ISSN: 2595-8402
DOI: 10.61411/rsc77405

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

GERENCIAMENTO DE AMEAÇAS DA INTERNET USANDO SISTEMAS DE HONEYPOT DE BAIXA E MÉDIA INTERATIVIDADE

Eliel Castro da Silva Junior[1]; Nikison de Assis Lima[2]; Fernando Cosme da Silva Neto[3]; Ângela Timótia Pereira Lima[4]

[1;2;3;4]FAMETRO-AM, Manaus, Brasil
elielmarolly@hotmail.com
nikisonassis@gmail.com
fcosme8@gmail.com
angela.lima@fametro.edu.br

RESUMO

O presente artigo busca apresentar sistemas que usam Honeypot de baixa e média interatividade, como o Dionaea e o Cowrie, para o gerenciamento de ameaças da internet, além de mostrar como configurar o ambiente de ambos. Tem como objetivo final gerar um protótipo de um site informativo sobre o assunto tratado usando como metodologia a pesquisa bibliográfica. Foi utilizada a ferramenta VISUAL STUDIO CODE (VSCODE) com a linguagem de programação JAVAScript, além da parte visual do protótipo ser feita em HyperText Markup Language (HTML), Cascading Style Sheets (CSS) e o framework BOOTSTRAP.

PALAVRAS-CHAVE: Honeypot, Internet, Segurança.

1 INTRODUÇÃO

Os ataques cibernéticos estão se adaptando e evoluindo com os avanços tecnológicos, o que é uma grande preocupação. Phishing, cripto trojans e fraudes cibernéticas são alguns dos ataques mais perigosos e comuns realizados por hackers. Eles buscam explorar e lucrar com as informações confidenciais dos usuários. [1]. Um exemplo notório de ransomware é o WannaCry Ransomware. Esse malware pode restringir o acesso do usuário aos seus arquivos ou sistemas, criptografando o

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

dispositivo e exigindo um resgate para liberá-lo. A vítima só recupera o acesso depois de pagar pelo resgate e obter a chave de descriptografia. [2].

O malware na web é uma ameaça persistente e mutável, tanto em termos de formas de disseminação quanto de tecnologia de software. Com o surgimento de novos ataques e variações nas ameaças, o malware pode prejudicar o desempenho dos sistemas. [2]

Segundo VS DeviPriya e S. Sibi Chakkaravarthy [1] descreveu que baseado no Relatório da IBM, o custo médio de uma violação de dados tem crescido constantemente. Em 2021, o custo médio era de 4,24 milhões de dólares, que aumentou 2,6% para 4,35 milhões de dólares em 2022. Isso representa um aumento de 12,7% em relação ao custo médio de 3,86 milhões de dólares relatado em 2020. A análise de segurança é a principal forma de antecipar e se preparar para esses ataques. Isso se deve à grande quantidade de dados de ataque que ainda não foram analisados e utilizados de forma eficiente. Segundo Sathiyandrakumar, Srinivasan; P, Deepalakshmi [2], a implementação de sensores de segurança, como o Honeypot, é uma estratégia eficaz para coletar dados de ataque que podem ser usados para identificar malwares.

Um honeypot oferece aos times de segurança cibernética uma visão mais ampla, permitindo que eles se defendam contra-ataques que até mesmo um firewall pode não conseguir bloquear. Várias instituições ao redor do mundo usam honeypots como uma camada extra de proteção para combater riscos internos e externos. Um honeypot, ou isca digital, atrai invasores para um alvo falso. Ele é um sistema de computador projetado para ser atacado, funcionando como uma distração para desviar ataques cibernéticos. Ele simula alvos reais de phishing e usa técnicas de infiltração para obter informações sobre os invasores e seus métodos, ou para proteger seus verdadeiros objetivos. Os sistemas honeypot são muito eficientes na coleta de dados e podem incluir detecção de intrusão baseada em assinaturas, captura de tráfego e análise de protocolo de Internet, além de filtragem adaptativa e ajuste fino. [1]

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

O objetivo deste artigo é apresentar a tecnologia Honeypot no gerenciamento de ameaças da internet com um tutorial de como configurar e usar duas aplicações chamadas Dionaea e Cowrie além da apresentação de um protótipo de site desenvolvido para uma melhor compreensão do tema.

2 REFERENCIAL TEÓRICO

Um dos primeiros usos de um honeypot foi em 1986. Conforme descrito no livro de Clifford Stoll, , The Cuckoo's Egg, na época em que ele era administrador de sistemas da US Berkeley o mesmo notou que alguém estava acessando o sistema frequentemente com privilégios de superusuário. Para tentar identificar esse invasor, Stoll criou duas armadilhas em forma de honeypot. Consistindo em conectar terminais emprestados a todas as linhas telefônicas de entrada no sistema e depois esperar que o invasor desconhecido ligasse. Essa estratégia permitiu que eles descobrissem exatamente o que o invasor estava procurando e ele até caiu em um departamento inventado. Isso levou à prisão de um alemão que trabalhava para a KGB e marcou a primeira operação bem-sucedida de honeypot. [3]

Os honeypots podem ser classificados em dois tipos, que são Honeypots de Pesquisa e de Produção. O objetivo principal de um honeypot de pesquisa é analisar como os agentes maliciosos realizam seus ataques e ver a variedade de técnicas que eles usam. Canner explica isso como uma plataforma para observar as técnicas de invasão usadas pelos invasores para acessar sistemas, aumentar privilégios e depois se infiltrar no sistema ou na rede. Esses honeypots são geralmente configurados por acadêmicos, pesquisadores de segurança, órgãos governamentais e empresas de segurança para avaliar e medir o cenário de riscos. Essa atividade fornece dados que podem ser examinados e usados para descobrir as táticas, técnicas e procedimentos dos agentes da ameaça. [3]

Os honeypots de produção usam uma infraestrutura mais específica e configurada com precisão para mitigar ataques atuais ou potenciais contra uma

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

organização . Eles são implantados próximos à infraestrutura de produção atual da organização e seguem uma arquitetura de segurança semelhante. Essa abordagem faz com que o honeypot pareça quase idêntico aos outros serviços da empresa para atrair um invasor, em vez dos serviços legítimos. Os serviços simulados são geralmente configurados para sistemas operacionais e serviços parecidos com portas padrões. Isso permite que ocorra a coleta de dados para analisar qual aspecto da infraestrutura falhou e por que um ataque foi bem-sucedido. Esses honeypots também podem ser úteis para distinguir entre ataques automatizados e ataques manuais conduzidos por humanos, o que possibilitará a criação de um modelo de ameaça mais realista. [3]

