Universidade Tecnológica Federal do Paraná – UTFPR

Campus:
Campo Mourão

Professor:
Prof. Dr. Luiz Arthur Feitosa dos Santos

E-mail:
luizsantos@utfpr.edu.br

Sumário:

2018

O assunto **segurança** em computadores e redes de computadores atualmente **faz parte de nosso cotidiano**. Isto acontece por que a **sociedade** esta cada vez mais **dependente dos computadores** e dos benefícios oferecidos pela alta tecnologia.

É fácil constatar isto, por exemplo:

- Praticamente **todo mundo sabe o que é um vírus** de computador e que temos que atualizar os programas **antivírus** para evitar esta praga.

- Todo mundo sabe o transtorno que dá quando vamos fazer uma tarefa e aparece a **mensagem "Sistema indisponível temporariamente"** (sim!!! isto é um problema de segurança... vamos ver o por que nos slides seguintes).

Estes são apenas pequenos exemplos mas já dá uma noção do quanto estamos ligados aos computadores e como a segurança ou a falta de segurança destes nos afetam.

O principal objetivo desses slides é introduzir o leitor ao mundo da cibersegurança. Contudo tal mundo está repleto de termos peculiares. Algumas **terminologias** serão apresentadas no decorrer dos slides, mas por enquanto são apresentados alguns termos importantes segundo a CEH (*Certified Ethical Hacker*) (GRAVES, 2007):

- **Cibersegurança**: é a segurança em âmbito computacional, ou seja, ligada à segurança software ou hardware, visando proteger esses contra ameaças, que também são chamadas, neste caso, de ciberameaças;
- **Ameaça**: é um ambiente ou situação que pode levar a falhas de segurança;
- **Vulnerabilidade**: é uma falha existente em software ou hardware que pode levar a um evento indesejado, tal como a execução de comandos maliciosos em sistemas;
- ***Exploit***: é normalmente um software que utiliza falhas (*bugs*) ou vulnerabilidades para realizar um ataque. Há dois tipos de *exploits*: *remote exploit*, que é utilizado via rede e *local exploit* que precisa ser executado no local do ataque;
- **Alvo** (*target of evaluation*): é um sistema, programa ou rede que é objetivo de analise de segurança ou ataque.
- **Ataque**: ocorre quando um sistema tem sua segurança comprometida através de uma vulnerabilidade. Muitos ataques são executados utilizando-se *exploits*.

Cibersegurança e a informação

Quando falamos de segurança na área da informática **a maioria das pessoas pensão em proteger o computador** ou os recursos físicos do sistema. Isto é importante e vai ser feito em alguns casos.

Porém, o que devemos proteger na maioria dos casos são as informações contidas nesses computadores.

O **hardware** hoje é relativamente **barato**, mas **perder** todas as **informações** de seu computador **pode** lhe **custar muito caro**.

Muitas pessoas ainda não perceberam isto. É por isto que estes slides levam o título de Segurança da Informação e não Segurança de Computadores.

Outro exemplo que mostra a importância da informação é o seguinte: **Imagine que você perca o telefone celular!**

As reações na perca de um *smartfone* provavelmente **serão**:

- Primeiramente **a pessoa vai se lamentar pela perda do hardware** e vai ficar pensando o quanto vai custar outro aparelho;

- Depois de passar o susto da perca do equipamento, a **pessoa vai lembrar e lamentar profundamente a perda de telefones importantes que havia na agenda**. Alguns desses contatos telefônicos podem nunca mais ser recuperados.

- Ou ainda da possibilidade de informações sensíveis (presentes no telefone ou que esse tem acesso), caírem em mãos erradas.

Então, **com a perda do telefone** a pessoa provavelmente vai acabar com um **aparelho novo** (em alguns casos melhor do que o anterior). **Mas** quanto **as informações** contidas no celular? **provavelmente essas não retornarão em sua completude** no celular novo. **E se** no momento em que a pessoa perdeu o celular **aquela proposta de trabalho milionária chama no seu celular?** A pessoa acabou de perder muito dinheiro, mais do que o seu aparelho celular poderia valer...




Quem é o inimigo?

Hacker

"Sabichão"
Não *hacker*

Usuário comum

Funcionário insatisfeito

Quem é o inimigo?

Talvez

Hacker

Provavelmente

"Sabichão"
Não *hacker*

Sim

Usuário comum

Com certeza

Funcionário insatisfeito

Quem é o inimigo? É preciso entender que...

A segurança da informação, principalmente no que envolve computadores é um **assunto muito vasto e complexo**. Tanto é que hoje existem **poucos profissionais dedicados a esta área**.

Diariamente, no mundo inteiro **computadores e suas redes estão sendo invadidos**. **É muito difícil saber detalhes sobre todas as técnicas de invasão** existentes, pois elas podem ser de diversas naturezas. **Mas é possível** conhecer os conceitos básicos destas e **prevenir os problemas de segurança**.

O nível de sofisticação **destes ataques vária amplamente**, embora a maioria das invasões se da devido a **senhas fracas**, **e** outras **poucas** estão **relacionadas a elaboradas técnicas de invasão**.

Ser humano x Segurança

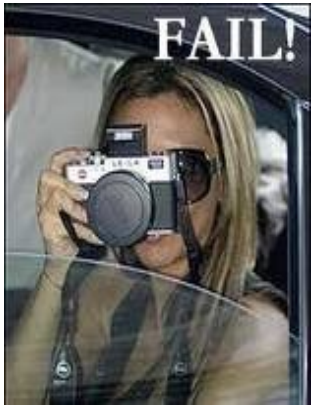
A principal ameaça para qualquer segurança é sem duvida o **ser humano**, todo processo de segurança inicia e termina no usuário do sistema.

Não adianta gastar fortunas em segurança da informação se não conhecermos **quem utilizará nossos sistemas** e quem pode ter acesso a eles mesmo sem autorização.

É necessário conhecer as pessoas que utilizam nossos sistemas direta ou indiretamente. Para manter a segurança **é bom ter um mapa detalhado de como funciona o nosso sistema**, **tanto em aspectos físicos** como **lógicos** e quem pode ou não acessar tal sistema.

Precisamos saber do que e de quem proteger o sistema. Possibilitando desta maneira que o sistema esteja com o maior grau de segurança possível.

Lembre-se errar é humano:



Situações que podem gerar insegurança

Assegurar a informação é uma tarefa um tanto quanto complicada, pois esta é complexa e pode abranger várias situações, como:

Antes de prosseguir vamos tentar imaginar o que pode gerar insegurança!

Então a pergunta é:

“O que causa a falta de segurança?”

Situações que podem gerar insegurança

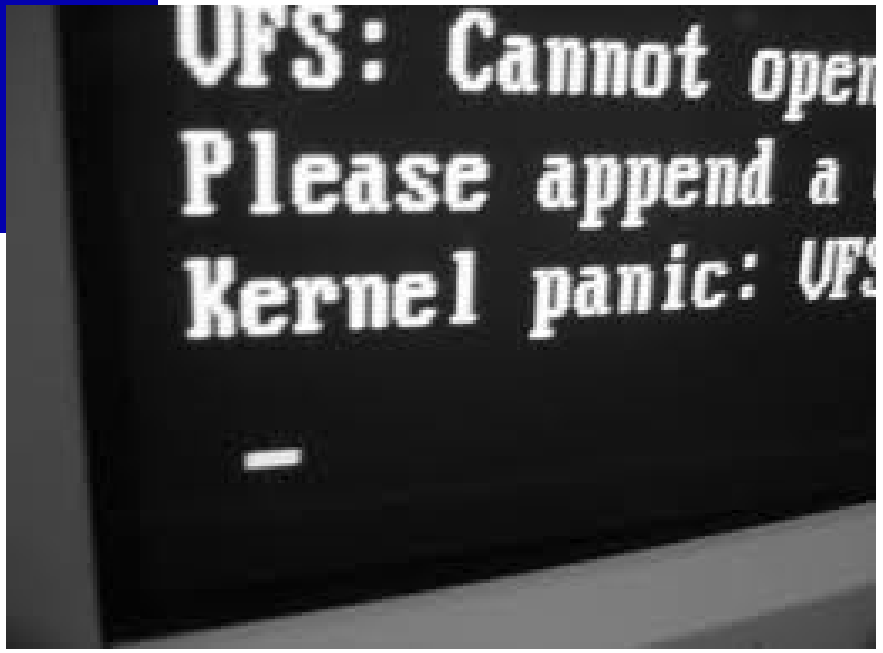
Assegurar a informação é uma tarefa um tanto quanto complicada, pois esta é complexa e pode abranger várias situações, como:

- **Erro;**
- **Displicência;**
- **Ignorância do valor da informação;**
- **Acesso indevido;**
- **Roubo;**
- **Fraude;**
- **Sabotagem;**
- **Causas da natureza;**
- **Etc.**

Vamos analisar estas situações mais em detalhes. É você quem vai dar exemplos dessas situações (pense no que você já passou no seu dia a dia).

