**Revisão de Sistemas Computacionais e Segurança**

Prof. Calvetti

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

Pentest é uma operação que replica a invasão de sistemas, redes ou aplicativos no mundo real com o objetivo de descobrir e reparar fraquezas antes que um ataque seja feito contra eles por outros.

**2 - Explique o funcionamento de 3 ataques de segurança cibernética que podem comprometer diretamente a DISPONIBILIDADE de sistemas:**

* Ataques DDoS (Distributed Denial of Service) sobrecarregam um servidor ou rede com tráfego excessivo e tornam o sistema inacessível a usuários legítimos.
* Ransomware criptografa informações ou sistemas, exige pagamento e é capaz de bloquear completamente o acesso a informações e serviços.
* Exploração de vulnerabilidades de software (por exemplo, estouro de buffer), pode travar sistemas ou causar reinicializações forçadas e impacta a disponibilidade, causando falhas e tempo de inatividade.

**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

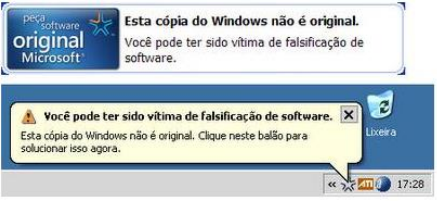
**4 - Existem vários recursos de software e hardware para estabelecer diversos níveis de segurança em uma rede de computadores. Entre outros, podemos citar os firewalls e os sensores (IDS e IPS). Faça um quadro comparativo resumindo as características de cada um dos três recursos.**

| **Recursos** | **Função Principal** | **Age Como:** | **Ações** | **Locais** |
| --- | --- | --- | --- | --- |
| **Firewall** | Controla o tráfego de entrada e saída | Filtra o acesso | Permite ou bloqueia tráfego | perímetro de rede |
| **IDS** | Detecta atividades suspeitas | Sensor passivo | Apenas Alerta | Dentro ou fora da rede |
| **IPS** | Previne ataques em tempo real | Sensor ativo | Alerta e Bloqueia | Paralelo a rede |

**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 exclusivas
* Habilite a autenticação de dois fatores (2FA)
* Use um gerenciador de senhas

**6 - Observe a imagem a seguir.**



**Do ponto de vista da segurança da informação, identifique:**

**a) Vulnerabilidade:**

Instalação de uma cópia pirata do sistema operacional. Isso implica que o sistema está em risco, sem atualizações de segurança ou proteção adequada, ou provavelmente sob ameaça.

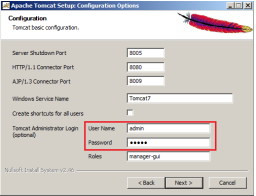
**b) Uma ameaça:**

Instalação de software falsificado ou malicioso com software malicioso incorporado, para tornar o sistema vulnerável a ameaças como códigos de vazamento de dados, instalação de malware ou perda de integridade do sistema.

**c) Uma ação defensiva para combater a ameaça:**

Uso de software original/licenciado, para proteger e preservar a proteção e a integridade do sistema ou implemente uma política de segurança da informação, como restringir a aquisição e a instalação de software apenas a meios autorizados.

**7 - Observe a imagem a seguir.**

****

**Do ponto de vista da segurança da informação, identifique:**

**a) A vulnerabilidade:**  
 A utilização de credenciais padrão (usuário “admin”) durante a configuração do Apache Tomcat. Essa prática expõe o sistema a acessos não autorizados, especialmente se a senha também for fraca ou padrão.

**b) A ameaça:**  
 A possibilidade de ataques de força bruta, acesso não autorizado ou exploração por hackers, que podem assumir o controle do servidor de aplicações, comprometer dados e serviços hospedados, ou usar o servidor para ataques a terceiros.

**c) Uma ação defensiva para mitigar a ameaça:**

* Alterar o nome de usuário e utilizar senhas fortes, com combinação de letras, números e caracteres especiais.
* Desabilitar o acesso remoto à interface administrativa, caso não seja necessário.
* Restringir o acesso por IPs confiáveis e usar mecanismos como autenticação multifator (MFA) sempre que possível.
* Manter o Tomcat e demais softwares atualizados, aplicando patches de segurança regularmente.

**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:**

Ana deseja garantir o sigilo da mensagem, ou seja, que apenas Bob possa lê-la.  
 Portanto, Ana deve cifrar a mensagem utilizando a chave pública de Bob.

### **b) Como Bob deverá decifrar a mensagem de Ana corretamente**

Como a mensagem foi cifrada com a chave pública de Bob,  
 Bob deverá usar sua chave privada para decifrar a mensagem.

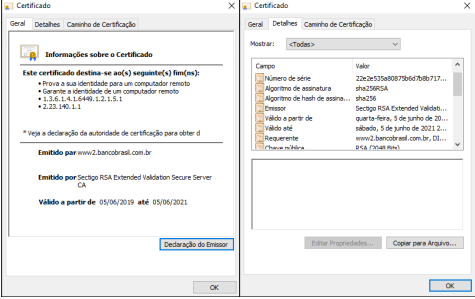
### **c) Como Ana deverá cifrar a mensagem antes de enviar para Carlos:**

Carlos não está preocupado com o sigilo, mas deseja garantir a autenticidade, ou seja, que a mensagem tenha sido enviada por Ana.  
 Para isso, Ana deve cifrar (ou assinar digitalmente) a mensagem utilizando sua chave privada

### **d) Como Carlos deverá decifrar a mensagem de Ana corretamente:**

Para verificar se a mensagem foi realmente enviada por Ana,  
 Carlos deve utilizar a chave pública de Ana para decifrar ou verificar a assinatura da mensagem.

**9 - Observe as imagens a seguir:**

****

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

**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 utilização do certificado digital ocorre de forma que, ao acessar o site do Banco do Brasil, o navegador do usuário (origem) recebe do servidor (destino) o certificado digital contendo a chave pública do banco. O navegador verifica se o certificado é válido e confiável e, em seguida, utiliza a chave pública do banco para criptografar uma chave de sessão simétrica, que será utilizada para a comunicação segura. Essa chave de sessão simétrica é enviada ao servidor, que a descriptografa com sua chave privada. Posteriormente, toda a comunicação entre o servidor e o cliente é criptografada com a chave simétrica. Assim, a chave pública do Banco do Brasil é utilizada pelo cliente para garantir a confidencialidade no envio da chave de sessão, e a chave privada do banco é utilizada pelo próprio servidor para descriptografar essa chave e estabelecer a conexão segura.

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

Dois benefícios de segurança essenciais que uma transação eletrônica obtém com o uso do certificado digital do Banco do Brasil são a autenticidade e a confidencialidade. A confidencialidade garante que os dados comunicados entre o banco e o cliente sejam criptografados e, portanto, não possam ser acessados ​​por terceiros. A autenticação garante que o usuário esteja de fato se comunicando com o servidor legítimo do Banco do Brasil e não com fraudes, como sites fraudulentos ou ataques do tipo "man-in-the-middle".

**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.**

* Acessos ao sistema, incluindo data, hora, usuário e local de acesso, para identificar quem entrou no ambiente e quando isso ocorreu.
* Alterações em arquivos ou dados sensíveis, como modificações em informações confidenciais ou exclusão de arquivos, permitindo rastrear ações que podem comprometer a integridade ou a confidencialidade dos dados.
* Tentativas de acesso sem sucesso, como erros de senha ou tentativas de acesso a áreas não autorizadas, pois esses eventos podem indicar tentativas de invasão ou mau uso por parte de usuários internos.