FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE - FANESE
NÚCLEO DE PÓS-GRADUAÇÃO E EXTENSÃO – NPGE
CURSO DE PÓS-GRADUAÇÃO "LATO SENSU"
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

KARINNE ROCHA QUEIROZ MENEZES

SEGURANÇA EM REDES DE COMPUTADORES: melhores práticas de segurança em redes de computadores

Aracaju – SE
2010

KARINNE ROCHA QUEIROZ MENEZES

SEGURANÇA EM REDES DE COMPUTADORES: melhores práticas de segurança em redes de computadores

Trabalho de Conclusão de Curso apresentado ao Núcleo de Pós-Graduação e Extensão da FANESE, como requisito para obtenção do título de Especialista em Redes de computadores.

Orientador:

Aracaju – SE
2010

KARINNE ROCHA QUEIROZ MENEZES

SEGURANÇA EM REDES DE COMPUTADORES: melhores práticas de segurança em redes de computadores

Trabalho de Conclusão de Curso apresentado ao Núcleo de Pós-Graduação e Extensão – NPGE, da Faculdade de Administração de Negócios de Sergipe – FANESE, como requisito para a obtenção do título de Especialista em Redes de Computadores.

_____

Nome completo do Avaliador

_____

Nome completo do Coordenador de Curso

_____

Nome completo do Aluno

Aprovado (a) com média: _____

Aracaju (SE), ____ de _____ de 2009.

RESUMO

Em uma rede de computadores estão envolvidos ativos de redes, equipamentos, sistemas operacionais, sistemas desenvolvidos por programadores e analista, infra-estrutura de rede, sala de servidores, computadores e por final o ser humano. Assim, o fator humano sendo como o elo mais fraco da segurança, este é o fator que deve ser mais tratado, até porque mesmo tendo aplicado as melhores práticas de segurança recomendado pelos especialistas, os melhores produtos de segurança recomendado, mesmo assim esta empresa ainda está vulnerável. Neste artigo iremos explanar as melhores práticas de segurança para proteger as redes de computadores, abordaremos como proteger o sistema operacional e toda infra-estrutura que existe para se manter redes e também falaremos do fator humano e o quanto contribui para as diversas falhas que ocorrem no nosso dia a dia, aplicado as melhores práticas de segurança recomendado pelos especialistas, e os melhores produtos de segurança.

Palavras-chave: Redes de computadores. Segurança. Fator Humano. Vulnerabilidade. *Hardening*. Ataques.

ABSTRACT

In a computer network involves active networks, equipment, operating systems, systems developed by programmers and analyst, infrastructure, network, server room, computers and ultimately humans.
Thus, the human factor as being the weakest link in security is the factor that should be further treated, because even having applied the best practices recommended by security experts, the best security products recommended, even so the company is vulnerable.
In this article we will explain the best security practices to protect computer networks, we will discuss how to protect the operating system and all the infrastructure that exists to maintain networks and also talk of the human factor and his contributions to the various failures which occur in our day by day, applied to the best practices recommended by security experts, and the best security products.

Keywords: Computer networks. Security. Human Factor. Vulnerability. Hardening. Attacks.

LISTA DE TABELAS

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

No inicio as redes de computadores surgiram com o intuito de compartilhar recursos computacionais, ligação entre equipamentos, dados e dessa forma, interligando várias redes. A interoperabilidade estava em voga, mais não segurança. Então as redes de computadores foram crescendo e interligando o mundo, cada rede que surgia tinha o elemento de conexão que interligava redes com outras redes e ainda nem se tinha surgido à internet. (Tanenbaum, 2002)

A configuração de redes relativamente pequenas não é uma tarefa difícil, agora configurar uma rede corporativa, envolvendo outras redes, situadas em pontos remotos, pode se tornar algo um tanto difícil e complexo.

No mundo de hoje, onde vermos a convergência de todas as tecnologias, onde se prega a interoperabilidade entre os sistemas, disponibilidades, integridade, está cada vez mais difícil evitar os ataques que acontecem nas empresas, corporações, escolas, entidade governamentais, federais e entre outros. Devido que o mundo gira em torno de informações que é o maior bem que uma empresa possui, como por exemplo, o cadastro de clientes onde possui dados sigilosos como nome, CPF endereço, número de cartão de crédito e etc. São informações preciosas.

Não é de hoje que o homem vem guardando as informações, temos, por exemplo, na época dos antigos reinos em que se pintava um jarro e ali naquela pintura estava codificada a mensagem e só a decifrava o autentico destinatário. E hoje não é tão diferente, pois a mensagem é escrita e encaminhada por meios que a deixem cifrada e quando chegar ao seu destino correto a mesma seja decifrada, nota-se que ambos os processos houve segurança na informação para que a mesma chegue ao seu destino de forma inviolável e em ambas as épocas, tanto nessa nossa atualidade existe mecanismos, políticas para o sigilo, assim como também na época dos antigos reis existiam mecanismos que guardavam o sigilo das mensagens, já pensou se vaza a informação que o rei mandou matar o seu traidor, ou nos dias de hoje se vaza a informação da senha bancária de Bil Gates.

Todos esses aspectos estão atrelados ao fator humano, este pode burlar qualquer das melhores práticas que sejam utilizadas para se manter a segurança, pois é o elo mais fraco que existe e notamos que as corporações estão investindo muito na modernização dos seus parques tecnológicos e estão deixando de lado o fator humano. No decorrer deste artigo iremos explicar as melhores práticas que

devemos utilizar e assim, dessa forma, dificultarmos os acessos indevidos, ataques que venham a causar danos irreversíveis.

Dessa maneira, o objetivo deste trabalho é estudar a segurança em redes de computadores de modo que os administradores de rede e profissionais da área conheçam melhor as melhores práticas de segurança em redes de computadores e estejam mais preparados para aplicar melhorias em suas infra-estruturas.

O estudo será dividido em três etapas. A primeira, que neste trabalho será apresenta a segurança de uma maneira geral e focando a segurança em redes de computadores, mostrando o que devemos proteger, utilizando as melhores práticas. Em uma segunda etapa, vamos analisar o fator humano, sendo este o elo mais fraco dentro da segurança em redes. E na terceira etapa abordaremos os métodos que devemos utilizar para torná-lo mais robusto, o sistema operacional Windows na sua versão XP e como aplicar.

O método utilizado deste estudo foi a pesquisa bibliográfica de vários livros e artigos publicados. A idéia em si foi fazer uma revisão literária dos livros, artigos científicos, sites da internet, bibliotecas virtuais fazendo uma contextualização. Todo esse material sobre o assunto foi organizado, selecionado, analisado e dessa forma, trazer um resultado que possa ser aplicado em diversas redes de computadores e assim, possa trazer melhor controle, qualidade e segurança, no complexo mundo virtual em que vivemos hoje.

