Projeto

- Administração de Sistemas Virtuais (ASV)
- Serviços de Rede Seguros (SRS)
- Cibersegurança Ativa (CA)

1º Semestre / 2º ano

POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

1. Informações Gerais

Descrição

Este projeto tem como objetivo a implementação de diferentes sistemas de virtualização, criando ambientes de serviços virtuais que demonstrem as capacidades, segurança e robustez dos mesmos. Cada grupo deverá definir os requisitos do trabalho, idealizando uma entidade fictícia e as suas necessidades tecnológicas, de modo a guiar a implementação.

2. Expectativas e Objetivos

A implementação do trabalho deve cumprir os seguintes objetivos gerais:

UC	Objetivos
ASV	• Implementar uma infraestrutura virtualizada recorrendo a hipervisores (*hypervisores*) do tipo 1 e do tipo 2, para garantir uma solução de alta disponibilidade. • Adicionalmente, a solução deve incluir 2 tipos de sistemas operativos diferentes para as máquinas virtuais (*VMs*). • Deve incluir também (mínimo) 1 *storage* partilhado.
SRS	• Instalação e Configuração de Serviços de rede de forma segura e robusta; • Interligação dos diferentes serviços de rede;
CA	• Desenvolvimento de um pedido de autorização para realização de um *pentest* (*pentest request*); • Realização de um relatório de *footprinting* a um domínio à vossa escolha; • Realização de um relatório de penetração à solução implementada nas outras duas UC's.

3. Grupos de estudantes

Os grupos de trabalho serão constituídos preferencialmente por **3 elementos**. Um número diferente de elementos deve ser solicitado com justificação. A inscrição no grupo deve ser realizada até à data exigida pelo docente responsável no moodle em cada respetiva página da UC.

4. Avaliação de ASV

Cada grupo deverá submeter as seguintes entregas como parte da avaliação do projeto:

- **Entrega1** (20%) : Relatório inicial com o planeamento
- **Entrega2** (80%) : Relatório Final + Apresentação do funcionamento da solução

Nota Final = 20% x **Entrega1** + 80% x **Entrega2** [65%Implementação+15%Apresentação] x Defesa

Entrega 1 (ASV):

Na entrega 1 (**Planeamento**) devem escrever um **documento PDF** que inclua:

- A apresentação do caso de estudo, indicando e caracterizando a entidade fictícia;
- Descrição dos pressupostos e desenho da solução de rede, bem como o endereçamento IP e servidores DHCP;
- Planeamento que inclua o hardware e a sua ligação (EX: incluir *storage* partilhado com rede dedicada iSCSI; rede de gestão; firewall externa; servidor de backup NFS; dimensionamento do hardware; redundância; ligação à Internet; DMZ);
- Realização de diagrama lógico com VMs e *switches* virtuais, mas ainda sem os *hosts* alojados nos *hipervisores*;
- Documento inicial de modo a obter o feedback do docente antes da implementação final.

Entrega 2 (ASV):

Na entrega 2 (**Relatório Final + Apresentação da solução**) devem entregar um **documento PDF** que inclua:

- Planeamento com dimensionamento das VM; qual a ordem pela qual as máquinas físicas e VMs devem ser ligadas e desligadas; permissões;
- Implementação com o detalhe dos *hosts* alojados no *VMware Workstation* ou *VirtualBox*; este planeamento pode ser modificado (justificando) para permitir a implementação face aos recursos de hardware ou licenças disponíveis e outras limitações; descrever o hardware físico disponível utilizado; a parte da implementação não exequível por limitação de hardware, deve ser apresentada sob a forma de como seria realizada; apresentação dos serviços e as respetivas informações.

As entregas são efetuadas em formato digital, descrevendo cenários de virtualização, explicação da implementação e testes realizados que comprovem o correto funcionamento.

A **apresentação** final deve ser realizada pelo grupo durante **15 minutos**. Sugere-se uma breve apresentação do projeto seguida da **demonstração do funcionamento da solução**. Ter vídeos e/ou imagens da solução em funcionamento pode ser muito útil no caso de algum imprevisto acontecer no dia da apresentação. Depois da apresentação haverá uma **discussão**, também para avaliação dos conhecimentos de cada estudante sobre o trabalho apresentado.

