UNIVERSIDADE FEDERAL DE SANTA MARIA
COLÉGIO AGRÍCOLA DE FREDERICO WESTPHALEN
PÓS-GRADUAÇÃO EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO

SEGURANÇA DA INFORMAÇÃO APLICADA A SERVIDORES UTILIZANDO TÉCNICAS DE HARDENING

MONOGRAFIA DE PÓS GRADUAÇÃO

Regis Titon

Frederico Westphalen, RS, Brasil
2013

SEGURANÇA DA INFORMAÇÃO APLICADA A SERVIDORES UTILIZANDO TÉCNICAS DE HARDENING

por

Regis Titon

Monografia apresentada ao Curso de Pós-graduação em Gestão de Tecnologia da Informação, da Universidade Federal de Santa Maria (UFSM-RS), como requisito parcial para a obtenção do **grau de Especialista em Tecnologia da Informação**

Orientador: Profº Msc. Roberto Franciscatto

Frederico Westphalen, RS, Brasil

2013

Universidade Federal de Santa Maria
Colégio Agrícola de Frederico Westphalen
Pós-graduação em Gestão de Tecnologia da Informação

A Comissão Examinadora, abaixo assinada,
aprova a Monografia de Especialização

SEGURANÇA DA INFORMAÇÃO APLICADA A SERVIDORES UTILIZANDO TÉCNICAS DE HARDENING

elaborada por
Regis Titon

como requisito parcial para obtenção do grau de
Especialista em Tecnologia da Informação

COMISÃO EXAMINADORA:

Profº Msc. Roberto Franciscatto
(Presidente/Orientador)

Prof° Msc. Evandro Preuss

Prof° Msc. Tiago Perlin

Frederico Westphalen, 13 de dezembro de 2013.

RESUMO

Monografia de Especialização
Programa de Pós-Graduação em Gestão de Tecnologia da Informação
Universidade Federal de Santa Maria

SEGURANÇA DA INFORMAÇÃO APLICADA A SERVIDORES UTILIZANDO TÉCNICAS DE HARDENING
AUTOR: REGIS TITON
ORIENTADOR: ROBERTO FRANCISCATTO
Data e Local da Defesa: Frederico Westphalen, 13 dezembro de 2013

As técnicas de Hardening são elaboradas e tratadas para que se obtenha um aumento significativo na segurança dos servidores. Isto permite alcançar níveis de segurança mais altos, com um desempenho constante do ponto de vista da confiabilidade dos sistemas. Este trabalho teve como objetivo: revisar as principais técnicas de *Hardening* aplicadas a servidores que utilizam sistemas operacionais *Windows* e *Linux*, bem como analisá-las e documentá-las em forma de manual de boas práticas para aqueles que carecem de segurança aplicada a servidores no dia-a-dia de sua organização. Demonstrando as percepções necessárias para determinar quais as etapas e caminhos que devem ser seguidos perante os problemas exibidos nos servidores. Procurando ressaltar a importância da equipe de segurança da informação a qual é responsável por desenvolver, estudar e implementar técnicas, garantindo a integridade, confiabilidade e disponibilidade dos dados.

Palavras-chave: Tecnologia da Informação, Servidores, *Hardening*

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

INTRODUÇÃO

Na atualidade a segurança da informação tem chamado a atenção nas empresas, função essa desempenhada pelos administradores de rede, os quais exercem papel fundamental na administração e controle da infraestrutura da empresa. Sendo assim a empresa deve estar preparada para os investimentos necessários em tecnologia e gestão de pessoas.

Frente a isso, a opção de estudar a segurança da informação aplicada a servidores, veio da relevância deste assunto, pois a informação, seja ela escrita ou falada, deve ser protegida e armazenada, é necessário o conhecimento de ferramentas e métodos para aplicar a técnica de *hardening* para os servidores, evitando que as informações referentes à empresa vazem, produzindo confiabilidade ao administrador da empresa e aos departamentos envolvidos, além da integridade da informação ali gerada.

Algumas das estratégias adotadas por empresas que trabalham na área de Tecnologia da Informação, e especificamente sua equipe de segurança da informação são desenvolver, estudar e implementar técnicas de segurança, com a finalidade de garantir a integridade, confiabilidade e disponibilidade dos dados, tornando-os corresponsáveis nesse elo de estratégia da segurança.

O presente trabalho tem como objetivo geral: Revisar as principais técnicas de *Hardening* aplicadas a servidores que utilizam sistemas operacionais *Windows* e *Linux*, bem como analisá-las, documentá-las em forma de manual de boas práticas para aqueles que carecem de segurança aplicada a servidores, no dia-a-dia de sua organização.

E objetivos específicos: Implementar uma política adequada e coerente de segurança; Controlar os níveis de atualização de hardware/software (*updates* & *upgrades*); Controlar e aplicar ajustes finos em serviços necessários e/ou oferecidos; Criar mecanismos de proteção e configuração que visam dificultar ataques; Instalar, configurar e controlar as manutenções de ferramentas de segurança; Realizar a validação de segurança do sistema operacional com ferramentas de *benchmark*; Elaborar um manual com as principais práticas de *hardening* em servidores Linux e Windows.

Estando dividido em cinco capítulos tratando respectivamente de: revisão de literatura (Segurança da Informação; Servidor Linux; Servidor Windows; Principais serviços dos Servidores Linux e Windows e Hardening); desenvolvimento (Interface: navegacional no sistema Linux; Interface: navegacional no sistema Windows. Analise das técnicas de Hardening); e as considerações do autor sobre os seus achados.

2. REVISÃO BIBLIOGRÁFICA

A revisão bibliográfica enfoca pontos relativos à Segurança da Informação, sendo esta responsável por garantir que as informações permaneçam protegidas contra o acesso de pessoas não autorizadas, permanecendo disponíveis e confiáveis. Com vistas a embasar este estudo. Para tal fim, são abordadas questões relativas à segurança da informação, servidores *Windows* e *Linux* e as ferramentas de apoio.

2.1. Segurança da informação

As informações publicadas no ambiente virtual podem ser utilizadas de diferentes formas, que vai desde o conhecimento adquirido através delas (por ter em suas mãos o acesso a todo o tipo de informação, seja em nível regional ou global), até o favorecimento de pessoas mal intencionadas, que se vale de estratégias para obter informações sigilosas.

Estudiosos acreditam que há, no mínimo, três explicações para que isso ocorra: o desconhecimento do perigo que isso pode provocar; a negligência em tratar as informações e a imperícia em lidar com assuntos relativos à segurança e tratá-las de forma amadora, achando que está sendo profissional (DAWEL, 2005).

Diante disso, outro estudo realizado em 2006, denominado "CSI/FBI *Computer Crime and Security Survey*", ressalva a questão gerencial aliada à tecnologia, pois as informações estão livres para serem usadas, mas é preciso o comprometimento e a colaboração dos trabalhadores, em saber filtrar tais informações para o bem social.

Na Figura 01 observa-se a baixa conscientização dos trabalhadores e usuários, sendo isto um dos motivos responsáveis pela falta de segurança da informação.

Figura 2. Principais obstáculos para a implantação da segurança
Fonte: 10ª Pesquisa Nacional de Segurança da Informação (2006, p.7)

Possuir uma atuação eficaz na segurança da informação se torna aconselhável, pois a mesma permite ampliar uma visão abrangente para a compreensão das demandas e ações a serem desenvolvidas. No desempenho dos trabalhadores e usuários, está intrínseca uma maior mobilidade, sendo que as ações de segurança devem estar vinculadas à capacidade de construírem ações conjuntas: servidores e usuários.

Cada usuário deve ser compreendido como um sujeito único, o qual dispunha de necessidades e especificidades, que devem ser atendidas pelos servidores, abdicando a existência de uma situação estática, passando a construir e reconstruir diferentes ferramentas, que vêm ao encontro de um objetivo em comum: a segurança da informação.

Entretanto, com o avanço tecnológico, o aumento do uso e das facilidades que o computador proporciona, torna-se necessário a inovação da segurança da informação e o desenvolvimento de normas e padrões que servem como guias de melhores práticas e auxiliam na sua estruturação (BARBOSA, 2012).

Nesse aspecto, Fontes (2000) relata que para a segurança da informação obter sucesso na sua implementação, é necessário que ela envolva todas as áreas da empresa, além da conscientização do uso das políticas de segurança da informação, formando uma cultura da organização.

Assim, a Política de Segurança da Informação (PSI), é um documento que deve ser elaborado pela equipe técnica, juntamente com a direção, visando estabelecer regras, normas e diretrizes de acordo com cada empresa. A mesma deve garantir que todas as áreas e recursos da empresa sejam abrangidos e ser coerente com a sua visão, missão e objetivos, além de ser elaborado em uma linguagem de fácil entendimento por todos, evitando utilização de termos técnicos e aspectos de implementação (FONTES, 2000).

Ao elaborar a PSI, deve ter em mente que a sua implantação demanda de um processo longo, em que deve ser realizada de maneira formal e adaptável à realidade existente de cada empresa. Sendo assim um processo contínuo, passando por revisão e adaptação, de acordo com as necessidades e importância de cada servidor. (FONTES, 2000).

Proporcionar conhecimento por meio da segurança da informação torna-se, tanto para os trabalhadores quanto para usuários, um processo constante, um momento de troca de informações, potencializando o serviço e as metas propostas. Diante disso, a PSI, deve estar baseada em alguns tópicos, os quais garantirão a credibilidade da mesma, como apresenta Fontes (2000):

- A informação como uma propriedade da empresa;
- Autoridade do acesso a informação;

- Definição do administrador da informação;
- Responsabilidades do usuário, da gerência e do administrador da informação;
- Preparação para situações de reserva, garantindo a continuidade da execução do negócio;
- Definição do uso profissional da informação da empresa;
- Definição da possibilidade, ou não, da empresa acessar arquivos pessoais do usuário, quando de investigação;
- Definição da identificação do usuário como pessoal e única, bem como a responsabilidade do sigilo da senha;
- Conscientização dos usuários;
- Medidas disciplinares que serão utilizadas caso a PSI não seja cumprida.

Desta forma, fica notório que atuar com a segurança da informação é utilizar de vários artifícios, sejam eles a comunicação, a tecnologia, comprometimento da equipe, é se sentir parte fundamental no processo de organização de uma empresa.

Vindo ao encontro dessa conceituação, encontra-se em Barbosa (2012), que a segurança da informação tem como objetivo a proteção das informações através de um conjunto de orientações, normas, procedimentos, políticas e demais ações para garantir a sua preservação contra possíveis danos, perdas, furtos e mau uso, afetando a continuidade do negócio e alcance de seus objetivos.

Como em qualquer serviço, a segurança da informação pode sofrer vulnerabilidades, ou seja, ameaças, falhas no sistema operacional, devido a uma configuração inadequada, acarretando assim, um sistema suscetível a um ataque ou invasão. Ou seja, demanda de uma condição causada muitas vezes pela ausência ou ineficiência das medidas de segurança elaboradas nos aplicativos dos servidores (SÊMOLA, 2002).

Com base em Moreira (2001), as vulnerabilidades podem ter natureza: física, natural, *hardware*, *software*, mídias, comunicação e humana. Sendo que a sua identificação, quanto a sua natureza, implica em medidas de segurança mais eficazes e especificas para cada caso, contribuindo assim, para a continuidade da ação iniciada. Como já mencionado, as vulnerabilidades de natureza humana é um dos fatores que mais merece atenção, devido a sua fragilidade, podendo estar relacionada:

- À negligência ou não conhecimento das políticas de segurança;
- Falta de treinamento;
- Sabotagens;

- Compartilhamento de informações confidenciais;
- Envio de e-mails a pessoa não autorizada;
- Destruição ou roubo de propriedade ou dados, entre outros (SÊMOLA, 2002).

Sendo assim, a segurança da informação, não se restringe apenas a senhas e códigos, mas numa relação intensa entre seres humanos e máquinas, os quais são responsáveis por armazenar, transmitir, compilar e assegurar as informações. Evitando que qualquer ameaça advinda da vulnerabilidade, provoque danos da confidencialidade, integridade e disponibilidade dos servidores, em relação aos serviços prestados aos usuários.

Barbosa (2012) adverte que as ameaças de natureza humana, ocorrem de ordem como perda dos dados (apagar ou sobrescrever um arquivo), ou pelo não conhecimento das configurações instaladas de segurança, originando muitos problemas nas empresas. Promovendo assim, uma preocupação acentuada por parte dos executivos, em relação à proteção da informação, pois estão convencidos de que ela é um ativo de grande importância e valor. Um dos pontos relevantes para que a proteção dessa informação ocorra é a conscientização dos seus funcionários quanto à utilização desse ativo.

De acordo com Fontes (2006), estar conscientizado acerca da proteção da informação é internalizar os conceitos e agir com naturalidade no cumprimento dos regulamentos. Significa que a mesma deve fazer parte do dia-a-dia e não ser considerada apenas como um conceito nas responsabilidades profissionais para a organização. Os executivos da organização devem avaliar e estar comprometidos com o nível estabelecido para a proteção.

Promovendo uma visão ampla de um conjunto, o qual agrega investimento tecnológico e gestão de pessoas, em que este último ponto é o mais problemático para a organização, por ser o único aspecto que não pode ser diretamente inspecionado, como ocorre nos sistemas de segurança organizacionais. Assim, os servidores devem alocar na prática todas as táticas de segurança, suas regras e políticas de adesão, tendo um criterioso processo de seleção treinamento, atualizações, enfim, buscando diariamente novidades no ramo da segurança (FONTES, 2006).

Neste sentido, Mitnick (2003), apresenta um programa de conscientização e treinamento, o qual pode ser desenvolvido aos usuários ameaçados. Oferecendo seis tendências básicas de natureza humana:

- Autoridades*:* as pessoas têm a tendência de atender solicitações que são feitas por pessoas com autoridades ou que estão autorizados a fazer tal solicitação.

- Afabilidade*:* as pessoas têm a tendência de atender solicitações quando o solicitante se faz passar por alguém agradável ou com interesses, crenças e atitudes semelhantes aos da vítima.
- Reciprocidade*:* costumamos atender a solicitações quando acreditamos que recebe-se algo de valor como retribuição.
- Consistência*:* após fazer um comprometimento público ou adotar uma causa as pessoas têm a tendência de atender as solicitações para não parecem pouco confiáveis ou indesejáveis.
- Validação Social*:* o cooperativismo quando a ação parece estar de acordo com aquilo que as pessoas estão fazendo aparentando estar de forma correta e apropriada.
- Escassez*:* as pessoas costumam cooperar quando o objeto que está sendo procurado está em falta ou disponível por um curto período de tempo e que outras pessoas estão competindo por ele.

O programa de conscientização e treinamento deve visar à mudança de comportamento dos trabalhadores motivando-os a querer fazer parte do programa protegendo os ativos da empresa e também as suas próprias informações. Ele deve atingir cada usuário que tem acesso às informações confidenciais ou aos sistemas corporativos de computadores, devendo ser realizado de forma contínua e atualizado sobre as novas vulnerabilidades, divulgando à todos os envolvidos, para que assim o elo de aprendizagem abranja desde os servidores aos usuários, na tentativa de invasão aos dados confidenciais.

O programa de conscientização deve ser realizado de forma constante, além de ser criativo e utilizar todos os canais disponíveis de comunicação para que todos os colaboradores tenham acesso às mensagens e possam ter em mente os bons hábitos de segurança. Outra tática que pode ser utilizada é a linguagem no qual as mensagens são redigidas evitando que elas tornem familiares demais para serem ignoradas (MITNICK; SIMON, 2006).

Outro fator que deve-ser salientado na segurança da informação, é a utilização das regras ABNT NBR ISO/IEC 2700, sendo estas advindas dos primeiros padrões de segurança, a BS 7799. A sua primeira formulação ocorreu em 1995, com a nomenclatura de Código de Política para Gerenciamento de Segurança da Informação, a qual objetivava estabelecer um conjunto detalhado dos controles para o gerenciamento à certificação ISO, em 2000 torno-se o padrão ISO 17799 (KNOWLEDGELEADER, 2003).

Frente a esse processo de reestruturação, em 2005 a ISO 17799 tornou-se a ISO 27002, sendo traduzida e publicada pela ABNT através da norma NBR ISO/ IEC 27002, vale

ressaltar, que o seu conteúdo técnico, continuou igual ao da NBR ISO/IEC 27002 (ABNT, 2008). A NBR ISO/IEC 27002 é um código de boas práticas para a Segurança da Informação, a qual descreve o controle e os objetivos, que dão suporte ao controle de gestão nessa área do desenvolvimento, podendo ser um documento utilizado com o intuito de usar a conformidade com a ISO na gestão da Segurança da Informação.

Outra norma que sofreu modificações foi a NBR ISO/IEC 27001, a qual foi originada da ISO 27001(KNOWLEDGELEADER, 2003). Esta norma tem por objetivo "(...) prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação." (ISO 27001, 2006).

Os objetivos de controle descritos na ABNT NBR ISO/IEC 27001, são derivados diretamente da ABNT NBR ISO/IEC 27002. Assim, a norma ABNT NBR ISO/IEC 27001 é o documento utilizado por um auditor a fim de comprovar os controles da NBR ISO/IEC 27002 implementados em uma instituição, a qual tem por objetivo a certificação ISO 27001.

Em 2005 surge a BS77993 (STANDARDS, 2005) com denominação "Guia para gerenciamento de riscos em segurança da informação", a qual em 2008 tornou-se ISO 27005 (ISO, 2008), publicada pela ABNT através da NBR ISO/IEC 27005.

Em 2007 surgiu o padrão ISO 27006 denominado "Exigências para as organizações que fornecem o exame e a certificação de sistemas de gestão da Segurança da Informação", sendo destinado a empresas que fornecem certificação em segurança da informação.

Simplificando e agregando a sua descrição e equivalência, as normas ISO serão apresentadas no Quadro 01.

Norma ISSO	Descrição	Equivalência
ISO 27002	Código de prática para a gestão da segurança da informação;	BS 77991 (ISO 17799)
ISO 27001	Sistemas de gestão de segurança da informação Requisitos;	BS 77992
ISO 27005	Gestão de riscos de segurança da informação;	BS 77993
ISO 27006	Exigências para as organizações que fornecem o exame e a certificação de sistemas de gestão da segurança da informação;	Não possui equivalência

Quadro 01: Normas ISO

Frente às informações apresentadas, fica notório que trata-se de um mundo a ser descoberto diariamente, devido ao grande avanço tecnológico, o qual reserva muitos ensinamentos, questionamentos e aprendizagem nesse sistema marcado por transformações constantes. É importante salientar as lacunas existentes na segurança da informação, suas intercorrências, o que muitas vezes passam despercebidas aos olhos dos trabalhadores e usuários, mas que servem de indicadores para novas pesquisas.

Vindo ao encontro de Rodrigues (2008), que todo computador conectado à internet corre sérios riscos, e pode ser infectado, caso não esteja devidamente protegido. Estas recomendações visam dificultar e coibir a ação de usuários mal-intencionados, diminuindo os riscos de comprometimento, educando e conscientizando o usuário final.

2.2 Servidor Linux

O Linux é um sistema operacional que foi desenvolvido pelo finlandês Linus Torvalds, no qual seu código fonte é disponível sobre a licença GPL (General Public License), em que qualquer pessoa possa utilizar estudar, modificar e distribuir livremente conforme o acorde dos termos de licença (MORIMOTO, 2006).

Com o aumento das ameaças existentes na internet e nos ambientes corporativos, faz-se necessário o uso de novas técnicas capazes de prover segurança, proporcionando uma maior estabilidade nos servidores (ABADI 2013).

É importante observarmos, de acordo com Campos (2006), que o sistema operacional Linux, se tornou muito popular devido à portabilidade de seu sistema, fácil acesso garantido por parte dos códigos de aplicativos disponíveis para outros sistemas pudessem executar nesse sistema operacional, garantindo maior credibilidade e confiabilidade.

Segundo o Noyes (2010), o Linux é comparado com o Windows, conforme o melhor servidor. sendo algumas razões:

- *Estabilidade:* O sistema Linux é conhecido por sua capacidade de funcionar anos sem falhas. De fato, isso é interessante para uma pequena e média empresa, nas quais uma interrupção em seu sistema pode trazer consequências desastrosas. O Linux também trabalha com grande número de processos simultâneos, de uma forma melhor que o sistema Windows, isso pode degradar rapidamente a estabilidade do Windows. Quase todas as mudanças de configuração do Linux podem ser feitas com o sistema

funcionando e sem afetar outros serviços. Os servidores Windows precisam ser desfragmentados com frequência, no Linux isso foi praticamente eliminado.

- *Segurança:* O Linux é nativamente mais seguro, seja em servidores, desktop ou ambiente embarcado, comparado ao Windows. Isso se deve ao Linux ser baseado em Unix, com isso apenas o administrador ou o usuário *root* tem privilégios administrativos. O Linux também sofre ataques, mas com menos frequência que os sistemas Windows, pois todas as suas vulnerabilidades tendem a serem descobertas e corrigidas mais rapidamente, já que possuem desenvolvedores e usuário no qual podem mexer no seu código fonte. No Linux o administrador possui uma visão clara do sistema de arquivos e esta sempre no controle do sistema.
- *Hardware:* O Linux é um sistema operacional leve, flexível e escalável, e funciona praticamente em qualquer computador, pode ser instalado para qualquer processador e arquitetura de uma maquina. O Linux pode ser facilmente reconfigurado para incluir apenas os serviços que serão necessários no determinado momento para a determinada empresa, isso reduzindo o requisito de memória, melhorando desempenho e mantendo o funcionamento simples e contínuo.

Os servidores Linux executam diversos serviços, no qual podem ser instalados e configurados conforme a necessidade do administrador de redes ou da empresa. Alguns dos serviços prestados pelo Linux: DNS, DHCP, FIREWALL, PROXY, FTP, E-MAIL, WEB, Banco de Dados, Acesso Remoto, etc.

2.3 Servidor Windows

Ao abranger o mundo dos servidores, devemos ter em mente que o mesmo possui muitas funções no ambiente do sistema entre usuário e servidor. Sendo que os servidores são configurados para fornecer autenticação e/ou executar aplicativos. Permitindo também, a comunicação dos usuários com outros servidores e recursos da rede (PORTAL DA EDUCAÇÃO, 2008).

Em Abril de 2003 a Microsoft lançou o Windows Server 2003, conhecido como Windows 2003, que é um sistema operacional no qual teve como seu desenvolvimento base o Windows 2000 Server. Em seu núcleo estava funcionando a versão do Windows XP com algumas funções desativadas para permitir o que o seu funcionamento seja estável. Com o Windows Server 2003 a Microsoft realizou melhorias em seu serviço de rede e ao *Active Directory* (PROCÓPIO, 2008).

O Active Directory é o serviço de diretórios do Windows Server 2003. Serve como um serviço de rede no qual faz a identificação de todos os recursos disponíveis em uma rede, mantendo informações sobre os dispositivos como conta de Usuários, grupo, computadores, recurso, política de segurança e etc., assim em um banco de dados ele se torna recurso disponível para usuários e aplicações (VIDAL, 2006).

Além disso, os servidores Windows executam diversos serviços, no qual podem ser instalados e configurados conforme a necessidade do administrador de redes ou da empresa. Alguns dos serviços prestados pelo Windows Server são: DNS, DHCP, FIREWALL, PROXY, FTP, E-MAIL, WEB, Banco de Dados, Acesso Remoto, etc.

Morimoto (2008) complementa que o Windows Server 2003 possui diversas versões de seu sistema operacional, sendo importante conhecer e diferenciar as mesmas para assim criar um plano de segurança o qual atenda as suas necessidades existentes. Como demonstrado no Quadro 02:

Standard Edition	Esta é a versão padrão do sistema, destinada ao uso em servidores de forma geral. Ela oferece suporte a máquinas com até 04 processadores e a até 04 GB de memória RAM. Junto com a versão x64-bit, esta é a versão que indicada em um servidor de rede local.
Web Edition	É uma versão limitada do sistema, destinada a ser usada em servidores Web, que é oferecida para empresas de hospedagem a custos reduzidos. Ela oferece suporte a máquinas com até dois processadores e a até 2 GB de memória RAM e oferece um conjunto limitado de serviços. Ao locar um servidor web com o Windows, esta é provavelmente a versão que será utilizada.
Enterprise Edition	Esta versão roda em uma arquitetura proprietária de hardware, que pode utilizar até 64 processadores. O sistema é fornecido junto com o hardware e com um pacote de serviços que inclui a implementação, o que o torna uma solução incrivelmente cara, reservada a alguns nichos específicos.
x64-bit Edition	É a versão com suporte a processadores de 64 bits. Ela oferece os mesmos recursos da Standard Edition e é configurada da mesma forma, mas oferece suporte a mais memória RAM e pode rodar aplicativos otimizados para o uso de instruções de 64 bits.

Quadro 02: Versões do Windows Server

Fonte: Morimoto, C.E. Configurando um servidor Windows, 2008.

Em 27 de fevereiro de 2008 foi lançado pela Microsoft, um sistema operacional para servidores o Windows Server 2008 tinha como objetivo ser o sucessor do Windows Server 2003. Projetado para capacitar a próxima geração de redes, aplicativos e serviços Web, esses sistemas operacionais ajudam você a desenvolver, fornecer e gerenciar experiências e aplicativos avançados para usuários, fornecer uma infraestrutura de rede altamente segura e aumentar a eficiência tecnológica na sua organização.

Assim com o *Windows* Server 2003, o Windows Server 2008 possui quatro versões de seu sistema operacional, no qual é demonstrado no Quadro 03.

