Uma Análise da Segurança da Informação no Contexto da Vulnerabilidade Técnica do Painel Administrativo de um Website

Roney Damasceno Freitas[1], **Rhyan Ximenes de Brito**[2],
Janaide Nogueira de Sousa Ximenes[3]
Ronieri Nogueira de Sousa [4]

[1]Faculdade IEducare (FIED) – Rua Conselheiro João Lourenço, 406 -
Caixa Postal 62320-000 – Tianguá – CE – Brasil

[2]Instituto Federal de Educação, Ciência e Tecnologia do Ceará–(IFCE)
Av. 13 de Maio, 2081 – Caixa Postal 60040-531 – Fortaleza – CE – Brasil

[3]Mestrado Acadêmico em Ciências da Computação – Universidade Estadual do Ceará (UECE) –
Av. Dr. Silas Munguba, 1700 – Caixa Postal 60.714.903 – Fortaleza – CE – Brasil

[4]Faculdade IEducare (FIED) – Rua Conselheiro João Lourenço, 406 -
Caixa Postal 62320-000 – Tianguá – CE – Brasil

{roneyfreitas, rxbrito, nogueirajanaide, nsronieri}@gmail.com

Abstract. *On the Internet, large amounts of data travel, many of which are in secure environments, and managed only by authorized people who have credentials that allow them to be manipulated correctly. The present work addresses a study on security and information management with a focus on web applications. The overall objective of this study is to perform intrusion testing using a virtual machine together with the Kali Linux operating system through some tools to show vulnerabilities that exist in the administrative panel of a site.*

Resumo. *Na Internet trafegam grandes quantidades de dados, muitos deles estão em ambientes seguros e gerenciáveis apenas por pessoas autorizadas que possuem credenciais que permitem a manipulação de forma correta. O presente trabalho aborda um estudo sobre a segurança e gestão da informação com foco em aplicações web. O objetivo geral desse estudo é realizar testes de invasão utilizando uma máquina virtual juntamente com o sistema operacional Kali Linux através de algumas ferramentas com a finalidade de mostrar vulnerabilidades que existem no painel administrativo de um site.*

1. Introdução

Este trabalho está direcionado a gestão da segurança da informação voltado ao painel administrativo de um site, onde apenas pessoas autorizadas devem ter acesso ao gerenciamento das informações administrativas do site e terá o controle dos dados que serão expostos ao público em geral. A motivação para investigar tal temática, foi a participação como membro da equipe de desenvolvimento do site, tendo a percepção e vivência do quanto se faz necessário preocupar-se com a segurança e a integridade das informações na web. Dentro dessa perspectiva a segurança da informação é algo importante, pelo fato

de que criminosos estão sempre em busca de vulnerabilidades, que podem resultar em ataques ou mesmo ameaças. Assim as aplicações web sofrem constantemente com esses ataques que tem como objetivo adquirir acesso as informações confidenciais, podendo expor ou alterar tais informações.

Buscando-se, deste modo, uma clara abordagem na identificação dos elementos, os quais serão indagados para a contribuição do levantamento científico teórico, trazendo de forma clara e concreta a resolução para o problema exposto. Segundo [Dias 2000], a segurança visa proteger informações, sistemas, recursos e serviços contra manipulação não autorizada e desastres visando a redução do impacto e diminuir a probabilidade de incidentes de segurança.

Em uma abordagem de [Carneiro 2002], define segurança sendo, um conjunto de medidas e procedimentos, com o objetivo de proteger informações, contra destruição indevida, ou mesmo alterações de forma não organizada. Pode-se então, destacar com [Ferreira 2003], que a segurança da informação protege a informação dos diversos tipos de ameaças. Dessa forma a segurança da informação é de fundamental importância contra acessos indevidos de pessoas não autorizadas que possuem o objetivo de manipular as informações.

2. Conceitos Básicos de Segurança da Informação

As organizações, as quais fazem parte do meio tecnológico, estão constantemente sujeitas a exploração de vulnerabilidades, fazendo-se necessário o uso da gestão de segurança da informação com a finalidade de buscar a proteção das informações. A exploração dessas fraquezas é realizada por meios de ações de origem humana, que quando são exploradas estão sujeitas a identificar fendas, onde a partir desses pontos críticos pode-se produzir ataques, e logo, comprometer as informações, causando a perda de um ou mais pilares básicos da segurança da informação, como por exemplo a confidencialidade, disponibilidade, integridade e autenticidade.