2 SEGURANÇA

Nos dias atuais se preza muito pela segurança, seja esta para proteger a integridade ou bem-estar físico ou para garantir a segurança dos bens ou interesses protegendo de riscos, perigos ou perdas, ou seja, é uma proteção que sempre almejamos que muitas vezes de forma bruta é tirada e quando menos esperamos existe um invasor que esteja dentro de sua casa, burlando normas e condutas. Geralmente são pessoas mal intencionadas que querem tirar proveito de alguma coisa.

No mundo da informática não é tão diferente do mundo físico, a diferença é que lá o mundo é virtual e as invasões é uma realidade virtual, onde se explora as vulnerabilidades. Assim, devemos também proteger os nossos ativos, utilizando segredos, fechando portas de comunicação, colocando barreiras, buscando várias formas de dificultar o acesso. Iremos também abordar a segurança da informação, o maior bem que uma empresa possui e como protegê-la de possíveis furtos. (Mitnick. Simon, 2003).

Os tipos mais comuns de vulnerabilidades são:

- Físicas - uma pessoa não autorizada acessa o ambiente físico causando um ato de vandalismo ou sabotagem.
- Naturais - Como exemplo teve o furação catrina que destruiu várias redes de computadores, ou seja, são desastres naturais e se acontecer somos vulneráveis.
- Hardware - Software – Sempre é necessário ter redundância de hardware e software, pois existindo falhas pode comprometer toda segurança que foi implantada deixando brechas para uma invasão.
- Mídias – Fitas dat, CDs e DVDs ROM podem ser danificados ou roubados.
- Comunicação – Este deve ser tratada mais delicadamente para que não seja capturada e alterada na sua origem e destino, trazendo dados incorretos que venham a trazer transtornos à organização. Assim, todos esses, mecanismos devem ser utilizados para garantir toda comunicação existente na rede de computadores.

- Humanas – O elo mais fraco na segurança, pois pessoas sem treinamentos podem utilizar sistemas de forma indevida, ou simplesmente entregando a sua senha para outra pessoa e tantas outras coisas podem acontecer.

> As ameaças são divididas em três categorias: natural, não-intencional e intencional. A natural atinge qualquer tipo de espaço físico ou parte de equipamentos como exemplos: incêndios, inundações, entre outros desastres. A não-intencional acontece por ignorância do usuário ou do administrador do sistema, onde os mesmos não são treinados apropriadamente. A intencional é aquela que alguém propositadamente toma atitudes no sentido de danificar, roubar, acessar ou alterar algum sistema ou informação alheia. Disponível em < http://www.frb.br/ciente/2006_2/BSI/BSI.SANCHES.etal.F1%20_Rev.%2028.11.06_.pdf

2.1 Seguranças de redes

Logo quando surgiram as redes de computadores, esta foi principalmente utilizada por pesquisadores universitários, com a finalidade de enviar e receber mensagens de correio eletrônico, e também por funcionários de empresas, para compartilhar recursos, como impressoras, scanners e leitura ótica.

Dessa forma, não existia a preocupação com a segurança. Mas como hoje em dia milhões de pessoas estão usando as redes para acessar informações como contas bancárias, fazer compras e guardar a sua devolução de imposto de renda.

A segurança é um assunto abrangente e inclui inúmeros tipos de problemas. E na sua forma mais simples, a segurança se preocupa em garantir que pessoas mal intencionadas não leiam ou modifiquem mensagem enviadas a outros destinatários. E também há pessoas que tentam ter acessos remotos a serviços que não estão autorizados a utilizar. (Kurose, 2004)

> Segurança em uma rede, é a proteção de um sistema de computador e seus dados contra perda ou danos, implementada especialmente para que só usuários autorizados possam obter acesso a arquivos compartilhados. Disponível em <http://://www.juliobattisti.com.br/tutoriais/keniareis/dicionarioinfo007.asp />. Acesso em: 03 Dez. 2009.

2.2 - Princípios da Segurança em Redes de Computadores

Para que haja comunicação segura é necessário que sejam adotadas políticas de segurança de forma adequadamente, sabendo que cada situação deve ser analisada e devendo identificar os principais pontos de vulnerabilidades. Dessa forma, podemos identificar esses pontos através de princípios básicos de segurança.

Quando há a utilização desses princípios básicos de segurança há redução de riscos de fraudes, erros, vazamentos ou roubo de informação, sabotagens, uso indevido e outros.

Os pilares de qualquer política de segurança incluem o seguinte: Autenticação: Controla a autenticidade, assegura que é legítima verdadeira a identificação de um usuário ou computador, ou verificar que os contatos são feitos com pessoas que são exatamente representando a sua identidade.

Política de Privacidade: A capacidade de manter as coisas privadas e confidenciais, ou seja, proteger a informação de pessoas não autorizadas contra leitura e/ou cópia.

Disponibilidade: é a garantia de que uma informação sempre poderá ser acessada, pelas pessoas e processos autorizados, independentemente do momento em que ela é requisitada e do local no qual está armazenada.

A disponibilidade está vinculada à redundância, confiabilidade (precisão, taxas de erros, estabilidade e período de tempo entre falhas) e à recuperação de desastres.

Integridade: Processo de garantir um sistema ainda não foi comprometido e permanecer seguro, inviolável, ou seja, a informação foi manipula mais continua com as características originais do proprietário.

2.3 Criptografia

A palavra *criptografia* origina-se das palavras gregas *kryptos* (ocultar) e *logo* (palavra) e está longe ser nova. De fato, os antigos egípcios utilizavam criptografia há 4.000 anos. A criptografia tem uma vasta utilização principalmente na tecnologia da informação.

A criptografia é utilizada desde antes de Cristo com o objetivo de cifrar as informações, gerando uma nova mensagem cifrada onde somente o receptor autorizado tem como decifrá-la resgatando a mensagem original. Existem diversos tipos de algoritmos de criptografia, como exemplo o RSA, MD5, SHA, Quântico. Estes são classificados ou tipificados como algoritmos Simétricos, Assimétricos, *Hash* e Quântico.

2.3.1 Criptografia simétrica

A criptografia simétrica, também conhecida como chave privada, é baseada em uma chave secreta que é compartilhada pelas duas partes envolvidas na "negociação". Esta é a criptografia tradicional, onde a mesma chave utilizada na codificação dever utilizada da decodificação. (Gues; Nakamura, 2003).

Além do mais, a criptografia de chave simétrica – modelo único até a década de 1970 – apresentava a dificuldade do problema da distribuição de chaves (Burnett & Paine, 2002).

WADLOW, Thomas A, descreve que essa técnica é bastante eficiente em conexões seguras para a internet, onde processos computacionais trocam informações temporárias para algumas transmissões críticas. Quando se navega pela internet e visita sites ditos "seguros", onde geralmente são preenchidos dados sigilosos, estamos utilizando o SSL (*secure sokets Layer*) que funciona à base de criptografia simétrica, algoritmo é RSA.

