**Atividade**

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

Um penetration test (teste de penetração) é um “teste de invasão autorizado”.  
A ideia é simular o trabalho de um invasor para descobrir falhas antes que um criminoso real as explore.

Planejamento – combinam‑se objetivo, escopo e permissão legal.

Coleta de informações (reconhecimento) – pesquisam‑se dados públicos e tecnologias usadas pelo alvo.

Varredura e enumeração – escaneiam‑se portas e serviços para listar possíveis pontos fracos.

Exploração – tentam‑se explorar as vulnerabilidades encontradas.

Pós‑exploração – verifica‑se até onde é possível avançar (aumentar privilégios, acessar dados).

Relatório – documentam‑se falhas, provas de exploração e recomendações de correção.

Re‑teste (opcional) – executa‑se um novo teste depois que o cliente corrige as falhas.

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

DISPONIBILIDADE de sistemas.

Dos/ddos (negação de serviço) – um único computador (dos) ou uma rede de máquinas zumbis (ddos) bombardeia o servidor com requisições até esgotar CPU, memória ou banda. Resultado: o serviço fica extremamente lento ou cai.

Ransomware – malware que criptografa arquivos ou discos inteiros e exige pagamento para liberar a chave. Enquanto isso, usuários e sistemas não conseguem acessar os dados.

Sabotagem de DNS – sobrecarga ou envenenamento de servidores DNS, impedindo que nomes de domínio sejam resolvidos. Mesmo que o site continue on‑line, ninguém consegue chegar a ele.

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)?

Compliance – a necessidade de cumprir leis, políticas internas, contratos e acordos.

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.

Firewall: filtro na borda; só deixa passar o tráfego que obedece às regras.

IDS: só espia o tráfego; detecta anomalias e avisa.

IPS: fica no caminho; detecta e bloqueia na hora.

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.

Pensou por um segundo

Gerenciador de senhas: gere e armazene senhas fortes com uma única senha mestra.

MFA: ative dois fatores para exigir um segundo código além da senha.

Sem reciclar: use senhas diferentes para cada serviço.

6) Observe a imagem a seguir.

Do ponto de vista da segurança da informação, identifique:

A) A vulnerabilidade

Uso ou disponibilidade de software não original/pirateado dentro da empresa.

B) A ameaça

Instalador adulterado conter malware‑espionagem ou backdoor que comprometa sistemas e dados.

C) Uma ação defensiva para mitigar a ameaça

Adotar política de licenciamento estrito – somente software adquirido de canais oficiais; varreduras periódicas para detectar cópias ilegais; conscientização dos usuários sobre os riscos.

7) Observe a imagem a seguir.

Do ponto de vista da segurança da informação, identifique:

A) A vulnerabilidade o usuário esta opcional ou seja qualquer um pode entrar

B) A ameaça acesso indevido

C) Uma ação defensiva para mitigar a ameaça colocar cadastro obrigatório

8) Ana tem duas mensagens para enviar de forma criptografada para dois amigos: Bob e Carlos. Bob deseja receber aMensagem 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 cifra a mensagem com a chave pública de Bob.

B) como Bob deverá decifrar a mensagem de Ana corretamente;

Correspondente

C) como Ana deverá cifrar a mensagem antes de enviar para Carlos;

Ana assina/cifra a mensagem com sua própria chave privada

D) como Carlos deverá decifrar a mensagem de Ana corretamente.

Se abrir, sabe que veio dela.

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.

Servidor BB: guarda a chave privada; prova quem é e lê o segredo de sessão.

Cliente: recebe o certificado, valida‑o e usa a chave pública do banco para cifrar o segredo inicial.

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

Banco.

Autentica o site oficial (evita phishing).

Criptografa e integra o tráfego (ninguém lê ou altera a transação).

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.

Autenticação e logon/logoff de usuários (data, hora, origem, sucesso ou falha).

Acesso ou alteração a arquivos sensíveis ou configurações críticas.

Tentativas de privilégio elevado (execução de comandos administrativos, uso de sudo, alteração de grupo/root).

**Estudo de caso 2**

Trabalhando com servidores proxy e firewalls em nível de aplicativo\*

Ron Hall estava sonhando com suas próximas férias. Ele trabalhava para Andy Ying, gerente do

grupo de consultoria de segurança, em um projeto muito exigente, há quase seis meses.

Hoje ele finalmente terminou o trabalho e teve alguns minutos para navegar na Web e planejar

sua próxima viagem à Nova Zelândia.

Ron sabia que a ATI não permitia a navegação indiscriminada na Web e que eles usavam um

servidor proxy para garantir a conformidade com essa política, mas ele sentiu que merecia esse

tratamento e acreditava que Andy não teria problemas com um pouco de navegação recreativa

na Web. Além disso, eram quase 17h e estava quase na hora de ir para casa.

O Google foi autorizado pelo servidor proxy, então Ron foi até lá para iniciar sua busca. Ele

digitou “pontos de férias na Nova Zelândia”. Mais rápido do que ele conseguia piscar, o gigante

mecanismo de busca Google voltou com uma lista de links relevantes. A primeira entrada

parecia promissora: “New Zealand Tourism Online: New Zealand Travel Guide”. Mas o segundo

ficou ainda melhor: “Fotos da Nova Zelândia”. Ele clicou nesse URL.

Nenhuma imagem foi aberta. Nada de vales verdes. Sem recifes de coral. Nada de belas

montanhas. Apenas uma tela branca com letras pretas que diziam:

ACESSO PROIBIDO — ENTRE EM CONTATO COM O ADMINISTRADOR DO PROXY SERVER PARA

INSTRUÇÕES DE COMO ACESSAR O CONTEÚDO SOLICITADO.