Windows Server 2008 Standard Edition	Em substituição ao Windows Server 2003, foi projetada para fornecer serviços e recursos para outros sistemas em uma rede. O sistema operacional tem um abundante conjunto de recursos e opções de configuração.
Windows Enterprise Edition	Windows Server 2008 Standard Edition para proporcionar maior estabilidade e disponibilidade e dar suporte a serviços adicionais como o Cluster e Serviço de Federação do Active Directory.
Windows Server 2008 Datacenter Edition	Versão mais robusta do Windows Server 2008 com aperfeiçoamentos nos recursos de cluster e suporte a configurações de memória muito amplas com até 64 GB de RAM em sistemas x86 e dois TB RAM em sistemas de 64 *bits*. Tem requisito mínimo de CPU e pode dar suporte a até 64 CPUs.

Windows Web Server 2008	Versão Web Edition do Windows Server 2008. Uma vez que foi projetada para fornecer serviços Web para a implantação de sites e aplicativos baseados nesta, essa versão do servidor só dá suporte a recursos relacionados. Especialmente, ela inclui o Microsoft.NET Frameworks, o Microsoft Internet Information Services (IIS), o ASP.NET, além do servidor de aplicativos e recursos de balanceamento de carga de rede. No entanto, não possui vários outros recursos, incluindo o *Active Directory*, e exige a instalação do *server core* para obter alguma funcionalidade padrão. O *Windows Web Server* 2008 dá suporte a até 32 GB de RAM e 4 CPUs x64.

Quadro 03: Versões do Sistema Operacional do Windows Server 2008

De acordo com Morimoto (2008), a Microsoft lançou no dia 4 de setembro de 2012 seu nosso software voltado a servidores o Windows Server 2012 é um sistema operacional destinado a administradores de redes que desejam utiliza-lo em servidores. Assim o Windows Server 2012 eliminou a versão Enterprise trabalhando nas versões Standard, Datacenter, Essentials e Foundation.

O mesmo autor afirma que a licença do Windows Server 2012 Foundation somente pode ser adquirida junto com o servidor, enquanto a edição Essentials pode ser adquirida na compra do servidor ou separadamente, no departamento de vendas da Microsoft. A Foundation é, em poucas palavras, uma edição básica do Windows Server 2012. Isso significa que você pode usar a grande maioria das ferramentas presentes em outras edições, como Standard e Datacenter, porém, precisará de profissionais de TI experientes para configurá-lo e gerenciá-lo. A Essentials, por sua vez, é mais *limitad*, contudo mais simples.

Em adição à pré-configuração do domínio durante o Setup do Sistema Operacional, a Essentials dispõe de serviços como compartilhamento de arquivos, backup centralizado de desktops (Windows 7 e Windows 8), monitoração e relatórios da saúde da rede, acesso remoto e pela *web*, *Group Policy* simplificada, e integração opcional com o Office 365 ou *on-*

premise Exchange Servers (MORIMOTO,2008). Com isso a Microsoft inovou neste software a virtualização *Hyper*-V. A quantidade de memória e o processador que ele consegue gerenciar deu um grande avanço. Outro recurso do Windows Server 2012 é a migração das máquinas pela rede. É possível transferir dados de várias máquinas virtuais ao mesmo tempo sem interromper o uso.

2.4. Principais aplicativos dos servidores Linux e Windows

2.4.1. Apache

O apache surgiu em 1995 com Rob MCCool, pela empresa *Apache Software Fundation*, sendo este desenvolvido. Esta empresa é responsável por diversos projetos de tecnologias de transmissão via *web*, no qual trabalha com processamento de dados e execução de aplicativos distribuídos. (SILVA, 2006)

O apache processa o protocolo HTTP (*Hyper-Text Transfer Protocol*), sendo um padrão de servidor *web*, o qual é utilizado por navegadores para acesso a site, assim fazendo a solicitação ao determinado servidor *web* do *site*, que através do HTTP recebe e informa o conteúdo correspondente.

Além do HTTP, este servidor utiliza o protocolo HTTPS (*HyperText Transfer Protocol Secure*), este utiliza uma camada SSL (*Secure Socket Layer*) que criptografa todos os dados transferidos entre o usuário e o servidor, dando assim uma segurança, confiabilidade e confidencialidade nos dados. Este servidor pode ser trabalhado, pelos sistemas operacionais Linux e FreeBSD e na plataforma Windows. Abaixo, um relato das principais características, conforme Silva (2006, p.98):

> Possui suporte a scripts CGI usando linguagens como Perl, PHP (*Hypertext Preprocessor*), Shell Script, ASP, etc;
> Suporte a autorização de acesso podendo ser especificadas restrições de acesso separadamente para cada endereço/arquivo/diretório acessado no servidor;
> Autenticação requerendo um nome de usuário e senha válidos para acesso a alguma página/sub-diretório/arquivo (suportando criptografia via Crypto e MD5);
> Negociação de conteúdo, permitindo a exibição da página *Web* no idioma requisitado pelo cliente navegador;
> Suporte a tipos mime;
> Personalização de logs;
> Mensagens de erro;
> Suporte a virtual hosting (é possível servir 2 ou mais páginas com endereços/ portas diferentes através do mesmo processo ou usar mais de um processo para controlar mais de um endereço);

> Suporte a IP virtual hosting;
> Suporte a name virtual hosting;
> Suporte a servidor Proxy FTP e HTTP, com limite de acesso, caching (todas flexivelmente configuráveis);
> Suporte a proxy e redirecionamentos baseados em URLs (*Uniform Resource Locator*) para endereços Internos;
> Suporte a criptografia via SSL (*Transport Layer Security*),Certificados digitais;
> Módulos DSO (*Dynamic Shared Objects*) permitem adicionar/remover funcionalidades e recursos sem necessidade de recompilação do programa.

2.4.2 IIS – *Internet Information Services*

O IIS (*Internet Information Services*) é um servidor *web* desenvolvido pela *Microsoft* para os seus sistemas operacionais nos servidores. Atualmente a versão mais atual é a IIS 7.5 a qual esta disponível para os *Windows Server* 2008 R2 e *Windows* 7.

A sua característica e a utilização para a geração de páginas em HTML, dinâmica que diferentemente dos servidores *WEB* usam a tecnologia própria, o ASP (*Active Sever Pages*), podendo usar outras tecnologias com o auxilio de módulos de terceiros instalados no servidor. Para a instalação desse servidor em *Windows* é necessário adquirir uma licença para o uso e instalação (OFICINA, 2010).

Depois do lançamento da plataforma .NET em 2012 o IIS ganhou também algumas funções de gerenciamento o ASP.NET, o qual possui basicamente dois tipos de aplicações, segundo (SILVA, 2010). São elas:

- Paginas *WEB*: acesso tradicional, com um conteúdo de extensão ASPX;
- *WEB Services*: Funções disponíveis pela rede, chamadas de aplicativos ASMX;

O ASP.NET é um forte concorrente com o JSP (*Java Server Pages*), no qual é compilado antes da execução, isso trás vantagens para compiladores interpretador pelo ASP e PHP.

2.4.3 Sistema gerenciador de banco de dados MySQL

O MySQL é um sistema de gerenciamento de banco de dados em SGBD (Sistema de Gerenciamento de Banco de Dados), no qual utiliza a linguagem SQL (*Structured Query Language*) em sua interface. Foi criado na Suécia por dois suecos e um finlandês, David Axmark, Alla Larsson e Michael "Monty" Widenius, no qual desenvolveram este projeto desde a década de 1980 (PORTAL, 2008).

Nos dias atuais seu desenvolvimento e manutenção empregam aproximadamente 70 profissionais no mundo inteiro, sendo que o mesmo é testado e aperfeiçoado continuamente.

Este servidor apresenta as seguintes características, baseadas em Portal (2008):

- A portabilidade (suporta praticamente qualquer plataforma atual);
- Compatibilidade (existem drivers ODBC (*Open Database Connectivity*), JDBC (*Java Database Connectivity*) e .NET e módulos de interface para diversas linguagens de programação, como Delphi, Java, C/C++, Python, Perl, PHP e Ruby);
- Desempenho e estabilidade;
- Pouco recurso de *hardware*;
- Facilidade de uso;
- Software Livre;
- Suporte a vários tipos de tabelas (como *MyISAM, InnoDB* e Maria), cada um específico para um fim.

O servidor MySQL, apresenta uma vantagem, a qual agrega, maior desempenho e força, sendo que seu código operacional aberto, opera em diversos sistemas como: *Windows Linux*, FreeBSD, *Solaris*, Mac OS X, SunOS, SGI, etc, oportunizando ser um servidor de multitarefa e multiusuário.

Apartir das versões 4.1 foi adicionado suporte a transações, *SubSelects, Foreign Keys*, e na versão 5.0, o MySQL incorporou os recursos *views , triggers, storage* procederes e transações XA, avançando o sistema (PORTAL,2008).

2.4.4 Firewall

A implementação de *firewall* vem crescendo, devido à necessidade dos administradores em monitorar, controlar o acesso a sua rede de computadores. Possuindo ferramentas que podem ser utilizadas tanto para a implementação na filtragem de pacotes, que trabalha na camada de rede, como os servidores Proxy os quais trabalham na camada de aplicação, ou seja, no modelo *Transmition Control Portocol/Internet Protocol* (TCP/IP).

O *firewall* é uma barreira tecnológica entre os dois pontos da rede, no qual o único acesso entre as redes interna e a internet, devendo permitir somente a passagem de tráfego autorizado, pois ele terá a função de filtrar todo o tráfego que está passando pela rede, assim fazendo a aplicação de bloqueio e rejeição (CAMY,2003).

Temos o *IPTables* que é dividido em três tabelas que são subdivididas por suas regras denominadas *chains*. As tabelas são *filter, Network Address Translation* (NAT) e Mangle.

Tabela Filter: essa tabela do iptables é dividida em três *chains*, no qual é utilizada pelo firewall no filtro de pacotes.

- *Input*: realiza a filtragem de tráfego que entra no *firewall*.
- *Forward*: Realizada a filtragem do todo o tráfego que passa pelo firewall, no qual deverá ser redirecionada para outro host ou interface de rede.
- *Output*: faz a filtragem do tráfego de saída do *firewall*.

  Os pacotes são submetidos na tabela *filter*, como pode ser observado na Figura 2.

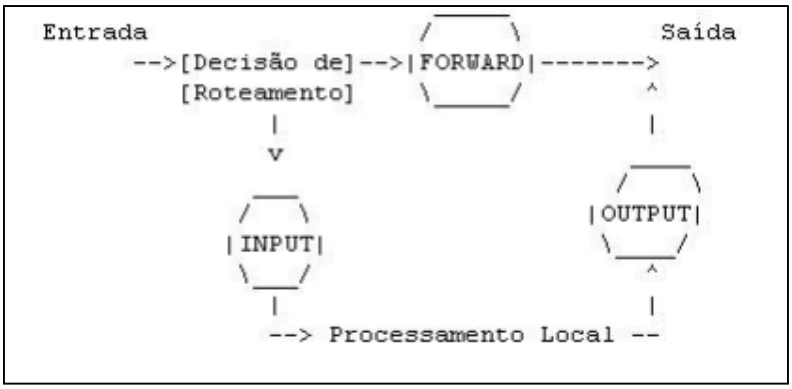


FIGURA 2: Tabela Filter
Fonte: Neto, 2004

Tabela NAT: Esta tabela do IPTables é dividida em três *chain* é implementada num firewall NAT:

- *Prerouting Destination-NAT* (DNAT)*:* esta realiza a alteração de pacotes antes do roteamento. Um exemplo é quando tem um firewall na borda, no qual as requisições chegar na porta *HyperText Transfer Protocol* (HTTP), da porta 80 para um servidor que esta pagina esta localizada em uma *DeMilitarized Zone* (DMZ), então esta regra é utilizada pois neste chain ele tratara o destino do NAT.
- *Postrouting Source-NAT* (SNAT)*:* esta regra é utilizada para fazer alterações em pacotes de roteamento.
- Output (NAT): regra na qual faz a liberação ou bloqueio de todos os pacotes com a origem no host do firewall.

Tabela Mangle: Esta tabela faz alterações especiais dos pacotes em um nível mais o de complexibilidade, no qual permite haver as alterações da prioridade do pacote, no qual será na entrada e saída, seguindo o seu *Type Of Service* (TOS). Isso é composto por cinco *chains*, no qual pode ser utilizado em um firewall implementado.

- *Prerouting*: marca e altera os pacotes antes do roteamento.
- *Input*: marca e altera os pacotes na entrada no host firewall.
- *Forward*: marca e altera os pacotes que estão redirecionado a outros host ou para interface de rede.
- *Output*: marca e altera pacotes antes de serem roteados.
- *Postrouting*: marca e altera os pacotes após o roteamento.

As regras da tabela *mangle*, são interpretadas antes da tabela *filter* e Nat.

Vale ressaltar, conforme Neto (2004), que o TOS, um campo no cabeçalho do protocolo IP, no qual ele tem a finalidade de especificar qual a prioridade do pacote, a vantagem da sua utilização é a priorização dos serviços. Pois todos têm a mesma prioridade normal do serviço no cabeçalho, somente este campo pode ser alterado no *firewal* na tabela *mangle*, um pacote com prioridade maior, conforme o serviço que ele presta.

2.4.5 Sistema gerenciado de banco de dados MS SQL Server

O MS SQL *Server* é um sistema de Gerenciamento de Banco de Dados (SGBD), sendo o mesmo desenvolvido pela *Microsoft*, em 1988 com a parceria de SyBase, perdurando essa parceria até 1994. Neste mesmo ano foi lançada a versão para *Windows* NT, em que a *Microsoft* continuou aperfeiçoando o MS SQL, podendo ser considerado como um Banco de Dados robusto e empregado por sistemas corporativos dos mais diversos portes (RAMALHO, 2002).

Frente a alta capacidade e utilidade que o mundo corporativo apresenta, entre elas a capacidade de implementar e criar soluções baseadas no seus bancos de dados, este sistema de gerenciamento, oportuniza uma busca rápida, precisa, de baixo custo e o gerenciamento para as aplicações a serem desenvolvidas.

O MS SQL *Server*, devido à melhorias significativas nos serviços, sua reengenharia na instalação, configuração e arquitetura, possibilita que a sua instalação será dinâmica, pois essas melhorias fazem com que os *bits* instalados estejam separados dos *bits* físicos do *hardware*, através de uma configuração, sendo que as empresas possam fornecer as configurações de instalação recomentada a cada parceiro do *software* (RAMALHO, 2002).

Ao que diz respeito, a resolução de problemas devido ao desempenho dos administradores em executarem esta tarefa, pois o mesmo envolve tempo e pesquisa, assim o MS-SQL incluiu uma coleção de dados e de desempenho em seu amplo repositório,

centralizando os dados e fornecendo novas ferramentas para relatório de monitoramento em relação a desempenho e a coleção de dados do software.

Outra tarefa que este sistema de gerenciamento oferece, é o Recurso de Captura de Alteração de Dados, ou seja, todas as mudanças que foram realizadas, capturadas e informadas à tabela de alteração, geram a captura dos dados, fazendo o cruzamento entre os dados alterados e os anteriores, impregnando essa nova organização, constituindo uma Data *Warehouse* desses dados.

Objetivando simplificar o desenvolvimento de suas aplicações o MS-SQL utilizada pela LINQ (*Language Integrated Query*), auxilia na utilização do objeto a endereçar as consultas em relação aos dados usados na linguagem de programação, como C#, ou VB.NET, ao invés de declarações de SQL. Permitindo com isso, consultas transparentes, intuídas e orientadas, escritas na linguagem NET., sendo executadas em ADO.Net (LINQ para SQL), ADO.Net DataSets (LINQ para DataSets), ADO.NET Entity Framework (LINQ para Entidades) e provedor de mapeamento de serviços de dados de entidade. Utilizando o novo provedor LINQ para SQL, permite que os desenvolvedores usem a LINQ diretamente nas tabelas e colunas do SQL Server (RAMALHO,2002).

Ao nos referirmos aos Backups de MS-SQL Server, os mesmos podem ter compressão, ou seja, redução do seu espaço em disco, sendo executada de forma rápida e segura (RAMALHO, 2002).

Com base nas informações apresentadas, fica notório que o MS-SQL fornece aos servidores e trabalhadores, uma plataforma abrangente, auxiliando e assessorando os sistemas e a linguagem de programação que for necessária.

2.4.6 PHP

O *Hypertext Preprocessor* (PHP), foi desenvolvido em 1995, por Rasmus Lerdorf, tendo por objetivo um *software* livre, licenciado sob a PHP Licença, incompatível com a GNU General Public. Licença (GPL) devido à restrições no uso do termo PHP. Sua implementação principal é a referência formal da linguagem, mantida por uma organização chamada The PHP Group.

O PHP é um acrônimo recursivo para "PHP: *Hypertext Preprocessor*" é uma linguagem interpretada livre ou *Open Source* e de uso geral, é muito utilizado para desenvolvimento de aplicações *web* embutido dentro de um *script html* assim instalado no servidor e gerando conteúdos dinâmicos na *World Wibe Web* (WWW), gerando uma página

web visualizada pelo usuário (ACHOUR et al, 2013).

Frente a isso, Achour et. al. (2013), explica que o PHP pode ser utilizado na maioria dos sistemas operacionais, incluindo *Linux, Windows, Mac* OS X, RISC OS, entre outros. O PHP pode ser executado pela maioria dos servidores *web* atuais, entre eles, *Apache, Microsoft Internet Information Server, Personal Web Server, Netscape and iPlanet Servers, Oreilly Website Pro Server, Caudium, Xitami, OmniHTTPd*. Podendo ser configurado como módulo para a maioria dos servidores, e para os outros como um CGI (*Common Gateway Interface*) comum.

Concorrente direto da tecnologia ASP pertencente à *Microsoft*, o PHP é utilizado em aplicações como o *MediaWiki*, *Facebook, Drupal*, *Joomla*, *WordPress* e o *Magento*. Sendo utilizados, para oferecer habilidade em geração de imagens, arquivos em PDF, animação em *Flash* e também a criação de padrão de texto como XHTML e outros arquivos XML.

O PHP tem a possibilidade de suporte em uma ampla variedade de bancos de dados, sendo eles, de acordo com Achour (et. al., 2013): *Adabas* D, *dBase*, *Empress*, *FilePro* (read-*only*), *Hyperwave*, IBM DB2, *Informix*, *Ingres*, *InterBase*, *FrontBase*, mSQL, *Direct* MS-SQL, MySQL, ODBC, *Oracle* (OCI7and OCI8), *Ovrimos*, *PostgreSQL*, *SQLite*, *Solid*, *Sybase*, *Velocis* e *Unix* dbm.

O PHP suporta ODBC (*Open Database Connection*, ou Padrão Aberto de Conexão com Bancos de Dados), permitindo a utilização de qualquer outro banco de dados que suporte esse padrão mundial.

2.4.7 ASP.NET

O ASP.NET (*Active Server Pages.NET*) é uma forma de se desenvolver páginas *WEB*, aplicativos *desktop*, aplicativos para dispositivos móveis, objetivando negócios para *web*, serviços, entre outros.

Essa plataforma .NET é similar à plataforma JAVA, mas o que as diferencia é que a linguagem JAVA se caracteriza por aplicativos hídricos (compilados e interpretados. Isso caracteriza que seus aplicativos sejam utilizados em multi-plataformas), nos quais o .NET utiliza-se de *Visual Basic*, C++, JScript.NET ou C# e os aplicativos no qual são gerados para a compilação em uma linguagem de MSIL (*Microsoft Intermediate Language*).

No desenvolvimento de uma página ASP.NET, a sua compilação é realizada no instante que ela é chamada pelo *browser*, no qual é apresentado o seu conteúdo final em HTML (*Hypertext Markup Language*). Para a execução das páginas se faz necessária a

utilização de IIS (*Internet Information Server*), além da instalação de aplicativos como .NET *Framework* SDK.

Com isso, a tecnologia ASP.NET é possível obter aplicativos *Web* com a facilidade de *desktop*, com o *Delphi* e demais ferramentas. Para se realizar as modificação dos dados em ASP.NET utiliza-se o ADO.NET (*ActiveX Data Objects .NET*), sendo esta uma interface de programação para ter acesso as dados.

O ASP.NET conta com um sistema de SGBD's (Sistemas Gerenciadores de Bancos de Dados)diversos, como o SQL Server, MySQL, *Oracle* e entre outros.

2.4.8 FTP

O *File Transfer Protocol* (FTP), ou em português Protocolo de Transferência de Arquivos, é uma forma rápida e versátil de transferir arquivos, no qual é muito utilizado na internet por meio de protocolo ou por programas que implementam este protocolo. Sendo baseado na TCP.

A transferência de arquivos ocorre entre o computador do usuário e do servidor, podendo ser feita via *software* específico, no qual será informado o IP ou endereço do servidor, juntamente com o usuário e senha, assim seleciona os arquivos e envia para o servidor. A porta de comunicação do padrão do FTP é a 21, conforme RFC 959 (1985).

O acesso a um servidor FTP pode ser realizada de dois modos:

1 - Via linhas de comando do *Linux,* e do *Windows* através do telnet em modo linha de comando.

2 - Via *Browser* como o *Internet Explorer*, *Firefox*, o *Windows Explorer,* entre outros, é possível o acesso ao servidor FTP, bastando apenas informar o endereço:
FTP://[username] : [password] @ [servidor].

2.4.9 Segurança no Terminal

A segurança no terminal deve-se ter um cuidado, pois a exploração da vulnerabilidade por uma ameaça remota e em certos momentos por ameaças internas são muitas vezes esquecidas e até mesmo submetidas.

Se uma pessoa mal intencionada tiver o acesso físico aos servidores pode ter acesso a um servidor logado como o usuário *root* e assim danificar o sistema como os demais servidores. Para isso existe a variável TMOUT a qual tem a função de executar um *logout*

automático após perceber o tempo de inércia no terminal (REIS, JULIO, VERBENA, 2011).

Assim, obtendo uma segurança no terminal, esta configuração é realizada em um arquivo no *Linux* /etc/profile, no qual o valor a ser acrescentado deve ser analisado pelo administrador com cuidado, evitando assim acesso indevido. Pois um valor muito alto poderá dar acesso ao usuário em uma estação logado como *root*, e se valores forem baixos podem interferir nas tarefas. O Arquivo/etc/profile, configurado com o valor de 60 segundo, conforme, Quadro 4:

```
#vim /etc/profile
TMOUT=60
export PATH TMOUT
```

Quadro 4: Configuração da Segurança Terminal
Fonte: Reis, Julio, Verbena, 2011.

O arquivo /etc/profile é somente lido durante o *boot* do sistema, por esta forma sempre utilizamos o comando *source*, para que o arquivo possa ser lido novamente e atribuído aos sistemas com as alterações realizadas conforme o comando: *#source /etc/profile.* Assim, após os 60 segundo de inatividade, o *Shell* fará o *logout* automático (REIS, JULIO, VERBENA,2011).

Deve-se ressaltar que se um usuário mal intencionado ou inexperiente tiver acesso aos servidores e der um o CTRL+ALT+DEL para reiniciar o servidor, irá interromper todo o serviço correspondente aquele servidor ou demais servidores. Para isso, é importante a segurança da informação, mais precisamente a política de segurança utilizando a norma ISO 27002, por tratar as questões de acesso físico à sala de servidores, para evitar problemas quando utilizar a função CTRL+ALT+DEL, editando o arquivo/etc/inittab, conforme comando, da Quadro 05:

```
#vim /etc/inittab
# Antes
# What to do when CTRL-ALT-DEL is pressed.
ca:12345:ctrlaltdel:/sbin/shutdown -t1 -a -r now
# Depois
# What to do when CTRL-ALT-DEL is pressed.
#ca:12345:ctrlaltdel:/sbin/shutdown -t1 -a -r now
#ou
# Depois
# What to do when CTRL-ALT-DEL is pressed.
ca:12345:ctrlaltdel:/bin/echo "Opção desativada !"
```

Quadro 5. Configuração da Segurança Terminal Windows
Fonte: Reis, Julio, Verbena, 2011.

Já o SSH (*Secure Shell*) é um programa utilizado para acesso remotamente, ele fornece uma autenticação forte e comunicação segura sobre os cais inseguros como *internet*. Este programa é utilizado para *logar* em sistemas *Linux*, utilizando através de uma máquina *Windows*, *Mac* ou mesmo outro *Linux*, na qual os tradicionais *telnet* e *rlogin* não fornecem criptografia de senha para a sessão. (REIS, JULIO, VERBENA, 2011).

Quando um servidor de SSH é configurado precisamos realizar algumas configurações importantes no qual devem ser feitas conforme Quadro 6:

```
#vim /etc/ssh/sshd_config
# Altere a porta padrão
Port 42129
# Protocolo 2 (anteriores possuem falhas de segurança)
Protocol 2
# Tempo ativado para digitar a senha
LoginGraceTime 45
# Não aceitar login como root
PermitRootLogin no
# Não aceitar login sem senha
PermitEmptyPasswords no
```

```
# Usar o módulo do pam para se autenticar
UsePAM yes
# Definir usuários que tem permissão de fazer login
```

Quadro 6. Configuração *SSH*
Fonte: Reis, Julio, Verbena,2011.

Realizada esta configuração, será preciso reiniciar o serviço de ssh do servidor conforme comando: *$invoke-rc.d ssh restart.*

2.4.10 Gerenciamento de Privilégios

Este subtema, esta baseado em Reis, Julio, Verbena (2011), que indicam, em servidores, o uso frequente de root para se *logar,* no qual este usuário é o mais visado por *cracker* e usuários mal intencionados, pois o mesmo tem permissão total sobre o servidor, com isso eles usam *script* para quebrar a senha de *root* em um servidor, tendo assim o controle sobre o sistema.