Nota: Outras considerações

Serão valorizados todos os mecanismos abordados relacionados com os sistemas de virtualização, além da implementação dos hipervisores e VMs. Exemplos:

- Agentes do *hypervisor* nas VM (VMware Tools e equivalentes)
- *Snapshots*
- Clonagem; *templates* de VMs
- Migração (*cold* ou live); *cluster* ou *pool* de *hosts*
- Arranque automático de VMs
- Simular necessidade de aumentar a *storage* em determinado momento (disco de VM e dataStores do host)
- *Port forwarding*
- Sincronização da hora da VM pelo *host*; sincronização da hora do *host*
    - Configurações de rede (segurança, reserva/limites de largura de banda, VLANs)
    - DHCP por MAC;
    - NIC *teaming*; *load balancing*; *failover*; *Network failure detection method*
- Reserva de recursos por VM (reserva, limite, *shares*)
- Conversão P2V
- *Upgrade* (ou *downgrade*) do hardware de uma VM
- ISO *libraries*
- vApp (Citrix)
- RAID
- *Storage* partilhada
- Monitorização
- *Users* e permissões

5. Avaliação de SRS

Cada grupo deverá submeter as seguintes entregas como parte da avaliação do projeto:

- **Entrega 1** (05%) : Planeamento
- **Entrega 2** (15%) : Relatório Intermédio + Apresentação
- **Entrega 3** (40%) : Relatório Final + Apresentação

Nota Final = Entrega 1(05%) + (Entrega 2 * Apresentação) (15%) + (Entrega 3* Apresentação) (40%)

Entrega 1 (SRS):

Na entrega 1 devem escrever um **documento PDF** que inclua:

- Apresentação do caso de estudo: uma empresa, indústria, escola.... e os respetivos intervenientes: clientes, utilizadores, redes, servidores e serviços;
- Apresentação dos serviços que irão instalar e configurar no cenário;
- Apresentação de um possível desenho da solução;
- Apresentação das opções de segurança que irão permitir aumentar a segurança dos serviços;
- Apresentação de como irá ser realizada a gestão, manutenção e administração dos serviços e dos sistemas operativos;

Entrega 2 (SRS):

Na entrega 2 devem entregar um **documento PDF** que inclua:

- Apresentação de todos os serviços instalados e configurados em cada máquina.
- Explicação dos objetivos de cada serviço no cenário.
- Apresentação do cenário de teste utilizado, identificando claramente, como as máquinas estão interligadas, quais os serviços configurados em cada uma, e quais os utilizadores.
- Apresentação e explicação de todas as configurações realizadas nos respetivos serviços;
- Apresentação de testes que realizaram para demonstrar a respetiva configuração e o bom funcionamento de cada serviço.

Devem **implementar** um **cenário de teste**, no qual devem:

- Utilizar pelo menos uma máquina virtual por cada estudante e distribuir os vários serviços.
- Instalar e configurar serviços abordados durante as aulas e outros que sejam relevantes;
- Configurar o serviço de nomes para o cenário implementado;
- Configurar o serviço web para o cenário implementado;
- Optar por configurações seguras - mais valorizadas (serviços, acessos e configurações);
- Automatizar tarefas sempre que possível;
- Configurar e utilizar acessos remotos seguros à linha de comandos das máquinas;
- Configurar e conhecer os registos de eventos(*logs*) dos serviços;
- Entregar os ficheiros de configuração de cada serviço;

A **apresentação** deve ser realizada pelo grupo durante **15 minutos**. Sugere-se uma breve apresentação do projeto seguida da **demonstração do funcionamento do sistema**. Ter vídeos e/ou imagens da solução em funcionamento pode ser muito útil no caso de algum imprevisto acontecer no dia da apresentação. Depois da apresentação haverá uma **discussão**, também para avaliação dos conhecimentos de cada estudante sobre o trabalho apresentado.

Entrega 3 (SRS):

Na entrega 3 devem entregar um **documento PDF** que inclua:

- Apresentação de todos os serviços instalados e configurados em cada máquina.
- Explicação dos objetivos de cada serviço no cenário.
- Apresentação do cenário de teste utilizado, identificando claramente, como as máquinas estão interligadas, quais os serviços configurados em cada uma, e quais os utilizadores.
- Apresentação e explicação de todas as configurações realizadas nos respetivos serviços;
- Apresentação de testes que realizaram para demonstrar a respetiva configuração e o bom funcionamento de cada serviço.

