UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

LÁZARO THIAGO DELAY DE OLIVEIRA

ESTUDO E LEVANTAMENTO DE ARTIGOS QUE USARAM TÉCNICAS DE HARDENING

MONOGRAFIA

CURITIBA
2015

LÁZARO THIAGO DELAY DE OLIVEIRA

ESTUDO E LEVANTAMENTO DE ARTIGOS QUE USARAM TÉCNICAS DE HARDENING

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de servidores e equipamentos de rede, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná – UTFPR.
Orientador: Prof. MSc. Juliano De Mello Pedroso

CURITIBA
2015

RESUMO

OLIVEIRA, Lázaro Thiago Delay. **Estudo e levantamento de artigos que usaram técnicas de Hardening.** 2015. 64 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

Esta é uma pesquisa de estudo e levantamento de artigos já publicados com exemplos de técnicas de Hardening aplicadas, utilizando o método bibliográfico. O objetivo desta pesquisa é descrever as vantagens e desvantagens de cada estratégia utilizada, de modo que ajude o leitor a definir uma melhor política de segurança para utilizar em seu dia a dia no ambiente corporativo, ou até mesmo em um ambiente pessoal (residencial). Com isso, pretende-se minimizar a vulnerabilidade dos equipamentos utilizados pelos usuários com exemplos reais devido a grande divergência de informações que hoje se encontra no mercado.

Palavras-chave: Segurança. Hardening. Segurança física. Tecnologia da informação.

ABSTRACT

OLIVEIRA, Lázaro Thiago Delay. **Study and survey of articles that used Hardening techniques.** 2015. 64 pages. Monograph (Specialization in Configuration and Management of Servers and Network Equipments) - Federal Technological University of Paraná. Curitiba, 2015.

This is a study and survey of articles published with examples of hardening techniques applied, using the literature method. This research objective is to describe the advantages and disadvantages of each strategy used in order to help the reader to better define a security policy to use in their corporate environment , or even in a personal environment (residential). This is intended to minimize the vulnerability of the equipment used by users with real examples because of the wide divergence of information that is on the market todays.

Keywords: Safety. Hardening. Physical Security. Information Technology.

LISTA DE SIGLAS

ACS - Assistente de Configuração de Segurança

ADSL - Assymetrical Digital Subscriber Line

CERT - Centro de estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CMS - Content Management System

DNS - Domain Name System

DoS - Denial of Service

FTP - File Transfer Protocol

GRUB - GRand Unifield Bootloader

IEE – Institute of Electrical and Electronic Engineers

IIS - Internet Information Services

IP – Internet Protocol

MBSA - Microsoft Baseline Security Analyzer

NAP - Network Access Protection

NTP - Network Time Protocol

QoS – Quality of Service

RDP - Remote Desktop Protocol

SIP - Session Initiation Protocol

SMTP - Simple Mail Transfer Protocol

SNMP - Simple Network Management Protocol

SQL - Structured Query Language

SSDP - Simple Service Discovery Protocol

SSH - Secure SHell

SSTP - Secure Socket Tunneling Protocol

TCP - Transmission Control Protocol

TI – Tecnologia da Informação

UDP - User Datagram Protocol

VoIP - Voice over Internet Protocol

VPN - Virtual Private Network

WSUS - Windows Server Update Services

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Neste capitulo é apresentado o tema da pesquisa: Estudo e levantamento de artigos que usaram técnicas de Hardening.

1.1 TEMA

Com a evolução e utilização da tecnologia atualmente nas empresas, o desenvolvimento começou a se expandir, junto com a facilidade de acesso a todas as informações imagináveis.

A expansão da internet e seus meios de comunicação deixaram os ambientes corporativos cada vez mais expostos ao ambiente virtual.

Devido a essa fácil integração entre usuários e seus sistemas, as equipes de TI estão se preparando e se estruturando cada vez mais para não ter o risco de ameaças físicas ou virtuais, que pode levar pessoas não autorizadas a ter acesso aos seus dados e equipamentos.

Devido a frequentes ataques virtuais que estão ocorrendo no dia a dia, as empresas com seus analistas de segurança da informação, estão e devem atuar fortemente para estarem preparados para enfrentar todo o tipo de ameaça que pode prejudicar suas estruturas ou informações. Esses métodos são aplicados através da segurança física em seus equipamentos de tecnologia, e com técnicas de Hardening.

Este artigo tem como objetivo explicar o conceito de Hardening e segurança física, mostrar como esta sendo implantada essa nova prática nas empresas, e, listar diversos tópicos, facilitando o entendimento de utilização desse processo. Apontando algumas táticas utilizadas pelos administradores de redes, e informar ao leitor suas vantagens e desvantagens.

1.2 OBJETIVOS

Nesta sessão serão trabalhados objetivo geral e objetivos específicos.

1.2.1 Objetivo Geral

Realizar um estudo de artigos que aplicaram técnicas de Hardening e segurança física, apontando suas principais vantagens e desvantagens.

