Análise de vulnerabilidade em servidores

Trabalho de Conclusão do Curso
Técnico em Informática

Gustavo de Moraes Grecco
Orientador(a): José Ricardo Borba

[1]Escola Técnica Estadual Marechal Mascarenhas de Moraes
Av Lídio Batista Soares, 700, Cachoeirinha – RS – Brasil

gustavogrecco3@gmail.com, jrborba.rs@gmail.com

Resumo. *Este trabalho apresenta o projeto e implementação do "MEU-SOFTWARE"que é um software para analise de vulnerabilidades em servidores web. O Software apresenta a analise de algumas falhas, classifica quais erros são de maior preocupação e cadastra um usuário para utilizar o software. Público Alvo: Profissionais que atuam na area de segurança da informação.*

1. Introdução

"Segurança nunca é demais", diz um ditado popular brasileiro e não é por menos já que nos últimos anos a taxa de latrocinio está aumentando e não é difícil encontrar notícias pela rede mundial de computadores abordando o assunto como mostram os sites do IG[IG 2017], Estadão[Estadão 2017], G1.com[G1 2017] e Veja online[Veja 2017],que noticiam crimes e mostram a realidade no Brasil. Sistemas informatizados, como a internet, também são vítimas de crimes, pois "HACKERS" atacam servidores de serviços pela internet para roubar de senhas, banco de bitcoins e informações(dados digitais), como pode ser conferido nos sites TecMundo[TecMundo 2017],CulturaMix[CulturaMix 2017] e Revista Exame[Exame 2017], que apresentam estatísticas e aborda amplamente o assunto "HACKER".Mas antes de prosseguir sobre crimes eletrônicos, primeiro é necessário esclarecer uma confusão comum entre leigos: O termo hacker é utilizado para descrever criminosos virtuais, o que é um erro, pois como descreve o site da Universidade Federal de Santa Catarina:

> *"HACKER é uma pessoa que possui um grande conhecimento informático e que se encontra em constante estudo sobre a área, capaz de invadir o sistema de outrem para entretenimento e aprendizagem, e não a fim de criminalizar, bem como auxiliar aqueles que não possuem seu conhecimento."*[UFSC 2017]

Logo, hacker é a definição de qualquer pessoa que tenha grande conhecimento sobre um determinado sistema(virtual ou real) e consiga usar as vulnerabilidades que o sistema possuir para melhorar seu conhecimento e assim ajudar quem está a merce dos problemas que o sistema apresentar. A notável universidade explica que:

> *"Cracker possui um alto grau de conhecimento informático, tendo como foco principal em seu estudo o funcionamento dos softwares (programas). São responsáveis pela criação dos cracks, que são ferramentas utilizadas na quebra da ativação de um software comercial, facilitando a pirataria. São definidos como criminosos, eis que operam*

> *em fraudes bancárias e eletrônicas, furto de dados, golpes, entre outros."*[UFSC 2017]

Isto posto, cracker é o criminosos que usa conhecimento para benefício próprio e crimes eletrônicos(já citados).Mas como um cracker usa as falhas de um sistema para satisfazer seu ego egoista? Não há uma resposta simples, mas sim um estudo longo, e divertido, que não será o foco deste artigo, porém este trabalho abrange alguns pontos mais utilizados por criminosos virtuais.
Para definir ameaça o Prof. Luís Rodrigo de O. Gonçalves escreve que:

> "Uma ameaça consiste de uma possível violação da segurança de um ambiente ou sistema."[de O. Gonçalves 2005]

e MEUSOFTWARE tem como objetivo analisar onde o sistema pode ser violado e neste trabalho vamos focar nas falhas de segurança em servidores WEB, servidor este que é "um software responsável por aceitar pedidos em HTTP de clientes, geralmente os navegadores, e servi-los com respostas em HTTP"[webdevelopersnotes 2017], ou seja, é o local que armazena as páginas da internet(em conceito leigo).
Analisar as possíveis falhas em servidores é fundamental para que o administrador do serviço possa corrigir falhas e prevenir perdas.
Wilson José de Oliveira escreve que:

> *"o invasor poderá fazer um teste de invasão, que é uma tentativa de invasão em partes, onde o objectivo é avaliar a segurança de uma rede e identificar os seus pontos vulneráveis."*[Oliveira 2003]

E assim pode escolher a melhor estratégia para cometer o crime pretendido.
A segurança de serviços web deve ser permanente para evitar abusos por criminoso, já que cada nova tecnologia poderá conter algum "bug"[Prada 2017] e como escreve Kevin D. Mitnick:

> "...os hackers estão achando novos pontos vulneráveis todos os dias."[e William L Simon 2005].