Ron não ficou surpreso, mas esperava. Ele clicou no botão “Voltar” e tentou o próximo link. Ele

recebeu a mesma mensagem. Ele tentou mais três ou quatro vezes e então percebeu que não

estava conseguindo nenhuma foto hoje.

Ron chegou à sua mesa um pouco cedo na manhã seguinte. Ele ligou seu PC e foi tomar uma

xícara de café enquanto ele inicializava. Quando voltou, abriu seu programa de e-mail. Na lista

de novos e-mails havia uma nota do grupo de segurança de rede. Ele abriu a mensagem e viu

que tinha sido endereçada a ele e a Andy Ying, seu chefe. Também tinha um CC para o

departamento de RH. A mensagem dizia:

Recentemente, sua conta foi usada para acessar conteúdo da Web que não foi aprovado para

uso dentro da ATI. Estamos pedindo que você explique suas ações ao seu supervisor. Você é

encorajado a se matricular em um curso sobre uso apropriado da Internet na ATI o quanto antes.

Até que você complete a aula ou seu supervisor entre em contato com este escritório, seus

privilégios de rede foram suspensos. Se esta tentativa de acesso foi para fins comerciais

legítimos, peça ao seu supervisor que nos notifique imediatamente para que este local da Web

possa ser adicionado à lista de locais da Web aprovados pela ATI.

Que aborrecimento. Ron não estava ansioso por sua conversa com Andy.

Questões

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

É rígida, mas tem razão de ser: proteger a rede e manter o foco no trabalho. Ainda assim, poderia prever exceções claras para pequenos usos pessoais depois do expediente.

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

Ele queria um descanso após meses de esforço, algo fácil de compreender. No entanto, conhecia a regra e, ao ignorá‑la, assumiu o risco de sanção.

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

e diligente?

Conversar com Ron, reconhecer seu bom histórico e explicar por que a regra existe. Solicitar à segurança de TI a liberação rápida do acesso, tratando o caso como deslize isolado, e propor ajustes na política que contemplem pausas curtas e seguras no futuro.

**Estudo de caso 1**

Criptografia e Firewalls

Padma Santhanam, a CTO da Linen Planet, estava se deslocando para o trabalho de sua maneira habitual – pegando o

trem da estação suburbana perto de sua casa para seu escritório em uma área comercial do outro lado da cidade. Ao

virar a página do jornal da manhã, seu celular tocou. Ela olhou para o identificador de chamadas e viu que era seu

assistente, David Kalb.

"Olá, David. E aí?"

“Oi, Padma. Crise aqui como sempre. Nosso representante de atendimento ao cliente na ATI está na outra linha. Ele

diz que você precisa fazer login no sistema de ordem de serviço e aprovar a solicitação de alteração o mais rápido

possível ou eles perderão a próxima janela de alteração para a nova versão do nosso aplicativo de crédito online.”

Padma disse: “Tudo bem. Estarei no escritório em 25 minutos ou mais. O trem acabou de sair da estação Broadmore.”

“Ele diz que eles não podem esperar tanto tempo. Você deveria fazer isso anteontem, e de alguma forma foi

esquecido. Eles dizem que precisam agora ou perderemos uma semana esperando pela próxima janela de mudança.”

Padma suspirou. Então ela disse: “Tudo bem. Eu quero que você navegue no site da ordem de serviço, você sabe o

que usamos em linhoplanet.biz/wo, e faça login para mim. Você pode aprovar o pedido de alteração e não perderemos

a janela. Vou mudar minha senha quando chegar lá. Meu nome de usuário é papa, serra, alfa, novembro, tango, alfa.

Percebido?"

David disse “Entendi. Senha?" Olhando para os dois lados primeiro, Padma abaixou um pouco a voz e disse: “Romeu,

lima, oito, quatro, bang, zulu, índia, vencedor, cifrão.”

David repetiu de volta. Ele disse: “OK, estou logado agora e acabei de aprovar a ordem de serviço. Vou dizer ao nosso

representante que estamos prontos para ir.”

“Obrigado, Davi.”

Na fila atrás de Padma, Maris Heath fechou o bloco de notas e fechou a caneta esferográfica. Sorrindo, ela ergueu a

bolsa do laptop e se levantou para sair do trem na próxima estação, que ela sabia que ficava bem ao lado de um

cibercafé. Maris abriu seu laptop e conectou seu navegador ao servidor Linen Planet Web. O firewall pediu seu nome

de usuário e senha. Ela abriu o bloco de notas e digitou os dados que havia anotado enquanto escutava a ligação do

celular de Padma. Seu navegador conectou em um instante. Ela notou que o ícone de segurança estava aparecendo

na parte inferior da janela do navegador. A criptografia entre seu navegador e o servidor estava agora em vigor. Pelo

menos nenhum outro hacker poderia observá-la enquanto ela colocava um backdoor nos servidores da Web do Linen

Planet.

Ela passaria várias horas nos próximos dias explorando a rede e planejando seu ataque...

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?

Sim, o servidor Web e o firewall fornecem criptografia. O ícone de segurança no navegador de Maris indica que a comunicação foi protegida com HTTPS, utilizando SSL/TLS. Isso garante que a transmissão de dados entre o cliente e o servidor foi criptografada e segura contra interceptações.

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

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

* MFA (autenticação multifatorial): Adicionar um segundo fator de autenticação para mais segurança.
* Senhas fortes: Usar senhas complexas e únicas, sem compartilhamento inseguro.
* Monitoramento: Detectar atividades suspeitas e alertar sobre acessos não autorizados.
* Criptografia ponta-a-ponta: Garantir que dados sensíveis também sejam criptografados ao serem armazenados.
* Autenticação com certificados digitais: Usar certificados em vez de senhas, dificultando o acesso para invasores.