2.3.2 Criptografia Assimétrica

A maneira de contornar os problemas da criptografia simétrica é a utilização da criptografia assimétrica ou de chave pública. A criptografia assimétrica está baseada no conceito de par de chaves: uma chave privada e uma chave pública. Qualquer uma das chaves é utilizada para cifrar uma mensagem e a outra para decifrá-la. As mensagens cifradas com uma das chaves do par só podem ser decifradas com a outra chave correspondente. A chave privada deve ser mantida secreta, enquanto a chave pública disponível livremente para qualquer interessado.

2.3.3 Hash

Um hash é uma seqüência de letras ou números gerados por um algoritmo de Hash. Esse tipo de criptografia é usado quando não é necessário recuperar o valor original do dado criptografado, são muito usados para comparação de senhas. A função hash, h(k), transforma uma chave k num endereço relativo do registro. (PIMENTEL,CRISTINA 2008)

Hosner define hash como "uma função matemática de via única (one-way function), que cria um sumário criptográfico de uma mensagem. Você alimenta um texto em uma função de hash, e ela retorna um bloco de texto cifrado de tamanho fixo que não pode ser revertido à mensagem original".

2.3.4 Criptografia quântica

As criptografias conhecidas atualmente são muito seguras, mas com a evolução da computação quântica a quebra de uma chave criptográfica que antes levaria anos passaria a ser resolvido em pouco tempo, pelo motivo que na computação quântica varias combinações pode ser testadas em paralelo, fato que não é possível na computação tradicional. Para tentar resolver este problema surgiu à criptografia quântica que a principio não tem relação direta com a computação quântica e sim pelo fato que as duas utilizam os princípios e características da física quântica.

A criptografia quântica surgiu bem antes do surgimento dos computadores quânticos na década de 60, em um artigo (que não chegou a ser publicado) criado por Stephen Wiesner. Os primeiros passos reais para a criptografia quântica se deram na década de 80, onde foram aplicados conceitos de chave publica. Mas sugiram alguns problemas, o armazenamento de fótons é impossível de serem realizados utilizando as tecnologias conhecidas atualmente, com isto os cientistas se voltaram para a troca de chaves de criptográficas que é um grande problema das criptografias atuais.

- **Fótons**

Os fótons são à base da criptografia quântica. A característica utilizada do fóton é a polarização, o fóton vibra em sua propagação podendo gerar três movimentos: linear, circular e elíptico. Esta polarização pode ser medida, mas após sua medição a polarização do fóton muda. Esta característica de mudança de polarização é utilizada para identificar se existe algum espião na escuta.

- **Aplicação da Criptografia Quântica**

Apesar do nome Criptografia Quântica já ter se tornado comum no meio científico, na realidade ela engloba apenas a troca segura de

> chaves, utilizando para isso, princípios da Mecânica Quântica, mais precisamente, a natureza quântica dos fótons. É preciso, portanto, utilizar métodos clássicos para a troca da mensagem propriamente dita. Devido a isso, a Criptografia Quântica também é conhecida como Distribuição Quântica de Chaves ou QKD (Quantum Key Distribuition). Disponível em http://www.dsc.ufcg.edu.br/~gmcc/mq/criptografia.html

2.4 Segurança da comunicação

Agora iremos tratar da comunicação e o que devemos fazer para que a informação saia da sua origem até o destino, levando os bits secretamente e sem alterações.

Em grandes corporações, já sabemos que a informação é o seu maior bem, como a mesma trafegar por várias redes até chegar o seu destino de forma segura, até porque hoje tudo está interligado a Internet e estamos em contato com o mundo e vice-versa podemos acessar recursos em servidores do mundo, porém o nosso computador também pode ser acessado por pessoas do mundo, se não tomarmos alguns cuidados básicos com segurança, então existem mecanismos que iremos descrever agora que são utilizados. (Tanenbaum, 2002).

Dessa forma, sempre utilize um programa de antivírus, escolha, instale um que saiba configurar e deve mantê-lo atualizado. Os custos são baixos se comprar um e existe até programas gratuitos. A não utilização é arriscada, pois mensagens contendo anexos com vírus, sites com conteúdo dinâmico que podem causar danos, etc., são muitas as ameaças e o antivírus é capaz de nos proteger de grande parte delas. Também é importante sempre se manter atualizado sobre informações de novos vírus que foram lançados, trotes que são passados por e-mail, novos tipos de ataques e perigos que possam comprometer a segurança do seu computador.

Existem diversos tipos de vírus e *worms* que podem vir embutidos em anexos que geralmente são enviados naquelas correntes que dizem que se você não encaminhar terá azar pro resto de suas vida se tantos outros artifícios utilizados. Então, devemos nos precaver para não ficarmos disseminando essa atitude de ficar todo tipo de e-mail encaminhado para toda lista de endereço e depois começamos a receber diversos e-mails de propagandas e muito delas é enganosa contendo programas maliciosos.

Vírus, *worms* e *trojans* são tipos de códigos maléficos da categoria *malware* (*malicious software*) desenvolvidos para executar ações que causam danos em um computador. Disponível em http://www.symantec.com.br/malwares.html

Outro mecanismo que devemos utilizar para evitar vazamentos de informações, principalmente dentro de empresas onde vírus, vermes e outras pestes digitais podem burlar a segurança, e destruir dados valiosos e consumir muito tempo dos administradores de redes.

Assim, devemos utilizar o mecanismo *firewall* que é uma forma antiga de segurança sendo utilizada nos dias atuais.

> Os firewalls são apenas umas adaptações moderna de uma antiga forma de segurança medieval: cavar um fosso profundo em torno do castelo. Esse recurso forçava todos aqueles que quisessem entrar ou sair do castelo a passar por uma única ponte levadiça, onde poderiam ser revistados por guardas. Nas redes, e possível usar o mesmo artifício: uma empresa pode ter muitas *LANs* conectadas de forma arbitraria, mas todo o trafego de saída ou de entrada da empresa e feito através de uma ponte levadiça eletrônica (*firewall*) (Tanenbaum, 2002)

Outra maneira de se prevenir é utilizando uma ferramenta de detecção de intrusão. A ferramenta funciona da seguinte forma, em segundo plano verificando se alguém está tentando entrar no seu sistema ou se algum usuário legitimo está fazendo mau uso do mesmo. Á medida que vai checando alguma coisa que é suspeita e ilegal envia uma notificação ou e-mail para o administrador do sistema.

Dessa forma, a utilização de uma ferramenta de detecção de intrusão para analisar as tentativas de ataques auxilia na segurança de redes de computadores.

Assim, poderemos detectar de onde está partindo uma invasão podendo então bloquear a comunicação com a origem, evitando uma possível violação.

3 ENGENHARIA SOCIAL

Método utilizado para se obter informações de maneira fácil, e também uma das técnicas mais antigas de roubo de informações, bastando somente passar um boa conversa e normalmente se ocorre quando queremos obter informações sigilosas. Isso é muito comum hoje em dia e acontece frequentemente, há exemplos do tipo de numa conversa de fim de semana bebendo uma cervejinha e comentamos que estamos conseguindo determinada meta e de repente o nosso amigo chega à frente. Devemos ter em mente que a informação deve ser tratada com sigilo, cautela, sempre saber o que dizer, para não falar mais do que o necessário e entregar o ouro ao bandido.