Análises são necessárias para visualizar falhas e hacking como descreve Christopher Duffy escreve:

> "Hacking não é uma auditoria, mas lida diretamente com o aproveitamento das vulnerabilidades exploráveis."[Duffy 2016]

tais vulnerabilidades são utilizadas por Crackers, então utilizando MEUSOFTWARE o profissional de segurança receberá um relatório com classificações das principais falhas existentes no seu sistema e pode consultar a qualquer momento ou lugar tal relatório, já que toda analise é salva em banco de dados.
As capacidades do MEUSOFTWARE: Novo cadastro de clientes, edição do cadastro, remover o cadastro, analisar portas do servidor, exibir pesquisa das vulnerabilidades conhecidas e retornar analise com classificação de vulnerabilidades.

2. Estado da Arte

É a descrição das funcionalidades dos principais e melhores softwares existentes no mercado.

2.1. Softwares líderes no mercado são:

1. Nessus;
2. OpenVAS(freeware);
3. Retina Network Security;
4. Nexpose;
5. GFI LANguard;

2.2. Descrição básica:

Segue resumo das principais funcionalidades:

Retina Network Security:

- Identifica vulnerabilidades conhecidas e imediatas para proteger bens valiosos de uma organização;

- Fornece avaliação de risco de segurança e permite a aplicação de práticas de segurança, fiscalização de políticas, compliance e auditorias regulatórias;

- Possui uma versão gratuita para teste limitada;

- Versão full do software paga;

- Exige uma boa quantidade de memoria RAM disponível no Computador em torno de 4 GB;

Nessus:

- O scanner de vulnerabilidades Nessus fornece revisão de patch, configuração e compliance auditing(auditoria de conformidade);

- Descoberta móvel, malware e botnet;

- Identificação sensível de dados e muitos outros recursos;

- Software proprietário muito caro.

Nexpose:

- Oferece visibilidade clara através da descoberta e avaliação de riscos para os negócios em ambientes físicos, virtuais e de nuvem.

- não realiza analise em alguns sites;

- Filtro de grupos não funcionam corretamente;

- Canais limitados ao site do fornecedor;

GFI LANguard:

- Permite a identificação e o escaneamento de portas;

- Gerenciamento de mudanças;

- Inventários de ativos de rede e auditorias de software;

- Não possui lista de prioridades;

- Scan de softwares depende do Sistema Operacional;

OpenVas:

- OpenVAS é uma estrutura de vários serviços e ferramentas que oferecem uma solução de vulnerabilidade e gerenciamento de vulnerabilidades.

- O framework faz parte da solução de gerenciamento de vulnerabilidades comerciais da Greenbone Networks da qual os desenvolvimentos são contribuídos para a comunidade Open Source desde 2009.

- Velocidade de escaneamento lenta;

- roda apenas em sistema operacional de codigo aberto;

MeuSoftware:

- É uma estrutura de serviço que pesquisa vulnerabilidades, classifica o resultado e salva o resultado em um banco de dados.

- Permite consulta do último relatório através de login de usuário. Realiza scan em portas de servidores web.

3. Referêncial teórico:

MEUSOFTWARE foi desenvolvido em python3, utiliza o banco de dados SQLite, software livre NMAP(port scan), HTML, CSS e JavaScript. Roda em um servidor. O usuário deverá acessar através de um browser compatível e conectará ao serviço através da url para realizar login e executar suas funcionalidades.
O Código fonte é escrito em Python, pois como diz Eric Matthes:

> *"Python é uma linguagem extremamente eficiente: seus programas farão mais com menos linhas de código, se comparados ao que muitas outras linguagens exigiriam. A sintaxe de Python também ajudará você a escrever um código "limpo". Seu código será fácil de ler, fácil de depurar, fácil de estender e de expandir"*[Matthes 2016]

Todos os sistemas operacionais com base em UNIX possuem uma versão pré-instalada(normalmente 2.7).

SQL é a linguagem utilizada para gerenciamento de banco de dados relacional.

NMAP é um serviço com licença livre que realiza scan de portas e serviços, está sempre atualizado e pode ser instalado em qualquer distribuição linux baseadas no debian.

HTML, CSS e JavaScript são as linguagens web mais famosas do mercado atual(2017) e são utilizadas para criar uma interface amigável para o usuário.