Com isso, para dificultar a invasão e ficarem longe as ameaças, é preciso desativar o *login* como o usuário *root* nos servidores em que são de modo texto, desta forma o administrador poderá ter acesso com outro *login* e usuário comum, sendo quando necessário executar alguma tarefa tornar-se um usuário root.

Importante também determinar a data de validade para a senha dos usuários com auxílio de comando *usermod,* fazer a remoção via *shells* válidos dos usuários que não está em uso, também são meios de proteger o servidor e o sistema, tendo assim uma *rodustes* em seu sistema.

2.4.11 Portas Abertas

Na instalação de um sistema novo alguns serviços podem deixar uma vulnerabilidade no sistema como determinada portas. Para isso recomenda a instalação do NMAP (*Network Mapper*), no qual esta ferramenta pode fazer a busca por todas as portas abertas no sistema, no qual pode ser criada regra no *firewall* para bloquear as que não poderão estar disponíveis para acesso, conforme comando apresentado no Quadro 07:

```
#nmap -A -p 1-65535 localhost
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     protocol 2.0
25/tcp   open  smtp    Postfix smtpd
53/tcp   open  domain  dnsmasq 2.47
80/tcp   open  http    httpd 2.2.11
631/tcp  open  ipp     CUPS 1.3.9
3306/tcp open  mysql   MySQL 5.0.75-0
```

Quadro 07. Configuração da Porta Aberta

Fonte: Reis, Julio, Verbena, 2011.

2.5 Trabalhos relacionados

Neste tópico serão apresentados alguns trabalhos relacionados ao tema do estudo – *Hardening*.

O estudo *Exploring attack graph for cost-benefit security hardening*: *A probabilistic approach,* de *Shuzhen, Zonghua, Youki* (2013), aponta que com o crescente aumento de serviços prestados pelos sistemas e a sua crescente vulnerabilidade, vem se criando um desafio cada vez maior para os administradores de segurança, no que diz respeito aos ataques a sistemas e de uma rede, com isso os administradores, através de ferramentas de análise, estão elaborando métodos de prevenção e detecção de seus sistemas.

Diante disso, este trabalho teve como abordagem verificar a vulnerabilidade do nível de segurança de um sistema, com a sua análise e nível de uma segurança com o auxílio aos administradores de segurança. Oferecendo custo benefício para a empresa, ao que se refere geração de gráficos, análise das vulnerabilidades, ação se algum ataque estiver sendo realizado, ocasionando a prevenção por meio das ferramentas de apoio.

Os autores abordam ainda, que existem três questões as quais devem ser cuidadosamente consideradas quando se refere a vulnerabilidade de ataque a sistema: deve-se avaliar as vulnerabilidades individuais, examinar as ações implicadas à vulnerabilidade explorada por um ataque, e a eficácia sobre a medida adotada por este ataque.

Assim a *Vulnerability Scoring System* (CVSS) tornou-se um padrão da indústria aceito para avaliação dos riscos e vulnerabilidade dos sistemas, além de gerar modelos de gráfico e forma de ataque (SCHIFFMAN,2005).

Outro estudo que contrapõem a esta temática é *An aspect-oriented approach for the systematic security hardening of code*, dos autores *Mourad, Laverdiére e Debbabi* (2008). Este esboço tem na sua abordagem na prevenção, detecção a intrusos e o rigidez de seu código fonte, no qual este sistema pode estar sendo executado em uma rede local ou web tendo em vista a segurança do sistema.

Esta segurança pode ser realizada através de um padrão de implementação e um código de segurança, sendo que quando necessário este é inserido ao sistema dando-lhe uma estabilidade evitando assim alguma desconfiguração e a descoberta de alguma vulnerabilidade no código.

Com isso os desenvolvedores de *softwares* sofrem muito com este quesito de segurança e muitas vezes deixam seus códigos equipados em relação à segurança e outros não a uma segurança adequada e nem como programar algo, pois seu código está bloqueado ou até mesmo perdido no caso de *Commercial-Off-The Shelf* (COTS). No entanto quando código foi de *Software* Livre e de Código Aberto há uma vasta gama de melhoramentos de segurança que podem ser aplicados com foco na segurança. O estudo acima citado foi desenvolvido com o Programa Orientado a Aspecto (AOP), assim fornecendo uma segurança para o código.

Seguindo esta linha de pensamentos, o estudo denominado *Practical application of information security models*, sob autoria de *Jirasek* (2012), aponta a gestão de risco em relação a segurança da informação como uma área que deve ter uma atenção toda especial, pois temos o surgimento de novas tecnologias, e com isso novas, ameaças e normas que devemos estar devidamente relacionadas a segurança da informação, pois tudo isso temos risco e informações disponíveis.

Assim deve ter uma estratégia de uma gestão de risco em uma empresa, pois como se tem uma gestão de negócio elaborado por administrador, deve também juntamente com administradores e o departamento de segurança da informação ter essa estratégia, pois se algo acontecer como proceder e qual medida tomar para evitar maiores transtornos à empresa que trabalha a área de tecnologia.

Gestão de riscos de segurança da informação é uma área que está em constante movimento para responder novas ameaças, normas e tecnologias. A segurança é agora uma parte do risco da informação gestão, que por sua vez tem um lugar na estratégia de gestão de risco global de negócios.

2.6. Hardening

Hardening é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas e com o foco na infraestrutura, e objetivo principal de torná-la preparada para enfrentar tentativas de ataques.

Assim, muitos executivos no ramo dos servidores, sem muita experiência na segurança da informação, instalam e deixam suas empresas com uma instalação básica permitindo meios de invasão, advindo que apenas deixam funcionando, não se preocupando em fechar portas e serviços desnecessários.

O Sistema *Linux* e *Windows* podem ser ótimos servidores desde que sejam feitas as configurações e permissões corretas, utilizando as técnicas de *hardening*, deixando esses servidores mais seguros e invioláveis, dando uma confiabilidade no serviço que eles executam (BARBOSA, 2012).

Neste sentido, Barbosa (2012), descreve que para as técnicas de *hardening* podemos utilizar três fatores, que são eles: a segurança, risco e flexibilidade. Sendo preciso equilibrar esses três fatores, para objetivar uma melhor produtividade e segurança desses servidores.

Entretanto, não podemos esquecer que não existe um servidor 100 % seguro, mas vale lembrar que quanto mas seguro for o servidor, menos risco este oferecerá e também pouca flexibilidade, assim tem que equilibrar para proporcionar um ótimo funcionamento.

Se o servidor, não apresentar uma grande flexibilidade, que permita qualquer programa nele, a nossa segurança ficará baixa e os riscos irão aumentar (MELO, 2006). Para tudo isso não tem uma regra, mas os itens segurança, risco e flexibilidade, poderão acontecer para cada situação e de acordo com a necessidade de cada administrador.

Com isso, vemos que cada implementação de um servidor poderá ser diferente e definida antes de ser realizada, devendo ser analisada, pois a técnica de *hardening* é extremamente importante, mas não se aplica em todas as situações. Inicialmente recomenda-se sempre instalar versões atuais dos sistemas operacionais, que contêm correções e patches de segurança, pois pode ser problemático utilizar uma versão antiga sem atualizações, deixando o sistema temporariamente vulnerável no caso da existência de pacotes com falhas. Serviços críticos como *web*, *email* e DNS, devem estar sempre nas versões mais atuais. *Softwares* desnecessários devem ser desinstalados e pacotes inseguros devem ser substituídos por alternativas mais confiáveis.

Para isso precisa ser analisado o procedimento que melhor se adapta à necessidade. Outro ponto importante é que o *hardening* é focado na camada de "*userland*", no qual *hardening* é composto por quatro etapas, definidas na tabela a seguir:

Mapeamento das ameaças	As ameaças são algo que podem gerar um impacto negativo em algo que está sendo executado em nosso equipamento, naquele determinado momento, sendo possível por uma vulnerabilidade no sistema. Com isso, se tem diversas vulnerabilidades em nosso servidor, podendo ter ameaças que comprometam nosso ambiente de trabalho e consequentemente pode-se ter um risco. Assim, as ameaças são circunstâncias e incidentes que podem gerar grandes impactos negativos, e devemos explorar a vulnerabilidade tornando um potência de risco menor (BARBOSA, 2012).
Mitigação do Risco	Para reduzir o risco possuímos três pilares da segurança da informação que seja utilizado para ataque que são: • Evitar o risco: Possuir medidas para que sejam tomadas, para assim eliminar toda e qualquer forma de ameaça, que não venha a acontecer nenhum incidente. • Suporta / Aceitar risco: Ter a consciência que risco devem ser aceitos e compreendidos. Isso para que quando algo acontecer, a medida de segurança tenha uma estratégia para minimizar e resolver determinado dano. EX: se houver um incêndio na sala devemos apagar o fogo com o extintor de incêndio. • Neutralizar o risco: Ter medida de proteção para que se a ameaça vir a acontecer, já se tenha um conhecimento do que se deve fazer e a organização opta pela tomada das combinações de preventiva, detetives e repressivas.
Ações corretivas e preventivas	As ações preventivas para os riscos em TI são ações que já fazem parte do dia-a-dia de técnicos e gerente de TI. No ambiente de trabalho do departamento de TI é recomendável que as ações preventivas sejam utilizadas com mais frequência que as corretivas, pois essas ações devem estar orçadas, contratadas e ter um

	acompanhamento dos equipamentos que estão sendo utilizados. As ações corretivas se baseiam pelo resultado e de um planejamento inadequado ou alguma falta de preparo. Com isso as ações corretivas ocorrem, na maioria das vezes, de uma forma emergencial, sem planejamento e dependendo do procedimento e as ferramentas utilizada podem ser mais nocivas para o ambiente de TI do que benéficas. Um exemplo de ação preventiva é a gestão de servidores: é recomendável que estes passem por manutenções preventivas de *hardware* periódicas com disco, memória, capacidade, desempenho e etc, assim como o ambiente operacional *software* gerenciamento, sistema operacional e demais sistemas sejam atualizados e conforme orientação do fornecedor. Se não estiver havendo manutenções e atualização preventiva de *Hardware* e *Software*, os riscos de uma indisponibilidade no ambiente podem ser potencializados. Pós as ações preventivas possibilitam os gestores de TI ter menos risco. (IETEC-Instituto de Educação Tecnológica) (BARBOSA, 2012).
Estratégia de Segurança	Tendo em vista que antes da implementação de um sistema de segurança deve-se ter conhecimento de algumas estratégias que têm que adotar na construção deste, usamos como a base um *firewall*. Privilégio Mínimo: Deve-se sempre garantir que o usuário só tenha acesso aos recursos que ele necessita de acesso, tendo o cuidado de não atribuir privilégios menores do que o necessário. Isso é utilizado com extrema importância para eliminar ou amenizar danos causados por pessoa mal intencionada. Em um contexto de Internet temos alguns exemplos: • Todos os usuários não precisam acessar todos os serviços de Internet; • Todos usuários não precisam modificar os arquivos em seu sistema; • Todos os usuários não precisam saber a senha de root (administrador) das máquinas; • Todos administradores de sistema não precisa conhecer as senha de *root* de todos os sistemas;

	Muitos dos problemas de segurança podem ser evitados com a utilização desses princípios (MELO, 2006). Segurança por Obscuridade: Este é um princípio no qual não é nada confiável, pois incide unicamente em ocultar informações. Exemplo deste método: • Instalar uma máquina na internet é pensar que ninguém tentará invadí-la, pois você não comentou nada a ninguém sobre ela; • Abrir em um servidor Apache uma porta diferente para que ninguém utilize, a não ser as pessoas que irão utilizar; • Utilizar a sua rede de tal maneira que os usuários internos observem as informações de tal maneira que os usuários externos (internet) não vejam essas informações, como por exemplo, portas e serviços prestado no servidor. **Alguns pontos que devemos ter conhecimento** • Usufruir de técnicas em conjunto com outras, para assim manter uma segurança, pois ter uma segurança através da obscuridade é ruim; • Não informar algo não é o mesmo que ocultá-lo; • A utilização de um sistema de criptografia desconhecida, não garante segurança. (MELO, 2006); **Segurança em Profundidade ou em camada:** A implementação do máximo de controle possível em uma ambiente para proteger os ativos, tem como o princípio da segurança para prevenção dos acidentes, assim podemos evitar que um problema isolado se alastre pelo sistema, instituindo múltiplos, redundantes e independentes níveis de proteção, no qual a ideia não seja apenas depender de um único método de defesa e sim vários níveis de proteção. Para que, se houve alguma tentativa de invasão arriscada demais seja cansativa para o atacante. Pois a chance de violar um nível de proteção de um sistema é maior do que um sistema com vários níveis de segurança e proteção (MELO, 2006).

Quadro 8: Etapas do *Hardening*
Fonte: BARBOSA, Felipe Santos. Fundamentos em Segurança e *Hardening* em Servidores *Linux* baseado na Norma ISO 27002, 2012.

A seguir são apresentadas algumas utilizações de *hardening* muito úteis na configuração de sistemas operacionais, citadas por Reis, Julio, Verbena (2011):

- *À procura de senha fraca:* esta senha deve ser única e intransferível, sendo de propriedade de apenas um usuário que utiliza o sistema, com isso o administrador da rede não deve ter conhecimento desta senha, ou seja, ele até pode gerar uma senha, mas que obrigue o usuário no seu primeiro *login* realizar a troca da mesma para dar confiabilidade e segurança ao usuário. Criar mecanismos de bloquear senhas fáceis como 123456, data de aniversário, nome próprio, entre outras. O administrador também pode criar rotinas de verificação das senhas do sistema, no qual podem ser utilizadas várias ferramentas capazes de avaliar se a senha do usuário é fraca ou não. Para isso, podemos utilizar o *John the Ripper*, no qual ele verifica as senhas dos usuários no sistema e cadastra como fraca assim informando ao administrado de rede para que as senhas sejam trocadas e seu sistema fique seguro.

- *Serviços desnecessários e inseguros*: após o sistema instalado deve ser realizar uma verificação minuciosa de todos os programas no qual foram instalados nos sistemas, para assim realizar a desinstalação do programa que não será utilizado pelo mesmo. Dependendo do servidor, ele nunca deverá conter programas no qual chamado de "cliente", estes são serviços de *telnet, rshd, rlogind, rwhod, ftpd, sendmail, identd, wget*, entre outros. Estes mesmos deverão ser removidos. Tais serviços podem ser desinstalados usando o gerenciador de pacotes do sistema operacional, ou desativando-os em todos os níveis de inicialização. Além disso, podem-se remover entradas específicas dos programas no boot do sistema operacional.
- *Usuários Inválidos*: o sistema Linux possui três tipos de usuários, *usuários root*, que é o administrador do sistema, *usuário comuns*, os quais possuem uma senha para logar no sistema e acesso a um diretório home, assim não tendo acesso aos demais diretórios, e por último o *usuários de sistema*, que são responsáveis por controlar requisições de serviços. O *shell* é a interface entre usuário e sistema. Sem um *shell* válido, não é possível digitar comandos e interagir com o sistema. O usuário de sistema www-data, responsável por

receber requisições do servidor *Web*, que esteja com um *shell* válido, poderá introduzir vulnerabilidades ao seu sistema.

- *Desconexão de usuários não autorizados*: é bom ter conhecimento de quais usuários pode ter acesso de dentro e fora da empresa. O acesso não autorizado por sistemas externos deve ser cancelado com extrema urgência, em especial se o usuário estiver ocultando sua identidade. Para os casos de acesso por usuários internos não autorizados, podem ser necessárias ações disciplinares dependendo da natureza do acesso. É importante salientar que, quando ocorre uma invasão de sistema, é fundamental que as evidências relacionadas ao acesso indevido sejam registradas antes da desativação da conta não autorizada, tendo cuidado para não destruir provas relacionadas ao crime.
- *Colocar senha criptografada no GRUB*: muitos administradores não estão preparados para lidar com estruturas críticas. O simples acesso físico de um usuário à sala de servidores pode representar uma violação de segurança grave, pois esse poderá conseguir acesso de *root*, se reiniciar o servidor e alterar a senha do *root* através do gerenciador de *boot* (*grub*). Esse processo poderá ser evitado se uma senha criptografada for adicionada ao gerenciador, não permitindo que um usuário qualquer inicie o sistema no modo de segurança.
- *Política de utilização de serviços de Rede*: o TCP *wrappers* oferecem controle de acesso a vários serviços. A maioria dos serviços de rede modernos, como *SSH*, Telnet e FTP, utilizam os TCP *wrappers*, que ficam monitorando a entrada de um pedido e o serviço requisitado. O uso do TCP *wrappers* é uma boa prática na implementação de segurança em redes, limitando o uso dos serviços de rede. Liberar acesso somente a IPs desejados, configurar as restrições do *SSH* não permitindo *login* como *root* e configurar os módulos do pam para restringir acesso ao servidor em determinado horário, são boas práticas que devem ser adotadas.

3. METODOLOGIA

Para a realização desse projeto, que prevê a implantação de serviços de segurança, com o intuito de compartilhar conhecimentos a respeito da técnica de *Hardening* em servidores, será realizado um estudo de cunho e interesse pesquisa e conhecimento**,** podendo assim ser utilizada por administradores e gerentes de TI, possibilitando uma visão das técnicas de *Hardening* utilizado em servidores *Linux* e *Windows*.

Assim, se fará a organização deste estudo:

- Instalação dos sistemas operacional *Linux* e o sistema operacional *Windows Server* em servidores distintos.
- Enumerar os serviços e verificação da utilização das configurações padrões dos servidores;
- Instalação das configurações das ferramentas (Apache, MySQL, FTP, ...).
- Implantação das técnicas de *Hardenig* para cada servidor, apontando os setores que expostos à brecha de segurança e fazer o tratamento destas;
- Apresentação dos resultados obtidos, por meio da elaboração de um manual didático, da melhor prática de implementação de um servidor *Linux* e *Windows* utilizando técnicas de *Hardening*.

4. DESENVOLVIMENTO

Este capítulo irá detalhar o desenvolvimento e aplicação das técnicas de hardening, nos sistemas operacionais *Linux* e *Windows*, sendo apresentada amostra das imagens do sistema desenvolvido, com a sua análise navegacional de toda a aplicação.

4.1 Interface navegacional no sistema Linux

A primeira página a ser exibida para a instalação dos *software*, podendo-se observar códigos de configuração, redirecionando para a efetivação do sistema e próximas subseções.

```
$ sudo apt-get update
$ sudo apt-get upgrade
$ sudo apt-get install apache2 php5
```

Quadro 09: Configuração Inicial
Fonte: Imagem criada pelo próprio autor.

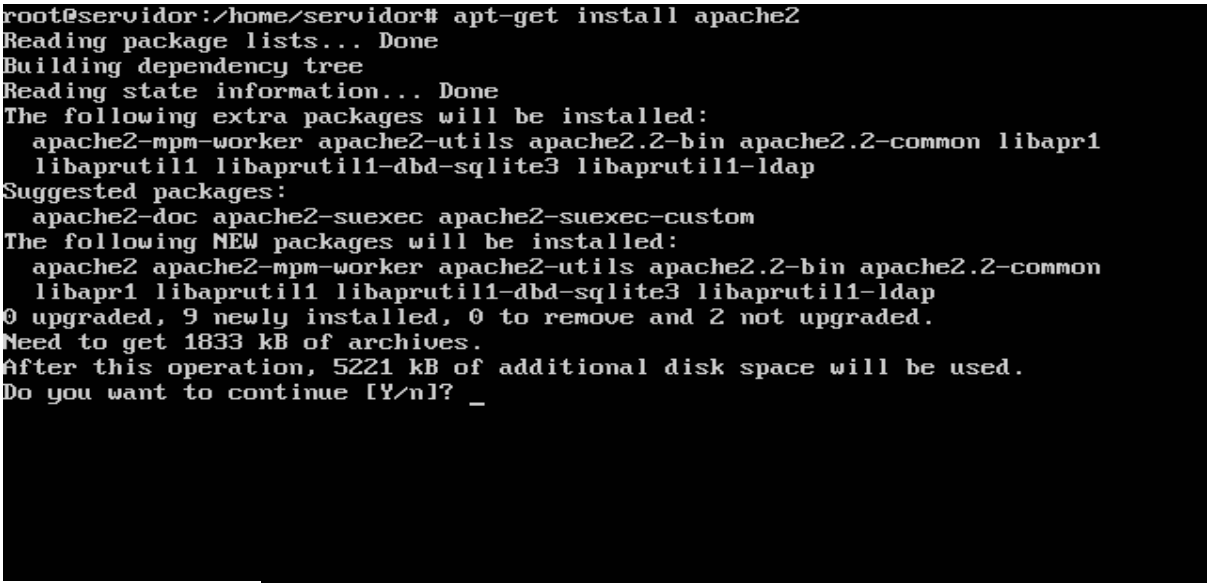


FIGURA 03: Tela inicial.
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Efetivando a configuração, do Quadro 10, é possível administrar o MySQL sendo esta uma das melhores configurações para este fim.

```
$ sudo apt-get install mysql-server-5.0 php5-mysql

$ sudo /etc/init.d/apache2 restart

$ sudo apt-get install phpmyadmin
```

Quadro 10: Configuração MySQL
Fonte: Imagem criada pelo próprio autor.

É importante ressaltar, que ao acessar o endereço http://localhost/phpmyadmin/, fornecendo o seu *login root* e a senha, a ferramenta MySQL, já se encontrará instalada, iniciando assim a configuração nas técnicas de hardening, no comando */usr/bin/mysql_secure_installation.* Observe no Quadro 11 a seguir:

Enter current password for root (enter for none): **Informe a senha do root do mysql ou pressione ENTER se a senha ainda não foi configurada**

Change the root password? [Y/n] **Pressine ENTER para criar uma nova senha**

Remove anonymous users? [Y/n] **Pressione ENTER**

Disallow root login remotely? [Y/n] **Pressione ENTER**

Remove test database and access to it? [Y/n] **Pressione ENTER**

Quadro 11: Configuração MySQL nas técnicas de Hardening
Fonte: Imagem criada pelo próprio autor.

Outra ferramenta ao ser utilizada no sistema *Linux* é a SSH, sendo alterada a sua configuração para a utilização do protocolo SSHv2.

A seguir no Quadro 12, será apresentada a sequência de formulação desta nova ferramenta.

Editar o arquivo /etc/ssh/sshd_config e trocar a linha: criar o grupo “sshlogin” para usuários que podem acessar o servidor remoto, e desabilitar o login do root no SSH: vi /etc/ssh/sshd_config Adicione as seguintes linhas: #AllowUsers root or PermitRootLogin no AllowGroups sshlogin

Quadro 12: Configuração SSH
Fonte: Imagem criada pelo próprio autor.

Seguindo este mesmo conceito de interface navegacional, a ferramenta FTP, também poderá ser instalada, como demonstra no Quadro 13:

apt-get install proftpd

Quadro 13: Instalação FTP
Fonte: Imagem criada pelo próprio autor.

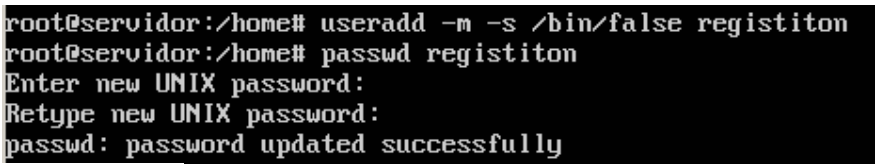


FIGURA 04: FTP
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Outra maneira para acessar esta ferramenta, é utilizando *browser* ou *softwares* de cliente *FTP*, como na Figura 05:

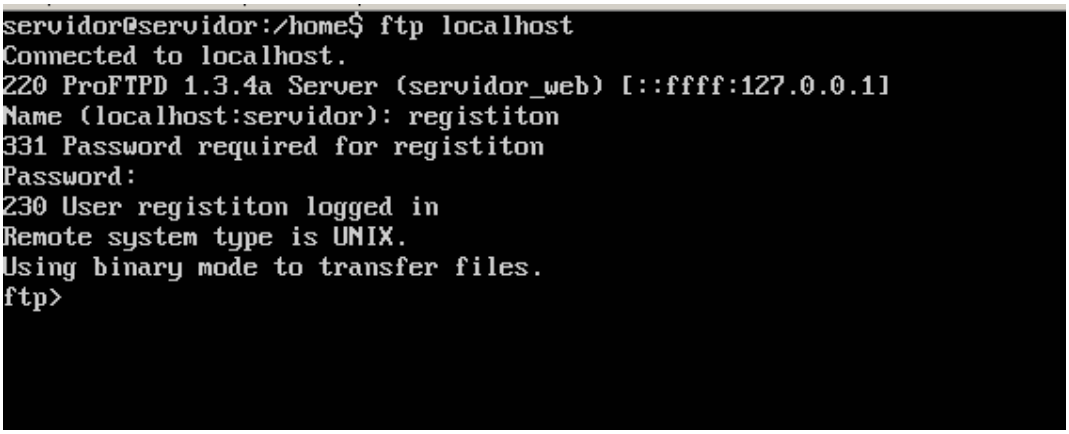


FIGURA 05: Softwares de cliente
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Ao falarmos de configuração ProFTPD, o seu arquivo de configuração. É importante observar, que as conexões ao servidor FTP não se torna possível, devido ao s*hell*, por isso se faz necessário alterações na configuração, como demonstra no Quadro 14:

Debian/Ubuntu: “/etc/proftpd/proftpd.conf”

Quadro 14: Configuração FTP
Fonte: Imagem criada pelo próprio autor.

```
#Nome do Servidor
ServerName “ servidor_web”
#Modo no qual rodará (standalone ou inetd)
ServerType standalone
DeferWelcome off
#Não exibe informações sobre que tipo de servidor está rodando
ServerIdent off
# Fuso horário universal (GMT) e não o local
TimesGMT off
MultilineRFC2228 on
#Tempo Máximo sem transferência de dados
TimeoutNoTransfer 600
#Tempo Máximo com transferência parada(travada)
TimeoutStalled 600
#Tempo Máximo conectado mas sem troca de dados
TimeoutIdle 1200
DisplayLogin welcome.msg
DisplayFirstChdir .message true
ListOptions "-l"
DenyFilter \*.*/
#Logs no Proftp
WtmpLog off
#Arquivo de log geral
SystemLog /var/log/proftpd.log
#Arquivo de log das transferências
TransferLog /var/log/xferlog
#Porta para socket de controle
Port 21
Umask 022 022
#Máximo de usuários autenticados
MaxClientes    4   # "Mensagem de erro para usuário"
#Numero Máximo de tentativas de login
MaxLoginAttempts 3
#Usuário sob qual o servidor irá rodar
User    proftpd
#Grupo
Group nogroup
#Os Usuários não poderão sair de seu diretório home
```

```
DefaultRoot ~
#Não permite o login do usuário root
RootLogin off
#Não requer que os usuários tenham um shell válido
RequireValidShell
off
#Não bloqueia usuários baseando-se no arquivo /etc/ftpusers
UseFtpUsers off
```

Quadro 15: Configuração FTP
Fonte: Imagem criada pelo próprio autor.

