Heloisa Soares Ferreira RA: 824152581

Exercicios de revisão:

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

Pentest (Penetration Test) é um teste de penetração utilizado para identificar vulnerabilidades em sistemas, redes ou aplicativos, explorando-as como um atacante faria.

Etapas de um pentest:

- Planejamento e reconhecimento: Entendimento do escopo e coleta de informações sobre o alvo.
- Varredura: Utilização de ferramentas para identificar vulnerabilidades e entender como o alvo responde a ataques.
- Obtenção de acesso: Tentativa de explorar as vulnerabilidades descobertas.
- Manutenção do acesso: Verificar se o acesso pode ser mantido para ataques futuros.
- Relatório: Documentar os resultados, vulnerabilidades descobertas e recomendações de mitigação.

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

- **DDoS (Distributed Denial of Service)**: Inunda o sistema com tráfego excessivo, fazendo com que ele se torne indisponível.
- **Ransomware**: O software malicioso criptografa arquivos e torna o sistema inutilizável até que um resgate seja pago.
- **Ataque de Exaustão de Recursos**: Consome os recursos de um sistema (como CPU ou memória) através de solicitações repetitivas ou maliciosas, causando falha ou lentidão.

3 - Conceito relacionado ao cumprimento de requisitos de segurança, regulamentos internos e acordos internacionais (em uma palavra)?

Conformidade.

4 - **Comparação entre firewalls, IDS e IPS**:

- **Firewall**: Monitora e controla o tráfego de rede, atuando como uma barreira entre redes confiáveis e não confiáveis.
- **IDS (Intrusion Detection System)**: Sistema de detecção de intrusões que monitora atividades suspeitas e gera alertas, mas não toma ações corretivas.
- **IPS (Intrusion Prevention System)**: Sistema de prevenção de intrusões que não apenas detecta atividades suspeitas, mas também bloqueia ações maliciosas automaticamente.

5 - **Três conselhos para proteger senhas**:

- Use senhas longas e complexas, combinando letras, números e caracteres especiais.
- Ative a autenticação de dois fatores (2FA) sempre que possível.
- Utilize um gerenciador de senhas para armazenar suas credenciais com segurança.

6 - Do ponto de vista da segurança da informação, identifique:

- **a) Vulnerabilidade**: Qualquer falha ou fraqueza em um sistema que pode ser explorada.
- **b) Ameaça**: O possível risco ou agente que pode explorar a vulnerabilidade (por exemplo, um invasor).
- **c) Ação defensiva**: Implementar patches de segurança, firewalls, ou monitoramento contínuo para mitigar a ameaça.

8 - Ana deseja criptografar mensagens para Bob e Carlos. Como deve fazer?

- **Para Bob**:
  - **Cifrar para Bob**: Ana deve usar a chave pública de Bob para criptografar a mensagem.
  - **Decifrar por Bob**: Bob deve usar sua chave privada para decifrar a mensagem.
- **Para Carlos**:
  - **Cifrar para Carlos**: Ana deve assinar digitalmente a mensagem usando sua chave privada, provando a autenticidade.
  - **Decifrar por Carlos**: Carlos usará a chave pública de Ana para verificar a assinatura e garantir que a mensagem é legítima.

9 - **a)** O certificado digital é utilizado para garantir a autenticação entre o cliente e o servidor, criptografando as informações trocadas. O Banco do Brasil utiliza sua chave privada para criar assinaturas digitais, enquanto os usuários utilizam a chave pública para verificar a autenticidade e garantir a integridade dos dados.

9- **b)** Benefícios de segurança:

Confidencialidade: As informações trocadas são criptografadas, protegendo contra interceptação.

Autenticidade: Garante que o site é legítimo e que as informações vêm de uma fonte confiável.

10 - **Três registros importantes para auditoria de segurança (conforme ISO 27002:2013)**:

- Registros de login/logout dos usuários.
- Registros de acessos a dados confidenciais.
- Registros de tentativas de falhas ou acessos não autorizados.

Heloisa Soares Ferreira RA: 824152581

Atividade caso de uso 1:

1. Políticas de Acesso e Controle de Usuários

Políticas Propostas

- **Autenticação de Usuários**: Todos os funcionários devem usar senhas fortes e únicas.
- **Revisão de Acesso**: As permissões de acesso devem ser revisadas mensalmente para garantir que apenas os usuários autorizados mantenham o acesso.

Justificativa

Essas medidas ajudam a diminuir o risco de acessos não autorizados por pessoas de fora da organização e garantem que os dados sensíveis sejam acessados apenas por usuários que realmente necessitam.

2. Política de Uso de Dispositivos Móveis e Redes

Políticas Propostas

- **Uso de Dispositivos Móveis**: Os funcionários devem usar apenas dispositivos autorizados para acessar informações da empresa. Dispositivos pessoais podem ser utilizados apenas sob condições pontuais e monitoradas.
- **Proibição de Redes Públicas**: O uso de redes Wi-Fi públicas para acessar dados da empresa é proibido, a menos que uma VPN autorizado pela organização esteja em uso.

Justificativa

Essas políticas garantem que os dados da empresa permaneçam protegidos, mesmo quando acessados fora do ambiente corporativo.

3. Diretrizes para Resposta a Incidentes de Segurança

Políticas Propostas

- **Identificação de Incidentes**: Todos os colaboradores devem ser treinados para identificar e relatar incidentes de segurança imediatamente.
- **Equipes de Resposta a Incidentes**: Contratar uma empresa especializada em consultoria de segurança da informação para responder rapidamente a incidentes de segurança.

Justificativa

Uma resposta rápida e organizada é fundamental para limitar o impacto dos incidentes e proteger a integridade dos dados da empresa.

4. Política de Backup e Recuperação de Desastres

Políticas Propostas

- **Armazenamento Seguro**: Os backups devem ser armazenados em local seguro, com uma cópia off-site para proteger contra desastres locais.
- **Teste de Recuperação**: Recuperações de backup devem ser testadas trimestralmente para garantir a eficácia do plano.

Justificativa

Um bom plano de backup e recuperação é essencial para garantir a continuidade dos negócios e a integridade dos dados, minimizando o impacto de falhas ou desastres.

Atividade caso de uso 2

Heloisa Soares Ferreira RA: 824152581

Questões – 01

A) 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: É citado o serviço de criptografia no texto, porém não foi colocada uma chave, pública ou privada, de segurança.

B) Como o acesso ao servidor Web da Linen Planet poderia ser mais seguro?

R: Poderia ser usado a autenticação de dois fatores, tendo assim uma política de privacidade mais segura.

Questões – 02

A) A política da ATI sobre o uso da Web parece dura para você? Por que sim ou por que não?

R: Não. É uma política adequada para o ambiente de trabalho, a fim de evitar distrações e coisas do tipo, além de impedir o acesso mesmo que por descuido em links maliciosos

B) Você acha que Ron foi justificado em suas ações?

R: Sim, após terminar o trabalho ele achou que teria certo direito de ter essa regalia, algo justo a meu ver. Se o trabalho está pronto e estava próximo ao horário de saída não há por que "prende-lo"

C) Como Andy deve reagir a essa situação se Ron é conhecido por ser um funcionário confiável e diligente?

R: De forma amigável, apenas reforçando a política da empresa e pontuando que é não há nenhum problema, contanto que não se repita futuramente.