1.2.2 Objetivos Específicos

- Levantar artigos já publicados que utilizaram técnicas de Hardening;
- Analisar e descrever a vulnerabilidade do equipamento/sistema e qual técnica de Hardening foi aplicado;
- Analisar e descrever as vantagens e as desvantagens do Hardening aplicado*;*

1.3 JUSTIFICATIVA

Esta pesquisa é fundamental para auxiliar administradores de redes ou equipes da área de segurança virtual e física, a identificarem melhores técnicas de Hardening e segurança física para seus sistemas e equipamentos. Tendo conhecimento de procedimentos, para serem utilizados em suas atividades do dia a dia.

Através desse artigo, até mesmo as pessoas leigas na área de tecnologia, podem identificar possíveis falhas em suas corporações, e como devem se comportar perante essas situações.

1.4 PROCEDIMENTOS METODOLÓGICOS

Para conseguir atingir os meus objetivos desta pesquisa, realizei o estudo em cima de vários artigos científicos, livros, internet, revistas, jornais, entre outros relacionados a este tema. Realizei algumas pesquisas de campo, conhecendo a estrutura de algumas empresas da área tecnológica que não autorizaram a citação de seus nomes nesta monografia.
Meu planejamento para o desenvolvimento do trabalho foi seguido através do seguinte cronograma abaixo:

- Levantamento bibliográfico do Hardening, segurança da informação, segurança física e lógica, táticas de fortalecimento e atuais ameaças na área de informática.
- Visitar empresas para identificar como é aplicado o Hardening em suas estruturas, e quais ameaças já teve em suas dependências.
- Identificar técnicas de Hardening, e citar suas vantagens e desvantagens, facilitando ao leitor qual a melhor escolha de utilização.

1.5 EMBASAMENTO TEÓRICO

A política de segurança de TI deve ser elaborada, avaliada, atualizada e gerenciada constantemente. Para tanto, é fundamental a criação de um conselho composto por executivos e gestores que devem cumprir efetivamente as regras e diretrizes estabelecidas no documento e assim alcançar suas metas e objetivos, assegurar e minimizar o impacto relativo a falhas e vulnerabilidades físicas, lógicas e humanas para proteção do patrimônio e informações relevantes da empresa. Considerando que o investimento em segurança física e lógica é permanente, pois os equipamentos possuem um tempo de vida útil e também há necessidade de ampliação dos recursos de TI conforme a expansão, substituição e atualização do equipamento ou sistema. Diante deste cenário, avalia-se de forma positiva o investimento com infraestrutura, controle acesso e segurança dos recursos físicos e lógicos na empresa, uma vez que aplicando estes investimentos posteriores ocorrerão de forma gradativa (LEITE, Cristiano Monteiro, 2011).

Devemos levar em consideração que a segurança da informação é composta de várias etapas e processos, e funciona da mesma maneira que uma pirâmide, onde cada peça é importante para o todo. A melhoria constante só é possível quando levado em consideração todas as possibilidades possíveis e onde somente através de um trabalho em conjunto é obtido efeito expressivo.

Mas devemos considerar também que uma causa constante de ataques é a engenharia social, onde através de um funcionário não capacitado o atacante consegue informações sigilosas. Para combater este tipo de prática todos os funcionários das corporações devem receber treinamento adequado, diminuindo cada vez mais este tipo de prática. (RIBEIRO, Wilson Antônio Dos Anjos; CRUZ, Léo Victor Nascimento).

1.6 ESTRUTURA

Essa monografia é composta por 4 capítulos. O capítulo 1 tratará da parte introdutória, sendo apresentado o tema, os objetivos a serem atingidos, justificativa da escolha, metodologia utilizada para a pesquisa e um embasamento teórico.

O capítulo 2 é representado pelo referencial teórico do projeto. Definido pelos assuntos: Hardening, Segurança física e ataques virtuais. Este capítulo tem como finalidade dar uma explicação e compreensão ao leitor conceitos, técnicas, objetivos dos temas abordados, para assim, entender o desenvolvimento e conclusão desta pesquisa.

O desenvolvimento esta representado no capítulo 3, que ira mostrar um estudo extraído de artigos que utilizaram técnicas de Hardening em seus servidores, e expor em meu ponto de vista suas reais vantagens e desvantagens. Facilitando assim, ao administrador de rede identificar métodos que pode utilizar em seus servidores. Seja ele Windows ou Linux.

Para finalizar, o capítulo 4 traz a conclusão realizada da pesquisa, junto com todo o material pesquisado e utilizado como referência para a criação e elaboração desta monografia.

2 REFERENCIAIS TEÓRICOS

2.1 HARDENING

São ajustes finos efetuados no sistema após uma instalação. É o processo de proteger um sistema contra ameaças desconhecidas. Os administradores de sistema devem fortalecer uma instalação contra o que eles acham que poderia ser uma ameaça.

Uma instalação padrão de qualquer sistema que tenha a finalidade de servidor, o administrador tem por obrigação de melhorar a segurança ativando controles nativos ou implementando-os, esse processo é conhecido como Hardening (RIBEIRO, WILSON ANTONIO DOS ANJOS; CRUZ, Léo Victor Nascimento, 2013).

Em computação, hardening é o processo de customizar um sistema em busca de maior segurança proativo, para que ele se torne o mais resistente possível a ataques de crackers. Isso tipicamente inclui remoção dos usuários que não serão usados e da desativação ou remoção dos serviços e programas desnecessários (ZUCCO, JERONIMO CLEBERSON, 2008).

