Honeypot, uma ferramenta para auxílio na segurança de dados.

Hallef Herbeth Lisboa Vieira; Thiago Rocha Brasil

Juazeiro do Norte - CE

hallef.vieira@aluno.fapce.edu.br; thiagobrasil@gmail.com

Introdução

Este estudo de caso, faz uso de um servidor centralizado *Modern Honey Network*[1] (MHN), para coleta e gerência de dados gerados a partir de *honeypots*[2], que também podem ser chamados de sensores, com a função de simular ambientes vulneráveis dentro de uma determinada intranet de forma prática, a partir de uma interface amigável. Este servidor apresenta *scripts*[3] de instalação para diversas *Honeypots,* dentre elas: *Dionaea*, *Snort*, *Cowrie* e outras.

De acordo com Spitzner (2003), as *Honeypots* popularmente conhecidas como "potes de mel" são recursos computacionais de segurança dedicado a ser sondado, atacado ou comprometido. O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.Br) classifica as *Honeypots* em 2 categorias: Alta ou Baixa Interatividade, variando apenas a gama de recursos entre as mesmas.

A aplicação do servidor MHN foi instalada em um *Virtual Private Server*[4] (VPS) com as especificações: 30GB ssd de armazenamento interno, 2GB de memória RAM com um endereço ip estático, rodando o sistema operacional Ubuntu Server versão 18.04 x64.

Objetivos

Coletar ataques por meio de uma *honeypot* escolhida, e analisar as principais formas de comportamento dos ataques detectados, para que fique explícito o nível de inseguridade das redes, e com isso apontar como uma das ferramentas de auxílio e acompanhamento contra falhas e ataques, às *honeypots*.

Metodologia

O trabalho assume uma abordagem quantitativa e qualitativa, tratando-se de um estudo de caso realizado em uma rede isolada de um provedor específico da região do

1 Modern Honey Network: é um servidor centralizado para gerenciamento e coleta de dados de sensores, visíveis a partir de uma interface da web elegante.

2 Honeypot: É um recurso computacional que funciona como sensor de segurança dedicado a ser sondado, atacado ou comprometido.

3 Script: conjunto de instruções para que uma função seja executada em determinado aplicativo.

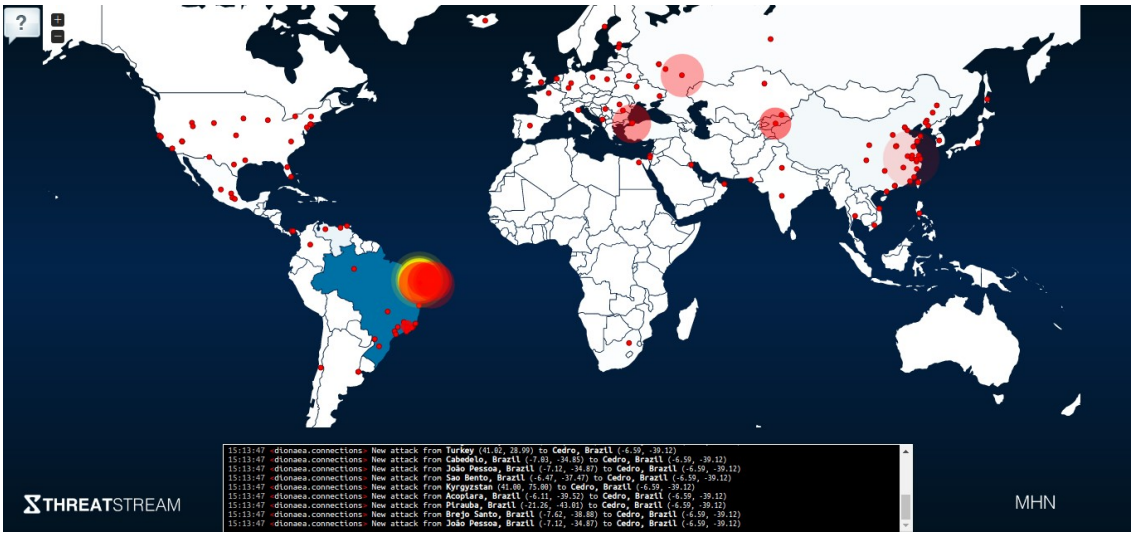
4 Virtual Private Server: é uma máquina virtual vendida como um serviço por uma empresa de hospedagem

