TECNOLOGIAS WEB

SEGURANÇA NA INTERNET

Olá!

Nesta aula, iremos aprender o que é segurança de Internet. Como podemos nos proteger. Conheceremos os principais métodos de ataque e proteção utilizados na rede.

Veremos, ainda, como aumentar a segurança de nossos sistemas utilizando controles de sessão e cookies.

Ao final desta aula, você será capaz de:

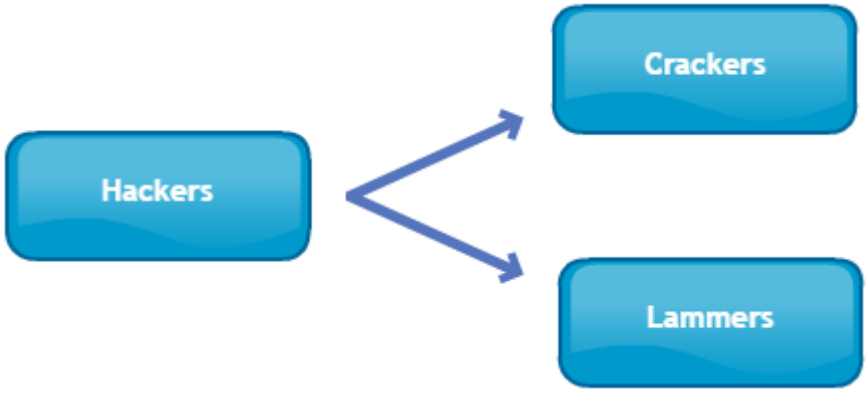
1. Apresentar os principais aspectos de segurança tanto no lado cliente quanto no servidor.
2. Compreender as implicações de segurança individual e seus métodos de proteção.
3. Compreender o uso da criptografia e da assinatura digital, suas vantagens e desvantagens.

1 A internet é segura?

Você se lembra que na Aula 1 falamos a respeito da proliferação de Worms desde a época da ARPANET? Está lembrado? Pois bem, desde a criação da Internet, a segurança das informações está sempre em pauta na mesa dos especialistas, pois, na concepção da mesma, existiu uma ideia de que, se um nó fosse atacado, o outro deveria servir de caminho alternativo. Ora, isto nada mais é do que caminhos alternativos para os invasores explorarem, pois, se em nossa rede temos vários caminhos para ir e vir, nada mais lógico que aquele que se propõe a invadir nossa rede também tente percorrê-los.

Acompanhe nossa aula e veja como tornar sua navegação mais segura.

Antes de qualquer um começar, é interessante sabermos como se categorizam os invasores de sistemas, fazendo uma análise correta de cada um deles:



Hackers	São grandes administradores de sistemas, especialistas com habilidade suficiente para descobrir problemas de segurança e operação em aplicativos ou em sistemas operacionais que se divertem em atacar uma rede. Eles se justificam dizendo trabalharem pelo prazer na superação dos limites. Existem diversos subtipos de hackers: White hat, Grey hat, Black hat, Newbie, Phreaker, Cracker e Lammer.
Crackers	Eles utilizam suas habilidades para o mal. Se aproveitam da falha dos sistemas para roubarem, chantagearem ou darem prejuízo a terceiros sejam estes pessoas físicas ou jurídicas. São os "quebradores" de sistemas. Um termo genérico para "Black hat".
Lammers	São iniciantes na arte da invasão que se apropriam de códigos ou táticas explicitados em revistas e sites para atacarem computadores sem saber, às vezes, o que estão fazendo. Eles simplesmente executam algo que não sabem como funciona. Quando as tentativas de invasão são bem-sucedidas se autodenominam hackers.

Conheça dois Hackers/Crackers muito famosos:

Eric Steven Raymond

Autor de um dos melhores livros a respeito da forma de organização para o desenvolvimento de sistemas. Este livro, gratuito para download, nos faz refletir a respeito da Engenharia de Software.

Figura 1 - Eric Steven Raymond

Kevin David Mitnick

Foi preso em 1995 e libertado em 2000. Sua área de atuação foi a pirataria de sistemas telefônicos. Foi capturado por um grande especialista em segurança, Tsutomu Shimomura.