A técnica de Hardening pode ser utilizada em qualquer sistema operacional. Com o grande aumento no número de ameaças existentes na Internet é fundamental que o sistema de um servidor esteja preparado para superar todas as tentativas de invasão. Esta técnica não deve ser implementada somente em servidores que ficam conectados diretamente a Internet, muitas vezes fornecendo serviços como, por exemplo servidores web, mas também em máquinas que provêm serviços internos de rede como servidores de arquivos e de impressão.

Com a blindagem de sistemas é possível aumentar o desempenho do hardware, liberando recursos que estão sendo utilizado por aplicativos desnecessários, implementando configurações específicas em alguns serviços, além de gerar um ambiente mais seguro.

Hardening pode ser utilizado para evitar que usuários mal intencionados aproveitem da ausência do administrador e implantem scripts maliciosos em servidores infectando toda a rede, bloquear que o usuário administrador faça login diretamente no terminal, efetuar logout por tempo de inatividade, remover

pacotes que não são utilizados, remover permissões especiais de binários executáveis, dentre outras técnicas (Revista, Infra Magazin, 1/20818).

2.2 SEGURANÇA FÍSICA

Segurança física e do ambiente são os recursos que regulamentam tanto o controle de acesso, quanto a prevenção de sinistros como tempestades, furacões, terremotos, acidentes, roubos, e outros. São medidas que previnem a empresa contra qualquer ocasião em que possa acontecer a perda, dano ou extravio de informações da empresa (ESPÍRITO SANTO, Adrielle Fernanda Silva).

Seu objetivo é prevenir a perda, o dano ou o comprometimento dos ativos da organização e a interrupção das atividades do negócio. Assim, os equipamentos, tantos os de dentro quantos os de fora das dependências físicas da organização, instalados e em alienação, devem ser fisicamente protegidos contra ameaças da segurança e perigos ambientais para evitar acessos não autorizados, perdas e dano aos dados. Os equipamentos devem ser instalados e protegidos contra ameaças ambientais, perigos e oportunidades de acessos não autorizados (AMARAL, Marcos Prado).

A segurança física da informação contempla a proteção física dos prédios e equipamentos (e dos softwares e informações contidos nos mesmos) contra roubos, vandalismo, desastres naturais, catástrofes humanas e danos acidentais, e, portanto requer prédios sólidos, estratégias eficientes em casos de emergência, fontes de tensão confiáveis, controle adequado da temperatura, e proteção apropriada contra intrusos (GABBAY, Max Simon).

O objetivo desta política é prevenir o acesso não autorizado, dano e interferência às informações e instalações físicas da organização. A segurança física dos equipamentos de informática e das informações da empresa deve ser protegida de possíveis danos (GABBAY, Max Simon).

Devemos atentar para ameaças sempre presentes, mas nem sempre lembradas; incêndios, desabamentos, relâmpagos, alagamentos, problemas na rede eléctrica, acesso indevido de pessoas ao Centro de Processamento de Dados, formação inadequada de funcionários, etc.

Medidas de proteção física, tais como serviços de guarda, uso de nobreaks, alarmes e fechaduras, circuito interno de televisão e sistemas de

escuta são realmente uma parte da segurança de dados. As medidas de proteção física são frequentemente citadas como "segurança computacional", visto que têm um importante papel também na prevenção dos itens citados no parágrafo acima.

O ponto-chave é que as técnicas de proteção de dados por mais sofisticadas que sejam não servem para grande coisa se a segurança física não for garantida.

Por mais seguro que o seu ambiente seja, ela não estará seguro da pessoa que deseja invadir o seu sistema se ele (a) tiver acesso físico ao mesmo (OLIVEIRA, Wilson. Pág. 58).

As pequenas e a médias empresas têm seus dados armazenados, geralmente, em servidores de rede ou em estações compartilhadas, e o acesso físico a estes equipamentos nem sempre é restrito. Na maioria das vezes, esse mesmo servidor ou estação possui acesso liberado e ilimitado à Internet, o que aumenta o risco de um incidente de segurança. Na média empresa, o cenário é menos problemático, porém não o ideal, principalmente, devido à conscientização dos funcionários sobre segurança da informação.

O controle de acesso aos recursos de TI, equipamentos para fornecimento ininterrupto de energia e firewalls são algumas das formas de se gerir a segurança desta camada (NETTO, Abner da Silva; SILVEIRA, Marco Antonio Pinheiro, 2007).

2.3 ATAQUES VIRTUAIS

Conforme a pesquisa realizada pela CERT (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), o aumento de ataques registrados entre 1999 a 2014 no Brasil, aumentou de forma expressiva. Isso mostra em gráfico comprovado, que com o passar dos anos e a evolução da tecnologia, o interesse por pessoas não autorizadas de acessarem arquivos de outras pessoas/empresas, ficou cada vez maior. E isso, é uma prova clara para os administradores de redes aplicarem e assegurar a segurança de seus sistemas corporativos ou pessoais.

Abaixo, na Figura1, podemos observar o gráfico com o aumento expressivo de ataques.