Os honeypots oferecem diferentes níveis de interação, que são baixo, médio e alto, o que reflete o quanto um invasor pode interagir com os serviços e respostas recebidas pelos honeypots. Um honeypot de baixa interação é capaz de simular serviços, suportar protocolos de rede e os principais recursos básicos que um sistema operacional real possui. Ele fornece ao invasor a quantidade mínima de informações para despertar seu interesse em realizar um ataque e suas ações serão registradas. [3]

No entanto, como Naik e Jenkins discutem, eles não fornecem proteção contra ataques de falsificação, ao contrário de níveis de interação mais elevados, devido à capacidade limitada das respostas que o honeypot pode retornar. [3]

Um honeypot de interação média combina os aspectos mais fortes das contrapartes de baixa e alta interação. Com isso, ele poderia obter uma melhor compreensão dos ataques, oferecendo um pouco mais de interação por meio de respostas e simulação de nível de serviço do que os honeypots de interação de baixo nível. A diferença entre interação média e alta é o nível de risco associado. Esse tipo de honeypot é executado na camada de aplicativo virtual e, portanto, não simula totalmente um ambiente de sistema operacional. Em vez disso, ele simula uma camada de aplicativo para registrar conexões, como honeypots de interação de baixo nível, mas também oferece mais interação. Por exemplo, pode ir tão longe quanto baixar qualquer amostra de malware sem o risco de afetar o resto do sistema . [3]

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

3 METODOLOGIA

Para este artigo foi realizada uma pesquisa bibliográfica envolvendo o estudo através de artigos, teses e publicações da área de tecnologia, visando aprofundar o conhecimento e potencialmente contribuir para a resolução de problemas conhecidos neste campo de atuação.

A coleta de estudos foi realizada entre setembro e novembro de 2023, utilizando o banco de dados Directory of Open Access Journals (DOAJ). Os critérios de inclusão foram: artigos originais publicados nos anos de 2021, 2022 e 2023; selecionado o assunto de Tecnologia; ordenado pelos artigos publicados recentemente no DOAJ e que abordam a temática em questão.

Os critérios de exclusão foram: estudos que não estão disponíveis na íntegra; artigos que não têm correlação com o tema; que não estão dentro do período selecionado e estudos repetidos. Os descritores utilizados para a coleta de dados foram: honeypot, segurança da informação e internet.

Para o desenvolvimento do protótipo de site foram utilizadas a ferramenta VISUAL STUDIO CODE (VSCODE)[4] com a linguagem de programação JAVAScript [5], além da parte visual ser feita em HyperText Markup Language (HTML)[6], Cascading Style Sheets (CSS)[7] e o framework BOOTSTRAP [8].

4 RESULTADOS E DISCUSSÃO

Nesta sessão foi utilizado o Dionaea que é um software livre que cria armadilhas virtuais como o Honeypot para atrair e capturar possíveis invasores na rede. Ele simula vários serviços de rede comuns, como Hypertext Transfer Protocol (HTTP)[9], File Transfer Protocol (FTP)[10], Simple Mail Transfer Protocol (SMTP)[11] e outros, para assim coletar dados sobre quem tenta acessá-los. Esses dados incluem o endereço IP e a localização do invasor, o nome de usuário e senha usados, o momento e a frequência das tentativas de conexão e os arquivos que foram enviados ou recebidos.[3]

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

4.1 CONFIGURANDO O AMBIENTE HONEYPOT DIONAEA

4.1.1 PRÉ-REQUISITOS:

Fazer o download da ferramenta Dionaea através do site https://dionaea.readthedocs.io/en/latest/ [12]

Download Ubuntu Server 18.04 no site ubuntu.com. [13]

É recomendado usar um Virtual Private Server (VPS) público para usar o Honeypot.

Os comandos utilizados nesta seção são padrões utilizados seguindo a sintaxe da linguagem de programação e do ambiente do Linux e foram utilizados baseados no site Kroland.no [14].

4.1.2 INSTALAÇÃO:

No console, será mudado para o usuário root.

($ su)

Foram feitas as atualizações do sistema utilizando os comandos abaixo.

($ apt-get update)
($ apt-get install sudo git)
($ /sbin/usermod -aG sudo SEU_NOME DE USUÁRIO)
($ /sbin/reboot)

Foram utilizados os códigos abaixo para baixar o código fonte.

($ cd ~)
($ git clone https://github.com/DinoTools/dionaea.git)
($ cd dionaea)

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Depois foram baixadas as dependências que serão necessárias copiando o código abaixo.

```
( $ sudo apt-get install \ )
( build-essential \ )
( cmake \ )
( check \ )
( cython3 \ )
( libcurl4-openssl-dev \ )
( libemu-dev \ )
( libev-dev \ )
( libglib2.0-dev \ )
( libloudmouth1-dev \ )
( libnetfilter-queue-dev \ )
( libnl-3 -dev \ )
( libpcap-dev \ )
( libssl-dev \ )
( libtool \ )
( libudns-dev \ )
( python3 \ )
( python3-dev \ )
( python3-bson \ )
( python3-yaml \ )
( python3-boto3 \ )
( fonts-liberation )
```

Ao instalar as dependências, foi criado um diretório de construção e usando o *CMake* foi configurado o processo de construção.

```
( $ sudo mkdir build )
```

```
( $ cd build )
```

```
( $ sudo cmake -DCMAKE_INSTALL_PREFIX:PATH=/opt/dionaea .. )
```

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Foi utilizado o comando *make* para construir e *make install* para instalar em nosso sistema.

($ sudo make)
($ sudo make install)

Depois disso o Dionaea foi instalado e disponibilizado em "*>opt>dionaea*"

4.1.3 CONFIGURAÇÕES:

Ao configurar o Dionaea, 4 pastas principais estarão disponíveis (ihandlers_available, ihandlers_enabled, services_available e services_ enabled) e um arquivo (dionaea.cfg).

4.1.4 IHANDLERS (REGISTRO)

Quando recebemos uma cópia do malware que foi enviado ao nosso Honeypot, precisamos tratar o tráfego de alguma forma. Para isso, usamos os plug-ins do ihandler. Eles estão localizados em duas pastas em "(opt/dionaea/etc/dionae)": "(ihandlers/available)" e "(ihandlers/enabled)". A pasta "(ihandlers/available)" contém os diferentes plug-ins que podemos ativar para o Dionaea, e a pasta "(ihandlers-enabled)" contém links simbólicos que apontam para os arquivos de configuração na pasta "ihandlers-available". Se criarmos um link simbólico, o plug-in correspondente será ativado.

