UC Sistemas Computacionais e Segurança – 2025.2
Exercícios de Revisão
Profs. 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 e respostas

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

Penetration Test é um método de testagem de segurança no qual os testadores visam componentes de software ou hardware em sistemas para determinar se vulnerabilidades podem ser exploradas para comprometer aplicativos, dados ou recursos de ambiente.

Penetration Test é "uma metodologia de teste na qual os avaliadores, normalmente trabalhando sob restrições específicas, tentam contornar ou anular os recursos de segurança de um sistema". (NIST)

As etapas são: varredura, exploração, escalação de privilégios e ocultação.

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

Citados no material curado: TCP SYN / SYN Flood / TCP ACK Attack; Teardrop; DoS / DDoS; Ransomware; ICMP Attack.

Outros ataques, como *rootkit,* cavalos de troia e ataques de força bruta, podem ocasionar indiretamente a indisponibilidade de sistemas.

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.

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.

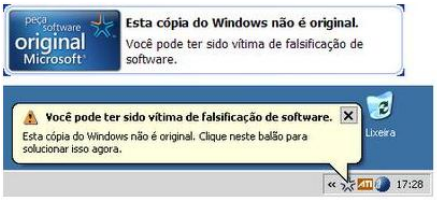
Parâmetro	**FIREWALL**	**IPS**	**IDS**
Filosofia	Firewall é um dispositivo de segurança de rede que filtra o tráfego de entrada e saída com base em regras predeterminadas	O IPS é um dispositivo ou software que inspeciona o tráfego, o detecta, classifica e impede proativamente o tráfego malicioso de ataques.	Um sistema de detecção de intrusão (IDS) é um dispositivo ou aplicativo de software que monitora um tráfego em busca de atividades maliciosas ou violações de políticas e envia alertas na detecção.
Princípio de trabalho	Filtra o tráfego com base no endereço IP e nos números de porta	Inspeciona o tráfego em tempo real e procura padrões de tráfego ou assinaturas de ataque e, em seguida, evita os ataques na detecção	Detecta tráfego em tempo real e procura padrões de tráfego ou assinaturas de ataque e gera alertas
Colocação na rede	Deve ser a 1ª linha de defesa (borda da rede)	Deve ser colocado após o dispositivo Firewall na rede	Deve ser colocado após o firewall
Ação	Bloquea o tráfego baseado nas regras configuradas	Bloqueia o tráfego suspeito	Gera alertas/alarmes quando detecta anomalias
Detecta ataques *zero day*?	Não, pois realiza apenas filtragem de pacotes com regras conhecidas.	Sim, pois realiza prevenção baseada em anomalias.	Sim, pois realiza detecção baseada em anomalias.

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.

Entre outros, podemos citar:

- Evitar usar senhas com dados que possam ser obtidos facilmente em redes sociais ou na internet, como nomes, sobrenomes, sequências de teclado, datas comemorativas familiares ou palavras conhecidas publicamente.
- Ao cadastrá-las, usar sempre números aleatórios com muitos dígitos e quantidade suficiente de caracteres especiais e letras maiúsculas e minúsculas.
- Ter cuidado ao digitar a senha, evitando observadores.
- Evitar computadores de terceiros.
- Não clicar em links recebidos pela internet
- Verificar se a conexão com a internet é segura ao utilizar senhas online.
- Não repetir a mesma senha em vários sistemas.
- Usar um gerenciador de senhas.
- Utilizar, se possível, a autenticação de múltiplos fatores.

6) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade

Sistema operacional falsificado instalado, logo não recebe atualizações

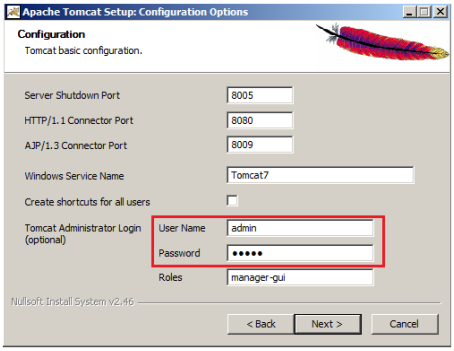
b) A ameaça

Possibilidade de infecção por malware; instabilidade e baixo desempenho a longo prazo

c) Uma ação defensiva para mitigar a ameaça

Retirar as cópias não licenciadas, instalando cópias legítimas e/ou fazendo opção por sistema operacional open source.

7) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade
Credenciais fracas para usuário administrador. “Admin” é um nome de usuário padrão em vários serviços.

b) A ameaça
Um cracker terá mais facilidade para quebrar as credenciais e invadir o sistema.

c) Uma ação defensiva para mitigar a ameaça
Renomear todos os usuários com privilégios de administração na rede.

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:**

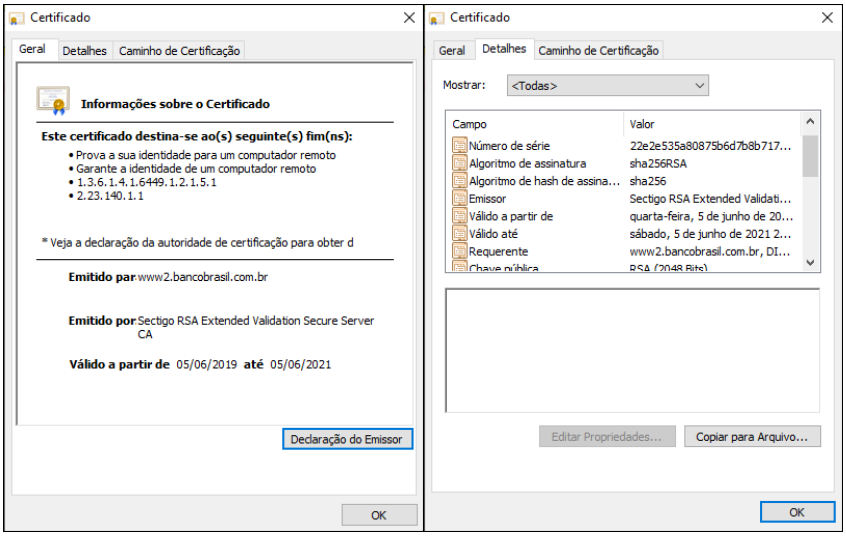
a) como Ana deverá cifrar a mensagem antes de enviar para Bob;
Com a chave pública de Bob.

b) como Bob deverá decifrar a mensagem de Ana corretamente;
Com a sua chave privada.

d) como Ana deverá cifrar a mensagem antes de enviar para Carlos;
Com a sua chave privada.

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

A CA Serctigo gera um resumo dos dados de identificação do Banco através de uma função HASH. O resultado da função HASH será criptografado com a chave privada da origem (Banco), assim obtém-se a assinatura digital.

Para a validação da assinatura digital, o cliente do banco deve decifrá-la com a chave pública do emissor, contida no certificado. Em seguida, o HASH deve ser calculado sobre a mensagem enviada. Se o valor calculado coincidir com o valor do HASH decifrado (a partir da assinatura digital), a mensagem é então validada.

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

Autenticação da origem: garantia de que as mensagens realmente vêm da origem especificada no certificado, no caso o Banco do Brasil.

Integridade: garantia de que as mensagens recebidas do Banco do Brasil estão íntegras, e não sofreram nenhuma alteração acidental ou intencional.

Pode, ainda, ser citado o não-repúdio – a garantia de que a origem (o Banco) não pode repudiar, ou refutar as mensagens por ele enviadas.

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.

Podem ser citados, entre outros:

a) identificação dos usuários (ID);
b) datas, horários e detalhes de eventos-chave, como, por exemplo, horário de entrada (*log-on*) e saída (*log-off*) no sistema;
c) registros das tentativas de acesso ao sistema, aceitas e rejeitadas;
d) registros das tentativas de acesso a outros recursos e dados, aceitos e rejeitados;
e) alterações na configuração do sistema;
f) uso de privilégios;
g) Uso de aplicações e utilitários do sistema;
h) arquivos acessados e o tipo de acesso;
i) endereços e protocolos de rede;
j) alarmes provocados pelo sistema de controle de acesso;
k) ativação e desativação dos sistemas de proteção, como sistemas de antivírus e sistemas de detecção de intrusos;
l) registros de transações executadas pelos usuários nas aplicações

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.