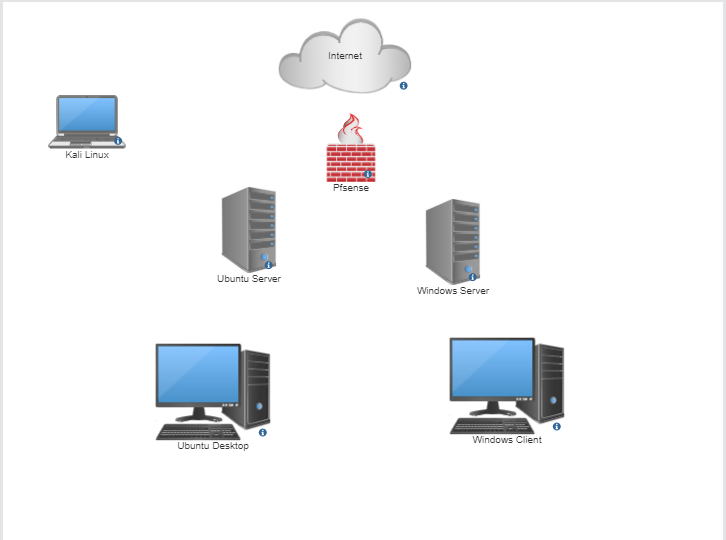
PROJETO UFCD 9189

1. Objetivos do projeto:
   1. Projetar e aplicar todos os conhecimentos adquiridos ao nível de redes e segurança;
   2. Projetar e aplicar todos os conhecimentos adquiridos ao nível de sistemas Linux e Microsoft, Kali entre outros.
2. Topologia de Rede:

No que concerne à parte de servidores e serviços pede-se que sejam instalados e configurados de acordo com o seguinte diagrama:



**Endereçamento:**

**Domínio:** ciseg.pt

**Rede Lisboa**: 192.168.10.0/24

Ubuntu Server:192.168.10.2 (5-10)

Windows Server Desktop: 192.168.10.1(5-10)

Windows Client e Ubuntu Client: DHCP

PfSense Lisboa: 192.168.10.254

1. Considerações iniciais e instruções:
   1. Cada aluno projeta e configura a topologia apresentada de acordo com as diretrizes definidas nos pontos seguintes.
   2. Qualquer situação omissa que não tenha sido mencionada neste enunciado, deve ser colocada ao formador, para posteriormente ser esclarecida/comunicada a todos os alunos.
   3. As tecnologias/diretrizes mencionadas neste enunciado são de implementação obrigatória, no entanto poderão ser implementadas mais tecnologias ou melhorias por forma a valorizar o trabalho. Melhorias essas que devem ser refletidas na apresentação e devidamente fundamentadas.
   4. Deve ser efetuada no final uma apresentação de **15** minutos sobre o trabalho efetuado.
      1. O formador irá solicitar/formular questões sobre o trabalho aos formandos.
2. **Serviços abordados**
3. DNS
4. DHCP
5. Postfix
6. Squid Proxy
7. Cockpit
8. Apache
9. IIS

**DHCP E DNS**

**Ações a desenvolver:**

Instalar e configurar o servidor de DHCP E DNS na máquina de Ubuntu Server Lisboa e Windows Server Lisboa.

Serviço ativo e bem configurado.

Estes dois serviços é para estarem obrigatoriamente a trabalhar nas duas máquinas e caso uma vá abaixo por qualquer motivo é a outra que fornece os serviços (failover).

Deve ser feito um script conforme feito em aula para confirmar que estão ambas a trabalhar em failover. Esse script deve ser configurado para passar a ser um serviço da máquina.

Criar registos de DNS para os diferentes serviços.

**POSTFIX**

**Ações a desenvolver aquando da instalação deste serviço:**

Criar uma conta de email para cada utilizador e também para o Administrator.

Serviço ativo e pronto a fazer troca de emails entre utilizadores.

**SSH**

**Ações a desenvolver aquando da instalação deste serviço:**

Aceder de uma forma segura de uma máquina para outra

Serviço ativo e configurado

Instalar o PUTTY/MobaXterm em todas as máquinas Windows

Mudar a porta do SSH.