4.1.5 SERVIÇOS

As pastas de serviço funcionam de forma semelhante às pastas ihandlers. Elas são duas: uma com os protocolos que podem ser imitados pelo Dionaea, e outra com os links simbólicos que ativam os protocolos desejados. O nosso Honeypot será configurado para imitar os protocolos HTTP e HTTPS, MYSQL e SMB.

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Revista Sociedade Científica

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

4.1.6 DIONAEA.CFG

Neste arquivo, configuramos o Dionaea. Ele vem com vários protocolos ativados por padrão, mas nós só queremos usar HTTP ou HTTPS, o MYSQL e SMB. Então, podemos remover os outros protocolos que não nos interessam. Para fazer isso basta excluir os links simbólicos na pasta de serviços.

($ cd /opt/dionaea/etc/dionaea/services-enabled)
($ sudo rm blackhole.yaml epmap.yaml ftp.yaml memcache.yaml mirror.yaml mongo.yaml mqtt.yaml mssql.yaml pptp.yaml sip.yaml tftp.yaml upnp.yaml printer.yaml)

Para gerenciar o Dionaea de forma facilitada, vamos deixar ele executado como um serviço em segundo plano usando o comando *systemd*.
Criamos um arquivo em "*etc>systemd>system*"

($ sudo nano /etc/systemd/system/dionaea.service)

Digitamos o código abaixo.

([Unit]Description = making network connection up)
(After = network.target)
([Service])
(ExecStart = /opt/dionaea/bin/dionaea)
([Install])
(WantedBy = multi-user.target)

Agora deve iniciar o Dionaea usando o comando *systemctl*.

($ systemctl start dionaea)

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Para reiniciar utilizar:

```
( $ systemctl restart dionaea )
```

Para parar utilizar:

```
( $ systemctl stop dionaea )
```

Para mostrar o Status atual do Dionaea:

```
( $ systemctl status dionaea )
```

Habilitar o Dionaea para iniciar na inicialização:

```
( $ systemctl enable dionaea )
```

4.2 GERENCIAMENTO DA REDE COM COWRIE

Cowrie é um honeypot de código aberto que simula um servidor SSH e um protocolo Telnet para capturar e analisar as ações dos invasores. SSH e Telnet são protocolos de rede que permitem o acesso remoto a computadores. Com o Cowrie, podemos obter informações sobre os invasores, como o seu endereço IP e localização, o seu nome de usuário e senha, o seu tempo e frequência de conexão e o seu comando de entrada. [3]

4.3 CONFIGURANDO O AMBIENTE HONEYPOT COWRIE

4.3.1 PRÉ-REQUISITOS:

Download do Ubuntu Server no site ubuntu.com[13]

É recomendado usar um Virtual Private Server (VPS) público para usar o Honeypot.

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Cowrie é um honeypot de código aberto que não exige muitos recursos técnicos para funcionar. Ele pode ser instalado em qualquer dispositivo com um Shell Linux e uma rede. Uma opção é usar um servidor virtual privado (VPS), que é uma máquina virtual oferecida por um provedor de hospedagem. Assim, o honeypot fica na porta 22, que é vulnerável e exposta à Internet. Foi utilizado o Debian, uma distribuição Linux estável e segura para desktop e servidor. Outra opção é instalar o honeypot em uma rede local (LAN), para detectar invasões e tentativas de acesso nessa rede. [15]

Os comandos utilizados neste artigo são padrões utilizados seguindo a sintaxe da linguagem de programação e do ambiente do Linux e foram utilizados baseados no site null-byte.wonderhowto.com [15].

4.3.2 PREPARANDO-SE PARA A INSTALAÇÃO DO COWRIE:

Atualizamos o sistema usando seu console com o código abaixo.

```
( sudo apt-get update && sudo apt-get upgrade )
```

Instalamos as dependências do Cowrie com este comando.

```
( sudo apt-get install git python-virtualenv libssl-dev libffi-dev build-essential libpython-dev python2.7-minimal authbind )
```

Movemos o Serviço SSH real para uma porta diferente.

```
( sudo nano /etc/ssh/sshd_config )
```

Escolhemos um número diferente de 22 e colocamos depois de “Port”. Se a linha começar com “#”, apagamos esse símbolo para ativar a configuração.
Depois que as alterações forem feitas no arquivo, elas podem ser salvas no Nano pressionando Ctrl + O e saindo do Nano com Ctrl + X .

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Após a alteração da configuração SSH, o serviço pode ser reiniciado com systemd usando o comando abaixo.

```
( sudo systemctl restart ssh )
```

Para se conectar à nossa máquina honeypot remotamente ou em um VPS, usamos o SSH com a opção -p e o número que você colocou depois de “Port”. Por exemplo, se você tivéssemos usado 9022, o comando seria assim, com o endereço do servidor no final:

```
( ssh-p9022 )
```

4.3.3 INSTALANDO O COWRIE

A primeira etapa do processo de instalação é criar uma nova conta de usuário especificamente para o Cowrie.Podemos fazer isso com o comando *adduser*. Assim criando um usuário sem senha e com o nome de usuário “cowrie”.

```
( sudo adduser --disabled-password cowrie )
```

Podemos fazer login nesta nova conta de usuário usando *sudo su.*

```
( sudo su - cowrie )
```

Copiamos o código-fonte do Cowrie na pasta inicial desta nova conta de usuário usando o Git.

```
( git clone https://github.com/micheloosterhof/cowrie )
```

Agora podemos ir para a pasta cowrie com o comando *cd.*

```
( cd cowrie )
```

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Dentro deste diretório, podemos criar um ambiente virtual para a ferramenta executando o comando abaixo.

```
( virtualenv cowrie-env )
```

Podemos então ativar este novo ambiente virtual.

```
( source cowrie-env/bin/activate )
```

A partir daqui, podemos usar o Pip para instalar requisitos adicionais. Primeiro, atualizamos o Pip com o seguinte comando.

```
( pip install --upgrade pip )
```

O arquivo **requirements.txt** incluído no Cowrie é usado como referência para as dependências do Python para instalação do Pip.

```
( pip install --upgrade -r requirements.txt )
```

A configuração do Cowrie é definida em dois arquivos, cowrie.cfg.dist e cowrie.cfg. Por padrão, apenas cowrie.cfg.dist é incluído quando a ferramenta é baixada, mas quaisquer configurações definidas em cowrie.cfg terão prioridade.

Para tornar a configuração um pouco mais simples, podemos criar uma cópia de cowrie.cfg.dist e usá-la para criar cowrie.cfg, de forma que haja um backup do arquivo original. Podemos fazer isso usamos o comando cp.

```
( cp cowrie.cfg.dist cowrie.cfg )
```

Podemos editar este arquivo de configuração no Nano executando nano **cowrie.cfg** no console. A primeira configuração que pode valer a pena alterar é o nome do host do honeypot. Em seguida, "listen_port" deve ser definido como "22" em vez de "2222", de modo que sejam permitidas tentativas de conexão na porta SSH padrão.

