ATIVIDADE 1.

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

Resposta: Pentest (ou teste de penetração) é um método de avaliação de segurança que simula ataques reais para identificar e explorar vulnerabilidades em sistemas, aplicativos ou redes.

As principais etapas são: varredura, exploração, elevação de privilégios e ocultação.

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

Resposta:

1. **DDoS (Distributed Denial of Service)**
2. **Ransomware**
3. **Wiper / Malware destrutivo**

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)?

Resposta: 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.

Recurso	Função principal	Atuação	Ação tomada	Tipo de proteção
Firewall	Controla o tráfego de rede	Preventiva	Bloqueia ou permite pacotes conforme regras	Filtragem de acesso
IDS (Intrusion Detection System)	Detecta atividades suspeitas	Passiva	Apenas alerta sobre invasões ou anomalias	Detecção
IPS (Intrusion Prevention System)	Detecta e bloqueia ataques em tempo real	Ativa	Interrompe o tráfego malicioso automaticamente	Prevenção

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.

1- **Use senhas fortes, com letras, números e símbolos.**
2- **Não repita a mesma senha em vários sites.**
3- **Ative a autenticação em dois fatores (2FA).**

6) Observe a imagem a seguir.

Do ponto de vista da segurança da informação, identifique:

a) Vulnerabilidade: Uso de sistema operacional pirata que não recebe atualizações.
b) Ameaça: Infecção por malware, falhas de segurança e baixo desempenho.
c) Ação defensiva: Substituir o sistema não licenciado por uma versão legítima ou por um sistema open source atualizado.

7) Do ponto de vista da segurança da informação, identifique:

a) Vulnerabilidade: Uso de credenciais fracas e nome de usuário padrão (“admin”).
b) Ameaça: Facilita a invasão do sistema por força bruta ou adivinhação de senha.
c) Ação defensiva: Alterar nomes de usuários administrativos e usar senhas fortes e únicas.

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: usando a chave pública de Bob.

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

c) como Ana deverá cifrar a mensagem antes de enviar para Carlos: usando a sua chave privada.

d) como Carlos deverá decifrar a mensagem de Ana corretamente: usando a chave pública de Ana.

9) Observe as imagens a seguir:

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.

Resposta: A CA Sectigo gera um resumo (hash) dos dados de identificação do banco. Esse hash é criptografado com a chave privada do banco, formando a assinatura digital.

Para validar, o cliente decifra a assinatura com a chave pública do banco (presente no certificado) e recalcula o hash da mensagem recebida. Se ambos os valores coincidirem, a mensagem é autêntica e íntegra.

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

Resposta:

1- **Autenticação da origem: garante que as mensagens realmente foram enviadas pelo Banco do Brasil.**
2- **Integridade: assegura que as mensagens não foram alteradas durante a transmissão.**
3- **Não-repúdio: impede que o Banco negue a autoria das mensagens enviadas.**

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.

RESPOSTA:

a) Identificação dos usuários (ID).
b) Datas, horários e detalhes de logon e logoff.
c) Registros das tentativas de acesso ao sistema, aceitas e rejeitadas.

ATIVIDADE 2.

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?

Resposta: Sim. O texto confirma que havia criptografia, indicada pelo "ícone de segurança" e pela frase "A criptografia entre seu navegador e o servidor estava agora em vigor". O tipo de proteção era a criptografia em trânsito (SSL/TLS), que protege os dados *durante* a transmissão, impedindo que sejam lidos na rede.

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

O acesso poderia ser mais seguro com:

1. **Autenticação Multifator (MFA): Exigir um segundo fator (como um código de app) além da senha. A invasora tinha a senha, mas não o celular da CTO.**
2. **Treinamento e Políticas: Criar uma política clara que proíba o compartilhamento de senhas e treinar funcionários (especialmente a alta gestão) para não discutir informações sensíveis em público.**
3. **Controles de Acesso: Exigir uma VPN para acesso externo a sistemas críticos, em vez de expô-los diretamente à internet.**

ATIVIDADE 3.

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

Não, a política de bloquear categorias de sites (como fotos/viagens) não é dura; é uma prática de segurança corporativa padrão, pois o proxy está agindo como um firewall de nível de aplicativo. Ele não bloqueia apenas URLs, mas categorias. Sites de "Fotos" ou "Viagem", mesmo que legítimos, são vetores comuns de *malware*, sendo assim, a empresa está mitigando um risco real.

Além do mais, a política garante que a largura de banda e os recursos da empresa sejam usados para fins comerciais, não para navegação pessoal.

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

Não. Do ponto de vista da ética corporativa e da segurança, Ron não foi justificado.

O caso afirma que "Ron sabia que a ATI não permitia a navegação indiscriminada" e estava ciente da existência do servidor proxy, não existe justificativa para violar conscientemente uma política da empresa usando ativos corporativos. Ele sabia que era errado e fez mesmo assim.

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

Andy deve equilibrar a necessidade de aplicar a política da empresa com a gestão de um bom funcionário. Ele deve tratar o caso como um incidente de aprendizado, e não como uma quebra de confiança que exija punição severa.

Andy deve seguir as instruções do e-mail. Ele deve contatar o grupo de segurança, informar que Ron não tinha um "propósito comercial legítimo, mas que foi um lapso de julgamento de um funcionário que acabou de concluir um projeto exaustivo. Ele deve solicitar o restabelecimento do acesso de Ron.

Além do mais, Andy deve ter uma conversa privada com Ron. Ele deve reconhecer o trabalho duro de Ron, mas reforçar que a as políticas de segurança são sérias.

Por último, ele deve garantir que Ron se inscreva no curso de treinamento exigido, tratando-o como uma formalidade necessária para fechar o "ticket" do incidente com o RH e a segurança.