Assim, também acontece em grandes empresas, órgãos do governo, instituições militares, financeiras e hospitais, o ataque já é executado por *hackers* pessoas mais especializadas em roubo de informações, tendo como objetivo ter acesso a sistemas não autorizado, sobrecarregar os sistemas.

3.1 Métodos comuns da engenharia social

Existem vários motivos que podem causar a falta de segurança e assim, uma informação sigilosa cair em mãos indevidas e ser usada para fins promíscuos. Descreveremos alguns perfis e os motivos que levam a fazer determinadas atitudes.

O estudante que fica se divertindo bisbilhotando as mensagens de correio eletrônico de outras pessoas. O Cracker que testar o sistema de segurança de alguém; roubar dados. Representante de vendas quer representar todo o mundo e não apenas uma região. Executivo almejar descobrir a estratégia de marketing do concorrente. Ex-funcionário vingar-se por ter sido demitido, ou por diversas humilhações passadas no ambiente de trabalho. Contador para desviar dinheiro de uma empresa. Corretor de valores nega uma promessa feita a um cliente através de uma mensagem de correio eletrônico. Vigarista Roubar números de cartão de credito e vendê-los. Espião querendo descobrir segredos militares ou industriais de um inimigo. Terrorista roubando segredos de armas bacteriológicas. (Tanenbaum, 2002)

Assim, juntamente com os motivos e atitudes de cada individuo possa vir a ter, também se utiliza de métodos comuns de engenharia social. É necessário que

as organizações, empresas informem aos seus funcionários os métodos utilizados da engenharia social.

Segue abaixo:

Finge ser um colega de trabalho; finge ser um empregado de um fornecedor, empresa parceira ou autoridade legal; finge ser alguém com autoridade; finge ser um empregado novo que solicita ajuda; finge ser um fornecedor ou fabricante de sistemas que liga para oferecer um *patch* ou uma atualização de sistema; oferece ajuda quando ocorrer um problema e, em seguida, faz o problema ocorrer para manipular a vítima e fazer com que ela ligue pedindo ajuda; envia software ou *patch* grátis para que a vítima o instale; envia um vírus ou Cavalo de Tróia como um anexo de correio eletrônico; usa uma janela *pop-up* falsa que pede para o usuário fazer o *login* novamente ou digitar uma senha; captura as teclas digitadas pela vítima com um sistema ou programa de computador; deixa um disquete ou CD com software malicioso em algum lugar do local de trabalho; usa jargão e terminologia interna para ganhar a confiança; oferece um prêmio pelo registro em um site *Web* com um nome de usuário e a senha; deixa um documento ou arquivo na sala de correspondência para entrega interna; modifica o cabeçalho de uma máquina de fax para que ele venha de uma localização interna; pede que uma recepcionista receba e, em seguida, encaminhe um fax; pede que um arquivo seja transferido para uma localização aparentemente interna; configura uma caixa de correio para que as ligações de retorno percebam o atacante como alguém de dentro da empresa; finge ser do escritório remoto e pede acesso local ao correio eletrônico. (Mitnick. Simon, 2003).

Sinais de um ataque:

Recusa em dar um número de retorno; Solicitação fora do comum; alegação de autoridade; ênfase na urgência; ameaça de conseqüências negativas em caso de não atendimento; mostra desconforto quando questionado; nome falso; cumprimentos ou lisonja; flerte. (Mitnick. Simon, 2003).

3.2. Local de Trabalho

Existem várias maneiras de se passar por outra pessoa, pois um hacker pode simplesmente se passar por um técnico de manutenção ou consultor e ter acesso livre à empresa e enquanto caminha ir capturando todas as informações que estejam expostas, conversar com pessoas, como recepcionistas, telefonistas,

assistentes administrativos, guardas segurança, *Help desk* ou suporte técnico, administradores de sistema, operadores de computador, administradores do sistema de telefones, que são alvos mais comuns de ataques e ir coletando informações.

Além disso, existem fatores que tornam as empresas mais vulneráveis aos ataques, quando geralmente se tem um número grande de empregados, diversas instalações, informações sobre o paradeiro dos empregados deixadas nas mensagens de *voice* mail, informações de ramal de telefone disponíveis, falta de treinamento em segurança, falta de sistema de classificação de dados, nenhum plano ou grupo de resposta aos incidentes de segurança.

3.3 Verificação e classificação de dados

Mais um método utilizado por um atacante é fazer uma verificação de dados mais profundamente e assim tornar a vítima mais vulnerável.

TABELA 01

Verificação de procedimento de identidade

AÇÃO	DESCRIÇÃO
ID de chamadas	Verifica se a ligação e interna e se o nome e número do ramal coincidem com a identidade do interlocutor.
Retorno de ligação (Callback)	Procura o solicitante no diretório da empresa e liga de volta para o ramal relacionado.
Endosso	Pede para um empregado de confiança endossar a identidade do solicitante.
Segredo comum compartilhado	Solicita um segredo compartilhado da empresa, tal como uma senha ou código diário.
Supervisor ou gerente	Contata o supervisor imediato do empregado e solicita a verificação da identidade e do status de emprego.
Correio eletrônico seguro	Solicita uma mensagem assinada digitalmente.
Reconhecimento pessoal de voz	Para um interlocutor conhecido do empregado, validado pela voz do interlocutor.
Pessoalmente	Exige que o solicitante apareça pessoalmente com um crachá de empregado ou outra

	identificação.
Senhas dinâmicas	Verifica com relação a uma solução de senha dinâmica, tal como um ID Seguro ou outro dispositivo de autenticação segura.

Fonte: A arte de enganar de Kevin Mitnick

4 HARDENING

Hardening é quando elevamos o nosso nível de segurança de um ativo da rede, personalizando, como fechando portas e serviços que não usadas, são todas as medidas necessárias para tornar mais robusto as aplicações, sistemas operacionais, swtiches, roteadores, bancos de dados, ou seja, tudo que tiver na rede e precisa ser protegido. Assim, podemos criar políticas de hardening incluindo tarefas como remover ou desativar funcionalidades desnecessárias e validar a configuração de acordo as melhores práticas. Iremos abordar algumas das melhores práticas que devem ser utilizadas para poder fortalecer, endurecer a segurança em redes de computadores e dessa forma, o que devemos proteger para garantir a continuidade de serviços que estejam rodando e que foram implementados. Até porque esse nivelamento serve como mais uma precaução, dificuldade para que não haja acessos indevidos que venham a violar e torna indisponíveis as redes de computadores. A melhor defesa é a prática da aplicação de medidas de segurança em todos os níveis da rede, uma defesa sólida contém defesas no perímetro exterior normalmente, firewalls e um sistema de detecção de intrusão. Também inclui defesas no interior da rede, como firewalls internos, segmentação da rede e controles de porta em nível de acesso. E os recursos podem ser protegidos em diversas maneiras, inclusive em firewalls pessoais, antivírus, software anti-spyware, criptografia de dados e de segurança. (Seagren, Watkins, 2007)

4.1 Realizando *Hardening* Básico

Por padrão todos os sistemas operacionais vêm com as configurações básicas e para poder torná-lo seguro devemos personalizar. Dessa forma na hora da instalação pode-se personalizar para garantir um uso melhor do sistema em seu ambiente e assim torná-lo mais difícil para um invasor e não comprometer o sistema. Independente de qual propósito serve o sistema existem alguns passos comuns de *hardening* que são aplicados para todos, são tarefas de alto nível, e como tal, os detalhes específico da implementação vão variar de sistemas, estas tarefas de alto nível de *hardening* serão descritas aqui.

