TESTE DE VULNERABILIDADES EM SISTEMAS WEB

Higor dos Santos MARTINS, Fábio Eder CARDOSO

Fundação Educacional do Município de Assis, Instituto Municipal de Ensino Superior de Assis, São Paulo-SP, Brasil

higor.dsm10@gmail.com, fabioeder.professor@gmail.com

RESUMO: Com o avanço das tecnologias, o desenvolvimento de sistemas para a Internet e o aumento de números de dispositivos conectados, pode-se ter acesso a diversos tipos de informações e dados, em tempo real. Essa conectividade está auxiliando as pessoas e as corporações a terem acessos a todas as informações e acontecimentos que ocorrem ao mundo inteiro, a qualquer hora e qualquer lugar. Contudo, a segurança da informação é um fator de grande importância, uma vez que as aplicações ficam disponíveis para todos e, assim, passíveis a ataques e manipulações por hackers. A falta de profissionais especializados em segurança para atuar na proteção e na mitigação dos ataques também contribui para o aumento dessa modalidade criminosa. Muitas empresas não investem em profissionais e equipamentos que auxiliam contra as ações maliciosas dos hackers, o que torna alvo fácil, e, por muitas vezes por falta de conhecimento e análise dos riscos que a falta deles faz, ou não investir por acreditar que tal fato não possa ocorrer. Este trabalho apresenta conceitos acerca de testes de vulnerabilidades de sistema.

PALAVRAS-CHAVE: Segurança da Informação, Hackers, Internet, Aplicações.

ABSTRACT: With the advancement of technologies, the development of systems for the Internet and the increasing number of connected devices, one can gain access to various types of information and data in real time. This connectivity is helping people and corporations gain access to all the information and happenings that occur worldwide, anytime, anywhere. However, information security is a major factor as applications are available to everyone and thus susceptible to hacking attacks and manipulations. The lack of security professionals to protect and mitigate attacks also contributes to the rise of this criminal modality. Many companies do not invest in professionals and equipment that help against malicious hacking actions, which makes them easy targets, and often for lack of knowledge and analysis of the risks that their lack does, or do not invest because they believe that fact cannot occur. This paper presents techniques and tools for system vulnerability testing.

KEYWORDS: Information Security, Hackers, Internet, Applications.

1. Introdução

Com o advento da Internet e dos dispositivos interconectados, dentre eles, dispositivos móveis, computadores e até televisões *"smart"*, houve uma preocupação maior com a segurança dos dados trafegados entre esses dispositivos e também, não obstante, a segurança com os servidores que proveem serviços e sistemas web *online*. Com isso tornou-se importante a presença de profissionais especialistas em segurança da informação, uma vez que estes, de forma ética, atuam profissionalmente provendo segurança a sistemas e *sites*.

De acordo com Moraes (2010) a segurança da informação pode ser conceituada como um conjunto de medidas com o objetivo de proteger e preservar informações e sistemas de informação onde toda e qualquer informação deve ser correta, precisa e estar disponível para ser armazenada, recuperada, processada e disponibilizada de forma segura e confiável

2. Problematização

A falta de segurança dos dados relacionados aos sistemas disponibilizados via Internet é um dos grandes desafios do desenvolvimento. A grande quantidade de dados gerados e recolhidos por uma multidão de páginas da web, torna a Internet quase um sub mundo de informações. A segurança dos sites é muito importante para a proteção dos arquivos, imagens, dados, vídeos sobre os usuários que utilizam aquele sistema. A alta quantidade de informações acessadas diariamente torna a extração e a integração um verdadeiro desafio. Fornecedores, contribuintes, empregadores, empresas de gestão, programas, mídias sociais e os próprios usuários são fontes em potencial para a coleta de dados.

3. Objetivos

3.1. Objetivo geral

O objetivo geral da pesquisa foi realizar estudo para demonstrar a necessidade e a importância da proteção dos sistemas de página web, a facilidade em burlar um sistema não devidamente protegido, e como se proteger e tornar seu sistema mais seguro. O uso das tecnologias de banco de dados e programação na forma adequada para combater essas ameaças virtuais. Demonstrar a capacidade das ferramentas de teste para obter informações do banco de dados e sistemas web por meio de técnicas e ferramentas para esse fim

3.2. Objetivos específicos

- Analisar o cenário tecnológico atual da Instituição e como a segurança da informação é tratada;
- Estudo de técnicas e conceitos no uso de ferramentas de exploração de vulnerabilidades web;
- Análise da importância de Pentesters e Hacker Éticos de forma a contribuir para a segurança de desenvolvimento para sistemas web.

