**AMBIENTES COMPUTACIONAIS E CONECTIVIDADAS – CALVETTI**

**- Guilherme Nolasco Tucunduva – RA: 82426695**

* ***Exercícios de Revisão, aula 7***

***Questões***

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

* **R:** Um pentest, é uma simulação controlada de um ataque cibernético contra um sistema, rede ou aplicação com o objetivo de identificar vulnerabilidades de segurança que poderiam ser exploradas por invasores reais. As etapas são: Planejamento e reconhecimento, numeração, ganho de acesso, escalada de privilégios, manutenção de Acesso, cobertura de rastros, relatório.

**2. Explique o funcionamento de 3 ataques de segurança cibernéticas que podem comprometer diretamente a disponibilidade de sistemas.**

* **R:** 1. Ataque DoS/DDoS (Denial of Service / Distributed Denial of Service)

Como funciona: O atacante envia uma grande quantidade de requisições ou dados para um servidor, serviço ou rede com o objetivo de sobrecarregar seus recursos (CPU, memória, largura de banda), fazendo com que ele fique lento ou totalmente indisponível. DoS (Denial of Service): ataque feito a partir de um único computador. DDoS (Distributed Denial of Service): ataque coordenado a partir de vários dispositivos (geralmente infectados, formando uma botnet). Seu impacto causa queda no sistema, perda de vendas, danos à reputação.

2. Ataque de Ransonware

Como funciona: O ransomware é um malware que criptografa os dados ou bloqueia o acesso ao sistema, exigindo um pagamento (resgate) para liberar o acesso novamente. Com seu impacto deixa sistemas críticos ficam indisponíveis até que os dados sejam recuperados.

3. Exploração de Recursos (Resource Exhaustion Attack)

Como funciona: O invasor envia comandos ou requisições que fazem o sistema consumir recursos excessivos como memória, processamento ou espaço em disco. Seu impacto deixa o servidor travado ou o reinicia, causando indisponibilidade.

**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)?**

* R: Conformidade, em inglês é conhecido como compliance.

**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.**

* **R: Firewall** é um recurso que controla o tráfego de rede com base em regras definidas, permitindo ou bloqueando acessos. Pode ser implementado via hardware ou software.

**IDS (Intrusion Detection System)** é um sistema de detecção de intrusos que apenas monitora o tráfego e gera alertas quando identifica atividades suspeitas, mas **não toma ações diretas**.

**IPS (Intrusion Prevention System)** é semelhante ao IDS, porém mais avançado: além de detectar, também **bloqueia automaticamente** ameaças em tempo real.

**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.**

* **R:** Criar senhas fortes, com letras, números e símbolos. Evitar usar a mesma senha em vários sites. Ativar a verificação em duas etapas sempre que possível.

**6. Observe a imagem a seguir. Do ponto de vista da segurança da informação identifique:**

**a) A vulnerabilidade;**

* **R:** O uso de um sistema operacional não original (pirata), isso pode ter falhas de segurança, ausência de atualizações e deixar o computador exposto a riscos.

**b) A ameaça;**

* **R**: Possibilidade de ataques, como vírus, malwares ou roubo de dados, justamente por causa da falta de proteção em um sistema pirata.

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

* **R:** Instalar uma versão original do Windows e manter o sistema sempre atualizado, além de usar antivírus confiável.

**7. Observe a imagem a seguir. Do ponto de vista da segurança da informação, identifique?**

**a) A vulnerabilidade;**

* **R:** Uso de nome de usuário padrão (admin), que é fácil de adivinhar.

**b) A ameaça;**

* **R:** Invasores podem acessar o sistema usando essas credenciais conhecidas.

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

* **R:** Trocar o nome de usuário e senha padrão por credenciais fortes e personalizadas.

**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;**

* **R:** Ana utiliza a chave pública de Bob para criptografar a mensagem, garantindo que somente ele, com a chave privada correspondente, consiga decifrá-la.

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

* **R:** Bob utiliza sua chave privada para decifrar a mensagem que foi cifrada com sua chave pública.

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

* **R:** Ana criptografa a mensagem (ou o hash dela) com sua chave privada, criando uma assinatura digital que garante que a mensagem é realmente dela e que não foi alterada.

**d) como Carlos deverá decifrar a mensagem de Ana corretamente.**

* **R:** Carlos usa a chave pública da Ana pra verificar a assinatura digital e, com isso, confirmar se a mensagem é mesmo dela e se não foi modificada.

**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.**

* R: O certificado digital assegura que apenas as partes envolvidas na transação (o cliente e o banco) possam acessar e ler os dados trocados. Isso acontece porque a mensagem é criptografada com a chave pública do destino (o banco) e só pode ser decifrada pela chave privada correspondente do banco.

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

* R: O certificado digital também garante que a transação tenha origem confiável (como o Banco do Brasil, no exemplo). Além disso, assegura que a mensagem não foi alterada durante o envio.

O uso de assinaturas digitais garante que qualquer modificação nos dados seja detectada, pois, caso os dados sejam alterados, a assinatura se torna inválida. E a data de validade no certificado digital dificulta a falsificação, pois limita o período em que ele pode ser usado, sendo automaticamente rejeitado após o vencimento.

Isso garante que qualquer tentativa de fraude no certificado seja detectada, evitando o uso de certificados expirados ou comprometidos e garantindo a verificação de sua autenticidade e integridade.

**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.**

* R: *Tentativas de login (bem-sucedidas e fracassadas):* ajudam a identificar acessos não autorizados ou suspeitos.

*Acessos a sistemas, arquivos ou informações sensíveis: i*ndicam quem acessou o quê, quando e por qual motivo.

*Alterações em configurações de sistema ou privilégios de usuário*: essenciais para rastrear mudanças críticas na infraestrutura.

Esses logs são fundamentais para detectar falhas, investigar incidentes e garantir conformidade com políticas de segurança.

* ***Estudo de caso, aula 7***

***Questões***

**1.** **O firewall e o servidor Web usados pela Linen Planet fornecem serviços de criptografia? Em caso afirmativo, que tipo de proteção estava em vigor?**

* **R:** Sim. O uso do protocolo HTTPS indica que há criptografia por SSL/TLS, protegendo os dados durante a transmissão entre navegador e servidor.

**2.** **Como o acesso ao servidor Web da Linen Planet poderia ser mais seguro?**

* **R:** O acesso seria mais seguro com autenticação multifator, uso de VPN, restrição de privilégios, e evitando o compartilhamento de senhas por telefone. Especialmente em locais públicos. Treinamento de segurança da informação também é essencial.
* ***Estudo de caso 2, aula 7***

***Questões***

**1. A política da ATI sobre o uso da Web parece dura para você? Por que ou por que não?**

* **R**: A política é rígida, mas compreensível em um ambiente corporativo que prioriza segurança e produtividade. No entanto, falta flexibilidade para lidar com situações pontuais de baixo risco.

**2. Você acha que Ron foi justificado em suas ações?**

* **R:** Embora compreensível pelo esforço e contexto, Ron desrespeitou uma norma clara da empresa. A ação foi emocionalmente justificável, mas tecnicamente incorreta.

**3. Como Andy deve reagir a essa situação se Ron é conhecido por ser um funcionário confiável e diligente?**

* **R:** Andy deve agir com equilíbrio: conversar com Ron, reforçar as políticas da empresa e ajudá-lo a resolver a situação, evitando punições severas e promovendo aprendizado.