→ O que é uma máquina virtual?

Uma máquina virtual é um ambiente virtual que funciona como um computador físico (tem cpu, memória, interface de rede e armaterenamento). O sistema virtual é criado a partir de um sistema de hardware físico. Um software chamado hypervisor separa do hardware os recursos utilizados pela máquina virtual e os provisiona adequadamente.

A máquina física, onde o hypervisor está instalado é chamada de host. O uso das máquinas virtuais permite a adoção de sistemas operacionais distintos executados simultaneamente num único computador. Cada sistema operacional é executado normalmente da mesma maneira como seria no hardware host.

• Como funcionam?

Através da virtualização que permite partilhar um sistema com vários ambientes virtuais. O hypervisor gere o hardware e separa os recursos físicos dos ambientes virtuais. Os recursos são parcionados, consoante o que se pretende, a partir do ambiente físico para as VMs.

→ Quais as vantagens das VMs?

- Mais conveniente e barato ter VMs do que comprar outro pc.
- Uso de vários VMs p/ diferentes propósitos, testes, etc
- Caso o pc crashe, é possível aceder à VM noutra máquina
- É mais seguro devido às partições e serviços isolados. Se uma VM crasha, as outras não são afetadas nem o pc em si.

→ Porque se usa o Debian como sistema operativo em vez do Rocky? Quais as diferenças entre eles?

Debian é um servidor mais antigo que o Rocky por isso pode ser mais fácil pedir apoio à comunidade na resolução de problemas.

A disponibilidade vasta de pacotes permite instalar facilmente e configurar váeias aplicações e serviços sem problemas para quem é novo em administração de sistemas. O pacote (APT) facilita as instalações.

Além disso, o sistema Debian parece ser mais intuitivo tornando-se mais "user-friendly".

→ O que é AppArmor e para que serve?

AppArmor é um módulo de segurança e um sistema de controlo de acesso obrigatório (MAC). É utilizado para restringir as capacidades de aplicações individuais e processos.

Na prática, o kernel do Linux consulta o AppArmor antes de cada chamada do sistema para saber se o processo está autorizado a fazer a operação dada.

No fundo, o AppArmor providencia uma camada adicional de segurança além das permissões do Linux, o que previne ações não autorizadas, limita o impacto de breaches.

→ O que são apt e aptitude e quais as diferenças?

Ambos são ferramentas de gestão de pacotes. APT (Advanced Package Tool)

O comando apt é uma interface de linha de comandos de alto nível para gestão de pacotes. Originalmente foi destinada para ser uma interface de utilizador final e ativa por definição.

O comando aptitude é a ferramenta de gestão de pacotes baseada no APT mais versátil.

Diferenças:

→ APT tem uma interface c/ linha de comandos
Aptitude tem uma interface interativa c/ texto.

→ Aptitude oferece uma experiência mais interativa

→ Aptitude é considerada mais robusta em resolver conflitos

→ Aptitude tende a ter recursos mais conservativos no que toca a ações em pacotes.
APT tem sugestões de abordagens mais diretas.

→ O que é o serviço SSH e como funciona?

SSH (Secure Shell) é um protocolo de rede que permite ter um acesso remoto seguro e comunicações seguras entre computadores usando uma rede não segura. Permite uma entrada segura para fazer login num sistema remoto, executar comandos, transferir ficheiros e gerir serviços de rede.

SSH usa encriptação para assegurar a comunicação entre cliente e servidor.

→ O que é uma firewall? Porque se usa UFW?

Firewall é um software de segurança de rede que controla o tráfego da rede c/ base em regras de segurança pré-determinadas. O principal propósito é proteger a rede ou o computador de acesso não autorizado, ataques maliciosos ou comunicações de rede indesejados.

UFW (Uncomplicated Firewall) é uma interface de linha de comandos "user-friendly" que gere regras de firewall em distribuições Linux. É usado p/ simplificar o processo de configuração e gestão de definições de firewall.

→ Porque se usa uma política de palavra-passe forte?

Usar esta política é crucial p/ manter a segurança de sistemas digitais, redes e contas elevada. As razões prendem-se com:

- Acesso não autorizado
- Proteger dados pessoais e/ou financeiros
- Reduz risco de ataques de força bruta, entre outras

Esta política deve incluir guias p/ palavras-passe fortes, expiração de password regulares, implementação de autenticação multi-fator e práticas de armazenamento de palavras-passe.

→ O que é o sudo? para que serve e porque tem regras restritas?

sudo ("superuser do") é um programa de linha de comando que permite a utilizadores autorizados executar comandos c/ privilégios elevados ou como outro utilizador, normalmente o user root. É uma forma de realizar tarefas administrativas enquanto se usa um ambiente seguro e controlado.

Tem regras restritas de maneira a minimizar os riscos de danos ao sistema.

→ O que é o root user?

Root user é um utilizador administrativo especial que tem todos os privilégios e acesso sem restrições no sistema inteiro.

→ O que é o script e qual a informação presente?

O script monitoring.sh é normalmente pedido para medir a "saúde" do sistema e reunir informação importante acerca dos recursos e do estado do sistema. Dentro do script temos:

- CPU usage: script pode usar comandos "top" ou "ps" p/ receber informação sobre o uso do CPU.
- Memory usage: informação sobre utilização da memória
- Disk Usage: comandos "df" ou "du" p/ determinar o espaço usado do disco.
- Network Statistics: informação relacionados à rede
- System Uptime: indicar há quanto tempo o sistema corre desde a última reiniciação.
- System Health Checks: verifica se SSH, Apache ou MySQL estão ativos.

→ O que é o cron?

É um relógio que permite aos utilizadores programar e automar a execução de comandos ou scripts a intervalos de tempo específicos.

→ O que são partições?

Partições são divisões lógicas de um dispositivo de armazenamento físico. Quando se usa partições, divide-se o disco em secções geridas individualmente e usadas em separado.

→ O que é LVM e para que serve?

LVM (Logical Volume Manager) é uma camada de software que permite uma abordagem flexível e dinâmica p/ gerir armazenamento. LVM permite criar volumes lógicos (parecidos a partições) que abrangem vários discos físicos e tem caracteríticas como redimensionar tamanho, snapshots e gestão de volumes

→ O que são os serviços lighttp, MariaDB e php?

- Lighttp: ~~software~~ web server software leve conhecido por ter uma marca de memória baixa e é eficiente ao gerir high loads. É desenhado para ser rápido, seguro e flexível sendo apto p/ servir conteúdo da web estático e dinâmico.

- MariaDB: ~~sistema de armazenamento~~ sistema open-source de gestão de dados relacionais e um substituto do mySQL.

- PHP: (Hypertext Preprocessor) é um script de linguagem desenhado p/ Web. Foi criado p/ criar páginas web dinâmicas e interativas ao incluir código PHP c/ HTML.

- Quando são usados os 3 juntos formam um stack que tem uma base sólida e eficiente p/ criar websites, permitindo o processo de conteúdo dinâmico, armazenamento de dados e mostrar páginas web a clientes.