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Revista Sociedade Científica

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Agora podemos fazer outras alterações no arquivo, salvá-las com **Ctrl + O** e sair do Nano com **Ctrl + X**.

Depois que o arquivo for salvo, também podemos atualizar a configuração de roteamento de porta do sistema ajustando o comando abaixo.

```
( iptables -t nat -A PREROUTING -p tcp --dport 22 -j REDIRECT --to-port 2222 )
```

Agora iniciamos o Cowrie executando na pasta Cowrie.

```
( bin/cowrie start )
```

O honeypot está em execução! Também é podemos pará-lo com o código abaixo.

```
( bin/cowrie stop )
```

4.4 PROTÓTIPO DE SITE

Para o desenvolvimento do protótipo foi modelado um diagrama de sequência apresentando o fluxo de telas do protótipo site, conforme ilustrado na Figura 1.

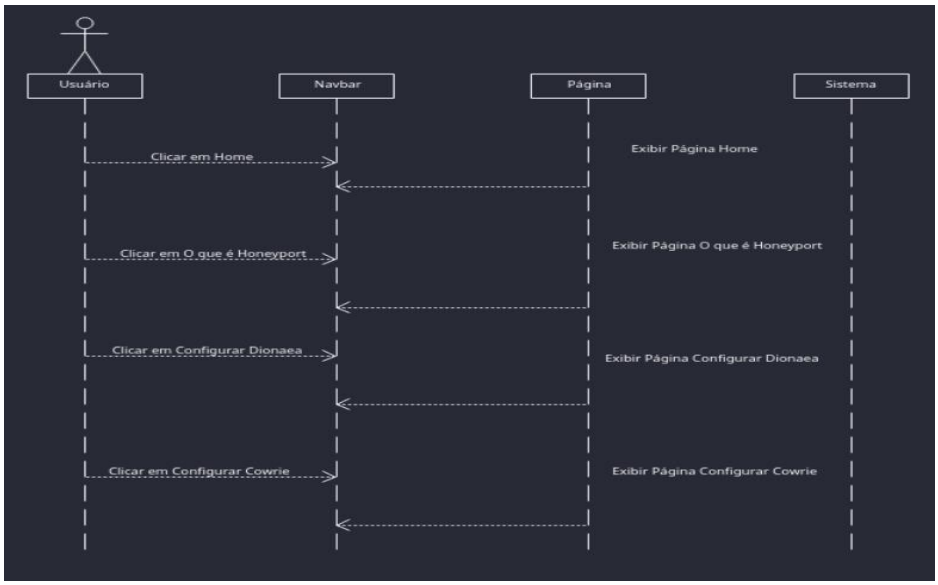

Figura 1 - Diagrama de Sequência

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Revista Sociedade Científica

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

O protótipo de site foi desenvolvido através da ferramenta VSCODE que permitiu a sua criação com informações sobre o método Honeypot, a Figura 2 ilustra a tela inicial exibindo o seu conceito.

Figura 2 - Tela Inicial do protótipo do site

Na Figura 3 é apresentado o software Dionaea e em seguida os primeiros passos a seguir.

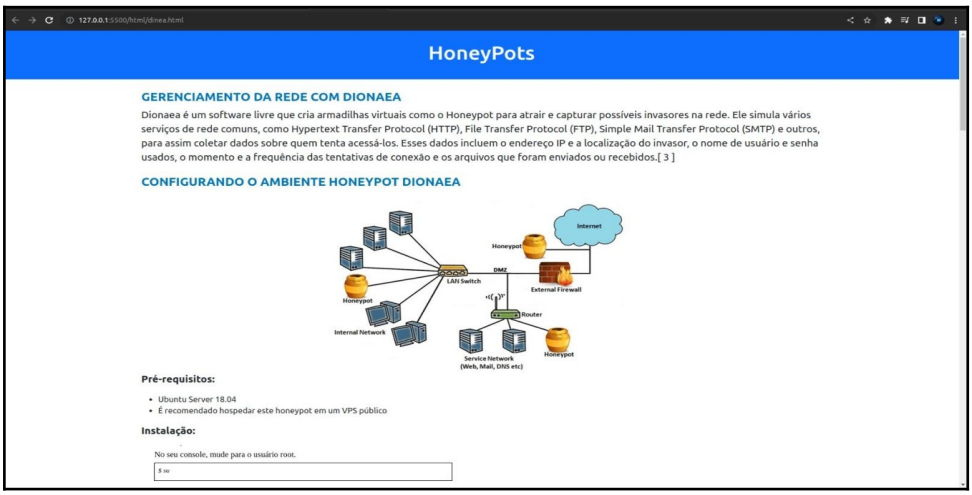

Figura 3 - Gerenciamento da Rede com Dionaea e Configuração do Ambiente, parte 1

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Revista Sociedade Científica

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Na Figura 4 é dado a continuação no passo-a-passo de como configurar o ambiente usando um padrão de comandos.