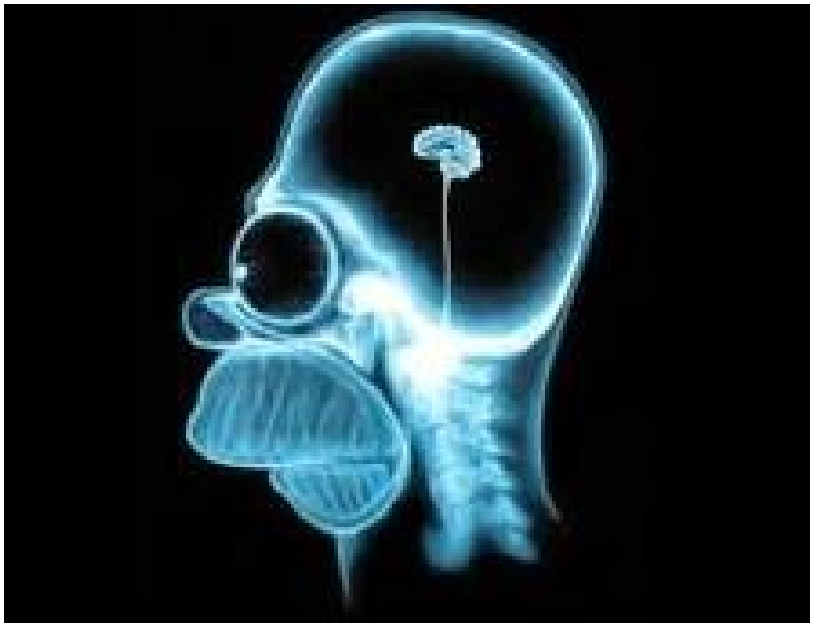
Erro


Windows
A fatal exception 0E has occurred at 0028:C0068BF0 in VxD VMM(01) +
00005FF0. The current application will be terminated.
* Press any key to terminate the application.
* Press CTRL+ALT+DEL to restart your computer. You will
lose any unsaved information in all applications.
Press any key to continue


VFS: Cannot open
Please append a
Kernel panic: VFS

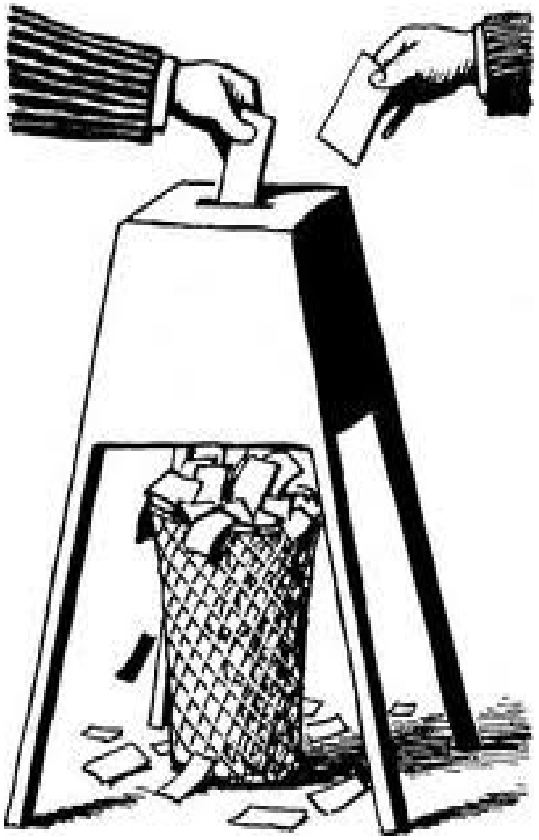
Displicência

Ignorância do valor da informação



Acesso indevido e Roubo

Fraude e Sabotagem



Causas da natureza e o pior etc

etc...

Todos os problemas vistos anteriormente tem relação direta ou indireta com a segurança da informação ou segurança de computadores. Ignorar qualquer problema desses vai levar o seu sistema, mais cedo ou mais tarde, a ter problemas de segurança.

Definição de segurança em informática

Para compreendermos melhor o que seria a segurança que estamos falando vamos defini-la mais formalmente:

A segurança da informação no âmbito da informática define-se como processo de proteção de informações e ativos digitais armazenados em computadores e/ou redes de processamento de dados.

Algumas pessoas pensam que como as informações hoje estão armazenadas em sua maioria em computadores, **apenas medidas tecnológicas devem ser tomadas**, mas **isto é uma ideia equivocada e muito errada**. É claro que vamos focar em proteções tecnológicas, entretanto temos que ter em mente que os problemas de segurança mais comuns e críticos não estão relacionados com assuntos de alta tecnologia.

Um conceito que devemos ter é que **segurança não é uma questão técnica, mas sim gerencial, educacional e humana**.

Portanto **a segurança** da informação de uma empresa **não esta ligada somente a produtos voltados à computadores** como:

- **Firewall;**
- **Antivírus;**
- **Software de encriptação de dados;**
- **IDS;**
- **VPN;**
- **etc.**

Mas **sua abrangência vai muito além disso**, podendo citar:

- **Análise de Risco;**
- **Política de Segurança;**
- **Controle de Acesso Físico e Lógico;**
- **Treinamento e Conscientização;**
- **Plano de Contingência;**
- **etc.**

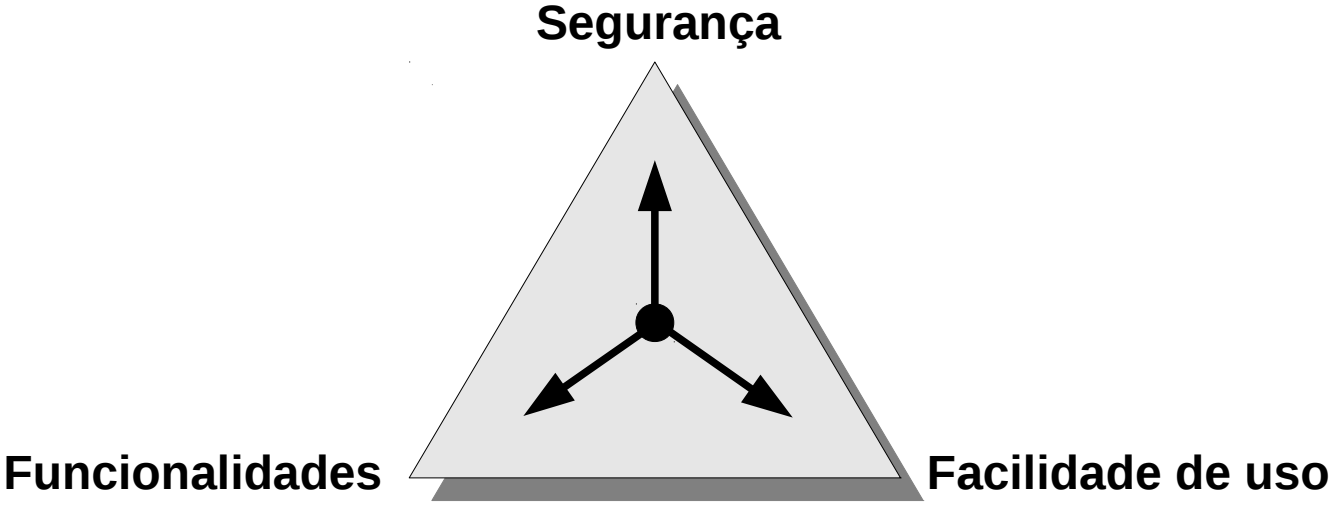
A **segurança** da informação pode e deve ser tratada como um **conjunto de mecanismo** conforme foi anteriormente exposto, **devendo ser adequada à necessidade de cada ambiente**.

Segurança, funcionalidades e facilidade de uso

Como esses slides abordam cibersegurança, é bem normal começar a pensar em criar **sistemas com altíssimo grau de segurança**. Bem isso é possível, mas normalmente **é necessário pagar um preço**.

Infelizmente **há conflitos entre segurança, funcionalidade e facilidade** de uso e o processo de desenvolvimento e/ou configuração de sistemas/redes exige um **balanceamento entre esses itens**.

No geral **quanto mais seguro é alguma coisa, menos usável e funcional é essa coisa**. Da mesma forma, quanto mais funcionalidades e/ou fácil de usar menos seguro é essa coisa.



Elementos básicos da segurança da informação

Como vimos a segurança envolvendo computadores é muito abrangente, mas um **ótimo ponto para** se **começar** a prover segurança **é na informação que esta armazenada ou em transito** em nossos computadores.

Isto é tão importante que alguns órgãos criaram **normas** para este tipo de segurança, tal como: A série de normas **ISO/IEC 27000** tratam de padrões para segurança da informação, tendo como referência ISO/IEC 17799:2005 que por sua vez foi influenciado pelo padrão **BS 7799**. A ISO/IEC 27002:2005 ainda é chamada de **17799:2005** para fins históricos.

Basicamente os padrões de segurança da informação contemplam os seguintes elementos:

- **Confidencialidade;**
- **Integridade;**
- **Disponibilidade.**

Em alguns casos esses elementos são chamados de CIA, do inglês *Confidentiality*, *Integrity* e *Availability* (WALKER, 2012). Vamos ver em detalhes estes itens.

Confidencialidade:

Como você definiria confidencialidade?

Como podemos fornecer confidencialidade?

Confidencialidade:

Como você definiria confidencialidade?

Confidencialidade significa proteger as informações confidencias contra revelações não autorizadas ou captação compreensível dos dados.

A perda de confidencialidade existe quando pessoas não autorizadas obtêm acessos às informações confidenciais.

Como podemos fornecer confidencialidade?

Confidencialidade:

Como você definiria confidencialidade?

Confidencialidade significa proteger as informações confidencias contra revelações não autorizadas ou captação compreensível dos dados.

A perda de confidencialidade existe quando pessoas não autorizadas obtêm acessos às informações confidenciais.