Devem implementar um cenário de teste, no qual devem:

- Utilizar pelo menos uma máquina virtual por cada estudante e distribuir os vários serviços.
- Instalar e configurar serviços abordados durante as aulas e outros que sejam relevantes;
- Configurar o serviço de nomes para o cenário implementado;
- Configurar o serviço web para o cenário implementado;
- Configurar o serviço de email para o cenário implementado;
- Configurar o serviço de monitorização para o cenário implementado;
- Integração de autenticação nos vários serviços;
- Optar por configurações seguras - mais valorizadas (serviços, acessos e configurações);
- Automatizar tarefas sempre que possível;
- Configurar e utilizar acessos remotos seguros à linha de comandos das máquinas;
- Configurar e conhecer os registos de eventos(*logs*) dos serviços;
- Entregar os ficheiros de configuração de cada serviço;

A **apresentação** deve ser realizada pelo grupo durante **15 minutos**. Sugere-se uma breve apresentação do projeto seguida da **demonstração do funcionamento do sistema**. Ter vídeos e/ou imagens da solução em funcionamento pode ser muito útil no caso de algum imprevisto acontecer no dia da apresentação. Depois da apresentação haverá uma **discussão**, também para avaliação dos conhecimentos de cada estudante sobre o trabalho apresentado.

Entregáveis (SRS):

Entrega 1: relatório (ficheiro PDF)

Entrega 2: relatório (ficheiro PDF) + ficheiros de configuração (ficheiro ZIP)

Entrega 3: relatório (ficheiro PDF) + ficheiros de configuração (ficheiro ZIP)

6. Avaliação de CA

Entrega 1 (CA):

Na entrega 1 (**Planeamento**) devem escrever um **documento PDF** que inclua:

- Desenvolvimento de um pedido de autorização para realização de um *pentest (pentest request*);
- Realização de um relatório de *footprinting* a um domínio a vossa escolha;
- Realização de um relatório de penetração à solução implementada nas outras duas UC's.

Entrega 2 (CA):

Na entrega 2 (**Relatório Intermédio + Apresentação**) devem entregar um **documento PDF** do *footprinting* realizado, com a seguinte estrutura:

- Quadro recapitulativo de informação
- Informação de DNS e IP
- Informação Plataformas
- Informação Utilizadores
- Informação Histórica
- Informação Soluções utilizadas
- Informação Diversa relevante

As entregas são efetuadas em formato digital, através do moodle.

A **apresentação** deve ser realizada pelo grupo durante **15 minutos**. Sugere-se uma breve apresentação do projeto seguida da **demonstração do funcionamento do sistema**. Ter vídeos e/ou imagens da solução em funcionamento pode ser muito útil no caso de algum imprevisto acontecer no dia da apresentação. Depois da apresentação haverá uma **discussão**, também para avaliação dos conhecimentos de cada estudante sobre o trabalho apresentado.

Entrega 3 (CA):

Na entrega 3 (**Relatório Final + Apresentação**) devem entregar um **documento PDF** do *footprinting* realizado, com a seguinte estrutura:

- Quadro recapitulativo de informação
- Informação de acesso
- Informação de plataformas
- Informação de vulnerabilidades
- Informação de testes de vulnerabilidades
- Informação Diversa relevante

As entregas são efetuadas em formato digital, através do moodle. As máquinas virtuais não são entregues, podendo, no entanto, ser posteriormente solicitadas pelo docente a algum dos grupos.

A **apresentação** deve ser realizada pelo grupo durante **15 minutos**. Sugere-se uma breve apresentação do projeto seguida da **demonstração do funcionamento do sistema**. Ter vídeos e/ou imagens da solução em funcionamento pode ser muito útil no caso de algum imprevisto acontecer no dia da apresentação. Depois da apresentação haverá uma **discussão**, também para avaliação dos conhecimentos de cada estudante sobre o trabalho apresentado.

A avaliação incide sobre os seguintes componentes sendo os dois últimos avaliados de forma individual:

- Planeamento (entrega do *Pentest request*)
- 2º entrega (entrega do relatório de *footprinting*)
- Relatório Final
- Apresentação
- Defesa: em percentagem

Nota final: (20% * 1ºentrtega + 20% * 2ºentrega + 60%*relatório final) * defesa

7. Estrutura do Relatório

Os relatórios deve seguir uma estrutura adequada, no mínimo com:

- Capa (logotipo ESTG, curso, UC, data, grupo, nomes e números)
- Introdução
- Conceitos
- Planeamento
- Desenvolvimento
- Testes e Resultados
- Conclusão (incluir principais dificuldades e conquistas)

8. Software de desenho (cenários, esquemas, …)

Algumas sugestões de software para desenhar os diagramas:

- Draw.io: https://app.diagrams.net/;
- Cisco Packet Tracer;
- Network Notepad Freeware Edition