Cariri. Onde foi necessário criar uma ferramenta de isca com quatro passos: (I) Instalar e configurar a plataforma MHN em uma máquina virtual (VPS), para armazenar os dados brutos dos sensores *honeypot* escolhidos; (II) A segunda etapa consiste em instalar e configurar os sensores Dionaea[5] para monitoramento de comandos shell e *Cowrie*[6] para monitorar ataques de força bruta; (III) A terceira etapa trata-se da instalação de uma ferramenta para interpretar e filtrar os dados brutos armazenados no servidor MHN originados dos sensores, por meio de um formato de representação de dados conhecido por JSON[7] (*JavaScript Object Notation*) baseado na linguagem javascript; (IV) A última etapa consiste em executar uma ferramenta da plataforma para agrupar e analisar os dados coletados, a fim de apontar uma fácil interpretação sobre os ataques sofridos no estudo de caso.

Resultados

Durante a execução da ferramenta, a funcionalidade *HoneyMap* exibiu em tempo real cada ataque sofrido pelas *honeypots* com um alerta em vermelho para identificar a origem no mapa, assim pode-se ver na figura 1, os países de onde são originados mais ataques.

Figura 1 - Mapa dos ataques em tempo real

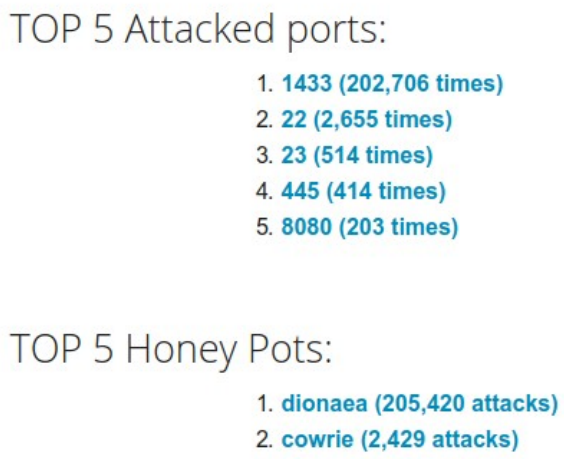


Fonte: elaboração do autor (2019)

Durante a análise da plataforma MHN, foi exibido o número de ataques que ambos os sensores sofreram e realizado um ranqueamento entre as principais portas de acesso utilizadas nos ataques como mostra na figura 2, visto que tratam-se de portas de serviços padrões como SSH, FTP, SMB, HTTP, usadas para funcionamento e troca de dados entre sistemas.

5 Dionaea: É um soft livre de detecção de intrusão voltado a códigos shell.
6 Snort: É um software livre de detecção de intrusão para rede capaz de desenvolver análise de tráfego em tempo real e registro de pacote em redes IP.
7 JSON: É um formato leve de intercâmbio de dados entre sistemas.

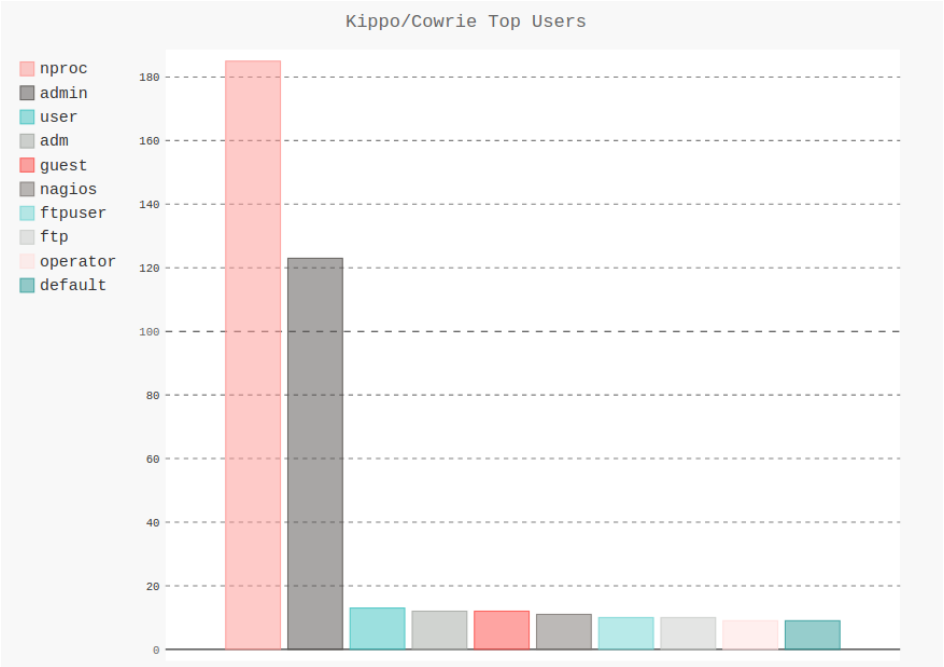
Figura 2 - Ranking de principais portas de serviço atacadas



