AVALIAÇÃO Born2BeRoot

1. Arquivo: *signature.txt* no repositório.
2. Como localizar código *.vdi*:
3. Pedir para duplicar VM para manter código.

VISÃO GERAL DO PROJETO

4. Explicar os seguintes:
    a. Como funciona uma máquina virtual:
        i. VM é um ambiente virtualizado, é um sistema com sua própria CPU, memória, interface de rede e armazenamento. Ou seja, é um outro computador que você pode usar através do seu computador de forma isolada, assim sem interferir no seu hardware físico. Pois o hardware que a VM é de responsabilidade do provedor da VM.
    b. Qual sistema operacional eu escolhi:
        i. Debian
    c. Diferenças básicas entre CentOS e Debian:
        i. O CentOS é voltado para empreendimentos e por causa das exigências de segurança e estabilidade para empresas, a sua atualização é muito mais complicada. CentOS já está quase fora de uso. O Debian é o OS mais velho e robusto do Linux, então ele tem muito mais suporte e pacotes de arquitetura. É fácil de atualizar e é usado tanto para trabalho quanto para uso pessoal.
    d. Objetivo das máquinas virtuais:
        i. O objetivo principal é a segurança e praticidade para testar, criar, instalar todo tipo de coisa sem danificar seu computador físico, já que que VM usam um sistema de nuvem.
    e. Diferença entre **aptitude** e **apt**:
        i. Ambos são gerenciadores de pacotes, usados para instalar, atualizar e deletar programas. A diferença é que o Aptitude é um gerenciador de alto nível, e possui sua própria interface, é mais user friendly e possui mais possibilidade e ferramentas para gerenciamento.
    f. O que é APPArmor:
        i. É um sistema de Controle de Acesso Mandatório (MAC). Ele é consultado toda vez que há uma chamada do sistema para saber se você tem autorização para executar tal comando. Isso deixa o uso de comandos mais seguro, já que com ele você limitar e decidir acesso e autorização.

CONFIGURAÇÃO SIMPLES

5. Senhas para login:
    a. Encriptada: **Born2BeRoot!42alien.7**
    b. ewolfghe: **Born2GoHorse!37**
    c. root: **Weirdo!2421**

6. Checar OS: ***cat /etc/os-release*** ou ***hostnamectl***
7. Checar partições: ***lsblk***
8. Checar UFW iniciado: ***sudo service ufw status***
9. Checar UFW ports: ***sudo ufw status***
10. Checar SSH iniciado: ***sudo service ssh status***
11. Checar APPArmor: ***sudo aa-status***

DO UTILIZADOR

12. Checar se pertence groups: ***groups <username>***
13. Checar users de group: ***getent group <groupname>***

14. Criar novo usuário, grupo e atribuir grupo:
    a. ***sudo adduser <username>***
    b. ***sudo addgroup <groupname>***
    c. ***sudo gpasswd -a <username> <groupname>***

15. Explicar como definir regras de senha e mostrar:
    a. Definir: ***sudo nano /etc/security/pwquality.conf***
    b. Mostrar: ***sudo nano /etc/login.defs***

16. Checar se pertence a grupo, existência user e status de senha:
    a. ***getent group <groupname>***
    b. ***getent passwd <username>***
    c. ***chage -l <username>***

17. Explicar vantagens e desvantagens dessa política de senhas:
    a. São muito mais seguras e difíceis de decifrar, a desvantagem seria lembrar delas.

NOME DO HOST E PARTIÇÕES

18. Verificar hostname: ***hostname***
19. Modificar nome de host pelo login do avaliador e reiniciar:
    a. ***sudo hostnamectl set-hostname <newname>***
    b. ***hostnamectl status***
    c. ***reboot***

20. Verificar partições: ***lsblk***
21. Explicar como funciona LVM e do que se trata:

a. LVM é um gerenciador de discos do Kernel. Permite que discos e partições sejam trocados sem interrupção do serviço, alterar o tamanho dos volumes, criar backup de imagens dos volumes, criar um volume único a partir de vários ou criar volumes espelhados em mais de um disco. Seu objetivo é a flexibilidade no gerenciamento de discos.

SUDO

22. Se sudo está instalado: ***apt-cache policy sudo***
23. Atribuir user to sudo: ***sudo gpasswd -a <username> sudo***
24. Explicar valor e funcionamento do sudo e mostrar implementações das regras:
    a. O sudo é usado para que você possa executar um comando de root, administrador sem precisar trocar de usuário. Eu posso autorizar meu usuário a usá-lo, assim não precisaria usar a senha de administrador. Isso deixa mais seguro a execução de comando, já que é muito mais arriscado usar o root, qualquer alteração afetaria todo o sistema e não apenas um usuário.
25. Verificar arquivo na pasta /var/log/sudo/: ***cat /var/log/sudo/sudo.log***

UFW

26. Verificar se está instalado e funcionando: ***sudo service ufw status***
27. Explicar o que é UFW e seu valor:
    a. UFW é um firewall, uma medida de segurança para seu sistema. Seu valor é deixar mais seguro todo seu sistema, assim menos vulnerável a ataques cibernéticos.
28. Listar regras ativas no UFW: ***sudo ufw status***
29. Adicionar nova regra: ***sudo ufw allow 8080***
30. Listar regras ativas no UFW numeradas: ***sudo ufw status numbered***
31. Deletar nova regra: ***sudo ufw delete allow 8080***

SSH

32. Verificar se está instalado e funcionando: ***sudo service ssh status***
33. Explicar o que é SSH e o valor de usá-lo:
    a. SSH é um protocolo de segurança. Ele fornece mais segurança na troca de arquivos entre cliente e servidor de internet, usando criptografia. Seu objetivo é possibilitar a realização de alterações em sites e servidores utilizando uma conexão simples e segura.
34. Conectar no terminal pelo SSH:

a. IP: ***hostname -I***
b. ***ssh <username>@<ip> -p 4242***
c. ***exit***

MONITORAMENTO DE SCRIPT

35. Mostrar script monitoring: ***sudo nano /root/scripts/monitoring.sh***
36. Mostrar script sleep: ***sudo nano /root/scripts/sleep.sh***
37. Mostrar cron: ***sudo crontab -e***
38. Explicar o que é CRON:
    a. Cron é um comando no Linux que permite programar tarefas para serem executadas de maneira independente. Isso ajuda no monitoramento do sistema.
39. Desativar cron sem alterar script:
    a. sudo systemctl disable cron
    b. sudo reboot