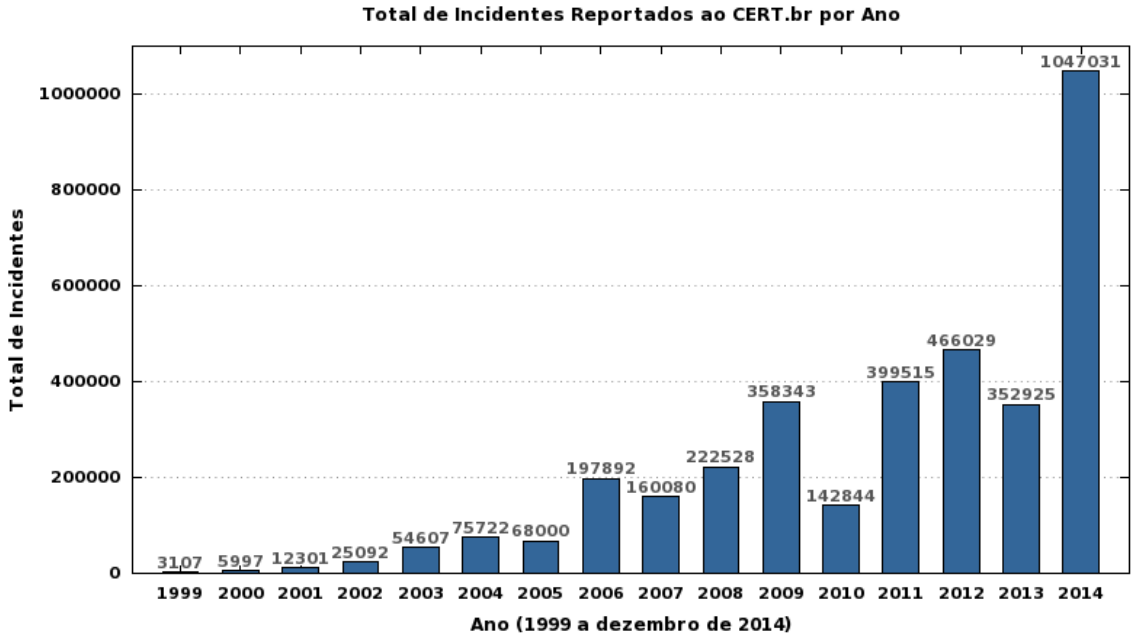

Figura 1 - Total de incidentes Reportados ao CERT.br por ano.

Fonte: CERT.BR – Estatísticas dos Incidentes Reportados ao CERT.br, 2015, 2015.

De acordo com a pesquisa da CERT abaixo, segue as principais ameaças reportadas entre Janeiro a Dezembro de 2014:

Ataques de Negação de Serviço

* Recebemos, no ano de 2014, 223.935 notificações sobre computadores que participaram de ataques de negação de serviço (DoS). Este número foi 217 vezes maior que o número de notificações recebidas em 2013;

* Notamos que grande parte das notificações dos ataques de DoS envolvem protocolos de rede que podem ser utilizados como amplificadores, tais como: CHARGEN (19/UDP), DNS (53/UDP), NTP (123/UDP), SNMP (161/UDP) e SSDP (1900/UDP). Juntos, estes cinco protocolos correspondem a mais de 90% das notificações de DoS.

Tentativas de Fraude

* As notificações de tentativas de fraude, em 2014, totalizaram 467.621, número cinco vezes maior que o de 2013;

* As notificações de casos de páginas falsas de bancos e sites de comércio eletrônico (phishing clássico) em 2014 cresceram 80% em relação a 2013;

* As notificações sobre Cavalos de Troia, utilizados para furtar informações e credenciais, tiveram um crescimento de 4% em relação ao ano de 2013;

* Notamos que em 2014 o número de notificações de casos de páginas falsas que não envolvem bancos e sites de comércio eletrônico teve um aumento de 73% em relação a 2013. Nesses casos estão incluídos os serviços de webmail e redes sociais por exemplo;

* Em 2014 recebemos 340.374 notificações relacionadas a eventuais quebras de direitos autorais, este número foi sessenta e sete vezes maior que o do ano de 2013. A maior parte das notificações foram recebidas entre junho e novembro de 2014.

Ataques a servidores Web

* No ano de 2014 houve um aumento de 54% nas notificações de ataques a servidores Web em relação a 2013, totalizando 28.808 notificações;

* Os atacantes exploram vulnerabilidades em aplicações Web para, então, hospedar nesses sites páginas falsas de instituições financeiras, Cavalos de Troia, ferramentas utilizadas em ataques a outros servidores Web e scripts para envio de spam ou scam;

* Continuamos a observar durante o ano de 2014, uma grande quantidade de notificações de ataques de força bruta contra sistemas de gerenciamento de conteúdo (Content Management System - CMS), tais como WordPress e Joomla. Estes ataques foram, em sua maioria, tentativas de adivinhação das senhas das contas de administração destes sistemas.

Varreduras e propagação de códigos maliciosos

* As notificações referentes a varreduras chegaram a 263.659 em 2014, representando um aumento de 59% em comparação ao ano de 2013;

* As notificações de varreduras de SMTP (25/TCP), que em 2013 eram 35% do total, continuam em destaque e agora correspondem a 24% de todas as varreduras;

* Os serviços que podem sofrer ataques de força bruta continuam sendo visados. SSH (22/TCP) corresponde a 21% das notificações de varreduras de 2014, FTP (21/TCP) a 12% e TELNET (23/TCP) a 10%. Desde o terceiro trimestre de 2011 o serviço de RDP (3389/TCP) tem sido visado, correspondendo agora a 4% das notificações de varreduras de 2014;

* As varreduras de TELNET (23/TCP) parecem visar equipamentos de rede alocados às casas de clientes, tais como modems ADSL, cable modems, roteadores Wi-Fi, etc.