Fonte: elaboração do autor (2019)

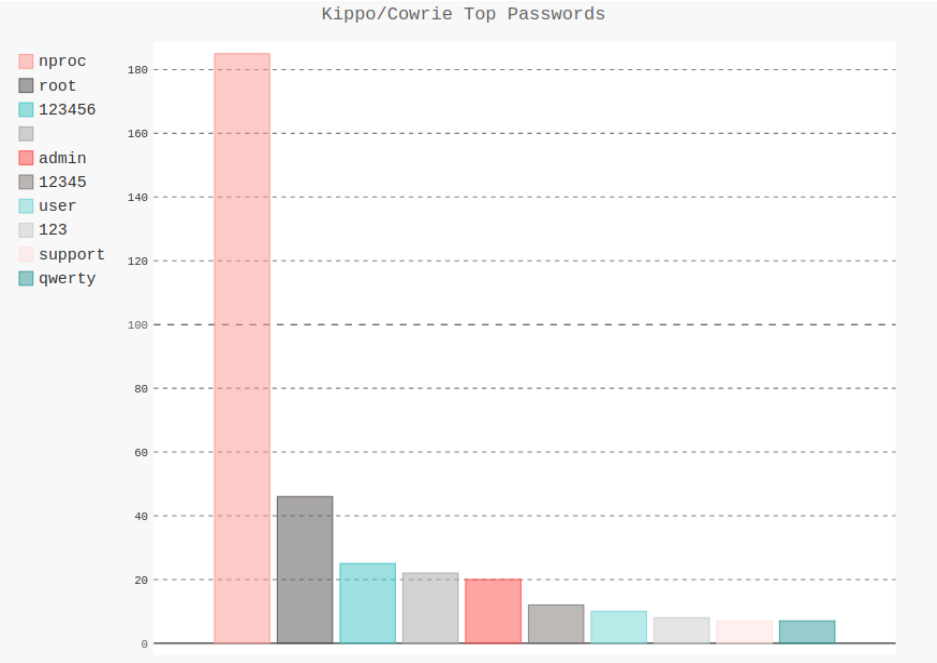
Ainda dentro da plataforma de análise, pôde-se observar um relatório gráfico informando as tentativas de invasão por força bruta com os usuários e senhas mais utilizados, como mostram as figuras 3 e 4:

Figura 3: Usuários mais utilizados durante os ataques de força bruta



Fonte: elaboração do autor (2019)

Figura 4: Senhas mais utilizadas durante os ataques de força bruta



Fonte: elaboração do autor (2019)

Desta forma, foi identificado que os países com maior índice de ataques originados são a Brasil, China, Estados Unidos e Rússia, dentre os ataques flagrados foi visto que a grande maioria das tentativas de invasões são voltados às portas 1433 e 22 responsáveis por serviços de Sql no Windows e SSH no linux respectivamente. Pôde-se observar também que por meio de ataques de força bruta, foram utilizados nomes genéricos ou palavras chaves utilizados por determinados fabricantes de hardwares e softwares.

Conclusão

Averiguamos que sensores *honeypots* para auxílio na prevenção de falhas e vulnerabilidades em redes corporativas, são essenciais para estimular a segurança da informação de forma objetiva. Intuímos que a verificação e análise de riscos podem nos ajudar no acompanhamento diário de novas ameaças a diversas intranets corporativas.

Trabalhos futuros

Futuramente pretendemos aplicar o uso de novos sensores destinados a dispositivos de Internet das coisas, para que possamos identificar os riscos e ameaças existentes aos dispositivos que vêm ganhando espaço dentro de nossas casas.

Referências

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert-Br). **Honeypots e Honeynets: Definições e Aplicações.** Disponível em: https://www.cert.br/docs/whitepapers/honeypots-honeynets/ Acesso em: 02 de Novembro de 2019 às 09:28.

Spitzner, Lance. **Honeypots: tracking hackers**. Vol. 1. Reading: Addison-Wesley, 2003.