasi DNS Server. Pastikan client bisa ping reply ke semua domain dan sub domain yang dibuat, sesuai dengan ketentuan.

*Catatan : urutan pengerjaan di atas (dari point a s.d d) wajib di dahulukan dan merupakan prasyarat bagi konfigurasi selanjutnya (point e s.d f). Jika konfigurasi pada point a s.d d belum dilaksanakan, maka konfigurasi semua service (point e) tidak dianggap dan diberi score nilai 0. Contoh kasus misalnya Anda sudah bisa melakukan konfigurasi web server. Akan tetapi belum melaksanakan urutan pekerjaan point c dan d (IP Address dan DNS). Akibatnya client belum bisa mengakses web server menggunakan web browser. Konfigurasi web server baru bisa diakses dari server itu sendiri. Maka pekerjaan web server tersebut belum bisa dinilai sampai client bisa mengakses service web server tersebut. Dan jika sampai waktu habis client tetap tidak bisa mengakses, maka pekerjaan web server diberi core nilai 0.*

1. Langkah berikutnya adalah melakukan instalasi dan konfigurasi service-service pada semua Server (Konfigurasi Layer 4 - 7).
2. Melakukan pengujian semua konfigurasi dari sisi Client.
3. Anda tidak diperkenankan untuk mengubah topologi, pengkabelan dan Pengalamatan IP (Layer 1 – 3) yang sudah ditentukan. Misal Anda mencolok langsung Client ke Server, tanpa melalui RTR-PUSAT, untuk menguji konfigurasi Web Server maupun service lainnya. Pengubahan topologi dan IP Address akan berakibat pekerjaan Anda tidak diakui, dan diberi score 0.
4. Ketentuan lain yang dianggap belum jelas, bisa ditanyakan kepada dewan juri.

SELAMAT MENGERJAKAN SEMOGA SUKSES