**ATIVIDADE 07 - Parte 01**

**Docente: Robson Calvetti**

**UC: Sistemas Computacionais e Segurança – SCS**

**Grupo**

**Marinna Pereira Carneiro da Silva - RA: 824142121**

**Mariana Hildebrand Dantas - RA: 824118462**

**Christian Batista de Lima - RA: 824126605**

**Beatriz Silva de Jesus – RA: 824219590**

**Mayara Fernandes dos Santos – RA: 824227938**

**Victor Pinas Arnault – RA: 82215768**

1) O que é um pentest? Quais são as etapas de um pentest?
Um pentest é basicamente um teste de invasão. É uma forma de tentar encontrar falhas e vulnerabilidades na segurança de sistemas e redes, simulando um ataque real de hackers para ver até onde eles poderiam chegar. As etapas do pentest geralmente incluem: planejamento e reconhecimento (onde se coleta informações sobre o alvo), varredura (para identificar portas abertas e serviços vulneráveis), obtenção de acesso (tentar invadir de fato), manutenção do acesso (caso o invasor consiga entrar, para manter o acesso por mais tempo), e finalmente a análise e relatório dos resultados, para que as vulnerabilidades encontradas sejam corrigidas.

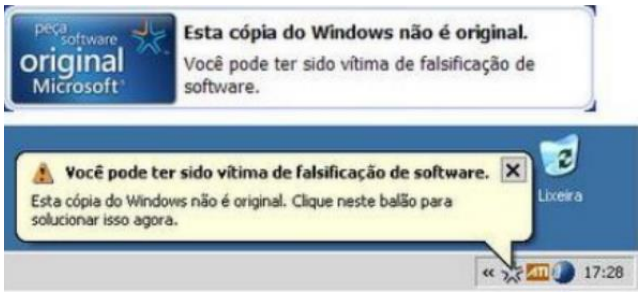
2) Explique o funcionamento de 3 ataques de segurança cibernética que podem comprometer diretamente a DISPONIBILIDADE de sistemas.
Três ataques que podem comprometer a disponibilidade de sistemas são: o DoS (Denial of Service), onde se sobrecarrega o sistema com uma quantidade absurda de solicitações para tirá-lo do ar; o DDoS (Distributed Denial of Service), que é parecido com o DoS, mas envolve múltiplos computadores atacando o alvo ao mesmo tempo; e o ataque de ransomware, onde um malware criptografa os dados e só os libera mediante pagamento, deixando o sistema indisponível até que a vítima pague o resgate.

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)?
O conceito mencionado no texto é "compliance", que se refere à conformidade com leis, regulamentos e padrões aplicáveis em uma organização.

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 (Sistema de Detecção de Intrusão) e IPS (Sistema de Prevenção de Intrusão) são utilizados para proteger redes. Firewalls controlam o tráfego de entrada e saída baseado em regras de segurança. IDS monitora a rede e alerta sobre atividades suspeitas, mas não interfere. IPS também detecta ameaças, mas age para bloquear o tráfego malicioso 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.
Para proteger suas senhas, é recomendado usar senhas longas e complexas, ativar a autenticação de dois fatores e evitar reutilizar senhas em diferentes serviços.

6) Observe a imagem a seguir.




Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade

A vulnerabilidade seria uma configuração

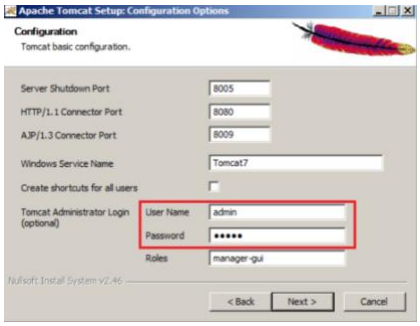
b) A ameaça

A ameaça seria a possibilidade de um ataque explorando essa falha.

c) Uma ação defensiva para mitigar a ameaça

Uma ação defensiva poderia ser atualizar o sistema e configurar regras de acesso mais restritivas.

7) Observe a imagem a seguir.




Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade

A vulnerabilidade seria a falta de proteção em uma interface de rede.

b) A ameaça

A ameaça seria um invasor que pudesse explorar essa vulnerabilidade.

c) Uma ação defensiva para mitigar a ameaça

Uma ação defensiva seria o uso de criptografia e autenticação para garantir o acesso seguro.

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:

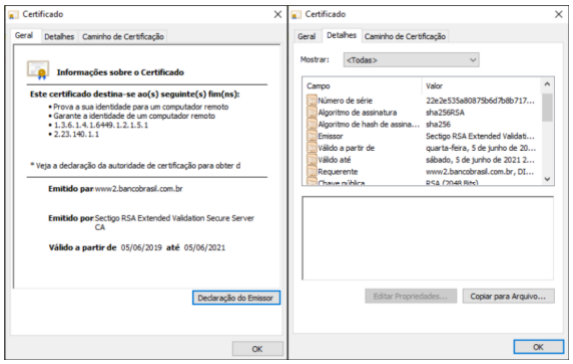
a) como Ana deverá cifrar a mensagem antes de enviar para Bob;
Ana deve cifrar a mensagem para Bob usando a chave pública de Bob.

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

c) como Ana deverá cifrar a mensagem antes de enviar para Carlos;
Para Carlos, Ana deve assinar a mensagem com a sua chave privada.

d) como Carlos deverá decifrar a mensagem de Ana corretamente.
Carlos verifica a assinatura usando 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:
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 é utilizado para autenticar o site e estabelecer uma conexão segura com os usuários, usando a chave pública do banco para criptografar os dados transmitidos.

b) Cite dois benefícios de segurança que uma transação eletrônica recebe com a utilização do certificado digital do Banco.
Os benefícios incluem a garantia de identidade do site e a proteção contra interceptação de dados.

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.
Então, três coisas que valem a pena registrar para poder revisar depois, caso role algum problema de segurança, seriam:
**Tentativas de login**: É legal anotar todas as vezes que alguém tenta entrar no sistema, tanto as que deram certo quanto as que não rolaram. Isso ajuda a sacar se alguém está tentando adivinhar a senha várias vezes ou se tem alguma coisa estranha acontecendo com os acessos.
**Acessos a arquivos importantes**: Sempre que alguém mexe em arquivos sensíveis ou importantes, tipo acessando, editando ou deletando, vale a pena deixar registrado. Assim, dá pra ver quem foi, quando foi e o que exatamente a pessoa fez, o que ajuda a detectar acessos indevidos.
**Mudanças nas configurações de segurança**: Quando alguém altera as configurações de segurança, como regras do firewall ou privilégios de usuários, é bom ter isso anotado. Esse registro facilita entender o que mudou e se essas alterações podem ter aberto brechas ou causado algum problema no sistema.