Como podemos fornecer confidencialidade?

Guardando informações sensíveis em lugares seguros. Isto inclui papeis em salas de acesso restrito.

Em computadores podemos fazer uso, por exemplo, de criptografia.

É claro que existem outras formas de se manter a confidencialidade.

Disponibilidade:

Como você definiria Disponibilidade?

Como podemos fornecer Disponibilidade?

Disponibilidade:

Como você definiria Disponibilidade?

Disponibilidade é garantir que informações e serviços vitais estejam disponíveis quando requeridos.

A informação deve estar disponível para a pessoa certa e no momento em que ela precisar.

Não basta ter a informação ela deve estar disponível no momento requerido.

Como podemos fornecer Disponibilidade?

Disponibilidade:

Como você definiria Disponibilidade?

Disponibilidade é garantir que informações e serviços vitais estejam disponíveis quando requeridos.

A informação deve estar disponível para a pessoa certa e no momento em que ela precisar.

Não basta ter a informação ela deve estar disponível no momento requerido.

Como podemos fornecer Disponibilidade?

Uma das maneiras de se fornecer disponibilidade é com redundância.

Antes de prosseguir com os elementos da segurança da informação vamos ver que um elemento da segurança pode influenciar na segurança de outro elemento.

Um elemento de segurança pode influenciar outro

Prover muita segurança em um elemento da informação pode gerar insegurança a outro elemento.

Exemplo, **caso apliquemos um alto grau de confidencialidade** (uma chave criptográfica muito grande, ou várias fechaduras) **podemos tornar a informação indisponível**. Isto pode ocorrer, por exemplo, por que perdemos a chave criptográfica ou a chave da porta onde está a informação.

Ou seja, a confidencialidade influenciou na disponibilidade do exemplo anterior. Assim devemos ter cuidado e dosar as medidas de segurança.

Sempre **avalie o custo e benefício/malefício de cada medida de segurança** que você adotar.

Vamos voltar aos itens de segurança.

Integridade:

Como você definiria Integridade?

Como podemos fornecer Integridade?

Integridade:

Como você definiria Integridade?

Integridade seria manter informações e sistemas computadorizados, dentre outros, ativos, exatos e completos.

Não basta ter a informação ela precisa ser exata e correta.

Manter o item integridade consiste em proteger a informação contra qualquer tipo de alteração sem a autorização explicita do autor da mesma.

A perda de integridade esta relacionada à alteração ou modificação do conteúdo ou do status, remoção da informação.

Como podemos fornecer Integridade?

Integridade:

Como você definiria Integridade?

Integridade seria manter informações e sistemas computadorizados, dentre outros, ativos, exatos e completos.

Não basta ter a informação ela precisa ser exata e correta.

Manter o item integridade consiste em proteger a informação contra qualquer tipo de alteração sem a autorização explicita do autor da mesma.

A perda de integridade, esta relacionada à alteração ou modificação do conteúdo ou do status, remoção da informação.

Como podemos fornecer Integridade?

Algoritmos hash são bem empregados para este fim.

Outros elementos normalmente requeridos para se manter a segurança de computadores (Krause, 1999; Teles, 2006)**:**

- **Autenticidade:** Impedir que pessoas não autorizadas tenham acesso aos recursos computacionais, ou seja, é necessário a identificação dos elementos que compõem uma transação eletrônica;

- **Não-repúdio:** Impedir a falsa negação de ações que alguém tenha realizado. O não repúdio pode ser entendido como sendo os esforços aplicados para garantir a autoria de determinadas ações;

- **Auditoria:** É a identificação de ações/eventos ocorridos no sistema. A auditoria é feita através de análise de registros que identifiquem:

    - Ações realizadas;
    - Pessoas envolvidas;
    - Ativos utilizados;
    - Operações realizadas;
    - Horários dos eventos/ações;
    - E qualquer dado relevante para realizar a auditoria.

Segurança envolve muitos elementos

Até aqui, já vimos que a **segurança** da informação **é primordial**, hoje em dia, **e envolve computadores e redes** de computadores.

Como **segurança é complexa** por envolver vários itens, indo do ser humano até computadores, **torna-se difícil explicar de forma simples** como se proteger de **todos os problemas** (isto pode ser até mesmo impossível).

Daqui para frente abordaremos alguns conceitos básicos que envolvem a segurança para que nas próximas aulas consigamos conectar estes conceitos e melhorar a nossa segurança da informação.

Então, **vamos definir**:

- **Fases para proteção,**
- **Problemas de segurança,**
- **Conceitos bem definidos em segurança;**
- **Algumas soluções para melhorar a segurança.**

Tipos de medidas de segurança:

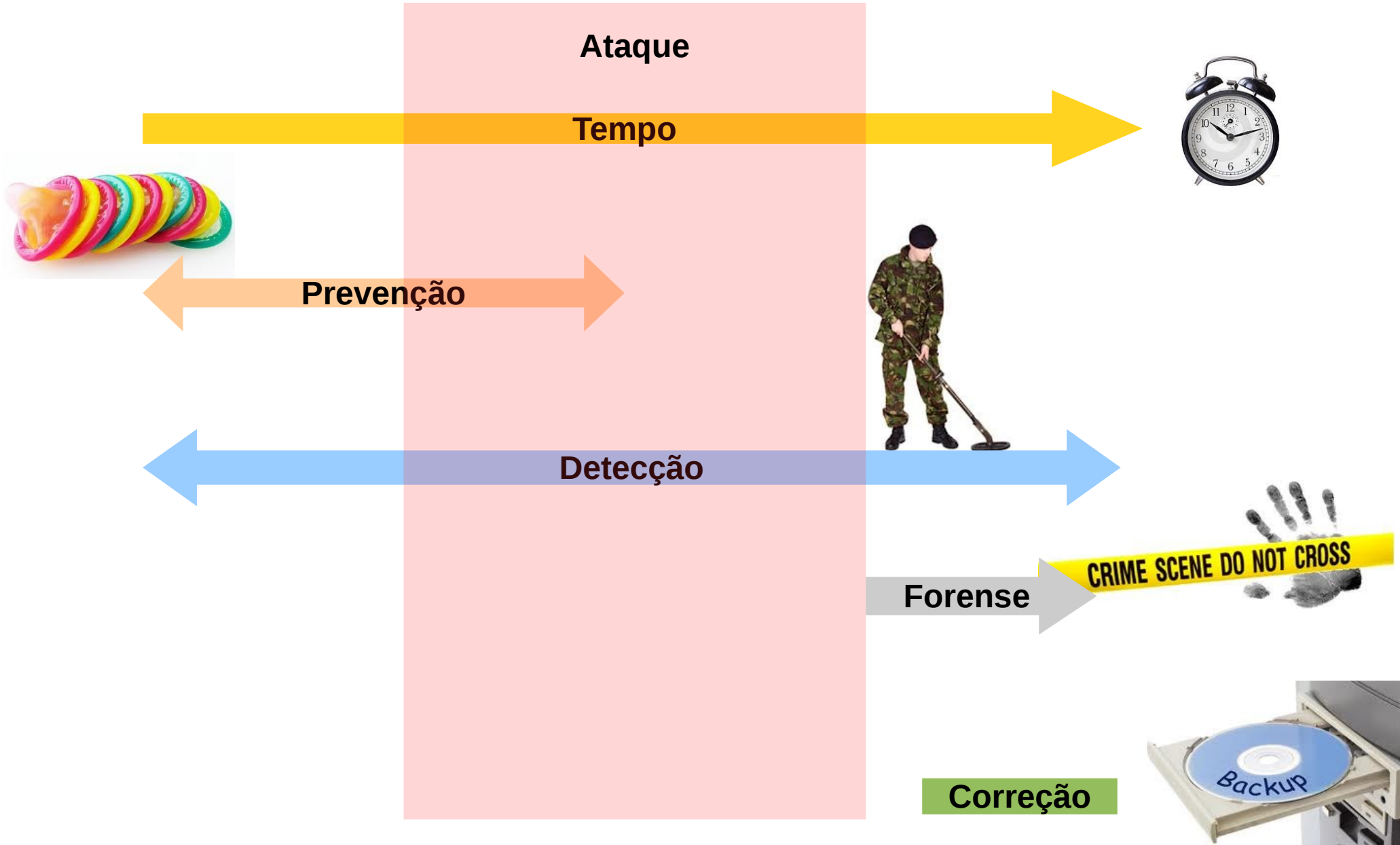
- **Preventiva:** São medidas aplicadas para evitar/prevenir a ocorrência de problemas de segurança. Normalmente só é possível a prevenção de ataques conhecidos;

- **Detectiva:** Medidas utilizadas para monitorar, identificar, detectar e em alguns casos tomar alguma atitude/ação, frente a problemas de segurança que estão acontecendo;

- **Corretiva:** Essa medidas tem como objetivo permitir a continuidade das operações do sistema. A medida corretiva é utilizada quando tudo mais falhou, ou seja, caso as medidas preventivas e detectivas não tenham sucesso, resta então aplicar medidas que corrijam os problemas que já ocorreram;

Além das medidas de segurança citadas anteriormente temos também a parte chamada de **forense**, que tem por objetivo permitir/realizar a investigação para se descobrir detalhes sobre o problema de segurança, apresentado resultados que contribuam para a melhoria da proteção do sistema ou forneça provas para identificar o problema e caso exista os seus autores dando base para ações jurídicas.

