Atividade 1 – Fundamentos de Segurança da Informação

O que é um Pentest?

Um teste de penetração (pentest) é uma simulação controlada de ataque cibernético com o objetivo de identificar falhas de segurança em sistemas, redes ou aplicações. Ele ajuda a entender como um invasor real poderia explorar essas vulnerabilidades.

Principais etapas:

- **Mapeamento:** identificação de ativos e serviços expostos.
- **Exploração:** tentativa de invasão usando falhas encontradas.
- **Escalada de privilégios:** busca por acesso mais amplo dentro do sistema.
- **Ocultação:** simulação de técnicas para evitar detecção.

Três ataques que afetam a disponibilidade de sistemas

1. **DDoS (Negação de Serviço Distribuída):** sobrecarrega servidores com tráfego falso, tornando serviços indisponíveis.
2. **Ransomware:** bloqueia o acesso a arquivos ou sistemas até que um resgate seja pago.
3. **Wiper (Malware destrutivo):** apaga dados de forma irreversível, comprometendo a continuidade do serviço.

Conceito-chave: Conformidade

O trecho citado trata da **conformidade**, que é o alinhamento da empresa com leis, normas internas, contratos e acordos internacionais. É essencial para garantir a segurança da informação e evitar penalidades legais.

Comparativo: Firewall, IDS e IPS

Dicas para proteger senhas

1. Crie senhas longas e complexas, misturando letras, números e símbolos.
2. Use senhas diferentes para cada serviço.

3. Ative a autenticação em dois fatores (2FA) sempre que possível.

Análise de vulnerabilidade em sistemas

Exemplo 1:

- Vulnerabilidade: uso de sistema pirata sem atualizações.
- Ameaça: infecção por vírus e falhas de segurança.
- Defesa: instalar sistema original ou versão open source atualizada.

Exemplo 2:

- Vulnerabilidade: uso de login padrão e senha fraca.
- Ameaça: invasão por força bruta.
- Defesa: trocar o nome de usuário e usar senhas fortes e únicas.

Criptografia: mensagens entre Ana, Bob e Carlos

- Para Bob (sigilo):
    - Ana cifra com a chave pública de Bob.
    - Bob decifra com sua chave privada.
- Para Carlos (autenticidade):
- Ana cifra com sua própria chave privada.
- Carlos verifica com a chave pública de Ana.

Certificados digitais e segurança

Como funciona:

O certificado digital contém uma assinatura feita com a chave privada do emissor (ex: Banco do Brasil). O destinatário usa a chave pública do banco para verificar a autenticidade e integridade da mensagem.

Benefícios:

1. Garante que a mensagem veio realmente do banco (autenticação).
2. Assegura que o conteúdo não foi alterado (integridade).
3. Impede que o emissor negue o envio (não-repúdio).

Registros importantes para auditoria

1. Identificação dos usuários (login utilizado).
2. Datas e horários de entrada e saída do sistema.
3. Tentativas de acesso, tanto bem-sucedidas quanto negadas.

Atividade 2 – Segurança em Ambientes Web

Criptografia no site da Linen Planet

Sim, o site utilizava criptografia, como indicado pelo ícone de segurança e pela mensagem sobre conexão protegida. A proteção em vigor era a criptografia durante a transmissão dos dados (SSL/TLS), que impede que terceiros leiam as informações trocadas.

Como melhorar a segurança do acesso

1. **Autenticação em dois fatores (MFA):** mesmo com a senha, o invasor não acessaria sem o segundo fator.
2. **Treinamento e políticas claras:** proibir o compartilhamento de senhas e orientar sobre cuidados com informações sensíveis.
3. **Acesso via VPN:** restringir o acesso remoto a sistemas críticos apenas por redes seguras.

Atividade 3 – Políticas de Uso e Ética

A política da ATI é rígida?

Não. Restringir o acesso a categorias de sites é uma prática comum em ambientes corporativos. Isso ajuda a evitar riscos de segurança, como infecção por malware, e garante que os recursos da empresa sejam usados para fins profissionais.

Ron agiu corretamente?

Não. Mesmo sendo um bom funcionário, ele sabia que a política da empresa proibia o acesso irrestrito à internet e tentou burlar essa regra. Isso representa uma violação consciente das normas internas.

Como Andy deve lidar com a situação?

Andy deve agir com equilíbrio. Ele pode:

- Informar o setor de segurança sobre o ocorrido, explicando que foi um erro de julgamento.
- Solicitar a reativação do acesso de Ron, destacando seu histórico positivo.
- Conversar com Ron para reforçar a importância das políticas de segurança.
- Garantir que Ron participe do treinamento obrigatório, encerrando o caso de forma educativa.