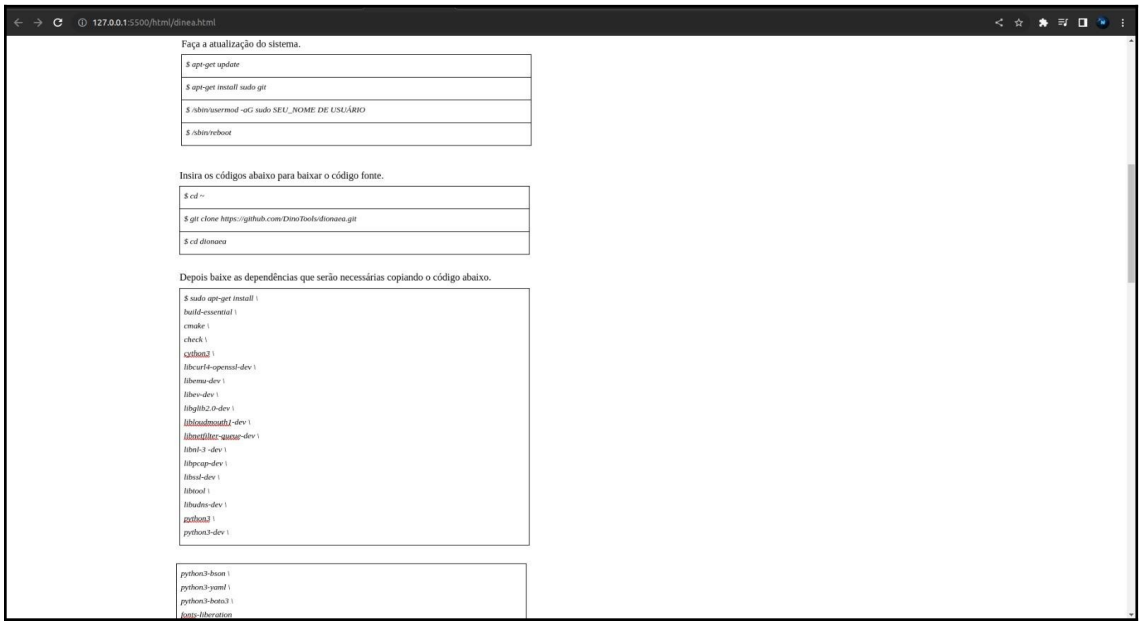

Figura 4 - Configurando o Ambiente Dionaea, parte 2

Na Figura 5 as dependências são apresentadas e o comando *Make*.

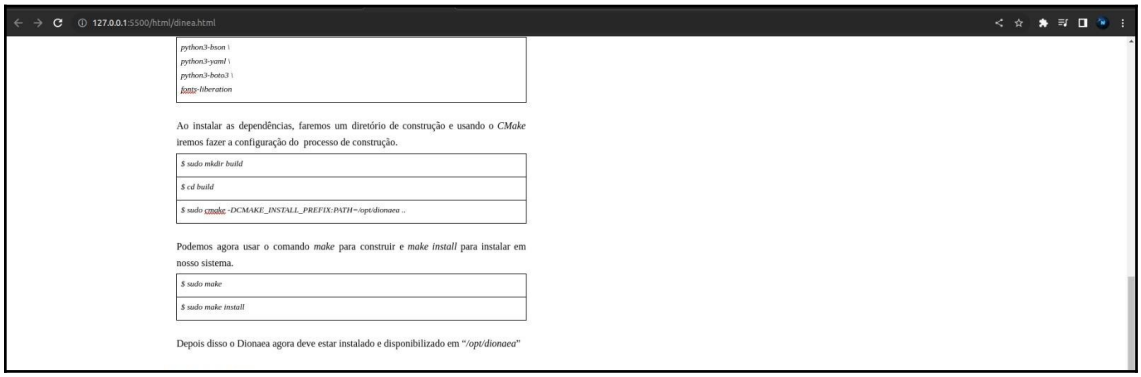

Figura 5 - Configurando o Ambiente Dionaea, parte 3

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Revista Sociedade Científica

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Na Figura 6 é apresentado um diagrama de como funcionaria o método Honeypot aplicado em uma rede e em seguida alguns conceitos usados como o de Serviços.

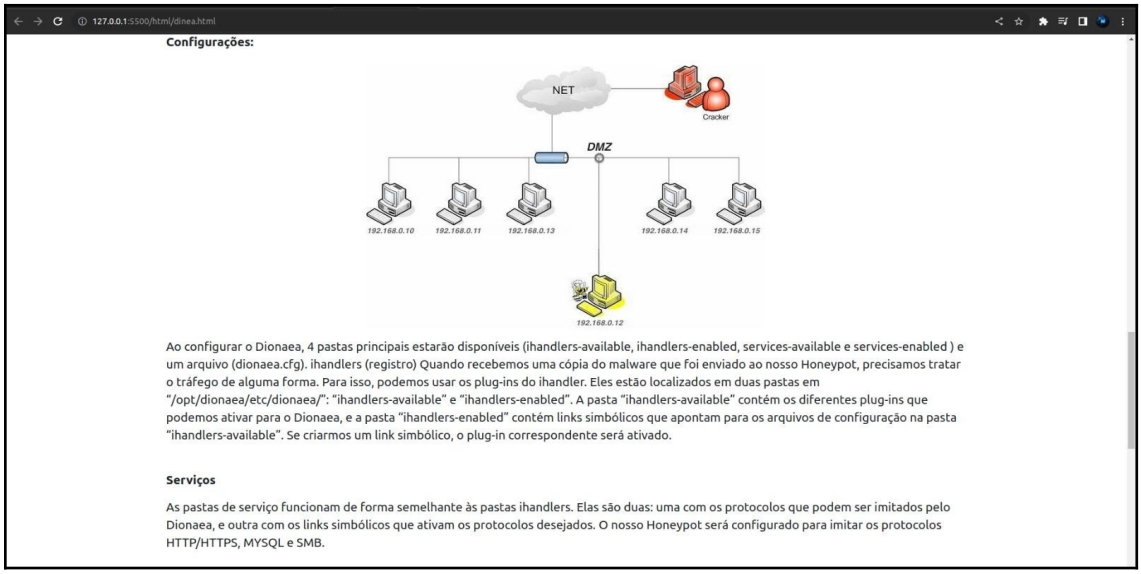

Figura 6 - Configurando o Ambiente Dionaea, parte 4

A Figura 7 continua a apresentar conceitos e em seguida é dado a continuação no passo-a-passo de como configurar protocolos a serem usados.

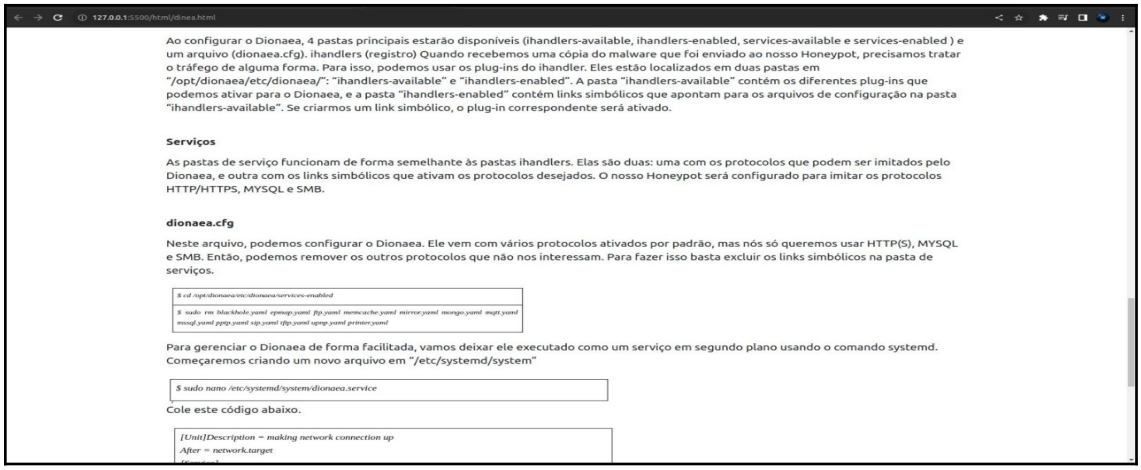

Figura 7 - Configurando o Ambiente Dionaea, parte 5

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Revista Sociedade Científica

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Na Figura 8 é apresentado códigos para algumas funções como reiniciar, parar, mostrar status e habilitar para iniciar na inicialização.