4. Metodologia e Proposta de solução:

Para realizar sua tarefa MEUSOFTWARE realiza conexão via internet com o servidor web alvo, coleta informações, compara com dados registrados no CVE[Corporation 2018](site oficial de vulnerabilidades conhecidas) e guardar as informações em um banco de dados relacional. Para executar o programa o usuário deverá inserir a url do site ou seu endereço ip no campo correto para então MEUSOFTWARE usar estas informações e executar o programa NMAP, que fará a varredura das portas do servidor e verificar quais serviços estão rodando em cada porta no servidor.Após termino da aplicação NMAP meu software coleta o resultado e busca na internet os riscos, consultando o site CVE[Corporation 2018] para classificar riscos. A classificação é baseada nas tabelas de riscos cadastradas no CVE[Corporation 2018], com uma nota variando de 0 a 10, onde 0 é baixo risco e 10 é alto risco para sofrer ataques. Esta busca e resultado são salvas em um banco de dados para que o usuário possa consultar sempre que logado no sistema, o usuário também pode fazer download em formato pdf escolhendo a opção de imprimir todas as vulnerabilidades como também limitar a faixa que deseja imprimir e assim o usuário poderá consultar o que deve corrigir.

5. Requisitos

5.1. Requisitos Não Funcionais:

1. Computador:
   - Sistema Operacional Windows 7 ou superior, linux e sistema mobile(Não testado);

2. Conexão banda larga de Internet:
   - Superior a 1 Mbps;
   - Conexão livre ao site do software e CVE;

3. Navegador de Internet:
   - Mozila FireFox(Versão 54 ou superior);
   - Google Chrome(versão 63 ou superior);

4. Servidor Web Alvo:
   - Endereço IP ou Nome do site do servidor analisado;

5. Acesso Site CVE:
   - Site do CVE[Corporation 2018] deverá estar online(acessível);
   - Não pode existir bloqueios/autenticações para acesso ao site CVE[Corporation 2018];

5.2. Requisitos Funcionais:

1. Cadastro de Usuários
   - Esta funcionalidade deverá permitir a inserção de novos usuários.
   - Os próprios usuários poderão selecionar a opção de criar conta no sistema.
   - Os dados cadastrados serão armazenados em um sistema de banco de dados informando: Nome, E-mail e Senha;

2. Editar Cadastro de Usuário:
   - Essa funcionalidade permite editar nome de login e e-mail de usuário já cadastrado;
   - O próprio usuário pode editar as informações cadastradas, selecionando a opção que deseja alterar;

3. Deletar usuário
   - Esta funcionalidade permite que o usuário delete seu cadastro no sistema;
   - O usuário seleciona a opção de excluir seu cadastro no sistema;
   - O usuário recebe um e-mail de confirmação que seu cadastro foi excluído;

4. Exibir Informações do Cadastro
   - Esta funcionalidade permite que o usuário cadastrado visualise suas informações cadastradas;
   - O usuário seleciona a opção (clica no link) de exibir as informações;
   -

5. Teste de Vulnerabilidade

   - Esta funcionalidade permite o software escanear as portas do servidor alvo;

   - O usuário deve informar o IP ou o nome do servidor para analise no campo indicado;

6. Apresentação do Resultado

   - Esta funcionalidade apresenta um relatório com nomes e nota das vulnerabilidades;

   - Salva as informações em um banco de dados;

   - Enviar e-mail com relatório do scan;

7. Consulta Escaneamento

   - Esta funcionalidade permite ao usuário consultar os dados obtidos após escaneamento salvas no banco de dados;

   - O usuário poderá visualizar uma tabela com os resultados obtidos;

   - O usuário poderá consultar vulnerabilidades pelo tipo de serviço, CVEID, nota ou palavras chaves presentes nos resumos do CVEID;

8. Imprimir Escaneamento

   - Está funcionalidade permite ao usuário gerar arquivos pdf da pesquisa;

   - O usuário poderá definir a faixa de notas para imprimir;

   - O usuário poderá imprimir a quantidade de notas(divididas por cor) e quantas o responsável marcou como resolvidas, bem como a comparação entre pendentes e total pesquisado.

