11ª Jornada Científica e Tecnológica do IFSULDEMINAS & 8º Simpósio de Pós-Graduação

ANÁLISE E LEVANTAMENTO DE POSSÍVEIS VULNERABILIDADES EM SEGURANÇA DA INFORMAÇÃO EM UMA PREFEITURA NO SUL DE MINAS GERAIS

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

RESUMO

Objetiva-se avaliar o cenário tecnológico com foco em segurança da informação em uma prefeitura do Sul de Minas. Pesquisas recentes demonstram um aumento no número de incidentes. Por isso, a motivação para este trabalho surgiu ao se analisar a quantidade de equipamentos, sistemas e aplicações que possuem baixa segurança de dados, ocasionando riscos. Esta análise tem como base a metodologia OSSTMM (*Open Source Security Testing Methodology Manual*). Os resultados indicam recomendações e melhorias a serem realizadas, que serão entregues detalhadamente por meio de um relatório final contendo todas as informações das vulnerabilidades encontradas.

Palavras-chave: Órgão público; Redes de Computadores; Proteção dos dados.

1. INTRODUÇÃO

Com o avanço da *web*, 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". De acordo com os dados do *Digital Reporting* 2019, atualmente a população mundial é estimada em mais de 7,6 bilhões de pessoas e o número de usuários da *internet* ultrapassa 4,3 bilhões.

Segundo Da Veiga e Martins (2015, p. 8), o objetivo principal da segurança da informação é proteger a informação das ameaças que têm impacto sobre a continuidade do negócio. Com o intuito de mitigar ameaças digitais, existem diversos mecanismos e serviços que auxiliam nesse processo, contudo, alguns são realizados por profissionais da segurança da informação. Dentre os principais mecanismos, destacam-se: políticas de segurança da informação (PSI), normas ISO, teste de intrusão, capacitação dos funcionários contra engenharia social, entre outros.

Pretende-se com este trabalho realizar a análise de vulnerabilidades em uma prefeitura do Sul de Minas, de forma 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

[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.

responsável pelo setor, por meio de um relatório para que sejam tomadas as devidas medidas preventivas.

2. MATERIAL E MÉTODOS

A proposta da pesquisa se caracteriza como aplicada, conforme Silveira e Gerhardt (2009, p. 34), "objetiva gerar conhecimentos para aplicação prática, dirigidos à solução de problemas específicos. Envolve verdades e interesses locais". De caráter descritiva e abordagem quantitativa, pois os resultados obtidos podem ser quantificados com base na análise dos dados recolhidos.

Existem vários tipos de metodologias utilizadas em um teste de invasão, sendo cada uma com sua devida funcionalidade, ou seja, para cada escopo de projeto devem ser definidos testes corretos. A metodologia escolhida é a OSSTMM, que foi aplicada para o desenvolvimento deste projeto, a qual tem por objetivo apresentar um padrão metodológico prático e consistente de verificação e avaliação da presença de segurança da informação (MORENO, 2015).

2.1 VISÃO GERAL

Inicialmente é de suma importância as devidas autorizações e o conhecimento da infraestrutura da rede do órgão municipal. Para isso, estabeleceu-se um termo de compromisso e confidencialidade, o qual expõe os interesses e responsabilidades, assim como a descrição da confidencialidade dos testes. A autorização foi analisada pelo departamento jurídico da Prefeitura e assinada pelos responsáveis.

A prefeitura analisada localiza-se em uma pequena cidade no sul de Minas Gerais, cuja infraestrutura é composta por 30 máquinas que se distribuem pelos setores informatizados como: recursos humanos, administração, jurídico, engenharia, contabilidade, tributos, gabinete, controladoria, tesouraria e tecnologia da informação. São dois *switches* que distribuem a rede cabeada por todas as salas da prefeitura, comunicando entre si através de uma rede local 192.168.X.X/24. Também são compartilhadas algumas impressoras nessa mesma rede. Logo após, foram realizados os testes básicos para analisar as vulnerabilidades.

2.2 INSTRUMENTOS

Foram utilizadas algumas ferramentas *online* e utilitários do sistema operacional *Kali Linux* para a realização dos testes de segurança, das quais podem-se citar: *Host*, *Whois*, *Dnsenum*, *Meterpreter Framework*, *Netcraft*[3], *Nmap*, *Nessus*[4], *Vega*[5], *Skipfish*. Cada ferramenta com uma

[3]Verifica informações como hospedagem de sites e de servidores web. Disponível em: https://www.netcraft.com/
[4]Detecta falhas detalhadas em servidores, sistemas e redes. Disponível em: https://www.tenable.com/downloads/nessus

função específica objetivando o descobrimento de informações relevantes sobre a prefeitura, que poderão ser utilizadas para fins de testes, como por exemplo, identificar endereços de IP (*Internet Protocol*)[6], *e-mails*, servidores, versões de sistemas, portas e serviços vulneráveis. Destaca-se o uso do sistema operacional obsoleto e sua vulnerabilidade, conforme ilustra-se na Figura 1.