Linha de tempo das medidas de segurança:



Hacker o mestre/vilão da segurança

Os termos segurança de computadores e Hackers são altamente ligados e constantemente um está relacionado ao outro.

Originalmente o termo Hacker, designava **qualquer pessoa extremamente especializada** em uma determinada área.

Assim, **quem é extremamente bom em algum assunto** pode ser denominado um Hacker, daquela área.

Um Hacker de computador seria uma pessoa especializada em diversas áreas da informática, possibilitando que esta pessoa tome proveito disto em relação a usuário menos experientes e/ou desavisados.

Então, por definição, um Hacker é uma **pessoa que possui uma grande facilidade de analise, assimilação, compreensão e capacidades surpreendentes com um computador**. O Hacker sabe perfeitamente que nenhum sistema é completamente livre de falhas, e sabe onde procurá-las utilizando de técnicas das mais variadas.

Derivações do termo hacker

O Hacker costuma levar a fama por coisas erradas que outras pessoas fazem. Muitas pessoas defendem que o título **Hacker** deve ser dado a uma pessoa que **faz o bem**, ou simplesmente não faz o mau utilizando o seu conhecimento especializados. Porém, a grande maioria das pessoas já tem como definição que Hacker é um “ladrão” dos computadores.

Vamos então ver as definições e **derivações dos hackers** e tentar analisar quem são os verdadeiros problemas:

Cracker: Possui tanto conhecimento quanto um Hacker, mas com a diferença de que, para eles, não basta invadir sistemas, quebrar senhas, e descobrir falhas eles tem que fazer o mau. **Cracker é o verdadeiro Hacker do mau**.

Os Crackers precisam deixar um aviso de que estiveram lá, geralmente com recados malcriados, ou destruindo partes do sistema, ou pior aniquilando tudo o que encontram pela frente.

Também são atribuídos aos Crackers programas que retiram travas em softwares, bem como os que alteram suas características, adicionando ou modificando opções, muitas vezes relacionadas à pirataria.

Phreaker: É especialista em telefonia. Fazendo parte de suas principais atividades as ligações gratuitas, reprogramação de centrais telefônicas, instalação de escutas, etc. O conhecimento de um Phreaker é essencial para se buscar informações que seriam muito uteis nas mãos mal-intencionados. Suas técnicas são muito apuradas, permitindo ficar invisível diante de um rastreamento.

Guru: O supra sumo dos Hackers. Hoje os sistemas são tão complexos que devem existir poucas pessoas com este título. Mas eles existem e são verdadeiros gênios.

Atenção! Se um Hacker quiser realmente te invadir é bem provável que ele consiga, independente do nível de segurança que você empregue. Nós não vamos nos proteger deste tipo de invasor, mas sim dos que virão a seguir.

Contra os Hackers podemos usar a **técnica da avestruz**, ou seja, **enfia a cabeça na terra e se esconde!** Utilizar muitas medidas de segurança podem chamar mais ainda a atenção do Hacker e agravar o problema.

Se você estiver frustrado com a técnica da avestruz, pare e pense! Por que os bancos, mesmo com todo o investimento em segurança, ainda são roubados?

Por que existem ladrões profissionais (Hackers dos bancos).

Segundo o *Certified Ethical Hacker* **há três classes de *hackers***:

• ***White hats***: São os **mocinhos**, ou seja, os *hackers* que usam suas habilidades para propósitos legais, tal como, defender pessoas de ciberataques. Esse tipo de *hacker* normalmente é representado por profissionais da área de cibersegurança;

• ***Black hats***: São os **vilões**, ou seja, são *crackers* que usam sua inteligência para fins maliciosos. Esses, invadem sistemas e normalmente destroem dados vitais e/ou interferem em serviços;

• ***Grey hats***: São *hackers* que podem trabalhar de forma ofensiva ou defensiva, dependendo da situação. Os *Grey hats* são a linha divisória entre os *hackers* e os *crackers*. Essa classificação existe pois algumas pessoas são tanto *Black hats* quanto *White hats*. Por fim, esse é um tipo difícil de se categorizar, pois não são bons nem maus. Um exemplo são *hackers* que querem testar alguma técnica de invasão, mas não pedem autorização para testá-la em uma empresa.

Também dá para incluir outro tipo aqui: os ***Ethical hackers*** (*Hackers* éticos), que são entusiastas, que visam descobrir e/ou corrigir problemas de cibersegurança, educar pessoas, etc (similar ao *White hat*). Por exemplo, sem ser contratado para isso, um *hacker* desse tipo pode invadir uma empresa e apontar as suas vulnerabilidades, contudo é preciso lembrar que não é toda empresa que vê isso com bons olhos.

Classificação dos NÃO *hackers*

Lammers*:** Aquele que deseja aprender sobre *hackers*, e sai perguntando para todo mundo: “como eu me torno um *hacker*? O que devo fazer?”. Os *hackers*, não gostam disso, e passam a chamar-lhes de ***Newbie (novatos).

***Wannabe*:** É um principiante que **aprendeu a usar alguns programas**, já prontos, para descobrir senhas ou invadir sistemas. Os *Wannabes* ainda não tem capacidade de criar suas próprias técnicas.

Larva: Este já está quase se tornando um Hacker. Este já **consegue desenvolver suas próprias técnicas** de como invadir sistemas.

É a partir deste nível que a nossa segurança deve começar a surtir efeito. Note que os não hacker são mais numerosos do que os hacker (que são poucos), então se nossa segurança conseguir barrar estes já teremos um alto grau de segurança.

Novamente usando bancos como referência. A segurança dos bancos é feita para barrar o ladrão pé de chinelo, que são a maioria, impedindo que qualquer pessoa de posse de uma arma tente assaltar o banco.

O pior - Os não hackers que pensam que são Hacker

O livro Hackers expostos brinca com o seguinte termo:

Arackers: São os Hackers de Araque, são a maioria absoluta no submundo cibernético. Algo em torno de 99,9%.

Os Arackers fingem ser os mais ousados e espertos usuários de computador, planejam ataques, fazem reuniões durante as madrugadas, contam de casos absurdamente fantasiosos, mas no final das contas vão fazer download de sites impróprios ou vão jogar. Resultando na mais engraçada espécie: a "odonto-hackers" - ou o Hacker da boca pra fora.

Porém **os Arackers são os piores! Pois tentando invadir sistemas ele trás vulnerabilidades para dentro de seu próprio sistema e o pior, sempre temos um Aracker dentro de nosso ambiente de trabalho ou em casa.**

Por incrível que pareça, a maioria das pessoas que acham que são Hackers, não são e uma minoria que juram não ter nenhuma relação com o submundo digital, são Hackers muito experientes, mas raramente perigosos. Os Hackers mais perigosos ficam entre esses dois mundos, já que eles são experientes, mas gostam de aparecer.

O que os hackers exploram?

Existem muitos métodos e ferramentas para localizar vulnerabilidades, executar *exploits* e comprometer sistemas (abordadas posteriormente). Muitos exploram fraquezas em quatro áreas da informática:

- **Sistemas Operacionais**: Muitos administradores instalam sistemas operacionais e não os configuram, ou seja, deixam com **configuração padrão**, o que normalmente resulta em brechas que podem ser exploradas durante ciberataques;

- **Aplicações**: **Softwares** normalmente **não são testados contra vulnerabilidades** de segurança durante o seu desenvolvimento, o que pode acarretar em falhas que podem ser exploradas;

- ***Shrink-wrap code***: Muitos **softwares** de prateleira vêm **com características extras que o usuário final não conhece** e essas podem ser usadas por *hackers*. Um exemplo é o Microsoft Word que permite que *hackers* executem programas através de **macros**;

- **Má configuração**: Sistemas também podem ser **configurados erroneamente ou deixados com baixo nível de segurança**, para facilitar seu uso. Contudo isso resulta em vulnerabilidades que podem ser exploradas durante ataques.

Fases/passos de *hacking*

Hackers utilizam várias técnicas para conseguir invadir sistemas e/ou redes. Todavia há basicamente cinco fases:

1. Reconhecendo: Qualquer invasor inteligente fará muitas pesquisas, antes de realizar qualquer tentativa de atacar sistemas/redes. **Qualquer informação no "campo de batalha" é fundamental**, tanto para o atacante quanto para o defensor. **Há reconhecimento passivo e ativo**.

O **reconhecimento passivo** envolve a **obtenção de informações sem que o alvo tome conhecimento**. Um exemplo é observar o habito de funcionários em uma empresa alvo. Atualmente muitos *hackers* conseguem muitas informações para essa fase através da Internet, principalmente em redes sociais. Outro exemplo de reconhecimento passivo é o uso de analisadores de tráfego de rede (*sniffing*).

Já o **reconhecimento ativo envolve sondar informações para descobrir redes, *hosts*, IPs e serviços.** O reconhecimento ativo normalmente **trás mais informações** a respeito do alvo (**a porta da frente está fechada?**), **mas também aumenta as chances do ataque ser identificado**.

2. Escaneamento: fazer uma **análise mais profunda do alvo utilizando as informações obtidas na fase anterior** (reconhecimento). É muito comum confundir as fases de reconhecimento com a de escaneamento, contudo a primeira é mais superficial, tal como levantamento de informações do alvo na Internet, já a presente fase consiste em uma análise mais profunda e detalhada das tecnologias e vulnerabilidades da vítima. As **ferramentas** normalmente utilizadas por *hackers* nessa fase são:

- Discadores (*dialers*);
- Escâneres de portas;
- Mapeamento de rede;
- Varredores (*sweepers*);
- Escâneres de vulnerabilidades.