6. Casos de uso

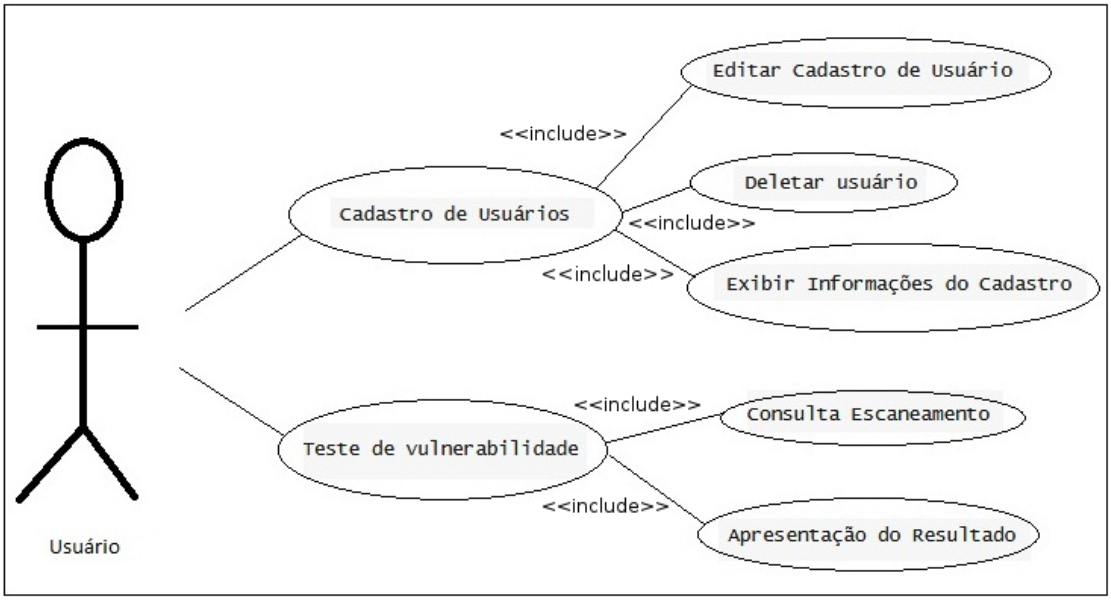

Figura 1. Casos de uso

7. Conclusão

Por fim MEUSOFTWARE possui CRUD completo para cadastrar usuários, editar informações, visualizar cadastro e deletar o cadastro do usuário, registra e realiza scan completo das portas do servidor alvo capturando os serviços de cada porta, salvando os dados da pesquisa em um banco de dados para assim permitir que o usuário possa visualizar e imprimir tais informações.Para melhor entendimento sobre o perfil hacker recomendo o livro *A arte de invadir - KEVIN D.MITICK e William L. Simon editora Prentice Hall*, para melhor entender a arte hacker. Sugiro também o livro *Guia do mestre Programador - Carlos Bueno - editora CASA DO CÓDIGO* ótima leitura para evitar a tentação de seguir o lado sombrio e evitar desanimar na busca pelo conhecimento.

