**Universidade São Judas Tadeu**

Anabelly Salles

Carolina Santos

Maria Eduarda Souza

# Estudos de Caso e Questionário:

# Análise de Risco

**São Paulo**

**2024**

## 1° Estudo de Caso

**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:** O servidor Web da Linen Planet utiliza criptografia. Isso é mostrado pelo ícone de segurança visto por Maris na janela de seu navegador, que representa a presença de uma conexão criptografada. Essa criptografia provavelmente foi implementada por meio de SSL (Secure Sockets Layer) ou TLS (Transport Layer Security), que garantem a proteção dos dados transmitidos entre o navegador e o servidor, prevenindo que sejam interceptados por terceiros.

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

Para aumentar a segurança do servidor Web da Linen Planet, algumas outras medidas poderiam ser tomadas, como por exemplo introduzir uma segunda etapa de verificação além da senha, como um código por exemplo gerado por um aplicativo ou enviado por SMS, garantiria maior proteção. Uma política de senhas mais seguras, a prática de Padma de compartilhar sua senha por telefone foi uma grande falha, nesse ato ele colocou várias coisas em risco, colocando uma política de senha ele terá melhor segurança, uma das medidas a serem tomadas pode ser senhas mais complexas, trocadas regularmente, e um protocolo que proíba o compartilhamento de senhas por meios inseguros, como por exemplo, por ligação de celular.

## 2° Estudo de Caso

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

**Resposta:** A política da ATI pode parecer rígida, mas faz sentido, especialmente porque a empresa quer garantir que os funcionários usem a internet de maneira responsável. Em empresas que lidam com informações sensíveis, como dados de clientes ou projetos importantes, é comum bloquear sites que não estão relacionados ao trabalho. Isso é feito para proteger a rede contra vírus ou ataques, além de garantir que os funcionários fiquem focados em suas tarefas.

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

**Resposta:** Embora Ron tenha trabalhado duro e achasse que merecia um descanso, suas ações não foram corretas porque ele sabia da regra e tentou acessá-la várias vezes. Mesmo que fosse quase o final do expediente, ele ainda estava no trabalho, onde a política de uso da internet é clara. Ele deveria ter esperado até estar em casa para fazer sua pesquisa sobre férias.

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

**Resposta:** Se Andy sabe que Ron é um funcionário responsável e trabalhador, ele pode ser mais compreensivo na conversa. Ele poderia usar a situação como um momento de aprendizado para Ron, explicando que as regras são importantes para todos, mas sem punições severas. Andy também poderia recomendar que Ron fizesse o curso sobre uso apropriado da internet, conforme o e-mail sugeriu, para garantir que Ron entenda completamente a política da empresa e evite futuros problemas.

## Questões

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

Resposta 1: “pentest” é um teste de penetração de simulação de ataque autorizado. Os testadores usam as mesmas ferramentas, técnicas e processos que os invasores para encontrar e demonstrar os impactos comerciais dos pontos fracos em um sistema, simulando uma variedade de ataques que poderia ameaçar uma empresa.

Resposta 2:

1) Planejamento e preparação

A função de um testador de penetração é planejar e preparar o processo de teste, o que inclui identificar o escopo do teste, os sistemas que serão testados e o cronograma do teste;

2) Coleta de informações

Para iniciar o processo, coletar o máximo de informações sobre o sistema-alvo (endereços IP, nomes de domínio, mapas e nomes de rede ou de domínio, servidores de e-mail, entre outros), para entender melhor o funcionamento do alvo e suas possíveis vulnerabilidades. Visa, portanto, identificar possíveis pontos fracos que podem ser explorados na próxima fase;

3) Varredura

Entender como o aplicativo de destino responderá a várias tentativas de invasão. Executada geralmente por meio da análise estática, que consiste em inspecionar o código de um aplicativo para estimar a maneira como ele se

comporta durante a execução. Essas ferramentas podem examinar todo o código em uma única passagem.
Há também o meio de análise dinâmica, que inspeciona o código de um aplicativo em um estado de execução. Essa é uma forma mais prática de varredura, pois fornece uma visão em tempo real do desempenho de um aplicativo.

4) Obter acesso

Esta etapa usa ataques a aplicativos da Web, como cross-site scripting, injeção de SQL e backdoors, para descobrir as vulnerabilidades de um alvo. Em seguida, os testadores tentam explorar essas vulnerabilidades, normalmente aumentando privilégios, roubando dados, interceptando tráfego etc., para entender os danos que podem causar.

5) Manter o acesso

O objetivo desta etapa é verificar se a vulnerabilidade pode ser usada para obter uma presença persistente no sistema explorado, por tempo suficiente para que um agente mal-intencionado obtenha acesso profundo. A ideia é imitar as ameaças persistentes avançadas, que geralmente permanecem em um sistema por meses para roubar os dados mais confidenciais de uma organização.

6) Relatórios e comunicações

O testador deve preparar um relatório detalhado das descobertas e recomendações para a empresa, que deve incluir um resumo do processo de teste, as vulnerabilidades identificadas e o impacto que elas podem ter sobre a segurança da empresa. O testador deve também se comunicar com a gerência e as equipes técnicas da empresa para garantir que elas entendam as vulnerabilidades e como resolvê-las, e fornecer orientação e suporte para os esforços de correção.
Ao final desse processo, o testador deve continuar a aprender e aprimorar suas habilidades para se manter atualizado com as ameaças e vulnerabilidades de segurança mais recentes.