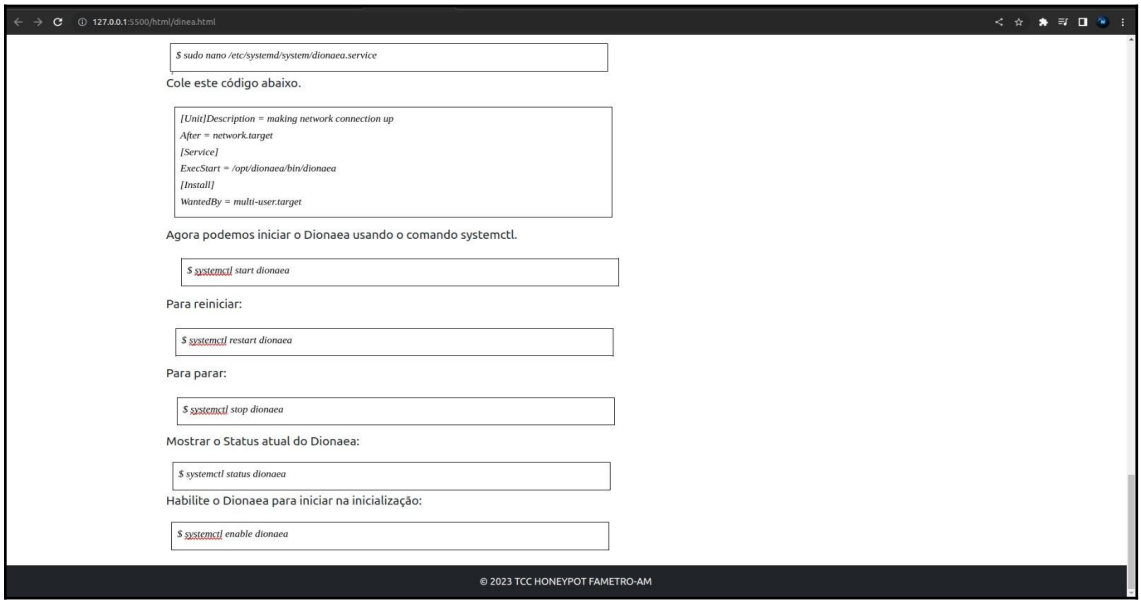

Figura 8 - Configurando Ambiente Dionaea, parte 6

A Figura 9 apresenta o conceito do software Cowrie e sua configuração de ambiente.

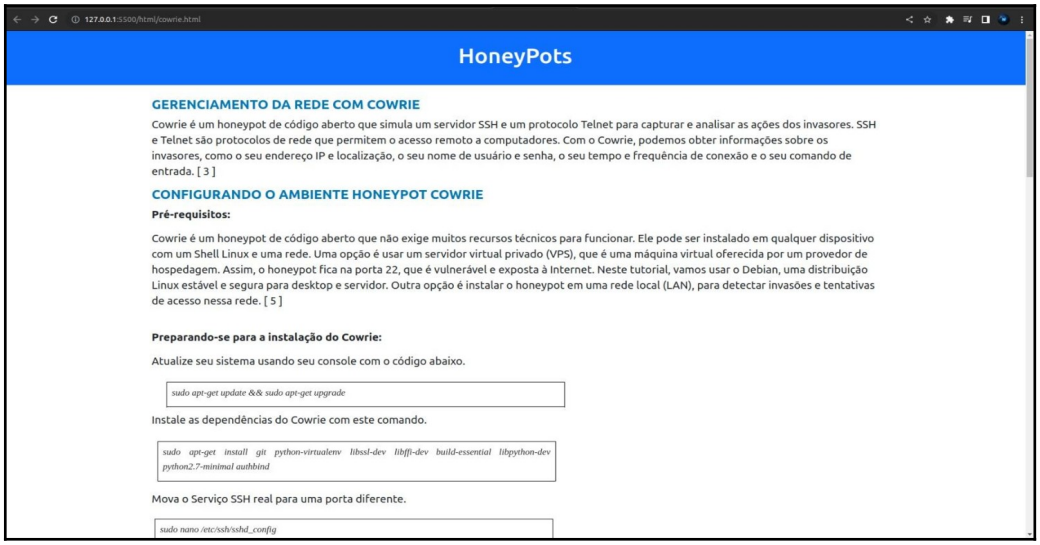

Figura 9 - Cowrie e Configuração do Ambiente, parte 1

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Revista Sociedade Científica

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Na Figura 10 a configuração da máquina remota ou VPS é configurada e a criação de uma nova conta de usuário no ambiente.

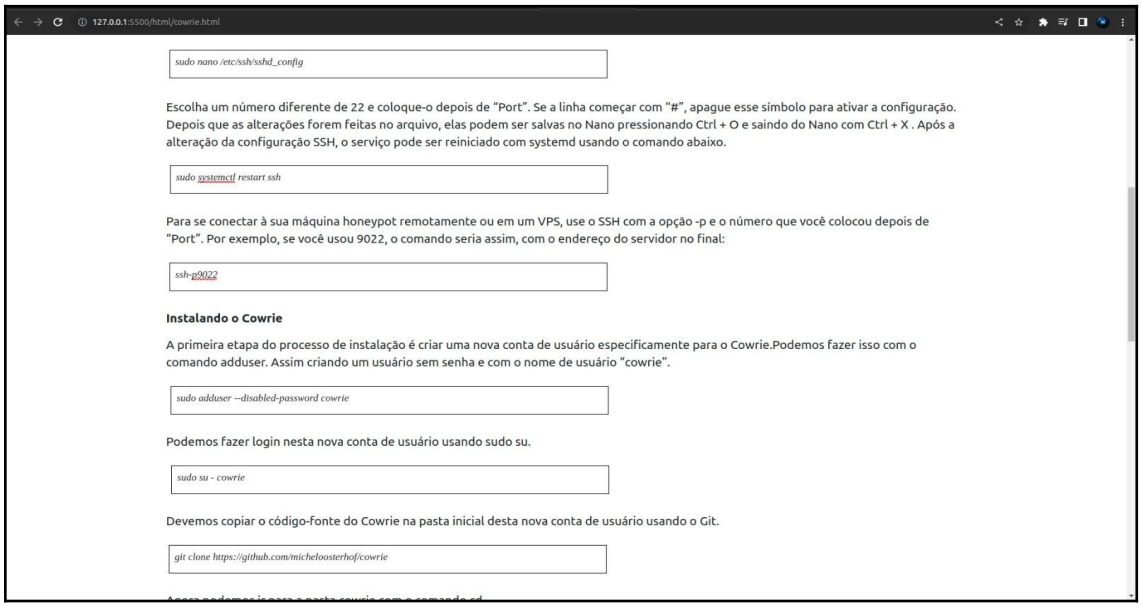

Figura 10 - Configuração do Ambiente Cowrie, parte 2

A Figura 11 mostra a criação do ambiente virtual no Cowrie.