8. Diagrama Entidade Relacionamento

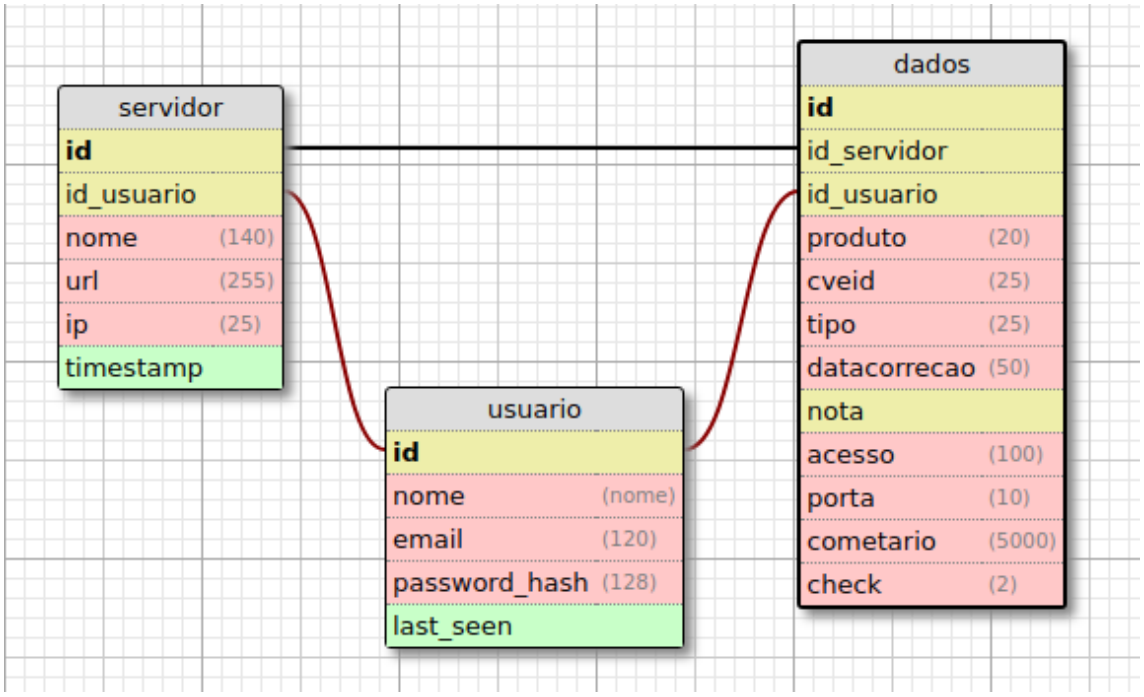

Figura 2. Diagrama Entidade Relacionamento

Tabela 1. Cronograma

Semana	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
RF1	X	X																
RF2			X	X														
RF3					X	X												
RF4							X	X										
RF5									X	X	X	X	X	X				
RF6															X	X	X	
RF7																	X	X

Referências

Corporation, T. M. (2018). Cve - common vulnerabilites and exposures. Disponivel em: <https://cve.mitre.org/>. [Acesso em: 29 de Janeiro de 2018].

CulturaMix (2017). **OS maiores ataque hackers da história**. Disponível em: <http://tecnologia.culturamix.com/noticias/os-maiores-ataques-hackers-da-historia>. [Acesso em: 15 de dezembro de 2017].

de O. Gonçalves, P. L. R. (2005). *Apostila do Curso de Segurança - DRAF*. Petrópolis,Rj - Brasil.

Duffy, C. (2016). *Aprendendo Pentest com Python*. Novatec Editora Ltda, São Paulo,SP - Brasil.

e William L Simon, K. D. M. (2005). *A arte de invadir: as verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos*. Pearson Prentice Hall, São Paulo,SP - Brasil.

Estadão, J. (2017). **latrocínios aumentam 58 porcento no País**. Disponível em: <http://brasil.estadao.com.br/noticias/geral,com-sete-casos-por-dia-latrocinios-aumentam-58-no-pais-em_-sete-anos,70002065437>. [Acesso em: 13 de dezembro de 2017].

Exame, R. (2017). **OS maiores ataque hackers da história**. Disponível em: <https://exame.abril.com.br/mercados/hackers-roubam-us-70-milhoes-em-bitcoins/>. [Acesso em: 15 de dezembro de 2017].

G1, G. (2017). **Aumento de latrocínios em SP em 2017 é o maior desde 2003**. Disponível em: <http://g1.globo.com/jornal-nacional/noticia/2017/08/aumento-de-latrocinios-em-sp-em-2017-e-o-maior-desde-2003_-diz-estudo.html>. [Acesso em: 13 de dezembro de 2017].

IG (2017). **Brasil tem recorde de violência**. Disponível em: <http://ultimosegundo.ig.com.br/brasil/2017-10-30/violencia.html>. [Acesso em: 13 de dezembro de 2017].

Matthes, E. (2016). *Curso Intensivo de Python*. Novatec Editora Ltda.

Oliveira, W. (2003). *TÉCNICAS PARA HACKERS - SOLUÇÕES PARA SEGURANÇA - Versão 2*. Centro Atlântico, Lda., Porto,Lisboa - Portugal.

Prada, R. (2017). **O que é um BUG**. Disponível em: <https://www.tecmundo.com.br/seguranca/213-o-que-e-bug-.htm>. [Acesso em: 16 de dezembro de 2017].

TecMundo (2017). **Anonymous Hackeia Associação da PF**. Disponível em: <https://www.tecmundo.com.br/seguranca/124135-anonymous-hackeia-associacao-pf-fim-da-operacao-la_va-jato.htm>. [Acesso em: 13 de dezembro de 2017].

UFSC (2017). **Diferença entre Hackers e Crackers**. Disponível em: <www.egov.ufsc.br/portal/conteudo/

saiba-diferena-entre-hackers-crackers-white-hat-black-hat_-gray-hat-entre-outros>. [Acesso em: 15 de dezembro de 2017].

Veja, A. (2017). **Com 7 casos por dia, latrocínio sobe**. Disponível em: <https://veja.abril.com.br/brasil/com-7-casos-por-dia-latrocinio-sobe-58-no-pais-em-7-anos/>. [Acesso em: 13 de dezembro de 2017].

webdevelopersnotes (2017). **What is web server**. Disponível em: <https://www.webdevelopersnotes.com/what-is-web-server>. [Acesso em: 16 de dezembro de 2017].