4.2 *Hardening* Windows XP

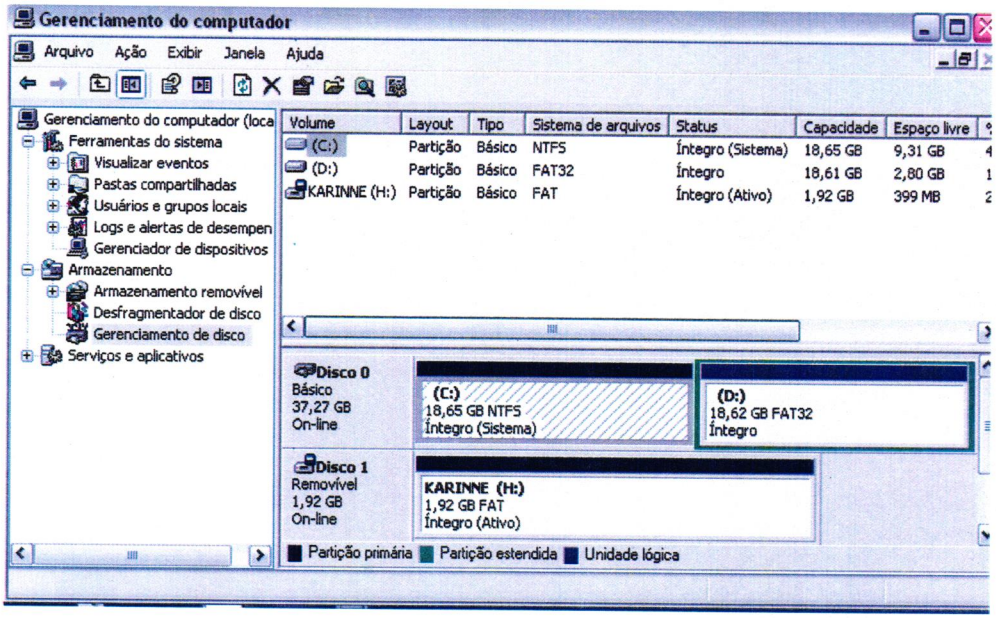
As recomendações a seguir aplicam-se ao sistema operacional Windows já que é a plataforma mais utilizada atualmente. Sabemos que os criadores de *malwares* tentam infectar o maior número possível de máquinas em um curto período de tempo. O Windows deve está sempre atualizado, os usuários devem esta conscientes para as paginas que acessam e os conteúdos navegados e sempre manter o *firewall* habilitado e o antivírus atualizado.

Verifique se todas as partições do disco estão formatadas com NTFS

Partições NTFS oferecem controle de acesso e proteções que não estão disponíveis com o FAT, FAT32 ou sistemas de arquivos FAT32x. Certifique-se de que todas as partições no seu computador são formatadas com o NTFS. Se necessário, use o utilitário convert para converter as partições para NTFS.

FIGURA 01

Gerenciamento do computador



Fonte: Computador pessoal

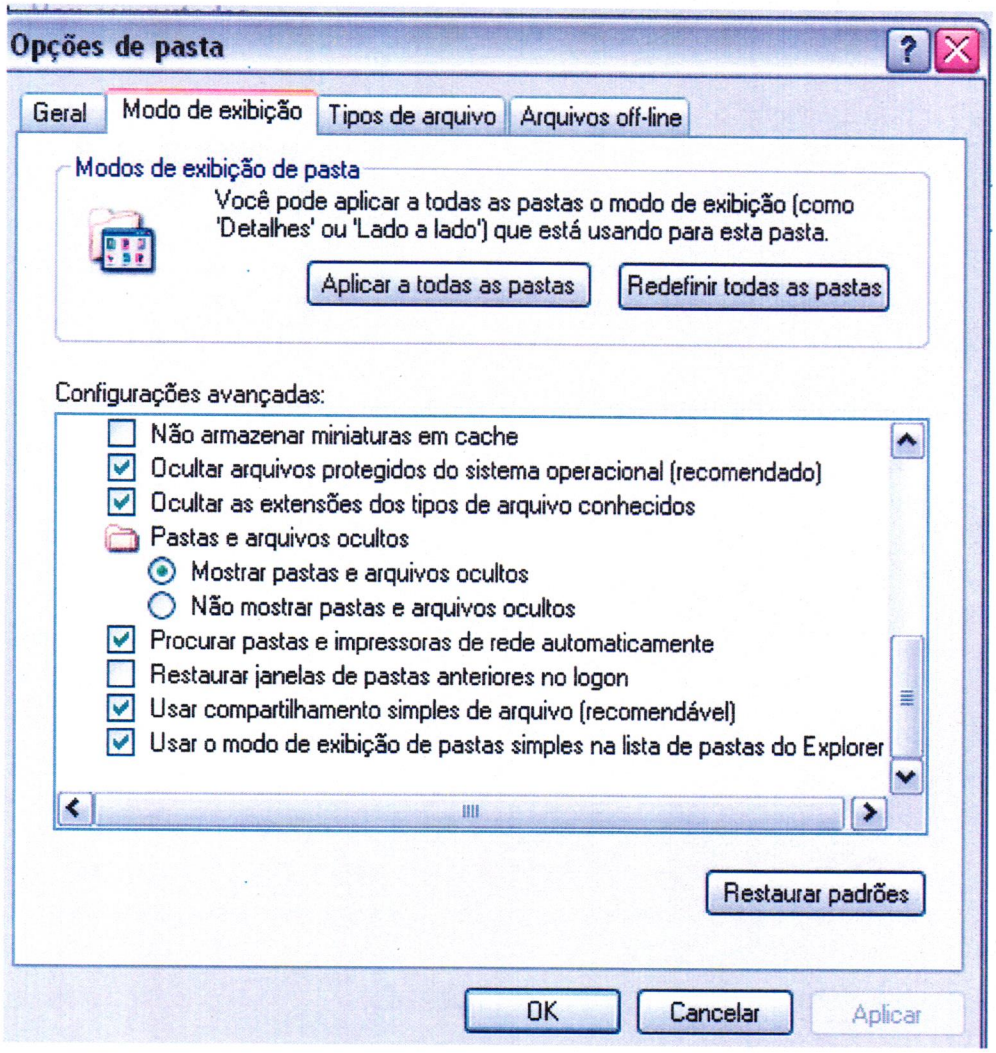
Proteja compartilhamentos de arquivos

Por padrão, os sistemas Windows XP Professional que não pertencem a um domínio utiliza um modelo de acesso à rede chamado "Compartilhamento simples de arquivo", onde todas as tentativas de fazer *logon* no computador através da rede serão forçadas a usar a conta do cliente. Isto significa que o acesso à rede

através de *Server Message Block* (SMB, usado para acesso a arquivos e impressão), bem como a chamada de procedimento remoto (*RPC*, usado pela maioria das ferramentas de gerenciamento remoto e acesso remoto ao Registro) só estará disponível na conta do cliente. Devemos mudar essa situação. Para mudar isso, vá para: Iniciar => Programas => Acessórios => Windows Explorer e caia no menu ferramentas e selecione 'Opções de pasta ".