4. Relevância/Justificativa

Em corporações que utilizam sistemas web para tratar seus processos informatizados, onde funcionários, clientes e fornecedores acessam o sistema como forma de trabalho, é extremamente importante que esteja com suas informações em segurança uma vez que se o sistema falhar ou entrar em colapso haverá muitas perdas e danos incalculáveis. Como forma de prevenção a estes ataques este projeto vislumbra o trabalho de testes de vulnerabilidades para que, desta maneira, possa ser implementado ferramentas que proveem maior segurança ao sistema resultando assim em um ambiente de trabalho mais seguro.

5. Revisão bibliográfica

5.1. Segurança da informação

Segundo o dicionário Aurélio, informação é o conjunto de dados acerca de alguém ou de algo, estendendo esse conceito, pode-se alegar que a informação é a interpretação desses dados. De nada vale um conjunto de dados sem que se faça a interpretação dos mesmos para se extrair um conhecimento útil.

"Pouco nos adiantará se conhecermos métodos de ataques e proteção de um sistema ou rede se não conhecermos os princípios básicos de segurança da informação. GIAVAROTO e SANTOS (2013, p.31)."

A segurança da informação se baseia em três princípios básicos que são:

Princípio da confidencialidade: este principio determina que apenas pessoas autorizadas possam ter acesso a determinadas informações. O acesso a um computador de forma "bruta" (por quebra de senha) para ser obter determinada informação seria uma violação deste princípio.

Princípio da Integridade: determina que uma informação que seja integra e que não foi modificada pode ser considerado uma informação confiável. A informação perde sua integridade a partir do momento que for alterada intencionalmente ou não. Exemplo: o aluno que tenta alterar sua média na escola de 4 para 10 em um sistema de notas estará adulterando a informação de forma intencional levando-a a informação perder a sua confiabilidade.

Princípio da Disponibilidade: define que a informação esteja sempre disponível a pessoa autorizada. Podemos considerar como violação deste principio um ataque de negação de serviço contra o servidor forçando - o a parar de funcionar levando as informações que se encontram nele a ficarem indisponíveis.

5.2. Protocolo TCP/IP

De acordo com TANEMBAUM (2003), o conjunto de protocolos TCP/IP foi criado pela DARPA (Defense Advanced Research Projects Agency) para fornecer a comunicação através da agencia. Os Estados Unidos da América queriam uma rede que pudesse sobreviver a qualquer guerra ou conflito, então criaram o TCP/IP, para garantir que os pacotes sempre chega-se ao seu objeto. Os protocolos TCP/IP são divididos em quatro camadas diferentes, sendo elas:

Camada de Aplicação: esta camada contém os protocolos de alto nível (HTTP, FTP, SMTP, entre outros). Todas as operações com esses procolos bem como suas propriedades, sessões e controle de dialogo são realizados nessa camada. Após o término do processo, os dados são empacotados e encaminhados para o próxima camada.

Camada de Transporte: responsável pelo controle de fluxo, confiabilidade e possíveis correções de erros na entrega de dados. Nessa camada encontram-se os protocolos TCP e UDP.

Camada de Internet: está camada possui a função de assegurar que os dados cheguem ao seu destino, independente do caminho (rotas) e das redes utilizadas para isso. O protocolo responsável por gerenciar está camada é o protocolo IP (Internet Protocol, que traduzido para o português fica Protocolo de Internet).

Camada de Rede ou Host-Rede: a tarefa desta camada é receber e enviar pacotes pela rede. Os protocolos utilizados nessa camada podem variar dependendo do tipo de rede que está sendo utilizado. Atualmente, o mais comum é o Ethernet.

5.3. Teste de vulnerabilidade web

Aplicações WEB podem ser consideradas como aplicações online, isto se refere à expansão e a facilidade do acesso a Internet, com o uso de computadores, smartphones, tablets, dentre outros. Por causa desta facilidade o risco de invasões e ataques são maiores. Quanto mais aplicações na rede, maiores as chances de ataques bem sucedidos. Já existem centenas de vulnerabilidades conhecidas, entretanto o tema ainda não é

tratado com a devida atenção; talvez pela falta de conhecimento das consequências que essas vulnerabilidades trazem.

A indiferença ou a falta de conhecimento em relação a este tema, as vulnerabilidades em serviços de redes disponíveis na Internet e o aumento crescente dos riscos aos usuários foram os principais motivos para a escolha do projeto, visando salientar a necessidade e a importância em criar aplicações mais seguras. Por meio de pesquisas na área, foram analisadas as mais conhecidas vulnerabilidades em aplicações Web, trazendo maiores detalhes de suas consequências e possíveis correções. Serão estudadas também algumas ferramentas que podem auxiliar na segurança por meio de um escaneamento completo da aplicação e identificação das vulnerabilidades encontradas. Um ataque bem sucedido em uma aplicação pode trazer grandes prejuízos, físicos ou morais aos usuários e as empresas, já que a gravidade desse ataque dependerá especialmente da experiência do atacante. As ferramentas que serão utilizadas poderão ser bastante eficientes se empregadas corretamente, e como resultado dos estudos e testes, será possível definir a melhor ferramenta, levando em consideração os recursos oferecidos, a flexibilidade, a facilidade, e os resultados obtidos nos referidos testes.