**APACHE**

**Ações a desenvolver aquando da instalação deste serviço:**

Importar um site com uma imagem acerca de cibersegurança e o título deve ser “Projeto Final CISEG”

Serviço ativo e bem configurado.

Mudar a porta do apache para uma à vossa escolha.

**IIS**

**Ações a desenvolver aquando da instalação deste serviço:**

O site do IIS deve ser uma réplica do site do Apache

Serviço ativo e bem configurado.

**PfSense**

**Ações a desenvolver aquando da configuração destas máquinas:**

Devem ser configuradas de maneira a aceder com o Administrator do Windows Server.

Os acessos terão que ser feitos obrigatoriamente por HTTPS, através da criação de um certificado.

As regras na Firewall devem estar de acordo às feitas em aula.

**Nessus no Kali**

**Ações a desenvolver aquando da configuração destas máquinas**

Utilizar o Serviço Nessus, no vosso kali e tentar enumerar as vulnerabilidades da vossa rede. Deve gerar um relatório com todos os dispositivos na rede e as suas vulnerabilidades.

Utilizar o nmap para verificar quais os hosts que aparecem no varrimento à rede LAN

Utilizador o OpenVas para identificar as vulnerabilidades da rede LAN.

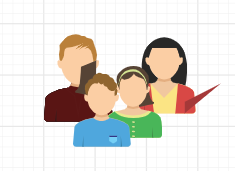
**SQUID PROXY:**

**Ações a desenvolver aquando da instalação deste serviço:**

O Squid e o Squid Guard devem estar instalados na PfSense de Lisboa.

Os **sites bloqueados** são: Citeforma.pt, abola.pt, linkedin.com, Facebook.com, policiajudiciaria.pt, record.pt.

Deve importar uma blacklist conforme feito em aula e mostrar a bloquear os sites definidos nessa blacklist.



**Utilizadores:**

-Maria

-Iolanda

-Vitor

-Alexandra

-Francisco

**Organizational Units (OU’s)**

Mulheres (Maria, Iolanda e Alexandra)

Homens (Vitor e Francisco)

**GPO’S**

Bloquear o MSPaint e a Calculadora **(Mulheres**)

Bloquear CMD **(Mulheres)**

Bloquear Gestor de Tarefas **( Mulheres)**

Remover possibilidade Logoff **( Mulheres)**

Bloquear Painel de Controlo **(Mulheres)**

Bloquear a barra de Tarefas **(Mulheres)**

Permitir a instalação de programas somente com privilégios de administrador **(Mulheres)**

Não permitir a instalação dos updates **(Mulheres)**

Não permitir a alteração das configurações de rede **(Mulheres)**

Remover o executar do menu Iniciar **(Mulheres)**

Bloquear USB com mensagem para o utilizador **(Mulheres)**

Esconder um disco **(Homens)**

Mostrar título ao fazer login **(Mulheres e Homens)**

Remover todos os ícones do Desktop**(Mulheres e Homens)**

Mostrar mensagem de texto ao fazer login **(Mulheres e Homens)**

Iniciar um script quando o PC iniciar **(Homens)**

Iniciar um programa quando um utilizador faz login **(Mulheres e Homens)**

Pedir a password quando retorna da suspensão **(Mulheres e Homens)**

Mudar o wallpaper para uma imagem ligada a hacking **(Mulheres e Homens)**

Desabilitar o uso da camera (**Mulheres**)

Não permitir que as passwords sejam guardadas (**Mulheres e Homens**)

Desligar as aplicações da Store **(Mulheres e Homens)**

Remover a possibilidade de mudar a password **(Mulheres e Homens)**

**NOTAS:**

Todas as máquinas devem estar no domínio inclusive a Pfsense.

Os utilizadores são criados no Windows Server.

Todos os serviços devem ser acedidos pelo nome do domínio e não por IP’s.

Todos os clientes e servidores só devem ter uma placa LAN.

As versões do Ubuntu Server e dos Client deve ser a versão 21.04.

As versões dos Windows Server devem ser a 2022.

As versões dos Windows Client devem ser a 10 pro.

1. Cotações:

|  |  |
| --- | --- |
| ***Tarefa*** | ***Valorização*** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| Melhorias/Tecnologias extra |  |
| Relatório |  |
| Total | 20,00 Valores |

1. Data de Entrega:
   1. Até ao dia xxxxx.