12ª Jornada Científica e Tecnológica
INSTITUTO FEDERAL Sul de Minas Gerais
ISSN 2319-0124

ANÁLISE E LEVANTAMENTO DE POSSÍVEIS VULNERABILIDADES EM SEGURANÇA DA INFORMAÇÃO EM ÓRGÃOS PÚBLICOS NO SUL DE MINAS GERAIS

Anelize P. de SOUZA[1]; Augusto M. da S. JÚNIOR[2]

RESUMO

Este trabalho de pesquisa/extensão apresenta um estudo sobre a segurança da informação em recentes pesquisas em órgãos públicos heterogêneos. Objetivou-se avaliar o cenário tecnológico com foco em segurança da informação no setor público municipal do Sul de Minas. Para tal, analisou-se a correlação das falhas relativas à segurança da informação dos trabalhos convergentes realizados anteriormente no Campus Muzambinho. Esta análise seguiu como base a metodologia OSSTMM (Open Source Security Testing Methodology Manual). Ademais, com o auxílio de ferramentas para extrair informações e possíveis vulnerabilidades. Foram encontrados indícios de falhas de segurança nos sistemas como um todo, além de ter sido possível a criação de relatórios para os responsáveis com o que fora encontrado e possíveis soluções preventivas.

Palavras-chave: Órgãos públicos, Segurança da Informação, Teste de invasão.

1. INTRODUÇÃO

Com o avanço da web muitos dados são gerados a cada segundo, sejam eles de interesse pessoal ou empresarial. Além disso, a internet proporciona facilidades e uma série de benefícios para a sociedade. Contudo, Eleutério e Machado (2011, p. 16) completam que "com as vantagens, traz também a possibilidade de realização de novas práticas ilegais e criminosas".

Face às novas necessidades impostas pelos desafios dos novos tempos, pretende-se com este trabalho realizar uma análise de vulnerabilidades em Órgãos públicos do Sul de Minas deforma a identificar se existe alguma falha de segurança nos sistemas de informação. No final, os resultados serão entregues ao Gerente de Tecnologia da Informação ou responsável pelo setor, por meio de um relatório para que sejam tomadas as devidas medidas preventivas. Por fim, sugere incrementar e comparar os dados com pesquisas prévias realizadas no IFSULDEMINAS-Campus Muzambinho .

[1] Orientada, IFSULDEMINAS – Campus Muzambinho. E-mail: anelize.souza.286@gmail.com.
[2] Orientador, IFSULDEMINAS – Campus Muzambinho. E-mail: augusto.junior@muz.ifsuldeminas.edu.br

2. FUNDAMENTAÇÃO TEÓRICA

A informação pode ser definida como um conjunto de dados organizados que proporcionam sentido ou significado a um determinado contexto. Diante disso, o papel da segurança da informação é fundamental e está diretamente conectada com a proteção do conjunto de informações e dados processados, sejam estes de origem computacional ou não.

Por outro lado, as ameaças lógicas abrangem qualquer processo de natureza lógica, por exemplo: ataques de quebra de senha, vírus, escuta de dados (sniffers), entre outros (MORENO, 2015). Outrossim, segundo dados do cert[3], de janeiro a junho do ano de 2020, houveram mais de 318697 incidentes de segurança de informação reportados.

3. MATERIAL E MÉTODOS

A proposta da pesquisa se caracteriza como aplicada, de caráter descritiva e abordagem quantitativa. Quanto aos objetivos classificados como pesquisa exploratória. Classificando estas pesquisas como um estudo de caso, com intuito de conhecer o porquê de determinada situação, busca compreender o ponto de vista dos participantes.

Estabeleceu-se um termo de compromisso e confidencialidade, o qual expõe os interesses e responsabilidades, assim como a descrição da confidencialidade dos testes. Examinou-se os interesses do órgão público quanto aos possíveis testes dentro do prazo da realização do trabalho. Conforme Assunção (2014) destaca a importância deste documento, de forma a proteger legalmente o *hacker* ético, pois o *Penetration Test* pode levar ao comprometimento do sistema pela exploração de vulnerabilidades, o que pode ocasionar acesso a informações confidenciais. Foram comparados os trabalhos de 3 projetos de pesquisas em 3 ambientes heterogêneos para obtenção de um cenário que possa indicar o atual cenário existente em nossa região do Sul de Minas.

3.1 - Instrumentos

Dentro do proposto na metodologia OSSTMM[4] (*Open Source Security Testing Methodology Manual*) para a realização da pesquisa foram utilizadas ferramentas *online* e utilitários do sistema operacional *Kali Linux* que foram utilizados para realizar os testes de

[3]Disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/tipos-ataque.html

[4] Manual de referência que abrange áreas da segurança da informação, envolvendo a parte da segurança física, lógica e humana.

segurança e as suas respectivas finalidades.