Após a realização das configurações, acima apresentadas é preciso restartar o sistema e fazer a nova leitura do arquivo.

```
# /etc/init.d/proftpd restart
```

Quadro 16: Configuração FTP
Fonte: Imagem criada pelo próprio autor.

Seguindo esta linha de pensamento, o *hardening* Apache, apresenta as seguintes configurações que devem ser alteradas, ao acessar o arquivo /etc/apache2/conf.d/security, como demonstra no Quadro 17:

DE	PARA
ServerToken Full *ServerSignature on* *TraceEnable on*	*ServerToken Prod* *ServerSignature off* *TraceEnable off*

Quadro 17: Configurações *hardening Apache*

A *ServerToken* é uma diretiva responsável por controlar o campo de cabeçalho de resposta do servidor, que é enviado de volta aos clientes, a qual inclui uma descrição genérica do tipo servidor, bem como informações sobre compilado em módulos.

A directiva *ServerSignature* permite a configuração de uma linha de rodapé no qual documentos gerados pelo servidor, por isso o modo OFF retira a linha de rodapé evitando de alguma informação seja repassada.

O *TraceEnable* é uma directiva, substitui o comportamento de rastreamento para o servidor núcleo e mod_proxy. *TraceEnable off* faz com que o servidor retorne uma mensagem de não permitido quando acessado pelo cliente.

Já os arquivos de configuração /etc/apache2/sites-available/, as alterações iniciam-se na configuração *Document*, como demonstrado na Quadro 18. Habilitando o server-status é o módulo de Status permite que um administrador de servidor para descobrir o quão bem o seu servidor está executando. Uma página HTML é apresentado que dá as estatísticas atuais do servidor , de forma facilmente legível, o qual é redimensionada, com o conteúdo do Quadro 18.

Order Deny,Allow
Deny from All
Options FollowSymLinks
AllowOverride None

<Location /server-status>
SetHandler server-status
Deny from all
Allow from localhost
</Location>

/etc/apache2/apache2.conf

Quadro 18: Configuração Apache
Fonte: Imagem criada pelo próprio autor.

Ao final, as configurações estão prontas para serem utilizadas e ligadas à quantidade de recursos, os quais se mostram disponíveis, como CPU, memória, banda, entre outras. A habilitação do SSL no Apache 2, seguem alguns passos necessários, desde a instalação de pacotes, criação de certificado até a sua reinicialização, como demonstrado a seguir no Quadro 19.

Instale os pacotes necessários

aptitude install openssl ssl-cert

Crie o certificado

openssl req $@ -new -x509 -days 365 -nodes -out /etc/apache2/apache.pem -keyout /etc/apache2/apache.pem

Defina a permissão para o arquivo criado

chmod 600 /etc/apache2/apache.pem

Edite o arquivo /etc/apache2/ports.conf e adicione a seguinte linha:

Listen 443

Habilite o suporte a SSL no apache2 da seguinte forma:

a2enmod ssl

Faça uma cópia do arquivo /etc/apache2/sites-available/default com o nome ssl.

cp /etc/apache2/sites-available/default /etc/apache2/sites-available/ssl

Faça um link simbólico para /etc/apache2/sites-enabled/

ln -s /etc/apache2/sites-available/ssl /etc/apache2/sites-enabled/

Edite o arquivo /etc/apache2/sites-available/ssl, adicionando as seguintes linhas:

*NameVirtualHost *:443*

ServerAdmin webmaster@localhost

CustomLog /var/log/apache2/access.log combined

SSLEngine on #Adicione esta linha

ServerSignature On

SSLCertificateFile /etc/apache2/apache.pem #Adicione esta linha

Reinicie o Apache

apache2ctl restart

Quadro 19: Habilitação SSL no Apache2
Fonte: Imagem criada pelo próprio autor.

Ao finalizarmos a interface navegacional no Sistema Linux, nos deparamos com o sistema Firewall, criando o arquivo ***/etc/init.d/firewall.sh,*** com a configuração, apresentada no Quadro 20.

```
#!/bin/bash

PATH=/bin:/usr/bin:/sbin:/usr/sbin
TCPOK="123 80 443″
UDPOK="53″

# Mudando as políticas para ACCEPT
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP

# Limpando as regras em memória
```

```
iptables -F -t filter
iptables -F -t mangle
iptables -F -t nat
iptables -X -t filter
iptables -X -t mangle
iptables -X -t nat
iptables -Z -t filter
iptables -Z -t mangle
iptables -Z -t nat

#Descarta pacotes nulo de entrada
iptables -A INPUT -p tcp –tcp-flags ALL NONE -j DROP

#Descarta pacotes XMAS
iptables -A INPUT -p tcp –tcp-flags ALL ALL -j DROP

#Proteção contra SynFlood
iptables -A INPUT -p tcp –syn -m limit –limit 1/s –limit-burst 3 -j RETURN

#Drop conexões de ping
iptables -A INPUT -p icmp –icmp-type echo-request -j DROP

iptables -A INPUT -j ACCEPT -i lo
iptables -A INPUT -j LOG -i ! lo -s 127.0.0.1/255.0.0.0
iptables -A INPUT -j DROP -i ! lo -s 127.0.0.1/255.0.0.0

iptables -A OUTPUT -j ACCEPT -o lo

# Permite ssh na porta 22
iptables -A INPUT -s 0.0.0.0 -p tcp –dport 22 -j ACCEPT

# Bloqueio do Telnet
$iptables –A INPUT –tcp –sport 23 –j drop
$iptables –A FORWARD –I $inet –p tcp –sport 23 –j DROP
$iptables –A FORWARD –o $inet –p tcp –dport 23 –j DROP


# Permite acesso a algumas portas
for PORTA in $TCPOK
do
  iptables -A INPUT -p tcp –dport $PORTA -j ACCEPT
done

# Permite acesso algumas portas UDP
for PORTA in $UDPOK
do
   iptables -A INPUT -p udp –dport $PORTA -j ACCEPT
done

# Verifica estado das conexões portas
```

iptables -A INPUT -m state –state ! ESTABLISHED,RELATED -j DROP iptables -A FORWARD -m state –state ESTABLISHED,RELATED -j ACCEPT # Proteção contra PortScan Iptables –A INPUT –p tcp –tcp-flags SYN,ACK,FIN,RST RST –m limit –limit 5/m –j ACCEPT

Quadro 20: Habilitação
Fonte: Imagem criada pelo próprio autor.

Finalizado tais habilitações, faz-se necessário, a inicialização do sistema, pelo script, update-rc.d firewall.sh defaults.

4.2 Interface navegacional no sistema Windows

A interface navegacional no Sistema Windows, apresenta algumas particularidades, sendo necessária a instalação do assistente de configuração de segurança. Para tal função é necessário, ir ao comando Adicionar e remover os componentes do Windows os quais detectar portas e serviços, e configurar as definições de registro e auditoria de acordo com a função do servidor. Como demonstrado no Quadro 21 e Figura 06:

Desabilite serviços desnecessários com base na função de servidor	Remova às regras de firewall não utilizadas e limite as regras de firewall existentes.	Definir políticas de auditoria restritas.
Para a configuração segue as seguintes etapas: **Iniciar → Ferramentas Administrativas → Assistente de Configuração de Segurança.**		

Quadro 21: Configurações *Windows*

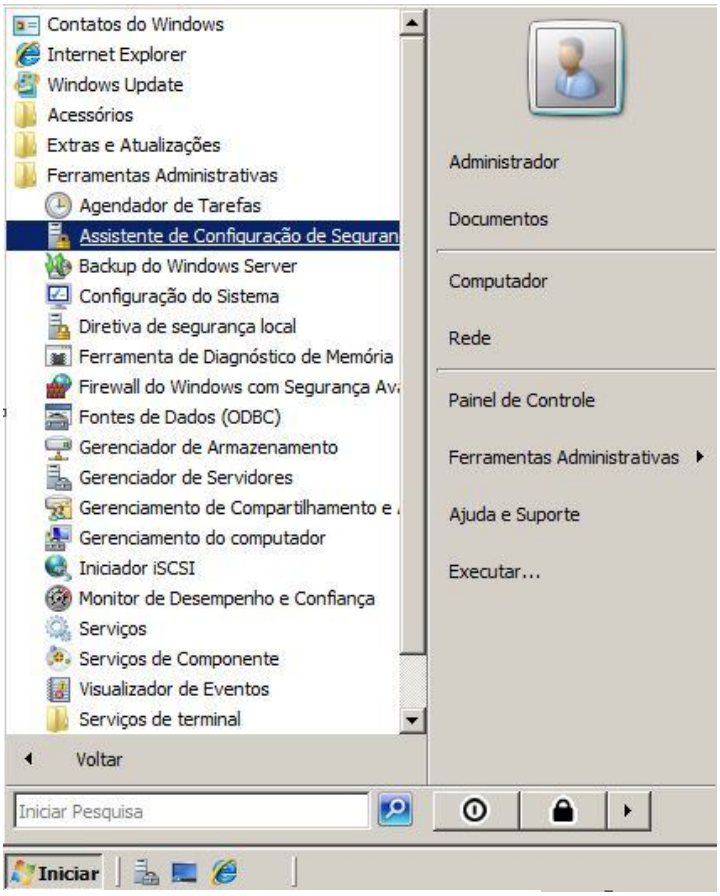


FIGURA 06:Assistente de configuração de segurança
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Ao desativar ou excluir as contas de segurança desnecessárias, muitos ataques ao sistema operacional podem ser evitados. Durante a instalação, por padrão, o administrador, convidado e assistente de ajuda é criado. Ambos visitantes ajudam contas e assistente devem ser desativados em todos os momentos. Como demonstrado no Quadro 22 e Figura 07:

Iniciar -> Programas -> Ferramentas Administrativas -> Gerenciador de Servidores -> Usuários e Grupos Locais -> Usuários Botão direito do mouse sobre o usuário -> Propriedades -> seleção para a conta está desativada

Quadro 22: Gerenciador de Servidores

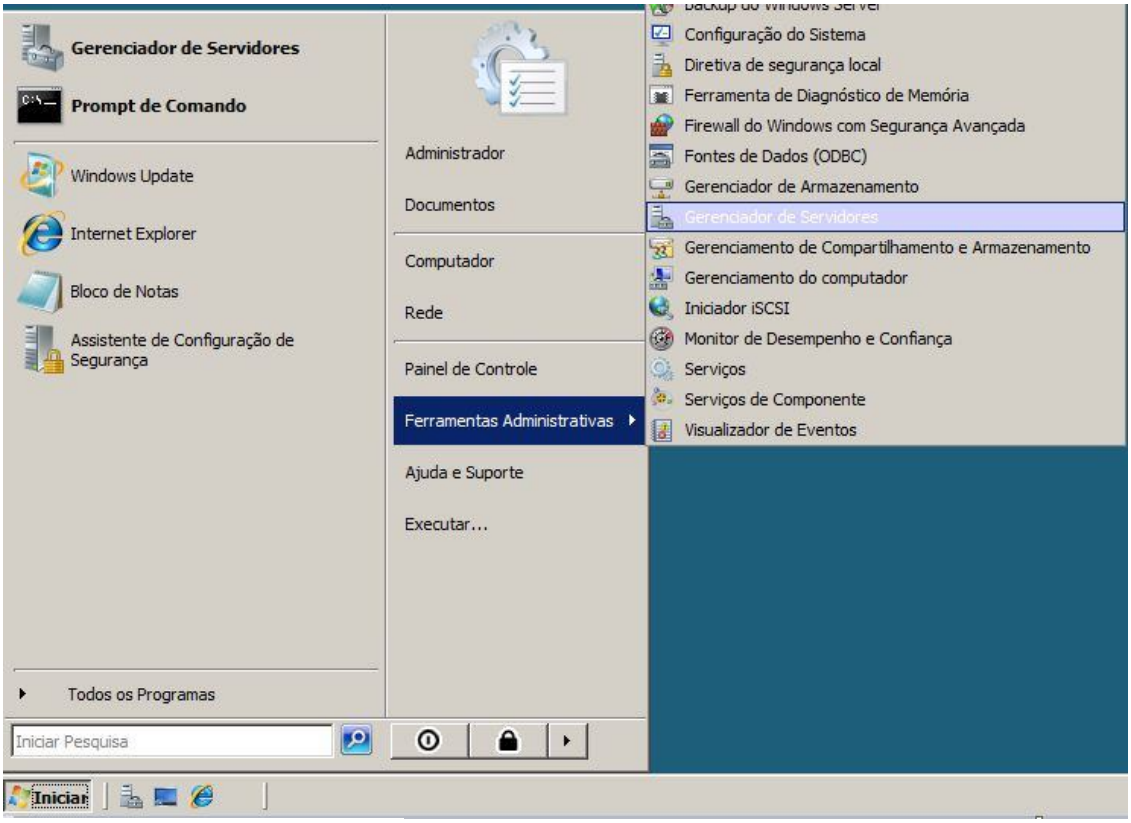


FIGURA 07: Gerenciador de servidores
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

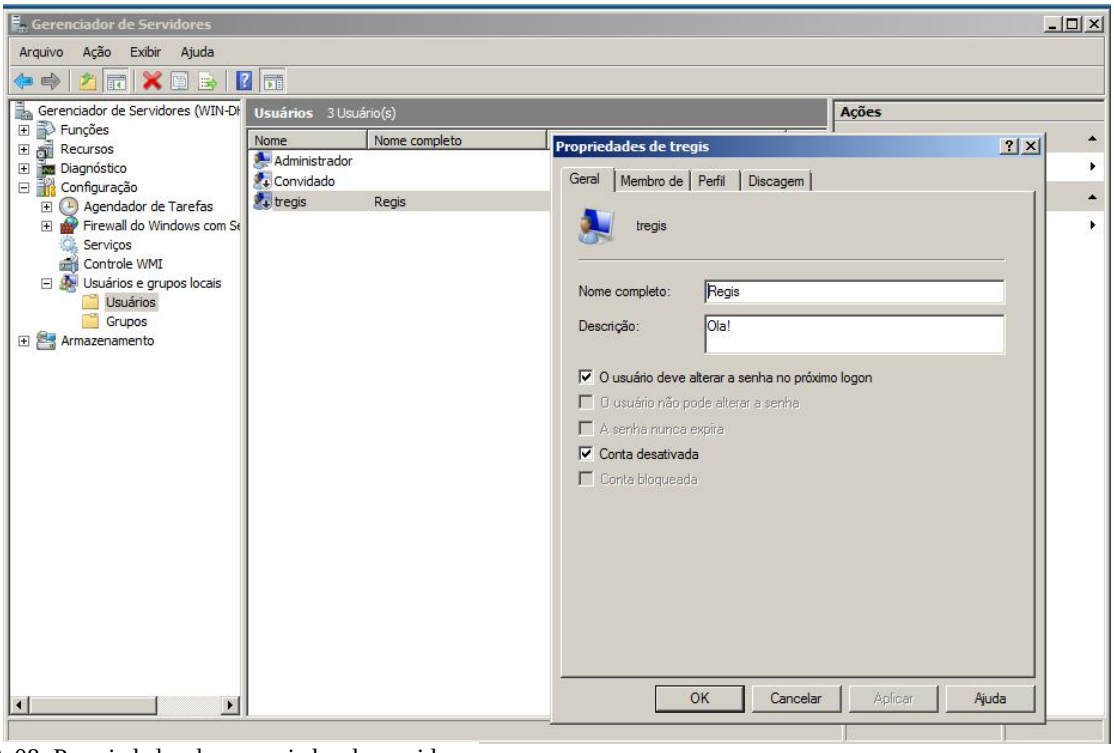


FIGURA 08: Propriedades do gerenciador de servidores
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Deve-se ser ter em mente é o número de aplicativos instalado nos servidores, sendo este um papel relacionado. Vale ressaltar que esses aplicativos devem ser testados antes de sua implantação na rede, pois os mesmos podem fazer uso de *backdoores*, de por sua vez podem comprometer a segurança do servidor.

O Belarc Advisor exibe o *software* e *hardware* instalado, faltando patches de correções, antivírus estado. É livre de custos e pode ser utilizado para uso pessoal, incluindo muitos mais recursos para o gerenciamento de segurança em vários computadores.

Para desinstalar o aplicativo desnecessário:
Vá em Iniciar -> Programas -> Ferramentas Administrativas -> Server Manager -> Funções -> clique em Remover papéis

Quadro 23: Desistalar aplicativo desnecessário

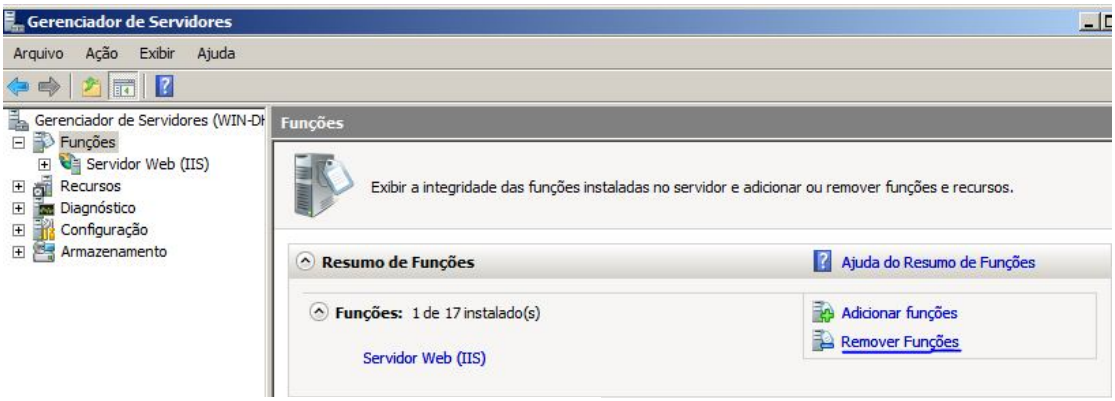


FIGURA 09: Resumo de funções gerenciador de servidores
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Já a configuração do *firewall* no Windows 2008, encontra-se com a denominação *Firewall* do *Windows* com o *Advanced* Segurança. Como uma prática recomendada de segurança, todos os servidores devem ter o seu próprio *firewall* baseado em *host*. Bidirecional *firewall*, que filtra o tráfego de saída, bem como o tráfego de entrada. IPSEC configurações de criptografia são integrados em uma única interface.

Usando as regras avançadas podem-se construir as regras de *firewall* utilizando o *Windows Active Directory* objetos, fonte e destino endereços IP e protocolos.

Para realizar tal configuração é necessário seguir alguns passos, como demonstrado no Quadro 24 e nas Figuras 10,11,12:

Iniciar -> Painel de Controle -> Firewall do Windows -> Alterar Configurações

Quadro 24: Configurar Firewall

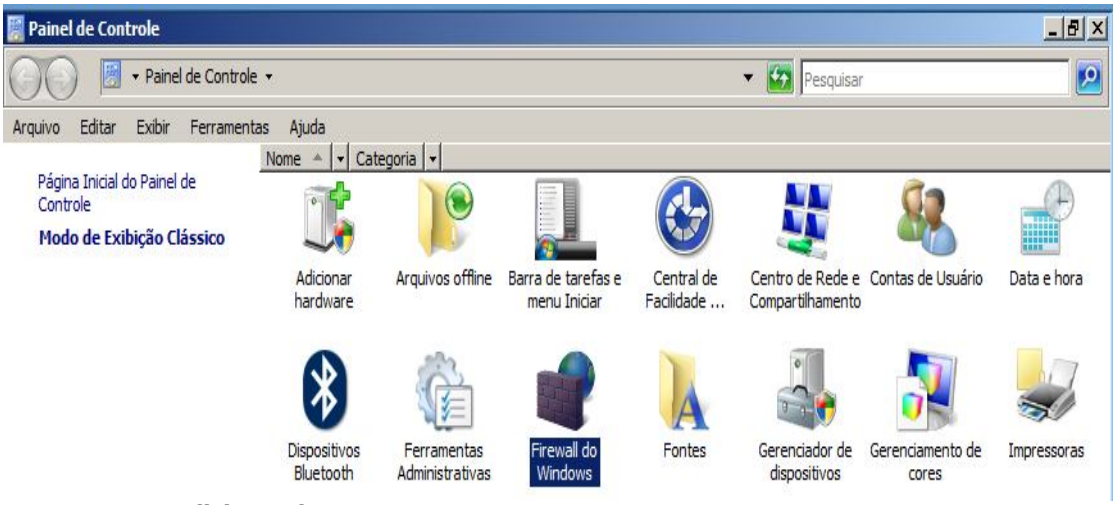


FIGURA 10: Firewall do Windows
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

FIGURA 11: Alteração da configuração
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

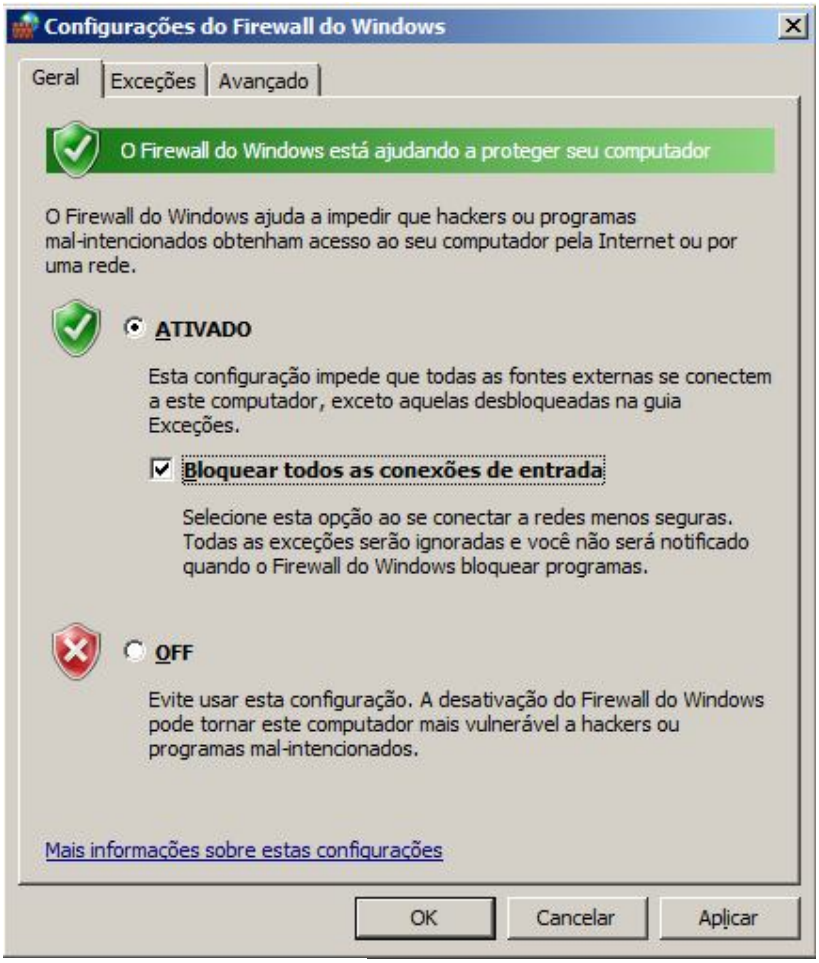


FIGURA 12: Configuração Firewall
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

A respeito das configurações para auditoria, se faz imprescindível o registro e editarão dos seguintes arquivos:

- Acesso ao serviço de diretório de auditoria;
- Acompanhamento de processos de auditoria;
- Auditoria de acesso a objetos;
- Auditoria de alteração de diretivas;
- Auditoria de eventos de sistema;
- Auditoria de uso de privilégio;
- Eventos de logon de auditoria;
- Eventos de logon de conta de auditoria;
- Gerenciamento de conta de auditoria;

Realizando as etapas de configuração, como demonstrado no Quadro 25:

Iniciar → Painel de Controle → Directivas Segurança Local → Diretivas Locais → Diretivas de auditoria