Nesse passo, os **hackers estão procurando qualquer informação** que possa ajudar a realizar o ataque, tais como, nomes e computadores, endereços IPs, contas de usuários, etc.

Por exemplo, **a fase de reconhecimento pode ter mostrado que a rede alvo tem 500 computadores** conectados em uma subrede dentro de um prédio. Já **a presente fase pode trazer informações que algumas dessas máquinas** possuem o sistema operacional Windows e que outras executam FTP.

3. Ganhando acesso: é onde a mágica acontece. Pois, é a **fase na qual realmente o hacker invade a vítima**. Para ganhar acesso o *hacker* utiliza as informações obtidas nas fases anteriores.

Os **métodos de invasão** podem ser;

- **Via Internet - WAN;**
- **Rede local – LAN;**
- **Localmente** no computador;
- ***offline***.

A invasão pode ser tão simples como acessar uma rede sem fio sem proteção **ou complexa** como submeter um servidor Web a um *buffer overflow* ou SQL *Injection*.

4. Mantendo acesso: uma vez que o *hacker* conseguiu invadir a vítima (passo anterior) é provável que ele queira **manter** esse **acesso para realizar ações futuras** (explorar melhor os recursos da vítima, ou usar o computador da vítima como ponte para outros ataques – zumbi).

A manutenção do acesso é normalmente realizada **através de *backdoors, rootkits* e *trojans***.

Alguns ***hackers* chegam ao ponto de melhorar o nível de segurança da máquina invadida para ter exclusividade** (evitar outros *hackers*).

5. Cobrindo os rastros: Com a máquina já comprometida, o último passo é **apagar todos os indícios que denunciem a invasão**.

Isso também **impede alguma ação legal** por parte da vítima. Apagar as pistas de uma ciber invasão significa:

- Remover dados em arquivos de *logs;*
- Apagar alertas de sistemas de detecção de intrusão
- Ocultar arquivos.

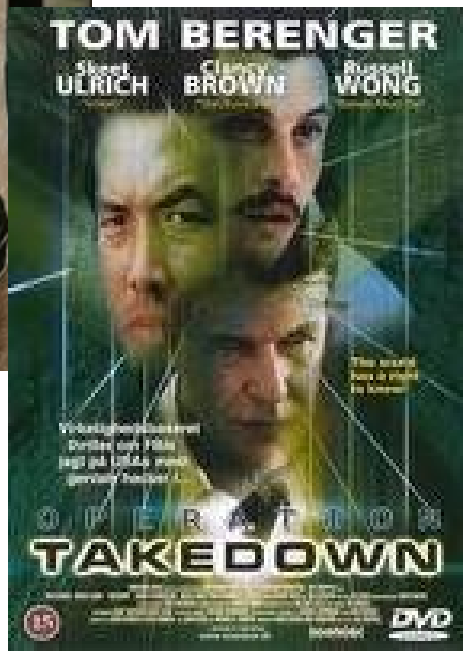
Outro exemplo é quando o ***hacker* utiliza túneis criptográficos** para impedir que um possível sistema de segurança compreenda a ação do *hacker* (comandos, arquivos, etc).

O objetivo destes slides não é aprofundar esses passos (não é focada em ensinar a invadir), para isso leia WALKER, 2012 e GRAVES, 2007.

Alguns Hackers famosos:

Vamos descrever apenas alguns Hackers conhecidos.

Kevin David Mitnick (EUA): O mais famoso hacker do mundo. Atualmente trabalha em uma empresa de segurança da informação, condenado por fraudes no sistema de telefonia, roubo de informações e invasão de sistemas. Os danos materiais que ele causou são incalculáveis.



Kevin Poulsen (EUA): Amigo de Mitnick, também especializado em telefonia, ganhava concursos em rádios. Ganhou um Porsche por ser o 102º ouvinte a ligar, mas na verdade ele tinha invadido a central telefônica.

Mark Abene (EUA): Com o apelido Phiber Optik inspirou toda uma geração a fuçar os sistemas públicos de comunicação e sua popularidade chegou ao nível de ser considerado uma das 100 pessoas mais “espertas” de New York. Divulgou informações sensíveis na Internet, até da Marinha da Austrália. Trabalha atualmente como consultor em segurança de sistema.

John Draper (EUA): Praticamente um ídolo dos três anteriores, introduziu o conceito de Phreaker, ao conseguir fazer ligações gratuitas utilizando um apito de plástico que vinha de brinde em uma caixa de cereais. Obrigou os EUA a trocar de sinalização de controle nos seus sistemas de telefonia. Conhecido como Capitão Crunch ou Crunchman.

Johan Helsingius (Finlândia): Responsável por um dos mais famosos servidores de e-mail anônimo. Foi preso após se recusar a fornecer dados de um acesso que publicou documentos secretos da Church of Scientology na Internet. Tinha para isso um 486 com HD de 200 Mb e nunca precisou usar seu próprio servidor.

Vladimir Levin (Rússia): Preso pela Interpol após meses de investigação, nos quais ele conseguiu transferir 10 milhões de dólares de contas bancarias do Citibank. Insiste na ideia de que um dos advogados contratados para defendê-lo é, na verdade, um agente do FBI.

citibank

Robert Morris (EUA): Espalhou "acidentalmente" um *worm* que infectou milhões de computadores e fez boa parte da Internet parar em 1988. Ele é filho de um cientista chefe do National Computer Security Center, parte da Agência Nacional de Segurança.

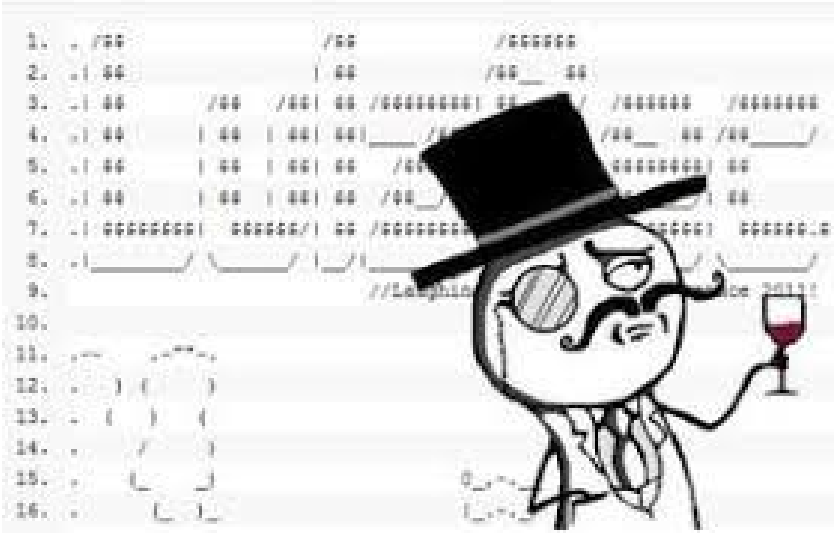
Atenção, os **jornais falam de *hackers*, por exemplo, quando prendem ladrões de caixas eletrônicos de bancos, mas na maioria das vezes esses não são *hackers***. O *hacker* é quem desenvolveu o sistema do roubo (esse tipo de *hacker* apenas vende a tecnologia do roubo e não faz parte diretamente do próprio roubo). Não vá confundir *hacker* com um simples ladrão ou quem usa a tecnologia desenvolvida por *hackers*!

Hacktivismo

As pessoas, apresentadas anteriormente, são *hackers* mais antigos, **atualmente** ainda existem muitos *hackers*. Porém quando ouvimos notícias de *hackers* nos jornais, geralmente estas falam de **grupos de *hackers*** e não de apenas um indivíduo.

Muitos **grupos de hackers estão engajados em algum propósito maior**, que não só o de invasão de computadores. Ou seja, atualmente muitos *hackers* se unem para realizar ações **com fins políticos e sociais**, **o que é denominado de Hacktivismo (*Hacktivism*)**.

Muitos grupos hacktivistas normalmente **têm como alvo** agencias do **governo,** grupos **políticos,** bem como outras **entidades ou indivíduos** que são **identificados como "ruins" ou "errados"**.



Quem são os alvos dos hackers?

- Sites Famosos;
- Empresas de tecnologia;
- Empresas de segurança;
- Concorrentes;
- Governo;
- Vitimas aleatórias;

X

Ataques de Hacker a pessoas comuns

Os Hackers de verdade dificilmente vão querer invadir o computador de uma pessoa comum. Isto por que na verdade um ataque pode ser tedioso e caso o Hacker não tenha uma motivação ele não vai fazer o ataque só por fazer! Mas isto não se aplica aos não Hackers que atacam só por diversão. Então, ataques a pessoas comuns geralmente são ataques de:

Ataques a Privacidade: É o ataque mais comum ao usuário domestico. Já que como é da natureza humana, os atacantes tem compulsão em dar uma olhadinha na vida da vitima e nos dias atuais os computadores são pratos cheios para este propósito.

Destruição: Este tipo de ação pode ser considerada a mais destrutiva, pois pode destruir informações segundos, esses ataques podem ocorrer devido a vírus (o mais comum) e *Crackers***.** O pior nestes casos é que usuários domésticos não têm o costume de fazer copias de segurança.

Obtenção de Vantagens: Para obter vantagens causando incidentes de segurança nos computadores pessoais, geralmente é necessário a utilização de técnicas no qual primeiro a vitima será exposta a ataques de privacidade ou destruição. As motivações deste tipo de ataque são tão distintas quanto seu próprio objetivo real.