4. RESULTADOS E DISCUSSÕES

Correlação dos resultados

Esta seção aborda, de forma resumida exemplificada em um quadro, a correlação dos resultados obtidos dos testes realizados nas Órgãos públicos dos trabalhos prévios (P1 e P2 respectivamente) e do presente projeto (P3), como apresenta-se no Quadro 1.

Quadro 1: Comparação dos resultados obtidos dos testes e suas respectivas ferramentas

Ferramenta	Resultado P1	Resultado P2	Resultado P3
The Harvester-Hunter	21 endereços de *e-mail* no *Site*	38 endereços de *e-mail* no *Site*	25 endereços de *e-mail* no *Site*
WhatWeb	Versão do servidor *web*, SO, *plugins*	Não foi constatado o uso	Servidor Apache, frameworks
Nmap (Zenmap)	Servidores: Versões desatualizadas; Portas e serviços vulneráveis	Foram analisadas as portas suspeitas, porém não foi encontrado algo relevante	Servidores: Versões desatualizadas; Portas e serviços vulneráveis
Nessus	Vulnerabilidades relacionadas: servidor Apache, serviço de compartilhamento de arquivo SMB e protocolo de acesso remoto SSH. Problemas de contas de usuários e de privilégios de acesso em arquivos	Existência de um arquivo que lista informações sobre o interpretador de PHP, executado no servidor. *Hosts* com versões obsoletas e vulneráveis ao SMB;	Possibilidade do *site* estar exposto ao ataque *clickjacking*[5] *Web Server info.php / phpinfo.php Detection* - instrui o usuário a criar um arquivo PHP que chame a função PHP 'phpinfo ()' para fins de depuração
Vega-Skipfish	88 vulnerabilidades altas, 7 médias e 3 baixas. Dentre elas, 9 relacionadas aos ataques de *SQL Injection*[6] e 7 relacionadas ao *Shell Injection*[7]	Problemas de conteúdos externos adicionados à página(arquivo este que lista informações sobre o interpretador de PHP que está sendo executado no servidor). *Framework* de desenvolvimento *Web* em PHP não recebe mais suporte	152 vulnerabilidades altas, 25 médias e 22 baixas. Nota-se que existem 133 relacionadas a *Shell Injection*

[5] Técnica fraudulenta para roubo de informações. Armadilha preparada para que o usuário clique no botão ou *link* infectado e é direcionado para página que pode baixar arquivos maliciosos para o computador da vítima.

[6] Técnica de ataque baseada na manipulação do código SQL(linguagem utilizada para troca de informações entre aplicativos e bancos de dados). O invasor pode inserir ou manipular consultas criadas pela aplicação, que são enviadas diretamente para o banco de dados.

[7] Injeção de comando é um ataque no qual o objetivo é a execução de comandos no SO através de um aplicativo vulnerável. São possíveis quando um aplicativo passa dados inseguros fornecidos pelo usuário (formulários, *cookies*, cabeçalhos HTTP, entre outros).

5. CONCLUSÕES

Após a realização dos testes e comparação dos resultados supra-citados, foi possível obter indícios de problemas de vulnerabilidades em diferentes órgãos públicos. Ademais, após os testes devidamente autorizados, foram entregues relatórios apontando as vulnerabilidades no sentido de contribuir de forma assertiva para correção deste cenário .

REFERÊNCIAS

ASSUNÇÃO, Marcos F. Segredos do Hacker Ético. 5 ed. Florianópolis: Visual Books, 2014.

DA VEIGA, Adele; MARTINS, Nico. Information security culture and in ormation protection culture: A validated assessment instrument. Computer Law Security Review, [S.l.], v. 31, n. 2, p.243-256, abr. 2015.

ELEUTÉRIO, Pedro M. S.; MACHADO, Marcio P.. Desvendando a Com putação Forense. São Paulo: Novatec Editora Ltda., 2011. 200 p.

MARANGONI, Vinícius H.. Análise e mapeamento de vulnerabilidades em uma prefeitura do sul de Minas Gerais. 2016. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – IFSULDEMINAS-Campus Muzambinho, Muzambinho, 2016.

MARTINS, Welington S.. Análise preventiva de vulnerabilidades em sistemas computacionais - um estudo de caso aplicado a uma prefeitura do sul de Minas. 2015. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – IFSULDEMINAS-Campus Muzambinho, Muzambinho,
2015.

MORENO, Daniel. Introdução ao pentest. 1. ed. São Paulo: Novatec, 2015. 294 p.
SILVEIRA, D. T.; GERHARDT, T. E. Métodos de pesquisa. Universidade Aberta do Brasil – UAB/ 91 UFRGS e pelo Curso de Graduação Tecnológica – Planejamento e Gestão para o Desenvolvimento Rural da SEAD/UFRGS, 2009.