A segurança da informação para [Sêmola 2014], é a proteção de diversos tipos de ameaças as informações, preservando seus atributos. Pode-se destacar que, ter um conhecimento mais aprofundado sobre os principais pilares da GSI(Gestão da Segurança da Informação) é essencial para entender de forma detalhada o conceito de segurança da informação.

De acordo com [RAMOS 2008], é definido o atributo de confidencialidade da segurança da informação como o sigilo da informação, então preservar a confidencialidade significa garantir que apenas as pessoas autorizadas poderão ter acesso. Diferentes tipos de informação terão diferentes necessidades em termos de confidencialidade. Já no que diz respeito a integridade, fato esse meramente importante para qualquer organização referente ao tratamento das informações, no qual [RAMOS 2008] destaca que a preservação da integridade envolve proteger as informações contra modificações em seu estado original. Essas modificações podem ser tanto intencionais quanto acidentais.

Quando se diz respeito a disponibilidade, quer dizer que a informação precisa estar disponível a todo o momento. [RAMOS 2008] aborda que uma informação disponível é aquela que pode ser acessada por aqueles que dela necessitam, no momento em que seja

necessário. Já para [Silva et al. 2003] , disponibilidade é vital ao acesso a informação, de modo que ter a informação necessária, mas não ter disponível no momento desejado, equivale a não possuir qualquer informação. É destacado também o atributo de autenticidade, onde o mesmo pode garantir a identidade de quem está enviando algum tipo de informação.

Uma ameaça pode ser considerada física ou virtual, podendo comprometer toda a segurança da informação, esse acontecimento pode ser causado por um fenômeno natural ou por uma simples ação humana. Entre as ameaças possíveis, pode-se citar criminosos virtuais e vírus. Segundo [Dias 2000] uma ameaça é um evento ou atitude indesejável, ou seja, roubo, incêndio ou vírus, que tem um potencial de remover, desabilitar, danificar ou destruir um recurso.

Na rede mundial de computadores atualmente existem milhares de aplicações disponibilizando algum tipo de informação e todas as informações consequentemente estão em um ambiente inseguro, onde qualquer tipo de vulnerabilidade na aplicação pode possibilitar explorações por atacantes virtuais, com possibilidades de gerar grandes prejuízos. Sistemas web (online) são os alvos preferidos dos usuários mal intencionados, pois estando diretamente ligado a Internet viabiliza ao criminoso virtual se aproveitar do ambiente de forma camuflada para estar explorando as vulnerabilidades em busca de falhas de segurança.

Os ataques são resultados de ações realizadas por invasores que utilizam de ferramentas como vírus, com a finalidade de roubar informações das vítimas. Essas ações são realizadas geralmente em ambientes virtuais, devido o rápido alcance as informações, altos ganhos e o baixo risco que os criminosos podem estar expostos. Ele se trata de um acesso não autorizado que pode fazer modificações nas informações. Um ataque corresponde a concretização de uma ameaça, podendo ser bem sucedida ou não, mediante uma ação deliberada e por vezes meticulosamente planejada [Marciano 2009]

Já o risco é a possibilidade de que aconteça alguma ação prejudicial, é a possibilidade de um perigo iminente, onde se materializa a chance de se executar alguma ação perigosa. Para [Sêmola 2014] o risco é a probabilidade de que agentes, que são as ameaças, explorem vulnerabilidades, mostrando os ativos a perdas de confidencialidade, integridade e disponibilidade, e causando impactos.

O termo criptografia vem das palavras kryptos (oculto) e graphein (escrita), conhecida por ser a ciência que estuda maneiras para codificar as mensagens deixando seu conteúdo de forma secreta. O termo criptografia não é ocultar a existência da mensagem, e sim deixar escondido o seu significado, esse processo é conhecido como encriptação [SINGH 2008].

Através do método de codificação da informação, torna-se mais seguro o envio de mensagens através da Internet, como e-mails ou transações bancárias e comerciais, levando em consideração que os dados trafegam por um ambiente público e vulnerável. A cada dia técnicas criptográficas são aperfeiçoadas, com o objetivo de buscar altos níveis de segurança e impedir que informações mesmo que interceptadas por criminosos, não poderão decifrar a informação contida na mensagem.