Algumas técnicas de ataques utilizadas pelos Hackers:

- Ferramentas automatizadas;
- Engenharia Social;
- Lixo informático - *Spam*;
- *Backdoors*;
- *Wardialing*;
- Falhas clássicas de segurança;
- Falhas novas (*patchers*, *bugs*, etc...);
- Email, WWW, FTP, IRCs, NFS, Telnet, etc;
- Comunidade *underground*;

É claro que isto é apenas uma pequena lista das técnicas usadas por Hacker, inclusive algumas estão defasadas, mas dá para ter uma ideia das ferramentas e do que devemos nos protejer.

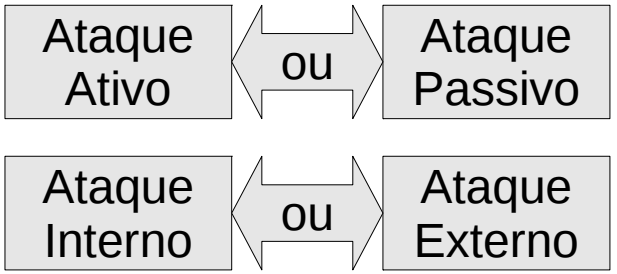
Um pouco mais a respeito de ciberataques

Hackers podem realizar diferentes tipos de ataques. Contudo **ataques podem ser categorizados em passivos e ativos**, sendo que ambos são realizados tanto em redes quanto em *hosts*.

Ataques ativos alteram o sistema ou rede que está sob ataque, afetando sua disponibilidade, integridade e autenticidade dos dados.

Já os **ataques passivos tentam obter informações** a respeito do sistema/rede, ou seja, **não altera o estado da vítima**. Assim, ataques passivos afetem contra a confidencialidade.

Os ataques também podem ser classificados como internos e externos. Os ataques externos partem de fora do ambiente a ser atacado (sistema/rede), atualmente muitos ataques têm como origem a Internet. Ataques internos partem de dentro do ambiente a ser atacado e normalmente esse ataque é mais devastador (GRAVES, 2007).



Outras ameaças fora os Hackers

Conforme os textos anteriores você tem uma chance mínima de ser atacado por um hacker, ou seja, dele pessoalmente arquitetar um ataque contra você ou sua empresa (isto não vale para quem trabalha em grandes empresas).

Mas você pode sofrer ataques de pragas (softwares) criadas por Hackers.

Você provavelmente terá mais problemas de segurança ligados a usuários internos ao seu sistema, fazendo tarefas incorretas, do que outra coisa. Mas fique atento a tudo o que pode afetar a sua segurança.

O seu principal alvo na luta pela segurança de seus dados provavelmente será o seu colega de trabalho, os visitantes do seu sistema, os bisbilhoteiros, o seu administrador de redes, um funcionário insatisfeito e você mesmo é um risco a sua segurança!

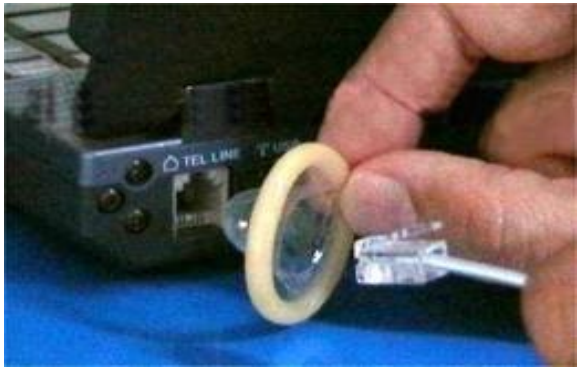
Vamos nos próximos slides ver alguns problemas de segurança comuns em sistemas de computadores.

Vírus

A grande maioria dos problemas relacionados a incidentes de segurança em computadores pessoais são causados por programas maliciosos, dentre os quais estão os vírus.

Vírus é um programa, com uma série de instruções normalmente “maldosas” para o seu computador executar. Em geral, ficam escondidos dentro de uma série de comandos de um programa maior. Mas eles não surgem do nada.

Grande parte da culpa por estragos gerados por vírus cabe à própria vitima. Uma vez que em quase todos os casos ela é a inocente cúmplice do ataque.



Que tipo de vírus de computador você conhece?

Quais já te atacaram? E o que fizeram?

Quem criam os vírus e porque?

É possível solucionar este problema?

Como se prevenir de vírus?

DoS - Denial of Service

DoS é um ataques cujo objetivo é a retirada de serviço do “ar”. É um **ataque a disponibilidade**.

A ideia de um ataque DoS é **tornar indisponível um serviço** tal como memória, disco rígido, um computador pessoal, um servidor, etc.

DDoS - Distributed Denial of Service

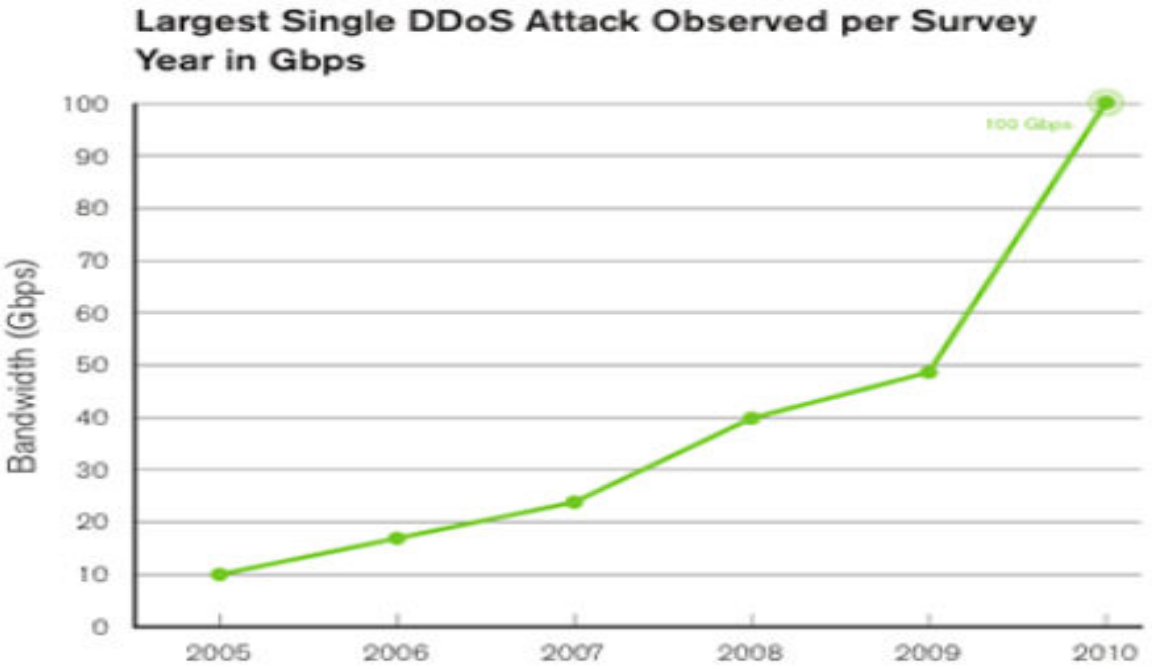
O termo Distributed refere-se a um aperfeiçoamento da técnica do ataque DoS, na qual **a origem do ataque é distribuída** por até milhares de computadores.

Segundo Olhar Digital: *“O Ataque de Negação de Serviço Distribuída - DDoS - consistem em **sobrecarregar os sistemas de serviços populares** da Internet ou sites através do envio maciço de dados para o servidor vítima do ataque. Geralmente, o ataque parte de uma única máquina (Master) que roda um cliente pelo qual outras máquinas (chamadas Handlers) tentam acessar um mesmo servidor da Internet para derrubá-lo através do excesso de dados”*.

Segundo http://olhardigital.uol.com.br

A Arbor Networks divulgou em 01/02/2011 um **relatório aponta** um **crescimento** surpreendente dos ataques DDoS, que pela primeira vez ultrapassaram a marca de 100 Gbps (gigabits por segundo) e cresceram mais de **1000%** nos últimos seis anos. A pesquisa chega a apontar **2010 como "o Ano do DDoS"**, segundo o Security Week.

Segundo a pesquisa da Arbor Networks, o DDoS cresceu em sofisticação e impacto em 2010 e continuará como uma **forma de cyber-protesto ou cyber-crime** de baixo custo durante o ano de 2011. O mesmo é constatado em m relatórios de segurança de 2017 (ver link).



Engenharia Social

Engenharia social é a arte de enganar. Um bom Hacker sabe que **é bem mais fácil corromper pessoas** do que sistemas automatizados.

Esta técnica não é exclusiva dos Hackers, mas sim vem emprestada dos famosos **malandros**.

O que é mais simples tentar quebrar uma senha por força bruta (testando uma a uma por tentativa e erro) **ou perguntar a senha a alguém?** Mas por que uma pessoa passaria a senha? Para isto podemos basicamente ligar para alguém fazendo se passar pelo pessoal da informática da empresa e mentir para um funcionário dizendo:

"sou responsável pelo servidor da empresa e estamos testando se as senhas são adequadas ao sistema! Então você pode me passar a sua senha para mim lhe dizer se está é forte ou fraca?"

Se apenas um funcionário lhe dizer esta senha, é possível quebrar todo o sistema de segurança.