* Observamos durante o ano de 2014 o crescimento de varreduras de SIP (5060/UDP). No ano de 2012 representava menos que 0,7% do total de

varreduras mas saltou para 2,1% no ano de 2013 e agora representa 2,3% das notificações recebidas;

* O SIP é um protocolo de comunicação muito utilizado na transmissão de Voz sobre IP (VoIP). O protocolo SIP é amplamente utilizado por dispositivos multimídias e centrais telefônicas. Estudos apontam que boa parte das varreduras ao protocolo SIP destinam-se a centrais telefônicas onde busca-se abusar a infraestrutura VoIP e utilizá-la de maneira indevida;

* As notificações de atividades relacionadas com a propagação de worms e bots (categoria worm) totalizaram 42.191 em 2014, aumentando 51% em comparação com 2013.

Computadores comprometidos

* Em 2014 recebemos 6.509 notificações de máquinas comprometidas. Este total foi 42% menor do que o número de notificações recebidas em 2013;

* A grande maioria das notificações de computadores comprometidos foi referente a servidores Web que tiveram suas páginas desfiguradas (defacement).

Outros incidentes reportados

* Em 2014 recebemos 14.308 notificações que se enquadram na categoria "outros", correspondendo a um número 67% menor que o total de 2013 (CERT. br - Centro de Estudos, Resposta e Tratamento de incidentes de Segurança no Brasil, 2015).

3 ESTUDO DE CAMPO

Este capítulo apresentará algumas técnicas de Hardening aplicada por outros autores, que foram publicadas em artigos ou monografias. Será realizada uma análise de cada técnica, e apresentado ao leitor suas vantagens e desvantagens.

3.1 HARDENING EM SERVIDORES WINDOWS

Analisando o artigo realizado por Léo Victor Nascimento da Cruz e Wilson Antônio dos Anjos Ribeiro, em 2013, foi realizado técnicas de Hardening em servidores Windows. Em uma empresa, eles analisaram quais as ferramentas e técnicas de seguranças que já estavam aplicadas nos servidores, e as possíveis falhas. Após coletar os dados, apresentaram para a empresa quais os problemas encontrados, e apresentaram soluções com outras técnicas de Hardening, para garantir total segurança do equipamento sem grande investimento.

O objetivo dos autores é deixar o servidor Windows preparado para tentativas de ataques, e, com a utilização de ferramentas identificarem de forma ágil, possíveis falhas de segurança que ocorreram no sistema ou nos dados armazenados, aplicando uma correção.

3.1.1 MÉTODOS UTILIZADOS

Para realizar a análise de vulnerabilidades do servidor Windows, foi utilizada a ferramenta MBSA, que consegue identificar e apontar falhas como: senhas fracas, vulnerabilidades do SQL e IIS. Para assim, deixar o sistema do servidor cada vez mais seguro.

Para criação de políticas de segurança no servidor, foi utilizado a ACS, que torna possível obter as informações do servidor e apresentar ao usuário uma opção de solução a ser aplicada ao sistema de destino.

Já na parte de atualização dos aplicativos e do sistema operacional da rede, os autores decidiram utilizar o software WSUS, pois além de deixar toda a parte sistêmica atualizada, consegue emitir relatórios para o usuário informando quais atualizações estão faltando, minimizando assim, chances de um possível acesso não autorizado nos aplicativos da empresa.

As portas e serviços não utilizados no servidor, e que estavam liberados, foram desativados, pois muitos dos ataques são realizados através desses pequenos detalhes que muitos administradores esquecem em seus sistemas. Desativando também, contas que são criadas automaticamente pelo sistema, e que podem ser utilizadas para fazer login indevido no sistema.

Foi configurada uma política de auditoria também nos servidores, para controlar quem e quais dados foram alterados no sistema, mapeando alguns eventos que devem ser registrados e auditados. Tais como:

Auditoria da conta de eventos de Logon.

Auditoria de gerenciamento de contas.

Auditoria de acesso ao serviço de diretório.

Auditoria de acesso a objetos.

Auditoria da política de mudanças.

Auditoria de uso de privilégios.

Auditoria de acompanhamento de processos.

Auditoria dos eventos do Sistema.

Através do levantamento desses dados, é possível identificar as falhas e correções de alguns problemas no servidor.

Como antivírus, foi utilizado o NAP, uma ferramenta que possibilita o usuário a isolar o vírus, impedindo que ele contamine as demais máquinas que estão na rede. Possui uma regra de politica que limpa as máquinas afetadas pelos vírus, e só permite o acesso a rede novamente quando o sistema identificar que a máquina esta protegida sem nenhuma falha novamente.

Buscando a solução de mobilidade para o usuário, caso o mesmo solicite realizar um acesso ao servidor remotamente, é utilizado o SSTP, um protocolo para conectar o usuário remotamente no sistema através da VPN.

Esta solução, permite a pessoa acessar de um local externo, o ambiente da empresa como se estivesse fisicamente em sua empresa.