5.4. Definição de Pentest

Pentest é um conjunto de testes realizados em redes ou sistemas de computadores, podendo ser direcionado para websites, redes sem fio, banco de dados, aplicativos e programas. Sendo asssim esses testes são importantes normalmente para corporações a fim de descobrir as falhas existentes e a partir desse recurso é possível criar mecanismos de defesas para solucionar ou prover o menor prejuízo possível. (MORENO, 2015)

5.5. Fases do Pentest

De acordo com LEPESQUEUR e OLIVEIRA (2012) os testes de vulnerabilidade são divididos em 3 fases sendo eles, planejamento, execução e pós execução.

Planejamento: levantamento inicial de informações que serão utilizadas para realização dos testes, incluindo dados sobre a infraestrutura, recursos e equipamentos necessários para realização dos testes, definição de ameaças de interesse, controles de segurança,

planos de gerenciamento, requisitos, responsabilidades técnicas, metas, objetivos, fatores de sucesso, suposições.

Execução: fase onde são executados os testes, divide-se em: -Obtenção de informação: procedimento utilizado para modelar os ataques e definir caminho a ser utilizado na exploração. -Scanning e mapeamento: varredura e mapeamento da rede a partir das informações obtidas anteriormente. -Identificação de vulnerabilidades: após o mapeamento dos sistemas e serviços pertencentes a rede destaca-se as vulnerabilidades conhecidas ou processos que podem ser realizados para ter êxito na invasão, determinando possível impacto que cada uma pode causar -Ataques: realizados após identificar-se as vulnerabilidades obtendo acesso não autorizado com maior nível de privilégio possível

Pós-execução: etapa final dos testes de vulnerabilidades. Aqui é analisado todas as vulnerabilidades identificadas, reconhecendo causas e definindo recomendações de mitigação de tais vulnerabilidades e riscos. Observa-se a importância de se gerar uma documentação durante a execução dos testes com objetivo de se manter o registro de tudo o que foi feito de forma clara.

5.6. Pentest e sua utilidade

O principal objetivo de realizar o pentest é para explorar as vulnerabilidades e a partir dessas informações criarem métodos de prevenção, porém a importância de encontrar essas falhas é para garantir que dados confidencias de uma organização não seja exposta. Se um atacante obtém acesso a tais informações pode ocasionar várias consequências, que irá depender da vontade do criminoso virtual, sendo eles:

· O roubo de informações confidenciais para benefício próprio.

· Roubos de senhas do internet banking.

· Utilização do computador infectado como laranja, para que faça outros crimes virtuais.

· Instalação de arquivos ou vírus para acesso remoto (*backdoors*).

· Paralização de um servidor, causando perdas financeiras de faturamento.

O teste deve conter no escopo de um projeto de redes, sendo que um atacante pode utilizar de inúmeras formas para obter acesso à rede e se esta for invadida, pode-se ocorrer sérios danos à empresa e a equipe de TI responsável. (MORENO, 2015).

Uma das técnicas é o uso de ferramentas para descoberta de vulnerabilidades ou fase de escaneamento. Duas tecnologias utilizadas nesta fase são apresentadas a seguir.

5.7. Nmap

O Nmap (*Network Mapper*) é um *software* de código-fonte gratuito e aberto, possuindo suporte técnico e apoio da comunidade. A ferramenta foi desenvolvida e tornou-se um *scanner* de segurança de rede mais popular no mundo (MORENO, 2015).

Com o Nmap é possível:

Examinar portas - Identificação da versão/serviço que estejam utilizando determinada porta lógica do sistema;

Identificar quais pacotes/firewall estão em uso ou vulneráveis;

Determinar quais hosts estão disponíveis na rede;

Gerenciamento de agendas de atualização de serviço e monitoramento do tempo de atividade do host ou serviço.

O Nmap pode ser utilizado em todos os principais sistemas operacionais de um computador, além disso, a ferramenta é disponibilizado em duas distribuições, sendo elas via console (modo texto) e via interface gráfica através da ferramenta Zenmap.

Zenmap é a interface gráfica oficial para o Nmap, sendo também um *software* de código aberto e uma ferramenta flexível de transferência. A principal função de sua utilização é facilitar o uso do Nmap para iniciantes ao mesmo que pode oferecer opções avançadas para usuários que sejam mais experientes (MORENO, 2015).