Este **é o famoso 171**, um exemplo deste golpe, fora do mundo dos computadores é o **CONTO DO BILHETE PREMIADO**.

Segundo GRAVES, 2007: **engenharia social é um método não técnico de quebrar a segurança de sistemas ou redes**. É o processo de enganar usuários de sistemas/redes e convencê-los de fornecer informações que podem ser usadas para anular ou burlar sistemas de segurança e/ou obter informações sensíveis.

A engenharia social é uma arma poderosa, pois os ***hackers*** **sabem que o ponto mais fraco da segurança é o ser humano**.

Há **dois tipos de engenharia social**:

- **Baseada em humanos**: refere-se à **interação pessoa-a-pessoa** para conseguir as informações desejadas. Um exemplo é ligar para a empresa e tentar conseguir senhas;

- **Baseada em computadores**: nessa o *hacker* **utiliza algum meio computacional** para tentar obter informações sensíveis. Um exemplo é enviar um e-mail para a vítima pedindo que a vítima entre com seu usuário e senha em uma página Web falsa (***phishing***).

Como a engenharia usa da ignorância humana, a **contramedida** para evitar esse tipo de ataque é **educar as pessoas**, para que elas saibam o que devem ou não passar de informações. Outro bom aliado, nesse sentindo é a **política de segurança**.

Técnicas para proteger o sistema

Vamos introduzir algumas técnicas que ajudam a manter a segurança de sistemas informatizados.

Criptografia

Criptografar significa transformar uma mensagem em outra, “escondendo” a mensagem original, com a elaboração de um algoritmo com funções matemáticas e uma senha especial, chamada chave.

Isto ajuda a manter a confidencialidade das informações.

Criptografia *vem da palavra grega “*kryptos*” = escondida e “*graphia*” = escrever.*

A criptografia basicamente consiste em pegar um texto e transformá-lo em outro incompromissível a pessoas não autorizadas. Para isto podemos simplesmente fazer uso de um algoritmo que ira criptografar o texto e depois o mesmo descriptografa. Ou o que é mais comum hoje, usar um algoritmo e uma espécie de senha (chamada chave) para fazer a criptografia e descriptografia.

Chaves Criptográfica

A chave consiste em uma *string* que pode ser alterada sempre que necessário. Mudando o segredo para se criptografar e descriptografar.

Desse modo, o algoritmo de criptografia pode ser conhecido e de domínio público.

Quando o algoritmo se torna público, vários especialistas tentam decodificar o sistema. Se, após alguns anos, nenhum deles conseguirem a proeza, significa que o algoritmo é bom.

Criptografia de Chave Única

Quando um sistema de criptografia utiliza chave única, quer dizer que **a mesma chave que cifra** a mensagem **serve para decifrá-la**.

Este método é mais útil para cifrar documentos que estejam em seu computador do que para enviar mensagens para amigos. Os métodos de criptografia de chave simples são rápidos e difíceis de decifrar.

As chaves consideradas seguras para este tipo de método de criptografia devem ter pelo menos 128 bits de comprimento.

Criptografia de Chaves Pública e Privada

Este tipo de criptografia utiliza duas chaves diferentes para cifrar e decifrar suas mensagens.

Eis como funciona: com **uma chave você consegue cifrar e com outra você consegue decifrar** a mensagem.

Qual a utilidade de se ter duas chaves então? Você distribui uma delas (a chave pública) para seus amigos e eles poderão cifrar as mensagens com ela, e como somente a sua outra chave (a chave privada) consegue decifrar, somente você poderá ler a mensagem.

Assinatura digital

A criptografia de chave pública/privada também funciona ao contrário, se você usa a chave privada para cifrar a mensagem, a chave pública consegue decifrá-la. Parece inútil, mas serve para implementar um outro tipo de serviço em suas mensagens (ou documentos): a assinatura eletrônica.

Já que podemos constatar que somente a chave pública de uma chave privada pode verificar a informação isto **prove não repúdio**.

A assinatura eletrônica funciona de seguinte maneira:

O texto de sua mensagem é verificado e nesta verificação é gerado um numero, e este número é calculado de tal forma que se apenas uma letra do texto for mudada, pelo menos 50% dos dígitos do número mudam também, este número será enviado junto com sua mensagem, mas será cifrado com sua chave privada.

Quem receber a mensagem e possuir sua chave pública vai verificar o texto da mensagem novamente e gerar um outro número. Se este número for igual ao que acompanhar a mensagem, então a pessoa que enviou o e-mail será mesmo que diz ser.

Hoje quando se fala em segurança logo se fala de criptografia. **Uma grande gama de soluções de segurança vão utilizar técnicas de criptografia para tentar manter o seu sistema seguro**, por sito é bom saber o básico sobre criptografia.

A maioria por navegadores da Internet, fazem uso da criptografia em site **HTTPS** por exemplo e fazem uso de certificados digitais (são os que proveem os “cadeadinhos” no canto do navegador dizendo que o site é seguro).

A Criptografia é Segura?

Por mais poderosa que seja a receita de criptografia, ainda assim ela pode ser decifrada. O importante é saber em quanto tempo isto pode ocorrer.

Por exemplo, no caso de métodos de chave única:

Chaves de 40 bits – em alguns dias podem ser decifradas, testando todas as 2^{40} chaves possíveis.

Chaves de 128 bits – um supercomputador demoraria alguns milhões de anos.

Mas isso é o caso de se testar todas as chaves possíveis e, é claro que podem existir falhas na receita da criptografia. E normalmente, as quebras das chaves são realizadas por força bruta mesmo, testando uma por uma até descobrir a chave utilizada.

Vantagens da Criptografia:

- Proteger a informação armazenada em trânsito;
- Deter alterações de dados;
- Identificar pessoas;

Desvantagens da Criptografia:

- Não há como impedir que um intruso apague todos os seus dados, estando eles criptografados ou não;
- Algum intruso pode modificar o programa para modificar a chave. Desse modo, o receptor não conseguira descriptografar com a sua chave;

Ambientes de redes de computadores e a segurança

Hoje em dia quase **todo o mundo está utilizando a Internet** para entretenimento e negócios.

Atualmente **existem empresas que apenas atuam na Internet** e que devem ter um cuidado além das outras com suas informações.

Na gestão empresarial integrada **na Empresa Virtual, os gestores devem se preocupar com**:

- Quão seguros estão os **bancos de dados** da empresa;
- Quais os **planos de contingência** em caso de catástrofe;
- Qual o **nível de confiança nas pessoas**, sejam internas, parceiros ou terceirizados;
- Qual o critério de **auditoria para prevenir desastres**;
- Qual tipo de **treinamento** para as pessoas envolvidas em todo o ciclo da informação;
- Quais os **aspectos jurídicos** a serem tratados com o uso incorreto da informação;
- Quais os procedimentos de **auditoria interna e externa** de sistemas;

Preocupações de empresas da Internet

Preocupações com **transações com cartão de credito** são uma das grandes preocupações tanto por parte do consumidor quanto da empresa eletrônica ou do banco.

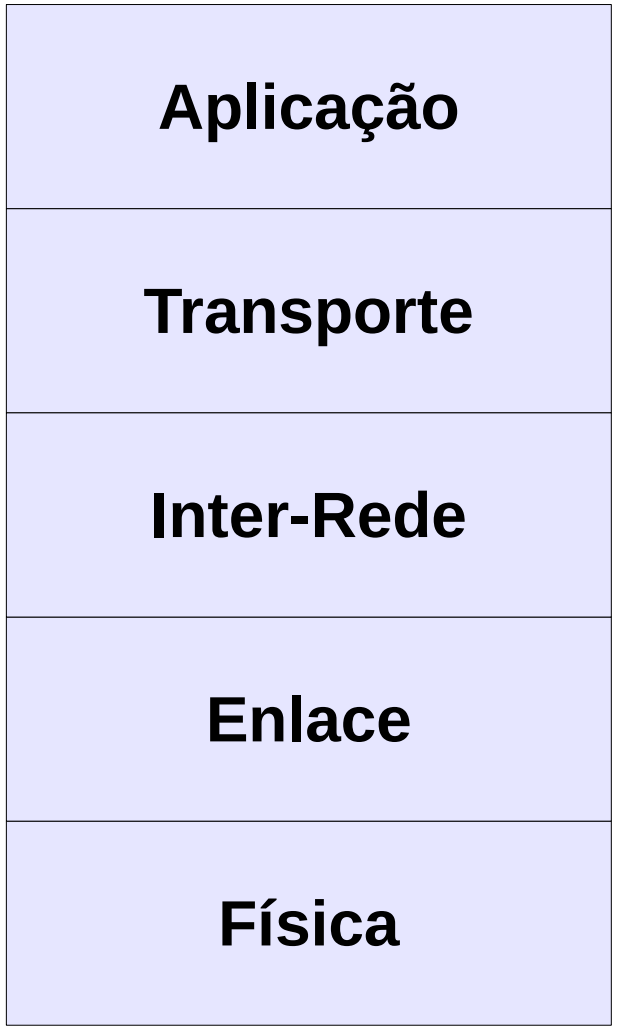
Existe a dificuldade das empresas de cartão de crédito aceitarem pagamento pela rede, devido ao fato de que elas estão bancando sozinhas, até então, o investimento na segurança. A saída está nas parcerias entre as instituições financeiras para a diluição desse custo.

A atual "ausência" de segurança no pagamento on-line está impedindo que grandes segmentos da população efetuem suas compras.