Para ter o controle dos acessos realizados nos sistemas, foi habilitado o NetLogon no servidor. Um serviço que verifica logins dos usuários, registros e autenticação no sistema. É possível através do NetLogon gerenciar a replicação das contas dos usuários no banco de dados e realizar backups.

3.1.2 VANTAGENS E DESVANTAGENS

A solução aplicada pelos autores Léo Victor Nascimento da Cruz e Wilson Antônio dos Anjos Ribeiro, em 2013, foi muito bem executada. Além de suprir as necessidades da empresa, conseguiram apresentar um projeto de baixo custo.

Uma das grandes vantagens dessas soluções de Hardening, é a utilização dos softwares gratuitos, o qual não vai gerar custo nenhum para a empresa, e os usuários podem explorar livremente as ferramentas disponíveis para o trabalho no dia a dia. Vale ressaltar, que as técnicas de Hardening aplicada neste caso, visa endurecer a máquina nos mínimos detalhes possíveis. Dificultando ao máximo qualquer tentativa de invasão ou acesso não autorizado no sistema. Deixando assim, a máquina preparada para enfrentar as ameaças atuais que temos nos dias de hoje.

Por se tratar de um ambiente Windows, os softwares utilizados são totalmente compatíveis com o sistema operacional do servidor. Embora a solução seja aplicada em um ambiente Windows Server, não há nenhum tipo de incompatibilidade com as ferramentas.

Apesar de o sistema operacional ser Windows (é necessário obter uma licença para utilização do software. Ou seja tem que realizar a compra, pagar o produto), é muito bem avaliado por todos os usuários que usam. Devido o projeto procurar o menor custo possível, a utilização de um sistema pago é uma grande desvantagem em meu ver. Poderia ter sido utilizado um sistema gratuito, como Linux.

3.2 HARDENING - BLINDANDO UM SERVIDOR GNU/LINUX

Analisando o artigo publicado pela revista Infra Magazine, Edição 1, foi levantado pelos autores algumas técnicas de Hardening para servidores GNU/Linux. Devido a diversas tentativas de ataques cibernéticos que ocorrem nos dias de hoje, o risco de invasão é igual para todos os tipos de sistemas operacionais. Sejam eles gratuitos ou pagos. E para cada situação, é possível encontrar soluções de segurança que mais se adaptam melhor. Neste artigo, as técnicas demonstradas são para um sistema operacional “Free”. Ou seja, um sistema operacional que é gratuito e que possui código aberto para o usuário, tendo total controle da ferramenta para modificar suas configurações.

Tendo como objetivo preparar um servidor GNU/Linux para enfrentar qualquer tipo de ameaça que apresente no dia. Impedindo ataques ou acessos de usuários não autorizados a utilizar o sistema. Protegendo assim, a integridade e confidencialidade dos dados, dentre outros itens que ira melhorar o rendimento do sistema.

3.2.1 MÉTODOS UTILIZADOS

Os autores tomam como primeira técnica de Hardening, realizar repartição no disco do servidor. Ou seja, separar os dados e serviços utilizados no servidor em partes. Pois, caso tenha o risco de danificar algum serviço ou infectar algum dado, ira atingir somente a partição que esta o dado atacado. Assim, caso aconteça o pior, os danos serão minimizados.

Como o sistema operacional Linux é aberto para os usuários, um software gratuito, ele possui vários serviços que são ativos por padrão do software, os quais facilitam as invasões e ataques de pessoas não autorizadas. Nesta solução, é orientado também o usuário a desativar os serviços desnecessários e inseguros. Tais como: telnet, rshd, rlogind, rwhod, ftpd, sendmail, identd, wget, dentre outros.

Quando um novo sistema é instalado, é normal que alguns aplicativos sejam ativados e ao mesmo tempo, liberando portas que podem expor o sistema. Pensando nesse problema, foi aplicada uma técnica junto ao software NMAP, que realiza uma busca em todo o sistema operacional do equipamento procurando por essas portas abertas e suas vulnerabilidades. É possível o administrador de redes obter via software, uma lista com todas as portas abertas, e definir uma regra de segurança. Se desejar permitir que ficassem abertas, ou que sejam bloqueadas através de um firewall.

Os acessos aos sistemas dependem de autenticações. Ou seja, o usuário que estiver acessando deve fornecer um nome de usuário e uma senha pessoal para conseguir acessar a aplicação. Porém, em muitos casos os usuários utilizam senhas fracas e fáceis de serem quebradas. Permitindo assim, que pessoas não autorizadas acessem os sistemas como se fossem usuários internos. Pensando nesse quesito, a solução foi utilizar o software John the Ripper, com a finalidade de encontrar essas senhas consideradas fracas.

Através dessa ferramenta, o administrador consegue ficar ciente de qual usuário esta com a senha vulnerável, e solicitar ao mesmo que altere para uma nova com um padrão de segurança definido internamente. Talvez essa técnica para alguns leitores possa parecer bastante conhecida, e muitos ainda pensem que nem exista esse risco. Mas isso é um engano, é normal em várias empresas os usuários utilizarem senhas como o exemplo: 123456, abcdef, datas comemorativas e etc. Essa é uma técnica de Hardening muito eficiente e

que é possível acompanhar o resultado com o passar do tempo e conscientização dos usuários. Tornando assim, o sistema mais preparado para enfrentar os ataques que podem vir ocorrer.

