EXERCÍCIOS DE REVISÃO

1.

Pentest é um teste de segurança que simula ataques cibernéticos para identificar vulnerabilidades em sistemas e redes. As etapas incluem coleta de informações, planejamento, exploração de vulnerabilidades, relatório, mitigação e reteste para verificar se as correções foram eficazes. É uma ferramenta essencial para fortalecer a segurança digital.

2.

[1] Ataques de negação de serviço (DoS/DDoS) sobrecarregam um servidor ou rede, impedindo acessos legítimos.

[2] Ransomware bloqueia o acesso a sistemas até que um resgate seja pago.

[3] Explorações de vulnerabilidades usam falhas em sistemas para causar interrupções e indisponibilidade.

3.

O conceito mencionado no texto é compliance. Ele se refere à conformidade com leis, regulamentos, políticas internas e obrigações contratuais, sendo essencial para garantir a segurança da informação e evitar riscos legais ou operacionais.

4.

RECURSO	FINALIDADE	COMO AGE	BENEFÍCIO	LIMITAÇÃO
FIREWALL	Controle de tráfego	Bloqueia ou permite acessos	Protege contra acessos externos	Não detecta ataques avançados
IDS	Monitoramento de intrusões	Alerta sobre atividades suspeitas	Identifica padrões de ataque	Não impede ataques diretamente
IPS	Prevenção de intrusões	Bloqueia tráfego malicioso em tempo real	Reduz risco de invasões	Pode bloquear acessos legítimos

5.

[1]. Use senhas fortes e únicas, combinando letras maiúsculas e minúsculas, números e caracteres especiais. Evite informações pessoais ou sequências óbvias.

[2]. Ative a autenticação de dois fatores (2FA) sempre que possível, adicionando uma camada extra de segurança.

[3]. Utilize gerenciadores de senhas para armazenar e criar senhas seguras, evitando o uso repetido em diferentes contas.

6.

a) a pessoa da imagem baixou uma versão falsificada do Windows.

b) Baixar o Windows falso traz riscos como malware, falta de atualizações de segurança, roubo de informações pessoais e possíveis problemas legais. É essencial usar versões oficiais para garantir segurança e proteção.

c)Para evitar baixar Windows falso, adquira-o de fontes confiáveis como o site oficial da Microsoft ou revendedores autorizados, verifique a autenticidade do produto e evite sites desconhecidos ou ofertas suspeitas. Utilize também ferramentas de segurança para verificar os arquivos antes da instalação.

7.

a) a utilização de credenciais padrão.

b)acesso não autorizado ao servidor.

c)fazer a mudança de credencial e restringir acesso.

8.

a) Para Bob: Ana deve cifrar a mensagem usando a chave pública de Bob. Ao fazer isso, ela garante que apenas Bob, com sua chave privada correspondente, seja capaz de decifrar a mensagem. Isso atende ao requisito de sigilo, permitindo que apenas Bob tenha acesso ao conteúdo.

b) Bob deve utilizar sua chave privada para decifrar a mensagem. Como Ana usou a chave pública de Bob na criptografia, a chave privada dele é essencial para desfazer o processo e acessar o conteúdo original da mensagem.

c) Para Carlos: Ana deve cifrar a mensagem usando sua própria chave privada. Isso permite que Carlos, ao decifrá-la, comprove que a mensagem veio de Ana. Esse método atende ao requisito de autenticidade, garantindo que apenas Ana poderia ter enviado aquela mensagem.

d) Carlos deve utilizar a chave pública de Ana para decifrar a mensagem. Ao fazer isso, ele verifica que a mensagem foi de fato cifrada com a chave privada de Ana, confirmando sua autenticidade.

9.

a) o servidor apresenta o certificado, o navegador valida e usa a chave pública para criptografia

b)

[1]. Confidencialidade da comunicação

[2]. Autenticidade do site acessado

10.

Três registros importantes para auditoria de segurança são: uso de privilégios elevados, arquivos acessados e tipo de acesso realizado.