QUADRO 25: Diretiva Auditoria

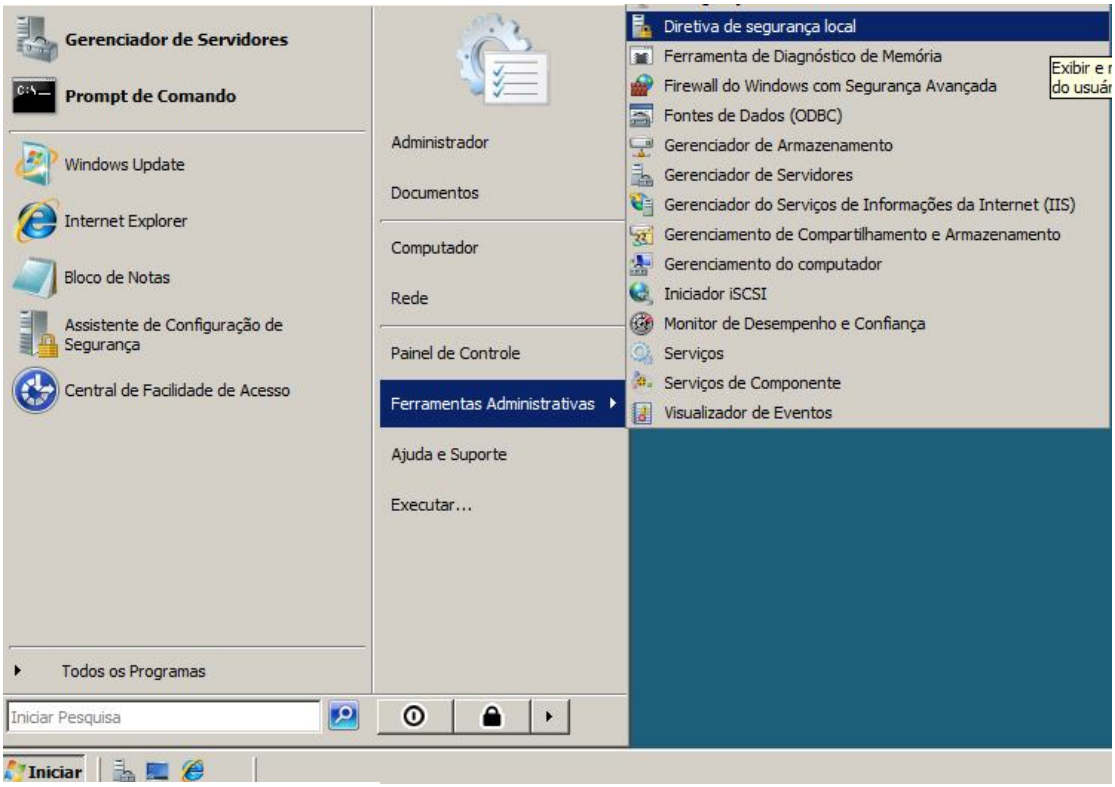


FIGURA 13: Configuração Auditoria
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

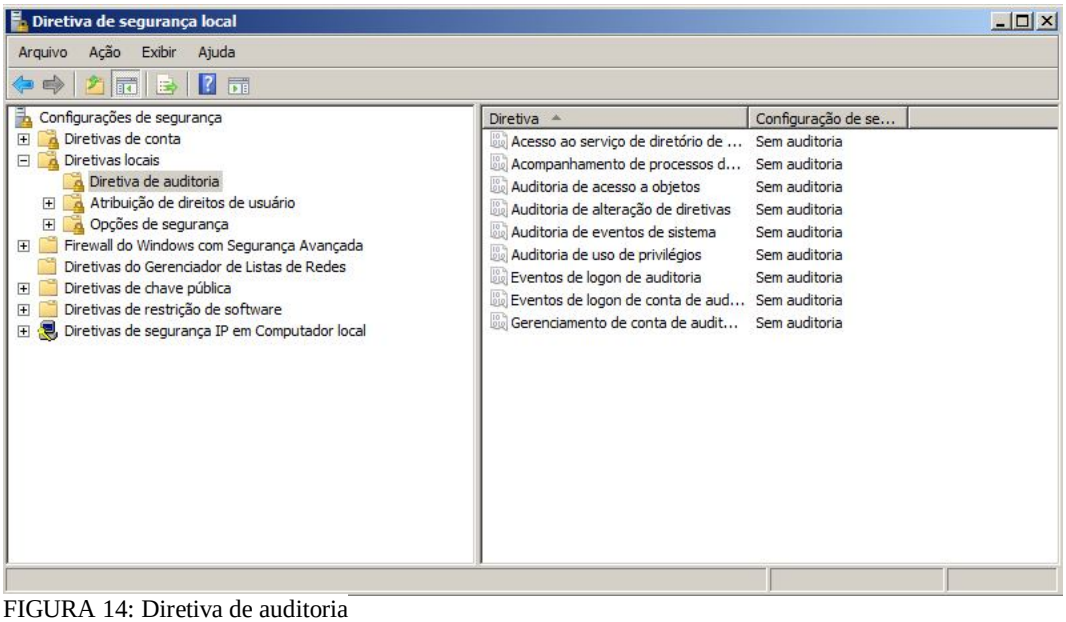


FIGURA 14: Diretiva de auditoria
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Windows Server 2008 tem a possibilidade de se trabalhar com um ambiente mais seguro. Conforme podemos observar nas figuras abaixo, temos a apresentação de telas de gerenciamento desta ferramenta, elas são divididas em três colunas, sendo que a primeira nos mostra as subcategorias existentes dentro do gerenciamento da ferramenta.

Existem dois tipos de regras, as de *inbound* (entrada) e *outbound* (saída), isso faz com que possamos ter maior controle do tráfego que entra e sai do *Windows*. As regras já criadas e as instituídas de forma personalizada estarão sendo mostradas da mesma forma.

Há uma diferenciação de cores entre as regras. Temos regras que estão em verde e as que estão em cinza, as que estão em verde são regras que estão ativas no momento e as regras que estão em cinza estão desabilitadas, ou seja, que suas configurações não estão sendo aplicadas. A última coluna é a coluna das ações que podem ser realizadas dentre as informações exibidas nas colunas anteriores.

No caso do exemplo abaixo é possível criar novas regras e fazer filtros de amostragem.

Iniciar -> Programas -> Ferramentas Administrativas -> Firewall do Windows com Segurança Avançada

Quadro 26: Regras e filtros de amostragem

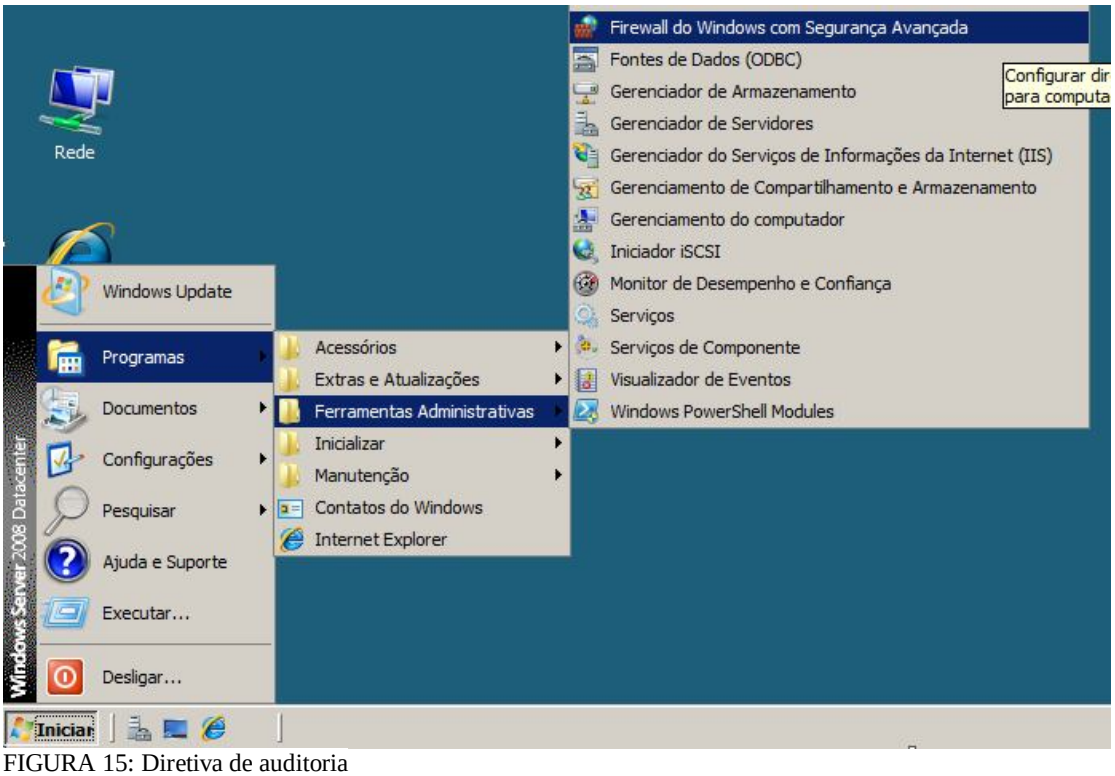


FIGURA 15: Diretiva de auditoria
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Assim nas figuras abaixo iremos demonstrar a configuração de regras necessárias para cada servidor.

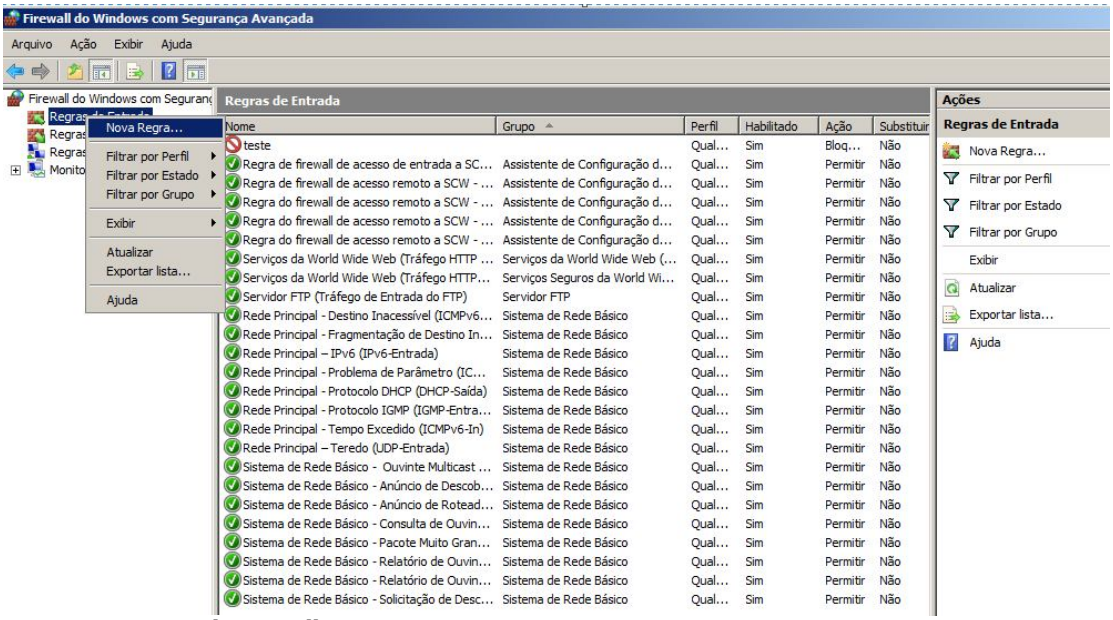


FIGURA 16: Regra de Firewall
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

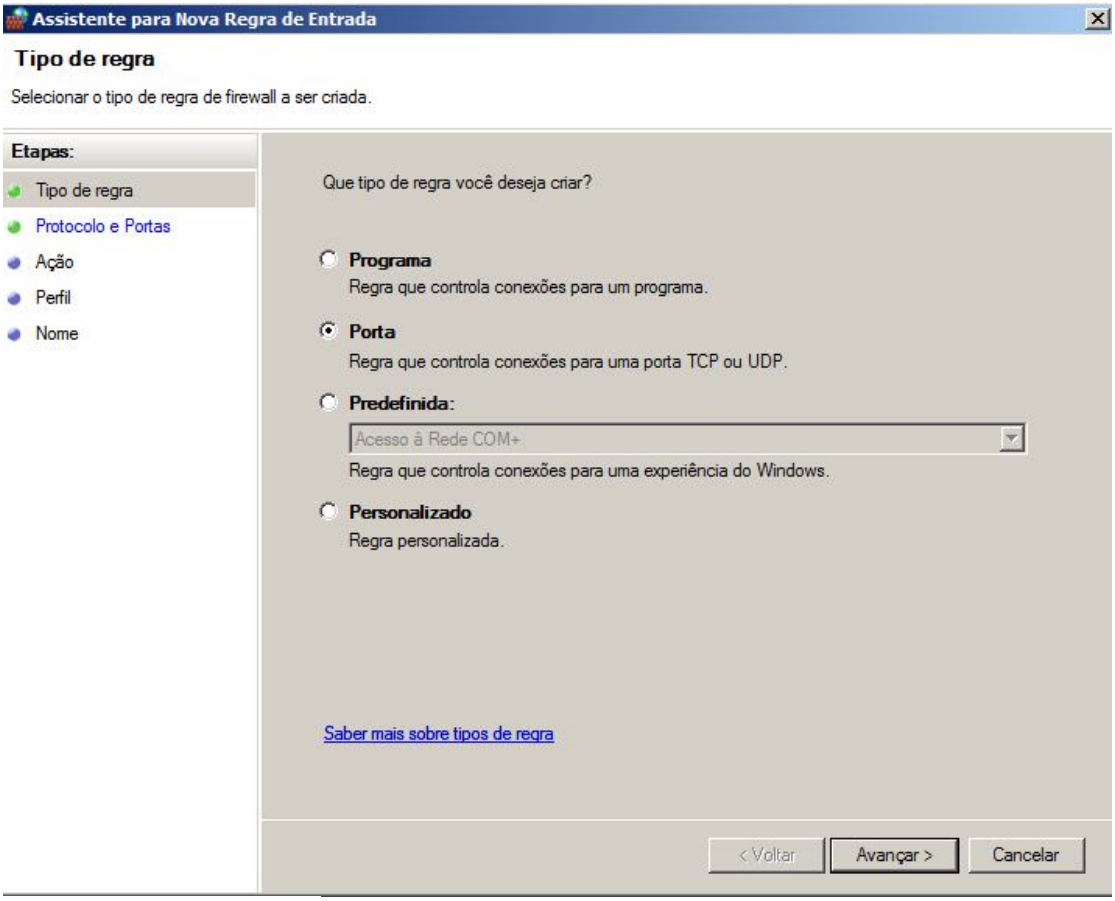


FIGURA 17: Regra de Firewall
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

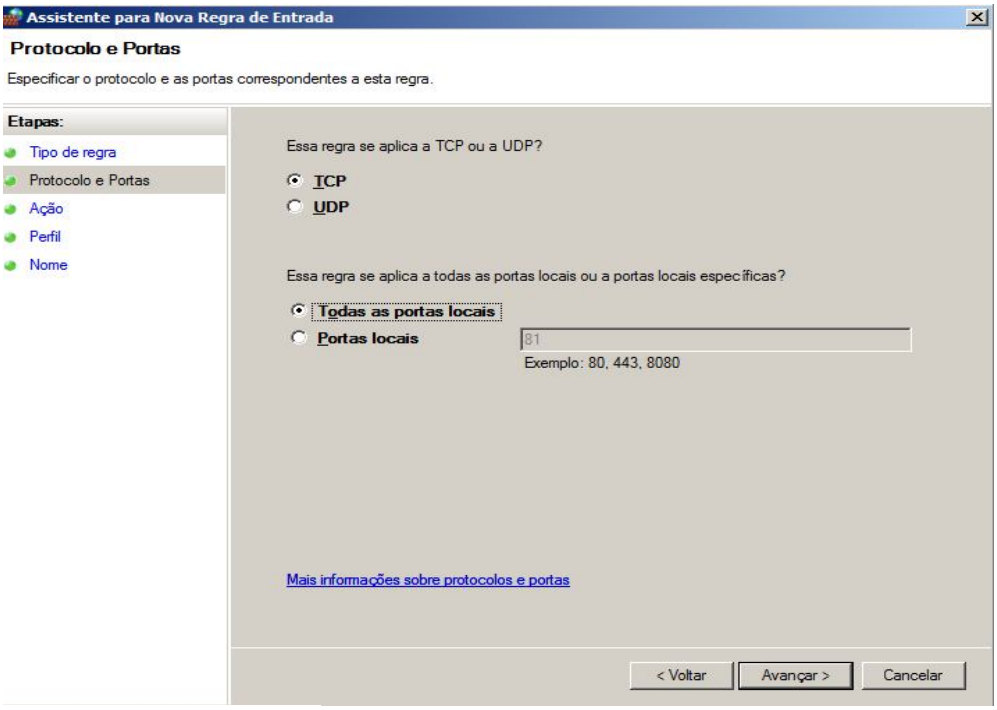


FIGURA 18: Regra de Firewall
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

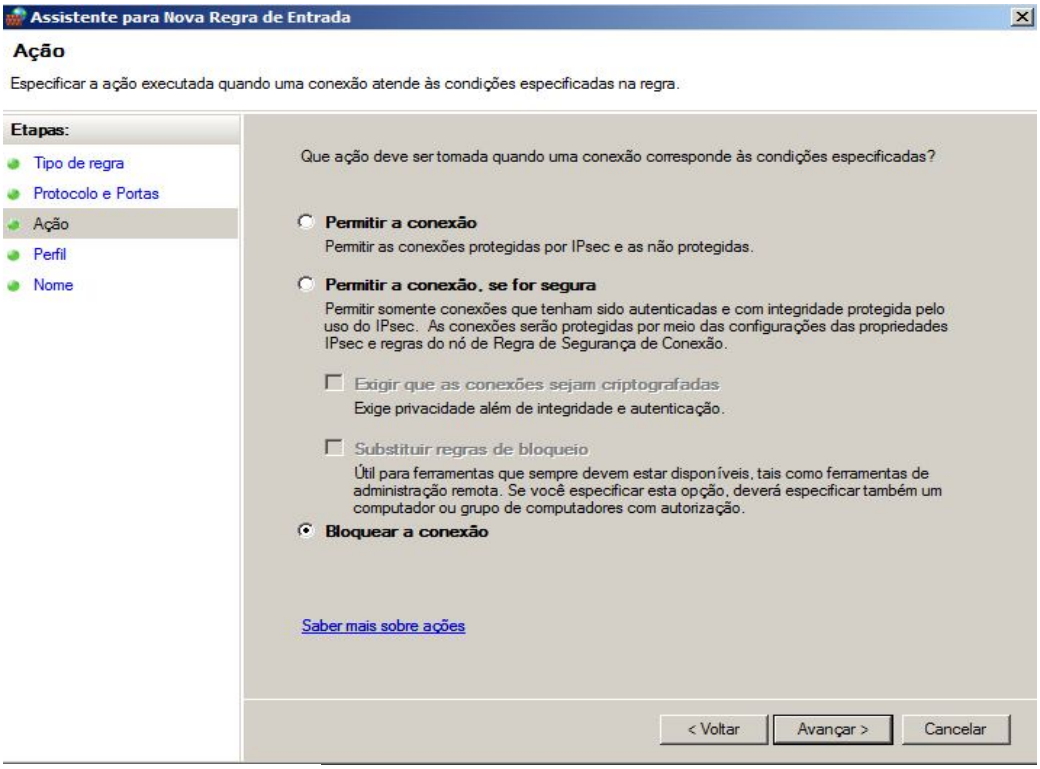


FIGURA 19: Regra de Firewall
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

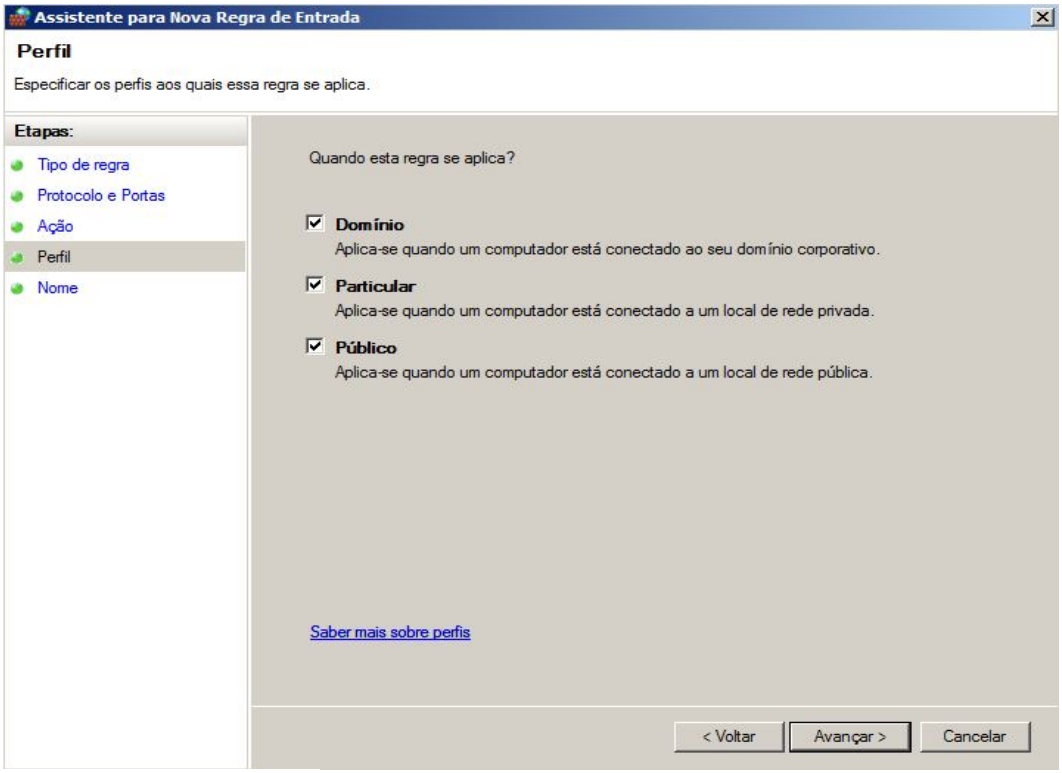


FIGURA 20: Regra de Firewall
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

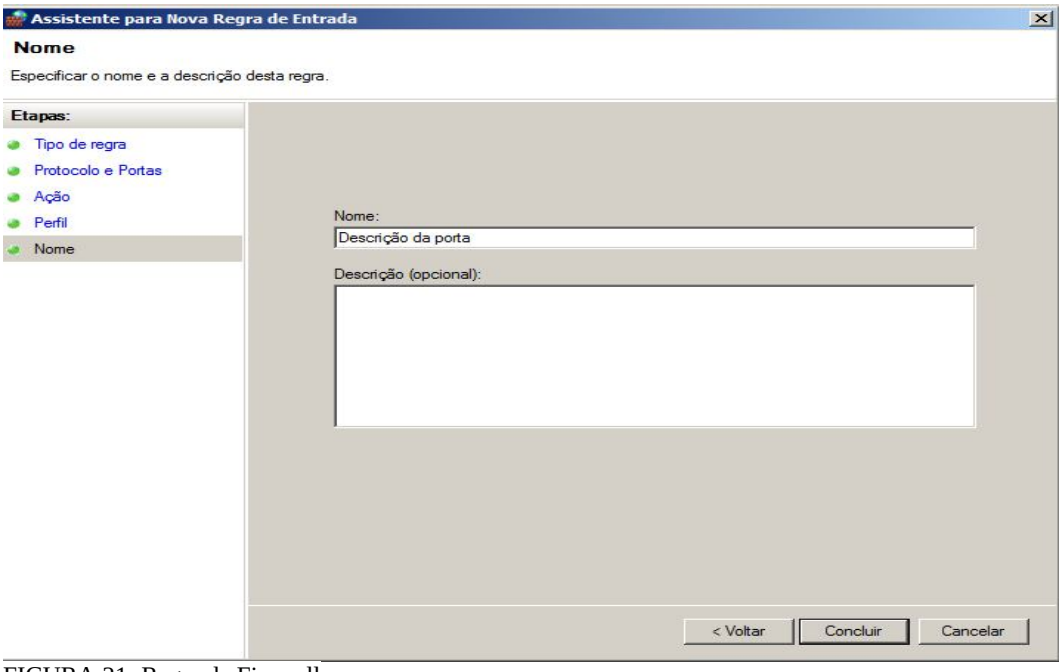


FIGURA 21: Regra de Firewall
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

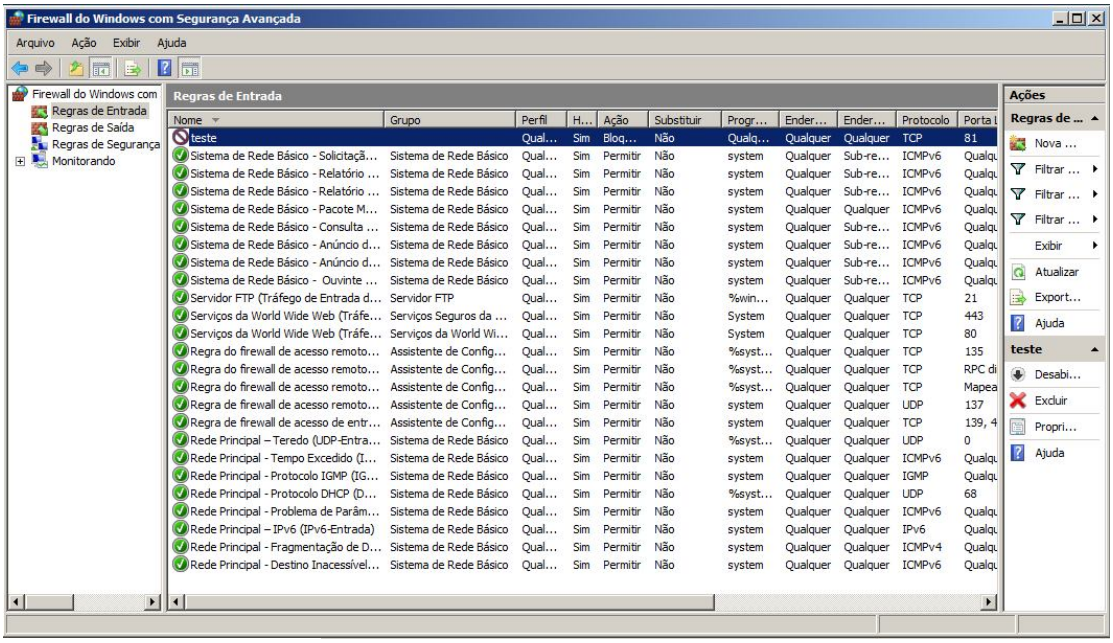


FIGURA 22: Regra de Firewall
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Outro padrão de configuração é a Criptografia. Sendo esta responsável pela informação sensível hospedeiro, para fazer uso do sistema de encriptação. O *Windows* fornece um recurso de criptografia de disco inteiro, denominado *Drive Encryption BitLocker* (*BitLocker*), o qual objetiva proteger o sistema operacional e os dados de armazenamento no disco. Para instalar o *BitLocker*, selecione-o no Gerenciador de Servidores ou digite: C: \ ServerManagerCmd-install BitLocker-restart, em um prompt de comando:

Para realizar tal configuração, segue-se os seguintes passos:

Iniciar -> Programas -> Ferramentas Administrativas -> Gerenciador do Servidor -> Resumo dos Recursos -> Bit Locker **Obs.** Ela só será acessada quando o Active Directory é instalado no Windows Server 2008

Quadro 27: Configuração de encriptação

Sobre as atualizações e patches, estes são elementos-chave para o endurecimento de um servidor. O sistema e segurança devem ser de constante atualização, sendo que os administradores devem verificar periodicamente sites do fornecedor para atualizações. *Windows Server Update Services* (WSUS) fornece um serviço de atualização de software para

o *Microsoft Windows* e outros softwares da *Microsoft*. Como demonstrado no Quadro 28 e na Figura 22:

Iniciar -> Windows Update (Certifique-se de Atualizações Automáticas está ligado)

Quadro 28: Atualização de Softwere

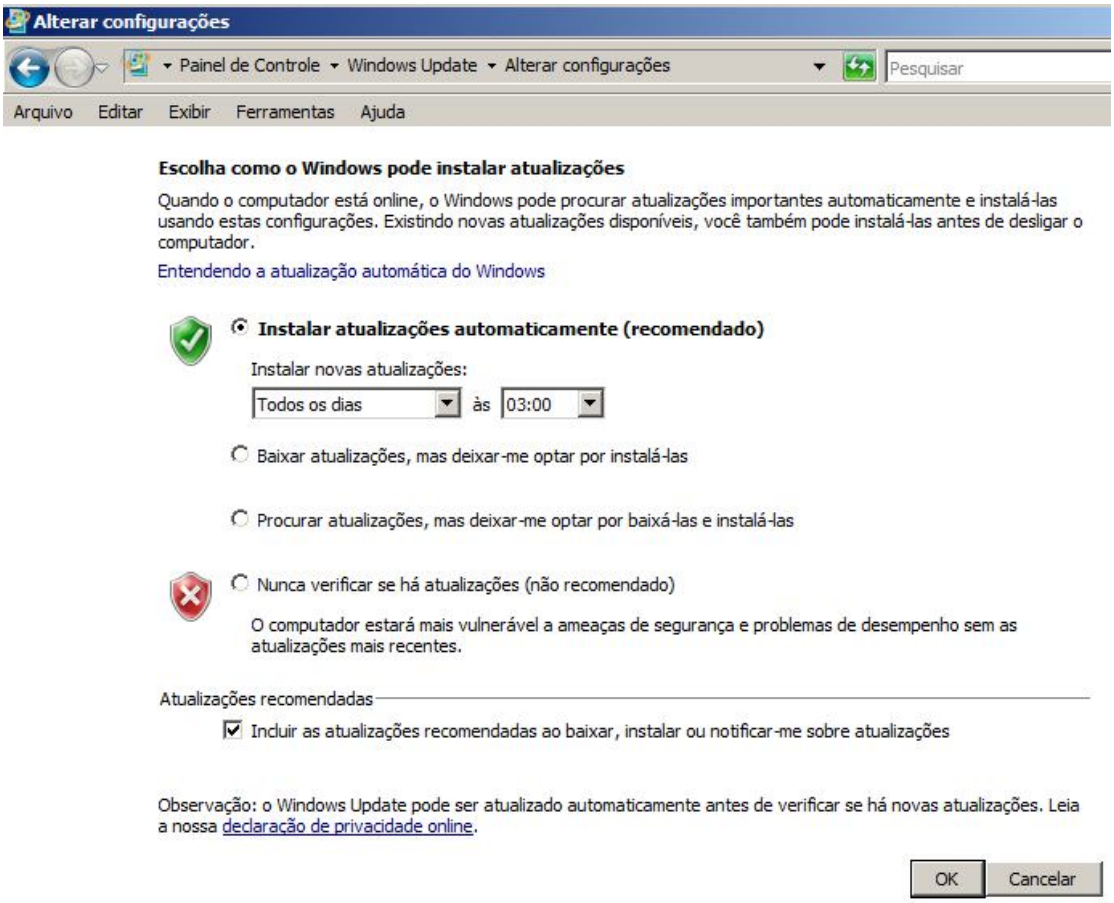


FIGURA 23: Atualização do Windows
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Sobre o *software* Anti-Virus, sendo esse um dos passos básicos e fundamentais para o fortalecimento de um servidor. *Windows Server* 2008 vem com um *Network Access Protection* (NAP), que ajuda a defesa contra vírus se espalhe para fora da rede. Utilizando de um conjunto de políticas que limpa as máquinas afetadas e quando elas são saudáveis, permitindo o acesso a partes da rede de produção.

O NAP consiste em uma tecnologia que digitaliza e identifica máquinas que não possuem as últimas assinaturas de vírus, *service packs* ou *patches* de segurança. A esse respeito faz-se a atualização do antivirus pelo endereço: http://www.microsoft.com/security/default.aspx.

A maioria das ameaças de segurança são, muitas vezes, causadas por altos privilégios, passado para usuários da conta. O servidor não deve ser configurado usando o *Enterprise* contas de administrador de largura. O *Script Logic Cload* é um produto que aumenta o sistema de arquivos do *Windows* NT (NTFS), com isso fornecendo maior segurança, auditorias mais precisas. Para termos mais segurança, devemos baixar o programa *Script Logic Cload* e instalar em seu servidor *Windows* 2008, com isso o sistema de arquivos estará mais seguro.

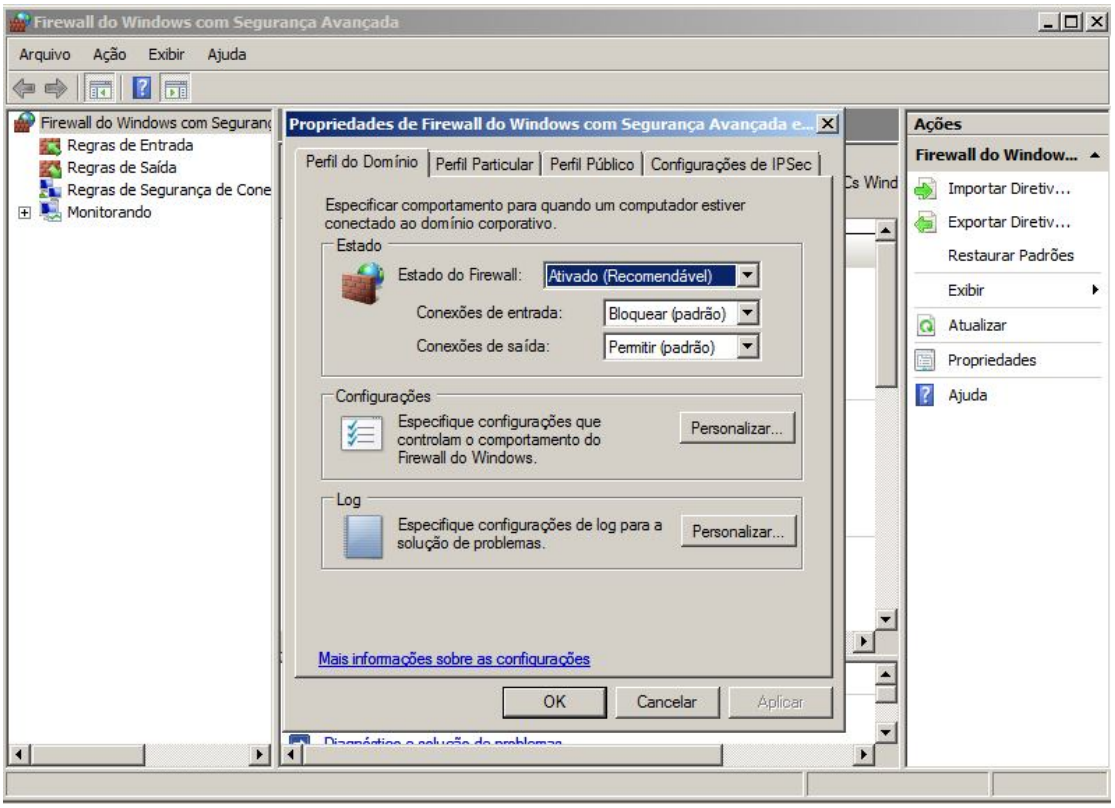


FIGURA 24: Segurança avançada
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Para desativar alguns serviços configurados na inicialização do servidor, é preciso realizar algumas etapas, como as descritas na tabela abaixo.

Iniciar -> Executar -> services.msc -> Desativar serviços desnecessários

Quadro 29: Desativar serviço desnecessários

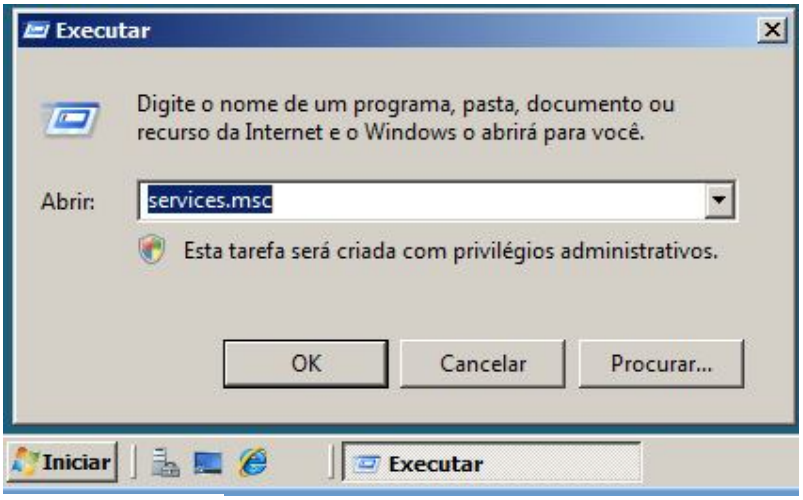


FIGURA 25:Executar
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

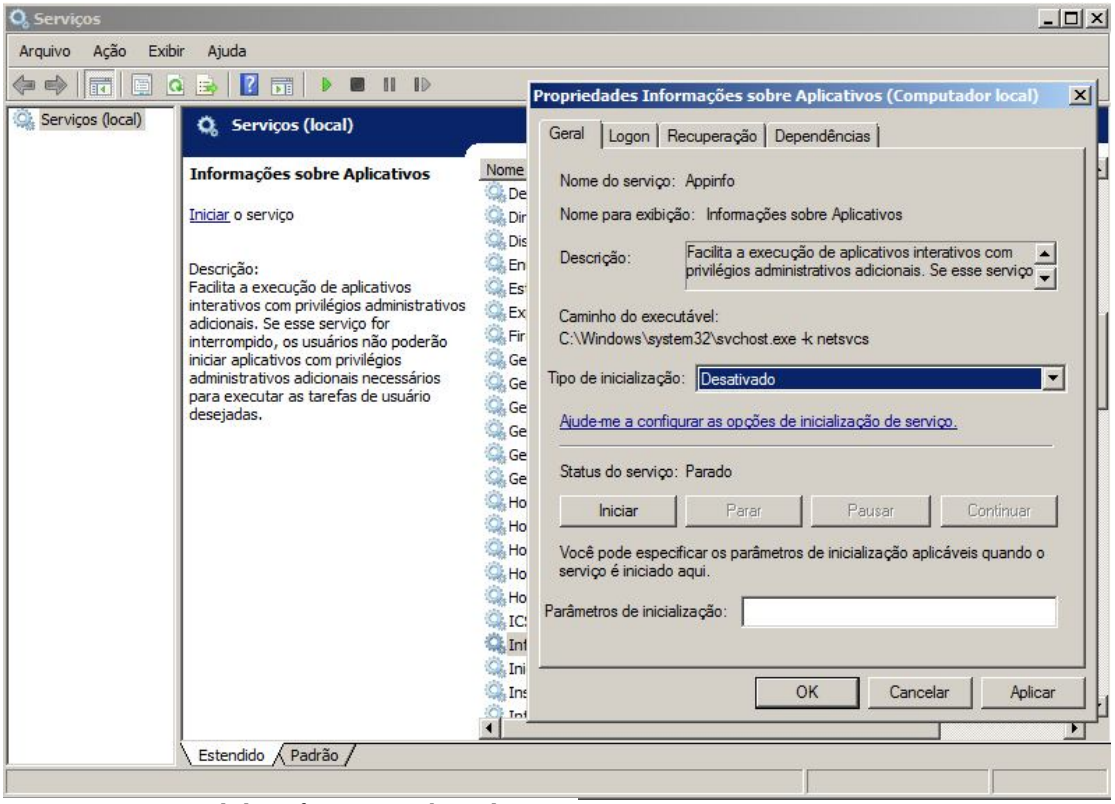


FIGURA 26: Propriedades informações sobre aplicativos
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Ao desativar o registro remoto, serviço este que permite o acesso de registro para usuários remotos autenticados. Mesmo ao ser bloqueado pelo *firewall* e ACLs, este serviço deve ser desligado, caso não se tenha nenhuma razão para permitir remoto acesso ao registro. Para realizar tal atividade segue-se a seguinte etapa:

Iniciar -> Painel de Controle -> Firewall do Windows -> ON

Quadro 30: Ativação Firewall

Vale ressaltar, que caso o usuário possua uma rede corporativa, os seguintes passos devem ser seguidos.

Clique em Iniciar - Executar -> digite "regedit" e pressione enter -> Navegue até HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Control \ SecureP ipeServers \ Selecione "winreg" Clique em Editar, selecione "Permissões" Selecione os usuários / grupos e permissões apropriadas como "Read" ou "controle total" apropriados. Clique em OK e sair.

Quadro 31: Configuração Winreg

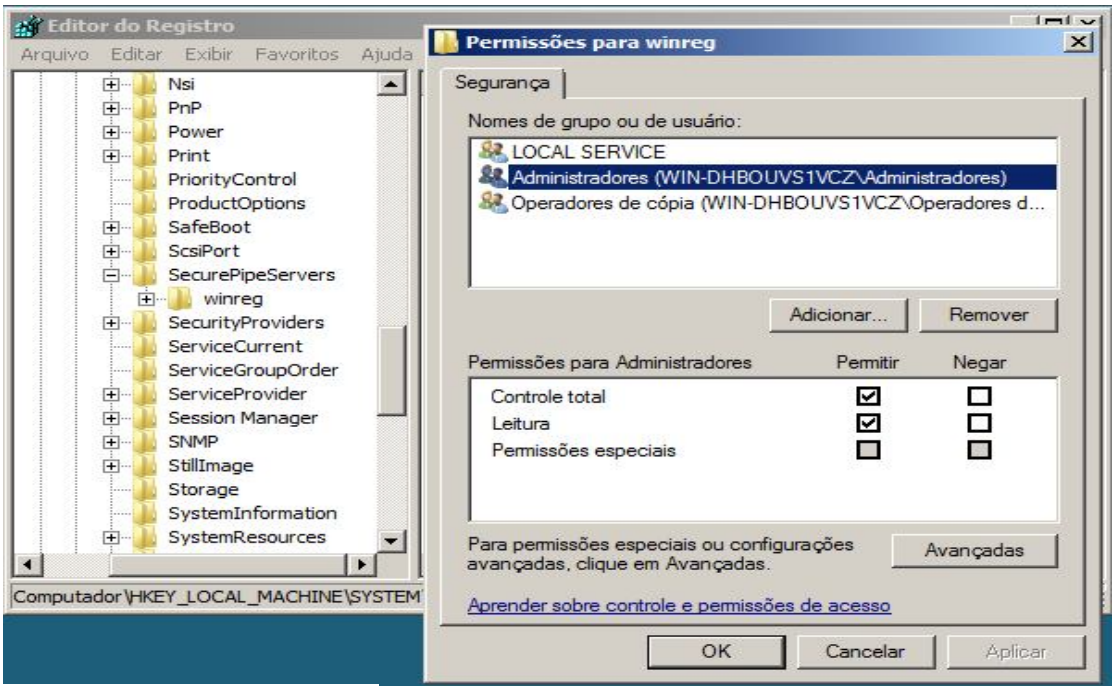


FIGURA 27: Permissões para winreg
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

O *Windows Error Reporting* (WER) é um conjunto de tecnologias do Windows que capturar o software de dados e suporte de relatórios de informações de falha do usuário final. Através de serviços *Winqual*, software e fornecedores de *hardware* podem acessar relatórios, a fim de analisar e responder a esses problemas. WER tecnologias são implementadas no Windows XP, Windows Server 2003, entre outros.

Vá para: Iniciar -> Programas -> Ferramentas Administrativas -> Gerenciador de servidor -> Configuração -> Usuários e grupos locais.

Quadro 32: Configurar WER

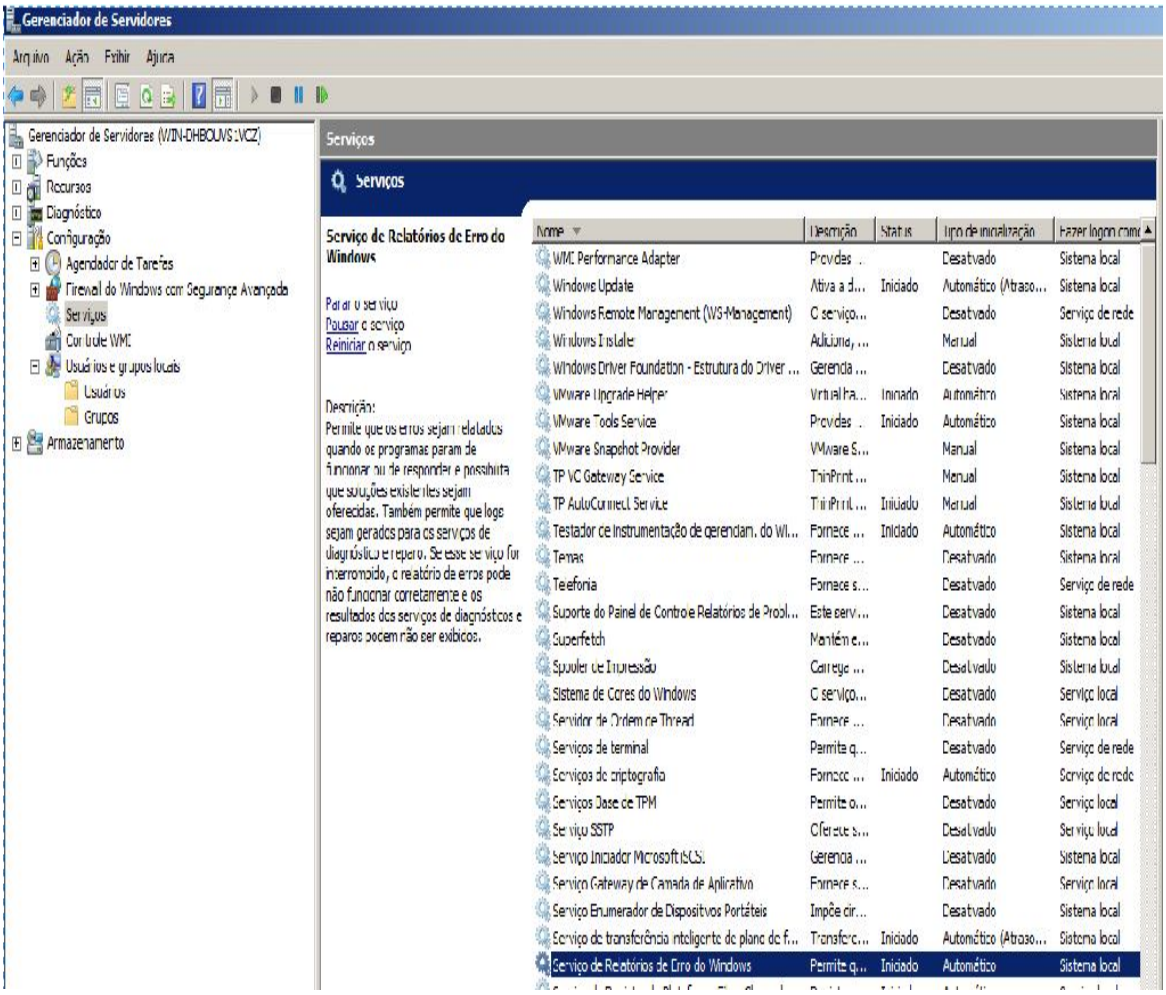


FIGURA 28: Serviços
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

À respeito da habilitação do serviço de gerenciamento *Web*, seu principal objetivo é obter um sentido para os negócios desta tecnologia e conduzir suas estratégias com base nisso. Para esta habilitação do Serviço de Gerenciamento da *Web*.

Iniciar → Programas → Ferramentas Administrativas → Gerenciado de Servidor → Funções.

Quadro 33: Habilitar Gerenciador Web

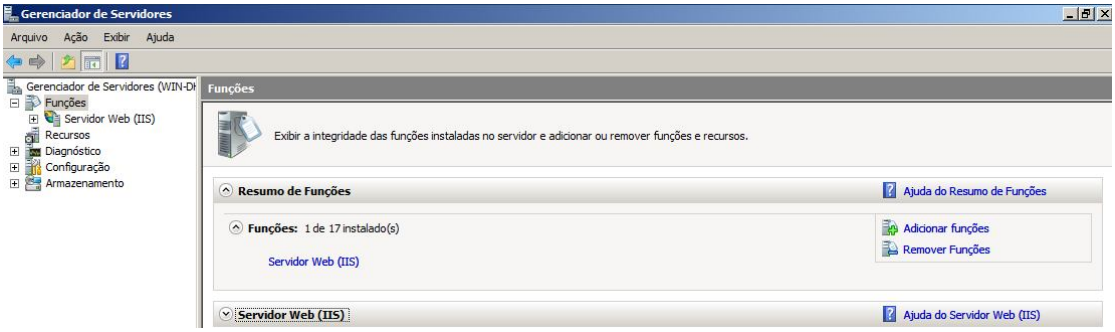


FIGURA 29: Gerenciador de servidores
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

A atualização do protocolo SSTP - *Serviço de Secure Socket*, para conectar computadores remotos, usando VPN. Se este serviço for desativado, os usuários não serão capazes de usar SSTP para acesso remoto servidores. O SSTP permite o tráfego de passar por *firewalls* que bloqueiam PPTP e L2TP/IPsec tráfego. Ele encapsula o tráfego PPP sobre o canal SSL do protocolo HTTPS (porta 443). Ele permite que os clientes por trás de *firewalls* e roteadores NAT para se conectar ao servidor VPN, sem a preocupação com a típica port problemas de bloqueio.

Para utilizar o serviço SSTP, segue a seguinte configuração:

Iniciar -> Executar -> services.msc -> Serviço SSTP

Quadro 34: Configurar SSTP

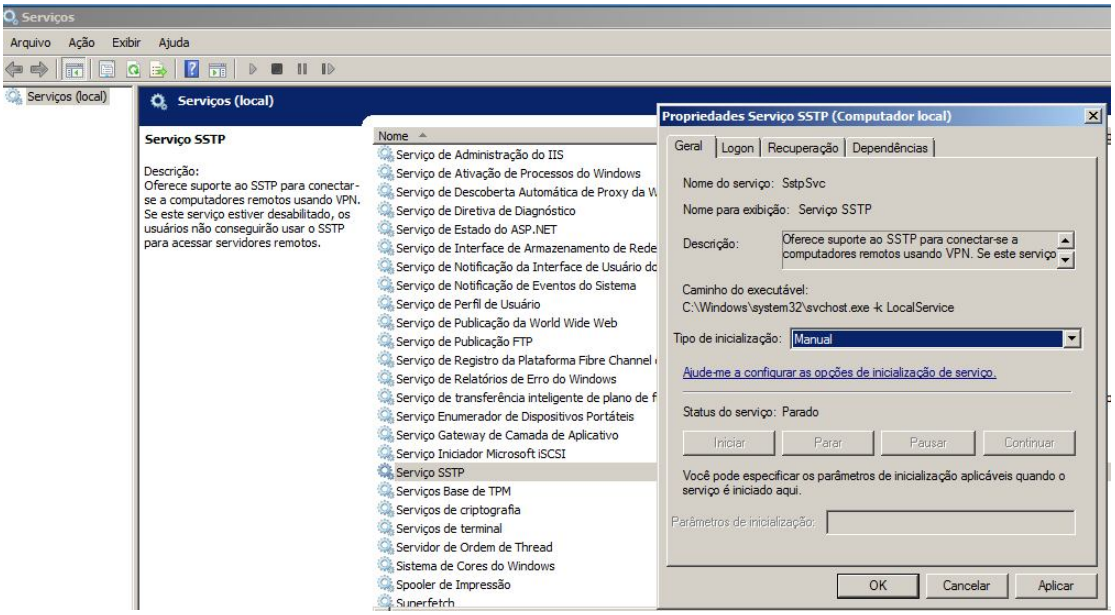


FIGURA 30: Propriedades SSTP
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Frente à ativação do *Login* de Rede, mantemos um canal entre o computador e o controlador de domínio. As lojas de sub-chave *logon,* informações para o *log-on* Net serviço, verifica se *log-on* pedidos e o registrador autentica, localizando controladores de domínio. Além disso, para manter a compatibilidade com versões anteriores, *Log-on Net* gerencia a replicação do banco de dados da conta do usuário para fazer *backup* de controladores de domínio executando o Windows NT 4.0 e versões anteriores.

