UC Sistemas Computacionais e Segurança – 2025.2
Exercícios de Revisão
Prof. Calvetti

Fontes de estudo principais

- Material curado da UC Sistemas Computacionais e Segurança no U-Life
- Curso Cisco Fundamentos de Segurança Cibernética
- Material das aulas

Questões

1) O que é um *pentest*? Quais são as etapas de um *pentest*?
Pentests significam “Penetration Test”. São procedimentos de testagem de partes sistêmicas com o objetivo de descobrir vulnerabilidades existentes dentro do sistema, divididos em varredura, exploração, aprimoramento de privilégios e ocultação.

2) Explique o funcionamento de 3 ataques de segurança cibernética que podem comprometer diretamente a DISPONIBILIDADE de sistemas.
Ransomware: criptografando os dados de uma base, o acesso a eles torna-se impossível.
DDoS: pacotando um sistema de modo a sobrecarregá-lo, ele irá negar o fornecimento de informações e uso para os outros usuários.
Malware Worm: através de alta replicação dentro da máquina infectada, o vírus pode comprometer a performance sistêmica e fazer com que ele seja derrubado por falta de memória ou dano causado aos componentes físicos da máquina de hospedagem.

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)

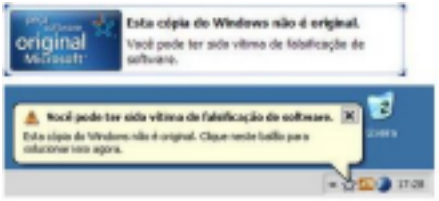
O texto acima se refere a um conceito que pode ser considerado importante quando se trata de segurança da informação. De qual conceito estamos falando (em uma palavra)?
Conformidade / Requisitos legais.

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.

Implementação	FIREWALL	IPS	IDS
Funcionamento	Software responsável por monitorar redes ou ambientes para infringir comportamentos ou conexões que fujam do padrão estabelecido.	Monitora o tráfego e o comportamento em um ambiente computacional em busca de **prevenir** ataques.	Monitora comportamentos para detectar invasões e **alertar** do ataque após o mesmo ter sido detectado pelo monitoramento.
Como monitora	Monitora os endereços de IP e portas da rede/ambiente.	Analisa a navegação em um ambiente buscando comportamentos fora do padrão.	Analisa a navegação em um ambiente buscando comportamentos fora do padrão para emitir alertas acerda do usuário suspeito.
Aplicação sistêmica	Primeira camada de segurança da rede	Instalado após o Firewall	Instalado após o Firewall
Medida tomada	Restringe a navegação total na rede ou de recursos da mesma	Bloqueia o usuário/bot navegando de modo suspeito	Cria avisos e alerts em caso de comportamentos suspeitos

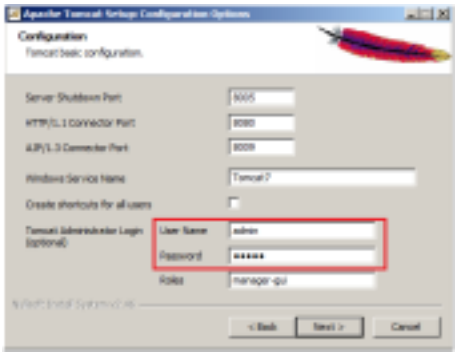
5) Uma pessoa lhe procura e pede ajuda sobre formas de proteger as suas senhas. Cite pelo menos três conselhos que você daria a essa pessoa.
- Não usar sequências numéricas sequenciais;
- Não usar o próprio nome nem o de pessoas próximas de si dentro da senha;
- Utilizar palavras não-léxicas e não existentes (ex: aosijf, sopqoiwr), de modo que a senha esteja mais protegida contra ataques a senhas comuns;
- Utilizar caracteres especiais;
- Utilizar uma senha diferente para cada acesso;
- Não usar datas de aniversário ou datas importantes (ou facilmente dedutíveis) dentro da senha);
- Utilizar gerenciador de senhas;

6) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade
O usuário está utilizando um sistema operacional pirata, o que não somente traz limitações, mas perigos (backdoor instalados nessa distribuição pirata, etc)
b) A ameaça
Maior risco de pegar vírus por ação própria do sistema ou por ausência de suporte ao usuário próprio do sistema original.
c) Uma ação defensiva para mitigar a ameaça
Instalando o sistema original através da própria provedora do mesmo.
7) Observe a imagem a seguir.



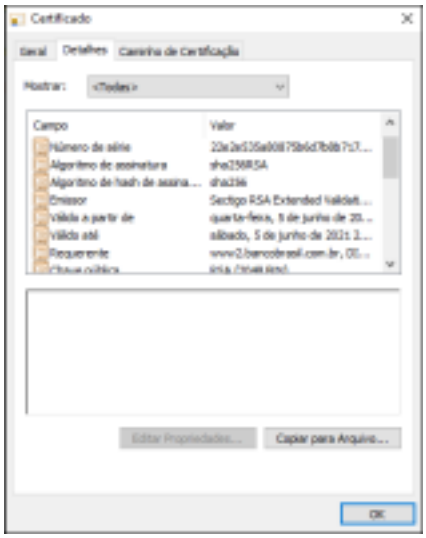
Do ponto de vista da segurança da informação, identifique:

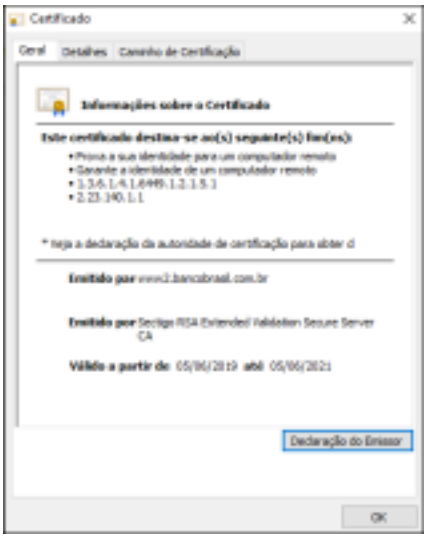
a) A vulnerabilidade
Nome de usuário padrão, “admin” é muito comum de ser usado e muito vulnerável de vazar ou ter ataques.
b) A ameaça
Pessoas que conhecem senhas default de um sistema poderão acessar essa instância.
c) Uma ação defensiva para mitigar a ameaça
Mudar o nome de usuário e a senha de usuários que tenham privilégios administrativos para nomes e senhas fora do padrão.

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;
Utilizando a chave de criptografia pública do Bob.
b) como Bob deverá decifrar a mensagem de Ana corretamente;
Utilizando a sua própria chave privada.
c) como Ana deverá cifrar a mensagem antes de enviar para Carlos;
Utilizando a sua própria chave privada.
d) como Carlos deverá decifrar a mensagem de Ana corretamente.
Utilizando a chave pública da 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.
Um hash é gerado e depois re-criptografado com uma chave privada para poder ser futuramente decifrado por uma chave pública para validar a autenticidade daquele certificado.

9.b) Cite dois benefícios de segurança que uma transação eletrônica recebe com a utilização do certificado digital do Banco.
Sabendo qual a chave utilizada para a criptografia/decifragem, é possível rastrear a origem de onde veio a a transação, uma vez que criptografias assimétricas garantem esta rastreabilidade da de/cifragem dos dados com base nas chaves.

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.

Atividades de remoção/adição de privilégios pra outros usuários dentro do sistema;

Alteração ou adição de informações financeiras do sistema;

Alteração e adição de arquivos hospedados dentro do sistema.

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.