FIGURA 02

Proteção de compartilhamento de arquivos



Fonte: Computador pessoal

No modelo usar compartilhamento simples de arquivos, os compartilhamentos de arquivos podem ser criados para que o acesso a partir da rede seja somente leitura, ou acesso a partir da rede seja capaz de ler, criar, alterar e excluir os arquivos. Compartilhamento Simples de Arquivos é destinado ao uso em uma rede doméstica protegida por um *firewall*, como os fornecidos pelo Windows

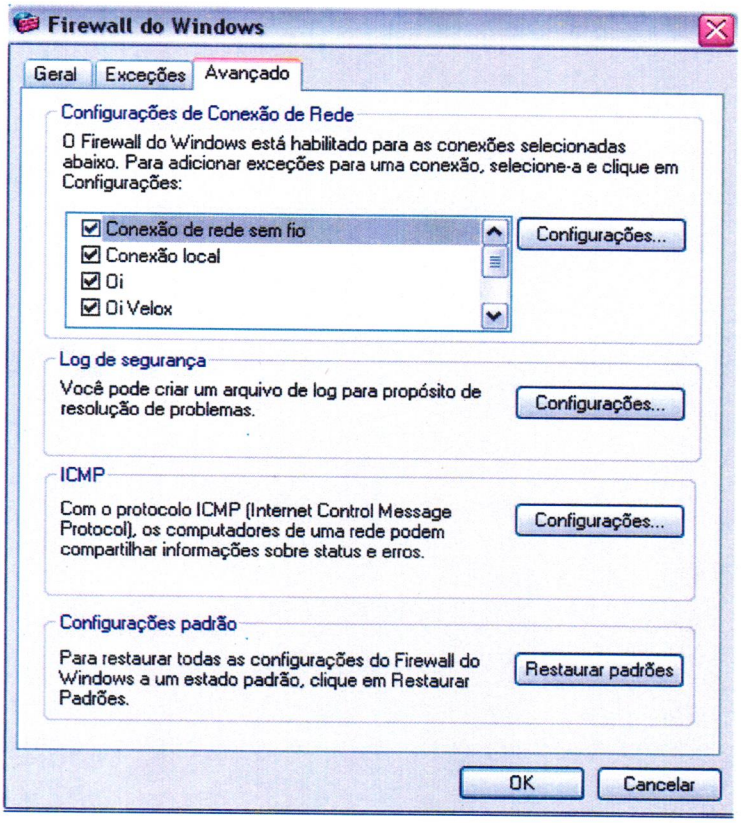
XP. Se você estiver conectado à Internet, e não está acessando atrás de um *firewall*, você deve se lembrar que qualquer compartilhamento de arquivo que você criar poderá ser acessível a qualquer usuário na Internet. Então se deve desmarcar a opção modelo usar compartilhamento simples de arquivos para evitar que algum usuário não autorizado possa acessar. (Hassell, 2006).

Habilitar o Internet Connection Firewall (ICF)

ICF fornece proteção para computadores com Windows XP que estão conectados diretamente à Internet, ou para os computadores ou dispositivos conectados à *Internet Connection Sharing* computador *host* que está executando o ICF.

FIGURA 03

Internet Connection Firewall (ICF)



Fonte: Computador pessoal

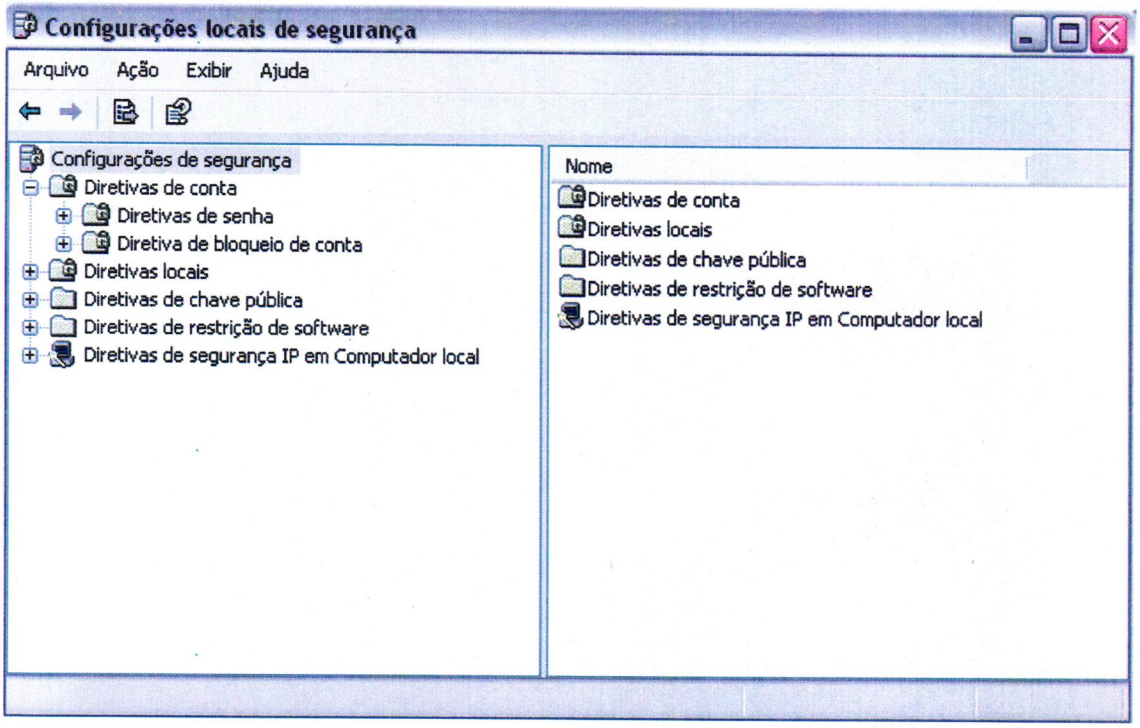
Dessa forma, habilita o ICF e têm-se uma proteção a mais para evitar acessos indevidos ao computador.