Figura 2 - Kevin David Mitnick

2 Tipos de ataque

Para você saber como proteger sua máquina na Internet, é importante que conheça os principais tipos de ataque utilizados pela maioria dos vilões do ciberespaço. São eles: Cavalo de Tróia, Quebra de Senha, Denial Of Service (DOS), Mail Bomb, Phreaking, Spoofing e Scamming.

- Cavalo de Tróia

  Este é um dos ataques mais comuns que há. Você pode receber um arquivo anexo em seu e-mail, por exemplo, indicando um link e acabar baixando um programa invasor ou, ainda, executar um programa anexo ao e-mail acreditando ser uma apresentação ou uma imagem.

  São do tipo Backdoor que utilizam conexão direta ou reversa entre a máquina alvo e o servidor do invasor.

Outro tipo de cavalo de troia, ou trojan, se destina a roubar senhas de bancos e aplicativos dos usuários da máquina alvo. Eles conseguem até monitorar a sequência do mouse nos teclados de senhas. Estes são do tipo Keylogger.

Alguns trojans populares são NetBus, Back Orifice e SubSeven.

- Quebra de Senha

Este tipo de invasão trabalha com a missão de crackear, ou seja, quebrar as senhas de sistemas e usuários, utilizando técnicas de dicionários de palavras ou, ainda, uma técnica chamada “força bruta”. A quebra de senhas é uma das tarefas que mais divertem os lammers, pois muitos scripts rodam durante dias e noites até encontrarem a senha desejada.

- Denial Of Service (DOS)

Este ataque se caracteriza pela utilização de computadores de usuários comuns para em um determinado momento sobrecarregarem um servidor com uma quantidade excessiva de solicitações de serviços tirando-os do ar.

Este tipo de ataque traz uma vantagem ao atacante, pois pulveriza as pistas que levariam ao autor principal. Sites como CNN, Yahoo!, ZD Net, AOL, Twitter, Facebook, Google blogs já sofreram este tipo de ataque.

Os invasores implantam, nas máquinas dos usuários, programas zumbis que ficam aguardando a ordem de atacar coletivamente em uma determinada data.

- Mail Bomb

Esta técnica é muito popular.

O invasor sobrecarrega o servidor de mensagens de correio eletrônico com mensagens, fazendo com que este pare de responder pelo acúmulo de carga de serviço.

- Phreaking

No passado, este tipo de invasão era bastante comum. Muitos usuários divulgavam métodos para burlar as empresas telefônicas e garantir ligações gratuitas ou a baixo custo.

Ainda hoje, estas técnicas são utilizadas em diversos países tanto para fixos quanto para celulares, mas ficaram restritas a especialistas.

- Spoofing

Esta técnica consiste em atacar um computador através de outro, fazendo com que o administrador do sistema pense que o computador que está atacando é aquele no final da comunicação, escondendo as informações do endereço IP do computador de origem.

- Scamming

  O intuito deste ataque é roubar senhas de bancos enviando ao usuário uma página simulando o site do banco do mesmo.

  Este é um dos ataques que mais logra êxito, pois muitos usuários não reparam no endereço da URL, nem mesmo no cadeado do site.

3 Como dificultar a quebra de senhas

Existem algumas maneiras de tornar a vida dos invasores um pouco mais chata e a sua um pouco mais tranquila.

Ao criar uma senha, siga as seguintes dicas:

- Nunca utilize senhas com menos de 6 caracteres, pois a combinação destes já dá mais trabalho ao invasor.
- Não utilize dados pessoais em suas senhas, tais como nomes de pessoas, animais de estimação, ou datas de aniversário.
- Utilize letras Maiúsculas combinadas com minúsculas para dificultar a vida dos invasores. Ex: AlOjPpKj.
- Inclua números em suas senhas. Ex: A0l2yu7sIa.
- Inclua caracteres especiais. Ex: Al156@ty%67.
- As senhas mais comuns para ataque são: senha, password, 123, 1234, 123456, 1234567890, amor, Deus, Deuse10, Jesus, Jesusteama, qwerty, brazil, abc123, myspace1.