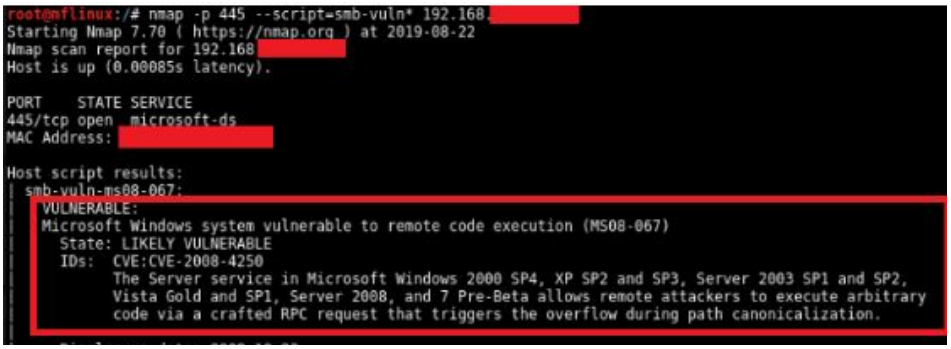

Figura 1: Saída do nmap-host vulnerável
Fonte: Autora

3. RESULTADOS E DISCUSSÕES

Após as análises, destacou-se a importância de tomar algumas medidas de precaução a curto e médio prazo. Pôde-se observar resultados como: versões desatualizadas de servidores de *e-mail* e *web*, ausência de segmentação de rede e de PSI. A atualização de sistemas e *softwares* é essencial para que todos os programas e aplicativos estejam em versões recentes. Além disso, é significativo aplicar boas práticas dos recursos de cabeçalhos e formulários no *site* da Prefeitura, para evitar exposição a ataques como SQL *injection*, *Clickjacking*/*Phishing*, conforme ilustra-se na Figura 2.

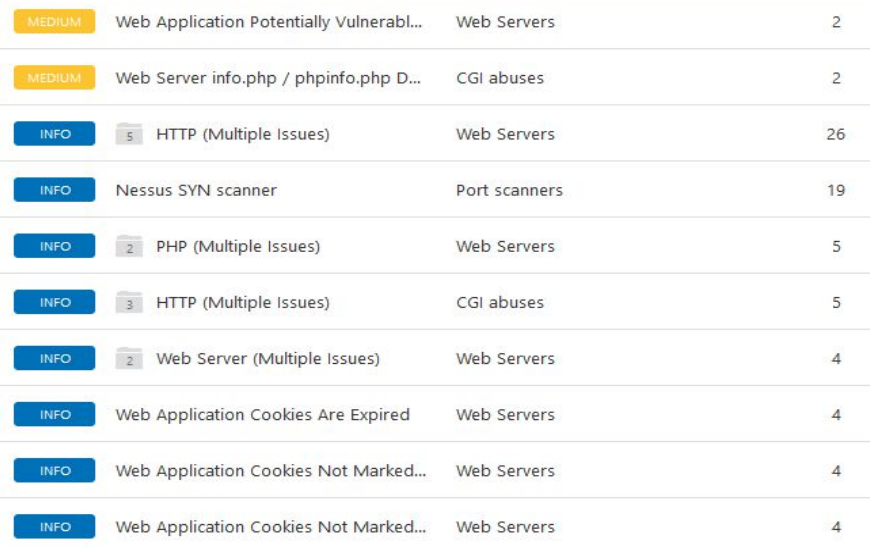

Figura 2: Saída do Nessus
Fonte: Autora

Em resumo, outras medidas a serem aplicadas são: restrição de acesso a setores críticos, para

[5]Reconhecimento e listagem detalhada de vulnerabilidades do site. Disponível em: https://subgraph.com/vega/
[6]Endereço numérico de identificação do dispositivo que se conecta na *internet*.

prevenir a rede contra intrusos que possuíssem acesso com privilégio regulado. Adquirir políticas de sistemas de cópias de segurança (*backup*). Recomenda-se o uso de sistemas atuais, e caso isto não seja possível por falta de orçamento direcionado a este fim, pode-se utilizar um sistema operacional gratuito, como as distribuições *Linux* atuais disponíveis na *internet.* Além disso, configurações padrões em ambientes de rede é um tipo errôneo de prática que pode colocar em risco os usuários da rede à ataques e táticas de invasão. A prefeitura analisada não possui ou não aplica políticas de segurança da informação, ocasionando vários problemas na instituição. Para reduzir riscos à segurança da informação, é altamente recomendado que algumas políticas de segurança da informação sejam implantadas.

4. CONCLUSÕES

Esta pesquisa teve como objetivo principal realizar indícios de vulnerabilidades em uma prefeitura do Sul de Minas. A segurança da informação inclui todas as condições que abrangem seu uso como processos, pessoas, sistemas, serviços, entre outros. De acordo com Moreno (2015, p. 17), os princípios básicos da segurança da informação são: confidencialidade, autenticidade, integridade, disponibilidade e legalidade. Violar estes princípios desintegram e colocam em risco a segurança da informação, podendo ocasionar a perda de todos os dados e acarretar a paralisação dos serviços prestados à população municipal. Em virtude dos fatos mencionados, acredita-se que a conscientização dos responsáveis de que a prevenção aos ataques faz-se necessária, pois sistemas frágeis podem constituir altos custos irreparáveis e prejuízos intangíveis.

REFERÊNCIAS

DA VEIGA, Adele; MARTINS, Nico. ***Information security culture and information 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 Computação Forense**. São Paulo: Novatec Editora Ltda., 2011. 200 p.

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/UFRGS e pelo Curso de Graduação Tecnológica – Planejamento e Gestão para o Desenvolvimento Rural da SEAD/UFRGS, 2009.