Políticas de restrição de utilização de software

Políticas de restrição de software fornecem aos administradores um mecanismo conduzido por diretiva que identifica o software funcionando em seu domínio, e controla a capacidade de que o software seja executado. Usando uma diretiva de restrição de software, um administrador pode impedir que programas indesejados sejam executados, o que inclui os vírus e cavalos de Tróia ou outro software que é conhecido por causar conflitos quando instalados. Políticas de restrição de software podem ser usadas em um computador autônomo, configurando a política de segurança local. As políticas de restrição de software também se integrar com a Diretiva de Grupo e *Active Directory*. (Hassell, 2006).

FIGURA 04

Configurações locais de segurança.



Fonte: Computador pessoal

Para acessar as diretivas locais de segurança e habilitar restrição de software deve-se seguir os seguintes passos. Iniciar => Painel de controle=> Ferramentas Administrativas => Diretiva de segurança local => Diretiva de restrição de software.

Desativar serviços desnecessários

Uma das maneiras mais fáceis que os *crackers* têm para explorarem falhas em seu sistema são através serviços abertos.

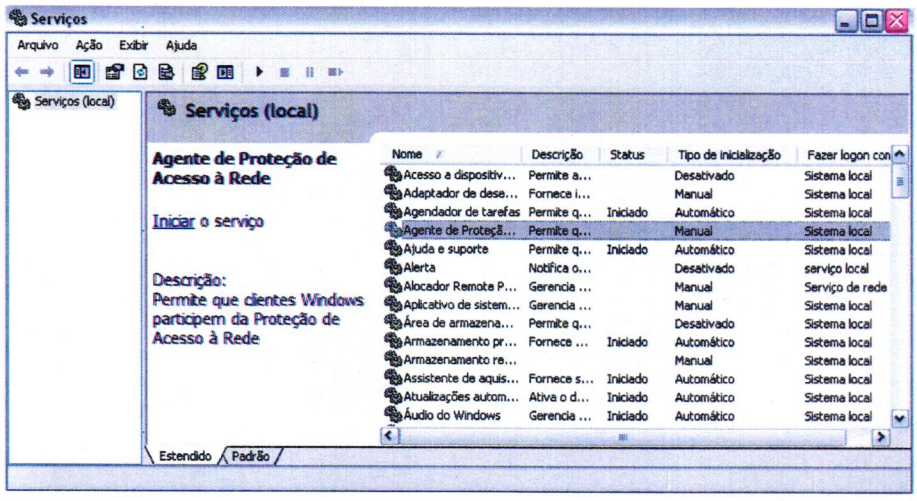
Além dos benefícios de segurança que começam a partir da auditoria e encerramento serviços não utilizados, você receberá uma melhoria de desempenho porque os programas estagnados não estão recebendo os recursos disponíveis. Além disso, uma auditoria de segurança completa do seu serviço pode revelar alguns detalhes interessantes sobre sua máquina. Ultimamente, os vírus foram disfarçados de serviços listados no Gerenciador de tarefas, tornando-os mais difíceis de detectar, limpa, e evitar.

Depois que instalar o Windows XP, devemos desabilitar os serviços de rede desnecessários, pois o mesmo vem com alguns acessos externos por padrão como terminal services (acesso remoto). Pois através de uma brecha deixada por um desses serviços pode-se ser atacado, invadido, por vírus que possam utilizar esse determinado serviço. (Kurtz, Scambray, Mcclure, 2007).

Para gerenciar os serviços que estão no seu computador devem-se seguir os seguintes passos: Iniciar => painel de controle => ferramentas administrativas => serviços.

FIGURA 05

Serviços

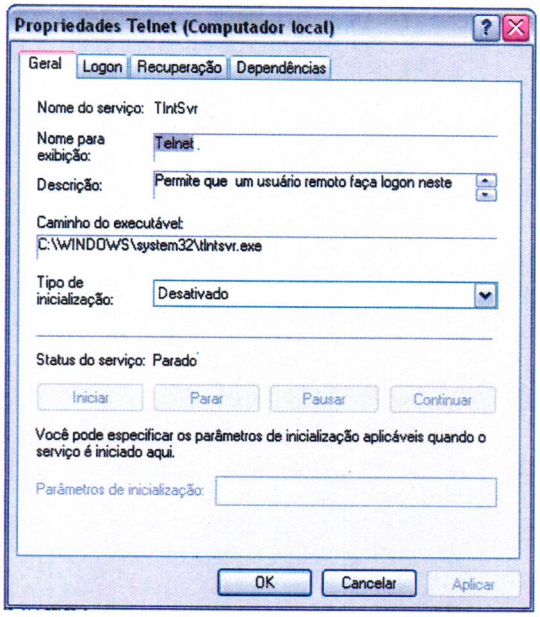


Fonte: Computador pessoal

Logo em seguida para poder gerenciar o serviço, verificar o status do sistema se vai deixá-lo ativo ou desativo depois dar-se um duplo clique no serviço e informa o tipo de inicialização.

FIGURA 06

Serviço desativado



Fonte: Computador pessoal

Vários serviços podem ser gerenciados, como por exemplos o *telnet* e dessa forma, endurecendo, tornando robusto o sistema operacional.

Neste item serviços se fossem realmente detalhar a quantidade dos mesmos poderíamos fazer outro artigo, apenas falando sobre serviços gerenciáveis.

Desativar ou excluir contas desnecessárias

No Windows XP é possível criar contas separadas para cada pessoa que usará o computador, dessa forma, cada usuário poderá ter suas próprias pastas de documentos e configurações como papel de parede, botão iniciar, estilo visual e assim por diante. Para criar e configurar contas de usuário, use a ferramenta contas de usuário, que pode ser encontrada no painel de controle.

Para abrir a ferramenta contas de usuário, abra o painel de controle no botão iniciar e clique duas vezes em Contas de usuário. Essa praticidade de cada usuário obter o seu próprio perfil é que pode ocorrer de ficar contas ativas sem

estarem mais sendo utilizadas, sendo dessa forma, uma brecha na segurança porque através de um ataque de força bruta ou dicionário se pode descobrir a senha e um *hacker* se passar pelo usuário e ficar obtendo informações privilegiadas, assim deve-se sempre desativar ou excluir contas desnecessárias.

Para fazer alterações em uma conta

1. Clique em alterar uma conta na caixa de listagem escolha uma tarefa.
2. Clique na conta que deseja alterar.
3. Selecione o item que deseja alterar:

- Clique em alterar o nome para alterar o nome exibido na tela de boas-vindas da conta.
- Clique em alterar a imagem para alterar a imagem que é usada para representar a conta de usuário. Você pode usar qualquer arquivo de imagem do computador como imagem do usuário.
- Clique em alterar o tipo de conta para alterar o tipo de conta, de modo a aumentar ou diminuir os direitos do usuário no computador.
- Clique em criar uma senha para criar ou alterar a senha do usuário e a dica de senha.
- Clique em excluir a conta para excluir a conta de usuário do computador. Ao excluir a conta, você terá a opção de salvar os arquivos do usuário no computador.