No mundo internacional das redes e com o comércio eletrônico, todo sistema de computador se tornou um alvo em potencial para intrusos. O problema é que não há como saber os motivos que levam o intruso a agir e nem quando ele pode atacar.

Contudo **é importante tentar se prevenir utilizando mecanismos de proteção**, impedindo, ou pelo menos dificultando, o acesso por pessoas não autorizadas.

Alguns elementos da segurança de redes - referenciados em TCP/IP



Proxy, etc.

Firewall, etc.

Roteadores, etc.

Switch, criptografia, etc.

Meios de transmissão – fibra, cobre, wireless, etc.

Vamos definir que tipo de segurança que alguns desses elementos nos proporcionam.

Segurança na Camada Física

A camada física deve ser a camada que mais **sofre com** problemas relacionados a **erros**, só isto já é um grande problema de segurança.

Outro grande problema com a camada física é que ela **é a mais vulnerável quanto a interceptação**. Isto se dá devido a transmissão do sinal pelo meio físico por difusão. Da mesma forma que podemos capturar conversas telefônicas em cabos de cobre (par trançado, por exemplo), podemos também fazer escuta de dados.

Em meios de transmissão sem fio o problema de escuta só cresce! Quem é que nunca ouviu falar da Sky do Paraguai? Este problema ocorre devido a fragilidade da camada física.

A maioria das soluções para a falta de segurança na camada física se dão na camada de enlace. Mas algumas possíveis **soluções** da própria camada física são:

- O uso de **fibra óptica**, que dificulta o acesso ao meio sem interromper a transmissão.
- O uso de **cabos com gás pressurizado** que “avisam” quando alguém tentar fazer um grampo.

Segurança na Camada de Enlace

Como vimos a camada física é cercada de problemas de segurança.

A camada de enlace pode ser a primeira linha de defesa do host.

Em ambientes onde é difícil controlar que recebe a difusão do sinal, tal como em rede sem fio, podemos implementar algum tipo de **criptografia de dados** e só quem tem a chave é que vai receber o sinal. Isto é usado em redes WiFi com WEP e WPA, por exemplo. A SKY se protege da mesma maneira dos aparelhos “hermanos”. A ideia é que o sinal chegue a qualquer um pela camada física, mas a camada de enlace pode selecionar para quem os dados serão disponíveis.

O **Switch** também ajuda e muito na segurança, pois ele **não permite a difusão de pacotes para todas as portas** do switch, como faria um hub. O Switch segmenta a transmissão dos dados apenas da porta de origem para a porta de destino o que escutas por software promíscuos (sniffers). Antes do switch era comum usuários obterem facilmente senhas pela rede.

As **VPN's** que criptografam dados também iniciam seu funcionamento na camada de enlace e se estendem até a camada de aplicação.

Segurança na Camada de Inter-Rede

Os **roteadores**, peças fundamentais da camada de Inter-Rede podem fazer o papel de guardas dizendo quem pode ou não acessar uma dada rede.

Roteador são dispositivos que encaminham pacotes pelas redes. Responsáveis por saber como toda a rede está conectada e como transferir informações de uma parte da rede para outra. Em poucas palavras, eles evitam que os hosts percam tempo assimilando conhecimento sobre a rede.

Roteadores podem estar conectados a duas ou mais redes.

Em se tratando de segurança, o objetivo de um roteador **pode ser manter um isolamento "político"**. Estes roteadores permitem que dois grupos de equipamentos comuniquem-se entre si e ao mesmo tempo continuem isolados fisicamente.

Os roteadores, em sua maioria, possuem função de filtragem de pacotes, que permitem ao administrador de rede controlar com rigor quem utiliza a rede e o que é utilizado na mesma.

Isto é muito próximo do que faz um firewall, que veremos a seguir.

Segurança na Camada de Transporte

Um roteador poderia ver apenas endereços de origem e destino, o protocolo que o datagrama IP carrega, fazendo filtragem baseados nessas informações.

Para poder fazer filtragem por serviço de rede temos que subir para a camada de transporte. Aqui podemos **filtrar pacotes baseados em serviços** e em alguns casos até regular o **sentido do fluxo de pacotes**. É justamente par isto que surge o **firewall** de filtro de pacotes na camada de transporte.

O Firewall é um conjunto de hardware e software utilizado para proteger computadores na rede, ou até mesmo proteger a rede.

Muitas organizações optam por proteger a sua rede interna de ataques externos, com uma espécie de isolamento, onde as pessoas de “fora” não atacam a sua rede interna sem primeiro contatar suas premissas.

Esse “isolamento” é criado utilizando o *Firewall*, que do mesmo modo pode controlar o acesso da rede interna à Internet.

Portanto o *Firewall* é uma **barreira inteligente entre a rede local e a Internet**, através da qual só passa tráfego autorizado.

Segurança na Camada de Aplicação

O Firewall não consegue ver o conteúdo dos pacotes na camada de aplicação, então para resolver este problema surgem os proxys.

Uma maneira de se tornar seguro um serviço, é não permitir que cliente e nem servidor interajam diretamente. ***Proxy*** *System* são sistemas que **atuam em nome do cliente** de uma forma transparente.

O *Proxy System* atua como um procurador que aceita as chamadas que chegam e verifica se é uma operação valida. Se a chamada solicitada é permitida, o servidor procurador envia adiante a solicitação para o servidor real.

Depois que a sessão é estabelecida à aplicação procuradora atua como uma retransmissora e copia os dados entre o cliente que iniciou a aplicação e o servidor. Devido ao fato de todos os dados e que todos os dados entre o cliente e o servidor serem interceptados pelo *Application Proxy*, ele tem controle total sobre a sessão e pode realizar um *logging* tão detalhado como desejado. **O proxy pode filtrar o conteúdo da camada de aplicação.**

Existem várias outras ferramentas de segurança nesta camada mas por enquanto vamos parar por aqui.

Vamos concluir com premissas básicas de segurança:

“Não existem sistema 100% seguro”
“Não existe rede 100% segura”
“Nada é totalmente seguro”

Isto é uma afirmação!!! E uma verdade que deve ser conhecida por todos...

Então:

- Você usaria hoje, em seu computador pessoal, um programa de *Internet banking* para fazer transferência de dinheiro?
- Você faria compras na Internet, mesmo sabendo que o site/loja possui um servidor seguro, digitando seu cartão de credito no seu computador pessoal?
- Você trataria de assuntos importantes da sua vida pessoal e profissional, na qual se utiliza de dados particulares, através de simples e-mails, MSN, IRC, ICQ, etc...?
- Se você respondeu não para todas essas perguntas então para que serve a Internet?

Calma...

Felizmente **temos meios tentar reduzir os riscos**, das ações contra a nossa vida na on-line. Portanto o risco sempre vai existir, já que como foi dito anteriormente:

“Não existem sistemas 100% seguros”

Mas **podemos aumenta no nível de confiabilidade** da rede, de modo que possamos evoluir na utilização da tecnologia até um patamar mais confiável e consequentemente mais eficaz.

Uma grande lição a ser aprendida

Da mesma forma que não existe sistema 100% seguro **não existe uma solução milagrosa** que você compra em uma prateleira e que resolva todos os seus problemas de segurança.

Pense bem, se este tipo de solução existisse será que um dos homens mais ricos do mundo não compraria e incorporaria no seu sistema operacional?

Cuidar da segurança é como cuidar de um jardim ou subir uma escada rolante infinita que desce enquanto você sobe.

Segurança é como jardim

Tempo

Segurança é subir uma escada rolante infinita no sentido contrário

Conclusão

Como foi dito a **segurança não é um processo que tem fim**... Você pode trabalhar em um sistema para deixá-lo muito, muito seguro mas, a partir do momento em que você virar as costas, falhas de segurança começaram a brotar neste sistema. Depois de alguns dias ou semanas este sistema vai estar tão inseguro ou mais do que quando você iniciou o processo.

A **segurança deve ser cultivada dia a dia**, tal como um jardim. Caso contrário as ervas daninhas vão aparecer.

Saber que o seu sistema nunca vai estar 100% seguro é o primeiro passo para um nível de segurança maior. Pois se você sabe que tem problemas você vai se proteger e não ficar na ignorância que o seu sistema é a prova de falhas.

Lembre-se que a segurança computacional é muito ampla e você não vai conseguir contemplar todos os itens... então **foque no principal**, que geralmente é a **informação** contida em seu sistema.

Não vá também “tentar matar uma pulga com uma espingarda”. **Pondere custo versus benefício** caso contrário você falhará também devido a cortes de custo.

Referência:

WALKER, Matt. CEH Certified Ethical Hacker – Exam Guide. McGraw-Hill Companies. 2012.

GRAVES, Kimberly. CEH Official Certified Ethical Hacker Review Guide. Wiley Publishing. 2007.

TANENBAUM, Andrew S. Redes de Computadores. Editora Campus, 4 Edição. 2003.

WADLOW, Thomas. Segurança de Redes. Editora Campus. 2000.

MCCLURE, Stuart; SCAMBRAY, Joel; GEORGE, Kurtz. Hackers Expostos. Editora Makron Books. 2002.

DIGITAL, Olhar. Ataques DDoS crescem 1000% em seis anos. Disponível em: http://olhardigital.uol.com.br/produtos/digital_news/noticias/ataques_ddos_crescem_1000_desde_2005 Acessado em: 03/02/2011.

Algumas informações sobre Hackers foram retiradas de http://www.wikipedia.org/ em 02/02/2011.

Fim!