Existem três tipos de contas que são criadas por padrão em um sistema GNU/Linux conforme a revista Infra Magazine. São elas: Usuários comuns, usuários de sistema e o ROOT. É considerada uma conta de usuário comum, os usuários que possuem uma senha pessoal para entrar nos sistemas e acessar suas permissões de acordo como esta liberada para o seu perfil. Os usuários de sistema são aqueles que controlam requisições de serviços. E o ROOT, é o administrador do sistema. É necessário o administrador de rede quando for criar contas de usuários no sistema, definir exatamente o perfil adequado para cada pessoa, e autorizar somente os acessos necessários. Pois, a segurança do sistema deve valer tanto externamente como internamente.

Considerando que o usuário ROOT é o mais importante do sistema e capaz de realizar todas as alterações possíveis no servidor, automaticamente é a conta mais procurada por usuários mal-intencionados. Uma boa técnica a ser aplicada é desativar o login da conta root em terminais que apresentam modo texto. Obrigando assim, o usuário a realizar o login com uma conta sem privilégios exclusivos.

Continuando na mesma abordagem de contas dos usuários, uma técnica de Hardening utilizada é a desconexão de usuários não autorizados. Ou seja, ao identificar a tentativa de algum acesso não autorizado, o administrador de redes deve desconectar imediatamente o usuário e realizar a desativação da conta. Dificultando assim, o acesso indevido. Porém, antes de realizar essas ações, é muito importante que o administrador de redes registre as evidências do ataque para caso necessário, apresente como provas de crime externo/interno.

O sistema GNU/Linux possui o gerenciamento GRUB, melhor definindo, é através dele que o usuário consegue realizar a inicialização do sistema operacional da máquina. Através dos autores desse artigo, se um usuário conseguir o acesso físico ao servidor poderá conseguir acesso de root se reiniciar o servidor, e, alterar a senha do root através do gerenciador de boot (GRUB). É possível evitar essa situação aplicando uma técnica de Hardenig, de criptografar a senha utilizada para acessar o GRUB. Através dessa técnica, é possível impedir uma pessoa não autorizada a iniciar o sistema em modo de segurança, e operar normalmente no sistema como um administrador. Uma técnica ótima é a ativação da função “TMOUT”, que tem como objetivo executar um logout automático no sistema caso o usuário se apresentar inativo perante o sistema em um tempo determinado pelo administrador de redes. Pois, existe uma grande possibilidade do usuário entrar no sistema, se ausentar

fisicamente do equipamento com sua senha no sistema acessando normalmente, e outra pessoa aproveitar essa ausência e realizar modificações.

Já na utilização dos serviços de redes, as técnicas utilizadas são: Autorizar o usuário a acessar somente endereços IPs identificados e liberados pelo administrador de rede e restringir o acesso SSH não permitindo que o acesso seja realizado através da conta ROOT.

Para um acesso remoto seguro no servidor, a técnica escolhida foi o acesso via SSH. Pois, possui o processo de criptografia, se diferenciando dos outros métodos (Telnet, rlogin) que não fornecem essa segurança para o usuário que esta utilizando.

3.2.2 VANTAGENS E DESVANTAGENS

As técnicas de Hardening implementadas em um servidor GNU/Linux através da revista Infa Magazie, são muito úteis. Pois, as técnicas se encaixam muito bem para uma rede empresarial, corporativa, como também para uma rede particular, domésticas. Isso é uma grande vantagem para quem procura uma solução simples independente do ambiente.

Devido a várias empresas nos dias de hoje procurarem grandes soluções sem precisar realizar grandes investimentos financeiros, esse é um grande exemplo que é possível ter uma rede segura sem ter gastos com os sistemas. Todos os softwares utilizados são de código aberto, ou seja, gratuitos. Não é necessário obter licença ou realizar pagamentos. Os usuários podem explorar livremente as aplicações sem limitações.

Se houver uma conscientização para os usuários que utilizam o sistema, as chances de ocorrer algum ataque interno são mínimas. Se todas as técnicas citadas acima forem aplicadas, um ataque externo dificilmente irá obter sucesso. Mas, basta uma falha interna, seja divulgar/emprestar uma senha do sistema para outro usuário, que a possibilidade de ocorrer algum dano ao sistema é enorme.

Os autores ressaltam muito sobre a segurança do acesso ao GRUB, e que os responsáveis pelo servidor devem também se proteger com a segurança física do equipamento. Mas, em nenhum momento listam técnicas de Hardening para segurança física do servidor. Não adianta proteger o sistema apenas internamente, se sua parte física fica totalmente exposta para todas as pessoas.

Podemos considerar abaixo algumas técnicas de segurança física:

Monitoramento 24x7: Ter uma monitoração do espaço físico 24 horas por dia nos 7 dias da semana. Pode ser utilizado câmeras de segurança, vigilantes humanos.

Riscos ambientais - Preparar o ambiente que o equipamento irá ficar alocado para as possíveis causas: Incêndio, Problemas elétricos (Disponibilização de um Nobreak), Fumaças e gases, Inundações, Vandalismo.