A criptografia é uma ferramenta extremamente importante para a sociedade, ela tem o objetivo de manter as informações confidenciais, proporciona integridade, auten-

ticidade e maior segurança. Atualmente existem vários sistemas criptográficos que são baseados em algoritmos, onde os mesmos são responsáveis em deixar os dados criptografados usando transformações complexas em sua execução, transformando um texto simples em um texto cifrado ou criptografado. Pode-se destacar alguns algoritmos importantes nesse processo criptográfico, como o DES (Data Encryption Standard), AES (Advanced Encryption Standard), RSA (Devido aos seus desenvolvedores Rivest, Shamir, e Adleman) e MD5 (Message-Digest algorithm 5).

3. Mecanismos de Segurança Implementados no Painel de Controle

Pensando na segurança das senhas dos usuários, foi realizado a implementação do algoritmo de função criptografia MD5 hash, utilizado para deixar as senhas armazenadas no banco de dados de forma cifrada, onde nem mesmo o próprio administrador ou um possível acesso indevido ao banco de dados, poderão ter acesso ao texto claro da senha e sim um texto cifrado, dificultando qualquer possibilidade de uso indevido com as credenciais dos usuários do sistema. Um dos sistemas de criptografia e autenticação que apresenta segurança computacional que é utilizado nas mais diversas aplicações é o algoritmo de chave pública MD5 [Azevedo 2006].

3.1. Forma de Autenticação

O método de autenticação utilizado foi baseado no reconhecimento do login e senha como mostra na Figura 1:

Figura 1. Tela de Login
Fonte: Elaborado pelos autores.

A Figura 2, mostra parte do código utilizado na implementação, responsável pela verificação de validação de usuários do sistema, onde é realizado o processo de recebimentos de nome de usuário e senha, para acesso ao painel. No código, a função empty tem como finalidade verificar se o usuário está passando dados vazios, caso isso aconteça a função evitará tal ação, a função addslashes tem a finalidade de retornar string com barras invertidas quando são usados caracteres indevidos que podem ser utilizados em ataques como SQL Injection, já a função md5 tem a finalidade de gerar a criptografia da senha ingressada e será verificada se a mesma corresponde a senha já gravada no banco de dados. Quando o usuário ingressa seu login e senha é submetida a uma verificação se os dados correspondem aos dados armazenados no banco de dados, caso essa verificação seja verdadeira o usuário terá acesso ao painel administrativo, caso contrário o acesso é evitado.

O processo de identificação define para o computador que realmente é o usuário e a senha corresponde a um autenticador, isto é, ela prova ao computador que o usuário é quem realmente ele diz ser [Santos and Silva 2012].

```php
<?php
    if(isset($_POST['entrar'])){
        if(!(empty($_POST['nome'])) && !(empty($_POST['senha']))){
            $nome =addslashes($_POST['nome']);
            $senha =md5(addslashes($_POST['senha']));
```

Figura 2. Implementação das variáveis de login e senha
Fonte: Elaborado pelos autores.

3.2. Controle de Usuário

Os usuários que têm acesso ao painel administrativo são controlados por níveis, onde o nível 1, corresponde aos usuários administradores do sistema, podendo realizar desde criação de usuários até a publicação e aprovação de conteúdos, o nível 2, corresponde aos usuários administradores que poderão apenas gerenciar a publicação e aprovação dos conteúdos a partir do painel.

login_user	nivel_user
Francisco	2
admin	1
Juliana	1

Figura 3. Niveis de usuário
Fonte: Elaborado pelos autores.

4. Simulações, Testes e Resultado de Ataques ao Painel do Site

Com o objetivo de verificar e futuramente corrigir falhas de segurança no painel administrativo do site, foram realizados alguns testes de invasão a fim de ganhar acesso a área administrativa do painel. Foram utilizadas algumas ferramentas para a exploração de vulnerabilidades e ataques onde o sistema operacional utilizado como cenário da realização das análises foi o Kali Linux instalado no ambiente virtualizado com o VirtualBox.

O ambiente é criado com um aplicativo de virtualização onde permite a instalação e execução de vários sistemas operacionais dentro de várias máquinas virtuais ao mesmo tempo, proporcionando também o compartilhamento do mesmo hardware. O sistema operacional Kali Linux é uma distribuição Linux baseada em Debian destinada a testes de penetração avançados e auditoria de segurança. O sistema contém várias ferramentas destinadas à realizar testes de segurança e adaptado especialmente as necessidades dos profissionais. Na figura 4, mostra a execução do Kali Linux na VM (Máquina Virtual).

