Integrantes:

Arthur Galassi | RA: 82422433

Kauê Soares | RA: 824117267

Leonardo Macedo | RA: 82422817

Luiz Washington | RA: 824148694

Lucas Suarez | RA: 824138683

George Geronimo | RA: 824148488

1) O que é um pentest? Quais são as etapas de um pentest?

Resposta: Pentest é um teste de intrusão que simula ataques de hackers antecipadamente para que a empresa possa encontrar e corrigir as vulnerabilidades.

2) Explique o funcionamento de 3 ataques de segurança cibernética que podem comprometer diretamente a disponibilidade de sistemas.

1) DDOS: É um tipo de ataque que utilizam de maquinas virtuais ou de maquinas fantasmas(“ maquinas invadidas por crackers que são pré programadas para esta função”), para fazer requisições de acesso para o servidor do sistema e assim congestionando o acesso e barrando usuários verdadeiros do sistema.

2) Código Malicioso: O cracker pode fazer um código malicioso disfarçado de um software comum, para que rode programas em loop até que a memoria do computador se esgote e seja forçado a ser desligado.

3) Ransomware: É um programa malicioso que executa na maquina da vitima fazendo com que todos os arquivos importantes sejam criptografados e para serem decifrados teriam de pagar um resgate para tal.

3) Leia o fragmento de texto a seguir.

Todas as empresas devem observar a legislação local, os seus regulamentos internos e as obrigações contratuais, além dos acordos internacionais. Os requisitos de segurança que uma empresa deve cumprir estão fortemente relacionados a isso. (HINTZBERGEN, 2018)

O texto acima se refere a um conceito que pode ser considerado importante quando se trata de segurança da informação. De qual conceito estamos falando (em uma palavra)?

Resposta: Conformidade

4) Existem vários recursos de software e hardware para estabelecer diversos níveis de segurança em uma rede de computadores. Entre outros, podemos citar os firewalls e os sensores (IDS e IPS). Faça um quadro comparativo resumindo as características de cada um dos três recursos.

FIREWALLS	IDS	IPS
Um firewall é um mecanismo de segurança que controla o fluxo de informações na rede, permitindo ou proibindo informações de acordo com normas de segurança. Ele funciona como um filtro entre uma rede interna segura e redes externas, resguardando contra acessos não permitidos, invasões cibernéticas e outros riscos É um recurso ativo que (detecta e toma as medidas preventivas).	Um IDS é uma ferramenta que monitora a rede ou os sistemas em busca de atividades maliciosas ou violações de políticas de segurança.Sua principal função é de detectar e alertar sobre possíveis ataques ou comportamentos suspeitos sem tomar uma ação direta contra o para bloquear o ataque. É um recurso passivo pois apenas detecta e notifica.	Tem como função principal monitorar e bloquear atividades suspeitas . Ele é um recurso ativo que detecta e previne ameaças em tempo real, interrompendo o tráfego suspeito automaticamente.

5)Uma pessoa lhe procura e pede ajuda sobre formas de proteger as suas senhas. Cite pelo menos três conselhos que você daria a essa pessoa.

Resposta:

1- Uma senha com pelo menos 12 caracteres que tenha letras maiusculas, minúsculas e caracteres especiais.

2- ter verificação de duas etapas

3-atualizar a senha com frequência

6) Observe a imagem a seguir.

Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade

Resposta: Antivírus desatualizado podendo causar vulnerabilidade no sistema.

b) A ameaça

Resposta: Novos vírus que poderão invadir o sistema por falta de atualização no software de segurança.

c) Uma ação defensiva para mitigar a ameaça

Resposta: Adquirir uma licença original do windows.

7) Observe a imagem a seguir.Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade

Resposta: Senha com poucos caracteres ou senha fraca.

b) A ameaça

Resposta: Possível descobrimento de senha por terceiros.

c) Uma ação defensiva para mitigar a ameaça

Resposta:atualizar a senha para deixá-la mais difícil de descobri-la.

8) Ana tem duas mensagens para enviar de forma criptografada para dois amigos: Bob e Carlos. Bob deseja receber a mensagem de maneira que apenas ele possa decifrá-la. Carlos não está preocupado com o sigilo da mensagem, mas deseja ter certeza de que foi mesmo Ana que a enviou. Assuma que todos têm seu par de chaves pública e privada, que todas as chaves públicas são acessíveis. Visando a atender os requisitos de Bob e Carlos, descreva, em termos de uso das chaves:

a) como Ana deverá cifrar a mensagem antes de enviar para Bob;

Resposta: Ana deverá cifrar com a Chave pública

b) como Bob deverá decifrar a mensagem de Ana corretamente;

Resposta: Bob deve decifrar com a chave privada

c) como Ana deverá cifrar a mensagem antes de enviar para Carlos;

Resposta: Ana deve cifrar com a chave privada

d) como Carlos deverá decifrar a mensagem de Ana corretamente.

Resposta:carlos deverá decifrar com a Chave pública

9) Observe as imagens a seguir:

As imagens apresentam informações do certificado digital do site www.bb.com.br. Com base nelas, responda:

9.a) Como se dá a utilização do certificado na origem e no destino? Identifique como são utilizadas as chaves criptográficas do Banco do Brasil.

Resposta: O banco envia o certificado com uma chave privada (só o banco poderia ter enviado aquele certificado). e é descriptografado com uma chave pública(qualquer um pode ler)

9.b) Cite dois benefícios de segurança que uma transação eletrônica recebe com a utilização do certificado digital do Banco.

Resposta:O certificado garante a autenticação da transação do banco e do cliente sem que terceiros se passem por algum dos lados na transação

e também como a transação é criptografada garante que apenas o destinatário visualize a mensagem

10) Observe a imagem a seguir:

De acordo com a norma ISO 27002: 2013, "convém que registros (log) de eventos das atividades do usuário, exceções,

falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos

regulares". ABNT (2013).

Cite 3 registros importantes da atividade dos usuários que podem ser registrados para posterior auditoria de segurança.

resposta:

1 - Registro de acesso

2 - Registro de alteração de dados

3 - Registro de alteração na segurança