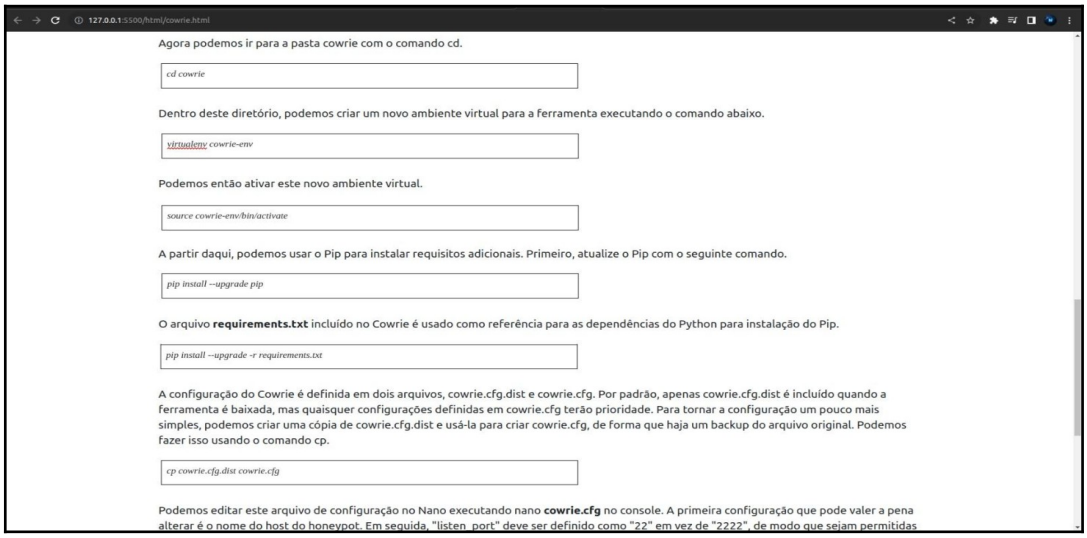

Figura 11 - Configuração do Ambiente Cowrie, parte 3

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Revista Sociedade Científica

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Na Figura 12 é apresentada a configuração por arquivos do Cowrie.

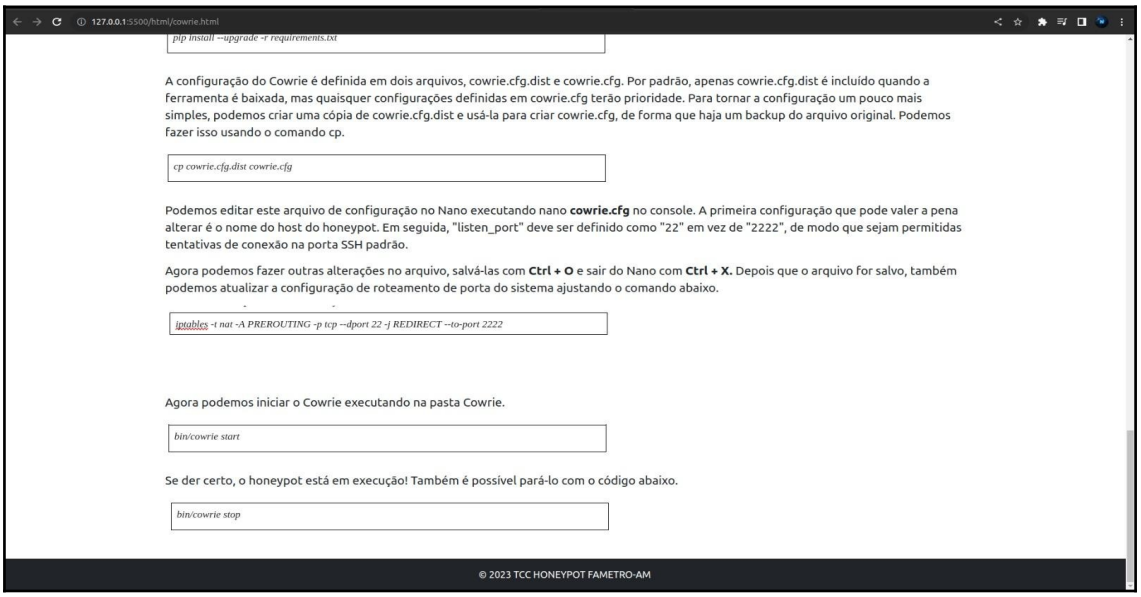

Figura 12 - Configuração do Ambiente Cowrie, parte 4

A Figura 13 apresenta uma parte do código-fonte usado para criar o protótipo do site.

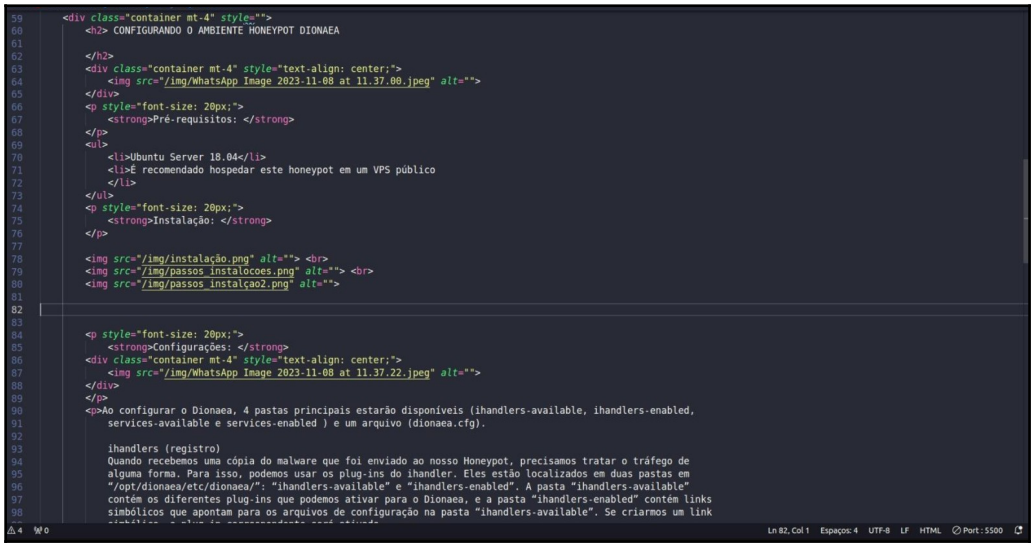

Figura 13 - Código-fonte do site em HTML e CSS

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Dessa forma foi possível apresentar a usabilidade e aplicação das ferramentas que usam Honeypot.