4.1. Nessus

Após a preparação do ambiente, foi utilizado o software Nessus, um dos mais populares para realização de testes de análises de vulnerabilidades, com o objetivo de detectar os pontos considerados fracos em seus serviços de execução. [Pauli 2014] e [Weidman 2014], apontam que o Nessus é um dos scanners de vulnerabilidades disponíveis mais populares para realizar o passo de scanning de vulnerabilidades onde seu banco de dados inclui vulnerabilidades em plataformas e protocolos, e o seu scanner realiza uma série de verificações para detecção de problemas conhecidos. Na Figura 5 é mostrado os resultados realizado pelo Nessus no módulo de testes para aplicações web.

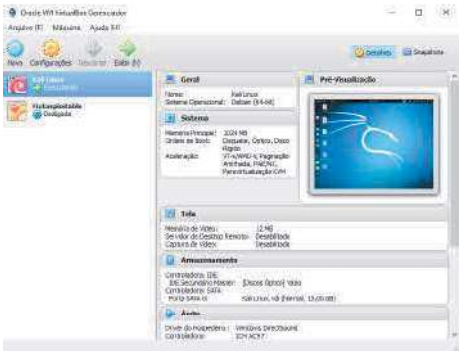

Figura 4. Execução do Kali Linux na VM
Fonte: Elaborado pelos autores.

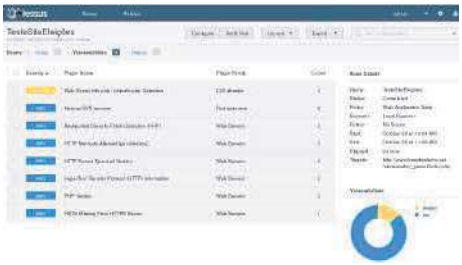

Figura 5. Histórico de vulnerabilidades encontradas pelo Nessus no Site
Fonte: Elaborado pelos autores.

Como pode ser observado na Figura 5, os resultados da varredura mostra que existem duas vulnerabilidades média e o restante apenas informações, onde os níveis são classificados como, crítico, alto, médio, baixo e informativo. Em relação as vulnerabilidades de nível médio encontradas o Nessus relata que, caso o arquivo php.info seja acessado por um invasor remoto ele pode descobrir uma grande quantidade de informações sobre o servidor web remoto, como o nome do usuário que instalou o php e se é usuário SUDO (possui todas as permissões do sistema), endereço do host, versão do sistema operacional, versão do servidor web, diretório raiz do servidor web e configuração sobre instalação remota do php. O Nessus mostra como solução para eliminar essas vulnerabilidades encontradas efetuar a remoção do arquivo afetado php.info.

4.2. Nmap

O Nmap tem como finalidade fazer varreduras no alvo a procura de portas abertas, serviços ativos, versões de sistemas operacionais e vários outros tipos de scan. Segundo [Pauli 2014], o Nmap é o scanner de porta popularmente mais utilizado e continua a ganhar destaque como o melhor scanner de portas do mundo, com funcionalidades adicionais para exploração de falhas e scanning de vulnerabilidades. Na Figura 6, mostra os resultados obtidos pela Nmap.

Como mostra a Figura 6, o comando executado ”nmap -sV -sS -O 186.202.153.147”realiza as seguintes ações: I- sV: designa o scan como um scan de versão, que mostrará como resultado as versões específicas dos serviços em execução. II- sS: inicia um scan camuflado, ou seja, ele descobre se uma porta está aberta sem se conectar totalmente com o alvo. III -O retorna informações referentes ao sistema operacional. o IP (Protocolo de Internet) 186.202.153.147 é equivalente ao domínio

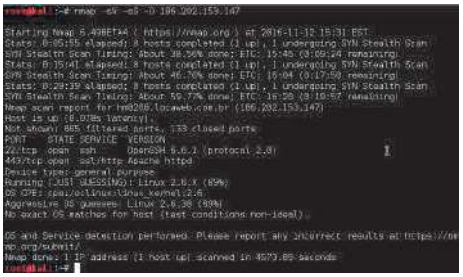

Figura 6. Resultados obtidos pela ferramenta Nmap
Fonte: Elaborado pelos autores.

http://www.brasilsystems.net/*. O resultado mostra duas portas abertas com seus respectivos serviços e versões, revelando também a existência de uma probabilidade de 89% que o sistema operacional é o Linux 2.6.38.