Para a sua habilitação vá para:

Iniciar -> Executar -> services.msc -> Logon de rede -> Automatic

Quadro 35: Ativação Login de Redes

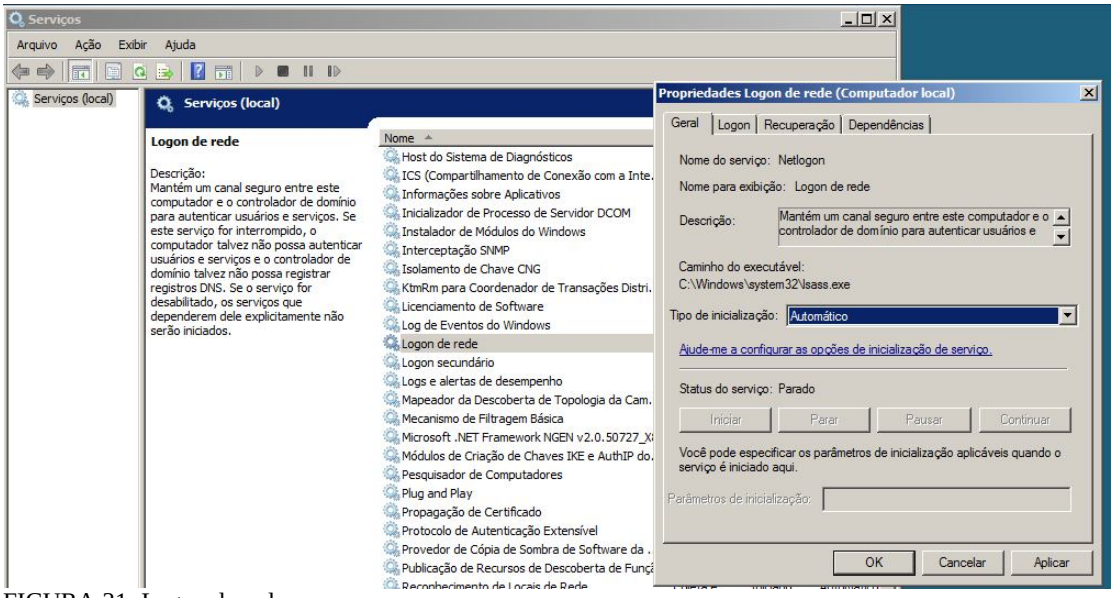


FIGURA 31: Logon de rede
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

A Administração Especial *Console Helper*, permite que os administradores acessem remotamente um prompt de comando. O Console de Administração Especial (SAC) pode se conectar a uma máquina, onde este serviço está sendo executado. No caso do *Windows* na máquina para de funcionar devido a um erro de parada mensagem.

O SAC é um ambiente de linha de comando auxiliar *Emergency Management Services* com as seguintes funções principais:

• Redirecionamento de erro de parada mensagem de texto explicativo.

• Reinicie o sistema.

• Obter informações de identificação do computador.

Para ativar o mesmo, segue os seguintes passos:

Iniciar -> Executar -> services.msc -> especial do console de administração helper -> automático

Quadro 36: Configuração SAC

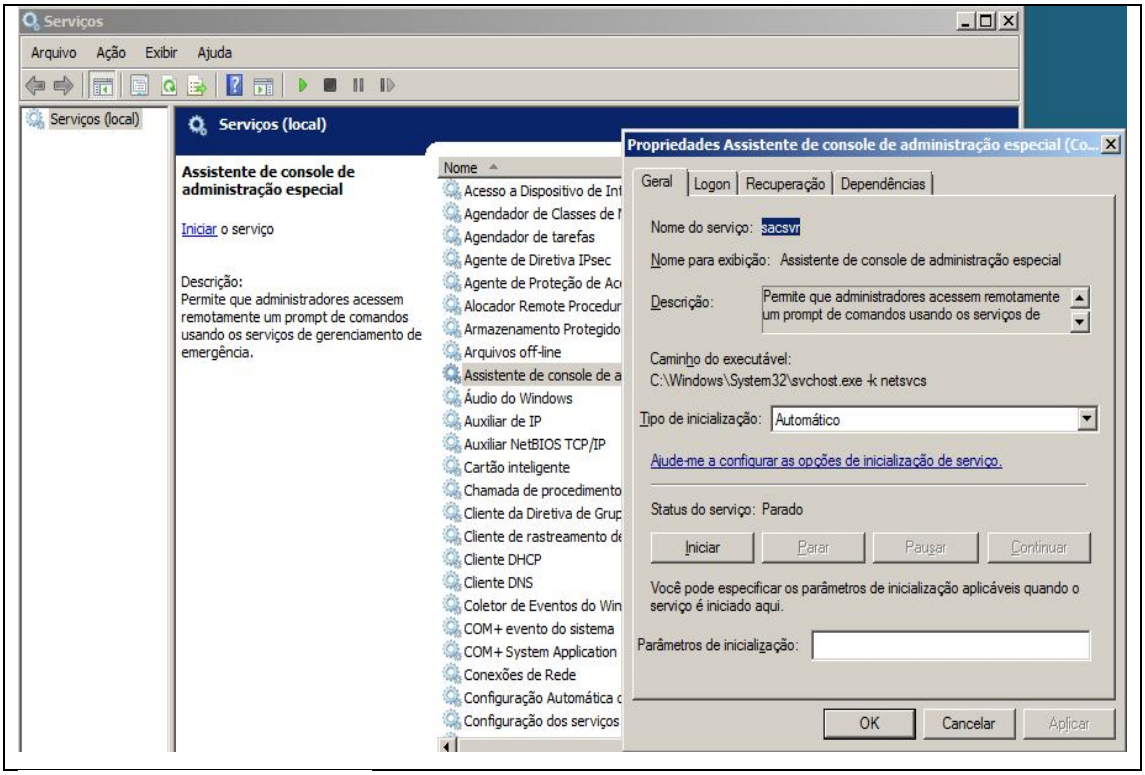


FIGURA 32: Assistente de console
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

4.3 Análise das técnicas de hardening

Neste tópico será relacionado o antes e o depois dos resultados nas aplicações das técnicas de *hardening* para o servidor *Linux*, utilizado à ferramenta *Lynis*, uma ferramenta *opensource* que faz uma varredura a procura de possíveis falhas no seu sistema operacional.

A instalação dessa ferramenta é bem simples como pode ser observada, no Quadro 37:

```
wget http://www.rootkit.nl/files/lynis-1.3.0.tar.gz
tar xvfvz lynis-1.3.0.tar.gz
./lynis-1.3.0/lynis --check-all -Q
```

Quadro 37: Ferramenta opensource
Fonte: Imagem criada pelo próprio autor.

As categorias que o Lynis observou-se no sistema, o qual esta sendo demonstrado a seguir. Na Figura 33 não foi aplicado nenhuma técnica de *hardenig*, pois este é o padrão da configuração para acesso via SSH.

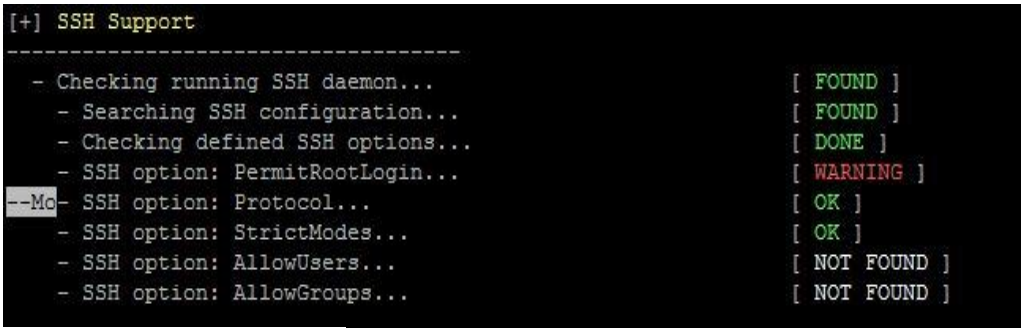


FIGURA 33: SSH sem Hardening
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Após a aplicação da técnica de *hardening* para o SSH, notamos que a técnica alterou informações dando maior segurança no acesso via SSH ao servidor.

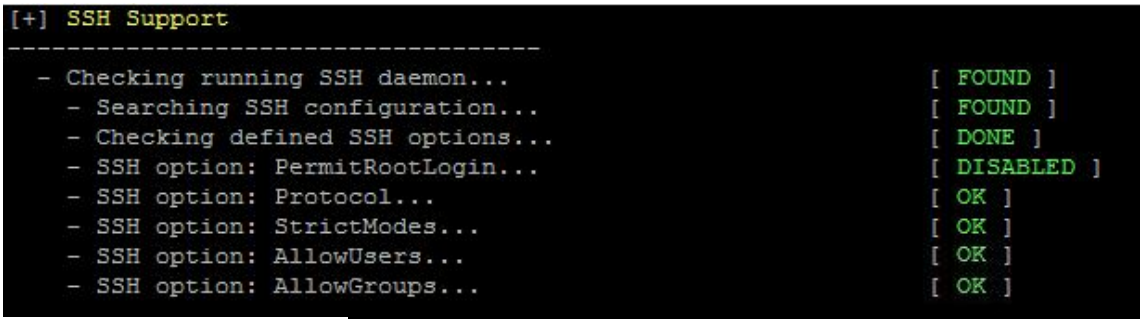


FIGURA 34: SSH com Hardening
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Na Figura 35 temos a parte de configuração do apache no qual na primeira imagem o software esta instalado não esta rodando, mas já pode ser visualizado pela ferramenta Lynis.

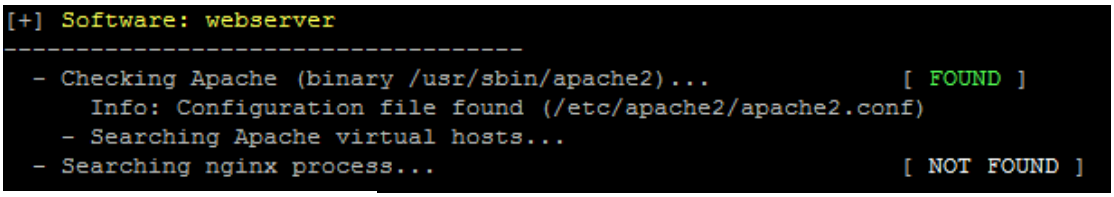


FIGURA 35: Apache sem Hardening
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Após a aplicação da técnica de *hardening* para o apache, podemos notar que a técnica alterou informações dando maior segurança ao servidor.

FIGURA 36: Apache com Hardening
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Na Figura 37, temos a parte de configuração do PHP no qual na primeira imagem o software esta instalado sem *hardening*.

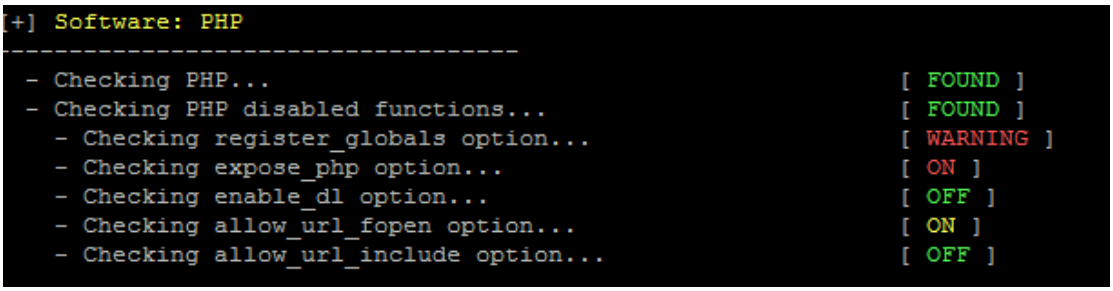


FIGURA 37: PHP sem Hardening
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Após a aplicação da técnica de *hardening* para o PHP, podemos notar que a técnica alterou informações dando maior segurança ao servidor, as marcações em amarelo são devido a sugestões no qual podem ser realizados.

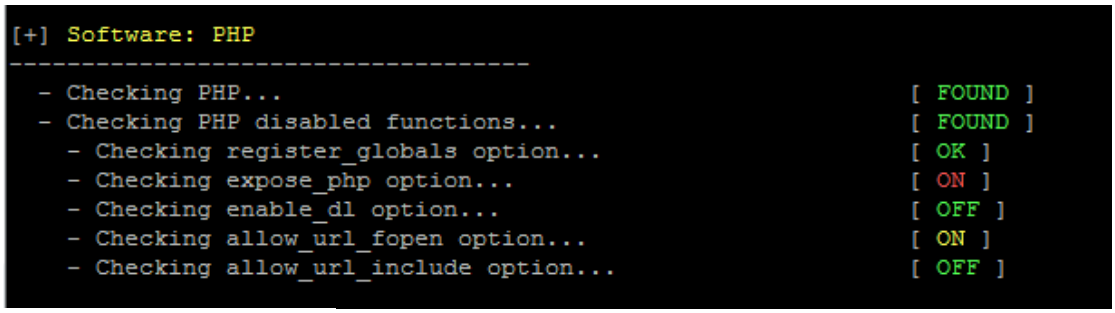


FIGURA 38: PHP com Hardenig
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Na Figura 39 temos a parte de configuração do MySQL o software está instalado e funcionando com as técnica de *hardening*.

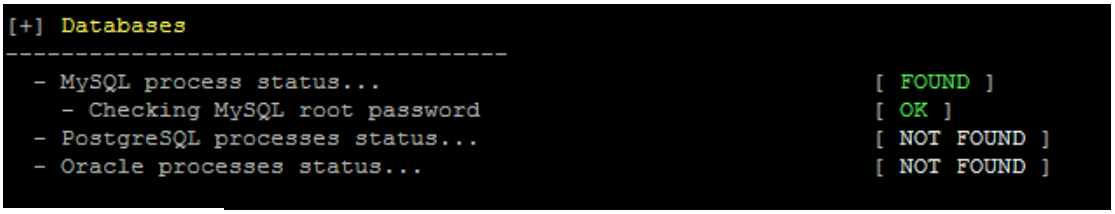


FIGURA 39: MySQL
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Na Figura 40 temos a parte de configuração do firewall no qual não possui nenhuma regra e esta em funcionamento.

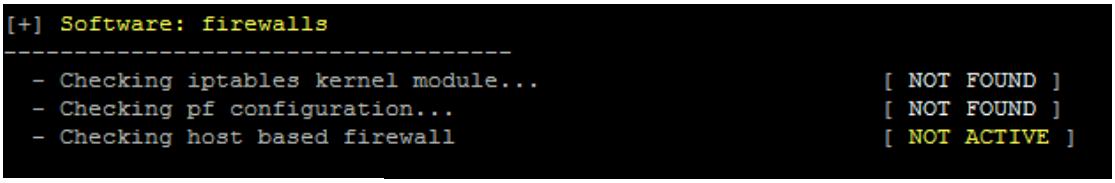


FIGURA 40: Firewall sem Hardening
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Na Figura 41 temos a parte de configuração do *firewall* no qual as regra para *hardening* já foram aplicadas.

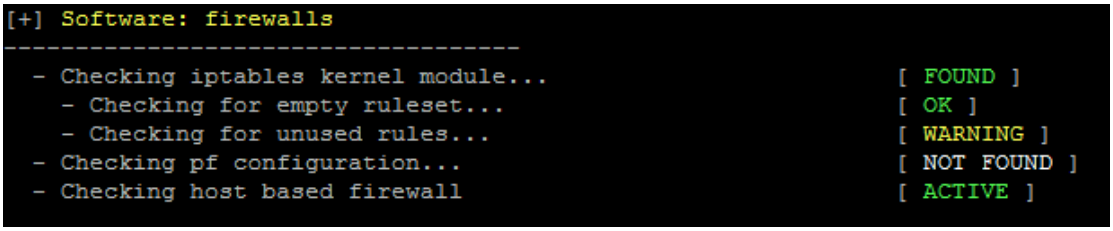


FIGURA 41: Firewall com Hardening
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

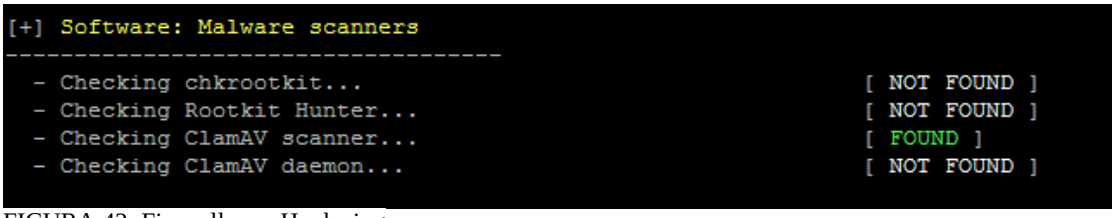


FIGURA 42: Firewall com Hardening
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Ao final de todas as configurações atualizadas, o sistema gera um quadro de sugestões no qual pode ser melhorado em seu sistema, conforme mostramos na Figura:

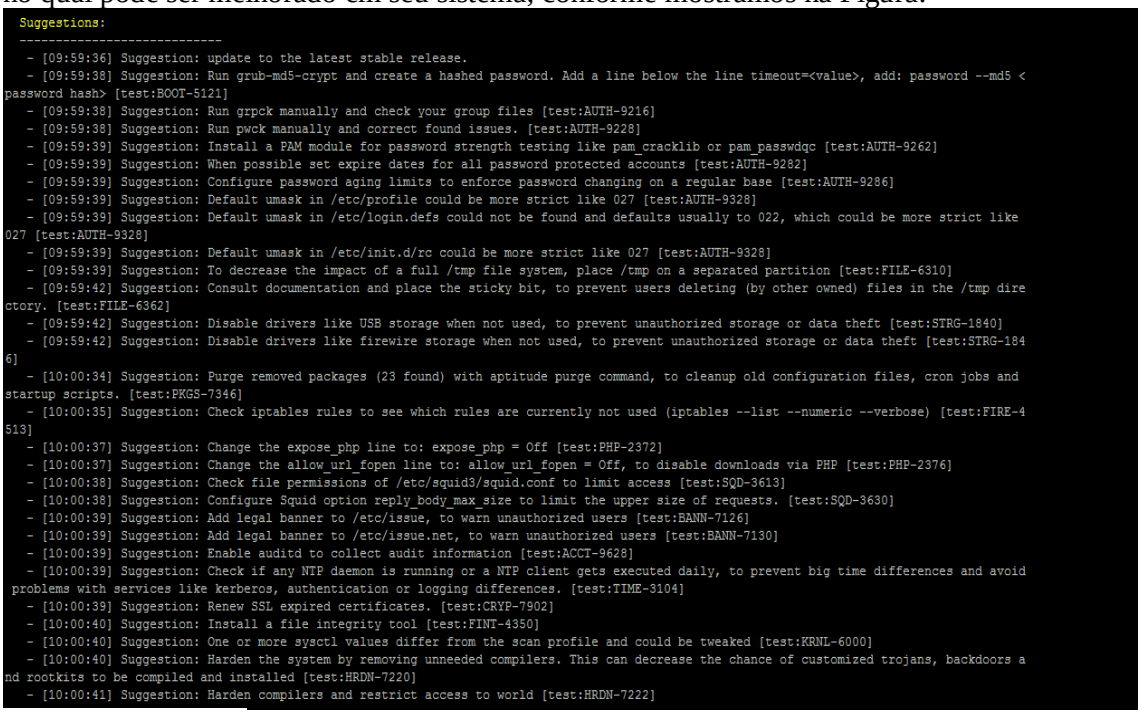


FIGURA 43: Sugestões
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Em mãos do conhecimento adquirido no servidor *Linux*, daremos continuidade a aplicação da técnica de *hardening* para o servidor *Windows Server*. Para obter os resultados neste servidor, antes e após a aplicação da técnica, precisamos instalar a ferramenta *Microsoft Baseline Security Analyzer* (MBSA), um software gratuito e utilizado pela Microsoft para análise.

A instalação dessa ferramenta é de simples manuseio, precisando baixar o software no site da *Microsoft* e realizando o seu *download*. Em seguida, daremos um duplo clique para abrir *Microsoft Baseline Security Analyzer* 2.3, e posteriormente em " *Scan a computer*".

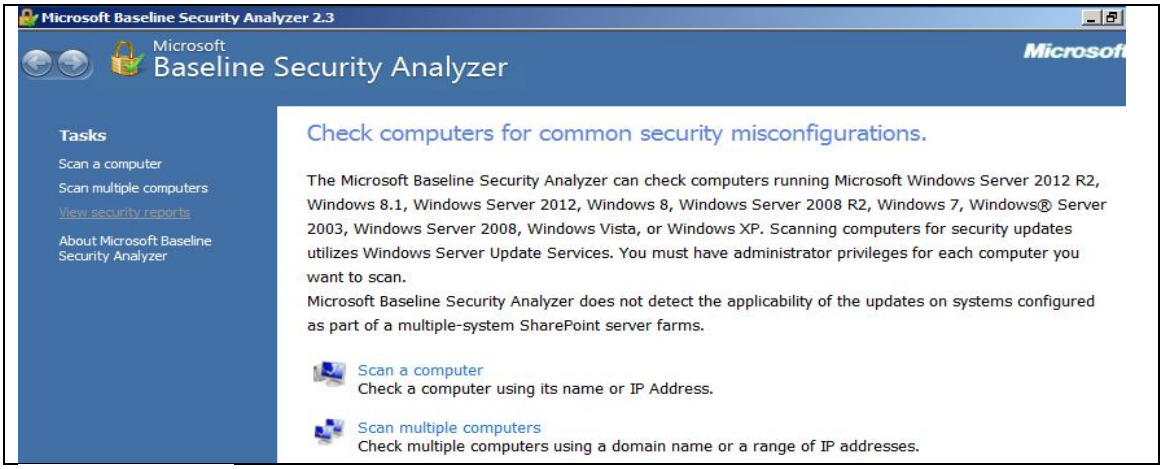


FIGURA 44: MBSA
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Após abre-se uma janela, com possibilidade de escolha ao que quer ser analisado. Neste estudo, optou-se pelas seguintes requisitos, os quais podem ser visualizados na Figura 45:

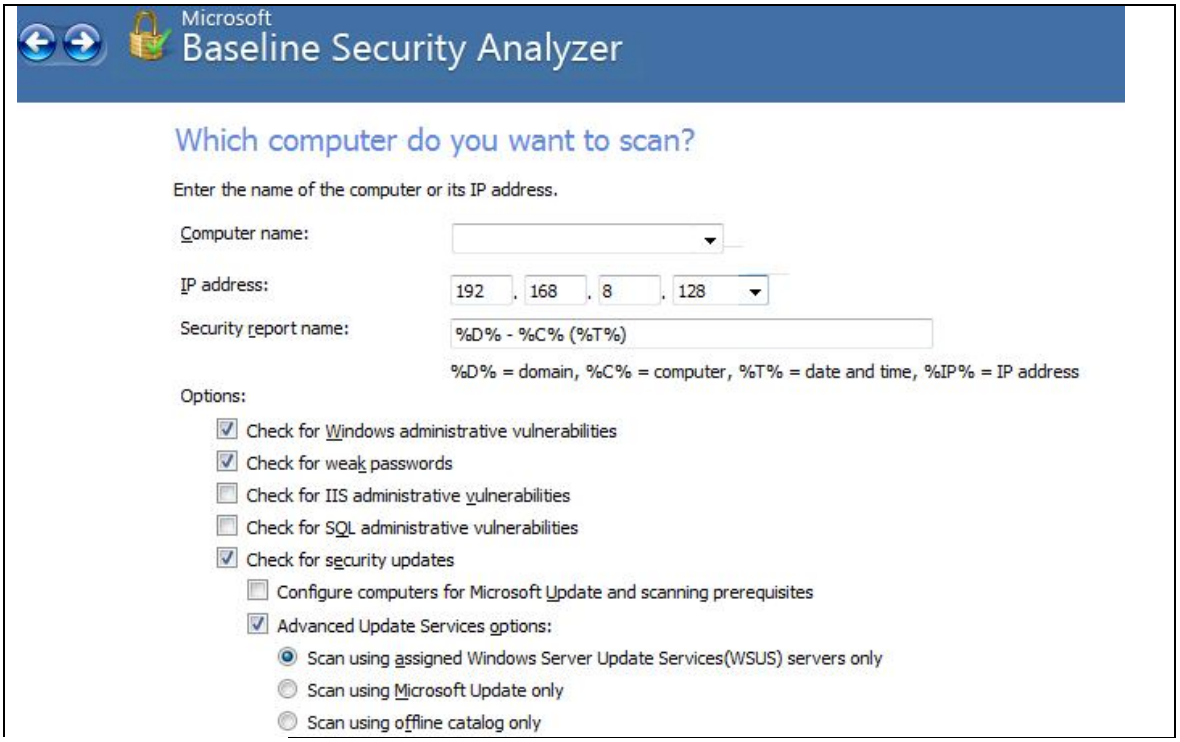


FIGURA 45: Check MBSA
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

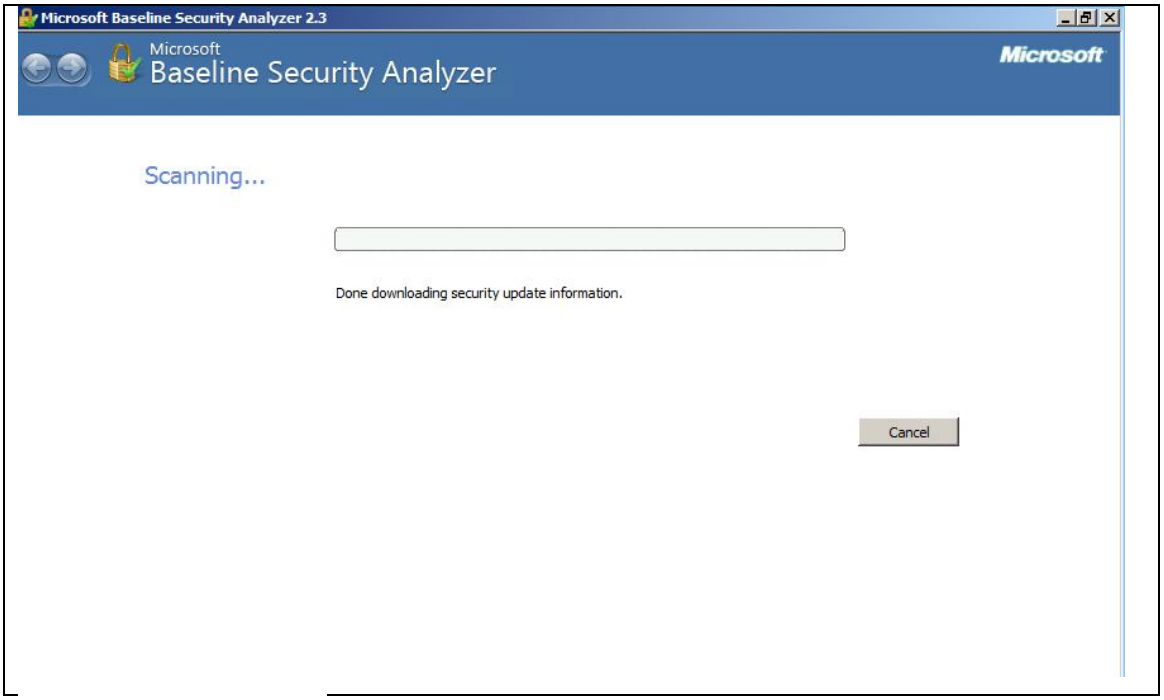


FIGURA 46: *Scanning* MBSA
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Realizada esta etapa, o MBSA fara o *scan* dos arquivos selecionados no servidor, gerando um relatório organizado, demonstrando os detalhes do que foi verificado, seus resultados e também o que deve ser corrigido.