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

Resposta: Os ataques de Negação de Serviço (DoS/DdoS) sobrecarregam sistemas com um grande volume de requisições, tornando-os inacessíveis aos usuários legítimos. Ransomware sequestra e criptografa dados ou sistemas, exigindo resgate, e resultando na indisponibilidade imediata de operações essenciais. Já os ataques de corte de energia visam infraestruturas críticas, como redes elétricas, causando apagões que afetam sistemas e serviços, sendo de alto risco para serviços públicos. Todos esses ataques comprometem diretamente a disponibilidade dos sistemas.

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: O conceito é 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.

Resposta:

| Recurso | Função Principal | Modo de Operação | Ação em Caso de Ameaça | Vantagem Principal | Desvantagem |
|---|---|---|---|---|---|
| Firewall | Controla o tráfego de rede, permitindo ou bloqueando pacotes com base em regras predefinidas. | Atua na camada de rede (filtro de pacotes) e camada de aplicação (proxy). | Bloqueia ou permite pacotes com base nas regras configuradas. | Protege contra acessos não autorizados e filtra o tráfego. | Pode não detectar ataques mais sofisticados ou internos. |
| IDS (Sistema de Detecção de Intrusão) | Monitora o tráfego de rede ou atividades de sistema para detectar atividades suspeitas. | Atua de forma passiva, analisando e alertando administradores sobre possíveis ameaças. | Gera alertas e logs, mas não interfere no tráfego. | Detecta atividades suspeitas e pode ser configurado para vários tipos de ataques. | Não bloqueia ataques diretamente, apenas alerta. |
| IPS (Sistema de Prevenção de Intrusão) | Monitora e bloqueia o tráfego de rede suspeito para prevenir intrusões. | Atua de forma ativa, analisando e bloqueando tráfego em tempo real. | Bloqueia automaticamente o tráfego suspeito com base nas políticas definidas. | Previne ataques em tempo real, bloqueando-os antes de causarem danos. | Pode gerar falsos positivos, interrompendo o tráfego legítimo. |

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

Resposta:
Não abra o seus aplicativos de banco em redes de wifi públicas
Crie senhas fortes, que não tenham uma sequencia ordenada. Tenha o costume de alterar sua senha periodicamente.
Tenha a VPM do seu celular ativada e sempre  monitorando as atualizações do seu dispositivo.

6) Observe a imagem a seguir.

Do ponto de vista da segurança da informação, identifique:
a) A vulnerabilidade: Falsificação do sistema.
b) A ameaça: Provável infecção por malware.
c) Uma ação defensiva para mitigar a ameaça: Formatação do computador e exclusão das cópias.

7) Observe a imagem a seguir.

Do ponto de vista da segurança da informação, identifique:
a) A vulnerabilidade: User Name muito fraca quando falamos em segurança e prevenção.
b) A ameaça: Mais facilidade de acesso a conta do usuário devido ao user name fracos.
c) Uma ação defensiva para mitigar a ameaça: Atualizar o User Name para um nome mais difícil de decifrar.

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;
b) como Bob deverá decifrar a mensagem de Ana corretamente;
c) como Ana deverá cifrar a mensagem antes de enviar para Carlos;
d) como Carlos deverá decifrar a mensagem de Ana corretamente.

Resposta:
Mensagem para Bob (sigilo): Ana cifra a mensagem com a chave pública de Bob, e Bob decifra com sua chave privada. Apenas Bob pode ler a mensagem.
Mensagem para Carlos (autenticidade): Ana cifra a mensagem com sua chave privada para garantir autenticidade. Carlos decifra usando a chave pública de Ana, confirmando que foi ela quem enviou.
Esse processo garante tanto a privacidade (para Bob) quanto a autenticação (para Carlos).

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

Resposta:

a) Utilização do certificado na origem e no destino e chaves criptográficas do Banco do Brasil

O certificado digital do Banco do Brasil contém sua chave pública, que é enviada ao navegador do usuário ao acessar o site. O usuário utiliza essa chave pública para criptografar informações sensíveis, garantindo que apenas o banco, com sua chave privada, possa decifrá-las. Além disso, o banco utiliza sua chave privada para assinar digitalmente as respostas, e o navegador do usuário verifica essa assinatura usando a chave pública.

b) Dois benefícios de segurança

Confidencialidade: As informações enviadas são criptografadas e protegidas contra interceptação.
Autenticidade e Integridade: Garante que o usuário está se comunicando com o verdadeiro Banco do Brasil e que os dados não foram alterados.

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:

Três registros importantes da atividade dos usuários que podem ser registrados para auditoria de segurança são:
Tentativas de login (bem-sucedidas e falhas): Monitorar tentativas de login, incluindo data, hora e origem, ajuda a identificar acessos não autorizados ou tentativas de invasão.

Alterações em configurações de segurança: Qualquer modificação nas configurações de segurança do sistema, como mudanças em permissões ou políticas de acesso, deve ser registrada para auditoria e rastreamento de potenciais violações.
Acesso a dados sensíveis: Registros de quando e por quem dados confidenciais foram acessados podem ajudar a identificar acessos indevidos ou vazamentos de informação.

## Referências


- ABNT (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS). NBR ISO/IEC 27002:2013: Tecnologia da informação –

Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2013.

- HINTZGBERGEN, Jule. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. 3. Ed.

Brasport, Rio de Janeiro, 2018.


https://drive.google.com/drive/folders/1L4JWafYSVZYhBd7ooggPvjlykIiFi2I3

https://drive.google.com/drive/folders/1PUSHQCRj7nMGA3eU_G37rvRoi9jNWhn9