**Estudos de Caso**

Curso: Segurança da Informação

Disciplina: Sistemas Computacionais e Segurança - 2025.1

Professor: Robson Calvetti

Aluno: Vinícius Batista Bertini Conceição

RA: 825153866

**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?

R: Sim, o firewall e o servidor web usados fornecem serviços de criptografia. No texto é mencionado que o firewall pediu seu nome de usuário e senha, ela notou também que o ícone de segurança estava aparecendo

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

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

R: O servidor poderia ser mais seguro utilizando uma VPN, fazendo treinamento de seus funcionários para que não tenha compartilhamento de senhas ou dados e métodos de autenticação de dois fatores.

\*WHITMAN, Michael E. MATTORD, Herbert J. Readings and Cases in Information Security: Law and Ethics. Course

Technology, Cengage Learning: Boston (MA), 2011.

**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?

R: A política da ATI não parece dura quando o objetivo é garantir a segurança, o uso sem restrições da internet pode trazer problemas para a empresa quando usada de maneira incorreta.

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

R: Ron descumpriu as normas de segurança da empresa e ele sabia que não poderia acessar sites aleatórios.

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

e diligente?

R: Andy pode conversar com Ron de maneira construtiva e relembrar as normas de segurança da empresa e solicitar que o funcionário faça um curso para reforçar a importância de manter das normas.

\*WHITMAN, Michael E. MATTORD, Herbert J. Readings and Cases in Information Security: Law

and Ethics. Course Technology, Cengage Learning: Boston (MA), 2011.

**UC Sistemas Computacionais e Segurança – 2025.1**

**Exercícios de Revisão**

**Prof. Calvetti**

**Fontes de estudo principais**

- Material curado da UC Sistemas Computacionais e Segurança no U-Life

- Curso Cisco Fundamentos de Segurança Cibernética

- Material das aulas

**Questões**

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

R: Pentest é um processo controlado que simula ataques cibernéticos com objetivo de identificar falhas e vulnerabilidades em um sistema. As etapas de um pentest incluem o

planejamento, o reconhecimento, a coleta de informações, análise de vulnerabilidades, exploração e a elaboração de um relatório com os achados, evidências e recomendações.

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

R: Ataque de negação de serviço distribuído (DDoS), onde diversos dispositivos comprometidos são usados para gerar uma grande quantidade de tráfego contra um servidor ou serviço fazendo com que o mesmo fique sobrecarregado e indisponível para usuários. O Ransomware, é um software malicioso que sequestra dados, exigindo um resgate para liberá-los. Já as botnets são redes de dispositivos zumbis controlados remotamente que podem ser ativados em massa para derrubar sistemas ou realizar outras ações coordenadas que afetam a disponibilidade.

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)?

R: O conceito mencionado no texto é "conformidade". Ele se refere à necessidade das empresas seguirem legislações, regulamentos internos, contratos e acordos internacionais, estando alinhadas com normas de segurança e boas práticas.

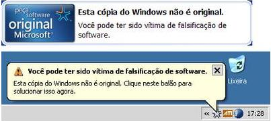
4) Existem vários recursos de software e hardware para estabelecer diversos níveis de segurança em uma rede de computadores. Entre outros, podemos citar os firewalls e os sensores (IDS e IPS). Faça um quadro comparativo resumindo as características de cada um dos três recursos.

R: Os firewalls atuam como barreiras que filtram o tráfego de rede com base em regras previamente configuradas, permitindo ou bloqueando pacotes com base em critérios específicos. Já o IDS, tem a função de monitorar e analisar o tráfego para detectar comportamentos suspeitos ou ataques em andamento, gerando alertas. O IPS, além de detectar, ele é capaz de agir automaticamente para bloquear a ameaça identificada.

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.

R: O primeiro conselho seria não utilizar datas e nomes pois isso torna a senha mais previsível, utilizar pelo menos 12 caracteres incluindo letras maiusculas, minúsculas, números e caracteres especiais. Por último, trocar de senha a cada trimestre, anotar as senhas em um local seguro.

6) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade

R: A vulnerabilidade é o uso de um sistema operacional falsificado.

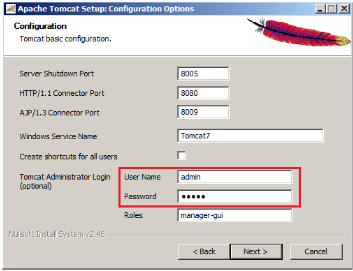
b) A ameaça

R: A ameaça é a possibilidade do sistema operacional estar desprotegido e desatualizado comprometendo a segurança do dispositívo.

c) Uma ação defensiva para mitigar a ameaça

R: Usar uma versão original do windows ou migrar para outro sistema operacional que se mantenha sempre atualizado.

7) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade

R: A vulnerabilidade está em usar um User Name genérico e muito conhecido.

b) A ameaça

R: A ameaça é uma pessoa mal intencionada invadir a sistema.

c) Uma ação defensiva para mitigar a ameaça

R: Para mitigar a ameaça pode ser mudado o nome de usuário para algo menos previsível e ocultar a quantidade de caracteres.

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;

R: Para enviar a mensagem de forma que apenas Bob possa decifrá-la, Ana deverá cifrá-la usando a chave pública de Bob. Assim, apenas Bob, que possui a respectiva chave privada, conseguirá decifrar a mensagem.

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

R: Bob deverá decifrar a mensagem utilizando sua própria chave privada.

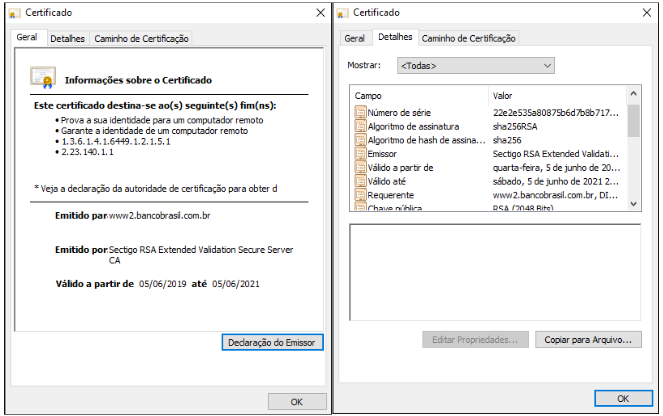
c) como Ana deverá cifrar a mensagem antes de enviar para Carlos;

R: Ela deverá assinar digitalmente a mensagem utilizando sua chave privada.

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

R: Carlos deverá usar a chave pública de Ana para verificar a assinatura digital.

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.

R: A utilização do certificado digital envolve a autenticação da identidade do Banco do Brasil e o estabelecimento de uma conexão segura com o cliente. Quando o usuário acessa o site, o servidor apresenta seu certificado digital, que contém sua chave pública. O navegador verifica a autenticidade desse certificado por meio da autoridade certificadora emissora. Caso seja válido, inicia-se uma troca segura de informações. As chaves criptográficas são utilizadas da seguinte forma: a chave pública do banco é usada pelo navegador para cifrar os dados sensíveis enviados pelo usuário, como senhas e dados bancários. Somente o banco, com sua chave privada correspondente, poderá decifrar essas informações. Esse processo assegura que os dados trocados estejam protegidos contra interceptação.

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

R: Dois importantes benefícios de segurança proporcionados pelo uso do certificado digital são:

Confidencialidade, pois garante que os dados trocados entre o cliente e o banco são criptografados, impedindo que terceiros tenham acesso a informações sensíveis.

Autenticidade, já que o certificado assegura que o site acessado é realmente o do Banco do Brasil, prevenindo ataques de phishing e conexões com servidores falsos.

Referências

- HINTZGBERGEN, Jule. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. 3. Ed. Brasport, Rio de Janeiro, 2018.