Redundância dos equipamentos: Todo equipamento e toda peça tem um tempo útil de vida, ou seja, não funciona para sempre. É necessário planejar a redundância para todos os equipamentos caso venha ocorrer alguma falha técnica. Substituir o equipamento e rodar uma configuração já predefinida minimiza expressivamente o impacto do problema.

Basta algum acesso físico não autorizado para acabar com toda a segurança lógica realizada no servidor. Portanto, esse é o meu ponto negativo para esse artigo que alertou para tomar cuidado com a segurança física do servidor, mas não apontou nenhuma técnica a ser realizada.

4 CONSIDERAÇÕES FINAIS

A quantidade de ameaças que temos nos dias atuais na área de TI chega a ser exagerada. É verdade que não existe nenhuma rede ou equipamento 100% seguro, mas é possível sim se prevenir para as ameaças constantes. Devido às informações que trafegam pelas empresas, sendo que muitas delas são sigilosas, fazem os administradores de redes olharem de uma forma diferente para a segurança física e lógica da empresa referente à parte de tecnologia.

Com a pesquisa bibliográfica e o estudo de campo concluído, pode-se afirmar que é possível sim manter uma rede segura e preparar seu servidor para enfrentar diversas ameaças reais que existem hoje, através de técnicas de Hardening. E principalmente, com custo minimizado. Sendo esse um dos principais fatores que as empresas procuram uma ótima segurança para seus sistemas e seus equipamentos sem a necessidade de realizar um alto investimento financeiro. É possível afirmar através desta pesquisa também, que as técnicas de Hardening podem ser aplicadas em qualquer servidor independente do seu sistema operacional, seja ele gratuito ou não.

Recomenda-se a utilização de técnicas de Hardening e segurança física, em todos os sistemas e equipamentos que o usuário identificar a necessidade de proteger algum dado ou informação. Não se limitando apenas a servidores, e sim, falando de uma maneira geral. A segurança é importante para todos, e devemos estar prontos para todas as ameaças que podem aparecer em qualquer momento.

REFERÊNCIAS

AMARAL, Marcos Prado. **Segurança da informação em ambientes computacionais complexos: Uma abordagem baseada na gestão de projetos.** Disponível em <http://www.lsi.cefetmg.br/files/downloads/dissertacoes/2001-PPGTec-DissertMest-AMARAL_Marcos_Prado-20010925.pdf>

Acesso em 22/06/15

CERT. BR. **Estatísticas dos Incidentes Reportados.** Disponível em < http://www.cert.br/stats/incidentes/>

Acesso em 02/07/15

CERT. BR. **Análise de principais ataques virtuais.** Disponível em <http://www.cert.br/stats/incidentes/2014-jan-dec/analise.html>

Acesso em 02/07/15

ESPÍRITO SANTO, Adrielle Fernanda Silva. **SEGURANÇA DA INFORMAÇÃO.** Disponível em <http://www.ice.edu.br/TNX/encontrocomputacao/artigos-internos/aluno_adrielle_fernanda_seguranca_da_informacao.pdf>

Acesso em 21/06/15

GABBAY, Max Simon. **Fatores influenciadores da implementação de ações de gestão de segurança da informação: Um estudo com executivos e gerentes de tecnologia da informação em empresas do rio grande do norte.** Disponível em <http://www.repositorio.ufrn.br:8080/jspui/bitstream/123456789/14985/1/Max%20Simon%20Gabbay.pdf>

Acesso em 28/06/15

LEITE, Cristiano Monteiro. **Políticas de segurança física e lógica em ambientes institucionais que utilizam tecnologia da informação.** Disponível em <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/400/1/CT_GESER_1_2011_08.pdf>

Acesso em 09/06/15

MAGAZINE, Infra. **Segurança – Utilizando Hardening e Sistemas de Detecção de Intrusão.** Disponível em < http://www.devmedia.com.br/websys.5/webreader.asp?cat=62&artigo=3403&revista=inframagazine_1#a-3403>

Acesso em 18/06/15

NETTO, Abner da Silva; SILVEIRA, Marco Antônio Pinheiro. **Gestão da segurança da informação: Fatores que influenciam sua adoção em pequenas e médias empresas.** Disponível em <http://www.scielo.br/pdf/jistm/v4n3/07.pdf>

Acesso em 02/07/15

OLIVEIRA, Wilson. **Técnicas para Hackers - Soluções para segurança.** 2ª versão., Lisboa: Editora Centro Atlântico, 2003.

Acesso em 30/06/15

RIBEIRO, Wilson Antonio dos Anjos; CRUZ, Léo Victor Nascimento. **Hardening em servidores Windows: Fortalecendo seu sistema em alguns passos.** Disponível em <http://www3.iesam-pa.edu.br/ojs/index.php/sistemas/article/viewFile/1105/746>

Acesso em 16/06/15

SPANCESKI, Francini Reitz. **Política de Segurança da Informação – Desenvolvimento de um modelo voltado para instituições de ensino.** Disponível em < http://hotsites.cnps.embrapa.br/blogs/pesq/wp-content/uploads/2009/08/ist_2004_francini_politicas.pdf>

Acesso em 02/07/15

ZUCCO, Jeronimo Cleberson. **Hardening Linux Usando Controle de Acesso Mandatório.** Disponível em <http://www.seer.ufrgs.br/testeCPD/issue/viewFile/487/6>

Acesso em 11/06/15