MBSA exibe ícones diferentes na pontuação colunas do relatório, dependendo se a vulnerabilidade foi encontrada no servidor. Para as verificações de vulnerabilidades administrativas, um X vermelho é usado quando um cheque falha crítica (por exemplo, o usuário tem uma senha em branco). O X amarelo é usado quando um cheque não falha crítica (por exemplo, uma conta tem uma senha que não expira). Uma marca de seleção verde é usada quando um cheque passa (ou seja, nenhum problema foi encontrado para que cheque especial). Um asterisco azul é usado para verificações de melhores práticas (por exemplo, verificar se a auditoria está habilitada), e um ícone informativo asterisco azul é usado para verificações que simplesmente fornecem informações sobre o servidor.

Na Figura 47 temos o resultado no qual demostra o que foi verificado e as falhas existentes no servidor para assim realizar a correção.

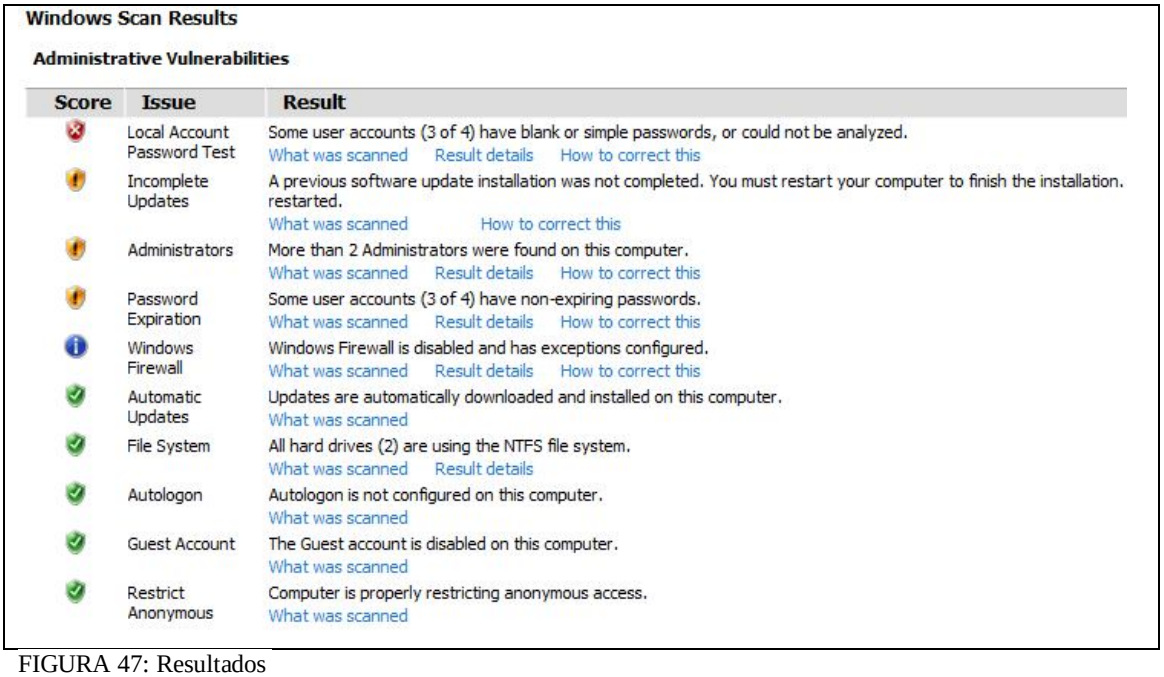


FIGURA 47: Resultados
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Realizada tal etapa, faz-se novamente a checagem no qual ele ira verificar apenas *o Check for IIS administrative vulnerabilities* e Check for SQL *adminstrative vulnerabilities* conforme demonstra na Figura 48.

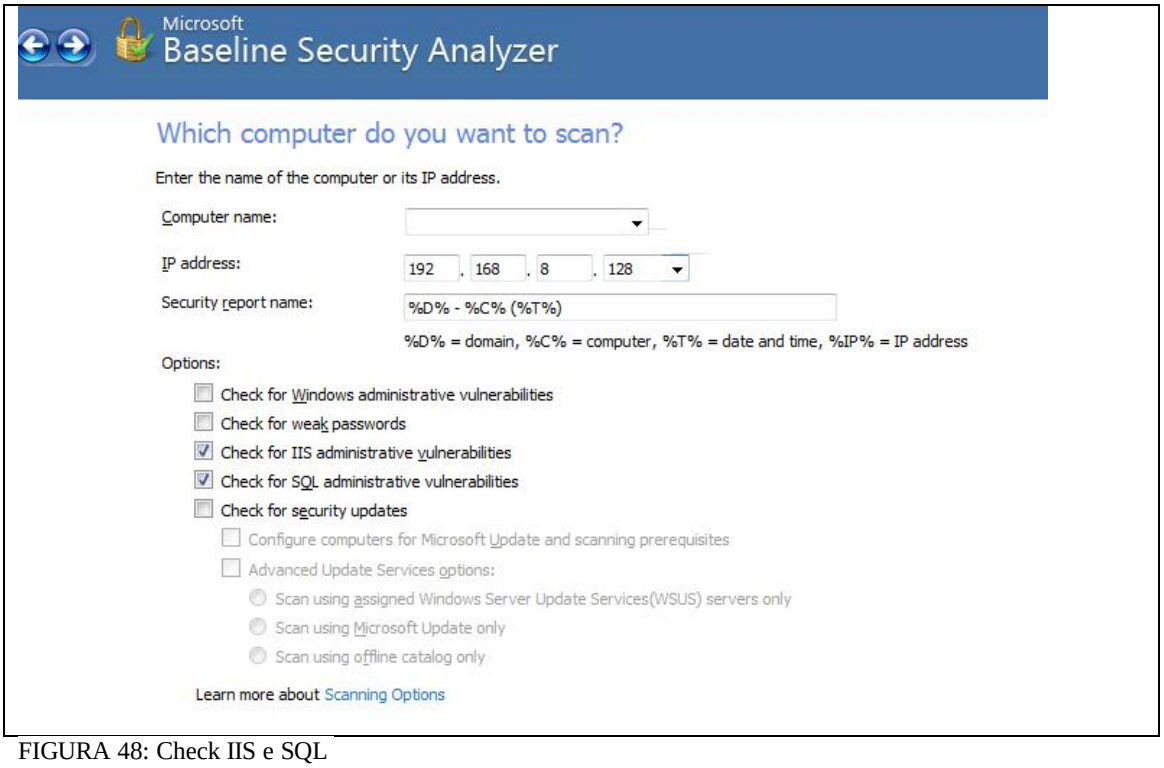
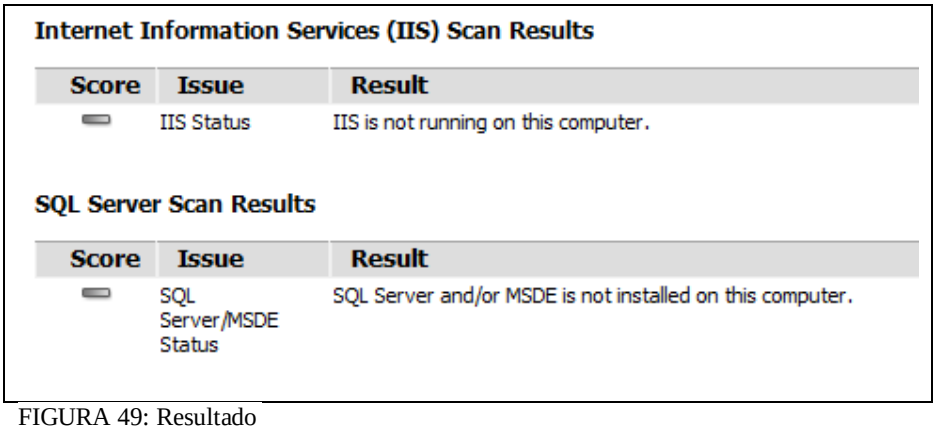


FIGURA 48: Check IIS e SQL
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

Resultado no qual não estava instalado e nem aplicado o *hardening*:



Internet Information Services (IIS) Scan Results

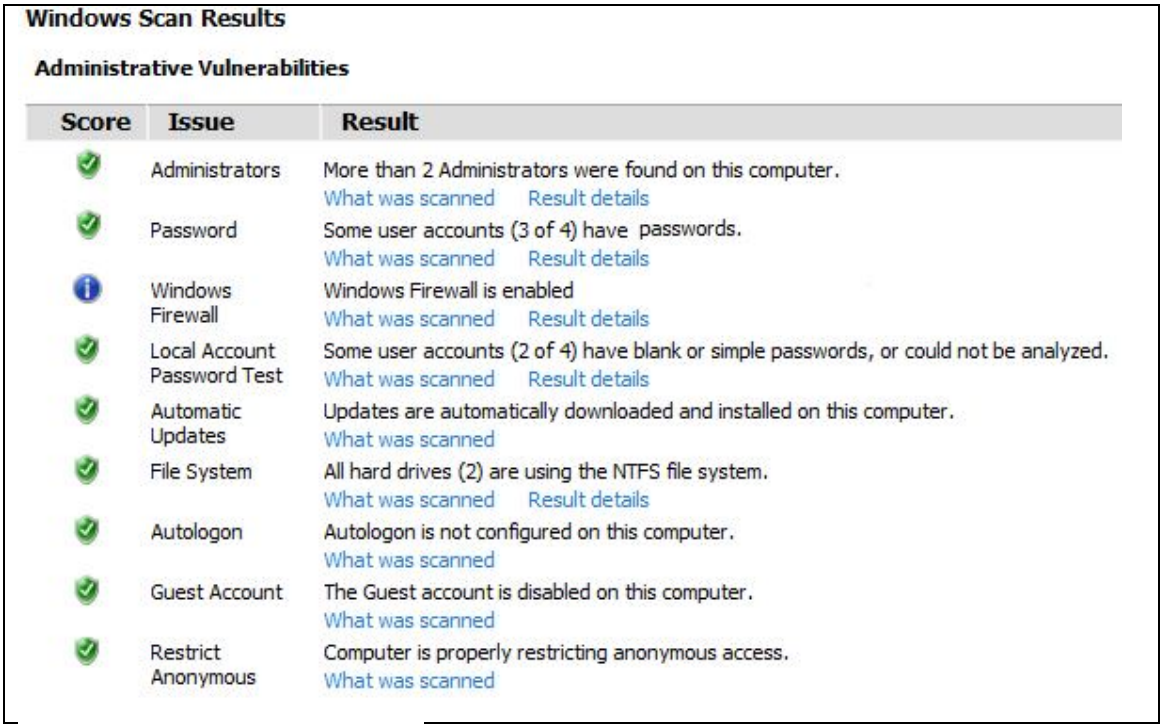
Score	Issue	Result
—	IIS Status	IIS is not running on this computer.

SQL Server Scan Results

Score	Issue	Result
—	SQL Server/MSDE Status	SQL Server and/or MSDE is not installed on this computer.

FIGURA 49: Resultado
Fonte: Imagem salva pelo próprio autor utilizando o sistema.

De acordo com a Figura 49, gerado pelo MBSA, pode-se observar que o níveis de informações foram corrigidos e falhas que antes existiam praticamente desapareceram, assim, a aplicação das técnicas de *hardening* nos servidores *Windows* foram válidas e proporcionaram maior segurança ao sistema.



Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
✓	Administrators	More than 2 Administrators were found on this computer. What was scanned Result details
✓	Password	Some user accounts (3 of 4) have passwords. What was scanned Result details
ℹ	Windows Firewall	Windows Firewall is enabled What was scanned Result details
✓	Local Account Password Test	Some user accounts (2 of 4) have blank or simple passwords, or could not be analyzed. What was scanned Result details
✓	Automatic Updates	Updates are automatically downloaded and installed on this computer. What was scanned
✓	File System	All hard drives (2) are using the NTFS file system. What was scanned Result details
✓	Autologon	Autologon is not configured on this computer. What was scanned
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned

FIGURA 50: Resultado após *hardening*
Fonte: Imagem salva pelo próprio autor utilizando o sistema

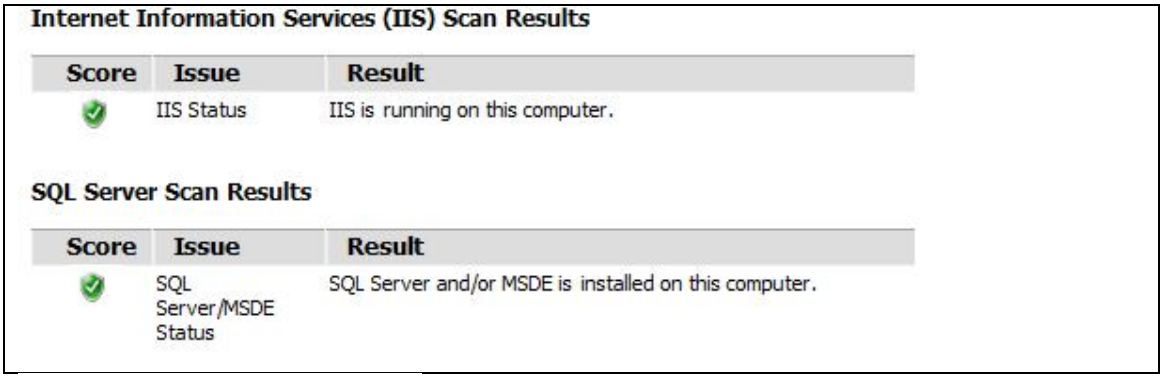


FIGURA 51: Resultado após hardening
Fonte: Imagem salva pelo próprio autor utilizando o sistema

Implementar um plano de segurança é um processo demorado, o qual exige uma analise detalhada de cada um dos sistemas operacionais. Frente, a tal analise os sistemas encontram-se vulneráveis podendo assim estarem comprometidos ou operando inadequadamente, permitindo o escape de informações, sua lentidão e infectando as demais redes integradas.

Com base na aplicação das técnicas de *Hardening* para os Servidores *Linux* e *Windows* podem-se obter resultados satisfatórios ao que diz respeito na sua aplicabilidade quanto a segurança dos Servidores, seu aplicativos instalados e no gerenciamento da rede envolvida.

CONCLUSÃO

A segurança da informação visa o desenvolvimento da proteção de um conjunto de informações, tanto no âmbito individual ou de uma empresa no seu sentido mais abrangente. Neste aspecto, o estudo realizado desvelou as estratégias utilizadas pelos sistemas *Windows* e *Linux*, com as suas características básicas - confidencialidade, disponibilidade, bem como promoveu a aproximação de conceitos de *Hardening*, frente a esses sistemas operacionais.

De acordo com os testes realizados foi possível realizar uma reflexão acerca da importância dos planos de segurança, as suas relações no que diz respeito aos status de segurança, sendo estes percebíveis devido a problemas de *hardware*. Percepções estas necessárias para determinar quais as etapas / caminhos que devem ser seguidos perante o real problema ali instalado.

Fica notário, que há uma grande inquietação e insegurança quando se trata de problemas gerencias, relacionados às praticas de segurança da informação, fazendo-se necessário a criação, análise e implementação de planos de segurança. Fazendo jus, mais uma vez a temática deste estudo, ou seja, o *hardening*, o qual permite que novos projetos sejam formulados, analisados e assim implementados.

Paralelamente, às diversas ameaças que podem afetar desde um servidor, alastrando-se por toda a rede. Frente à isso, o analista de rede deverá ter um *firewall* bem configurado e assegurado, trabalhando aliado ao conjunto de Apache, MySQL, PHP, IIS, FTP, os quais contribuíram na efetivação da ações adequadas às reais necessidades dos sistemas.

A presença do analista de rede, e a atualização contínua dos programas e equipamentos, dá a garantia de que os sistemas operacionais, sendo eles *Windows* ou *Linux*, manterão o seu ambiente de trabalho mais qualificado e seguro. Desta forma, o analista torna-se peça fundamental na equipe de trabalho, contribuindo para efetivação de sistemas mais seguros.

Ressalva-se assim que trabalhos desta natureza devem continuar sendo elaborados, pois as tecnologias da informação estão em contínua ascensão, necessitando diariamente de novos estudos, experimentos e inovações, entre eles a técnica de *Hardening* voltado para Linux aplicando diretamente ao *Kernel*.

REFERÊNCIAS

ABADI, Marcos. Hardening em Servidores Linux. São Paulo, 2010. Disponível em: http://marcosabadi.blogspot.com.br/2010/02/hardening-em-servidores-linux.html. Acesso em: 12/mar/2013.

Associação Brasileira de Normas Técnicas, [ABNT 2700], 2008. Disponível em https://www.abntnet.com.br/ecommerce/ssl/pesquisaresultado.aspx. Acesso em Maio de 2013.

ACHOUR, Mehdi et al. PHP Manual, 2006. Disponível em http://www.php.net/manual/pt_BR/. Acesso em Mar/2013.

BARBOSA, Felipe Santos. Fundamentos em Segurança e Hardening em Servidores Linux baseado na Norma ISO 27002. In: Anais do V ENUCOMP 2012, Parnaíba, PI, 12 a 14 de novembro de 2012: [recurso eletrônico]/ Organização [de] Thiago C. de Sousa e Rodrigo Augusto R. S. Baluz. -Parnaíba: FUESPI, 2012.

CAMPOS, Augusto. O que é Linux. BR-Linux. Florianópolis, março de 2006. Disponível em <http://br-linux.org/faq-linux>. Acesso em: Mar/2013.

CAMY, Alexandre Rosa; SILVA, Evandro R.N.; RIGUI, Rafael. Seminário de firewall. 2003. 27 f. Seminario-Curso e Pós Graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis.

DAWEL, George. A segurança da informação nas empresas. Rio de Janeiro: Editora Ciência Moderna Ltda., 2005.

DICAS de Hospedagem. Vantagens de Servidores Windows. 2010. Disponível em: <http://dicasdehospedagem.com/vantagens-de-servidores-windows/>. Acesso em Março de 2013.

FONTES, Edison Luiz Gonçalves. Segurança da informação: o usuário faz a diferença. São Paulo: Saraiva, 2006.

_____**.** Vivendo a segurança da informação: orientações práticas para as organizações. São Paulo :Sicurezza Brasiliano & Associados, 2000.

[ISO 27001, 2006] – ABNT ISO27001, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão de segurança da informação – Requisitos, 2006.

JIRASEK, Vladimir. Practical application of information security models Original Research Article. *Information Security Technical Report, Volume 17, Issues 1–2, February 2012, Pages 1-8.*

KNOWLEDGELEADER, Knowledge Leader, disponível em <http://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content /ChecklistsGuidesBritishStandard7799!OpenDocument>, Acessado em 04/05/2013, 2003.

MELO, Sandro. BS7799 Linux da Tática à Prática em Servidores. São Paulo: Alta Books, 2006.

MITNICK, Kevin D. A arte de enganar. São Paulo: Pearson Education do Brasil Ltda, 2003.

MITNICK, Kevin D.; SIMON, Willian L. **A arte de invadir**. São Paulo: Pearson Education do Brasil Ltda, 2006.

MOREIRA, Nilton Stringasci. **Segurança mínima**: uma visão corporativa da segurança de informações. Rio de Janeiro: Axcel Books, 2001.

MORIMOTO, Carlos E. **Redes e Servidores Linux**, 2ed. Porto Alegre: GDH Press e Sul Editores 2006.

_____. Configurando um servidor Windows, 2008. Disponível em: http://www.hardware.com.br/tutoriais/configurando-servidor-windows/. Acesso em: Mar/2013.

MOURAD, Azzam; LAVERDIÈRE, Marc-André; DEBBAB, Mourad. An aspect-oriented approach for the systematic security hardening of code Original Research Article *Computers & Security, Volume 27, Issues 3–4, May–June 2008, Pages 101-114*

NETO, Urubatan. Dominando Linux Firewall Iptables. Rio de Janeiro: Ciência Moderna Ltda., 2004

NOYES, Katherine, Veja Porque o Linux está a Frente do Windows em Servidores. 2010 Disponível em: <http://pcworld.uol.com.br/noticias/2010/08/31/veja-porque-o-linux-esta-a-frente-do-windows-em-servidores/>. Acesso em: Mar/2013.

OFICINA da Net. Internet Information Services. 2010. Disponível em: <http://www.oficinadanet.com.br/artigo/servidores/internet_information_services> Acesso em: Mar/2013.

PORTAL Educação. Funções do servidor em Windows Server 2003. 2008. Disponível em: <http://www.portaleducacao.com.br/informatica/artigos/6032/funcoes-do-servidor-em-windows-server-2003#ixzz2NoijMkkt> Acesso em: Mar/2013.

PORTAL Educação. O que é Mysql?. 2008. Disponível em: http://www.portaleducacao.com.br/informatica/artigos/4398/o-que-e-mysql. Acesso em: Mar/2013.

PROCÓPIO, Leandro Luiz Raimundo. Trabalho sobre as versões Windows e Linux. 2008 Disponível em: http://www.ebah.com.br/content/ABAAAAJfAAD/trabalho-sobre-as-versoes-windows-linux. Acesso em: Mar/2013.

RAMALHO, José Antonio. Oracle. Aprenda a criar bancos de dados, tabelas, índices, visões e outros objetos. São Paulo: Breckley Brasil, 2002

RFC 959 (1985), Disponivel em http://www.ietf.org/rfc/rfc959.txt Acesso em: Marco de 2013.

REIS, Flavio A; JULIO Eduardo P; VERBENA, Marcos F. Hardening. 2011. Disponível em: http://www.devmedia.com.br/websys.4/webreader.asp?cat=62&revista=inframagazine_1#a-3403. Acesso em: Mar/2013.

RODRIGUES, Bernardo Maia. Windows Hardening, 2008. Disponível em: http://www.csirt.pop-mg.rnp.br/docs/hardening/windows.html Acesso em: Mar/2013

SCHIFFMAN, M. (2005). A complete guide to the common vulnerability scoring system (cvss). http://www.first.org/cvss/cvss-guide.html Consultado em Novembro de 2013

SEMOLA, Marcos. Gestão da Segurança da Informação**:** uma visão executiva. Rio de Janeiro: Campus, 2002.

SILVA, Gleydson Mazioli. Guia Foca/Linux. 2006. Disponível em: http://www.guiafoca.org/. Consultado Março 2013

SILVA. Alexandre Roberto da. Baboo.com.br 2010. Disponível em:http://www.baboo.com.br/2012/05/implantacao-de-aplicativos-do-asp-net-com-o-iis-7/ Consultado em Março de 2013.

[STANDARDS, 2005] Standarts Direct – International Standards And Documentation, 2005. Disponível em http://17799.standardsdirect.org/bs7799.htm. Consultado em Maio 2013.

VIDAL. Josue. Imasters.com.br.2006 Disponível em: http://imasters.com.br/artigo/4735/redes-e-servidores/entendendo-active-directory/ Consultado em Março de 2013

WANG, Shuzhen; ZHANG, Zonghua; KADOBAYASHI, Youki. Exploring attack graph for cost-benefit security hardening: A probabilistic approach Original Research Article *Computers & Security, Volume 32, February 2013, Pages 158-169.*