Jean Carvalho Ortiz

SEM TITULO
AINDA

Campo Grande, MS

21 de novembro de 2018

Jean Carvalho Ortiz

SEM TITULO
AINDA

Trabalho de Conclusão do Curso de Ciência da Computação da Faculdade de Computação na Universidade Federal de Mato Grosso do Sul, na área de Segurança em Rede.

Universidade Federal de Mato Grosso do Sul - UFMS

Faculdade de Computação - FACOM

Ciência da Computação

Orientador: Carlos Alberto da Silva

Campo Grande, MS

21 de novembro de 2018

Jean Carvalho Ortiz
SEM TITULO
AINDA/ Jean Carvalho Ortiz. – Campo Grande, MS, 21 de novembro de 2018-
43 p. : il. ; 30 cm.

Orientador: Carlos Alberto da Silva

Conclusão de Curso – Universidade Federal de Mato Grosso do Sul - UFMS
Faculdade de Computação - FACOM
Ciência da Computação, 21 de novembro de 2018.

1. Nessus. 2. Ethical Hacking. 2. Network Security. I. Carlos Alberto da Silva. II. Universidade Federal de Mato Grosso do Sul. III. Faculdade de Computação. IV. SEM TITULO AINDA

Jean Carvalho Ortiz

SEM TITULO
AINDA

Trabalho de Conclusão do Curso de Ciência da Computação da Faculdade de Computação na Universidade Federal de Mato Grosso do Sul, na área de Segurança em Rede.

Trabalho aprovado. Campo Grande, MS, 24 de novembro de 2012:

Carlos Alberto da Silva
Orientador

Professor
Convidado 1

Professor
Convidado 2

Campo Grande, MS
21 de novembro de 2018

Que a Força esteja com você.

Agradecimentos

TODO

Resumo

TODO

Palavras-chave: nessus. segurança em rede. hacking ético.

Abstract

TODO

Keywords: nessus. network security. ethical hacking.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

SO	Sistema Operacional
Kali	Kali Linux
IP	*Internet Protocol*

Sumário

Introdução

Este trabalho tem como objetivo a análise de possíveis falhas de segurança em *websites*, utilizando a ferramenta **Nessus**.
Após verificação das falhas de segurança, serão apresentadas possíveis soluções para o problema em questão, assim como possíveis modos para explorar essas falhas. Elas serão classificadas conforme o dano que pode ser causado ao sistema.

Parte I

Preparação da pesquisa

1 Kali Linux

1.1 Escolha do Sistema Operacional

Para o desenvolvimento desse estudo foi escolhido o Kali Linux como sistema operacional, pois esse SO é enriquecido com várias ferramentas para realização de *Pentests*, entre outras atividades de *hacking*.
O Kali Linux é uma distribuição GNU/Linux baseada no Debian e é um sistema *Open-Source* distribuído sob a licença **GNU GPL**. Ele é desenvolvido e mantido pela Offensive Security Ltd.

2 Nessus

2.1 Sobre o Nessus

A ferramenta utilizada nesse estudo é a Nessus Home, que é uma versão para uso pessoal e estudos, as diferenças entre a versão *Professional* é que há uma limitação de 16 endereços de IP por escaneamento, não há acesso ao suporte da ferramenta e não é possível realizar verificações de conformidade e auditoria de conteúdo.
Nessus é desenvolvido e distribuido pela Tenable Network Security, Inc e distribuído sob os termos da Licença Pública Geral GNU. Ele é composto por um cliente e um servidor, sendo o *scan* feito pelo servidor.
O *nessusd* (servidor Nessus) realiza um escaneamento e portas ao alvo e após encontrar uma porta aberta, é executado diversos scripts escritos em NASL (Nessus Attack Scripting Language) que verificam as vulnerabilidade.

2.2 Instalação

Primeiramente para realizar a instalação do Nessus Home é necessário adquirir uma licença pelo URL http://www.nessus.org/products/nessus/nessus-plugins/obtain-an-activation-code. A licença de ativação será enviada para o e-mail registrado. Após realizar o registro, é necessário fazer o *download* do pacote de instalação através da URL http://www.tenable.com/products/nessus/select-your-operating-system, selecionando o seu SO.
Na distribuição Kali, a instalação pode ser feita através do terminal, navegando até a pasta onde foi feito o *download* e executar o comando: **sudo dpkg -i Nessus-*.deb**.
Após a instalação ser concluída, o terminal irá mostrar o endereço de acesso ao Nessus, por exemplo http://kali:8834/.
Para iniciar o serviço do Nessus, basta executar no terminal o comando: **service nessusd start**, acessar o endereço que foi dado anteriormente e entrar com o código de ativação. Será executado a compilação de todos os *plugins* utilizados pela ferramenta.

2.3 Configuração

Para a realização dos testes foi realizado a criação de uma politica de *plugins*, na qual são definidos quais as vulnerabilidades que serão buscadas durante o *scan*.
Para esse estudo foi utilizado um *scan* completo do *website* utilizando todos os *plugins*

disponíveis, na qual retornam várias informações sobre a página, além de suas vulnerabilidades.

Parte II

Testes

3 Tipos de Testes

Os *plugins* utilizados nesse estudo são os seguintes:

TODO TODO

4 Resultados

5 Comparações

6 Possíveis soluções para os problemas

7 Explorando as falhas

8 Conclusão

Referências