5.8. OpenVAS

OpenVAS é considerado um scanner de vulnerabilidades composto com diversos serviços e ferramentas afim de obter o melhor resultado na busca por vulnerabilidades (PERINI, 2018). A ferramenta foi desenvolvida com a intenção de servir como alternativa à ferramenta Nessus, esta proprietária, após uma mudança de licença, sendo assim, passou a ter o código fonte fechado. O OpenVAS é um mecanismo *opensource*, é considerado de fácil utilização, desde que ocorram alguns ajustes. A aplicação desse mecanismo disponibiliza relatar quais vulnerabilidades estão presentes dentro de um *host*, além de sugerir possíveis soluções ao administrador, porém é necessário a utilização de *plugins*. Sua utilização é disponibilizada por interface, sendo acessada por meio de navegadores *web*, onde é possível configurar atividades executadas, detecções ou demonstrar resultados que foram obtidos (GODINHO, 2016).

6. Conclusão

O presente projeto proporcionou o conhecimento de técnicas de análise de vulnerabilidades em sistemas web, e também em tecnologias mais atuais existentes no mercado. Também ampliou a capacidade e a abstração de conhecimento para dar continuidade ao projeto e resultar, possivelmente, na escrita e apresentação do trabalho de conclusão de curso. Os conceitos acercaa de Redes de Computadores e Sistemas Operacionais também puderam ser aplicados e estudados. A princípio o projeto seria utilizado para aplicar as técnicas de descoberta de vulnerabilidades nos sistemas web da FEMA, entretanto, por questões de segurança, viabilidade e escalabilidade, ele foi apenas aplicado em um ambiente controlado, ou seja, em ambiente virtual.

Referências bibliográficas

AHARONI, Mati et al (2017) Kali Linux Oficial Documentation Disponível em: <http://docs.kali.org/introduction/what-is-kali-linux> Acesso em: 12 de novembro de 2018.

FILHO, Cróvis Luiz de Amorim; CAVALCANTI, Paulo Diego de Oliveira Bezerra; FILHO, Marcello Benigno de Barros Bargos (2008), SQL Injection em ambiente Web. Disponível em: <http://www.devmedia.com.br/articles/post-9733-SQL-Injection-em-ambientes-Web.html> Acesso em: 14 de novembro de 2018.

GIAVAROTO, Sílvio César Roxo; SANTOS, Gerson R. dos. BacktTrack Linux e Teste de Invasão em Redes de Computadores, 1. ed. Rio de Janeiro: Editora Ciência Moderna, 2013

GODINHO, Pedro Xavier Monteiro. *Preventive Vulnerability Scanner*: Sistema de detecção de vulnerabilidade em aplicações instaladas em sistemas Windows. 2016.

GUIMARÃES, B. D. A. e Stampar, M.. (2011) Sqlmap user's manual. Versão 0.9, 10 de abril de 2011. Disponível em: <http://sqlmap.sourceforge.net/doc/README.html>. Acesso em: 14 de novembro de 2018.

KUMAR, Chandar (2017) How to Find SQL Injection Attack Vulnarebility? Disponível em: <https://geekflare.com/find-sql-injection> Acesso em: 04 de dezembro de 2018.

LEPESQUEUR, Alexandre Mendes Alvim; OLIVEIRA, Italo Diego Rodrigues. Pentest, análise e mitigação de vulnerabilidades. 2012.

MACORATTI,José Carlos. Previna-se contra a injeção SQL. Disponível em : <http://www.macoratti.net/sql_inj.htm>. Acesso em: 09 de dezembro de 2018.

MCCLURE, Stuart at al, Hackers Expostos. 7ª ed. Editora Bookman. 2014.

MORAES, Alexandre F. Segurança em redes: fundamentos. São Paulo: Érica, 2010.

MORENO, Daniel, Introdução ao PENTEST, São Paulo: Novatec Editora Ltda, 2015

PERINI, Vinícius Lahn, *et al*. Integração de ferramentas de administração e segurança BYOD. 2018.

PYTHON SOFTWARE FOUNDATION.(2012) The Python Language Reference, versão 2.7, Disponível em: <http://docs.python.org/reference/>. Acesso em: 22 de novembro de 2018.

REVELLI, Alberto e ICESURFER. (2008) SQLNINJA ...a SQL Server Injection & takeover tool. Disponível em: <http://sqlninja.sourceforge.net/index.html>. Acesso em: 13 de novembro de 2018.

TANEMBAUM, Andrew. S. Redes de Computadores, 4ª edição. São Paulo: Saraiva, 2003.

WALL, Larry Online Perl Documentation, versão 24,0. Disponível em: <https://www.perl.org/docs.html>. Acesso em: 13 de novembro de 2018.