4 Como dificultar o roubo de informações via e-mail

Esta é uma prática comum, pois, quando utilizamos listas ou correntes (aquelas mensagens que pedem para você encaminhar para outros 20 para obter um milagre), expomos nosso endereço de e-mail para a Internet. Muitos sites armazenam mensagens de listas expondo o e-mail de seus participantes.

Algumas dicas são importantes para a proteção da identidade.

O e-mail é uma carta e, desta forma, deve ser revisada antes de ser encaminhada.

Muitas pessoas demonstram, ao responder um e-mail, total displicência com relação à forma, ao conteúdo e às informações nele contidas.

O invasor se vale desta pressa para poder levantar dados dos usuários a serem atacados.

5 Dicas para proteger seu e-mail

Você pode aumentar a proteção do seu e-mail evitando algumas falhas importantes e muito comuns.

Veja quais são elas:

- Não divulgue seu e-mail corporativo em listas, correntes ou outros locais fora do ambiente de trabalho. Pessoas inescrupulosas se valem desta informação para chegarem até você. Utilize e-mails gratuitos para falar de coisas que não se relacionam com trabalho.
- Preste atenção na assinatura automática do seu e-mail. Se você falhar na regra anterior, vai ficar triste por expor, também, seu endereço, empresa e cargo.
- Preencha seu e-mail com calma. Se está de cabeça quente, pare, respire, pois muitas informações, depois de postadas, não têm como serem apagadas de listas e outros sites que "capturam" e-mails.
- Utilize CCO ou BCC, isto é, poste com cópia oculta para não revelar aos invasores a lista dos copiados, mas seja ético, informe a todos dentro do e-mail que está sendo copiado: Copiando para Fulano, Beltrano etc. Assim, todos saberão quem está recebendo, menos os invasores. Evite o CC, com cópia simples, pois, caso haja um programa invasor na máquina do amigo que recebeu a cópia do seu e-mail, este poderá, com a lista de destinatários aberta (CC), levantar um banco de e-mails válidos para enviarem SPAMS.
- Utilize assinaturas digitais. Este é um hábito que, aos poucos, está aumentando. Sites oferecem o serviço gratuito de identificação de originalidade do seu e-mail, indicando àquele que recebe sua mensagem que você é você e não um invasor dissimulado. Procure na internet "e-mail certificado grátis". Existem boas empresas com ótimos serviços para pessoa física.
- Utilize e-mails, principalmente para dentro da empresa, criptografados. Isto é importante para "esconder" informações que não são públicas dos encaminhamentos não autorizados. Este é um hábito que, se tivermos, evitaremos muitos problemas de segurança dentro e fora da empresa. No próximo tópico, abordaremos mais detalhadamente as formas de criptografia.

6 Criptografia

É a tecnologia que tenta manter em segredo mensagens em trânsito.

Não cabe a este estudo inicial um aprofundamento das técnicas de criptografia e, portanto, abordaremos sua versão mais voltada para a Internet.

Os objetivos da criptografia é manter a confiabilidade da mensagem, mantendo-a íntegra, autenticando, dessa forma, o remetente que não poderá negar a autenticidade da mesma.

Existem dois tipos de Criptografia. São eles:

Chave simétrica

Onde tanto o emissor quanto o receptor compartilham a mesma chave. O aspecto negativo dessa técnica é o gerenciamento seguro da chave.

Chave pública

A criptografia assimétrica procura corrigir o problema do gerenciamento seguro da chave utilizado pela chave simétrica, pois nela a chave de criptografia é diferente da chave de decriptografia.

O PGP pode ser utilizado por qualquer pessoa que cria uma chave pública e uma chave privada para si, divulgando somente a chave pública. Existem servidores que armazenam esta chave pública gratuitamente como o servidor da RNP.

O que vem na próxima aula

Na próxima aula, você vai estudar:

- os principais aplicativos para a Internet, seus usos e vantagens.

CONCLUSÃO

Nesta aula, você:

- Aprendeu a importância da segurança na Internet e seus principais riscos.
- Aprendeu quais são os ataques mais comuns
- Aprendeu quais são as soluções do lado cliente e do lado servidor.