4.3. Nikto

O Nikto é uma ferramenta que tem o objetivo de constatar diversos tipos de arquivos, configurações de programas padrões e inseguros nos servidores web que podem ser passivos a algum tipo de ataque. [Pauli 2014], relata que o Nikto realiza verificações relativas a 6.400 arquivos e scripts potencialmente perigosos, 1200 versões desatualizadas de servidores e cerca de 300 problemas específicos de versões de servidores web, é um scanning de vulnerabilidades de código aberto. De acordo com [Weidman 2014], o Nikto é um scanner de vulnerabilidades de aplicações web, que procura problemas como arquivos perigosos, versões desatualizadas e erros de configuração. Na Figura 7, mostra os resultados obtidos pela ferramenta Nikto.

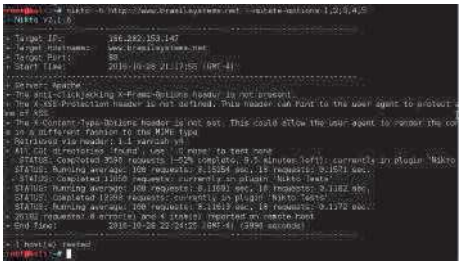

Figura 7. Resultados obtidos pela ferramenta Nikto
Fonte: Elaborado pelos autores.

Como pode ser observado, o comando realizado na Figura 7, foram executadas uma série de consultas simultâneas, com o objetivo principal de verificar todos os diretórios raiz, tentar adivinhar diretórios, enumera nomes de usuários via apache realizando força bruta em alguns serviços, lista nomes de usuários via CGI (Common Gateway Interface) e testa força bruta em subdomínios. De acordo com os resultados apresentados, alguns dados como o IP e servidor, apresenta que apenas alguns tipos de cabeçalhos não estão definidos, mas as principais consultas não conseguiram trazer resultados relevantes.

5. Considerações Finais

O presente trabalho apresentou conceitos sobre a segurança da informação além da realização de analises de vulnerabilidades ao painel do site. Nesse contexto sabe-se que

todas as aplicações web na Internet, estão suscetíveis a serem alvos fáceis para os criminosos virtuais, onde buscam por vulnerabilidades para a efetivação de seus ataques. Diante de tal fato, fica evidente a necessidade de buscar métodos de segurança que colaborem e contribuam contra a inibição de qualquer tipo de ataques contra aplicações web.

A realização de testes em aplicações web é de fundamental importância, pois é nesse processo onde se pode mensurar e precaver os riscos, evitando graves problemas de invasões. Durante a elaboração deste trabalho foram utilizadas de várias ferramentas para auxiliar na composição de ataques ao painel administrativo do site, com a finalidade de identificar suas vulnerabilidades.

Como sugestão de trabalhos futuros, serão analisados e testados novos métodos de ataques, com a finalidade de focar nos níveis de segurança da aplicação, de maneira a aprimorar mecanismos de autenticação, criação de usuários, senhas, métodos de criptografia, validação de formulários, dentre outros. Buscando sempre proporcionar a segurança da informação na aplicação, evitando qualquer tipo de ataques realizados por criminosos virtuais que venham a comprometer a segurança das informações.

Referências

Azevedo, M. S. S. (2006). *Protocolo Híbrido para Autenticação Quântica de Mensagens Clássicas com uso do Gerador de Seqüências Pseudo-aleatórias Blum-Blum-Shub*. PhD thesis, Universidade Federal de Campina Grande.

Carneiro, A. (2002). *Introdução à segurança dos sistemas de informação*.

Dias, C. (2000). *Segurança e auditoria da tecnologia da informação*. Axcel Books.

Ferreira, M. (2003). Propaganda eleitoral na internet.

Marciano, J. L. P. (2009). Segurança da informação: uma abordagem social.

Pauli, J. (2014). *Introdução ao Web Hacking: Ferramentas e técnicas para invasão de aplicações web*. Novatec Editora.

RAMOS, A. (2008). Security officer–1: Guia oficial para formação de gestores em segurança. *Segunda Edição. Porto Alegre–RS: Editora Zouk*.

Santos, D. L. R. and Silva, R. M. S. (2012). Segurança da informação: a norma iso/iec 27000 e iso/iec.

Sêmola, M. (2014). *Gestão da segurança da informação*, volume 2. Elsevier Brasil.

Silva, P. T., Carvalho, H., and Torres, C. B. (2003). *Segurança dos sistemas de informação: gestão estratégica da segurança empresarial*.

SINGH, S. (2008). O livro dos códigos. a ciência do sigilo-do antigo egitoa criptografia quântica. *Sétima ediçao*.

Weidman, G. (2014). *Testes de invasão: Uma introdução pratica ao hacking*. Novatec Editora.