Nome: Yasmin Victória Alves de Sousa RA: 824210011

Nome: Natasha Melo de Sousa RA: 82429222

Questões

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

Um pentest (Penetration Test) é um teste de penetração, no qual especialistas simulam ataques cibernéticos para identificar vulnerabilidades em sistemas. As etapas incluem o planejamento, varredura de fraquezas, tentativa de exploração dessas falhas e, por fim, a elaboração de um relatório com as descobertas e sugestões de correção. O objetivo é reforçar a segurança antes que invasores reais possam explorar as brechas.

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

Ransomware: Malware que criptografa arquivos de um sistema e impede o acesso até que um resgate seja pago, comprometendo a disponibilidade de dados essenciais.

Backdoors: Vulnerabilidades exploradas por invasores para obter acesso não autorizado a sistemas, permitindo que eles contornem a autenticação e comprometam a integridade e a disponibilidade.

Phishing: Ataque de engenharia social onde invasores se fazem passar por entidades confiáveis para roubar informações sensíveis, resultando na perda de acesso a contas e serviços e comprometendo a disponibilidade.

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.

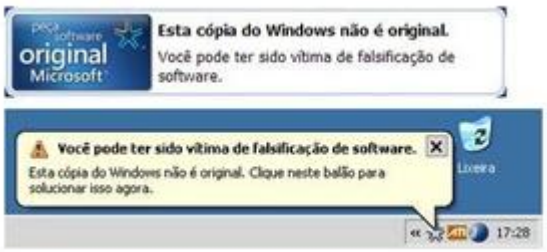
4) Existem vários recursos de software e hardware para estabelecer diversos níveis de segurança em uma rede de computadores. Entre outros, podemos citar os firewalls e os sensores (IDS e IPS). Faça um quadro comparativo resumindo as características de cada um dos três recursos.

Caracteristicas	FIREWALL	IPS	IDS
Função Principal	**O Firewall é um dispositivo de segurança que atua como uma barreira entre redes, controlando o fluxo de dados entre elas.**	**O IPS é um sistema que monitora o tráfego de rede em tempo real e bloqueia automaticamente atividades maliciosas.**	**O IDS é um sistema que analisa o tráfego de rede em busca de atividades suspeitas e gera alertas para a equipe de segurança.**
Método de Operação	**Permite ou bloqueia pacotes com base em regras predefinidas.**	**Inspeciona o tráfego em tempo real, procurando padrões ou assinaturas de ataque, e evita ataques quando os detecta.**	**Detecta tráfego em tempo real, procurando padrões de ataque ou anomalias, e gera alertas.**
Localização	**Fica entre a rede interna e a rede externa.**	**Similar ao IDS, é instalado em pontos estratégicos da rede ou em hosts.**	**Pode ser posicionado em pontos estratégicos da rede ou em hosts.**
Resposta a Ameaças	**Não responde ativamente; apenas filtra o tráfego.**	**Responde em tempo real, bloqueando o tráfego suspeito.**	**Emite alertas para ações manuais de intervenção.**
Desempenho	**Pode impactar o desempenho da rede se mal configurado.**	**Pode impactar o desempenho da rede ao bloquear tráfego, mas oferece uma proteção mais proativa.**	**Pode gerar falsos positivos, necessitando ajustes frequentes.**

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.

- **Use senhas fortes e únicas: Combine letras, números e símbolos, e não repita senhas em diferentes serviços.**
- **Evite usar informações pessoais: Não use nomes, datas de nascimento ou números fáceis de adivinhar em suas senhas.**
- **Ative a autenticação em duas etapas (2FA): Adicione uma segunda verificação além da senha.**
- **Use um gerenciador de senhas: Ele armazena e gera senhas seguras para o usuário.**
- **Não repetir a mesma senha em outros sistemas.**

6) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade

Sistema operacional não original tem falhas de segurança, porque não recebe atualizações, o que se torna mais flexível a explorações e malware.

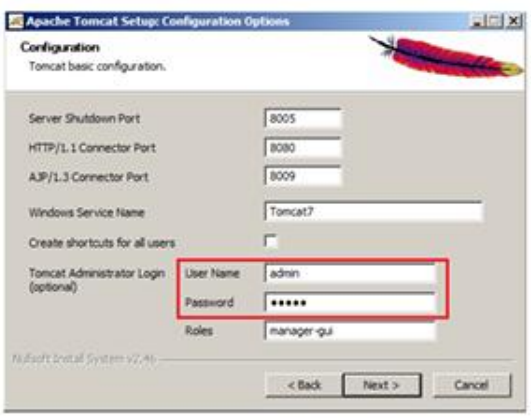
b) A ameaça

Permite a instalação de malware, infiltração de dados e códigos no sistema. O que também leva a exposição de ataques por meio de brechas não corrigidas.

c) Uma ação defensiva para mitigar a ameaça

Instalar uma versão legítima e licenciada do Windows. O que permite atualizações de segurança, protegendo contra falhas e ameaças emergentes imprevistas.

7) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade

Uso de credenciais padrão.

b) A ameaça

Um invasor acessa com facilidade o sistema.

c) Uma ação defensiva para mitigar a ameaça

Alterar as credenciais padrão e inserir mecanismos de autenticação multifator (MFA).

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. Assume 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;

Com a chave pública de Bob.

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

Com a sua privada.

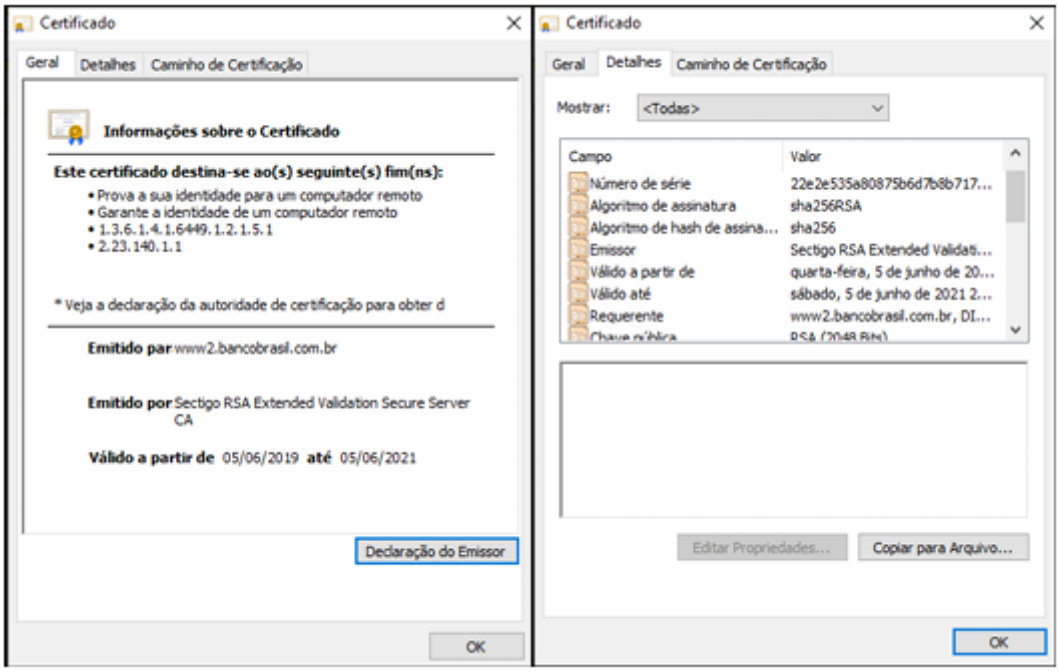
c) como Ana deverá cifrar a mensagem antes de enviar para Carlos;

Com a sua chave privada.

d) como Carlos deverá decifrar a mensagem de Ana;

Com a chave pública de Ana.

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.

O certificado digital apresenta a chave pública do Banco do Brasil, a qual é autenticada por uma Autoridade Certificadora (CA) de confiança. Quando um usuário (cliente) acessa o website do Banco do Brasil, o servidor transmite seu certificado digital, que inclui a chave pública, para o cliente.

O cliente (navegador do usuário) avalia a validade do certificado através da cadeia de confiança até a Autoridade Certificadora, que assegura a autenticidade do documento. Após a verificação do certificado, o cliente cria uma chave de sessão (um tipo de chave simétrica destinada a essa conexão específica) e a cifra utilizando a chave pública do Banco do Brasil. O servidor,

por sua vez, utiliza sua chave privada para decifrar a chave de sessão. A partir desse momento, a comunicação entre o cliente e o servidor é realizada por meio dessa chave simétrica, que é ágil e eficaz para a criptografia e descriptografia dos dados durante a sessão.

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

Confidencialidade: A implementação de chaves criptográficas assegura que todas as informações trocadas entre o cliente e o Banco do Brasil sejam devidamente encriptadas. Isso protege dados sensíveis, como senhas, números de contas e informações financeiras, de possíveis interceptações por terceiros durante o envio. Autenticidade e Integridade: O uso de um certificado digital garante que o usuário realmente está se comunicando com o Banco do Brasil, evitando que interações ocorram com sites falsos (ataques de phishing). Ademais, a integridade das informações é mantida, pois qualquer modificação nos dados durante a transmissão seria facilmente identificada, graças à verificação da assinatura digital e à adoção de técnicas como hashing.

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 registrados para posterior auditoria de segurança.

Alterações nas permissões e privilégios de usuários

Tentativas de login (sucesso e falha)

Acesso e modificação de dados críticos

Referências

- ABNT (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS). NBR ISO/IEC 27002:2013: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2013.

– HINTZGBERGEN, Jule. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. 3. ed. Brasport, Rio de Janeiro, 2018.