

ATIVIDADE 07 - Parte 02

Docente: Robson Calvetti

UC: Sistemas Computacionais e Segurança – SCS

Grupo

Marinna Pereira Carneiro da Silva - RA: 824142121

Mariana Hildebrand Dantas - RA: 824118462

Christian Batista de Lima - RA: 824126605

Beatriz Silva de Jesus – RA: 824219590

Mayara Fernandes dos Santos – RA: 824227938

Victor Pinas Arnault – RA: 82215768

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, cifrao."

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?

O firewall e o servidor web da Linen Planet estavam, sim, usando criptografia. Quando a Maris viu o ícone de segurança no navegador, isso indicava que havia uma proteção ativa

por meio do protocolo HTTPS, que utiliza SSL/TLS para criptografar a comunicação entre o navegador e o servidor. Essa camada de segurança impede que os dados sejam interceptados ou visualizados por terceiros enquanto trafegam pela rede

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

O acesso ao servidor web da Linen Planet poderia ser mais seguro adotando algumas medidas adicionais, como a autenticação multifator (MFA), que exigiria mais de uma forma de verificação para garantir que só pessoas autorizadas tenham acesso. Além disso, a empresa poderia exigir senhas mais fortes e trocas periódicas, monitorar as atividades de login para detectar comportamentos suspeitos, e usar uma VPN para proteger as conexões dos funcionários em redes públicas. Outra coisa importante seria treinar os funcionários para que eles estejam cientes de boas práticas de segurança e saibam como proteger melhor as informações.

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?

A política da ATI pode parecer um pouco dura, mas ela é justificada, considerando que eles precisam garantir a segurança e manter a produtividade dos funcionários. Limitar o acesso a sites não autorizados é uma forma de evitar distrações e proteger a rede contra ameaças, como vírus e malwares que podem estar escondidos em páginas menos confiáveis. Porém, é compreensível que um pouco mais de flexibilidade possa ser considerado em certos casos.

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

O Ron achou que estava justificado por querer relaxar um pouco depois de meses de trabalho duro, mas ele acabou infringindo as regras da empresa. As políticas de uso da ATI foram feitas para garantir a segurança e a conformidade, e, mesmo que ele não tivesse a intenção de causar problemas, ele deveria ter respeitado as diretrizes estabelecidas.

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

O Andy deve lidar com essa situação levando em conta o histórico do Ron. Se ele é um funcionário confiável e essa foi a primeira vez que algo assim aconteceu, uma conversa direta para entender a situação pode ser o suficiente. O Andy pode pedir que o Ron participe do curso de uso adequado da internet, mas também pode aproveitar para ver se há algo que possa ser feito para tornar as políticas um pouco mais flexíveis, permitindo algum acesso recreativo em momentos apropriados sem comprometer a segurança.