5 CONSIDERAÇÕES FINAIS

Através deste artigo foi atingido o objetivo de apresentar a tecnologia Honeypot assim como mostrar a configuração das aplicações Dionaea e Cowrie, além da criação do protótipo do site.

No decorrer da configuração foi constatada uma certa dificuldade ao lidar com códigos do sistema Ubuntu, já que os membros da equipe estão acostumados com códigos de outras linguagens como o sistema Windows.

Conclui-se que ao usar o Honeypot para a assegurar a rede de internet é eficaz no levantamento de dados sobre ataques que possam ocorrer, já que ao configurar o ambiente cria-se uma forma de gerar informações úteis. Em um mundo cada vez mais evoluído e tecnológico dar-se necessária a eterna vigilância para assim combater crimes cibernéticos e buscar amenizar essa situação.

6 REFERÊNCIAS BIBLIOGRÁFICAS

[1] V. S. Devi, Priya ; S. Sibi, Chakkaravarthy. **Containerized cloud-based honeypot deception for tracking attackers.** Scientific Reports, volume 13, Article number: 1437; 25, January 2023

[2] Sathiyandrakumar, Srinivasan; P, Deepalakshmi. **Enhancing the security in cyber-world by detecting the botnets using ensemble classification based machine learning.** Sciencedirect, Measurement: Sensors, Volume 25, February 2023.

[3] Yang, Xingyuan; Jie, Yuan; Yang, Hao; Kong, Ya; Zhang, Hao; Zhao, Jinyu. **A Highly Interactive Honeypot-Based Approach to Network Threat Management**. MDPI-Future Internet, Volume 15, Number 127, 2023

[4] Visual Studio Code. **Visual Studio Code - Code Editing. Redefined**. Disponível em: <https://code.visualstudio.com/>. Acesso em: 21, Novembro de 2023.

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Revista Sociedade Científica

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

[5] Redação XPEducação.**O que é JavaScript? Saiba onde ela é utilizada na tecnologia**. 16, Junho de 2023. Disponível em: <https://blog.xpeducacao.com.br/o-que-e-javascript/?gad_source=1&gclid=CjwKCAiAx_GqBhBQEiwAlDNAZtNL9yj5BgYUep02x5cmMDlI95R3wFpNXtC8vPrUXjrXJYWs4tfGcxoCNBAQAvD_BwE>. Acesso em: 21, Novembro de 2023.

[6] Redação XPEducação**. O que é HTML, para que serve e sua importância**. 16, Junho de 2023. Disponível em: <https://blog.xpeducacao.com.br/o-que-e-html/?gad_source=1&gclid=CjwKCAiAx_GqBhBQEiwAlDNAZi_UUz5SUmpK2gR8nGs5ct8SEjjGYMov8nhnxz8pn7ENxaT8pfNOKRoCwG8QAvD_BwE>. Acesso em: 21, Novembro de 2023.

[7] Ariane G. **O que é CSS? Guia Básico para Iniciantes**. Disponível em: <https://www.hostinger.com.br/tutoriais/o-que-e-css-guia-basico-de-css>. Acesso em: 21, Novembro de 2023.

[8] Andrei L. **Desvendando o Bootstrap: O Que É e Como Usar?**. 28, Julho de 2023. Disponível em: <https://www.hostinger.com.br/tutoriais/o-que-e-bootstrap>. Acesso em: 21, Novembro de 2023.

[9] Rafael-Nercessian. **Qual é a diferença entre HTTP e HTTPS?**. 16, Junho de 2023. Disponível em: <https://www.alura.com.br/artigos/qual-e-diferenca-entre-http-e-https?utm_term=&utm_campaign=%5BSearch%5D+%5BPerformance%5D+-+Dynamic+Search+Ads+-+Artigos+e+Conte%C3%BAdos&utm_source=adwords&utm_medium=ppc&hsa_acc=7964138385&hsa_cam=11384329873&hsa_grp=111087461203&hsa_ad=681579447483&hsa_src=g&hsa_tgt=aud-456779235754:dsa-843358956400&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=CjwKCAiAx_GqBhBQEiwAlDNAZk0o4N0q4T9ZcQGEwxCOPZHO-5YT5B8tu_94KEQjncvSeJA2owqVXRoCdOUQAvD_BwE>. Acesso em: 21, Novembro de 2023.

[10] Ronaldo Gogoni. **O que é FTP? – Tecnoblog**. Disponível em: <https://tecnoblog.net/responde/o-que-e-ftp/>. Acesso em: 21, Novembro de 2023.

[11] KingHost. **O que é SMTP? Entenda mais sobre o protocolo e como ele funciona**. 20, Dezembro de 2022. Disponível em: <https://king.host/blog/solucoes-marketing/o-que-e-smtp/>. Acesso em: 21, Novembro de 2023.

ISSN: 2595-8402
DOI: 10.61411/rsc77405

Publicado em 14 de dezembro de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

[12] Dionaea. **Welcome to dionaea's documentation! — dionaea 0.11.0 documentation**. Disponível em: <https://dionaea.readthedocs.io/en/latest/>. Acesso em: 21, Novembro de 2023.

[13] Ubuntu. **Get Ubuntu Server | Download. Ubuntu**. Disponível em: <https://ubuntu.com/download/server/choose>. Acesso em: 21, Novembro de 2023.

[14] Kroland. **Dionaea - Setting up a Honeypot environment (Part 2)**. Disponível em:<https://kroland.no/2019/10/14/dionaea-setting-up-a-honeypot-environment-part-2/>. Acesso em: 08, Novembro de 2023.

[15] TAKHION. **Use the Cowrie SSH Honeypot to Catch Attackers on Your Network**. Wonder How To Null Byte. 01, Maio de 2018. Disponível em: <https://null-byte.wonderhowto.com/how-to/use-cowrie-ssh-honeypot-catch-attackers-your-network-0181600/>. Acesso em: 08, Novembro de 2023.