Limitando contas de usuários

Outra medida que deve ser utilizada é a limitação de contas de usuários, dessa forma, podemos fazer a maioria das atividades diárias como, navegar na internet, ler e-mails, escutar música, conversar através de programas de mensagens instantâneas e etc. Estas atividades não se necessitam de privilégios administrativos, assim, limitamos essas contas.

Este procedimento simples inibe a ação de várias *exploits* (falhas), que necessitam de privilégios elevados para explorarem falhas remotas. A partir do momento que um intruso tenha em posse a conta de administrador pode efetuar diversas ações, como por exemplo:

- Instalar e executar serviços;
- Acessar dados de outros usuários;
- Capturar/Registrar as ações de todos os usuários;
- Substituir os Arquivos de Programas do sistema operacional com Trojans (cavalo de tróia, programas maliciosos);
- Desabilitar/Desinstalar antivírus;
- Cobrir os rastros apagando logs (registros) do sistema;
- Desativar o boot do sistema;
- Se a mesma conta for usada em outros computadores da sub-rede, o intruso pode ganhar controle sobre várias máquinas.

Conta de convidado

Esta conta já vem por padrão no Windows XP e o intuito dela é para usuários sem conta no sistema acessem o computador. Na instalação a mesma já vem desabilita, e correto renomear essa conta ou proteger com senha forte podendo evitar possíveis acessos ao computador remotamente.

Definir políticas de senhas fortes

Para proteger os usuários que não colocam senha em suas contas, por padrão o Windows XP só permite *logon* no computador local, não podendo mais efetuar l*ogon* remotamente na rede, ou para qualquer atividade de inicio de sessão. Devendo reforçar as políticas de segurança local seguindo as da Microsoft.

- Defina o comprimento mínimo de senha, no mínimo, oito caracteres;
- Definir uma senha idade mínima adequada à sua rede (tipicamente entre um e sete dias);
- Definir uma duração máxima da senha apropriada a sua rede.

5 CONCLUSÃO

Na era da Informação onde o conhecimento é o maior bem que a empresa possui, o uso das melhores práticas de segurança em redes de computadores é indispensável e essencial.

Pois como a informação é divulgada e transmitida de forma muito dinâmica e em todo tipo de meio, empresa publica e privadas, prezam pela integridade, confidencialidade e autenticidade da informação gerada. Para isto podem utilizar todos os métodos supracitados.

Atualmente quase todas as informações são transportadas por meio eletrônico. Sendo assim para poder garantir que as informações divulgadas sejam corretas, devemos aplicar todas as técnicas que foram citadas neste artigo, colocando mais barreiras para o invasor.

É importante ressaltar que o fator humano, este deve ser bem trabalhado para que possa minimizar os problemas venha existir por falta de cautela ao obter informações privilegiadas.

Também devemos fortalecer o sistema operacional utilizado, fechando todas as brechas possíveis, fazendo ajustes finos, personalizando e tirando a configuração padrão, e dessa forma, evitar problemas de invasão e o roubo de informações preciosas.

Com esses estudos realizados, conseguimos obter resultados importantes na utilização de técnicas que nos orienta e assim, podemos utilizá-las tanto em ambientes corporativos, como também em computadores pessoais, trazendo segurança da informação, ou seja, um benéfico para sociedade que está cada vez mais informatizada.

REFERÊNCIAS

McCLURE, stuart . SCAMBRAY, joel.KURTZ, george. **Hacking Exposed Windows:** Microsoft Windows Security Secrets and Solutions, Third Edition . McGraw-Hill Osborne Media; 3 edition, 2007.

HASSELL,Jonathan. **Hardening Windows.** Second Edition. Apress

MESSER, James. **Secrets of Network Cartography**: A Comprehensive Guide to Nmap. A NetworkUptime.com

STALLINGS, William.**Cryptography and Network Security Principles and Practices,** Fourth Edition. Prentice Hall. November 16, 2005

ANONYMOUS. **A Hacker's Guide to Protecting Your Internet Site and Network**. Sams; Bk&CD-Rom edition (June 1997).

MITNICK, Kevin D, SIMON, William L. **Ataques de Hackers:** Controlando o Fator Humano na Segurança da Informação. MAKRON BOOKS.

SEAGREN, Eric. WATKINS, Stephen. **Secure Your Network for Free.** Syngress.

OREBAUGH, Angela. PINKARD, Becky .**nmap in the enterprise your guide to network scanning**. Syngress.

TANENBAUM, Andrew. **Redes de Computadores quarta edição.** CAMPUS

KUROSE, James, ROSS, Keith. **Redes de Computadores e a Internet**: Uma abordagem top-down. PEARSON EDUCATION

GEUS, Paulo Lício de; NAKAMURA, Emílio Tissato. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Futura, 2003. 472p.

WADLOW, Thomas A; tradução Fabio de Freitas da Silva. **Segurança de Redes:** projeto e gerenciamento de redes seguras. Rio de Janeiro: Campus,2000. 269p.

BURNETT Steve. & PAINE Stephen. **Criptografia e Segurança** – O Guia Oficial RSA. Rio de Janeiro: Editora Campus, 2002 367p.

http://www.scribd.com/doc/7448828/Algoritmos-de-Criptografia Acesso em: 21 Dez. 2009

http://www.gta.ufrj.br/grad/07_1/ass-dig/TiposdeCriptografia.html Acesso em: 06 Maio. 2009

http://www.icmc.usp.br/manuals/sce183/hash1.html Acesso em: 18 Dez. 2009

http://blog.caelum.com.br/2006/09/04/ensinando-que-e-o-hashcode/ Acesso em: 14 Nov. 2009

http://www.gta.ufrj.br/grad/08_1/quantica/cap1.html. Acesso em: 14 Nov.

http://www.sbis.org.br/cbis/arquivos/824.pdf. Acesso em: 06 Maio. 2009

http://imasters.uol.com.br/artigo/2221/visual_basic/criptografia/ Acesso em: 06 Maio. 2009

http://www.microsoft.com/brasil/security/guidance/topics/devsec/secmo. mspx. Acesso em: 21 Nov 2009

http://software.newsforge.com/article.pl?sid=05/11/0 2/2056250&from=rss Acesso em: 06 Dez. 2009

http://www.invasao.com.br/2009/01/31/vulnerabilidades-em-aplicacoes-web/ Acesso em: 06 Maio. 2009

DIOGENES, Yuri; **Guia de Certificação Cisco.**

http://www.symantec.com.br/malwares.html Acesso em 09 jan 2010

http://www.frb.br/ciente/2006_2/BSI/BSI.SANCHES.etal.F1%20_Rev.%2028.11.06_.pdf Acessado em 12 jan 2010.

BATTISTI.Julio. Disponível em: http://www.juliobattisti.com.br/tutoriais/keniareis/dicionarioinfo007.asp >. Acessado em: 11 fev. 2007;